

**MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA**



TECNOLOGIA DA INFORMAÇÃO

ICA 7-30

**PROCESSO DE CONTROLE DE ACESSO À REDE
INTERNA E EXTERNA DO DEPARTAMENTO DE
CONTROLE DO ESPAÇO AÉREO**

2013

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



TECNOLOGIA DA INFORMAÇÃO

ICA 7-30

**PROCESSO DE CONTROLE DE ACESSO À REDE
INTERNA E EXTERNA DO DEPARTAMENTO DE
CONTROLE DO ESPAÇO AÉREO**

2013



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

PORTARIA DECEA Nº 93/DGCEA, DE 2 DE AGOSTO DE 2013.

Aprova a edição da Instrução relativa ao Processo de Controle de Acesso à Rede Interna e Externa do Departamento de Controle do Espaço Aéreo.

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

Art. 1º Aprovar a edição da ICA 7-30 “Processo de Controle de Acesso à Rede Interna e Externa do Departamento de Controle do Espaço Aéreo”, que com esta baixa.

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

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

(Publicado no BCA nº 163, de 26 de agosto de 2013.)

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
2 RESPONSABILIDADES	8
2.1 <u>SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA</u>	8
2.2 <u>COMANDANTES, CHEFES E DIRETORES</u>	8
2.3 <u>SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO</u>	8
2.4 <u>ELOS DE SERVIÇOS DE TI</u>	8
2.5 <u>GESTOR DO USUÁRIO</u>	8
3 PROCESSO DE CONTROLE DE ACESSO À REDE INTERNA E EXTERNA	9
3.1 <u>GESTÃO DE CONTROLE DE ACESSO</u>	9
3.2 <u>CONTROLE E MATURIDADE DO PROCESSO</u>	9
3.3 <u>FATORES CRÍTICOS DE SUCESSO</u>	11
4 DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO ...	12
4.1 <u>VISÃO GERAL DO PROCESSO</u>	12
4.2 <u>SUBPROCESSO “AUTORIZAR PERFIL DE ACESSO À REDE”</u>	12
4.3 <u>SUBPROCESSO “RETIRAR PERFIL DE ACESSO À REDE”</u>	13
4.4 <u>SUBPROCESSO “MANUTENÇÃO DE PERFIL DE ACESSO À REDE”</u>	15
4.5 <u>SUBPROCESSO “AUDITORIA DE PERFIL DE ACESSO”</u>	16
4.6 <u>SUBPROCESSO “MELHORIA CONTÍNUA”</u>	17
5 DISPOSIÇÕES FINAIS	19
Anexo A – Registro PCAR01 – Solicitação de Acesso à Rede	21
Anexo B – Registro PCAR02 – Solicitação de Retirada de Acesso	22
Anexo C – Registro PCAR03 – Solicitação de Alteração de Perfil de Acesso à Rede	23
Anexo D – Registro PCAR04 – Logins e Perfis de Acesso à Rede	24
Anexo E – Registro PCAR05 – Ações para Tratamento de NÃO-CONFORMIDADES	25
Anexo F – Registro PCAR06 – Identificação, Quantificação e Análise dos Indicadores do Processo	26

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Instrução tem por finalidade apresentar o Processo de Controle de Acesso à Rede Interna e Externa, bem como 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
OM	–	Organização Militar
PCAR	–	Processo de Controle de Acesso à Rede
SDTE	–	Subdepartamento Técnico
SSSI	–	Seção de Segurança de Sistemas da Informação
TI	–	Tecnologia da Informação

2 RESPONSABILIDADES

2.1 SDTE – SUBDEPARTAMENTO TÉCNICO DO DECEA

2.1.1 Manter atualizada a presente Instrução.

2.1.2 Verificar o cumprimento das orientações contidas na presente Norma por intermédio de Auditorias Técnicas.

2.2 COMANDANTES, CHEFES E DIRETORES

2.2.1 Zelar pelo fiel cumprimento das orientações contidas na presente Norma no âmbito das suas Organizações.

2.3 SSSI – SEÇÃO DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

2.3.1 Auditar, localmente, o processo de controle de acesso à rede interna e externa.

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

2.4 ELOS DE SERVIÇOS DE TI

2.4.1 Executar a atividade de conceder e cancelar o acesso à rede interna e externa.

2.4.2 Aprovar as solicitações de concessão e retirada de acesso à rede dos usuários.

2.4.3 Executar manutenção na rede de controle de acesso.

2.5 GESTOR DO USUÁRIO

2.5.1 Solicitar acesso à rede ao usuário sob a sua responsabilidade

2.5.2 Solicitar a retirada de acesso do usuário sob a sua responsabilidade

3 PROCESSO DE CONTROLE DE ACESSO À REDE INTERNA E EXTERNA

3.1 GESTÃO DE CONTROLE DE ACESSO

3.1.1 De acordo com o item 4.1.4, letra “j”, nº 30, do Plano Diretor de Segurança da Informação do Departamento de Controle do Espaço Aéreo, está prevista a realização do gerenciamento de segurança das redes digitais de telecomunicações de interesse do DECEA, visando contribuir para a proteção das informações em trânsito e dos ativos que compõem a sua infraestrutura. Assim, o DECEA deve estabelecer normas para o uso de todo e qualquer tipo de serviço e de tecnologias de rede, tanto no contexto de redes locais, como de redes de longa distância, capazes de estabelecer processos para monitoração e registro dos eventos relativos ao funcionamento dos demais serviços, sendo necessário o estabelecimento da gestão do Processo de Controle de Acesso à Rede Interna e Externa nas Organizações Subordinadas.

3.2 CONTROLE E MATURIDADE DO PROCESSO

3.2.1 Os mecanismos de controle do processo são: Medição do Nível de Maturidade e Acompanhamento por Indicadores.

3.2.2 MEDIÇÃO DO NÍVEL DE MATURIDADE ATUAL DO PROCESSO

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

0 – Não Existente: O Processo de Controle de Acesso a Rede Interna e Externa não ocorre. A Organização não considera os impactos no negócio associados ao processo. O Processo de Controle de Acesso à Rede Interna e Externa não tem sido identificado como relevante para a aquisição de soluções de TI e para entregar os serviços de TI.

1 – Inicial/*Ad Hoc*: O Processo de Controle de Acesso à Rede Interna e Externa é levado em consideração de maneira *Ad Hoc*. Existe uma compreensão 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 Controle de Acesso à Rede Interna e Externa existe, mesmo de modo imaturo, e está implementado. O gerenciamento do processo é normalmente de alto nível e tipicamente aplicado apenas aos projetos de redes importantes ou em resposta a problemas.

3 – Processo Definido: O Controle de Acesso à Rede Interna e Externa segue um processo definido e documentado. O treinamento no processo está disponível para todo o efetivo. As decisões para acompanhar o processo e para receber treinamento são deixadas a critério individual. A metodologia para o Controle de Acesso à Rede Interna e Externa é convincente e bem estruturada e garante que os principais riscos para o negócio sejam identificados.

4 – Gerenciado e Mensurável: A avaliação e o gerenciamento do Processo de Controle de Acesso à Rede Interna e Externa de vulnerabilidades são procedimentos padrões. O processo é avaliado em nível de projeto individual e também regularmente a respeito da operação de TI e Telecomunicações como um todo. Existe a capacidade de monitorar a posição dos riscos associados ao Controle de Acesso à Rede Interna e Externa e tomar decisões informadas referentes à exposição que deseja assumir.

5 – Otimizado: O Controle de Acesso à Rede Interna e Externa já se desenvolveu a um estágio em que um processo estruturado é executado e bem gerenciado. Boas práticas são aplicadas organizacionalmente. A captura, a análise e o relatório de dados de gerenciamento sobre o processo são altamente automatizados.

3.2.3 A tabela 1 apresenta as metas para a evolução dos níveis de maturidade:

Tabela 1 - Metas para a Evolução dos Níveis de Maturidade

Nível de Maturidade	Metas	Prazo
2 – Repetível e Intuitivo	<ul style="list-style-type: none"> • Possuir uma normativa interna do DECEA para o Processo de Controle de Acesso à Rede Interna e Externa. • Iniciar a implantação e testes do processo em pelo menos 50% das Organizações Subordinadas ao DECEA. 	Até junho de 2014
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. 	Até dezembro de 2014
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. 	Até junho de 2015
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. 	Até dezembro de 2015

3.2.4 ACOMPANHAMENTO DO PROCESSO POR INDICADORES

O acompanhamento do processo será feito por intermédio dos indicadores e métricas listadas na tabela 2 abaixo, contudo as metas serão definidas posteriormente pelo SDTE.

Tabela 2 – Acompanhamento do Processo

Objetivos do Processo	Indicadores do Processo
<ul style="list-style-type: none"> • Determinar e reduzir a ocorrência e o impacto de incidentes de segurança da informação na rede; e • Estabelecer planos de controles de segurança da informação para mitigar os riscos identificados no processo. 	<ul style="list-style-type: none"> • Quantidade de solicitações de concessão de perfil de acesso à rede; • Quantidade de solicitações de retirada de perfil de acesso à rede; e • Quantidade de não-conformidades identificadas no processo.

3.3 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 DESCRIÇÃO DOS PROCEDIMENTOS DE SEGURANÇA DA INFORMAÇÃO

4.1 VISÃO GERAL DO PROCESSO

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

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

4.1.3 No caso do processo de controle de acesso em tela, ele é composto por 5 (cinco) subprocessos a seguir descritos: Autorizar Perfil de Acesso à Rede, Retirar Perfil de Acesso à Rede, Manutenção do Perfil de Acesso, Auditoria do Perfil de Acesso e Melhoria Contínua, conforme ilustrado na figura 1.



Figura 1 - Visão Geral do Processo de Controle de Acesso à Rede

4.2 SUBPROCESSO “AUTORIZAR PERFIL DE ACESSO À REDE”

4.2.1 Este subprocesso é composto por 5 (cinco) etapas, a saber: envio de solicitação de acesso, análise da solicitação, aprovação da solicitação, realização de manutenção e comunicação de manutenção, conforme ilustrado na figura 2.

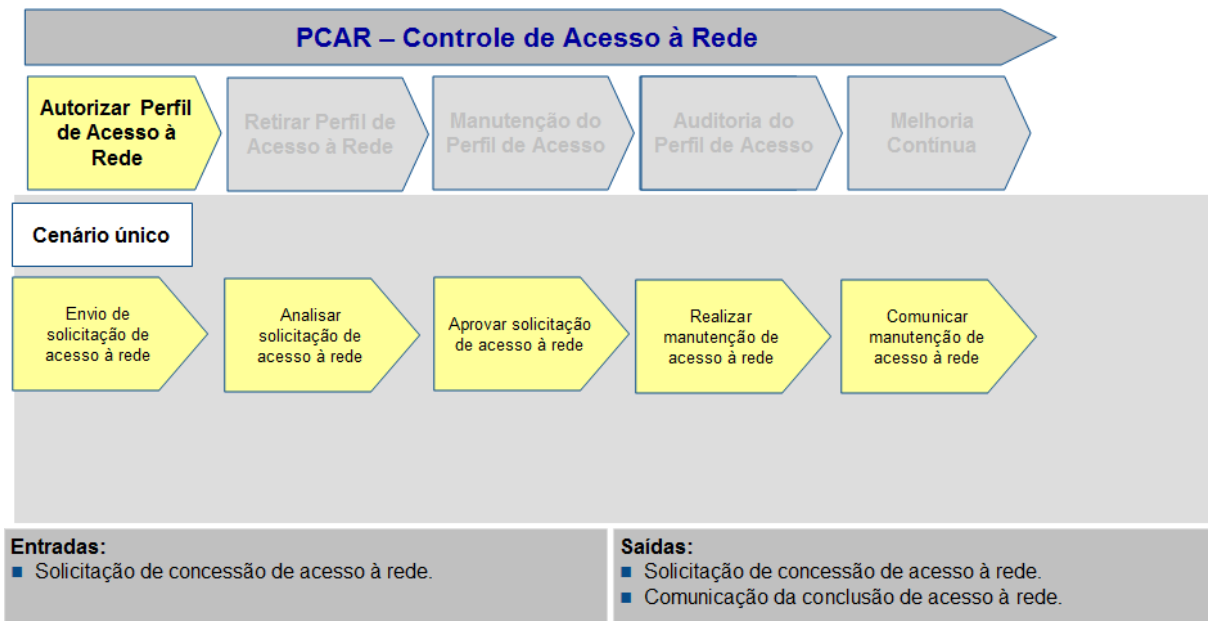


Figura 2 - Subprocesso para Autorizar Perfil de Acesso à Rede

4.2.2 Este subprocesso descreve as ações necessárias para conceder o perfil de acesso à Rede Interna e Externa.

4.2.3 Neste subprocesso, o acesso deverá ser solicitado, analisado, aprovado, mantido e comunicado às partes interessadas.

4.2.4 Em relação à etapa “Envio de solicitação de acesso à rede”, o responsável pela solicitação do acesso deverá fornecer as informações necessárias do acesso a ser concedido. Essas informações deverão ser transcritas no documento Solicitação de Acesso à Rede (PCAR01), conforme modelo contido no Anexo A.

4.2.5 No que tange à etapa “Analisar solicitação de acesso à rede”, após o recebimento da solicitação de acesso à rede, o responsável por conceder este acesso deverá analisar a solicitação de acordo com as políticas e regulamentos de segurança da informação em vigor na Organização Militar.

4.2.6 Na etapa “Aprovar Solicitação de acesso à rede”, o responsável pela autorização deverá aprovar a Solicitação de Acesso à Rede (PCAR01), conforme previsto no Anexo A.

4.2.7 No que concerne à etapa “Realizar a Manutenção de acesso à rede”, com o documento Solicitação de Acesso à Rede (PCAR01) aprovada pelo Gestor do usuário, o Elo de Serviço de TI deve conceder o acesso à rede interna e externa.

4.2.8 Já na etapa “Comunicar Manutenção de acesso à rede”, o Elo de Serviço de TI deve comunicar a concessão de acesso à rede ao gestor do usuário e este deverá comunicar ao usuário da sua área os acessos a ele permitidos.

4.3 SUBPROCESSO “RETIRAR PERFIL DE ACESSO À REDE”

4.3.1 Este subprocesso visa descrever as ações necessárias para retirar o perfil de acesso à Rede Interna e Externa. Também se subdivide em 5 (cinco) etapas, a saber: envio de solicitação de retirada de acesso, análise de solicitação, aprovação de solicitação de retirada,

realização de retirada de acesso e comunicação de retirada de acesso, conforme ilustrado na figura 3.

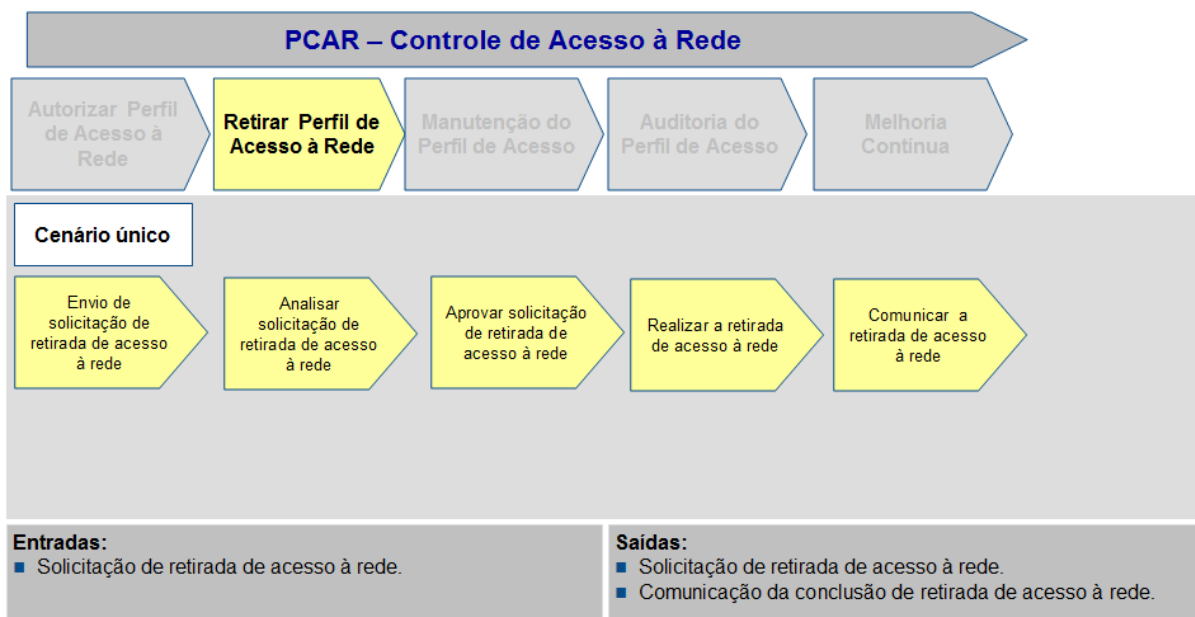


Figura 3 - Subprocesso para Retirar Perfil de Acesso à Rede

4.3.2 Este subprocesso descreve as ações necessárias para retirar o perfil de acesso à Rede Interna e Externa.

4.3.3 Neste subprocesso deverá ser solicitada e aprovada solicitação de remoção do perfil de acesso ao usuário após o encerramento de suas atividades, contratos ou acordos, ou ajustado após a mudança de suas atividades.

4.3.4 Na etapa “Envio de solicitação de retirada de acesso à rede”, o responsável pela solicitação da remoção do acesso deverá fornecer as informações necessárias do acesso a ser removido. Essas informações deverão ser transcritas no documento Solicitação de Retirada de Acesso à Rede (PCAR02), conforme modelo padronizado no Anexo B.

4.3.5 Quanto à etapa “Analisar solicitação de acesso à rede”, após o recebimento da solicitação de remoção de acesso à rede, o responsável por retirar este acesso deverá analisar a solicitação de acordo com as políticas e regulamentos de segurança da informação em vigor na Organização Militar.

4.3.6 No que tange à etapa “Aprovar Solicitação de retirada de acesso à rede”, o responsável pela aprovação da retirada de acesso à rede deve verificar se a documentação está preenchida corretamente no documento Solicitação de Retirada de Acesso à Rede (PCAR02) e aprovar esta solicitação de retirada de acesso à rede.

4.3.7 Em relação à etapa “Realizar a Retirada de acesso à rede”, com o documento Solicitação de Retirada de Acesso à Rede (PCAR02) aprovada pelo Gestor do usuário, o Elo de Serviço de TI deve retirar o acesso à rede interna e externa.

4.3.8 Por fim, na etapa “Comunicar a Retirada de acesso à rede”, o Elo de Serviço de TI deve comunicar a retirada de acesso à rede ao gestor do usuário.

4.4 SUBPROCESSO “MANUTENÇÃO DE PERFIL DE ACESSO À REDE”

4.4.1 Este subprocesso visa descrever as ações necessárias para alterar o perfil de acesso à Rede Interna e Externa. Também se subdivide em 5 (cinco) etapas, a saber: envio de solicitação de alteração de acesso, análise de solicitação, aprovação de solicitação de alteração de acesso, realização de alteração de acesso e comunicação de alteração de acesso, conforme ilustrado na figura 4.

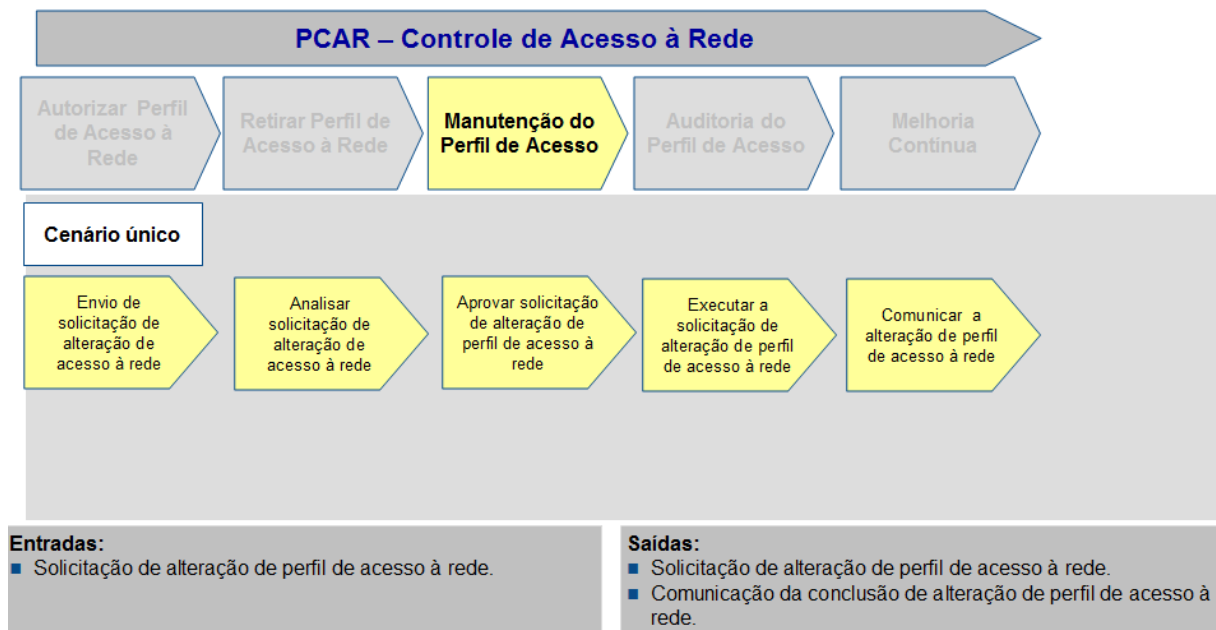


Figura 4 - Subprocesso para Manutenção do Perfil de Acesso à Rede

4.4.2 Este subprocesso descreve as ações necessárias para alterar o perfil de acesso à Rede Interna e Externa.

4.4.3 Neste subprocesso deverá ser requisitada e aprovada solicitação de alteração do perfil de acesso ao usuário antes da movimentação de pessoal no âmbito da OM e a reestruturação de Divisões e Seções.

4.4.4 Na etapa “Envio de solicitação de alteração de acesso à rede”, o responsável pela solicitação da alteração do acesso deverá fornecer as informações necessárias do acesso a ser alterado. Essas informações deverão ser transcritas no documento Solicitação de Alteração de Acesso à Rede (PCAR03), conforme modelo padronizado no Anexo C.

4.4.5 Quanto à etapa “Analisar solicitação de alteração de acesso à rede”, após o recebimento da solicitação de alteração de acesso à rede, o responsável por alterar este acesso deverá analisar a solicitação de acordo com as políticas e regulamentos de segurança da informação em vigor na Organização Militar.

4.4.6 No que tange à etapa “Aprovar Solicitação de alteração de acesso à rede”, o responsável pela aprovação da alteração de acesso a rede deve verificar se toda a documentação está preenchida corretamente no documento Solicitação de Alteração de Perfil de Acesso à Rede (PCAR03) e aprovar esta solicitação de alteração de acesso à rede.

4.4.7 Em relação à etapa “Executar a solicitação de alteração de perfil de acesso à rede”, com o documento Solicitação de Alteração de Perfil de Acesso à Rede (PCAR03) aprovado pelo Gestor do usuário, o Elo de Serviço de TI deve retirar o acesso à rede interna e externa.

4.4.8 Por fim, na etapa “Comunicar a Alteração de Perfil de acesso à rede”, o Elo de Serviço de TI deve comunicar a alteração de acesso à rede ao gestor do usuário.

4.5 SUBPROCESSO “AUDITORIA DE PERFIL DE ACESSO”

4.5.1 Visa descrever as ações necessárias para verificar a conformidade do processo com a documentação publicada pelo DECEA, sendo constituído de 3 (três) etapas, a saber: identificação dos usuários e perfis, validação dos perfis de acesso e elaboração de relatório, conforme fluxo detalhado na figura 5.

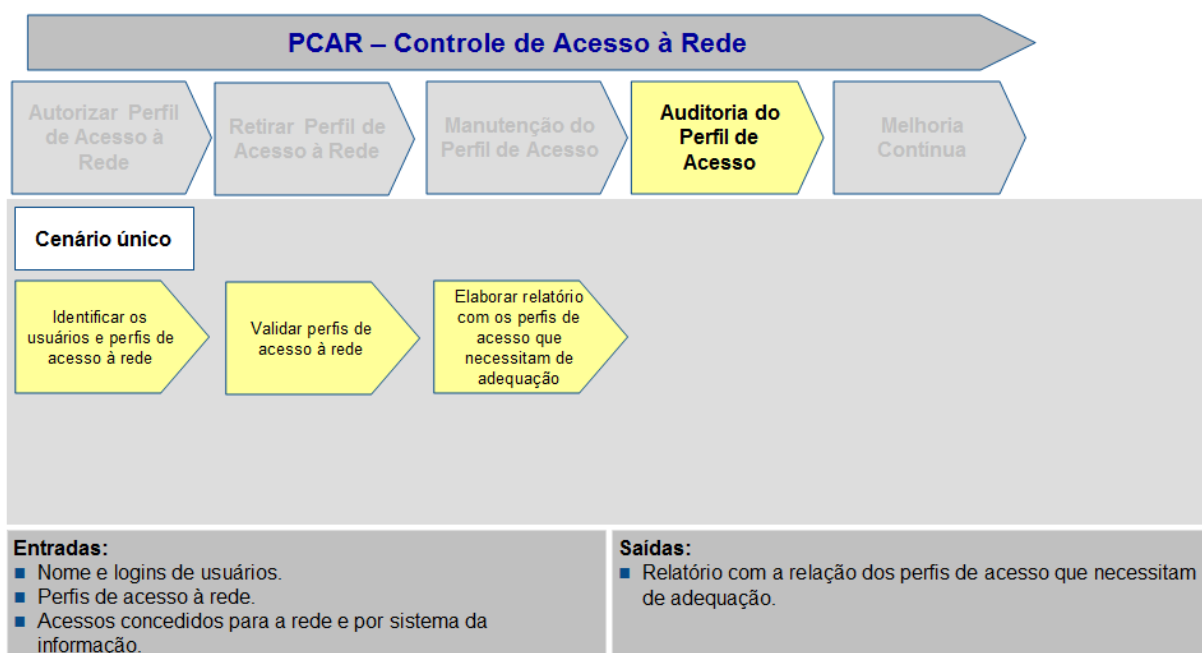


Figura 5 - Subprocesso para Auditoria de Perfil de Acesso

4.5.2 Na etapa “Identificar os usuários e perfis de acesso à rede”, a Seção de Segurança de Sistemas da Informação deve identificar as pessoas e os logins de acesso à rede que estão ativos na Organização Militar. Essas informações deverão ser transcritas no documento denominado de Logins e Perfis de Acesso à Rede (PCAR04), conforme modelo contido no Anexo D.

4.5.3 Já na etapa “Validar perfis de acesso à rede”, a Seção de Segurança de Sistemas da Informação deve verificar cuidadosamente a situação de cada usuário com o seu perfil atual de acesso à rede interna e externa.

4.5.3.1 A Seção de Segurança de Sistemas da Informação deve verificar se existem usuários ativos que já não fazem mais parte do efetivo da Organização Militar e analisar se os perfis de acesso condizem com a atual função do usuário.

4.5.3.2 Em relação à etapa “Elaborar Relatório com os perfis de acesso que necessitam de adequação”, a Seção de Segurança de Sistemas da Informação deve elaborar o relatório final da auditoria, que deve conter os seguintes campos:

- a) equipe de auditoria;
- b) lista de verificação;
- c) período da auditoria;
- d) não-conformidades; e
- e) recomendações com ações corretivas e preventivas.

4.6 SUBPROCESSO “MELHORIA CONTÍNUA”

4.6.1 Este subprocesso visa implantar as recomendações da auditoria e analisar a performance do processo de segurança procurando identificar oportunidades de melhorias no controle de acesso à Rede Interna e Externa. Ele é composto de 3 etapas e interage com o Processo de Gestão de Mudanças, conforme ilustrado na figura 6.

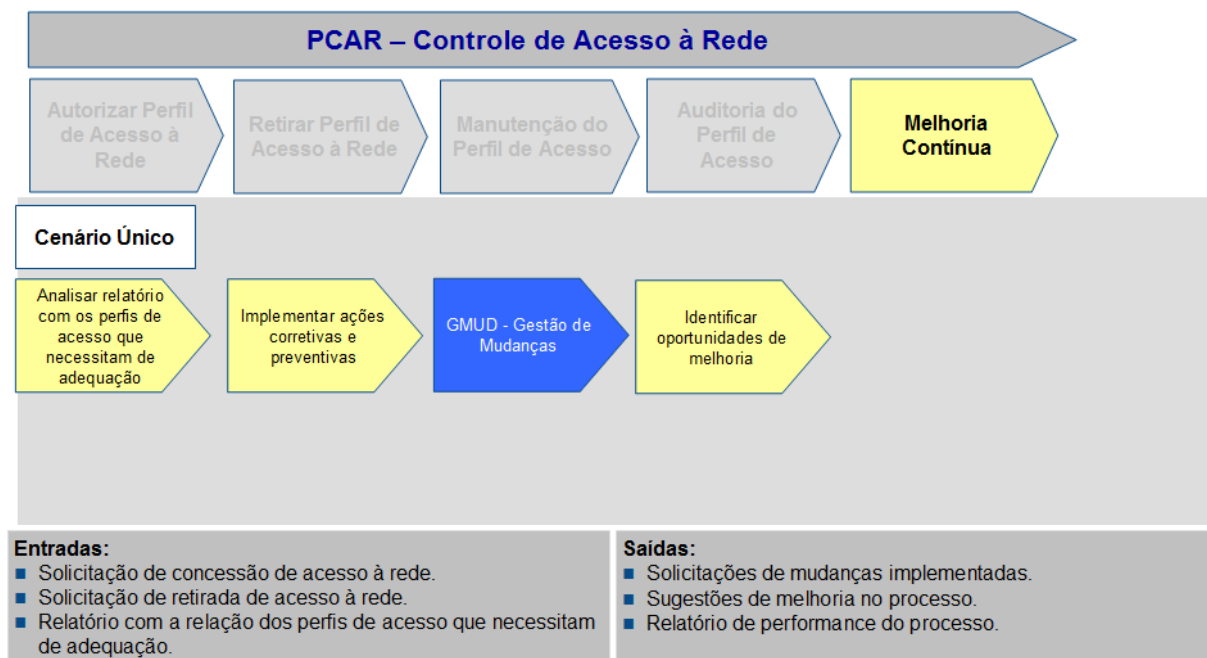


Figura 6 - Subprocesso para Melhoria Contínua

4.6.2 Na etapa “Analisar relatório com os perfis de acesso que necessitam de adequação” é processado o relatório da auditoria realizada no processo, verificando as não-conformidade que necessitam de ações corretivas e/ou preventivas.

4.6.3 Já na etapa “Implementar ações corretivas e preventivas”, para cada não-conformidade identificada a equipe técnica deveria apontar um ou mais controles de segurança que deverão ser implementados, o responsável pela implementação e a data desejada para implementação das ações de segurança. Essas informações deverão ser transcritas no documento Ações para Tratamento de Não-Conformidades (PCAR05), conforme modelo contido no Anexo E.

4.6.4 Após a elaboração do documento Ações para Tratamento de Não-Conformidades, (PCAR05) as ações deverão ser implementadas a partir do processo de Gestão de Mudanças.

4.6.5 Em relação à etapa “Identificar oportunidades de melhoria”, deve-se analisar as informações consolidadas do processo, através dos seus indicadores, e identificar oportunidades de melhoria. Essas informações deverão ser transcritas no documento

Identificação, Quantificação e Análise dos Indicadores do Processo (PCAR06), utilizando o modelo apresentado no Anexo F.

5 DISPOSIÇÕES FINAIS

5.1 O Processo e 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.

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

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

Anexo A - Registro PCAR01 – Solicitação de Acesso à Rede

COMANDO DA AERONÁUTICA				
<u>DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO</u>				
<inserir nome da organização por extenso>				
	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	PCAR01			
ASSUNTO	Solicitação de Acesso à Rede			
1 INFORMAÇÕES DO SOLICITANTE DO ACESSO				
Nome:				
Email:				
Telefone:				
Área:				
2 INFORMAÇÕES DO ACESSO A SER CONCEDIDO				
Nome:				
Email:				
Telefone:				
Login:				
Perfis de Acesso por Sistema:				
Solicitado por:			Data:	
Aprovado por:			Data:	
Responsável pela Execução:			Data:	


Anexo B – Registro PCAR02 – Solicitação de Retirada de Acesso

COMANDO DA AERONÁUTICA				
<u>DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO</u>				
<inserir nome da organização por extenso>				
	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	PCAR02			
ASSUNTO	Solicitação de Retirada de Acesso à Rede			
1 INFORMAÇÕES DO SOLICITANTE DA REMOÇÃO DO ACESSO				
Nome:				
Email:				
Telefone:				
Área:				
2 INFORMAÇÕES DO ACESSO A SER REMOVIDO				
Nome:				
Email:				
Telefone:				
Login:				
Perfis de Acesso por Sistema:				
Revisado Por:			Data:	
Aprovado Por:			Data:	
Responsável pela Execução:			Data:	

Anexo C – Registro PCAR03 – Solicitação de Alteração de Perfil de Acesso à Rede

COMANDO DA AERONÁUTICA				
<u>DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO</u>				
<inserir nome da organização por extenso>				
	CÓDIGO DO REGISTRO	DATA	CLASSIFICAÇÃO	LOCALIDADE
	PCAR03			
ASSUNTO	Solicitação de Retirada de Acesso à Rede			
1 INFORMAÇÕES DO SOLICITANTE DA ALTERAÇÃO DO ACESSO				
Nome:				
Email:				
Telefone:				
Área:				
2 INFORMAÇÕES DO ACESSO A SER ALTERADO				
Nome:				
Email:				
Telefone:				
Login:				
Perfis de Acesso por Sistema:				
Revisado Por:			Data:	
Aprovado Por:			Data:	
Responsável pela Execução:			Data:	

Anexo F – Registro PCAR06 – Identificação, Quantificação e Análise dos Indicadores do Processo

<p align="center">COMANDO DA AERONÁUTICA</p> <p align="center"><u>DEPARTAMENTO DE CONTROLE DO ESPAÇO AÉREO</u></p> <p align="center"><inserir nome da organização por extenso></p>				
	<p align="center">CÓDIGO DO REGISTRO</p>	<p align="center">DATA</p>	<p align="center">CLASSIFICAÇÃO</p>	<p align="center">LOCALIDADE</p>
	PCAR06			
<p>ASSUNTO</p>	<p>Identificação, Quantificação e Análise dos Indicadores do Processo</p>			
<p>1 MEDIÇÃO DOS INDICADORES</p>				
	Indicador	Quantitativo	Observações	
<p>2 ANÁLISE DOS INDICADORES</p>				
<p> </p>				
<p>3 AÇÕES DE MELHORIA CONTÍNUA</p>				
<p> </p>				
<p> </p>				