



MARINHA DO BRASIL

**DIRETORIA DE COMUNICAÇÕES E TECNOLOGIA
DA INFORMAÇÃO DA MARINHA**

31/010

Rio de Janeiro, RJ, 31 de outubro de 2023.

DCTIMARINST N° 31-07

Assunto: Auditoria de Segurança da Informação na Marinha do Brasil

Referência: DGMM-0540 (3ª Revisão).

Anexos: A) Modelo de Programação das Atividades de Auditoria de Segurança da Informação;
B) Modelo de Mensagem de Varredura na Rede Local da OM a ser Auditada;
C) Modelo da Capa do Relatório de Auditoria (RAD);
D) Modelo da Parte de Introdução do RAD;
E) Modelo da Parte de Constatações do RAD; e
F) Modelo da Parte de Considerações Finais da Assinatura do RAD.

1. PROPÓSITO

Estabelecer os procedimentos necessários para a realização de auditorias de Segurança da Informação (SI) com intuito de garantir a observância das políticas e normas em vigor da MB.

2. DISPOSIÇÕES GERAIS

A auditoria de SI é composta por uma Equipe de Auditoria (EA) designada previamente, cujo objetivo é verificar o fiel cumprimento das normas de SI, bem como estabelecer possíveis ações de correção e divulgação da mentalidade de SI, conforme art. 10.6 da referência.

2.1. Tipos de Auditoria

Os aspectos de SI podem ser verificados pelos seguintes tipos de auditoria:

- a) Auditoria Programada: requerida pela DCTIM ou CLTI, em uma data previamente determinada, conforme planejamento anual, a ser divulgado pela DCTIM e pelos CLTI antecipadamente às OM a serem auditadas;
- b) Auditoria Solicitada: requerida formalmente pela OM ou seu COMINSUP ao CLTI da sua área de jurisdição ou, na impossibilidade do mesmo, à DCTIM; e
- c) Auditoria Inopinada: requerida pela DCTIM ou CLTI, realizada por EA designada em data

63394.001558/2023-41

flexível, a ser definida conjuntamente com a OM a ser auditada.

É vedada a realização de auditorias de SI por empresas contratadas, por pessoal externo à MB ou por funcionários da OM contratados em caráter temporário.

3. COMPOSIÇÃO E RESPONSABILIDADES DA EA

A EA será constituída para cada auditoria de SI a ser realizada, na qual o mais antigo será designado como Chefe da EA. Os componentes da EA serão designados formalmente por Portaria de designação assinada pelo Titular da OM responsável por executar a auditoria. Somente poderão ser designados para compor a EA o pessoal devidamente qualificado. O período de vigência de uma EA tem início na data prevista na Portaria de designação e se encerra com a aprovação do Relatório de Auditoria.

Compete à EA, após sua designação formal, as seguintes atividades:

- a) preparar todo o material necessário para plena realização das atividades de auditoria, obtendo as listas de verificação apropriadas na página da DCTIM, na Intranet;
- b) planejar as atividades específicas da auditoria a que foi designada;
- c) executar, de forma imparcial, soberana e independente, as atividades de auditoria;
- d) garantir o sigilo de toda informação obtida pela auditoria;
- e) elaborar o Relatório de Auditoria (RAD) conforme as normas vigentes e submetê-lo à aprovação do Titular da OM responsável por executar a auditoria no prazo estabelecido; e
- f) divulgar os resultados de auditoria a OM auditada e enviar uma cópia do RAD para a DCTIM.

4. INSTRUÇÕES GERAIS PARA AUDITORIAS

O planejamento e o controle das auditorias de SI são de responsabilidade da DCTIM e CLTI. Caberá a DCTIM realizar as auditorias programadas nos CLTI e estes deverão realizar as auditorias nas OM de sua área de jurisdição.

4.1. Planejamento das Auditorias de SI

O planejamento das auditorias de SI será elaborado pela DCTIM e pelos CLTI de modo a que as OM sejam submetidas pelo menos a uma delas, quer seja programada, inopinada ou solicitada, a cada dois anos.

- a) Auditoria Programada: o planejamento das auditorias de SI programada, para o ano N+1, deve ser elaborado e divulgado no ano N;
- b) Auditoria Solicitada: serão realizadas a partir de um planejamento prévio conjunto entre a DCTIM ou CLTI e a OM a ser auditada; e
- c) Auditoria Inopinadas: realizada em data aleatória, sem o conhecimento da OM, quando identificado um problema que possa causar alguma vulnerabilidade grave ou represente uma ameaça à RECI.

4.2. Procedimentos para Auditorias de SI

No caso de auditorias programadas, solicitadas ou inopinadas, o CLTI da(s) OM envolvida(s) deverá apresentar por mensagem, conforme anexo A, uma proposta para a programação do(s) evento(s) a ser(em) auditado(s) na OM. No período entre D-60 a D-30, será definido entre o CLTI e OM a ser auditada, toda as ações a serem realizadas na fase remota e presencial pela EA, como a varredura na rede local a ser auditada, de acordo com modelo constante no anexo B. A OM a ser auditada enviará ao Chefe da EA, cifrado na chave orion, até o dia D-30, a Lista de Auditoria preenchida, que encontra-se disponível no sítio de Intranet da DCTIM.

A Portaria de designação da EA deverá apresentar, além da relação nominal dos

componentes, o escopo da auditoria, o período que a mesma será realizada com o grau de sigilo, no mínimo, “RESERVADO”. A auditoria terá início, na fase presencial, no dia D, quando toda a EA, o representante da OM auditada e o respectivo pessoal envolvido da OM a ser inspecionada, estiverem presente para apresentação e início das atividades. Nessa reunião, o Chefe da EA deverá apresentar os auditores, a programação e o escopo das atividades de auditoria, e o representante da OM deverá apresentar o seu pessoal diretamente envolvido.

No último dia da auditoria, D+4, haverá uma reunião crítica para apresentação dos aspectos relevantes constatados. Após o término da auditoria presencial será elaborado o RAD, que será submetido a aprovação do Titular da OM responsável pela EA.

Em (D+60)+45, a OM a ser auditada enviará um cronograma de implementação das ações recomendadas no RAD a OM do Chefe da EA.

Segue abaixo uma tabela de resumo do planejamento de auditoria:

FASE	DATA	EVENTO	TIPO DE AUDITORIA
1	D-65	Designação da EA	AP - AS - Alno
2	D-60	Divulgação da proposta de programação para a OM a ser auditada	AP - AS - Alno
3	(D-60) a (D-30)	Início da fase remota da auditoria	AP - AS - Alno
4	Até D-30	A OM a ser auditada enviará a lista de auditoria preenchida e cifrada na chave Orion do Chefe da EA	AP - AS - Alno
5	D	Início da fase local da auditoria nas instalações físicas da rede local da OM	AP - AS - Alno
6	D+4	Conclusão da auditoria na OM	AP - AS - Alno
7	D+60	Elaboração do RAD + Aprovação do RAD	AP - AS - Alno
8	(D+60)+45	A OM auditada elaborará um cronograma de implementação das ações recomendadas no RAD	AP - AS - Alno

Legenda: Auditoria Programada (AP), Auditoria Solicitada (AS) e Auditoria Inopinada (Alno).

As auditorias inopinadas poderão ter as datas reduzidas nas fases 1 a 4, 7 e 8.

Todas as auditorias serão divididas em duas fases a seguir:

a) Remota: busca-se reduzir o tempo de execução da auditoria de SI na OM, através de atividades que possam ser efetuadas prévia e remotamente, por programas específicos. Esta atividade remota deverá ser definida na fase de planejamento e será realizada em laboratório específico nas instalações do CTIM ou do CLTI ou em outro lugar apropriado, devidamente autorizado pela DCTIM, por mensagem, de acordo com a anexo B, com cópia para o CTIM; e

b) Local: deve se restringir à avaliação das conformidades das Listas de Verificação disponibilizadas na página da DCTIM na Intranet e ao levantamento de outras informações, por meio de programas específicos para esse tipo de auditoria, utilizados pela DCTIM, CTIM e CLTI.

4.3. Auditorias de SI programadas

A auditoria de SI programada será executada pela EA formalmente designada pelo CLTI ou DCTIM. Sua composição e as responsabilidades da EA estão apresentadas no item 3, nos prazos descritos anteriormente. Para otimizar o tempo de execução dessa auditoria nas instalações físicas da rede local da OM, a EA deverá planejar e testar com a devida antecedência todo o material necessário para a sua realização. No caso de auditoria de SI programada, estas ações de planejamento deverão ser devidamente documentadas e efetuadas sob coordenação do

Chefe da Equipe de Auditoria.

4.4. Auditorias de SI solicitadas

Este tipo de auditoria será feito a partir de uma solicitação formal de uma OM ou seu COMIMSUP ao CLTI da sua área de jurisdição ou, na impossibilidade do mesmo, à DCTIM. A necessidade geradora de uma auditoria de SI solicitada deve ser avaliada pelo Titular da OM (assessorado pelo Oficial de Segurança da Informação da OM), exceto quando oriunda do COMIMSUP.

Após receber a solicitação, o CLTI ou DCTIM procederá uma análise de disponibilidade de recursos humanos e financeiros sobre a possibilidade de seu atendimento com a maior brevidade possível. Após a análise, o CLTI ou DCTIM programará uma data adequada e formalizará a designação da EA referente à auditoria.

4.5. Auditorias de SI inopinadas

As auditorias de SI inopinadas serão realizadas nas OM, com finalidade específica, a EA para este tipo de auditoria será designada pelo CLTI ou DCTIM com grau de sigilo, no mínimo, “RESERVADO” e cumprirá orientações específicas para sua execução. Mesmo sendo de caráter inopinado, o CLTI ou DCTIM deverá informar ao COMIMSUP, formalmente, sobre a realização da auditoria na OM.

4.6. Relatório de Auditoria (RAD) de SI

a) Composição do RAD

O RAD elaborado pela EA é composto das seguintes partes:

I) Capa: tem por finalidade apresentar os dados iniciais da auditoria de SI realizada e de seus executores (integrantes da EA), juntamente com a assinatura de aprovação do titular da OM responsável por executar a auditoria. O modelo de “Capa” para o RAD encontra-se no anexo C.

II) Introdução: apresentar os documentos de designação da EA, as referências, os prazos envolvidos, seu tipo, sigilo e escopo, bem como o nome da OM onde foi realizada a auditoria de SI. O modelo da parte de “Introdução” do RAD encontra-se no anexo D. Pelo seu caráter mais específico, as auditorias inopinadas e solicitadas devem ter os aspectos a serem constatados claramente definidos na Introdução do RAD; e

III) Constatações da Auditoria de SI: tem por finalidade apresentar as constatações da auditoria, podendo ser agrupadas sob os seguintes aspectos:

- quanto ao adestramento;
- quanto à administração da rede local;
- quanto à documentação;
- quanto às Estações de Trabalho;
- quanto aos incidentes; e
- quanto à segurança física.

Pelo seu caráter mais específico, as auditorias inopinadas e solicitadas não precisam observar todos esses seis aspectos acima. Cada item listado nesta parte do RAD deve conter os seguintes campos:

- Constatação: apresentar a ocorrência, a vulnerabilidade ou o fato constatado;
- Comentário: explicar as possíveis consequências ou prejuízos à SI decorrentes da constatação efetuada; e
- Ação a empreender: recomendar soluções para a constatação efetuada e listar os documentos, normas, publicações e outras referências nos quais as recomendações

apresentadas estão fundamentadas. O modelo da parte de “Constatações” do RAD encontra-se no anexo E.

IV) Considerações Finais da Equipe de Auditoria de SI: apresentar as considerações finais da Equipe de Auditoria de SI. O modelo da parte de “Considerações Finais” do RAD encontra-se no anexo E.

V) Assinatura: constar a assinatura do Chefe da EA, que elaborou o RAD. O modelo da parte de “Assinatura” do RAD também encontra-se no anexo E.

b) Encaminhamento do RAD

EVENTOS	ENCAMINHAMENTO DO RAD
Auditorias realizadas pelos CLTI	Para a OM auditada e cópia para a DCTIM
Auditorias realizadas pela DCTIM	Para a OM auditada
Auditorias Inopinadas realizadas pelo CLTI, ou na impossibilidade do mesmo, pela DCTIM	Para a OM auditada, seu respectivo COMIMSUP e cópia para a DCTIM

O RAD somente será enviado após aprovação pelo Titular da OM responsável por executar a auditoria, no prazo máximo de D+60.

c) Implementação das ações recomendadas pelo RAD

A partir do recebimento do RAD, a OM deverá apresentar ao CLTI, à DCTIM e ao seu COMIMSUP, em até 45 dias, o planejamento e o cronograma de implementação das ações recomendadas (cuja data de início pode ser anterior a essa apresentação), mantendo-os informados e atualizando o HRL (conforme previsto no Capítulo 10, da referência) à medida que forem sendo concluídas as ações previstas.

5. VIGÊNCIA

Esta DCTIMARINST entra em vigor na presente data.

MARCELO GURGEL DE SOUZA
Contra-Almirante
Diretor

ASSINADO DIGITALMENTE

Distribuição:
Lista 1
Arquivo