MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-23

PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2013

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

TECNOLOGIA DA INFORMAÇÃO

ICA 7-23

PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

2013

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

PORTARIA DECEA Nº 60/DGCEA, DE 4 DE JUNHO DE 2013.

Aprova a edição da Instrução relativa ao Processo de Gestão de Incidentes de Segurança da Informação do Departamento de Controle do Espaço Aéreo.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere 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. 11, 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 7-23 "Processo de Gestão de Incidentes de Segurança da Informação 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

(Publicada no BCA nº 121, de 27 de junho de 2013)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES 7
1.1 FINALIDADE 7
1.2 ÂMBITO E GRAU DE SIGILO 7
1.3 ABREVIATURAS 7
1.4 DEFINIÇÕES 7

2 DESCRIÇÃO DO DOCUMENTO 8
2.1 UTILIZAÇÃO 8
2.2 DOCUMENTO NORMATIVO DE SEGURANÇA DA INFORMAÇÃO 8

3 RESPONSABILIDADES 9
3.1 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA 9
3.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO 9
3.3 USUÁRIO DAS INFORMAÇÕES 9

4 PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 10
4.1 DESCRIÇÃO DO PROCESSO 10
4.2 DIRETRIZES DO PROCESSO 10
4.3 CONTROLE E MATURIDADE DO PROCESSO 11
4.4 FATORES CRÍTICOS DE SUCESSO 13

5 DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO 14
5.1 VISÃO GERAL DO PROCESSO 14
5.2 SUBPROCESSO “DETECTAR INCIDENTE DE SEGURANÇA” 15
5.3 SUBPROCESSO “INVESTIGAR INCIDENTE” 18
5.4 SUBPROCESSO “CONTER E CORRIGIR INCIDENTE” 19
5.5 SUBPROCESSO “FECHAR INCIDENTE” 21
5.6 SUBPROCESSO “ANALISAR INCIDENTES E PERFORMANCE” 22

6 DISPOSIÇÕES FINAIS 23

REFERÊNCIA 24

Anexo A – GINC01 – Registro de Incidentes de Segurança da Informação 25
Anexo B – GINC02 – Identificação, Quantificação e Análise dos Indicadores do Processo 27

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar o Processo de Gestão de Incidentes de Segurança da Informação para o 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

GINC – Gestão de Incidentes de Segurança da Informação

OM – Organização Militar

SDTE – Subdepartamento Técnico do Departamento de Controle do Espaço Aéreo

SSSI – Seção de Segurança de Sistemas da Informação

1.4 DEFINIÇÕES

Os conceitos e definições estão listados no Glossário de Segurança da Informação do DECEA (MCA 7-1).

2 DESCRIÇÃO DO DOCUMENTO

2.1 UTILIZAÇÃO

2.1.1 Como requisito para a utilização deste Processo, as Organizações Militares devem estar estruturadas de acordo com o estabelecido pelo Plano Diretor de Segurança da Informação do DECEA (PCA 7-11), ou seja, devem possuir uma Seção de Segurança de Sistemas de Informação (SSSI) responsável pela garantia do cumprimento da Política de Segurança da Informação do DECEA (DCA 7-2).

2.1.2 As Seções de Segurança de Sistema da Informação de cada OM devem seguir as diretrizes estabelecidas nesta Instrução e pelos documentos normativos de segurança da informação dela derivados.

2.2 DOCUMENTO NORMATIVO DE SEGURANÇA DA INFORMAÇÃO

2.2.1 Este Procedimento de Segurança da Informação trata da identificação, investigação, contenção, correção, fechamento e análise crítica dos incidentes de segurança da informação.

3 RESPONSABILIDADES

3.1 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA

3.1.1 Coordenar o cumprimento e evolução da maturidade do processo de Gestão de Incidentes de Segurança da Informação.

3.1.2 Assessorar tecnicamente, quando necessário, as Seções de Segurança de Sistemas de Informação.

3.1.3 Assessorar na tomada de decisão quanto às questões relacionadas aos incidentes de segurança da informação.

3.1.4 Aprovar as medidas de contenção, correção e erradicação para incidentes de segurança da informação.

3.2 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

3.2.1 Coordenar a Equipe de Resposta e Tratamento de incidentes de segurança da Informação

3.2.2 Detectar, registrar, investigar, tratar e concluir os incidentes de segurança da informação.

3.2.3 Implantar as medidas de contenção, correção e erradicação para incidentes de segurança da informação.

3.2.4 Comunicar o tratamento de incidentes às áreas envolvidas.

3.2.5 Auxiliar o SDTE na geração de indicadores do processo.

3.3 USUÁRIO DAS INFORMAÇÕES

3.3.1 Notificar os incidentes de segurança da informação.

4 PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

4.1 DESCRIÇÃO DO PROCESSO

4.1.1 De acordo com itens 4.1.4 e 18 do Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo (PCA 7-11), e do item 6.15 da DCA 7-2, o DECEA deve implantar e manter uma estrutura que promova atividades de gerenciamento de incidentes de segurança da informação em todas as Organizações Subordinadas, sendo necessário, portanto, o estabelecimento de um processo de gestão de incidentes no DECEA e nas Organizações Subordinadas.

4.2 DIRETRIZES DO PROCESSO

4.2.1 Este processo tem como principal objetivo restaurar a operação normal do serviço na brevidade requerida, minimizando os prejuízos à operação do negócio e garantindo assim o melhor nível de serviço e disponibilidade. As etapas principais são: detectar, identificar, conter, investigar, corrigir, restabelecer e analisar os incidentes.

4.2.2 A Equipe de Resposta e Tratamento de Incidentes de Segurança da Informação deverá ser composta por integrantes da Seção de Segurança de Sistemas da Informação, da Seção de Tecnologia da Informação e por especialista para apoiar na resposta e tratamento de incidentes de Segurança da Informação na Organização Militar onde ocorreu o incidente ou nas organizações militares sob a sua responsabilidade.

4.2.3 O Chefe da Seção de Segurança da Informação deverá coordenar a Equipe de Resposta e Tratamento de Incidentes de Segurança da Informação.

4.2.4 As Seções de Segurança da Informação (SSSI) devem avaliar os eventos suspeitos para definir se são efetivamente incidentes de segurança da informação, determinando qual o impacto desses incidentes na missão da Organização.

4.2.5 Os incidentes de segurança da informação podem ser notificados por qualquer setor da Organização, ou identificados pelo setor de monitoração de segurança da informação.

4.2.6 As Seções de Segurança da Informação (SSSI) devem investigar os incidentes de segurança com o acionamento das equipes de resposta e tratamento de incidentes de segurança da informação e do Plano de Comunicação, o envolvimento das áreas e acionamento do Plano de Investigação, identificando suas causas, alternativas de contenção e correção e impactos no ambiente do usuário.

4.2.7 As Seções de Segurança da Informação (SSSI) devem definir o Plano de Contenção, correção e erradicação, conforme previsto no item 17 do formulário de Registro de Incidentes de Segurança da Informação (GINC01) do Anexo A e executar as correções e validá-las com as áreas afetadas para conter o incidente, restabelecendo o ambiente onde ocorreu o incidente de Segurança da Informação no menor tempo possível.

4.2.8 As áreas envolvidas na investigação, contenção e correção devem se reunir para revisar todo o processo, identificar potenciais vulnerabilidades, oportunidades de melhorias e conhecimento gerado.

4.2.9 As SSSI devem analisar o conjunto de incidentes ocorridos e a performance dos processos de segurança e operação, procurando identificar problemas de segurança, potenciais vulnerabilidades e oportunidades de melhorias de processo.

4.3 CONTROLE E MATURIDADE DO PROCESSO

4.3.1 MEDIÇÃO DO NÍVEL DE MATURIDADE ATUAL DO PROCESSO

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

0 – Não Existente: Não existe um processo de gerenciamento de incidentes.

1– Inicial/*Ad Hoc*: A organização reconhece que um processo apoiado por ferramentas e pessoal é necessário para gerenciar resolução de incidentes. Não existe, porém, processo padronizado e apenas apoio reativo é fornecido. O gerenciamento não monitora incidentes. Não existe processo de escalonamento para garantir que os incidentes sejam resolvidos.

2 – Repetível e Intuitivo: Existe conscientização organizacional da necessidade de um processo de gerenciamento de incidentes. O suporte está disponível em uma base informal através de uma rede de pessoas conhecidas. Essas pessoas dispõem de ferramentas comuns para ajudar na resolução de incidentes. Não existe treinamento formal nem comunicação sobre procedimentos padrões, e a responsabilidade é deixada ao indivíduo.

3 – Processo Definido: A necessidade de um processo de gerenciamento de incidentes é reconhecida e aceita. Os procedimentos foram padronizados e documentados, e o treinamento ocorre de maneira informal. É, porém, deixado ao indivíduo obter o treinamento e acompanhar os padrões. Incidentes são rastreados em uma base manual e monitorados individualmente, mas não existe sistema formal de relatórios. A resposta conveniente a dúvidas e incidentes não é avaliada e os incidentes podem ficar não resolvidos. Os usuários receberam claras comunicações sobre como e onde relatar a respeito de incidentes.

4 – Gerenciado e Mensurável: Existe o completo entendimento das vantagens de um processo de gerenciamento de incidentes em todos os níveis de organização. As ferramentas e técnicas são automatizadas com uma base de conhecimentos centralizada. As responsabilidades são claras e a efetividade é monitorada. Os procedimentos de comunicação, escalonamento e resolução de incidentes são determinados e comunicados.

5 – Otimizado: O processo de gerenciamento de incidentes é determinado e bem organizado. Indicadores de Performance e de Gerenciamento são sistematicamente avaliados e relatados. Ferramentas são implantadas para possibilitar aos usuários se autodiagnosticar e resolver incidentes. Incidentes são resolvidos rapidamente dentro de um processo de escalonamento estruturado. O gerenciamento utiliza uma ferramenta integrada para as estatísticas de desempenho do processo de gerenciamento de incidentes. Os processos foram refinados no nível das melhores práticas de mercado, com base nos resultados da análise dos Indicadores de Performance e de Gerenciamento e melhoria contínua.

4.3.1.2 A tabela abaixo apresenta as metas para a evolução dos níveis de maturidade e seus respectivos prazos:

Nível de Maturidade	Metas	Prazo
2 – Repetível e Intuitivo	• Possuir uma normativa interna do DECEA para gestão de incidentes de segurança da informação • Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA	Até junho de 2014
3 – Processo Definido	• Implantar o processo em todas as Organizações Subordinadas ao DECEA • Capacitar todos os chefes das seções de segurança da informação	Até dezembro 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 do SDTE	Até junho de 2015
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

4.3.2 ACOMPANHAMENTO DO PROCESSO POR INDICADORES

Objetivos do Processo	Indicadores do Processo
• Analisar, documentar e realizar o levantamento de incidentes de segurança da informação no tempo correto; e • Responder a incidentes de forma precisa e no tempo correto.	• Quantidade de Incidentes de Segurança Identificados; • Quantidade de Incidentes Abertos; • Quantidade de Incidentes Fechados; • Quantidade de Incidentes de Segurança Tratados por Período de Tempo; • Quantidade de Incidentes de Segurança por Nível de Alerta; e • Tempo Médio de Resposta a Incidentes.

4.4 FATORES CRÍTICOS DE SUCESSO

Os fatores críticos de sucesso listados abaixo são requisitos para alcançar os objetivos definidos para o processo, bem como nortear as avaliações dos resultados alcançados:

a) garantir cumprimento das responsabilidades atribuídas no processo;

b) monitoração e registro das tendências;

c) garantir cumprimento dos procedimentos relacionados ao processo;

d) acompanhamento da situação do processo e apresentação de relatórios; e

e) garantir comunicação eficiente e eficaz do processo a todas as partes interessadas e envolvidas.

5 DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

O processo de Gestão de Incidentes de Segurança da Informação deve ser contínuo e aplicado na implementação e operação do Sistema de Gestão de Segurança da Informação (SGSI).

5.1 VISÃO GERAL DO PROCESSO

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.

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.

No caso do processo de gestão de incidentes em tela, ele é composto por 5 (cinco) subprocessos a seguir descritos: detectar incidente de segurança, investigar incidente, conter e corrigir incidentes, fechar incidente e analisar incidentes e performance, conforme ilustrado na figura 1.

Figura 1 - Visão Geral do Processo de Gestão de Incidentes de Segurança da Informação

5.2 SUBPROCESSO "DETECTAR INCIDENTE DE SEGURANÇA"

5.2.1 Este subprocesso visa identificar informações sobre o evento, correlacionar o evento identificado com outros já avaliados, confirmar o incidente de segurança da informação, informar o responsável pelo comunicado e avaliar e descrever os impactos.

5.2.2 Os incidentes de segurança da informação podem ser notificados através de outras áreas da Organização Militar, por qualquer usuário, ou identificado na área de monitoração de segurança da informação.

5.2.3 Conforme a figura 2, quando o evento não for identificado pela área de monitoração de segurança, ou seja, o usuário do sistema de informação notificar a ocorrência de um incidente de segurança da informação, o mesmo deverá ser tratado por esta área de monitoramento e deverá ser emitido informe deste processo para o usuário/área notificadora do evento. Quando o evento é identificado pela área de monitoramento de segurança conforme a figura 3, não existe a necessidade de emissão de informes, já que o incidente já é conhecido e acompanhado pela área responsável.

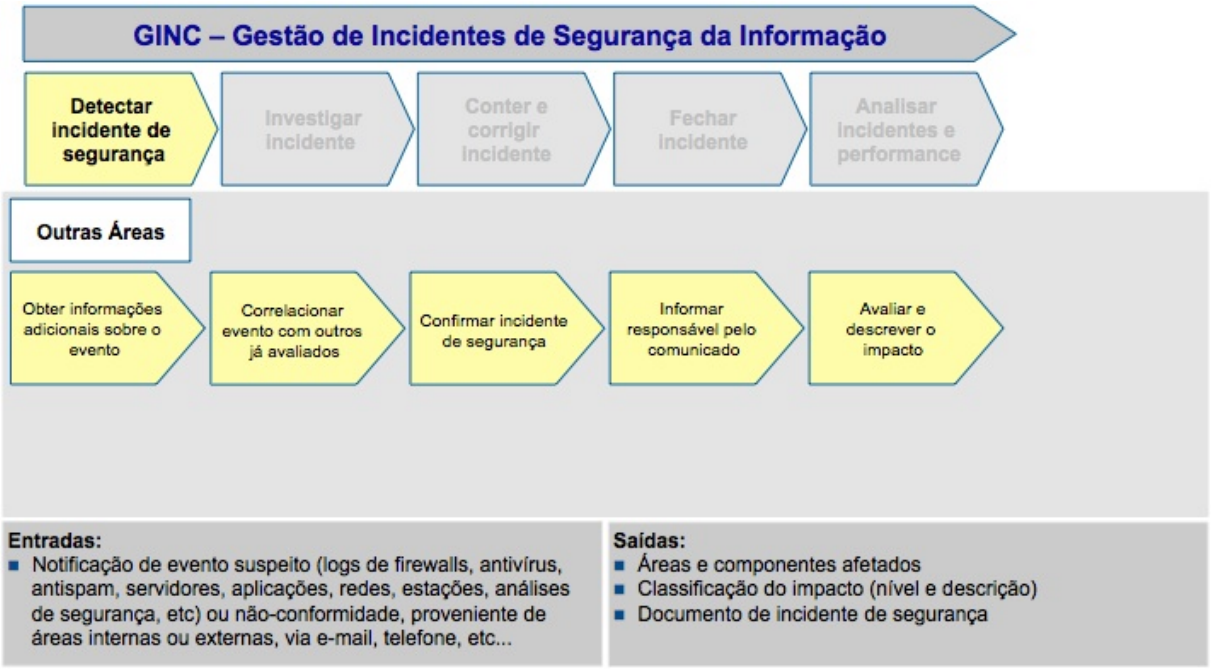

Figura 2 - Subprocesso para Detectar Incidente de Segurança da Informação Notificado por Outras Áreas.

Figura 3 - Subprocesso para Detectar Incidente de Segurança da Informação Notificado pelo Monitoramento de Segurança

5.2.4 ETAPA "OBTENÇÃO DE INFORMAÇÕES ADICIONAIS SOBRE O EVENTO"

5.2.4.1 Nesta etapa, deve ser obtido o maior número de informação disponível sobre o evento. Tais informações podem incluir:

a) nome e área do usuário notificador;

b) dia e hora que o evento ocorreu;

c) como foi detectado o incidente;

d) tipo de incidente;

e) quais operações estão indisponíveis; e

f) que sistemas foram afetados.

5.2.4.2 As informações detalhadas sobre o evento deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo os itens de 1 a 7, detalhado no Anexo A.

5.2.5 ETAPA **"**CORRELACIONAR EVENTO COM OUTROS JÁ AVALIADOS"

5.2.5.1 Vários eventos podem ser notificados e originados por uma única causa. Assim, nesta etapa o evento e as informações identificadas serão correlacionados com outros eventos avaliados visando identificar semelhanças e possíveis soluções.

5.2.5.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo o item 8 do Anexo A.

5.2.6 ETAPA "CONFIRMAR INCIDENTE DE SEGURANÇA E DEFINIR NÍVEL DE ALERTA"

5.2.6.1 A área de segurança deverá, através das informações obtidas, deve confirmar se o evento é um incidente de segurança da informação. Um nível de alerta (alto, médio ou baixo) do incidente para a Organização Militar deverá ser disponibilizado em função da análise realizada pela SSSI.

5.2.6.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo o item 9 do Anexo A.

5.2.7 ETAPA "INFORMAR RESPONSÁVEL PELO COMUNICADO"

5.2.7.1 A área de segurança deverá emitir comunicado para o responsável/área que informou o incidente de segurança.

5.2.7.2 Este comunicado deve conter as seguintes informações:

a) confirmação do incidente;

b) número identificado do incidente;

c) data e hora do incidente; e

d) confirmação dos componentes afetados.

5.2.8 ETAPA "AVALIAR, DESCREVER O IMPACTO E TEMPO DE RESPOSTA"

5.2.8.1 A área de segurança deverá descrever e avaliar os reais impactos do incidente de segurança da informação e o tempo de resposta necessário para investigação, contenção e correção do incidente em questão.

5.2.8.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo os itens 10 e 11 do Anexo A.

5.3 SUBPROCESSO "INVESTIGAR INCIDENTE"

5.3.1 Neste subprocesso, a área de segurança responsável por incidentes deverá acionar a equipe de resposta e tratamento de incidentes de segurança da informação e o plano de comunicação da OM, comunicar o incidente às áreas afetadas e envolvidas, identificar áreas que devem participar da investigação do incidente, adicionar ou definir um plano de investigação, investigar o incidente e comunicar conclusão às áreas afetadas e envolvidas.

Figura 4 - Subprocesso para Investigar Incidente de Segurança da Informação

5.3.2 ETAPA **"**ACIONAR EQUIPE DE RESPOSTA E PLANO DE COMUNICAÇÃO"

5.3.2.1 Após a fase de detecção do incidente de segurança da informação, é necessário acionar a equipe de resposta e tratamento de incidentes de segurança da informação e o Plano de Comunicação para tratar o incidente identificado. Este Plano deverá apresentar quais são as áreas/usuários participantes do processo de investigação, contenção e correção do incidente, quando serão comunicados e que informações serão partilhadas entre as partes.

5.3.2.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo os itens 12 e 13 do Anexo A.

5.3.3 ETAPA "COMUNICAR INCIDENTE ÀS ÁREAS AFETADAS E ENVOLVIDAS"

5.3.3.1 Nesta etapa, a equipe de segurança responsável pelos incidentes deverá acionar o Plano de Comunicação e comunicar as informações necessárias do processo de investigação, contenção e correção do incidente.

5.3.4 ETAPA "IDENTIFICAR ÁREAS QUE DEVEM PARTICIPAR DO PROCESSO DE INVESTIGAÇÃO"

5.3.4.1 Nesta etapa, a equipe de segurança responsável identifica as áreas da organização que atuarão em conjunto com a equipe de resposta e tratamento de incidentes de segurança da informação para contribuir com informações úteis durante o processo.

5.3.4.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo o item 14 do Anexo A.

5.3.5 ETAPA "DEFINIR E ACIONAR PLANO DE INVESTIGAÇÃO"

5.3.5.1 Nesta etapa, a equipe de segurança responsável define e aciona o Plano de Investigação com as etapas necessárias para atender aos requisitos do processo.

5.3.5.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo os itens 15 e 16 do Anexo A.

5.3.6 ETAPA "COMUNICAR CONCLUSÕES ÀS ÁREAS AFETADAS E ENVOLVIDAS"

5.3.6.1 Nesta etapa, a equipe de segurança responsável deverá comunicar os resultados da investigação às áreas afetadas e envolvidas.

5.4 <u>SUBPROCESSO "CONTER E CORRIGIR INCIDENTE"</u>

5.4.1 Neste subprocesso, a área de segurança responsável deverá definir o Plano de Contenção, Correção, Erradicação e acionar este plano, validar as correções com as áreas afetadas e comunicar as conclusões das correções às áreas afetadas e envolvidas.

Figura 5 - Subprocesso para Conter e Corrigir Incidente de Segurança da Informação

5.4.2 ETAPA “DEFINIR PLANO DE CONTENÇÃO, CORREÇÃO E ERRADICAÇÃO”

5.4.2.1 Nesta etapa, a área de segurança responsável deverá definir o Plano de Contenção, Correção e Erradicação do Incidente.

5.4.2.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo o item 17 do Anexo A.

5.4.3 ETAPA “CONTER, CORRIGIR E ERRADICAR INCIDENTE”

5.4.3.1 Nesta etapa, a área de segurança responsável deverá acionar o Plano de Contenção, Correção e Erradicação implantando as ações necessárias para tratar o incidente de segurança da informação.

5.4.3.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo o item 18 do Anexo A.

5.4.4 ETAPA “VALIDAR CORREÇÃO COM ÁREAS AFETADAS”

5.4.4.1 Nesta etapa, a área de segurança responsável pela implementação das medidas de tratamento do incidente deverá validar as correções com as áreas afetadas e verificar se os componentes afetados retornaram à situação de normalidade.

5.4.4.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação, preenchendo o item 19 do Anexo A.

5.4.5 ETAPA “COMUNICAR CONCLUSÕES DA CORREÇÃO ÀS ÁREAS AFETADAS E ENVOLVIDAS”

5.4.5.1 Nesta etapa, a equipe de segurança responsável deverá comunicar os resultados das correções às áreas afetadas e envolvidas.

5.5 SUBPROCESSO "FECHAR INCIDENTE"

5.5.1 Este subprocesso trata do fechamento do registro do incidente de segurança.

Figura 6 - Subprocesso para Fechar Incidente de Segurança da Informação

5.5.2 ETAPA "REGISTRAR INCIDENTE COMO FECHADO"

5.5.2.1 Nesta etapa, a equipe de segurança responsável analisa todas as informações do processo e registra o fechamento do incidente.

5.5.2.2 Essas informações deverão ser transcritas no documento GINC01 – Registro de Incidentes de Segurança da Informação do Anexo A.

5.6 SUBPROCESSO "ANALISAR INCIDENTES E PERFORMANCE"

5.6.1 Este subprocesso visa analisar o conjunto de incidentes ocorridos e a performance dos processos de segurança e operação, procurando identificar problemas de segurança, potenciais vulnerabilidades e oportunidades de melhorias de processo.

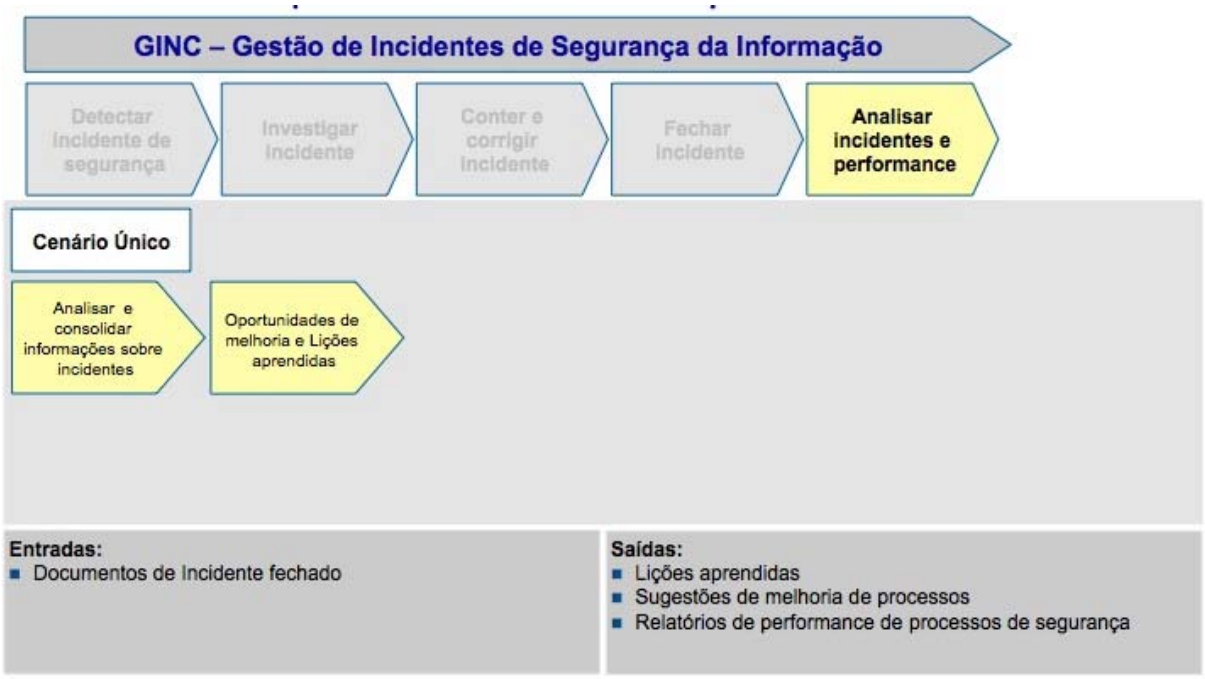

Figura 7 - Subprocesso para Analisar Incidentes de Segurança da Informação e Performance

5.6.2 ETAPA "ANALISAR E CONSOLIDAR INFORMAÇÕES SOBRE INCIDENTES"

5.6.2.1 Nesta etapa, deve-se identificar e quantificar os indicadores do processo no formulário GINC02, denominado de Identificação, Quantificação e Análise dos Indicadores do Processo (GINC02), conforme modelo apresentado no Anexo B.

5.6.3 ETAPA "IDENTIFICAR OPORTUNIDADES DE MELHORIA"

5.6.3.1 Nesta etapa, é feita a análise das informações consolidadas do processo, através dos seus indicadores, e a identificação de oportunidades de melhoria. Essas informações deverão ser transcritas no formulário GINC02, denominado de Identificação, Quantificação e Análise dos Indicadores do Processo (Anexo B).

6 DISPOSIÇÕES FINAIS

6.1 O Processo apresentado neste documento é de caráter geral e deve ser revisado a cada vinte e quatro meses.

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

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

REFERÊNCIA

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.

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. *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. *Preceitos de Segurança da Informação do DECEA*: **ICA 7-19**. Rio de Janeiro, RJ, 2012.

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. (Publicada no DOU Nº 156, de 17 Ago 2009 - Seção 1).

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. (Publicada no DOU Nº 162, de 24 Ago 2010 - Seção 1).

Anexo A – GINC01 – Registro de Incidentes de Segurança da Informação

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GINC01 – 001			OM
ASSUNTO	Registro de Incidentes de Segurança da Informação			

Área do Identificador do Incidente:	[Nome da Área do identificador do incidente]
Usuário Identificador do Incidente:	[Nome da pessoa que identificou o incidente]
Telefone/email:	[Telefone e email do identificador do incidente]
Situação do Incidente:	[aberto, em investigação, em correção, fechado]

1 Descrição do incidente

[Descrever o incidente ocorrido]

2 Como foi detectado o incidente

[Descrever como o usuário identificou o incidente]

3 Dia e hora em que o incidente ocorreu

[Informar o dia e a hora em que o incidente ocorreu]

4 Tipo de Incidente

☐ Perda de Serviços, Equipamento ou Recurso ☐ Mau Funcionamento de Sistemas

☐ Não-conformidade com Políticas ou Diretrizes ☐ Mudanças Descontroladas de Sistemas

☐ Violação de Acesso ☐ Spam ☐ Vírus/Worms

☐ Outros:_____

5 Quais operações estão indisponíveis

[Indicar quais operações foram afetadas pelo incidente identificado]

6 Quais sistemas foram afetados

[Indicar quais sistemas foram afetados pelo incidente identificado]

7	Outras informações relevantes
[Descrever outras informações que considere relevante para o tratamento deste incidente]	
8	**Correlação com outros incidentes**
[Descrever o resultado da correlação com outros incidentes já avaliados]	
9	**Nível de alerta do incidente**
[Confirmar o incidente e o nível de alerta (alto, médio ou baixo) para a organização]	
10	**Impactos do incidente**
[Descrever os reais impactos do incidente para a organização]	
11	**Tempo de resposta**
[Confirmar o tempo de resposta para investigar, conter e corrigir o incidente identificado]	
12	**Equipe de resposta**
[Identificar a equipe responsável por responder pelo incidente. Os dados de contato devem ser apresentados]	
13	**Plano de comunicação**
[Descrever o plano de comunicação do incidente]	
14	**Áreas envolvidas na investigação do incidente**
[Identificar as áreas envolvidas na investigação do incidente]	
15	**Plano de investigação do incidente**
[Descrever o plano para investigação do incidente]	
16	**Resultados da investigação do incidente**
[Descrever os resultados da execução do plano para investigação do incidente]	
17	**Plano de contenção, correção e erradicação do incidente**
[Descrever o plano para conter, corrigir e erradicar o incidente]	
18	**Resultados da contenção, correção e erradicação do incidente**
[Descrever os resultados da execução do plano para conter, corrigir e erradicar o incidente]	
19	**Resultados da validação da correção com as áreas afetadas**
[Descrever os resultados da validação da correção junto as áreas afetadas pelo incidente]	

Anexo B – GINC02 – Identificação, Quantificação e Análise dos Indicadores do Processo

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da OM por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	GINC01 – 001			OM
ASSUNTO	Identificação, Quantificação e Análise dos Indicadores do Processo			

1 MEDIÇÃO DOS INDICADORES

Indicador	Quantitativo	Observações
Quantidade de incidentes identificados		
Quantidade de incidentes por nível de criticidade		
Percentual de incidentes críticos identificados que possuem planos de ação desenvolvidos		

2 ANÁLISE DOS INDICADORES

3 AÇÕES DE MELHORIA CONTÍNUA