MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-28

PROCESSO DE GESTÃO DE LOG DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2013

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

TECNOLOGIA DA INFORMAÇÃO

ICA 7-28

PROCESSO DE GESTÃO DE LOG DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2013

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

PORTARIA DECEA Nº 64/DGCEA, DE 24 DE JUNHO DE 2013.

Aprova a edição da Instrução que trata do Processo de Gestão de *Logs* do Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe conferem o art. 195, inciso IV, do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1049/GC3, de 11 de novembro de 2009, e o art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 369/GC3, de 9 de junho de 2010, resolve:

Art. 1º Aprovar a edição da ICA 7-28 "Processo de Gestão de *Logs* do Departamento de Controle do Espaço Aéreo", que com esta baixa.

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

(a)Ten Brig Ar RAFAEL RODRIGUES FILHO
Diretor-Geral do DECEA

(Publicado no BCA nº 152, de 09 de agosto de 2013.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar o Processo de Gestão de *Logs* e os procedimentos correlatos do Departamento de Controle do Espaço Aéreo e suas Organizações Militares Subordinadas.

1.2 ÂMBITO E GRAU DE SIGILO

Esta Instrução se aplica ao DECEA e a todas as suas Organizações Militares Subordinadas, sendo considerado ostensivo o seu grau de sigilo.

1.3 ABREVIATURAS

DECEA – Departamento de Controle do Espaço Aéreo

GLOG – Gestão de *Logs*

NuCGTEC – Núcleo do Centro de Gerenciamento Técnico do SISCEAB

OM – Organização Militar

OPSTI – Organização Provedora de Serviços de Tecnologia da Informação

SDTE – Subdepartamento Técnico do DECEA

SI – Segurança da Informação

SSSI – Seção de Segurança de Sistemas da Informação

SISCEAB – Sistema de Controle do Espaço Aéreo Brasileiro

TI – Tecnologia da Informação

TIOP – Tecnologia da Informação Operacional

1.4 CONCEITOS

1.4.1 Os conceitos e definições estão listados na MCA 7-1 Glossário de Segurança da Informação do DECEA.

1.4.2 Para efeito deste Documento Normativo de Segurança da Informação, entende-se por:

a) Normalizar dados – conjunto de regras que visa minimizar as anomalias no armazenamento e modificação dos dados, além de proporcionar maior flexibilidade na sua utilização. Esses passos reduzem a redundância e a chance dos *logs* se tornarem inconsistentes quando forem analisados pela equipe responsável por identificar os incidentes de segurança da informação.

2 RESPONSABILIDADES

2.1 SUBDEPARTAMENTO TÉCNICO DO DECEA

2.1.1 Coordenar as ações, no nível estratégico, do Processo de Gestão de *Logs* do DECEA e OM subordinadas.

2.1.2 Normatizar e manter atualizado o Processo de Gestão de *Logs*

2.2 NÚCLEO DO CENTRO DE GERENCIAMENTO TÉCNICO

2.2.1 Gerenciar, no nível tático, o processo de gestão de *logs* no âmbito do DECEA.

2.2.2 Acompanhar o processo indicando ações de melhoria contínua.

2.2.3 Auditar o processo de gestão de *logs*.

2.2.4 Centralizar os *logs* dos sistemas de TI operacionais, embarcados e os de segurança perimetral (ataques cibernéticos).

2.3 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

2.3.1 Coordenar as ações no nível operacional.

2.3.2 Executar o tratamento e correlação de *logs*.

2.3.3 Apoiar o NuCGTEC na geração de indicadores.

2.3.4 Tratar, conjuntamente com a TIOP locais e os Elos de Serviço de TI, os incidentes de segurança da informação identificados durante a gestão de *logs*.

2.4 TIOP LOCAL – SEÇÃO DE TECNOLOGIA DA INFORMAÇÃO OPERACIONAL

2.4.1 Monitorar os *logs* dos sistemas de TI operacionais.

2.4.2 Tratar, conjuntamente com a SSSI, os incidentes de segurança da informação.

2.5 ELOS DE SERVIÇOS DE TI (OPSTI)

2.5.1 Armazenar e monitorar os *logs* dos sistemas de TI de suporte operacional e administrativo.

2.5.2 Acionar a SSSI para tratar, conjuntamente, os incidentes de segurança da informação.

2.6 EQUIPE DE RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

2.6.1 Tratar os incidentes de segurança da informação identificados no Processo de Gestão de *Logs*, em conformidade com a ICA 7-23 Processo de Gestão de Incidentes de Segurança da Informação do Departamento de Controle do Espaço Aéreo de 2013.

3 PROCESSO DE GESTÃO DE *LOGS*

3.1 DESCRIÇÃO DO PROCESSO

3.1.1 Conforme previsto na ação nº 18 do item 4.1.4 do PCA 7-11 Plano Diretor de Segurança da Informação do DECEA está preconizada a implantação do processo de gestão de incidentes de segurança da informação, visando monitorar e avaliar os eventos suspeitos, determinar os incidentes de segurança da informação, calcular seus respectivos impactos, investigá-los, identificar suas possíveis causas, elaborar estratégias para suas respectivas contenção e correção e restabelecer os ambientes afetados no menor tempo possível. Assim, é necessário o estabelecimento do processo de gestão de *logs* para suportar a gestão de incidentes no âmbito do DECEA e nas Organizações subordinadas.

3.1.2 A gestão de *Logs* deve apoiar o processo de gestão de incidentes tratando do relacionamento de eventos que devem ser investigados e encaminhados para o devido tratamento de incidentes de segurança da informação, conforme normativa vigente.

3.2 VISÃO GERAL DO PROCESSO

3.2.1 De modo geral, processo é um conjunto sequencial de ações ou atividades particulares com a finalidade de alcançar um determinado objetivo. Pode ser composto de uma ou mais entradas, que são processadas, retornando uma ou mais saídas.

3.2.2 Para a presente normatização, o processo será dividido em subprocessos, que por sua vez poderão também ser subdivididos em outros subprocessos denominados etapas ou fases.

3.2.3 No caso do processo de gestão de logs em tela, ele é composto por 3 (três) subprocessos a seguir nomeados: Tratamento, Correlação e Melhoria Contínua, conforme ilustrado na figura 1.

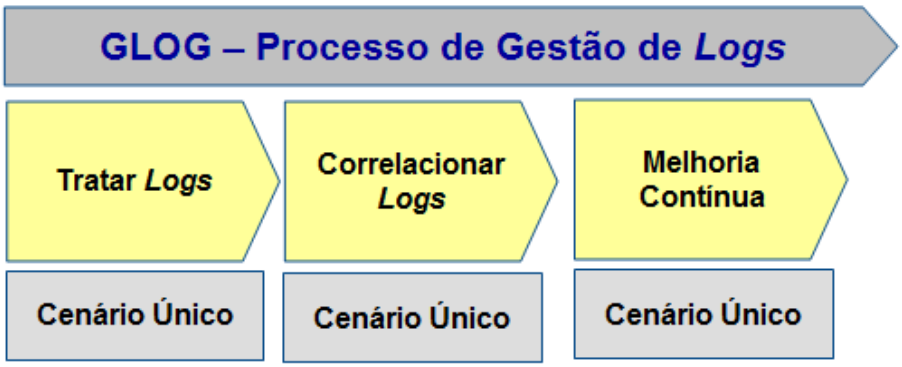

Figura 1 - Visão Geral do Processo de Gestão de *Logs*

3.3 SUBPROCESSO "TRATAR *LOGS*"

3.3.1 Este subprocesso visa proporcionar o adequado tratamento dos *logs* referentes aos sistemas de TI do DECEA, sendo subdividido em 4 etapas, conforme ilustrado na figura 2.

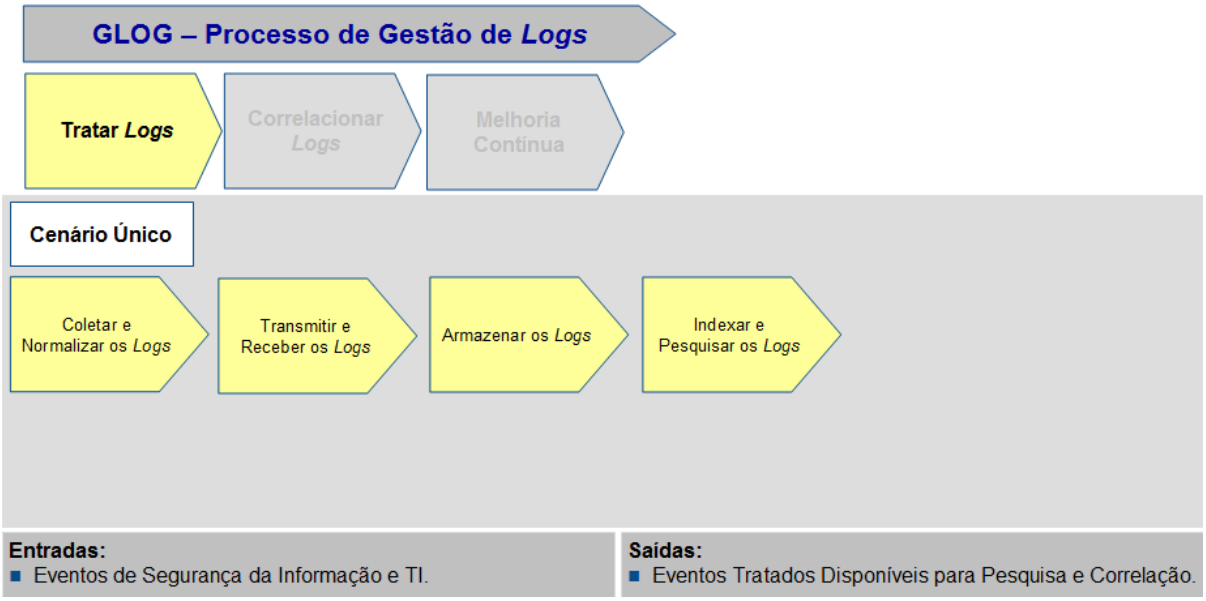

Figura 2 - Subprocesso Tratar *Logs*

3.3.2 Na Etapa "Coletar e Normalizar os *Logs*", todas as informações necessárias dos eventos de segurança da informação, contendo atividades dos usuários, exceções e outros eventos de segurança, serão coletadas e normalizadas a fim de que possam ser utilizadas de forma simplificada para pesquisa e análise.

3.3.3 Os sistemas que geram *logs* deverão ter seus relógios sincronizados com uma fonte de tempo precisa, como por exemplo, um servidor de *Network Time Protocol*. Dessa forma os *logs* estarão ajustados, e as informações poderão ser utilizadas de forma confiável, como, por exemplo, para tratamento de incidentes em segurança da informação ou perícia forense; portanto, todos os relógios de equipamentos deverão estar sincronizados com o servidor de *logs* do NuCGTEC.

3.3.4 Na etapa "Transmitir e Receber os *Logs*", os *logs*, após normalização, deverão ser transmitidos para uma central de armazenamento (Servidor de *Logs*) em cada OPSTI; posteriormente as OPSTI deverão enviá-los, após o tratamento, para o servidor dedicado do NuCGTEC.

3.3.5 Já na etapa "Armazenar *Logs*", os mesmos deverão ser armazenados de acordo com a DCA 7-2 Política de Segurança da Informação vigente no DECEA.

3.3.6 Finalmente, a etapa Indexar e Pesquisar permitirá a indexação dos *logs*, visando identificar quais *logs* podem conter acessos indevidos ou registros suspeitos que precisam ser disponibilizados os seus eventos de segurança da informação para a equipe de tratamento e resposta de incidentes de segurança da informação.

3.4 SUBPROCESSO "CORRELACIONAR *LOGS*"

3.4.1 Este subprocesso é composto por 4(quatro) etapas, a saber: identificar os eventos para correlação, executar e analisar a correlação, visualização e geração de alarme de incidentes, que por sua vez acionará o processo de gestão de incidentes, definido na ICA 7-23 Gestão de Incidentes de Segurança da Informação do DECEA, conforme ilustrado na figura 3.

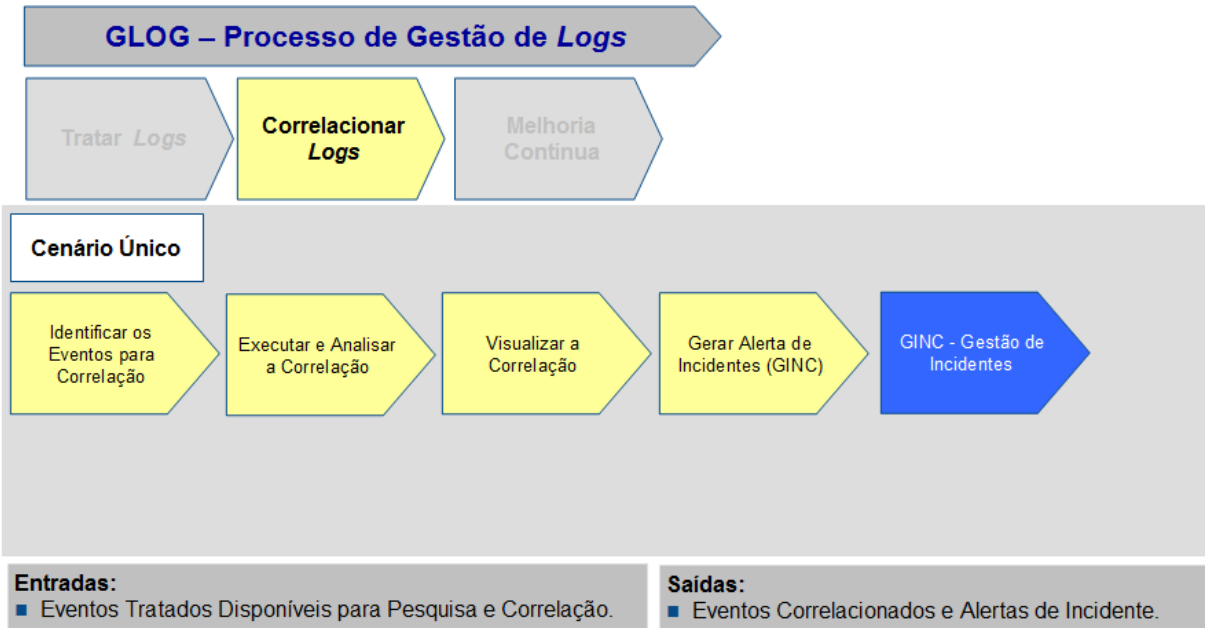

Figura 3 - Subprocesso Correlacionar *Logs*

3.4.2 Na etapa de identificação dos eventos para correlação deverão ser estabelecidos quais eventos serão selecionados para execução da correlação.

3.4.3 Na etapa de execução e análise da correlação efetivamente ocorre a pesquisa, a fim de identificar as possíveis causas dos incidentes de segurança da informação.

3.4.4 Após o processamento da etapa de execução e análise da correlação, os resultados deverão estar disponíveis para visualização da equipe de resposta e tratamento de incidentes da Organização conforme o item 2.6 desta instrução.

3.4.5 A etapa de geração de Alerta de Incidentes é responsável pela emissão de alerta e a respectiva notificação para a equipe de resposta e tratamento de incidentes da Organização conforme o item 2.6 desta instrução.

3.5 SUBPROCESSO "MELHORIA CONTÍNUA"

3.5.1 Este subprocesso visa analisar a performance do processo de segurança da informação com o objetivo de identificar oportunidades de melhorias na Gestão de *Logs*. Ele é dividido em duas etapas, a primeira denominada Análise e Consolidação e a segunda nomeada Identificação de Oportunidade de Melhoria, conforme ilustrado na figura 4.

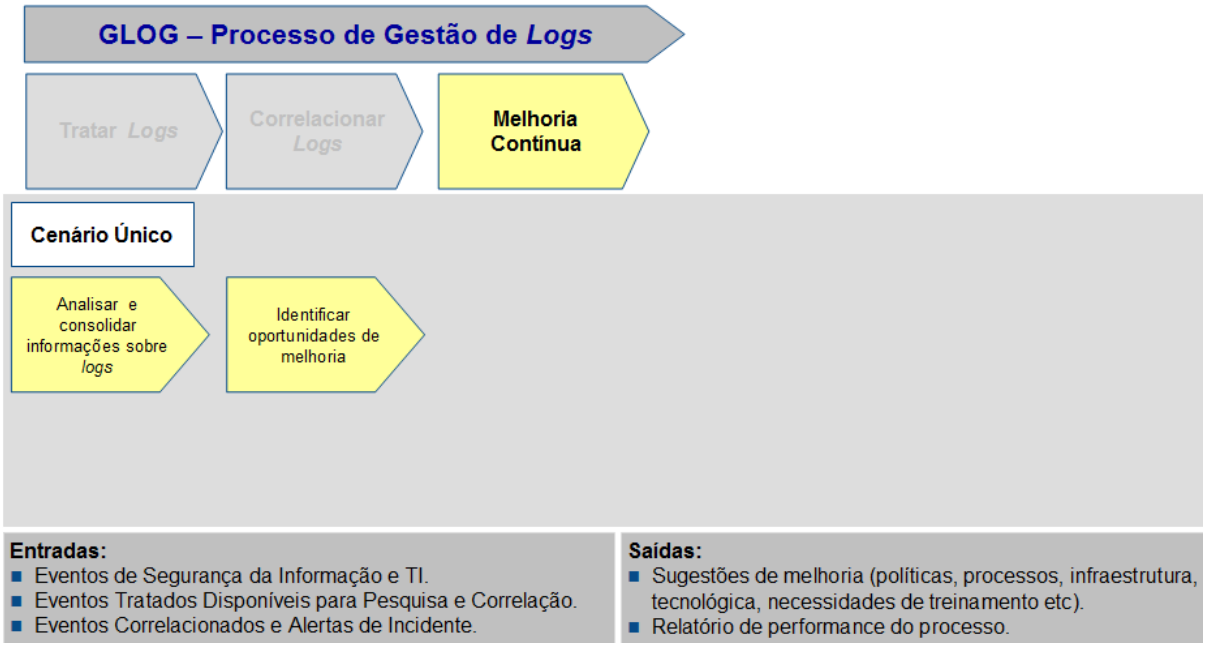

Figura 4 - Subprocesso para Melhoria Contínua

3.5.2 Na etapa "Analisar e Consolidar informações sobre *Logs*", deve-se identificar e quantificar os indicadores do processo no documento Identificação, Quantificação e Análise dos Indicadores do Processo (GLOG01), conforme modelo padronizado no Anexo A.

3.5.3 Já na etapa "Identificar Oportunidades de Melhoria", as informações consolidadas do processo devem ser analisadas, por intermédio dos seus indicadores com o objetivo de proporcionar a melhoria contínua do processo. Essas informações deverão ser transcritas no documento Identificação, Quantificação e Análise dos Indicadores do Processo (GLOG01), conforme modelo padronizado no Anexo A.

3.6 CONTROLE E MATURIDADE DO PROCESSO

3.6.1 MEDIÇÃO DO NÍVEL DE MATURIDADE ATUAL DO PROCESSO

3.6.1.1 A maturidade deste processo é medida através da seguinte escala:

0 – Não Existente: O Processo de Gestão de *Logs* não ocorre. A Organização não considera os impactos no negócio associados ao processo. O Processo de Gestão de *Logs* não tem sido identificado como relevante para aquisição de soluções de Tecnologia da Informação e para entrega dos serviços de TI.

1 – Inicial/*Ad Hoc*: O Processo de Gestão de *Logs* é conduzido *Ad Hoc*. Existe o entendimento emergente de que o processo é importante e deve ser executado com controles de segurança da informação pelos Administradores de Rede.

2 – Repetível e Intuitivo: Uma abordagem do Processo de Gestão de *Logs* existe, mesmo de modo imaturo, e está implementado. O gerenciamento do processo é controlado com a classificação estabelecida e tipicamente aplicado apenas aos projetos de redes importantes ou em resposta aos incidentes de SI. Os processos de correção das vulnerabilidades identificadas nas redes são incipientes.

3 – Processo Definido: A Gestão de *Logs* segue um processo definido e documentado. O treinamento no processo está disponível para todo o pessoal. As decisões para acompanhar o processo e para receber treinamento são deixadas a critério individual. A metodologia para a Gestão de *Logs* é convincente e bem estruturada e garante que os principais riscos para o negócio sejam identificados. Um processo para corrigir as vulnerabilidades identificadas é normalmente instituído.

4 – Gerenciado e Mensurável: A avaliação e o gerenciamento do Processo de Gestão de *Logs* são executados com procedimentos padrões. O processo é avaliado em nível de projeto individual e também regularmente a respeito da operação de TI e Telecomunicações como um todo. Existe a capacidade de monitorar a posição dos riscos associados à Gestão de *Logs* e tomar decisões informadas referentes à exposição que deseja assumir. Todas as vulnerabilidades identificadas deste processo têm um proprietário nomeado.

5 – Otimizado: A Gestão de *Logs* alcançou um estágio no qual ele é executada e bem gerenciada e suporta o controle e tratamento de incidentes de segurança da informação. Boas práticas são aplicadas na Organização Militar. A captura, a análise e os relatórios de gerenciamento estão automatizados.

3.6.1.2 A tabela abaixo apresenta as metas para a evolução dos níveis de maturidade:

Nível de Maturidade	Metas	Prazo
2 – Repetível, mas Intuitivo	• Possuir uma normativa interna do DECEA para a Gestão de *Logs*. • Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA.	Até dezembro de 2013
3 – Processo Definido	• Implantar o processo em todas as Organizações Subordinadas ao DECEA. • Capacitar todos os chefes das seções de segurança da informação.	Até junho de 2014
4 – Gerenciado e Mensurável	• Criar um painel para acompanhamento, através de indicadores gerenciais do processo, a fim de garantir a tomada de decisão pela Direção do DECEA.	Até dezembro de 2014
5 – Otimizado	• Realizar uma reunião semestral de análise crítica para melhoria contínua do processo. • Possuir sistema informatizado para emissão de relatórios automatizados.	Até dezembro de 2015

3.6.2 ACOMPANHAMENTO DO PROCESSO POR INDICADORES

O acompanhamento do processo será feito por intermédio dos indicadores e métricas listadas na Tabela abaixo, contudo as metas serão definidas posteriormente pelo SDTE.

Objetivos do Processo	Indicadores do Processo
• Determinar a redução de ocorrência e o impacto de incidentes de segurança da informação em ativos de informação; • Apoiar o processo de Gestão de Incidentes de Segurança da Informação; • Apoiar o processo de Gestão de Conformidade; e • Apoiar o processo de Auditoria de Segurança da Informação.	• Quantidade de ativos de informação com *logs* tratados e correlacionados; • Quantidade de incidentes de segurança da informação descobertos mediante o correlacionamento de *logs*; e • Quantidade de sugestões de melhorias no processo.

3.6.3 FATORES CRÍTICOS DE SUCESSO

São os seguintes os fatores críticos de sucesso para alcançar os objetivos definidos para o processo, bem como nortear as avaliações dos resultados alcançados:

a) garantia do cumprimento das responsabilidades atribuídas no processo;

b) garantia do cumprimento dos procedimentos relacionados ao processo;

c) acompanhamento da situação do processo e apresentação de relatórios periódicos; e

d) garantia da comunicação eficiente e eficaz do processo para todas às partes interessadas e envolvidas.

4 DISPOSIÇÕES FINAIS

4.1 O Processo e os procedimentos de Segurança da Informação apresentados neste documento são de caráter geral e devem ser revisados periodicamente a cada trinta e seis meses, ou quando fato relevante demandar atualização extemporânea.

4.2 Esta Instrução de Comando da Aeronáutica deverá estar em conformidade com as Diretrizes da DTI – Órgão Central do Sistema de Tecnologia da Aeronáutica – e sera revisada e atualizada sempre que forem atualizadas ou aprovadas Normas relativas ao assunto pela Diretoria de Tecnologia da Informação do Comando da Aeronáutica.

4.3 Casos não previstos nesta Instrução deverão ser levados à apreciação do Exmo. Sr. Diretor-Geral do DECEA.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27002. *Tecnologia da informação: Técnicas de segurança: Código de pratica para a gestão da segurança da informação*. Rio de Janeiro, RJ, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27005. *Tecnologia da informação: Técnicas de segurança: Gestão de riscos de segurança da informação*. Rio de Janeiro, RJ, 2008.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Política de Segurança da Informação do DECEA*: **DCA 7-2**. Rio de Janeiro, RJ, 2010.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Plano Diretor de Segurança da Informação do DECEA*: **PCA 7-11.** Rio de Janeiro, RJ, 2010.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Preceitos de Segurança da Informação do DECEA*: **ICA 7-19**. Rio de Janeiro, RJ, 2012.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Classificação dos Sistemas de Tecnologia de Informação do SISCEAB*: **ICA 7-22**. Rio de Janeiro, 2013.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Processo de Gestão de Incidentes de Segurança da Informação do DECEA*: **ICA 7-23**. Rio de Janeiro, RJ, 2013.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. *Estrutura e Competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica (STI)*: **NSCA 7-7.** Brasília, DF, 2004.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo*: **MCA 7-1**. Rio de Janeiro, RJ, 2012.

Anexo A – Registro GLOG01 – Identificação, Quantificação e Análise dos Indicadores do Processo

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome por extenso da OM>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GLOG01			
ASSUNTO	Identificação, Quantificação e Análise dos Indicadores do Processo			

1 MEDIÇÃO DOS INDICADORES

Indicador	Quantitativo	Observações

2 ANÁLISE DOS INDICADORES

3 AÇÕES DE MELHORIA CONTÍNUA