

## **ANEXO I**

### **EQUIPE DE TRATAMENTO E RESPOSTA A INCIDENTES EM REDES COMPUTACIONAIS - ETIR**

#### **1.1 - MISSÃO**

Planejar, coordenar e executar atividades de tratamento e resposta a incidentes de segurança da informação, confirmado ou sob suspeita, relacionado às redes de computadores, preservando os dados, as informações e a infraestrutura de TIC do Tribunal de Justiça do Acre.

#### **1.2 - PÚBLICO ALVO**

Usuários da rede corporativa de computadores e sistemas de informação do Tribunal de Justiça do Acre.

#### **1.3 - MODELO DE IMPLEMENTAÇÃO**

1.3.1 A ETIR será formada por membros das unidades vinculadas à Diretoria de Tecnologia da Informação - DITEC, que além de suas funções regulares, passarão a desempenhar as atividades relacionadas ao tratamento e resposta a incidentes de segurança na rede de computadores interna do TJAC.

1.3.2 A Equipe desempenhará suas atividades, via de regra, de forma reativa. Porém, é desejável a atribuição de responsabilidades para que os seus membros exerçam atividades proativas.

#### **1.4 - NÍVEL DE AUTONOMIA**

1.4.1 - A ETIR tem plena autonomia para tomada de decisão sobre quais medidas serão adotadas e poderá conduzir o público alvo para realizar ações ou as medidas necessárias para reforçar a resposta ou a postura da organização na recuperação de incidentes de segurança na rede interna de computadores. Durante um incidente de segurança, se justificável, a equipe poderá tomar a decisão de executar as medidas de recuperação, sem esperar pela aprovação de níveis superiores de gestão.

1.4.2 A ETIR poderá solicitar apoio multidisciplinar abrangendo as áreas de tecnologia da informação, jurídica, pesquisas judiciárias, comunicação, controle

interno, segurança institucional, dentre outras necessárias para responder aos incidentes de segurança de maneira adequada e tempestiva.

## **1.5 - DESIGNAÇÃO DE INTEGRANTES**

1.5.1 - A ETIR deve ser composta por servidores públicos ocupantes de cargo efetivo de carreira, com perfil técnico compatível, e deverá ser gerida pela Gerência de Segurança da Informação - GESEG.

1.5.2 Recomenda-se que os membros da ETIR sejam: administradores de sistemas ou de segurança, administradores de banco de dados, administradores de redes ou analistas de suporte.

1.5.3 - A ETIR será composta no mínimo por:

- a) 2 servidores (as) da Gerência de Segurança da Informação;
- b) 1 servidor (a) da Gerência de Sistemas;
- c) 1 servidor (a) da Gerência de Serviços;
- d) 1 servidor (a) de apoio indicado pelo Diretor da DITEC.

1.5.4 Para cada membro da Equipe deverá ser designado um substituto, que deverá ser treinado e orientado para a realização das tarefas e atividades da ETIR.

1.5.5 Portaria da DITEC indicará os servidores titulares e substitutos que irão compor a ETIR.

## **1.6 - CANAL DE COMUNICAÇÃO**

Os canais de comunicação com a ETIR e/ou para informar incidentes de segurança da informação estão publicados na página "Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do Tribunal de Justiça do Acre" disponível no site institucional, dentro da seção "Institucional Governança de TIC".

## **1.7 - SERVIÇOS QUE SERÃO PRESTADOS PELA ETIR (COMPETÊNCIAS)**

1.7.1 Execução do Processo de Gestão de Incidentes de Segurança da Informação do TJAC;

1.7.2 - Aplicar procedimentos técnicos e normativos no contexto de tratamento de incidentes de segurança em rede orientados pelo Centro de Tratamento e Resposta a Incidentes de Segurança em Redes de Computadores da Administração Pública Federal (CTIR GOV);

1.7.3 Registrar de forma detalhada a comunicação de ocorrência ou suspeita de incidente de segurança da informação na rede de computadores do TJAC;

1.7.4 Investigar, em conjunto com as demais áreas da DITEC, com base nas informações registradas, as possíveis causas, extensão e impacto do incidente;

1.7.5 Coletar e preservar as evidências, durante o processo de tratamento do incidente penalmente relevante, nos termos do Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário;

1.7.6 Comunicar às partes interessadas sobre ocorrência, extensão, impacto, resultados do tratamento e encerramento do incidente;

1.7.7 - Consolidar as ocorrências de incidentes comunicados pelos usuários por meio de relatórios de Incidentes de Segurança da Informação;

1.7.8 - Propor e acompanhar a execução das ações de contenção do incidente;

1.7.9 - Executar as ações de contenção do incidente, quando no âmbito da área técnica a que pertencem;

1.7.10 - Executar uma análise crítica sobre os registros de falhas para assegurar que elas foram satisfatoriamente resolvidas;

1.7.11 Implementar mecanismos para permitir a quantificação e monitorização dos tipos, volumes e custos de incidentes e falhas de funcionamento;

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

1.7.13 - Comunicar, de imediato, a ocorrência de todos os incidentes de segurança possíveis de serem notificados, ocorridos na sua área de atuação ao COCRI e ao CGESI, e aos órgãos competentes conforme estabelecem os Protocolos e Manuais de segurança da informação do Poder Judiciário.

1.7.14 - Realizar reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

1.7.15 - A ETIR, sob a supervisão da Gerência de Segurança da Informação do TJAC, durante o processo de tratamento do incidente, quando constatado crise cibernética, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas,

deverá, de imediato, comunicar o Comitê de Crises Cibernéticas e o Comitê Gestor de Segurança da Informação.

1.7.16 Elaborar Relatório de Incidente de Segurança da Informação, também chamado de Relatório de Comunicação de Incidente de Segurança em Redes Computacionais, descrevendo detalhadamente os eventos verificados, nos termos do Protocolo de Investigação para Ilícitos Cibernéticos no âmbito do Poder Judiciário, quando se tratar de incidente penalmente relevante.