

## ANEXO III – FLUXO DE TRABALHO PARA SEGURANÇA GERENCIADA

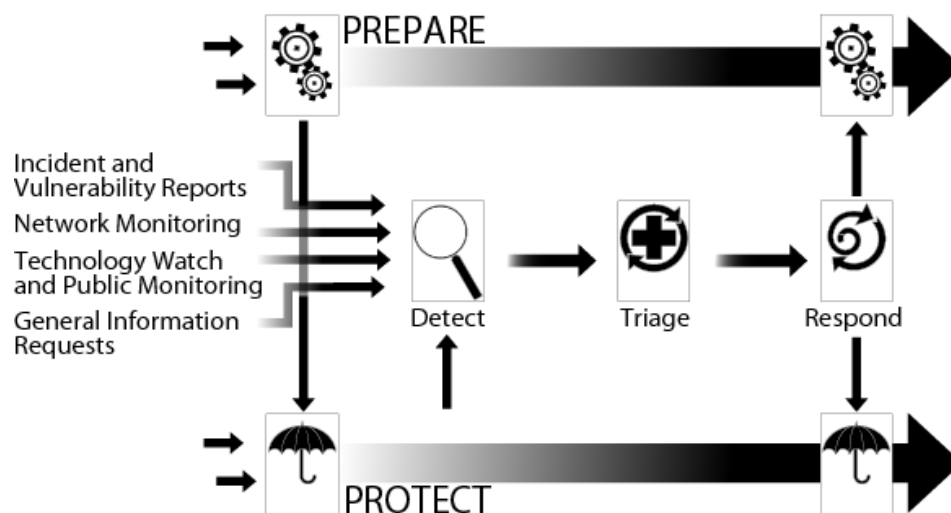
### 1. Objetivo do Processo de Gerenciamento de Incidentes- CIRT

1.1. O modelo de gerenciamento de incidentes para o CSIRT, tem como objetivo implementar o processo otimizado para gestão dos incidentes de segurança da informação, visando ter estratégias e processos de qualidade não apenas para tratar incidentes quando ocorrerem, mas para prevenir ocorrências ou recorrências e inclui processos para:

- Planejar a implementar a capacidade de gerenciar incidentes;
- Garantir a segurança e o hardening da infraestrutura organizacional afim de prevenir a ocorrência de incidentes ou mitigar um incidente em curso;
- Detectar, triar e responder a incidentes e eventos quando ocorrerem.

### 1.2. Modelo de Gerenciamento de Incidentes

1.2.1. A contratada deverá estabelecer os processos para gerenciamento dos incidentes de segurança da informação conforme exemplificado na figura abaixo de acordo com o CMU/SEI-2004-TR-015.



### 1.2.2. Preparação

- Definição de recursos e equipes de acordo com as capacidades técnicas de cada um;
- Ferramentas, equipamentos e infraestrutura para suporte, bem como comunicações, conexões de rede, base de incidentes já existente, relatórios e ferramentas de análise;
- Políticas, Procedimentos e padrões existentes.

### **1.2.3. Proteger a Infraestrutura**

- Alterações de regras em firewalls, roteadores ou servidores de e-mail para proibir que pacotes maliciosos entrem na infra-estrutura;
- Atualizações no IDS/IPS para incluir novas assinaturas;
- Mudanças nas configurações do sistema para desativar os serviços padrão;
- Instalação de patches para software vulnerável;
- Atualizações no software de verificação de vírus para incluir novas assinaturas para novas ameaças.

### **1.2.4. Detectar Eventos**

- Observar e relatar eventos;
- Receber notificações de eventos;
- Monitorar indicadores de dispositivos de gerenciamento de redes, IDS/IPS, firewall e outros mecanismos de segurança de forma proativa;
- Analisar os indicadores monitorados buscando comportamento malicioso ou ameaças a infraestrutura;
- Repassar qualquer evento suspeito ou notável para o processo de triagem;
- Repassar eventos para outras áreas fora do processo de gerenciamento de incidentes quando aplicável;
- Finalizar qualquer evento que não foi repassado ao processo de triagem.

### **1.2.5. Triar Eventos**

- Categorizar e correlacionar eventos;
- Priorizar eventos;
- Atribuir eventos para tratamento ou resposta;
- Repassar informações e dados relevantes para o processo de resposta;
- Repassar eventos para outras áreas fora do processo de gerenciamento de incidentes quando aplicável;
- Finalizar qualquer evento que não foi repassado ao processo de resposta ou à outras áreas.

#### **1.2.6. Responder a Incidentes**

- Analisar o evento;
- Planejar uma estratégia de resposta;
- Coordenar e prover uma resposta técnica, gerencial e legal que pode envolver ações para conter, resolver ou mitigar incidentes e ações para reparar e recuperar os sistemas afetados;
- Comunicar com as partes externas;
- Repassar eventos para outras áreas fora do processo de gerenciamento de incidentes quando aplicável;
- Finalizar a resposta a incidentes;
- Passar as lições aprendidas e os dados do incidente para o processo de preparação utilizar em uma futura análise pós morte.