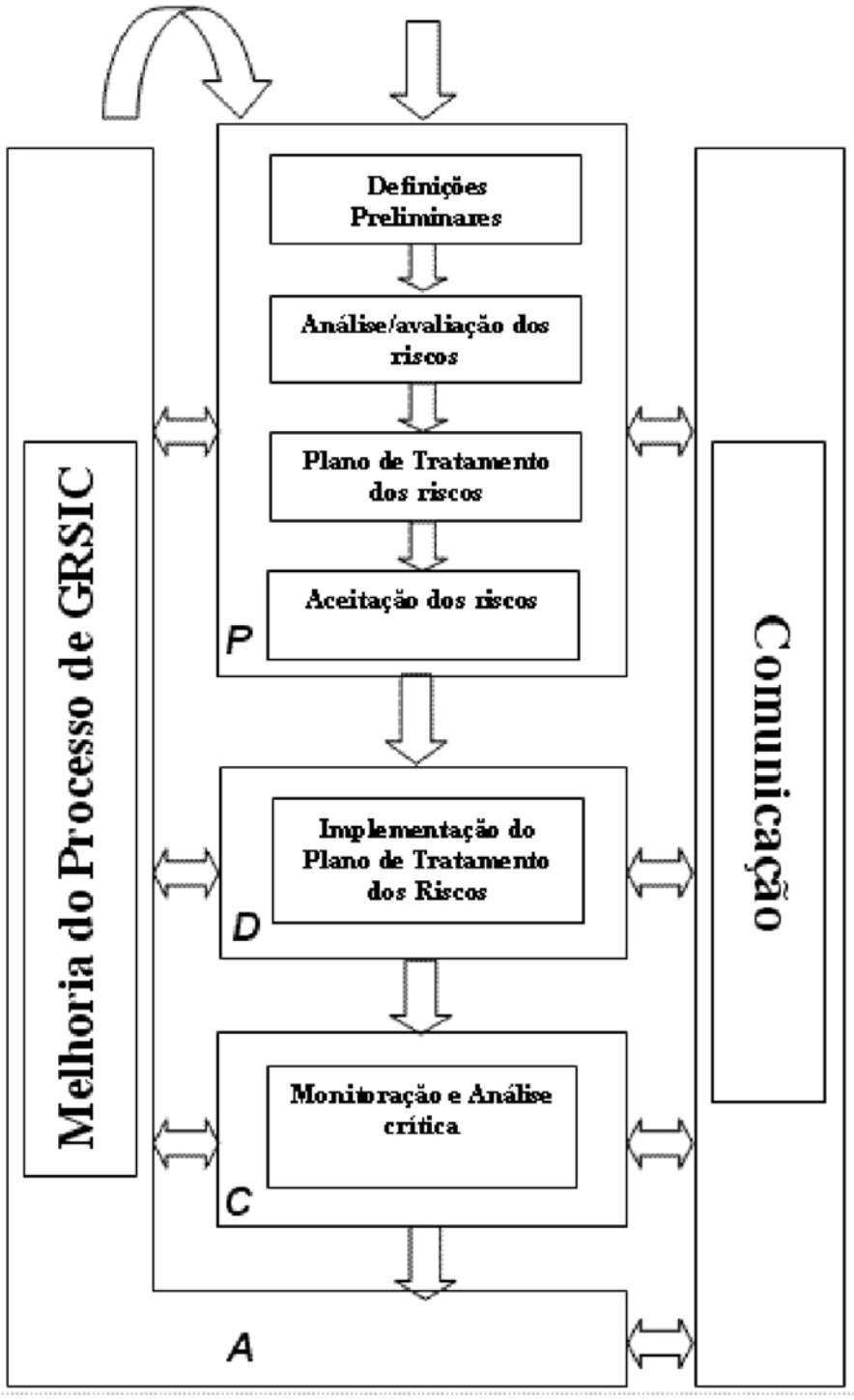
8 ANEXO

A - Processo de Gestão de Riscos de Segurança da Informação e Comunicações

ANEXO A

PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES



PORTARIA Nº 38, DE 14 DE AGOSTO DE 2009

Homologa a Norma Complementar nº 05/IN01/DSIC/GSIPR.

O MINISTRO DE ESTADO CHEFE DO GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA, na condição de **SECRETÁRIO-EXECUTIVO DO CONSELHO DE DEFESA NACIONAL**, no uso da atribuição que lhe confere o Art. 4º do Decreto nº 3.505, de 13 de junho de 2000, e o inciso IV do art. 1º do Anexo I do Decreto nº 5.772, de 08 de maio de 2006, resolve:

Art. 1º Fica homologada a Norma Complementar nº 05/IN01/DSIC/GSIPR que disciplina a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, aprovada pelo Diretor do Departamento de Segurança da Informação e Comunicações, em anexo.

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

JORGE ARMANDO FELIX

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações

CRIAÇÃO DE EQUIPES DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS - ETIR

ORIGEM
Departamento de Segurança da Informação e Comunicações

REFERÊNCIA NORMATIVA
Art. 6º da Lei nº 10.683, de 28 de maio de 2003.
Art. 8º do Anexo I do Decreto nº 5.772, de 8 de maio de 2006.
Decreto nº 3.505, de 13 de junho de 2000.
Instrução Normativa nº 01 do Gabinete de Segurança Institucional, de 13 de junho de 2008.
Incisos II e IV do art. 37 da Portaria nº 13 do Gabinete de Segurança Institucional, de 4 de agosto de 2006.

CAMPO DE APLICAÇÃO
Esta Norma Complementar se aplica no âmbito da Administração Pública Federal, direta e indireta.

SUMÁRIO

INFORMAÇÕES ADICIONAIS
Não há

APROVAÇÃO

RAPHAEL MANDARINO JUNIOR
Diretor do Departamento de Segurança da Informação e Comunicações

1 OBJETIVO

Disciplinar a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF.

2 CONSIDERAÇÕES INICIAIS

2.1 Nos últimos anos os órgãos públicos vêm implementando e consolidando redes locais de computadores cada vez mais amplas, como exigência para suportar o fluxo crescente de informações, bem como permitir que seus funcionários acessem à rede mundial de computadores para melhor desempenharem suas funções. Manter a segurança da informação e comunicações de uma organização em um ambiente computacional interconectado nos dias atuais é um grande desafio, que se torna mais difícil à medida que são lançados novos produtos para a Internet e novas ferramentas de ataque são desenvolvidas.

2.2 Diante da premissa de garantir e incrementar a segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta, há a necessidade de orientar a condução de políticas de segurança já existentes ou a serem implementadas.

2.3 Considerando a estratégia de segurança da informação composta por várias camadas, uma delas, que vem sendo adotada por diversas instituições, é a criação de Equipes de Tratamento e Resposta a Incidentes em Redes Computacionais, mundialmente conhecido como CSIRT® (do inglês "Computer Security Incident Response Team").

2.4 É competência da Coordenação-Geral de Tratamento de Incidentes de Redes do Departamento de Segurança da Informação e Comunicações - DSIC do Gabinete de Segurança Institucional - GSI apoiar os órgãos e entidades da Administração Pública Federal, direta e indireta, nas atividades de capacitação e tratamento de incidentes de segurança em redes de computadores, conforme disposto nos incisos III e VI do art. 39 do anexo da Portaria nº 13 do GSI, de 04 de agosto de 2006.

2.5 É condição necessária para a criação de uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, o órgão ou entidade possuir a competência formal e respectiva atribuição de administrar a infra-estrutura da rede de computadores de sua organização.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações - DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Administração Pública Federal, direta e indireta.

4 CONCEITOS E DEFINIÇÕES

Para os efeitos desta Norma Complementar são estabelecidos os seguintes conceitos e definições:

4.1 **Agente responsável**: Servidor Público ocupante de cargo efetivo ou militar de carreira de órgão ou entidade da Administração Pública Federal, direta ou indireta incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;

4.2 **Artefato malicioso**: é qualquer programa de computador, ou parte de um programa, construído com a intenção de provocar danos, obter informações não autorizadas ou interromper o funcionamento de sistemas e/ou redes de computadores;

4.3 **Comunidade ou Público Alvo:** é o conjunto de pessoas, setores, órgãos ou entidades atendidas por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais;