MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA TECNOLOGIA DO AMAPÁ

REGIMENTO INTERNO DA EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAPÁ

ETIR - IFAP

Macapá-AP, julho de 2012

TÍTULO I

DA MISSÃO

Art. 1º - A Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP 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 Instituto.

TÍTULO II

DO PÚBLICO ALVO

Art. 2º - Formam o público alvo da ETIR todos os usuários da rede de computadores e sistemas do IFAP em suas diversas unidades.

Parágrafo Único - A ETIR deverá reportar-se ao Gestor de Segurança da Informação e se relacionará internamente com as equipes locais no âmbito do IFAP. Externamente a ETIR se relacionará 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).

TÍTULO III

DO MODELO

Art. 3º - O modelo utilizado pela ETIR será misto e sendo composto por uma Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais central e Equipes distribuídas pelas unidades.

Art. 4º - A Equipe central será a responsável por criar as estratégias, gerenciar as atividades e distribuir as tarefas entre as Equipes descentralizadas, além de ser a responsável, perante toda a organização, pela comunicação com o CTIR GOV.

Art. 5º - As Equipes distribuídas serão responsáveis por implementar as estratégias e exercer suas atividades em suas respectivas áreas de responsabilidade nas usa as unidades de origem.

SEÇÃO I

DA ESTRUTURA ORGANIZACIONAL

Art. 6º - A ETIR ficará subordinada ao Comitê Gestor de Segurança da Informação na estrutura organizacional do IFAP.

SEÇÃO II

DAS ATRIBUIÇÕES

Art. 7º - 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 IFAP 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 Segurança da Informação fornecendo casos práticos de incidentes de segurança, garantindo-se a confidencialidade e devidos níveis de sigilo, sobre o que poderia acontecer, como reagir a tais incidentes e como evitá-los no futuro.

Parágrafo Único - Compete ao Gestor de Segurança da Informação coordenar a Equipe de Tratamento de Incidentes em Redes Computacionais do IFAP.

Art. 8º - 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 falha 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.

SEÇÃO III

DA COMPOSIÇÃO

Art. 9º - A ETIR será composta por:

I. Gestor de Segurança da Informação;

II. Analista de TI;

III. Técnico de TI;

IV. Auditor.

Art. 10 - Caso necessário, poderão ser convocados para comporem extraordinariamente a ETIR:

I. Procurador;

II. Pepresentante da área de Gestão de Pessoas;

III. Representante da Assessoria de Comunicação.

Art. 11 - Para cada uma das posições deverá ser designado 1 (um) suplente que deverá ter condições de substituir o titular e executar todas as suas atribuições como se o mesmo fosse.

Art. 12 - Nas unidades cada ETIR será composta de um Analista de TI e um Técnico de TI.

SEÇÃO IV

DA AUTONOMIA

Art. 13 - A autonomia da ETIR será compartilhada e trabalhará em conjunto com os outros setores da organização a fim de participar do processo de tomada de decisão sobre quais medidas serão adotadas.

SEÇÃO V

DOS SERVIÇOS

Art. 14 - A ETIR terá seus serviços classificados em 2 (dois) níveis:

I. Serviços Superiores: Quando tratarem de incidentes que comprometam de forma imediata

e/ou sejam classificados como de grande risco;

II. Serviços Comum: Quando os serviços servirem para suporte a outras tomadas de decisões fora do escopo da ETIR.

Art. 15 - A ETIR terá seu catálogo de serviços com os seguintes itens:

I. TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDES COMPUTACIONAIS:

I.1. Classe:

a) Superior.

I.2. Definição:

a) consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

I.3. Descrição das funções e procedimentos que compõem o serviço:

a) O Coordenador da Equipe Local realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.

I.4. Disponibilidade do serviço:

a) Será executado quando houver detecção de um incidente pela sua respectiva unidade através da ETIR Local.

I.5. Metodologia para execução do serviço:

a) O Coordenador da Equipe Local conjuntamente com seus técnicos analisará relatórios gerados por aplicativos devidamente instituídos no IFAP e a partir de tal informação tomar decisões em documento próprio com a ação e/ou recomendação a ser tomada;

b) Tempo de tratamento: imediato.

II. RELATÓRIO SOBRE ACESSO DE INTERNET:

II.1. Classe:

Comum.

II.2. Definição:

a) consiste em gerar relatório sobre acesso de dados a internet pelo equipamento do usuário que fizer a requisição ou pelo seu chefe imediato, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

II.3. Descrição das funções e procedimentos que compõem o serviço:

a) O Coordenador da Equipe Local realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.

II.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR Local.

II.5. Metodologia para execução do serviço:

a) O serviço só poderá ser requerido pelo próprio usuário, por sua chefia imediata ou hierarquicamente superior para o Coordenador da Equipe Local que emitirá os dados em até 10 (dez) dias em documento próprio;

b) Tempo de tratamento: até 10 (dez) dias.

III. TRATAMENTO DE ARTEFATOS MALICIOSOS:

III.1. Classe:

a) Superior.

III.2. Definição:

a) Consiste em analisar artefatos maliciosos, classificar seu grau de risco e o tratamento para o mesmo.

III.3. Descrição das funções e procedimentos que compõem o serviço:

a) O Coordenador da Equipe Local realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.

III.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR Local;

b) Será executado quando houver detecção por meio de software ou outra ferramenta de gestão pela ETIR.

III.5. Metodologia para execução do serviço:

a) O serviço será imediatamente de acordo com o risco que o artefato está classificado. O tratamento se dará primeiramente em tentativa de recuperação quando for um ativo do Instituto e de eliminação quando for objeto fora do escopo do IFAP;

b) Será feito um relatório em documento próprio sobre a referida incidência;

c) Tempo de tratamento: imediato.

IV. TRATAMENTO DE VULNERABILIDADES:

IV.1. Classe:

a) Superior.

IV.2. Definição:

a) Consiste em gerar relatório sobre as vulnerabilidades sobre um determinado ativo.

IV.3. Descrição das funções e procedimentos que compõem o serviço:

a) O Coordenador da Equipe Local realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negócio.

IV.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR Local;

b) Será executado antes e depois de qualquer aquisição de ativo de TI.

IV.5. Metodologia para execução do serviço:

a) O serviço só poderá ser requerido pelo próprio usuário, por sua chefia imediata ou hierarquicamente superior para o Coordenador da Equipe Local que emitirá os dados em até 10 (dez) dias em documento próprio;

b) Tempo de tratamento: até 10 (dez) dias.

V. EMISSÃO DE ALERTAS E ADVERTÊNCIAS:

V.1. Classe:

a) Superior.

V.2. Definição:

a) consiste em gerar comunicados e/ou relatórios sobre ações maliciosa e também a identificação de tendências que possam afetar as atividades do IFAP.

V.3. Descrição das funções e procedimentos que compõem o serviço:

a) O Coordenador da Equipe Local emitirá relatórios para divulgar perigos ativos na rede nacional de dados e/ou ataques que possam comprometer as atividades da organização.

V.4. Disponibilidade do serviço:

a) Será executado quando a ETIR Geral detectar a necessidade deste evento através do ambiente externo do IFAP;

b) Será executado quando um chefe de setor sentir a necessidade de conscientização por seus subordinados.

V.5. Metodologia para execução do serviço:

a) Os alertas e advertência serão enviados por meio eletrônico como a Intranet e/ou e-mail institucional;

b) Tempo de tratamento: 1 (um) dia.

VI. ANÚNCIOS:

VI.1. Classe:

a) Comum;

VI.2. Definição:

a) Consiste em na divulgação por meio de artefatos gerados com apoio da Assessoria de Comunicação com o intuito de conscientização de um determinado tema que atenda ao escopo da ETIR.

VI.3. Descrição das funções e procedimentos que compõem o serviço:

a) O Coordenador da Equipe Local em conjunto com a ASCOM realizará as atividades necessária para a divulgação eficiente de informação relevante ao tratamento de incidentes e segurança da informação.

VI.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR Local.

VI.5. Metodologia para execução do serviço:

a) A Equipe analisará a informação a ser divulgada contendo um texto simples, de fácil entendimento e que contemple a devida proposta de disseminação da conteúdo com a ASCOM;

b) Tempo de tratamento: 6 (seis) dias.

VII. PROSPECÇÃO OU MONITORAÇÃO DE NOVAS TECNOLOGIAS:

VII.1. Classe:

a) Superior.

VII.2. Definição:

a) Consiste em propor adequações a novas tendência no âmbito do IFAP, desenvolvendo tarefas que busquem analise prévia sobre os efeitos das mesmas sobre a área de TI e segurança da informação.

VII.3. Descrição das funções e procedimentos que compõem o serviço:

a) A Equipe desenvolverá estudos e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negocio e mudança.

VII.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR Local.

VII.5. Metodologia para execução do serviço:

a) A Equipe irá definir parâmetros para informar qual os benefícios, vulnerabilidades e riscos relacionados a esta nova tecnologia;

b) Tempo de tratamento: até 15 (quinze) dias.

VIII. AVALIAÇÃO DE SEGURANÇA:

VIII.1. Classe:

a) Comum.

VIII.2. Definição:

a) Consiste em analisar sobre um determinado ativo da rede do IFAP.

VIII.3. Descrição das funções e procedimentos que compõem o serviço:

a) O Coordenador da Equipe Local realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas.

VIII.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR Local.

VIII.5. Metodologia para execução do serviço:

a) A Equipe analisará o ativo em conjunto com seu ambiente e emitirá relatório sobre a segurança levando em consideração os Planos de Continuidade de Negócios e Tratamento de Riscos. Será emitido laudo em até 10 (dez) dias em documento próprio;

b) Tempo de tratamento: até 10 (dez) dias.

IX. DESENVOLVIMENTO DE FERRAMENTAS DE SEGURANÇA:

IX.1. Classe:

a) Superior.

IX.2. Definição:

a) Consiste no desenvolvimento de aplicações que dão suporte a área de segurança da informação no âmbito do IFAP.

IX.3. Descrição das funções e procedimentos que compõem o serviço:

a) A Equipe em conjunto com a Coordenação de Sistemas de informação realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e de acordo com os planos da gestão de continuidade do negocio.

IX.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento pela ETIR Geral ou as ETIR Distribuídas.

IX.5. Metodologia para execução do serviço:

a) A Equipe fornecerá todas as informações e requisitos necessários para fomentar as atividades de desenvolvimento a Coordenação de Sistemas. A Codificação ficará exclusivamente a cargo de tal coordenação. O prazo para entrega do serviço será feito no projeto do sistema;

b) Tempo de tratamento: determinado no projeto.

X. DETECÇÃO DE INTRUSÃO:

X.1. Classe:

a) Superior.

X.2. Definição:

a) Consiste em analisar tráfego de dados e ou outro mecanismo que comprove acesso indevido.

X.3. Descrição das funções e procedimentos que compõem o serviço:

a) A Equipe realizará as atividades e procedimentos de acordo com diretrizes devidamente normatizadas e coma legislação vigente.

X.4. Disponibilidade do serviço:

a) Será executado quando houver o requerimento por pessoa competente na sua respectiva unidade através da ETIR Local;

b) Será executado com houver indícios do acesso não autorizado.

X.5. Metodologia para execução do serviço:

a) A Equipe analisará ambiente e/ou os ativos envolvidos e emitirá relatório sobre invasão. Será emitido laudo em até 10 (dez) dias em documento próprio;

b) Tempo de tratamento: imediato.

XI. DISSEMINAÇÃO DE INFORMAÇÕES RELACIONADAS À SEGURANÇA:

XI.1. Classe:

a) Comum.

XI.2. Definição:

a) Consiste em gerar relatório sobre acesso de dados a internet pelo equipamento do usuário que fizer a requisição ou pelo seu chefe imediato, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

XI.3. Descrição das funções e procedimentos que compõem o serviço:

a) A Equipe realizará, preferencialmente, reuniões para divulgar as politicas do governo federal referente a segurança da informação e as atualização da legislação vigente sobre o tema.

XI.4. Disponibilidade do serviço:

a) Será executado quando a ETIR Geral detectar a necessidade deste evento através de atualização da legislação;

b) Será executado de acordo com o cronograma de anual atividades de TI.

XI.5. Metodologia para execução do serviço:

a) O coordenador se reunirá com o público-alvo para expor as informações.

b) Tempo de tratamento: até 6 (seis) dias.