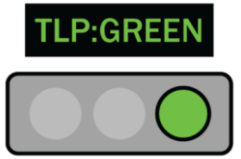


RNEP-GW

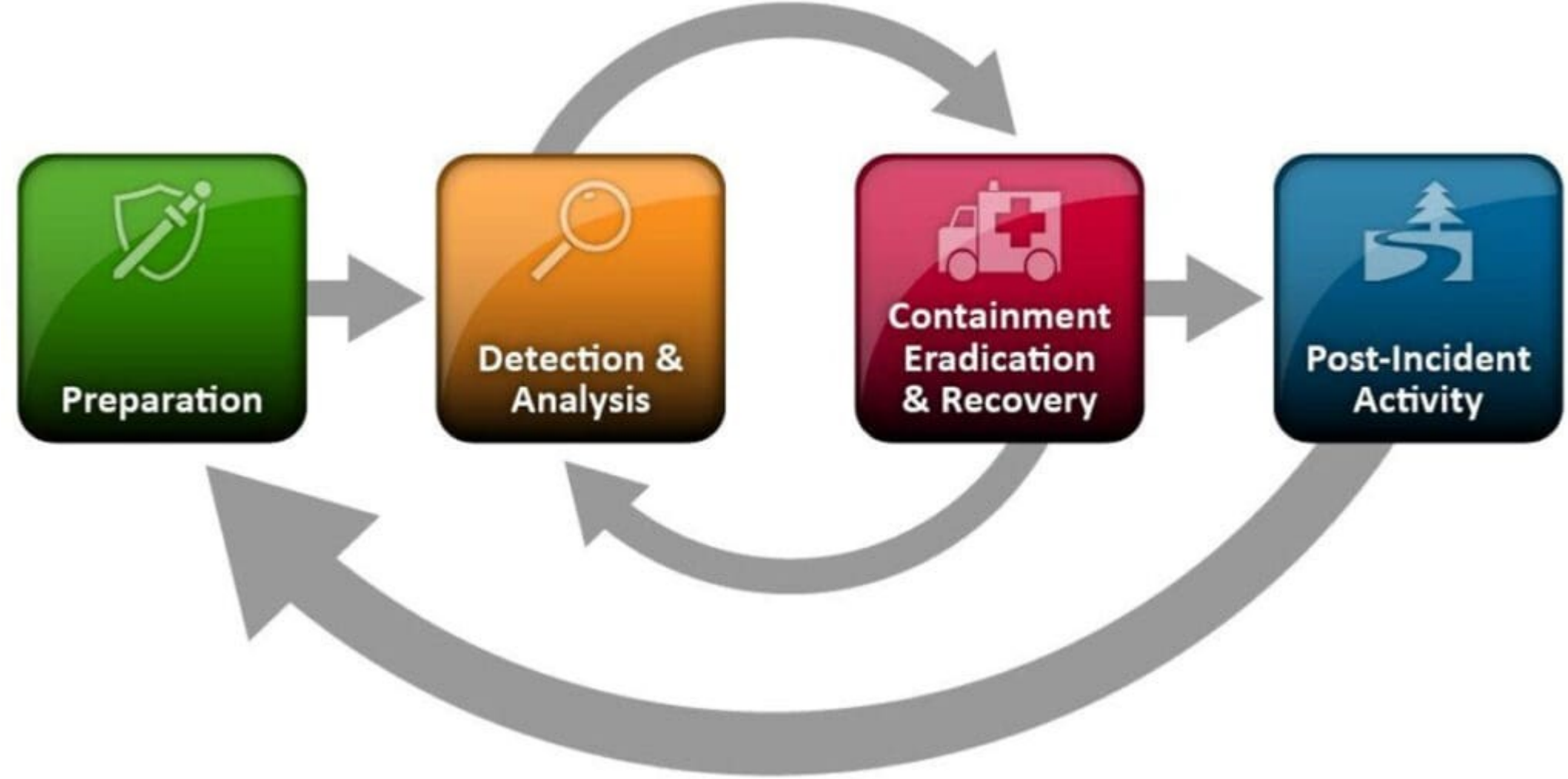
MÓDULO RESPOSTA A INCIDENTES

fct csirt

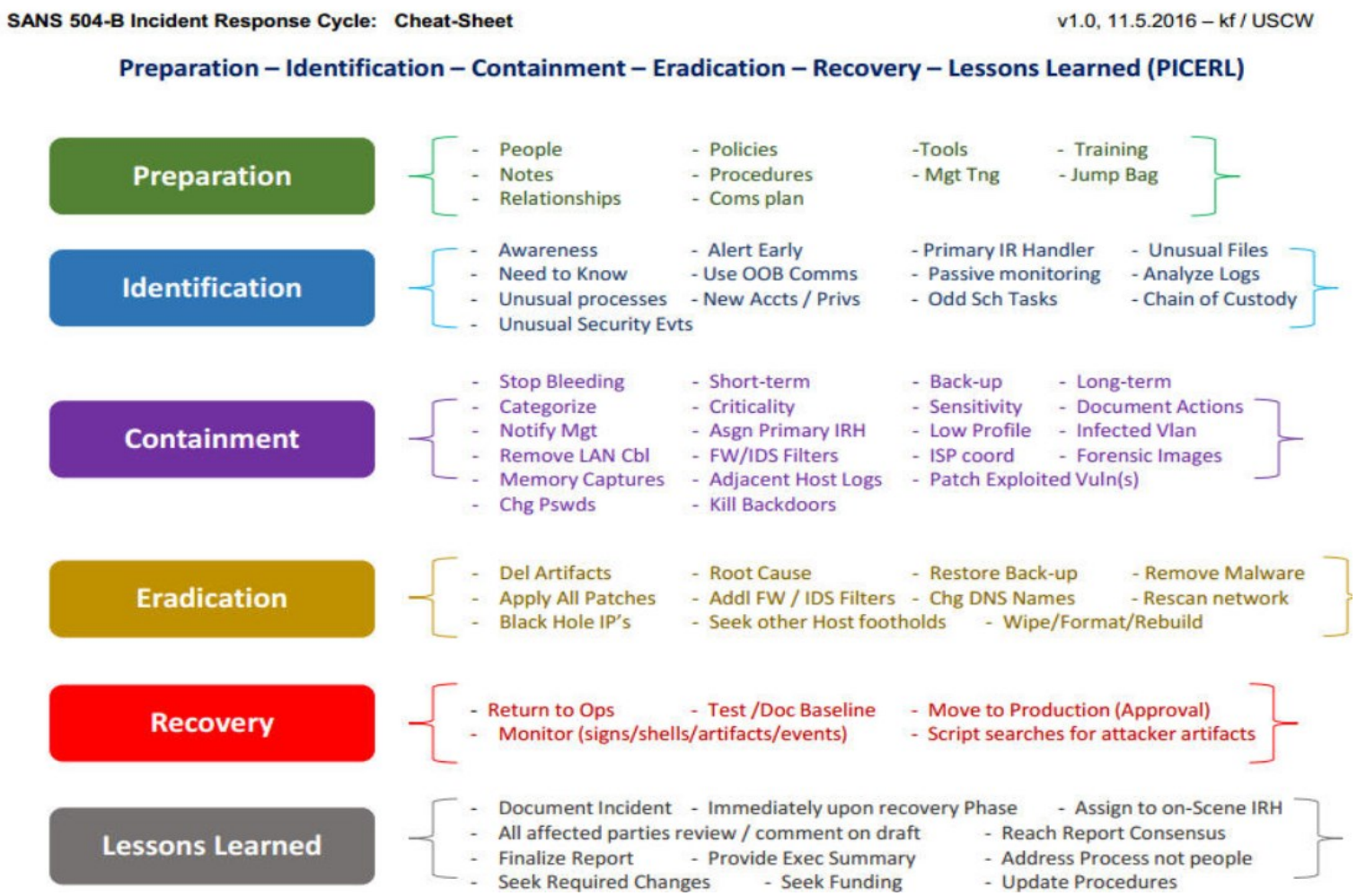
RNEP-GW

DEFINIÇÕES

NIST INCIDENT RESPONSE FRAMEWORK



FASES - NIST INCIDENT RESPONSE FRAMEWORK



FASES - NIST INCIDENT RESPONSE FRAMEWORK

É o resultado de uma ação ou conjunto de ações que possam causar uma perda de um ou vários pilares da CIA.

CRIAÇÃO DE UM INCIDENTE DE SEGURANÇA

Denúncias de atividades maliciosas

Deteção de atividades suspeitas

Anomalias face a padrões de funcionamento

NOTIFICAÇÃO

NOTIFICAÇÃO - REGISTO

Um incidente de segurança deve ser sempre registado

Gestão de incidentes centralizada

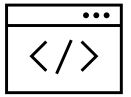
- Histórico
- IDs
- Filtrados
- Duplicados
- Correlacionar

Automatização

IA

Telefone

E-mail



Web

Outros

NOTIFICAÇÃO - FERRAMENTAS

REQUEST TRACKER INCIDENT RESPONSE

RTIR

Jira Service Management

Jira ITSM

bmc helix

BMC Helix ITSM

STORM powered by OTRS

STORM OTRS

osTicket Support Ticket System

osTicket

Outros...

TRIAGEM

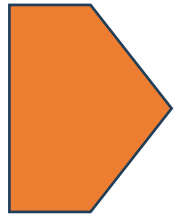
TRIAGEM 1/2

Telefone

E-mail

Web

Outros



TRIAGEM 2/2

É mesmo um incidente de segurança?

Quem reportou o incidente?

Faz parte do nosso âmbito?

Qual o impacto e a criticidade?

Que recursos necessitamos para o tratamento?

Quem deve tratar do incidente?

TRIAGEM - TAXONOMIA

Common language for incident response

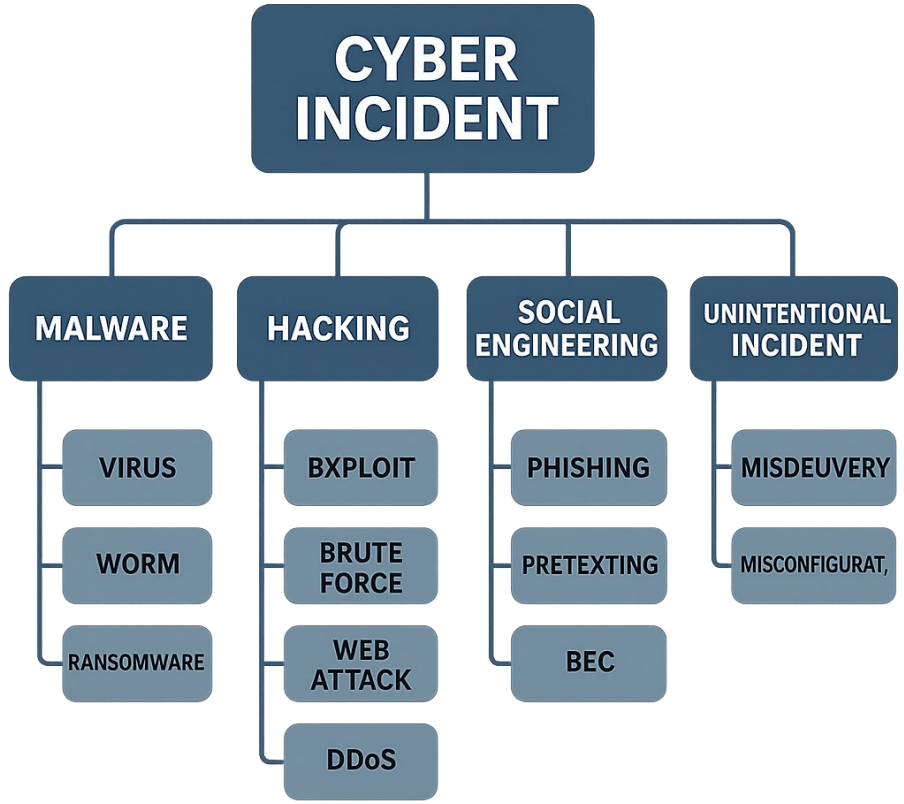
- By Carnegie Mellon University

Taxonomia eCSIRT.net

- Desenvolvida durante o projeto eCSIRT.net

Taxonomia própria

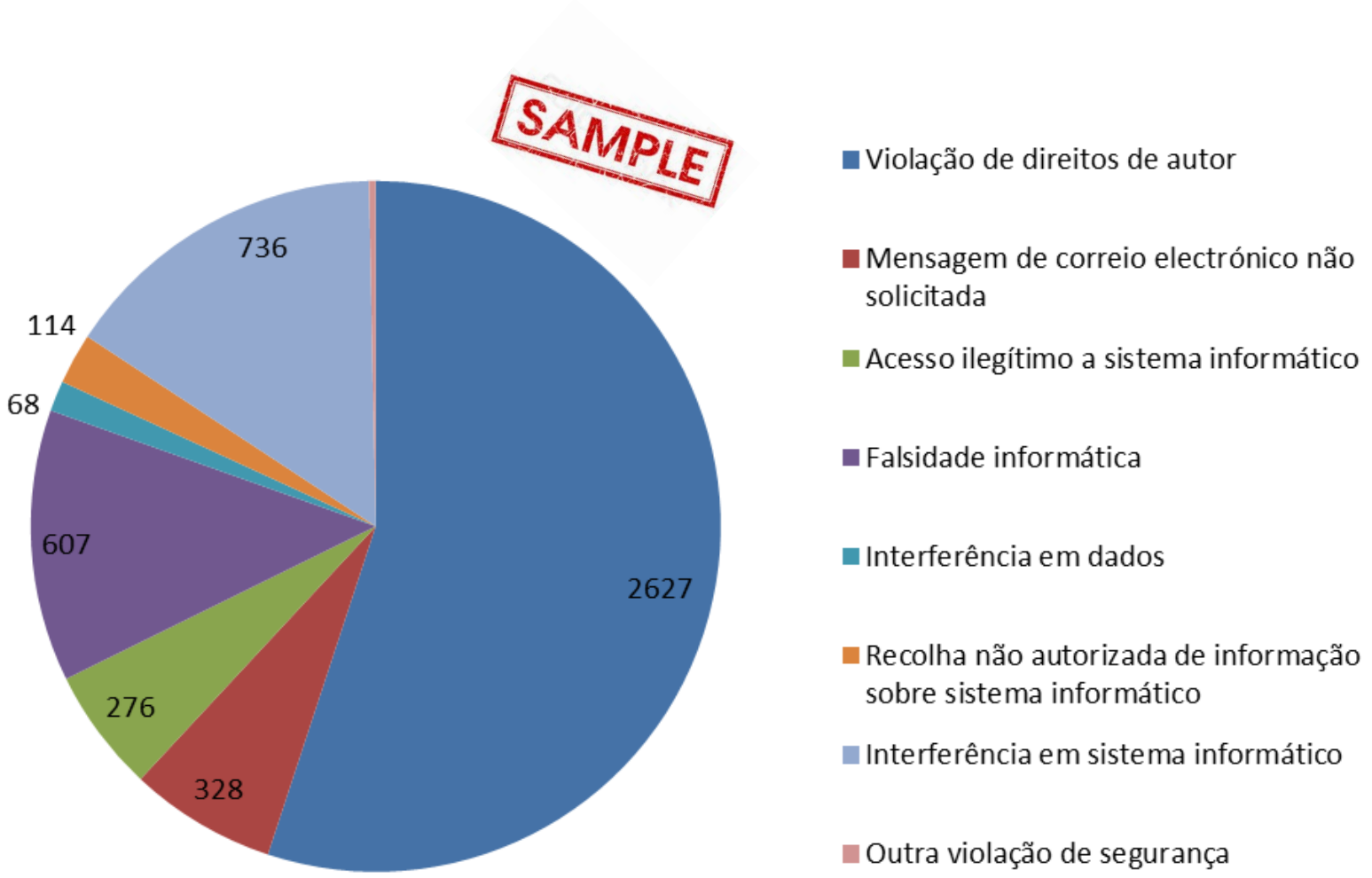
- Baseada em experiência



Taxonomia usada na RCTS (e RNCSIRT):

- https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf

TRIAGEM - CLASSIFICAÇÃO 1/2



TRIAGEM - CLASSIFICAÇÃO 2/2

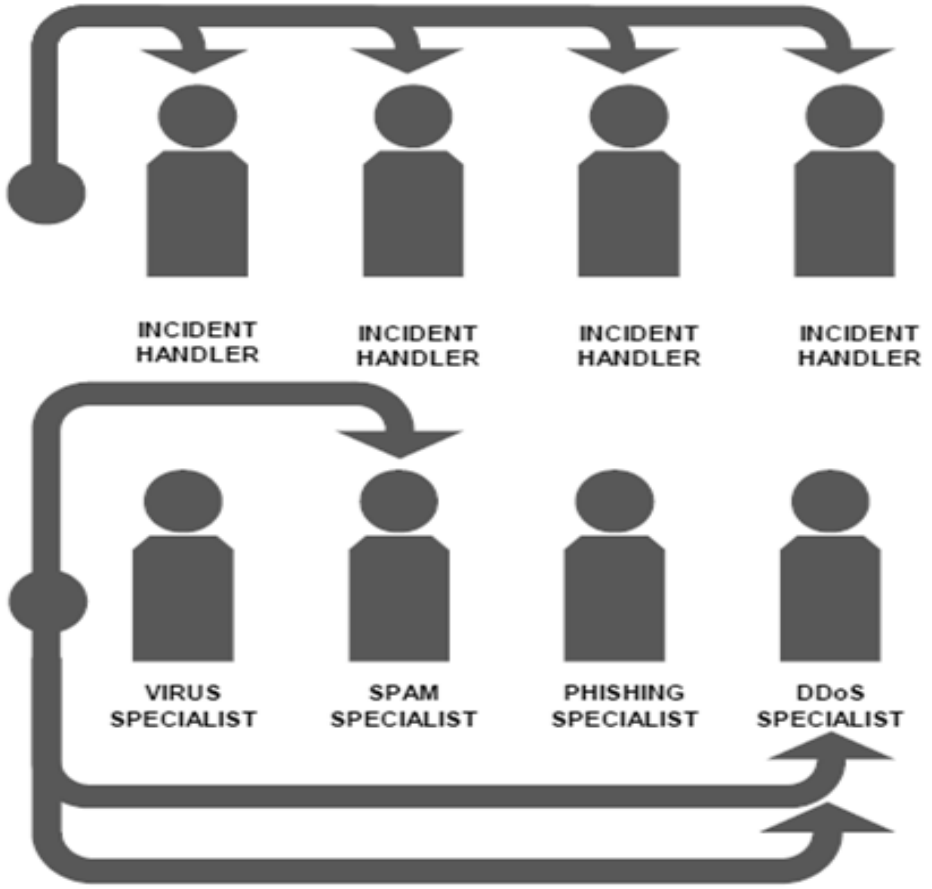
Classificar incidentes:

- Reconhecer tendências
- Extrair estatísticas
- Comparar dados
- Ver parte do panorama de ameaças

Desafios:

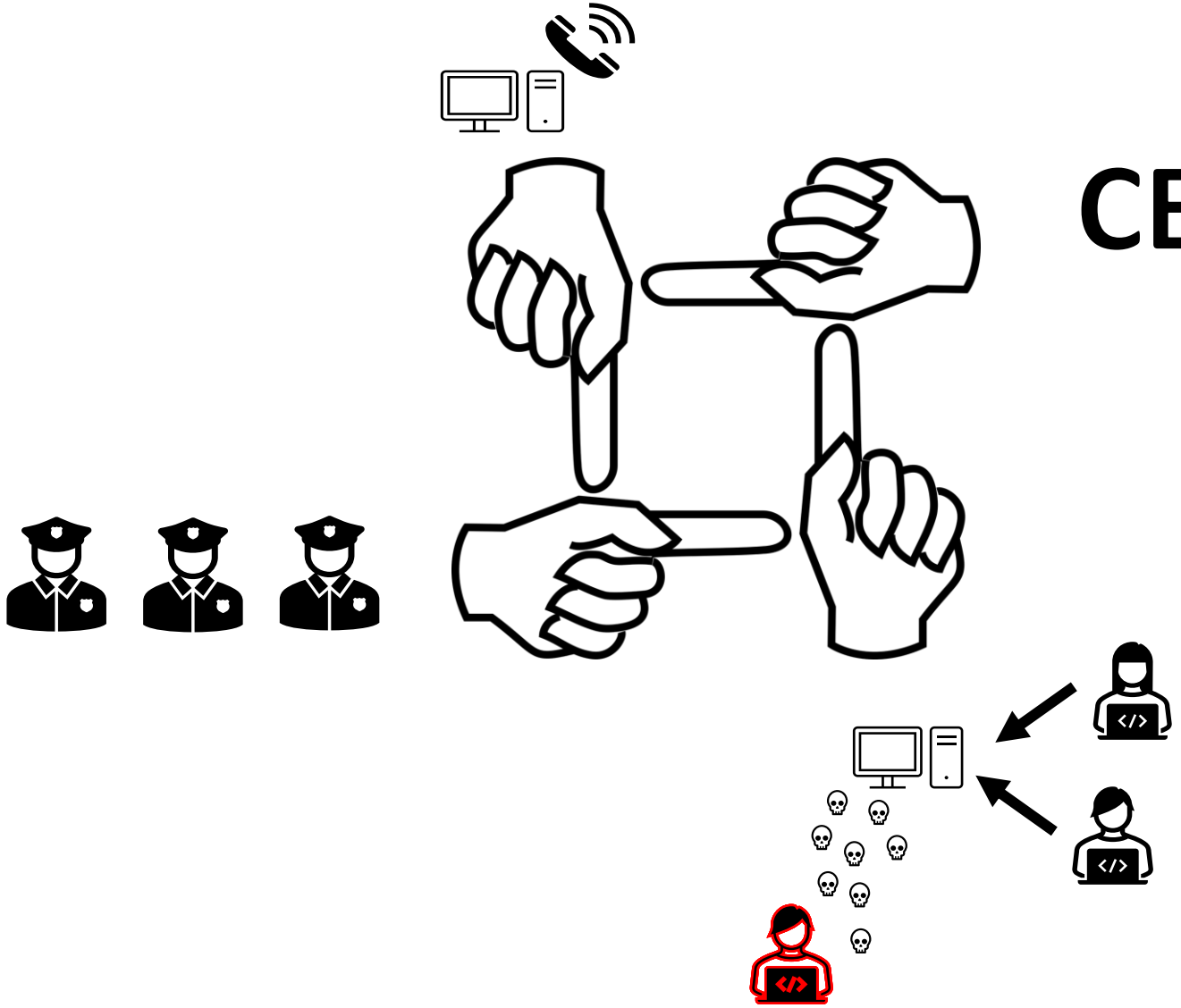
- Ambiguidades
- Perda de tempo (demasiados tipos de classificação)

TRIAGEM - ATRIBUIÇÃO



RESOLUÇÃO

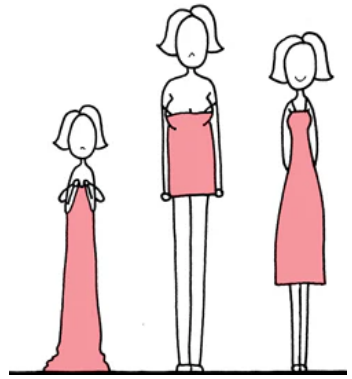
RESOLUÇÃO - COOPERAÇÃO



CERTS | CSIRTS

RESOLUÇÃO - MEDIDAS

Diferentes para diferentes intervenientes



Remediação na fonte

A influência sobre terceiros é limitada

RESOLUÇÃO - ANÁLISE

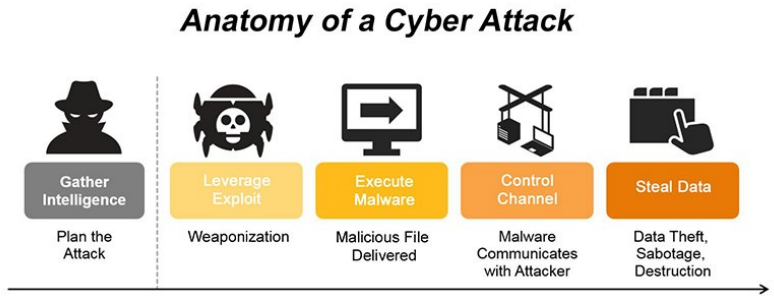
Analisadas
Discutidas
Conclusões

"Brainstorming"

Dados mais importantes
Fontes de maior confiança

RESOLUÇÃO - RECOMENDAÇÕES

Anatomia do ataque



Detalhes

Partilha

ANÁLISE POSTERIOR

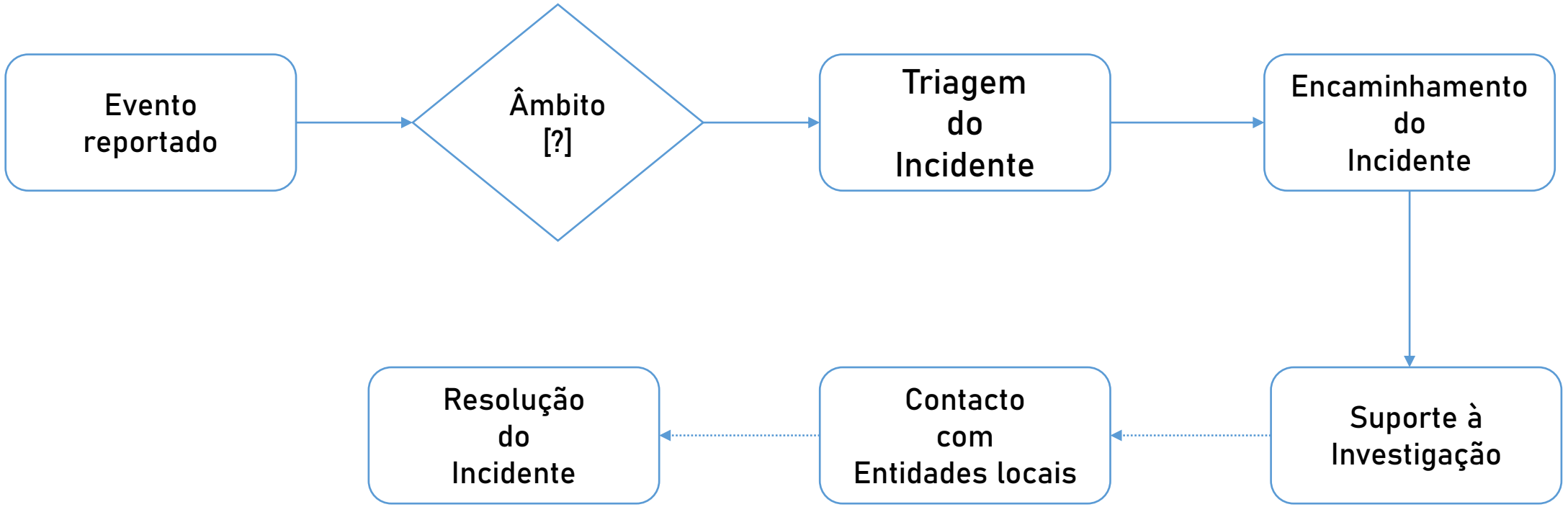
Exemplo de agenda para uma reunião pós-incidente:

a) Postmortem

b) Documentação

c) Lições extraídas
   - Lições extraídas
   - Fragilidades conhecidas
   - Propostas de melhoria

RESOLUÇÃO - WORKFLOW



EM RESUMO

- A resposta a incidentes é um fluxo processual composto por várias fases importantes.
- A utilização de uma ferramenta de registo/gestão de incidentes é essencial.
- Cada incidente deve ter uma conclusão e um rescaldo, permitindo a aprendizagem contínua.

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc