Anexo I da Norma N10/POSIC/MinC – Gestão de Incidentes de Segurança da Informação e Melhorias

DOCUMENTO DE CONSTITUIÇÃO DA ETIR

1. MISSÃO

1.1. A ETIR do Ministério da Cultura tem como missão prioritária facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais, receber e/ou notificar qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores, a fim de contribuir para a adequada prestação dos serviços do ministério.

2. PÚBLICO ALVO

2.1. Formam o público alvo da ETIR todos os usuários da rede corporativa e sistemas do Ministério da Cultura lotados na sede e também localizados nas Representações Regionais.

2.2. A ETIR deve se reportar ao Comitê de Segurança da Informação e Comunicações – CSIC e se relacionar internamente com a área de tecnologia da informação. Externamente a ETIR se relaciona com o Centro de Tratamento e Resposta de Incidentes em Redes Computacionais – CTIR Gov e outras equipes similares da organização pública da Administração Pública Federal - APF.

3. MODELO

3.1. A ETIR é formada a partir dos membros das equipes de TI do próprio órgão, que além de suas funções regulares passam a desempenhar as atividades relacionadas ao tratamento e respostas a incidentes em redes computacionais. Neste caso as funções e serviços de tratamento de incidente devem ser realizadas, preferencialmente, por administradores de rede ou de sistema ou, ainda, por peritos em segurança.

3.2. A Equipe desempenha suas atividades, em regra, de forma reativa, sendo desejável, porém que o Agente Responsável pela ETIR atribua responsabilidades para que os seus membros exerçam atividades proativas.

3.3. A Equipe é a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR Gov.

4. ESTRUTURA ORGANIZACIONAL

4.1. A ETIR fica subordinada à área de tecnologia da informação na estrutura organizacional do Ministério da Cultura.

4.2. Compete ao Gestor de Segurança da Informação e Comunicações coordenar a Equipe de Tratamento de Incidentes em Redes Computacionais do Ministério da Cultura. São atribuições do Gestor da ETIR:

I. Coordenar a instituição, implementação e manutenção da infraestrutura necessária à ETIR;

II. Garantir que os incidentes em Redes Computacionais da Rede de Computadores do Ministério da Cultura sejam monitorados;

III. Adotar procedimentos de *feedback* para assegurar que os usuários que comuniquem incidentes de segurança da informação e comunicações sejam informados dos procedimentos adotados;

IV. Apoiar os treinamentos relacionados à SIC fornecendo casos práticos de incidentes de segurança, garantindo-se a confidencialidade e os devidos níveis de sigilo, sobre o que pode vir a acontecer, como reagir a tais incidentes e como evitá-los no futuro.

4.3. É de competência da ETIR:

I. Recolher provas o quanto antes após a ocorrência de um incidente de SIC;

II. Executar uma análise crítica sobre os registros de falhas para assegurar que as mesmas foram satisfatoriamente resolvidas;

III. Investigar as causas dos incidentes de SIC;

IV. Implementar mecanismos para permitir a quantificação e monitoração dos tipos, volumes e custos de incidentes e falhas de funcionamento;

V. Indicar a necessidade de controles aperfeiçoados ou adicionais para limitar a frequência, os danos e o custo de futuras ocorrências de incidentes.

4.4. A ETIR será composta por:

I. Responsável pela área de Infraestrutura Tecnológica da área de TI do órgão;

II. Analista de Tecnologia da Informação – Lotado na área de TI do órgão;

4.5. Caso necessário, podem ser convocados para compor a ETIR:

I. Representante da Consultoria Jurídica do órgão;

II. Representante dos Recursos Humanos do órgão;

III. Representante da área de Logística do órgão.

4.6. Para cada um dos representantes, pode ser designado um suplente, que deve ter condições de substituir o titular e executar todas as suas atribuições como se o mesmo fosse.

5. AUTONOMIA

5.1. A autonomia da ETIR é compartilhada e trabalha em conjunto com os outros setores da organização, representado pelo Comitê de Segurança da Informação e Comunicações a fim de participar do processo de tomada de decisão sobre quais medidas serão adotadas.

6. SERVIÇOS

6.1. São serviços da ETIR:

I. Implementar, no mínimo, o Tratamento de Incidentes de Segurança em Redes Computacionais, contemplando tratamento de artefatos maliciosos

II. Tratamento de vulnerabilidades

III. Emissão de alertas e advertências

IV. Prospecção e monitoração de novas tecnologias

V. Avaliação de segurança

VI. Detecção de intrusão
VII. Disseminação de informações relacionadas à segurança
VIII. Desenvolvimento de ferramentas de segurança

7. DISPOSIÇÕES GERAIS

7.1. A Norma que disciplina o Gerenciamento de Incidentes de Segurança da Informação versará, dentre outras diretrizes inerentes, sobre os serviços a serem prestados pela ETIR.

7.2. Assim que possível, a implementação da ETIR deve ser migrada para o modelo "2 - Centralizado", conforme a Norma Complementar nº 05/IN01/DSIC/GSIPR, momento em que uma nova unidade da ETIR deve ser criada, com chefia e quadro próprios, novas atribuições proativas e maior nível de autonomia.

7.3. Este documento deve ser revisado periodicamente em intervalos de até 3 (três) anos.