

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



TECNOLOGIA DA INFORMAÇÃO

ICA 7-28

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

2024

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**

2024



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

PORTARIA DECEA Nº 1.236/SNOT, DE 23 DE JANEIRO DE 2024.
Protocolo COMAER nº 67600.001357/2024-01

Aprova a reedição 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, de conformidade com o previsto no art. 21, inciso I, da Estrutura Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 11.237, de 18 de outubro de 2022, e considerando o disposto no art. 10, inciso IV, do Regulamento do DECEA, aprovado pela Portaria nº 2.030/GC3, de 22 de novembro de 2019, resolve

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

Art. 2º Revogar a Portaria DECEA nº 64/DGCEA, de 24 de junho de 2013 publicada no Boletim do Comando da Aeronáutica nº 152, de 09 de agosto de 2013.

Art. 3º Esta Instrução entra em vigor em 1º de março de 2024.

No Imp Ten Brig Ar ALCIDES TEIXEIRA BARBACOV
Diretor-Geral do DECEA

Maj Brig Ar MÁRCIO BRUNO BONOTTO

(Publicado no BCA nº , de de 2024.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES	7
1.1 <u>FINALIDADE</u>	7
1.2 <u>ÂMBITO E GRAU DE SIGILO</u>	7
1.3 <u>ABREVIATURAS</u>	7
1.4 <u>CONCEITOS</u>	7
2 RESPONSABILIDADES.....	9
2.1 <u>SUBDEPARTAMENTO TÉCNICO DO DECEA</u>	9
2.2 <u>CENTRO DE GERENCIAMENTO TÉCNICO</u>	9
2.3 <u>SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO</u>	9
2.4 <u>TIOP LOCAL – SEÇÃO DE TECNOLOGIA DA INFORMAÇÃO OPERACIONAL</u>	9
2.5 <u>ELOS DE SERVIÇOS DE TI (OPSTI)</u>	9
2.6 <u>EQUIPE DE RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</u>	9
3 PROCESSO DE GESTÃO DE LOGS	10
3.1 <u>DESCRIÇÃO DO PROCESSO</u>	10
3.2 <u>VISÃO GERAL DO PROCESSO</u>	10
3.3 <u>SUBPROCESSO “TRATAR LOGS”</u>	11
3.4 <u>SUBPROCESSO “CORRELACIONAR LOGS”</u>	13
3.5 <u>SUBPROCESSO “MELHORIA CONTÍNUA”</u>	14
3.6 <u>CONTROLE E MATURIDADE DO PROCESSO</u>	15
4 DISPOSIÇÕES FINAIS.....	18
REFERÊNCIAS	19
Anexo A – Registro GLOG01 – Identificação, Quantificação e Análise dos Indicadores do Processo	21

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 <i>Logs</i>
LAI	–	Lei de Acesso à Informação
LGPD	–	Lei Geral de Proteção de Dados
CGTEC	–	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

Os conceitos e definições estão listados no Glossário de Segurança da Informação do DECEA (MCA 7-1) e no Glossário de Segurança da Informação (Portaria GSI/PR nº 93, de 18 de outubro de 2021).

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

1.4.1 ATIVO

Constitui-se em qualquer coisa que tenha valor para o DECEA.

1.4.2 ATIVO DE INFORMAÇÃO

Todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada e os equipamentos em que ela é manuseada, transportada e descartada. O termo ativo possui esta denominação por

ser considerado um elemento de valor para um indivíduo ou organização e que, por esse motivo, necessita de proteção adequada.

1.4.3 DESCARTE

Procedimento que tem por objetivo a eliminação correta de informações, documentos, mídias e acervos digitais.

1.4.4 EVENTO

Qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Pode também ser definida como qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente.

1.4.5 INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Um incidente de segurança da informação é indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar à perda dos princípios de segurança da informação.

1.4.6 LOG

Registro de atividades gerado por programas de computador. No caso de logs relativos a incidentes de segurança, eles normalmente são gerados por firewalls ou por IDSs.

1.4.7 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.

1.4.8 NTP (*Network Time Protocol*)

Protocolo de Tempo para Redes.

1.4.9 RISCO

Probabilidade de ameaças explorarem vulnerabilidades, provocando perdas de confidencialidade, de integridade e de disponibilidade nos ativos de informação, causando, possivelmente, impactos ao negócio.

1.4.10 SANITIZAÇÃO DOS DADOS

Eliminação efetiva de informação armazenada em qualquer meio eletrônico, garantindo que os dados não possam ser reconstruídos ou recuperados.

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 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 CGTEC na geração de indicadores.

2.3.4 Tratar, conjuntamente com a TIOP local ou o Elo de Serviço do STI, ou demais seções da OM que fazem uso de ativos de informação, 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 DO STI (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.

3 PROCESSO DE GESTÃO DE LOGS

3.1 DESCRIÇÃO DO PROCESSO

3.1.1 Conforme previsto no item 3.6 da DCA 14-8 - Política de Segurança da Informação do Comando da Aeronáutica, 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 dar suporte à 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.

3.2.4 Com a aprovação do SDTE, todos os formulários descritos nesta Instrução poderão ser reproduzidos e automatizados em ferramentas de software apropriadas.



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, atualizações de sistemas considerados críticos, exceções de regras da política ou qualquer outro evento nos ativos de informação de segurança existentes, serão coletadas e normalizadas a fim de que possam ser utilizadas de forma simplificada para pesquisa e análise.

3.3.3 Devem ser mapeados os ativos de informação que contenham configurações de log detalhadas, como identificação do usuário, endereço IP, número de porta, data e hora, acesso dos usuários com privilégios etc.

3.3.4 É indispensável a coleta dos logs de consultas de DNS e URL para fins de auditoria.

3.3.5 Podem ser incluídos nesta etapa, a coleta de logs de linha de comando (CLI), tais como Power Shell, BASH e terminais de acesso remotos.

3.3.6 Sempre que necessário, devem ser coletados os logs do provedor de serviços com informações de autenticação e gerenciamento de usuários, criação e exclusão de dados etc.

3.3.7 Os ativos de informação que não possuam dados detalhados devem ser mapeados pela Seção de SSSI.

3.3.8 Os sistemas que geram *logs* deverão ter seus relógios sincronizados com pelo menos duas fontes de tempo precisa via protocolo NTP (*Network Time Protocol*). Um tempo-padrão de referência para o DECEA e Organizações militares subordinadas deve ser definido e usado para garantir a exatidão dos registros (*logs*) para que as informações possam ser utilizadas de forma

confiável, como, por exemplo, para tratamento de incidentes em segurança da informação ou perícia forense.

3.3.9 Em caso de incidente de segurança da informação, ou quaisquer outros eventos de segurança, a Seção de SSSI deve coletar e preservar todos os registros de eventos e suas mídias de armazenamento de ativos de informação afetados pelo evento.

3.3.10 As Seções de SSSI devem manter a estrutura original de diretórios e de seus metadados constantes nos arquivos de configuração de logs.

3.3.11 Caso haja impossibilidade de preservar as evidências do evento de segurança, o CGTEC e os Elos de Serviço do STI (OPSTI) devem justificar em relatório, a falta destas evidências.

3.3.12 Em caso de indisponibilidade de sistema ou serviço, as ações para o seu restabelecimento não devem impossibilitar a coleta, a preservação e disponibilidade das evidências na sua integralidade.

3.3.13 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.

3.3.14 Já na etapa “Armazenar *Logs*”, os mesmos deverão ser armazenados de acordo com a DCA 7-2 Diretriz de Segurança da Informação vigente no DECEA.

3.3.15 A capacidade de armazenamento dos logs deve ser constantemente verificada.

3.3.16 Os logs e registros de auditoria de ativos da informação devem ser criados e armazenados para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

3.3.17 Os registros de auditoria devem ser retidos por um período mínimo de 1 (um) ano e desde que não sejam mais necessários para fins administrativos, legais ou outros fins operacionais.

3.3.18 As informações de eventos de registros e seus recursos devem ser protegidos contra acesso não autorizado e adulteração.

3.3.19 A exclusão de logs deve ser eficiente e com base nas melhores práticas de segurança da informação e atos normativos como LGPD e LAI.

3.3.20 Conforme previsto no art. 16 da LGPD, deve ser observado os logs armazenados que contiverem dados pessoais a fim de avaliar se os logs serão eliminados, no âmbito e nos limites técnicos das atividades, ou conservados após o término de seu tratamento.

3.3.21 As técnicas de descarte, ou sanitização dos dados, durante a fase de exclusão dos logs, devem estar de acordo com o item 4.7.3 da ICA 7-29 – Processo de Gestão de Cópias do Departamento de Controle do Espaço Aéreo.

3.3.22 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 Cada Organização Militar deve buscar soluções que visem a correlação de eventos de segurança de forma unificada quando houver tecnologias heterogêneas.

3.4.4 Quando houver mais de um repositório de logs ou fontes diversas de logs, os eventos devem ser correlacionados.

3.4.5 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.

3.4.6 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.

3.4.7 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.

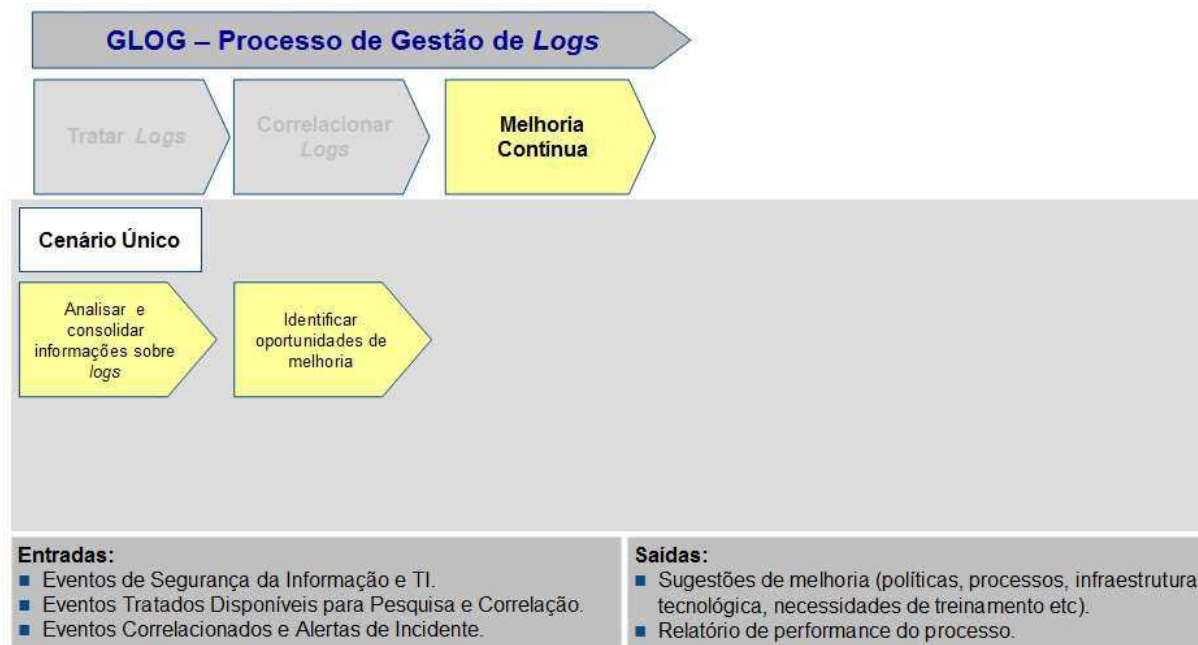


Figura 4 - Subprocesso para Melhoria Contínua

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 Deve ser analisado o comportamento dos ativos de informação com o objetivo de detectar e mitigar a execução de comandos e scripts que possam indicar ações maliciosas.

3.5.4 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.

3.5.5 Os indicadores relacionados a investigações de segurança da informação podem ser criados e adicionados em um ambiente de gerenciamento de logs para fins de melhoria contínua no processo de gestão de logs.

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, bem como 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
2 – Repetível, mas intuitivo	<ul style="list-style-type: none">• Possuir uma normativa interna do DECEA para a Gestão de <i>Logs</i>.• Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA.
3 – Processo Definido	<ul style="list-style-type: none">• Implantar o processo em todas as Organizações Subordinadas ao DECEA.• Capacitar todos os chefes das seções de segurança da informação.
4 – Gerenciado e Mensurável	<ul style="list-style-type: none">• Criar um painel para acompanhamento, através de indicadores gerenciais do processo, a fim de garantir a tomada de decisão pela Direção do DECEA.
5 – Otimizado	<ul style="list-style-type: none">• Realizar uma reunião semestral de análise crítica para melhoria contínua do processo.• Possuir sistema informatizado para emissão de relatórios automatizados.

3.6.1.3 Cada Organização deverá elaborar e encaminhar ao Subdepartamento Técnico do DECEA um Relatório de Evolução dos Níveis de Maturidade, que deverá ser atualizado anualmente e sempre que houver alteração no nível de maturidade.

3.6.1.4 O Relatório de Evolução dos Níveis de Maturidade deverá conter, no mínimo:

- a) O nível de maturidade e a meta atual;
- b) As mudanças e justificativas em relação ao nível de maturidade; e
- c) O prazo de evolução dos níveis de maturidade.

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
<ul style="list-style-type: none">• 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.	<ul style="list-style-type: none">• Quantidade de ativos de informação com <i>logs</i> tratados e correlacionados;• Quantidade de incidentes de segurança da informação descobertos mediante o correlacionamento de <i>logs</i>; 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 será 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 27001. **Tecnologia da informação: Técnicas de segurança: Sistemas de gestão de segurança da informação - Requisitos.** Rio de Janeiro, RJ, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT NBR ISO/IEC 27002. **Tecnologia da Informação: Técnicas de segurança: Código de práticas para a gestão da segurança da informação.** Rio de Janeiro, RJ, 2022.

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, 2019.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 143 /SNOT, de 16 de abril de 2022. Aprova a reedição da “Diretriz do Comando da Aeronáutica que dispõe sobre a Segurança da Informação do Departamento de Controle do Espaço Aéreo” = **DCA 7-2**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 83, 05 maio 2022.

BRASIL Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria GABAER nº 273/GC3, de 18 de abril de 2022. Aprova a Diretriz que estabelece a “Política de Segurança da Informação do Comando da Aeronáutica” = **DCA 14-8**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 74, 18 abr. 2022.

BRASIL. 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” = **ICA 7-23** Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2013, n. 121, 27 jun. 2013.

BRASIL. Comando da Aeronáutica. Estado-Maior da Aeronáutica. Portaria EMAER nº45/CEMAER, de 22 de novembro de 2022. “Estrutura e Competências do Sistema de Tecnologia da Informação do Comando da Aeronáutica” = **NSCA 7-7**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 224, 07 dez. 2022.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. Portaria DECEA nº 745 /DGCEA, de 14 de fevereiro de 2023. Aprova a reedição do “Glossário de Segurança da Informação do Departamento de Controle do Espaço Aéreo” = **MCA 7-1**. Boletim do Comando da Aeronáutica, Rio de Janeiro, RJ, 2022, n. 39, 01 mar. 2023.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 248, 27 dez. 2018 - Seção 1.

BRASIL. Instrução Normativa GSI nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 101, 28 maio 2020 – Seção 1.

BRASIL. Instrução Normativa GSI nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 101, 31 maio 2021 - Seção 1.

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011**. Lei de Acesso à Informação (LAI). **Diário Oficial da República Federativa do Brasil**, Brasília, DF, Edição Extra, 18 nov. 2018 - Seção 1.

BRASIL **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 157, 15 ago. 2018 – Seção 1.

BRASIL. Portaria GSI_PR Nº 93, de 18 de outubro de 2021. Glossário de Segurança Institucional da Presidência da República. Glossário de Segurança da Informação. **Diário Oficial da República Federativa do Brasil**, Brasília, DF, n. 197, 19 out. 2021, Seção 1.

Publicação do TCU sobre descarte de mídias. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp%3FfileId%3D8A8182A25232C6DE0152A27D76A458D8&sa=U&ved=2ahUKEwiytu-c59_4AhV9uZUCHXFaBPgQFnoECAgQAQ&usg=AOvVaw2zh_XgKRPST8_JoypXVdhE. Acesso em: 20/09/2022.

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

<div>COMANDO DA AERONÁUTICA</div> <div>DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO</div> <div><inserir nome por extenso da OM></div>				
	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				