MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

ICA 7-37

GESTÃO DE CONTROLE DE ACESSO, IDENTIDADE E CRIPTOGRAFIA DE TECNOLOGIA DA INFORMAÇÃO NO ÂMBITO DO DECEA

2015

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

TECNOLOGIA DA INFORMAÇÃO

ICA 7-37

GESTÃO DE CONTROLE DE ACESSO, IDENTIDADE E CRIPTOGRAFIA DE TECNOLOGIA DA INFORMAÇÃO NO ÂMBITO DO DECEA

2015

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

PORTARIA DECEA Nº 289/DGCEA, DE 1º DE SETEMBRO DE 2015.

Aprova a edição da Instrução de Gestão de Controle de Acesso, Identidade e Criptografia de Tecnologia da Informação no âmbito do DECEA.

O DIRETOR-GERAL DO DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO, no uso das atribuições que lhe confere o inciso IV art. 195 do Regimento Interno do Comando da Aeronáutica, aprovado pela Portaria nº 1049/GC3, de 11 de novembro de 2009, e o inciso IV do art. 10 do Regulamento do DECEA, aprovado pela Portaria nº 1.668/GC3, de 16 de setembro de 2013, resolve:

Art. 1º Aprovar a edição da ICA 7-37 "Gestão de Controle de Acesso, Identidade e Criptografia de Tecnologia da Informação no âmbito do DECEA", que com esta baixa.

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

(a)Ten Brig Ar CARLOS VUYK DE AQUINO
Diretor-Geral do DECEA

(Publicado no BCA nº 183, de 30 de setembro de 2015.)

SUMÁRIO

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar os processos de Gestão de Controle de Acessos, Identidade e Criptográfico, prevenindo os acessos físicos e lógicos não autorizados, bem como as regras para uso de chaves criptográficas. Esses processos visam à proteção da confidencialidade, à integridade, à autenticidade e ao não repúdio das informações de interesse do Departamento de Controle do Espaço Aéreo e suas Organizações Militares subordinadas.

1.2 CONCEITUAÇÕES

1.2.1 CONTA DE REDE

É uma conta que identifica e possibilita que o usuário acesse os serviços da rede interna da OM, tais como um computador ou um repositório devidamente configurado na rede.

1.2.2 CONTA DE SISTEMA

É uma conta que identifica e possibilita que o usuário acesse os sistemas de *software* da OM.

1.2.3 IDENTIFICAÇÃO POSITIVA DO USUÁRIO

Quando se tem certeza de que a pessoa que solicita um serviço é ela mesma.

1.2.4 MATRIZ RACI

RACI é o acrônimo em inglês para *Responsible* (responsável), *Accountable* (aprovador), *Consulted* (consultado), e *Informed* (informado). A matriz RACI apresenta a relação entre papéis desempenhados e atividades e/ou artefatos a serem entregues para um projeto. As atividades e os artefatos podem ser obtidos da EAP (Estrutura Analítica de Projetos ou WBS – Work Breakdown Structure), que é um processo de subdivisão das entregas e do trabalho do projeto em componentes menores e mais facilmente gerenciáveis. É estruturada em árvore exaustiva, hierárquica (de mais geral para mais específica) orientada às entregas, fases de ciclo de vida ou por sub-projetos (releases) que precisam ser feitas para completar um projeto.

1.2.5 NORMA PADRÃO DE AÇÃO (NPA)

É um documento interno usado para padronizar os procedimentos e processos rotineiros a serem seguidos em uma determinada atividade. É aprovada pelo Comandante da OM, quando elaborada por subordinado. Sua efetivação, alterações e cancelamento devem constar no Boletim Interno (BI) da OM.

1.2.6 PRESTADOR DE SERVIÇO

É a pessoa vinculada à empresa que atua dentro da OM.

1.2.7 PROCESSO

É um conjunto sequencial de ações ou atividades específicas com a finalidade de alcançar um determinado objetivo. Pode ser composto de uma ou mais entradas, que são processadas, retornando uma ou mais saídas.

1.2.8 REDE CORPORATIVA

Infraestrutura que permite a transmissão de dados entre diversos equipamentos de uma mesma corporação, tais como computadores pessoais, servidores de arquivos, impressoras, câmeras de vídeo. Essa infraestrutura também permite a troca de dados com a Internet (mundo externo).

1.2.9 SEÇÃO DE TECNOLOGIA DA INFORMAÇÃO (STI)

Seção responsável por executar as atividades de infraestrutura de TI da OM.

1.2.10 USUÁRIOS

São considerados usuários todas as pessoas alocadas na OM.

1.3 SIGLAS E ABREVIATURAS

DECEA - Departamento de Controle do Espaço Aéreo
NPA - Norma Padrão de Ação
OM - Organização Militar
OPSTI - Organização Provedora dos Serviços de TI
RACI - *Responsible, Accountable, Consulted, Informed*
SAUTI - Serviço de Atendimento aos Usuários de Tecnologia da Informação
SDTE - Subdepartamento Técnico do DECEA
SSSI - Seção de Segurança de Sistemas da Informação
STI - Seção de Tecnologia da Informação
TI - Tecnologia da Informação
VPN - *Virtual Private Network* (Rede Privada Virtual)

1.4 ÂMBITO

A presente Instrução aplica-se no âmbito do DECEA e Organizações Militares (OM) subordinadas.

2 PROCESSO DE GESTÃO DE CONTROLE DE ACESSOS

2.1 VISÃO GERAL DO PROCESSO

2.1.1 A segurança no processo de concessão de acesso à informação do DECEA é muito importante para a redução de risco de erro humano, fraude ou uso indevido das informações.

2.1.2 A assinatura do Termo de Sigilo e Confiabilidade é pré-requisito para obtenção de acesso aos sistemas, redes, acesso remoto, Internet e informações da OM, assim como para formalização das responsabilidades relacionadas a esses acessos.

2.1.3 Os acessos aos recursos, serviços e informações devem ser compatíveis com as reais necessidades de cada OM, restringindo o acesso a qualquer outro elemento considerado desnecessário. Para tanto é necessário que a concessão de acesso seja solicitada e autorizada pelo chefe imediato do solicitante e validado pela Seção de Tecnologia da Informação (STI).

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

2.1.5 No caso do processo de controle de acesso, ele é composto por 2 (dois) subprocessos a seguir descritos: controle de acesso lógico e controle de acesso físico.

2.2 CONTROLE DE ACESSO LÓGICO

Nesta etapa, o controle de acesso, na segurança da informação, é composto dos processos de autenticação, autorização e auditoria. Nesse contexto, o controle de acesso pode ser entendido como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo). A autenticação confirma a identidade do usuário (pessoa ou outro sistema) que acessa o sistema, a autorização determina o que um usuário autenticado pode executar e a auditoria diz o que o usuário fez.

2.2.1 CONTROLE DE ACESSO A CONTAS

2.2.1.1 Cada usuário deve possuir uma conta individual, pessoal e intransferível. Não devem existir contas corporativas ou contas compartilhadas por mais de um usuário.

2.2.1.2 O sistema de controle de acesso deve permitir ao usuário alterar sua senha sempre que desejar. A troca da senha de uma conta bloqueada só deve ser executada após a identificação positiva do usuário.

2.2.1.3 Todo pessoal efetivo, quando do seu desligamento da OM, deverá ter sua conta cancelada no ato do afastamento.

2.2.1.4 O setor de Recursos Humanos ao qual esteja vinculado o funcionário desligado ou afastado deve comunicar ao responsável de Segurança e Defesa e ao de TI da OM para as providências.

2.2.1.5 As senhas de acesso lógico aos equipamentos devem ser trocadas periodicamente, a cada 90 dias no máximo, não podendo ser reutilizadas as 3 (três) últimas senhas.

2.2.1.6 Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário.

2.2.1.7 Toda conta de usuário deve possuir senha e deve seguir os padrões estabelecidos nesta norma.

2.2.1.8 As contas de acesso serão bloqueadas depois de 3 (três) tentativas inválidas de entrada. Para desbloquear, o usuário deverá fazê-lo por intermédio do SAUTI.

2.2.1.9 As contas que ficarem inativas por mais de 90 (noventa) dias corridos deverão ser bloqueadas.

2.2.1.10 A senha deverá conter no mínimo 8 (oito) caracteres e deve ser definida com letras, números e caracteres especiais, tais como: #, @, $, %, &, !, *, ?, _, /, <, >, ;, {, }, [,], =, +.

2.2.1.11 O sistema de controle de acesso deve solicitar nova autenticação após certo tempo de inatividade da sessão (*timeout*), a ser definido pelo setor de TI de cada OM.

2.2.1.12 O setor de Recursos Humanos deve relacionar claramente as atribuições de cada função do efetivo, de acordo com a característica das atividades desenvolvidas, a fim de determinar o perfil necessário da pessoa.

2.2.1.13 Todos os usuários devem possuir contas sem privilégios de administrador, independentemente do nível hierárquico. As solicitações de contas administrativas serão analisadas pela STI.

2.2.1.14 As contas administrativas não devem possuir nomes que as identifiquem como administrativas.

2.2.1.15 As contas administrativas não devem ser compartilhadas. Cada usuário que necessitar de uma conta administrativa deve possuir uma conta individual, isso permite a rastreabilidade.

2.2.1.16 Uma conta/*login* de acesso com privilégios de administrador somente deverá ser utilizada para atividades que necessitem desses privilégios.

2.2.1.17 Atividades que não necessitem de privilégios de administrador devem obrigatoriamente ser realizadas por meio da credencial de acesso individual.

2.2.1.18 O uso inapropriado de privilégios de administrador de acesso pode ser um grande fator de contribuição para falhas ou violações, permitindo a divulgação ou modificação imprópria de informações, fraudes e sabotagens. Assim, os seguintes procedimentos devem ser adotados pelo setor de TI de cada OM:

a) a concessão de privilégios de administrador de acesso a usuários deve ser fornecida conforme sua necessidade de uso e em conformidade com a política de acesso;

b) a concessão de privilégios de administrador de acesso deve ser fornecida somente após a conclusão dos procedimentos de autorização formal; e

c) a concessão de privilégios de administrador somente deve ser autorizada mediante justificativa formal e avaliação individual quanto a sua real necessidade por parte do chefe da STI e das áreas envolvidas.

2.2.1.19 Todo usuário deve possuir uma identificação. É vedado o uso da identificação de outro usuário.

2.2.1.20 Os sistemas de *software*:

a) devem possuir recursos para restringir acesso apenas a pessoas autorizadas, isto é, devem possuir um sistema de autenticação de contas;

b) devem possuir recursos de registro de tentativa de autenticação de sucesso ou falhas, para ser analisados posteriormente em logs, conforme a ICA 7-28 – Procedimentos do Processo de Gestão de Logs;

c) devem possuir um sistema de alerta caso a política de acesso seja violada, para que esse tipo de falha seja monitorada;

d) devem restringir o tempo de conexão de acesso, ou seja, caso o sistema fique inativo por 10 minutos, a conta de acesso deve expirar;

e) devem possuir mecanismo de entrada com o mínimo de informação para evitar dar oportunidade às pessoas mal-intencionadas;

f) devem mostrar informações de ajuda do sistema apenas depois que a autenticação do usuário for confirmada;

g) devem conter um aviso na tela inicial descrevendo que apenas pessoas autorizadas podem ter acesso; e

h) podem utilizar uma solução centralizada para facilitar o gerenciamento do acesso ao sistema.

2.2.1.21 Para solicitar um acesso lógico, a sistemas ou roteadores, por exemplo, o chefe da seção deverá preencher o Formulário de Solicitação de Acesso (Anexo A) e enviar ao chefe da STI.

2.2.1.22 Para solicitar um acesso físico, a um prédio ou setor, por exemplo, o chefe da seção deverá preencher o Formulário de Solicitação de Acesso (Anexo A) e enviar ao chefe de Segurança e Defesa.

2.2.2 ACESSO REMOTO

2.2.2.1 O acesso remoto aos servidores deve ser realizado adotando os mecanismos de segurança predefinidos, para evitar ameaças à integridade e ao sigilo do serviço. As definições dos mecanismos de segurança e sua divulgação cabem à OM responsável pelo serviço.

2.2.2.2 Somente a STI pode fornecer acesso remoto à OM, sendo esses os responsáveis pela configuração do *hardware* e *software*.

2.2.2.3 A autenticação deve ser necessariamente por meio de senhas. Não deverá ser permitido múltiplo acesso simultâneo para o mesmo usuário, com exceção dos casos analisados e autorizados pelos chefes responsáveis.

2.2.2.4 Para solicitar acesso remoto (lógico), o Formulário de Solicitação de Acesso (Anexo A) deve ser preenchido e enviado pelo chefe da seção para a chefia da STI.

2.2.3 CONTROLE DE ACESSO A CORREIO ELETRÔNICO

2.2.3.1 Apenas usuários do efetivo da OM devem ter acesso ao correio eletrônico da Organização. O endereço de *e-mail* da Intraer deve ser padronizado, colocando o nome de guerra seguido das iniciais do nome e sobrenomes.

2.2.3.2 Para *e-mails* externos devem-se usar contas genéricas com o nome do departamento, por exemplo.

2.2.3.3 Os prestadores de serviços que precisarem ter acesso ao *e-mail*, tanto externo quanto interno, não devem seguir o mesmo padrão do efetivo interno, e devem identificar-se com o nome da empresa prestadora de serviço e departamento em que trabalham, para que sejam facilmente rastreados.

2.2.3.4 Todas as mensagens enviadas pelo correio eletrônico das OM são consideradas comunicação formal, cujo conteúdo deve ser ponderado antes da emissão.

2.2.3.5 O acesso ao correio eletrônico só é permitido se o colaborador já estiver cadastrado na Rede Corporativa.

2.2.3.6 A conta de *e-mail* é disponibilizada exclusivamente para uso institucional, não sendo admitido para uso pessoal.

2.2.3.7 Para solicitar acesso ao correio eletrônico, o Formulário de Solicitação de Acesso (Anexo A) deve ser preenchido e enviado pelo chefe da seção.

2.2.4 CONTROLE DE ACESSO À INTERNET

2.2.4.1 O acesso padrão à Internet concedido aos usuários deve restringir o acesso a *sites* que acarretem quaisquer tipos de risco a rede interna do DECEA, por meio de regras definidas pelo STI.

2.2.4.2 A limitação do acesso à Internet é prerrogativa da OM, quando considerar que esse recurso está sendo utilizado de maneira inadequada, ou afetando negativamente a disponibilidade e produtividade dos demais serviços, que se utilizam da rede de informática da OM.

2.2.4.3 O STI poderá bloquear acesso a *sites* sempre que comprometer o fluxo de dados de áreas críticas.

2.2.4.4 Quando houver alguma necessidade específica de acesso por meio dos protocolos (HTTP ou HTTPS), deverá ser solicitado e autorizado pelo setor de STI. Casos específicos que exijam outros tipos de serviço e protocolos deverão ser analisados e autorizados pela SSSI.

2.2.4.5 É proibida a divulgação de informações confidenciais da instituição em quaisquer grupos de discussão, listas ou bate-papos, não importando se a divulgação foi deliberada ou inadvertida, sendo possível sofrer as penalidades previstas nas políticas e procedimentos internos e/ou as sanções legais.

2.2.4.6 Para solicitar acesso à Internet, o Formulário de Solicitação de Acesso (Anexo A) deve ser preenchido e enviado pelo chefe da seção.

2.2.5 CONTROLE DE ACESSO A DIRETÓRIOS DA REDE

2.2.5.1 O Diretório é uma estrutura de pastas utilizada para organizar arquivos. Geralmente, o acesso é compartilhado por um grupo de pessoas.

2.2.5.2 O acesso deverá ser efetuado apenas por pessoas autorizadas, por meio de um servidor de arquivos.

2.2.5.3 Para criar um diretório de rede, o solicitante deve ter a aprovação do seu chefe imediato, ocasião em que será feita a análise da real necessidade pela STI.

2.2.5.4 Caso o diretório que se deseja acessar pertença a outra seção, a solicitação será avaliada pela STI e pelo chefe imediato da outra seção.

2.2.5.5 O Acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela administração da rede.

2.2.5.6 Para solicitar acesso ao diretório de rede, o Formulário de Solicitação de Acesso (Anexo A) deve ser preenchido e enviado pelo chefe da seção.

2.2.6 GESTÃO DE REVISÃO DE ACESSOS

2.2.6.1 A liberação de acessos a sistemas, diretórios, grupo de acessos ou perfis administrativos oferecidos aos usuários necessitam de revisão periódica, para assegurar que os acessos estejam compatíveis com o cargo, a seção e as funções exercidas.

2.2.6.2 Os direitos de acessos devem ser revisados periodicamente, a cada seis meses ou depois de alguma mudança de cargo ou desligamento.

2.2.6.3 Os direitos de acessos especiais devem ser revisados periodicamente, a cada três meses.

2.2.7 POLÍTICA DE MESA E TELA LIMPA

2.2.7.1 As OM devem adotar a política de mesa limpa de papéis e mídias de armazenamento e política de tela limpa para os recursos computacionais.

2.2.7.2 Informações reservadas em papel ou em mídia removível devem ser armazenadas em lugares seguros quando não estiverem em uso.

2.2.7.3 Documentos reservados devem ser removidos da impressora logo após sua impressão.

2.2.7.4 Recursos computacionais devem ser mantidos desligados ou com a tela bloqueada com mecanismo de senha quando não estiverem sendo usados.

2.3 <u>CONTROLE DE ACESSO FÍSICO</u>

2.3.1 O acesso a um espaço físico ou a uma propriedade deve ser controlado e somente pessoas autorizadas podem acessar esse local. Neste contexto, o controle de acesso físico pode ser entendido como a habilidade de permitir ou negar acesso a um local por um sujeito (uma entidade ativa, como um indivíduo).

2.3.2 CONTROLE DE ENTRADA

2.3.2.1 O acesso às dependências do DECEA e OM subordinadas só é permitido com identificação por meio de um crachá. A identificação deve estar visível.

2.3.2.2 No caso do prestador de serviço, o crachá deve possuir nome, foto e nome da empresa, além de ter o crachá de visitante da OM.

2.3.2.3 Caso alguém esteja nas dependências sem crachá, deve-se avisar ao setor de Segurança e Defesa imediatamente.

2.3.2.4 Para acessar as dependências do DECEA e OM subordinadas com um veículo, o mesmo deve estar devidamente cadastrado junto à seção de Segurança e Defesa e portar a identificação no para-brisa do veículo.

2.3.2.5 O acesso às seções deve ser controlado. Só é permitida a entrada em outras seções mediante autorização e acompanhamento de alguém do efetivo dessas seções.

2.3.2.6 No caso de um visitante ou prestador de serviço não autorizado, deve-se notificar imediatamente o setor de Segurança e Defesa e solicitar auxílio para remoção do mesmo.

2.3.2.7 Caso alguma pessoa cometa crime contra a propriedade pública, deve-se notificar o setor de Segurança e Defesa para que este entre em contato com as autoridades competentes.

2.3.2.8 Caso haja a necessidade do acesso ao prédio fora do expediente, deve ser solicitada autorização ao chefe da seção. O chefe deve preencher o Formulário de Acesso e enviar à seção de Segurança e Defesa (Anexo A).

2.3.2.9 O acesso com cartão é necessário para o efetivo, inclusive em horário comercial. Todas as portas externas devem estar bloqueadas fora do horário comercial.

2.3.2.10 Os visitantes devem identificar-se na portaria e realizar um cadastro.

2.3.3 ÁREAS SEGURAS

2.3.3.1 Aos prestadores de serviços que realizam manutenção deve ser concedido acesso restrito dentro das áreas seguras, quando necessário, além de ser autorizado e monitorado.

2.3.3.2 No STI, só deve ser permitida a entrada de pessoas autorizadas e com mecanismo eletrônico de controle de acesso. Quando alguém do efetivo necessitar de atendimento, o mesmo deverá aguardar em uma antessala.

2.3.3.3 As salas técnicas (CPD) devem permanecer sempre fechadas e refrigeradas. Devem conter equipamentos de detecção e combate a incêndio.

2.3.3.4 Todas as portas, fechaduras e métodos de acesso que não estejam funcionando devem ser informados ao setor de Segurança e Defesa. A segurança coordenará com o setor responsável pela manutenção a correção do equipamento defeituoso.

2.3.3.5 Não deve ser permitido o uso de qualquer equipamento fotográfico ou gravador de áudio ou vídeo dentro das áreas restritas.

2.3.3.6 Recomenda-se que o Controle de Acesso utilize como validação um sistema de cartão com PIN (*personal identification number*). Eventualmente, em locais mais críticos, pode-se optar também pela validação biométrica.

2.3.3.7 Qualquer pessoa dentro de uma área de segurança deverá dispor de identificação de acordo com a função por ela exercida.

2.3.3.8 Serviços realizados por trabalhadores/empregados de empresas contratadas em instalações de processamento devem ser agendados previamente. Deve ser fornecido o nome das pessoas que executarão o serviço, assim como o detalhamento da atividade a ser desenvolvida.

2.3.3.9 Tanto para o caso de trabalhadores/empregados de empresas contratadas quanto para visitantes, uma pessoa do efetivo da OM deve sempre acompanhar o trabalho, de forma que o visitante nunca fique sozinho nas instalações.

2.3.3.10 Deve-se utilizar Circuito Fechado de TV nas áreas consideradas estratégicas com vistas ao controle de acesso, havendo registro da imagem local por meio de câmeras de vídeo, que deverão ser armazenadas em alguma mídia ou dispositivo de armazenamento, de forma a poder ser resgatadas em caso de alguma ocorrência ou auditoria.

2.3.4 ENERGIA ELÉTRICA

2.3.4.1 As OM devem ter seus equipamentos protegidos contra falta de energia elétrica.

2.3.4.2 Recomenda-se o uso de UPS para suportar paradas e desligamento dos equipamentos e para manter equipamentos em operação durante situações críticas.

2.3.4.3 As UPS devem possuir plano de contingência em caso de falhas.

2.3.4.4 Deve ser considerado também um gerador de energia elétrica para garantir os serviços e equipamentos que em caso de falta de energia da concessionária precisem continuar com a operação.

2.3.4.5 Tanto as UPS quanto os geradores devem ser verificados em intervalos regulares para que o seu bom funcionamento seja garantido.

2.3.5 CABEAMENTO

2.3.5.1 Os cabeamentos de energia e os de dados devem ser protegidos contra danos.

2.3.5.2 Os cabeamentos de dados que vão para a sala técnica devem ser subterrâneos ou ficar abaixo do piso.

2.3.5.3 O cabeamento de dados deve ser protegido contra interceptação não autorizada, além de passar por um conduíte ou abaixo do piso.

2.3.5.4 Os cabos de dados e de energia devem ficar separados para evitar algum tipo de interferência.

2.3.6 DISPOSITIVOS MÓVEIS

2.3.6.1 Os dispositivos móveis como *notebooks* e celulares usados fora das dependências militares devem receber cuidados especiais. Os equipamentos devem possuir maletas para que haja proteção contra danos. Além disso, devem possuir senhas e, quando em locais públicos, não devem ficar sem supervisão em hipótese alguma.

2.3.6.2 Os *notebooks* que armazenam arquivos sigilosos devem ter seus discos rígidos (HD) criptografados.

2.3.7 DESCARTE DE MATERIAL

2.3.7.1 Os equipamentos e dispositivos que possuem mídias de armazenamento de dados devem ser examinados antes do descarte, para garantir que dados sigilosos e licenças de *softwares* sejam removidos por meios e técnicas que tornem os dados originais irrecuperáveis.

2.3.7.2 Os equipamentos defeituosos que contenham informações sensíveis deverão ter o seu risco analisado pela STI para determinar a destruição ou envio para conserto.

3 PROCESSO DE GESTÃO DE IDENTIDADE

3.1 VISÃO GERAL DO PROCESSO

3.1.1 A segurança no processo de gestão de identidade é fundamental para a proteção das informações da OM.

3.1.2 A gestão de identidade pode ser definida como a combinação de sistemas, regras e procedimentos que definem a posse, utilização e segurança de uma identidade digital, controlando todo o ciclo de vida (criação, manutenção e uso de identidades digitais) envolvido na execução deste processo.

3.1.3 Seu objetivo é estabelecer a confiança na associação de atributos a uma identidade digital e conectar essa identidade a uma entidade individual.

3.1.4 A criação de um portfólio de Gestão da Identidade no DECEA deverá contar com o apoio do STI, cujos conceitos são fundamentais para a criação de um ambiente seguro de gestão da identidade.

3.2 GESTÃO DE AUTENTICAÇÃO

3.2.1 A utilização de mecanismos de autenticação para aplicações WEB é fundamental para boa segurança. Alguns dos mecanismos essenciais são:

a) *Windows authentication*;

b) *Forms authentication*; e

c) *Passport authentication*.

3.2.2 Os dados que compõem a identidade devem ser vinculados a atributos, para que possam ter vínculo com o sistema que irá utilizá-los.

3.2.3 A autenticação baseada no conhecimento é o método mais utilizado em aplicações WEB.

3.2.4 Todos os servidores das OM devem suportar SSL, ou seja, a encriptação dos dados cliente/servidor.

3.2.5 O protocolo SSL provê a privacidade e a integridade de dados entre duas aplicações que estejam se comunicando pela Internet. Isso ocorre por meio da autenticação das partes envolvidas e da criptografia dos dados transmitidos entre as partes. Esse protocolo auxilia a prevenir que intermediários entre as duas pontas da comunicação tenham acesso indevido ou falsifiquem os dados sendo transmitidos.

3.3 GESTÃO DE PROVISIONAMENTO

3.3.1 Existência de pacotes básicos de acesso por função. Isso reduz drasticamente o número de solicitações de acesso a recursos.

3.3.2 As OM devem centralizar a administração dos usuários no mesmo repositório em uma interface unificada, reduzindo a complexidade de tarefas administrativas comuns.

3.3.3 As OM devem sincronizar usuários e senhas por meio de uma política segura, garantindo o nível adequado de acesso para cada funcionário;

3.3.4 Todos os usuários novos devem receber uma nova conta de acesso com usuário e senha para acessar várias aplicações dentro do ambiente do DECEA e OM subordinadas.

3.3.5 Os chefes de seção devem ser responsáveis pela aprovação do acesso dos novos funcionários aos sistemas.

3.3.6 A representação da conta de acesso deve ser feita através de um identificador único integrado a outros atributos, como um número de documento, nome completo, data de nascimento etc.

3.3.7 As OM devem possuir um responsável por estabelecer e manter os dados (regras de acesso, requisitos de credenciais) para uma determinada informação ou recurso que possa ser acessado.

3.3.8 O número de contas provisionadas deve acompanhar a quantidade de novos colaboradores da OM. Quando há uma discrepância significativa entre o número de contas provisionadas e o número total de novos usuários durante um determinado período, esse desequilíbrio indica que os processos de identidade estão ineficientes.

3.4 GESTÃO DE DESAPROVISIONAMENTO

3.4.1 Quando um usuário for transferido da OM, a conta deverá ser cancelada, assim como todos os sistemas e recursos relacionados. Isso deve ser feito alterando ou bloqueando a senha.

3.4.2 Quando o usuário for desligado da OM, deverá ser retirada sua credencial, identificação, *token*, crachá, uso de equipamentos, mecanismos. Ademais, acessos físicos e lógicos devem ser revogados.

3.4.3 Deverá haver ao menos três pessoas envolvidas para garantir que a conta do usuário seja reconfigurada corretamente para refletir suas novas responsabilidades:

a) usuário;

b) chefe da Seção Anterior; e

c) chefe da nova Seção.

3.4.4 O STI deve determinar o que deve ser feito para encerrar de forma clara as responsabilidades antigas do usuário e as ações para preparar a conta do usuário para suas novas responsabilidades.

3.4.5 O STI deve rever cuidadosamente a conta para garantir que tenha somente aqueles recursos e privilégios apropriados às novas responsabilidades do usuário.

3.5 MAPA DE FUNÇÃO

3.5.1 A gestão de identidade é o processo de automatizar as concessões de acesso da organização no mesmo repositório, por meio de fluxos integrados a uma plataforma centralizada de aprovisionamento, com a automatização de procedimentos e mapeamento dos perfis de acesso de usuários.

3.5.2 Para isso, é necessário realizar um mapeamento relativo à massa informacional agregada ao perfil dos colaboradores (cargo, centro de custo, gestor etc.), para garantir o controle do ciclo das identidades dos usuários por meio do projeto de gerenciamento nas diferentes plataformas da organização.

3.5.3 Cada OM deverá elaborar a matriz de responsabilidades (Matriz RACI), além de definir os atores envolvidos nos *workflows* (aprovadores, executores, gestores, normativos).

3.6 GESTÃO DE CONFIGURAÇÃO DE IDENTIDADES

3.6.1 As aplicações devem ser monitoradas para verificar as permissões de acesso. Como os papéis dos colaboradores mudam na Organização, seus acessos às informações devem mudar também. É importante que os usuários não continuem tendo acesso à informações da antiga seção quando são transferidos ou promovidos.

3.6.2 Esse monitoramento ocorre também com os diretórios da rede. Sempre que um usuário mudar de seção seu acesso ao diretório também dever ser cancelado e solicitado novo acesso para a nova seção.

3.6.3 Os usuários deverão ter acesso somente aos diretórios de sua seção na OM. Quando for necessário o acesso ao diretório de outra seção, o usuário deve ter uma autorização de seu chefe de seção e do chefe da seção responsável pelo diretório.

3.6.4 As OM devem possuir uma gestão de políticas e processos que definam como são fornecidos os direitos de acesso das entidades aos sistemas de informação.

3.7 AUDITORIA E RELATÓRIO

3.7.1 As OM devem possuir um responsável pelos processos que estabelecem e mantêm as políticas de controle de acesso que são incorporadas nas lógicas e regras de negócio. Normalmente, são políticas baseadas nos atributos e papéis associados a uma identidade.

3.7.2 O responsável (a ser definido pela matriz RACI da OM) deve gerenciar o que é permitido ou proibido ser acessado em uma determinada transação.

3.7.3 Para a realização do redesenho de perfis com ou sem análise de segregação de funções deve ser realizada uma avaliação da necessidade.

4 CONTROLES CRIPTOGRÁFICOS

4.1 VISÃO GERAL DO PROCESSO

4.1.1 Esta etapa de controles criptográficos é composta por um conjunto de regras que assegura a padronização das técnicas criptográficas, sua aplicação adequada e responsabilidades, de modo a garantir a segurança no transporte ou armazenamento das informações sem afetar o negócio da organização. Neste contexto, cada OM deverá fazer uma avaliação de risco para determinar o nível de proteção necessária às informações. Essa avaliação será usada para determinar se um controle criptográfico é apropriado, que tipo de controle deverá ser aplicado e para quais propósitos.

4.2 POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

4.2.1 Cada OM, em particular, deverá desenvolver uma política interna, por meio de uma NPA sobre o uso de controles criptográficos para proteção de suas informações. Tal política deverá maximizar os benefícios e minimizar os riscos de uso de técnicas criptográficas, evitando o uso inapropriado.

4.2.2 A política deve ter uma abordagem gerencial referente ao uso de controles criptográficos em cada OM, incluindo quais informações da OM devem ser protegidas.

4.2.3 A OM deverá ter uma política com uma abordagem para o gerenciamento de chaves, métodos para recuperação de informações criptografadas em caso de chaves perdidas, danificadas ou comprometidas.

4.3 CRIPTOGRAFIA

4.3.1 Criptografia é a técnica que pode ser usada para proteger a confidencialidade das informações.

4.3.2 As OM devem considerá-la para proteção de informações sensíveis ou críticas.

4.3.3 Considerando a avaliação de riscos (preencher Anexo A – Registro GRSTI01 – Definição do Contexto da Gestão de Riscos da ICA 7-26/2013), o nível de proteção deve ser identificado e definido, levando-se em conta o tipo e a qualidade do algoritmo de criptografia usado e o tamanho da chave criptografada a ser usada.

4.3.4 O uso de criptografia também deve ser considerado para proteger informações sensíveis, transportadas dentro de dispositivos removíveis, mídias removíveis ou dispositivos móveis e linhas de comunicação.

4.3.5 Ao implementar essa política de criptografia nas OM, devem ser considerados os regulamentos e as restrições nacionais.

4.4 ASSINATURA DIGITAL

4.4.1 As assinaturas digitais fornecem um meio de proteger a autenticidade e a integridade de documentos eletrônicos. Podem ser aplicadas em qualquer forma de documentos processados eletronicamente.

4.4.2 Ao implementar uma assinatura digital, as OM devem tomar cuidado para proteger a confidencialidade da chave privada.

4.4.3 A chave deve ser mantida em segredo, já que qualquer um que tenha acesso a essa chave pode assinar documentos, pagamentos e contratos, falsificando, dessa forma, a assinatura do proprietário da chave. Além disso, proteger a integridade da chave pública é importante. Essa proteção é fornecida mediante o uso de um certificado de chave pública.

4.5 GERENCIAMENTO DE CHAVES

4.5.1 O gerenciamento das chaves criptográficas é essencial para o uso eficaz das técnicas de criptografia. As OM devem ter uma atenção especial para evitar o comprometimento ou perda das chaves criptográficas que podem impactar a confidencialidade, autenticidade e/ou integridade das informações.

4.6 PADRÕES, MÉTODOS E PROCEDIMENTOS

4.6.1 As OM devem possuir um sistema de gerenciamento de chaves baseado em um conjunto acordado de padrões, procedimentos e métodos seguros.

4.6.2 Para reduzir a probabilidade de comprometimento, as chaves devem ter datas definidas de ativação e desativação, de modo que possam ser usadas apenas por um período limitado de tempo. Esse período de tempo deve ser dependente das circunstâncias em que o controle criptográfico está sendo usado e do risco percebido.

4.6.3 Além da questão de chaves secretas e privadas gerenciadas de forma segura, a proteção das chaves públicas também deve ser considerada. Existe a ameaça de que seja forjada uma assinatura digital substituindo uma chave pública do usuário por uma chave falsa. Esse problema é solucionado com o uso de um certificado de chave pública.

4.6.4 Estes certificados devem ser produzidos de maneira que associem informações relativas ao proprietário do par de chaves pública/privada com a chave pública. Portanto, é importante que se possa confiar no processo de gerenciamento que gera esses certificados. Esse processo é normalmente conduzido por uma autoridade de certificação, que deve ser uma organização reconhecida com controles adequados e procedimentos implantados para propiciar o grau exigido de confiança.

4.6.5 Os conteúdos de acordos ou contratos de níveis de serviço com fornecedores externos de serviços criptográficos, como uma autoridade de certificação, devem cobrir as questões de responsabilidades, confiabilidade dos serviços e tempos de resposta para o provimento dos serviços.

4.6.6 Um sistema de gerenciamento deve ser implantado para dar suporte as OM no uso dos dois tipos de técnicas criptográficas, que são:

a) a geração das chaves deverá garantir as propriedades adequadas para a aplicação e uma aleatoriedade que torne baixíssima a probabilidade da chave ser previsível. A entidade dona da chave deve gerar suas próprias chaves ou usar as chaves obtidas por meio de um componente confiável do sistema; e

b) técnicas de chave pública, nas quais cada usuário tem um par de chaves, uma chave pública (que pode ser revelada a qualquer um) e uma chave privada (que tem que ser mantida em segredo). As técnicas de chave pública podem

ser usadas para criptografia e para produzir assinaturas digitais.

4.6.7 Todas as chaves devem ser protegidas contra modificação e destruição, e chaves secretas e privadas precisam de proteção contra divulgação não autorizada. Técnicas criptográficas também podem ser usadas para esse propósito. Proteção física deve ser utilizada para proteger o equipamento usado para gerar, armazenar e arquivar as chaves.

4.6.8 As OM devem possuir procedimento para garantir a proteção das Chaves Criptográficas em todas as etapas do processo:

a) a geração de chaves que combinam a utilização dos métodos de criptografia de chave única e de chaves pública e privada garantem as conexões seguras. Os métodos de criptografia atualmente utilizados, e que apresentam bons níveis de segurança, são publicamente conhecidos e são seguros pela robustez de seus algoritmos e pelo tamanho das chaves que utilizam;

b) uma vez que a cópia de segurança ou o arquivamento tenham sido executados, deve haver um mecanismo que permita a recuperação do material criptográfico armazenado na cópia de segurança. Uma operação de restauração que reinstale uma chave que esteja em uso operacional só deve ser realizada se a chave foi perdida sem que a sua autenticidade tenha sido comprometida. Exemplos de perda da chave sem o seu comprometimento são a falha do *hardware* de armazenamento ou o simples esquecimento da mesma;

c) se a referência do armazenamento de chaves for especificada para uma configuração de dispositivo de *hardware*, o tempo de execução de segurança de serviços tentará primeiro obter o algoritmo criptográfico a partir do dispositivo de *hardware*. Se a aceleração de *hardware* for ativada, o tempo de execução de segurança dos serviços primeiro tentará utilizar o dispositivo de *hardware* para operações criptográficas;

d) se houver dados criptografados no computador, será necessário um meio para recuperar esses dados caso ocorra algo com a chave de criptografia. Se for perdida ou danificada a chave de criptografia e não houver como recuperar os dados, eles serão perdidos. Além disso, os dados serão perdidos ao armazenar a chave de criptografia em um cartão inteligente e este for danificado ou perdido. Para garantir que os dados criptográficos estarão sempre acessíveis, um *backup* da chave e do certificado de criptografia deverá ser feito;

e) a restauração da chave substitui a chave existente que está armazenada no banco de dados do servidor de relatório. A restauração de uma chave de criptografia substitui uma chave inutilizável por uma cópia que foi salva em disco anteriormente, e deverá excluir a chave existente e o conteúdo criptografado;

f) um protocolo de distribuição de chaves é capaz de fornecer, de forma segura, chaves criptografadas de sessão para o serviço de confiabilidade de dados de prover serviço de autenticação de origem e destino;

g) nesta fase, o material criptográfico é disponibilizado para uso conforme necessário, ficando disponível durante todo o criptoperíodo da chave ou até que ocorra algum evento específico, como comprometimento, perda ou

simplesmente a finalização de seu uso. O material criptográfico deve ser protegido, devendo ser armazenado num dispositivo adequado (módulo ou mídia), que esteja disponível para leitura quando necessário; e

h) passadas essas fases, a chave deve ser definitivamente cancelada e destruída. Isso significa que todas as cópias da chave devem ser removidas de forma segura de todos os dispositivos de armazenamento. Uma remoção segura nesse caso refere-se à remoção de todo e qualquer traço da existência da chave.

4.7 DEFINIR RESPONSÁVEIS PELA IMPLEMENTAÇÃO

4.7.1 Neste item, são definidos os papéis e as incumbências dos responsáveis por cada processo:

a) as OM devem ter um responsável pela implementação da política, para acompanhar o processo de implementação que deverá avaliar a adequação das diretrizes da política;

b) deve haver um responsável pelo gerenciamento de chaves criptografadas, incluindo a geração de chaves, renovação e destruição das chaves;

c) deve haver um responsável pelas normas a serem adotadas para a implementação eficaz em toda a organização (qual solução é usada para cada processo de negócio);

d) deve haver um responsável pelas regras para o uso de informações criptografadas em controles que dependem de inspeção de conteúdo (como detecção de vírus);

e) quando a política de organização de criptografia é implementada, deve levar em conta os regulamentos e restrições, que podem se aplicar ao uso de técnicas criptográficas em diferentes partes do mundo e as questões de excesso de informação fora das fronteiras nacionais;

f) a rede privada virtual (VPN) permite a troca de informações na Internet como se houvesse uma conexão direta a rede privada, beneficiando-se da funcionalidade, segurança e gerenciamento de políticas da rede privada;

g) a VPN deve utilizar métodos de autenticação, algoritmos de codificação e outras proteções para assegurar que os dados enviados entre os dois terminais de uma ligação permaneçam seguros; e

h) as OM devem compreender o impacto que uma VPN terá em toda a rede. Um planejamento e uma implementação adequados são fundamentais.

5 MODELO DE MATURIDADE DO PROCESSO

5.1 As OM são cada vez mais solicitadas a considerar quão bem a área de TI está sendo gerenciada. Cada OM realiza um gerenciamento independente, o que o aperfeiçoa e melhora o controle sobre a infraestrutura de informação.

5.2 É importante utilizar uma ferramenta de autoavaliação que possa ser utilizada para comparação entre as OM e também entre empresas do mercado. O gerenciamento de TI busca a avaliação para entender o que pode ser feito diferente.

5.3 O Modelo de Maturidade utilizado será o Modelo de Maturidade Genérico do CobiT, por ser um *Framework* cujo uso é incentivado pelo Governo Federal e por ser baseado num método de avaliar a organização, o gerenciamento e o controle dos processos de TI.

5.3.1 MODELO DE MATURIDADE GENÉRICO DO COBIT

5.3.1.1 A maturidade deste processo é medida por meio da seguinte escala:

0 – Inexistente: Completa falta de um processo reconhecido. A Organização não reconhece que existe uma questão a ser trabalhada.

1 – Inicial: Há evidências de que a OM reconheceu que a existência de questões que precisam ser trabalhadas. No entanto, não existe processo padronizado; ao contrário, existem iniciativas que tendem a ser aplicadas individualmente ou caso a caso. O enfoque geral de gerenciamento é desorganizado.

2 – Repetível e Intuitivo: O processo evoluiu para um estágio no qual procedimentos similares são seguidos por diferentes pessoas fazendo a mesma tarefa. Não existe treinamento formal ou uma comunicação dos procedimentos padronizados e a responsabilidade é deixada com o indivíduo. Há um alto grau de confiança no conhecimento dos indivíduos e consequentemente erros podem ocorrer.

3 – Processo Definido: Procedimentos foram padronizados, documentados e comunicados por meio de treinamento. É mandatório que esses processos sejam seguidos; no entanto, possivelmente desvios não serão detectados. Os procedimentos não são sofisticados, mas existe a formalização das práticas existentes.

4 – Gerenciado e Mensurável: A gerência monitora e mede a aderência aos procedimentos e adota ações onde os processos parecem não estar funcionando muito bem. Os processos estão sob constante aprimoramento e fornecem boas práticas. Automação e ferramentas são utilizadas de uma maneira limitada ou fragmentada.

5 – Otimizado: O processo foi refinado a um nível de boas práticas, baseado no resultado de um contínuo aprimoramento e modelagem da maturidade como outras organizações. A TI é utilizada como um caminho integrado para automatizar o fluxo de trabalho, provendo ferramentas para aprimorar a qualidade e efetividade, tornando a organização rapidamente adaptável.

5.4 A Tabela abaixo apresenta as metas para a evolução dos níveis de maturidade, servindo para os processos de Gestão de Acessos Lógicos e Físicos, Gestão de Identidade e Gestão de Controles Criptográficos:

Nível de Maturidade	**Metas**	**Prazo**
0 – Inexistente	O Processo não ocorre. A Organização não considera os impactos no negócio associados ao processo.	Atual
1 – Inicial	Existe a compreensão de que é importante a implementação do processo. Início de estudo para implementação do processo.	Atual
2 – Repetível e Intuitivo	Possuir uma normativa interna do DECEA para o processo. Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA.	2015
3 – Processo Definido	Implantar o processo em todas as Organizações Subordinadas ao DECEA. Capacitar todos os chefes das seções de Segurança da Informação.	2015
4 – Gerenciado e Mensurável	Criar um painel para acompanhamento, por meio de indicadores gerenciais do processo, a fim de garantir a tomada de decisão pela Direção do DECEA.	2016
5 – Otimizado	Realizar uma reunião semestral de análise crítica para melhoria contínua do processo. Possuir sistema informatizado para emissão de relatórios automatizados.	2016

6 RESPONSABILIDADES

6.1 SUBDEPARTAMENTO TÉCNICO DO DECEA - SDTE

6.1.1 Manter atualizada a presente Instrução.

6.1.2 Verificar o cumprimento das orientações contidas nesta norma por intermédio de Auditorias Técnicas.

6.1.3 Realizar varreduras físicas e eletrônicas nas instalações (áreas físicas, telefones e computadores) do DECEA e OM Subordinadas, segundo legislação em vigor.

6.2 COMANDANTES, CHEFES E DIRETORES

6.2.1 Zelar pelo fiel cumprimento das orientações contidas nesta norma no âmbito das suas Organizações.

6.3 SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO - SSSI

6.3.1 Auditar, localmente, esta norma.

6.3.2 Realizar, permanentemente, inspeções nos diversos sistemas de comunicações.

6.3.3 Propor manutenções e eventuais substituições dos sistemas de comunicações com proteção criptográfica, bem como o treinamento necessário aos operadores e/ou mantenedores.

6.3.4 Gerar indicadores próprios e os provenientes de orientações do SDTE.

6.3.5 Identificar os desvios praticados quanto aos procedimentos e ao uso dos meios de comunicações e criptografias, bem como implementar as correções apropriadas, comunicando o fato ao DECEA.

6.3.6 Promover palestras, reuniões e aulas com a finalidade de instruir o pessoal da sua OM sobre legislações, diretrizes, orientações e procedimentos ligados à utilização de recursos criptográficos e à segurança das comunicações.

6.4 SEÇÃO DE TECNOLOGIA DA INFORMAÇÃO - STI

6.4.1 Aprovar, junto às chefias envolvidas, e executar as solicitações de concessão e cancelamento do acesso à rede interna e externa, bem como acesso a e-mail, à Internet, aos diretórios da rede, aos sistemas internos e a outros serviços inerentes a esta norma

6.4.2 Manter o controle de acesso, revisando aqueles que já foram concedidos.

6.4.3 Gerar NPA que regule os procedimentos, técnicas e ferramentas que são utilizados na OM.

6.4.4 Revisar, periodicamente, as regras de proteção estabelecidas.

6.4.5 Impedir o acesso de militares desligados ou em processo de desligamento aos meios criptográficos.

6.4.6 Verificar e supervisionar, permanentemente, o fiel cumprimento das normas estabelecidas.

6.4.7 Detectar, identificar, registrar e comunicar ao comandante da OM e ao DECEA as violações, escutas ou tentativas de acesso não autorizadas.

6.4.8 Fornecer senhas de contas privilegiadas somente aos usuários que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle.

6.5 GESTOR DO USUÁRIO

6.5.1 Solicitar o acesso, bem como o seu cancelamento, à rede, à Internet, aos diretórios na rede, aos sistemas internos e a outros serviços inerentes a esta norma para todos os usuários sob sua responsabilidade.

6.6 DO EFETIVO

6.6.1 Todos do efetivo, que acessem meios de comunicações seguras da Organização, são responsáveis pela integridade dos mesmos, bem como pelo cumprimento das normas de segurança descritas na legislação em vigor. No caso de inobservância ou recusa em fazê-lo, devem ser imputadas as sanções disciplinares, legais e administrativas cabíveis.

6.6.2 Manter o caráter sigiloso da senha de acesso aos meios de comunicações, quando implementados.

6.6.3 Não permitir que assuntos ou documentos sigilosos sejam vinculados sem a devida proteção de criptografia, ou estejam disponíveis para quem não tenha a devida autorização de acesso.

6.6.4 Não permitir o acesso indevido aos meios de comunicações seguras da organização, utilizando ou permitindo a outrem a utilização do seu código de identificação ou, ainda, outro atributo para esse fim instituído.

7 DISPOSIÇÕES FINAIS

7.1 Os processos de Segurança da Informação apresentados neste documento são de caráter geral e devem ser revisados periodicamente a cada dois anos, ou quando fato relevante demandar atualização extemporânea.

7.2 Esta Instrução do Comando da Aeronáutica deverá estar em conformidade com as Diretrizes da DTI, Órgão Central do Sistema de Tecnologia da Informação do Comando 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.

7.3 Casos não previstos nesta Instrução deverão ser submetidos 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 prática para a gestão da segurança da informação*. Rio de Janeiro, RJ, 2005

BRASIL. Comando da Aeronáutica. Centro de Inteligência da Aeronáutica. *Medidas de Segurança para Equipamentos Criptotécnicos e de Comunicações*: **ICA 200-8**. Rio de Janeiro, RJ, 2009.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Padronização da Infraestrutura de Tecnologia da Informação no DECEA e OM Subordinadas*: **PCA 7-16**. Rio de Janeiro, RJ, 2011.

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

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

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Processo de Controle de Acesso à Rede Interna e Externa do Departamento de Controle do Espaço Aéreo*: **ICA 7-30**. Rio de Janeiro, RJ, 2013.

BRASIL. Comando da Aeronáutica. Departamento de Controle do Espaço Aéreo. *Processo de Gestão de Logs do Departamento de Controle do Espaço Aéreo*: **ICA 7-28**. Rio de Janeiro, RJ, 2013.

COBIT (2007). *Control Objectives for Information and related Technology* (CobiT), Version 4.1. ISACA – Information Systems Audit and Control Association, 2007.

Anexo A – FSA – Formulário de Solicitação de Acesso

COMANDO DA AERONÁUTICA

DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO

<inserir nome da organização por extenso>

	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	FSA			

ASSUNTO	☐Acesso à Rede Interna ☐Acesso Remoto ☐Acesso à Internet e Intraer ☐Solicitação de E-mail ☐Solicitação de Crachá ☐Acesso a Sistemas Internos ☐Acesso à Organização fora do Expediente ☐Acesso a Ativos de Transporte ☐Acesso e Criação de Diretório de Rede ☐Outro (_____)

Do Usuário	
Posto/Grad – Nome Completo	
Login	
Documento de Identidade	
CPF	
Telefone	
E-mail	
Setor / OM	
Da Chefia Responsável	
Posto / Nome Completo	
Setor / OM	
Motivação da Solicitação	
Do Solicitado	
Chefia (Posto/Nome Completo)	
Análise	□ **Deferido** ou □ **Indeferido**
Motivação da Análise	

_____ _____

(Solicitante) (Solicitado)