ancine
Agência Nacional do Cinema

PORTARIA Nº 139, 06 DE Julho DE 2015.

Aprova a instituição e o funcionamento da Equipe de Tratamento e Resposta a Incidentes em redes computacionais da Agência Nacional do Cinema – ANCINE.

A **DIRETORA-PRESIDENTE SUBSTITUTA DA AGÊNCIA NACIONAL DO CINEMA**, no uso das atribuições que lhe conferem o inciso IV, do artigo 13, do Anexo I, do Decreto nº 8.283, de 03 de julho de 2014, bem como o disposto no inciso III, do artigo 17, do Regimento Interno da ANCINE, e considerando:

a Resolução de Diretoria Colegiada ANCINE nº 63, de 23 de setembro de 2014, que institui a Política de Segurança da Informação e Comunicações da Agência Nacional do Cinema – ANCINE, e dá outras providências;

a Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal (APF);

a Norma Complementar nº 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, do Gabinete de Segurança Institucional da Presidência da República, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais – ETIR nos órgãos e entidades da APF;

a Norma Complementar nº 08/IN01/DSIC/GSIPR, de 19 agosto de 2010, do Gabinete de Segurança Institucional da Presidência da República, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da APF;

RESOLVE:

Art. 1º. Aprovar, na forma desta Portaria, a instituição e o funcionamento da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), da Agência Nacional do Cinema - ANCINE, em complemento à diretriz estabelecida pelo item 7.1, "e", da Política de Segurança da Informação e Comunicações - POSIC da ANCINE.

CAPÍTULO I

DOS TERMOS E DEFINIÇÕES

Art. 2º. Com base na NC 05/IN01/DSIC/GSIPR, de 14 de agosto de 2009, para efeitos desta resolução, ficam estabelecidos os seguintes termos e definições, em complemento àqueles definidos na POSIC da ANCINE:

I – Agente responsável: servidor público incumbido de chefiar e gerenciar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais, bem como responsável pelo relacionamento com o Centro de Tratamento de Incidentes de Segurança em Redes de Computadores da Administração Pública Federal - CTIR Gov.

II - 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.

III - CTIR GOV: Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal, subordinado ao Departamento de Segurança de Informação e Comunicações - DSIC do Gabinete de Segurança Institucional da Presidência da República – GSI.

IV - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

V - Serviço: é o conjunto de procedimentos, estruturados em um processo bem definido, oferecido à comunidade da Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais.

CAPÍTULO II

DAS RESPONSABILIDADES

Art. 3º. Compete ao Diretor Presidente da Agência Nacional do Cinema designar os membros da Equipe de Tratamento de Incidentes em Redes Computacionais da ANCINE.

Art. 4º. O Gerente de Tecnologia da Informação da ANCINE será o agente responsável pela ETIR.

Parágrafo único: O Gerente de Tecnologia da Informação será responsável, ainda, por manter a infraestrutura necessária à Equipe.

CAPÍTULO III

DA MISSÃO E DA ABRANGÊNCIA

Art. 5º. A ETIR tem como missão prioritária coordenar e realizar a prevenção, o tratamento e a resposta a incidentes de segurança na Rede Computacional da ANCINE.

Parágrafo único. São consideradas missões específicas: recuperação de sistemas; análise de ataques e intrusões; cooperação com outras equipes; e participação em fóruns e redes nacionais e internacionais.

Art. 6º. Considera-se público alvo das atividades pertinentes à ETIR da ANCINE:

I - todos os servidores e colaboradores que exercem suas atividades no âmbito da ANCINE; e

II - órgãos, entidades e empresas, públicas ou privadas, que tenham contratos, acordos ou convênios com a ANCINE para o intercâmbio de informações.

CAPÍTULO IV

DO MODELO DE IMPLEMENTAÇÃO

Art. 7º. A ETIR será composta por servidores da Gerência de Tecnologia da Informação da ANCINE, sem prejuízo das atribuições do cargo que ocupam, de acordo com o Modelo 1, descrito no item 7.1, da NC 05/IN01/DSIC/GSIPR.

CAPÍTULO V

DA ESTRUTURA ORGANIZACIONAL E DAS ATRIBUIÇÕES

Art. 8º. A ETIR ficará subordinada à Gerência de Tecnologia da Informação, da Secretaria de Gestão Interna, na estrutura organizacional da ANCINE.

Art. 9º. São atribuições da ETIR:

I - monitorar e analisar tecnicamente os incidentes de segurança nas redes de computadores;

II - implementar controles que permitam avaliar e mitigar os danos causados por incidentes de segurança nas redes de computadores;

III - apoiar e contribuir na capacitação relacionada ao tratamento de incidentes de segurança nas redes de computadores;

IV - realizar intercâmbio científico-tecnológico relacionado a Incidentes de Segurança nas Redes de Computadores junto a outras ETIR e com o CTIR.GOV.

Parágrafo único. A descrição dos serviços disponibilizados pela ETIR encontra-se no ANEXO I desta Portaria.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Art. 10. A ETIR terá autonomia completa, nos termos do item 9.1, da NC 05/IN01/DSIC/GSIPR, podendo executar as medidas de tratamento e recuperação de incidentes de segurança sem a aprovação prévia de níveis superiores de gestão.

Parágrafo único. Nos casos de incidentes de segurança de que trata o caput, o agente responsável pela ETIR deverá informar a ocorrência e as medidas aplicadas ao Diretor-Presidente da ANCINE imediatamente após a sua execução.

Art. 12. Casos omissos serão resolvidos pelo Secretário de Gestão Interna, ouvido o Gerente de Tecnologia da Informação, observando-se a legislação em vigor.

Art. 13. Esta Portaria entra em vigor na data de sua publicação.

Rosana dos Santos Alcântara
Diretora-Presidente Substituta

ancine
Agência Nacional do Cinema

ANEXO I – CATÁLOGO DE SERVIÇOS DA ETIR

I. TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS:

Definição: Consiste em receber, classificar, analisar e responder as solicitações e alertas relacionados aos incidentes de segurança em redes computacionais.

Descrição de procedimentos: O Coordenador da ETIR realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.

Disponibilidade do serviço: Será executado quando houver detecção de incidente de segurança.

Metodologia para execução do serviço: O Coordenador da ETIR, em conjunto com a equipe técnica, realizará análise dos alertas e solicitações e deverá tomar decisões em documento próprio, indicando a ação a ser realizada.

II. TRATAMENTO DE ARTEFATOS MALICIOSOS:

Definição: Consiste em analisar artefatos maliciosos, classificar o grau de risco e o indicar o tratamento adequado.

Descrição de procedimentos: O Coordenador da ETIR, em conjunto com a equipe técnica, realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas.

Disponibilidade do serviço: Será executado quando houver detecção de artefato malicioso pela ETIR.

Metodologia para execução do serviço: Deverá ser elaborado relatório sobre a análise e tratamento do artefato malicioso.

III. TRATAMENTO DE VULNERABILIDADES:

Definição: Consiste em analisar vulnerabilidades em redes e sistemas, e gerar relatórios sobre os resultados encontrados.

Descrição de procedimentos: O Coordenador da ETIR, em conjunto com a equipe técnica, realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas.

Disponibilidade do serviço: Será executado quando houver necessidade da Gerência de Tecnologia da Informação ou via requerimento por pessoa competente em sua respectiva unidade por meio da ETIR.

Metodologia para execução do serviço: O serviço somente poderá ser executado pela Gerência de Tecnologia da Informação da ANCINE.

IV. EMISSÃO DE ALERTAS E ADVERTÊNCIAS:

Definição: Consiste em gerar comunicados e relatórios sobre ações maliciosas e identificação de tendências que possam afetar as atividades da ANCINE.

Descrição de procedimentos: O Coordenador da Equipe emitirá comunicados e relatórios, sempre que necessário, para divulgar ameaças identificadas que possam comprometer as atividades da organização.

Disponibilidade do serviço: Será executado sempre que a ETIR julgar pertinente.

Metodologia para execução do serviço: Os alertas e advertência serão enviados por meio eletrônico.

V. AVALIAÇÃO DE SEGURANÇA:

Definição: Consiste em avaliar aspectos de segurança em ativos de rede, sistemas e serviços da ANCINE.

Descrição de procedimentos: Coordenador da Equipe, em conjunto com a equipe técnica, realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas.

Disponibilidade do serviço: Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade, ou sempre que a ETIR julgar necessário.

Metodologia para execução do serviço: A Equipe analisará o ativo, sistema ou serviço, e emitirá relatório sobre a segurança, levando em consideração os Planos de Continuidade de Negócios e Tratamento de Riscos. Deverá ser emitido laudo em documento próprio.