

MÓDULO: RESPOSTA A INCIDENTES

João Machado
RCTS CERT





AGENDA

Resposta a Incidentes

Notificação

Triagem

Resolução

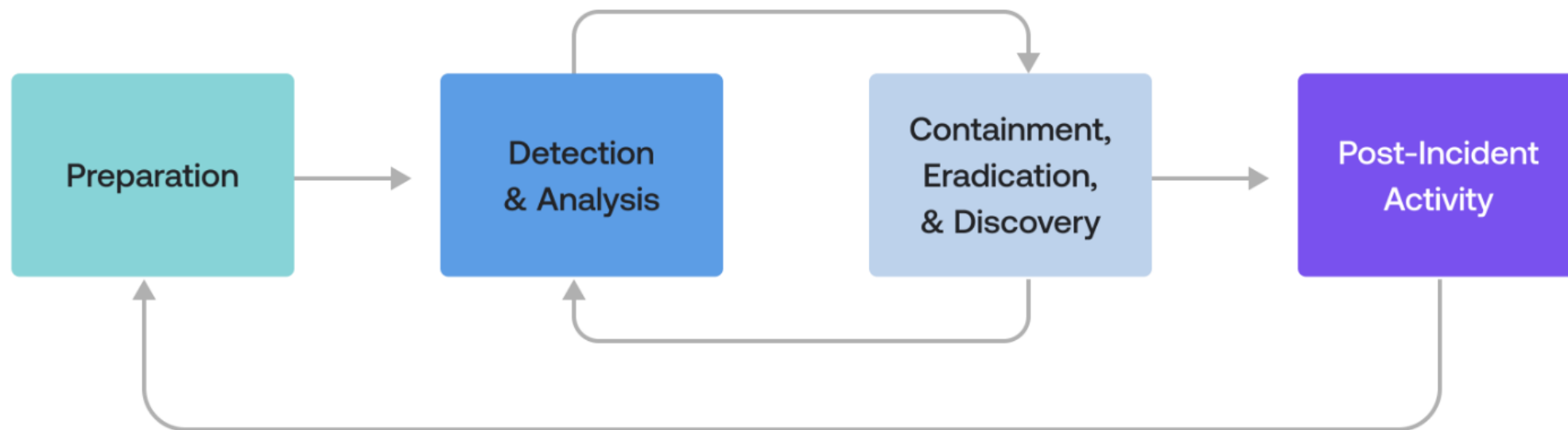
Análise Posterior



RESPOSTA A INCIDENTES



NIST Incident Response Cycle



RESPOSTA A INCIDENTES



SANS 504-B Incident Response Cycle: Cheat-Sheet

v1.0, 11.5.2016 – kf / USCW

Preparation – Identification – Containment – Eradication – Recovery – Lessons Learned (PICERL)



INCIDENTE DE SEGURANÇA



É o resultado de uma ação ou conjunto de ações que possam causar uma perda de:



CRIAÇÃO DE UM INCIDENTE DE SEGURANÇA



Denúncias de atividades maliciosas



Deteção de atividades suspeitas



Anomalias face a padrões de funcionamento

NOTIFICAÇÃO

REGISTO



Um incidente de segurança deve ser sempre registado, de forma a manter um histórico de ocorrências.

Deve ser utilizada um sistema ou ferramenta de gestão de incidentes centralizado.

Automatização quando e onde for possível e adequado.



NOTIFICAÇÃO

FERRAMENTAS



Algumas ferramentas de gestão de incidentes:



RTIR



BMC Helix ITSM



Outros...



Jira ITSM

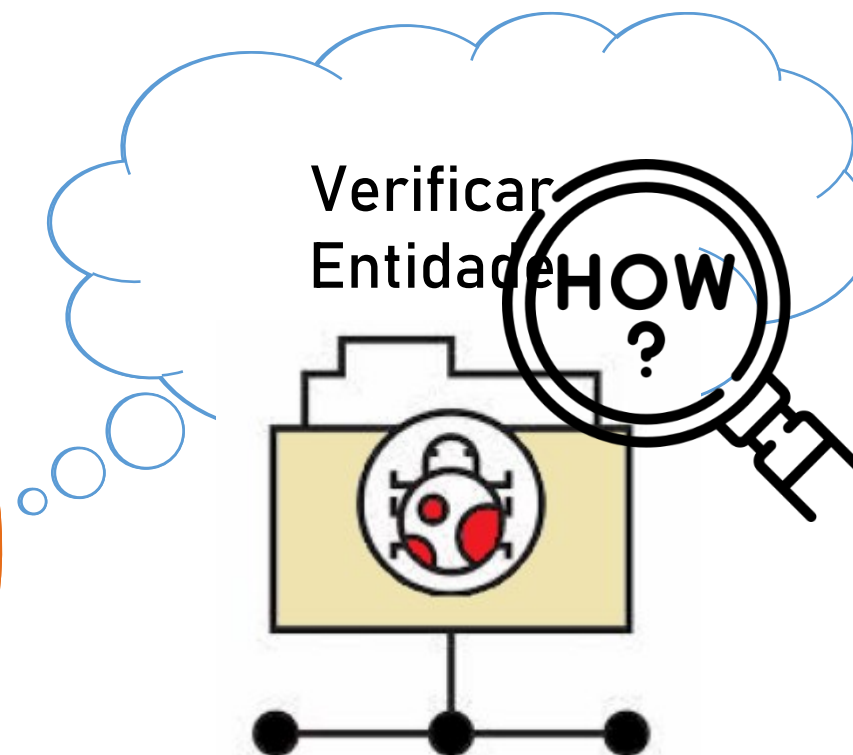
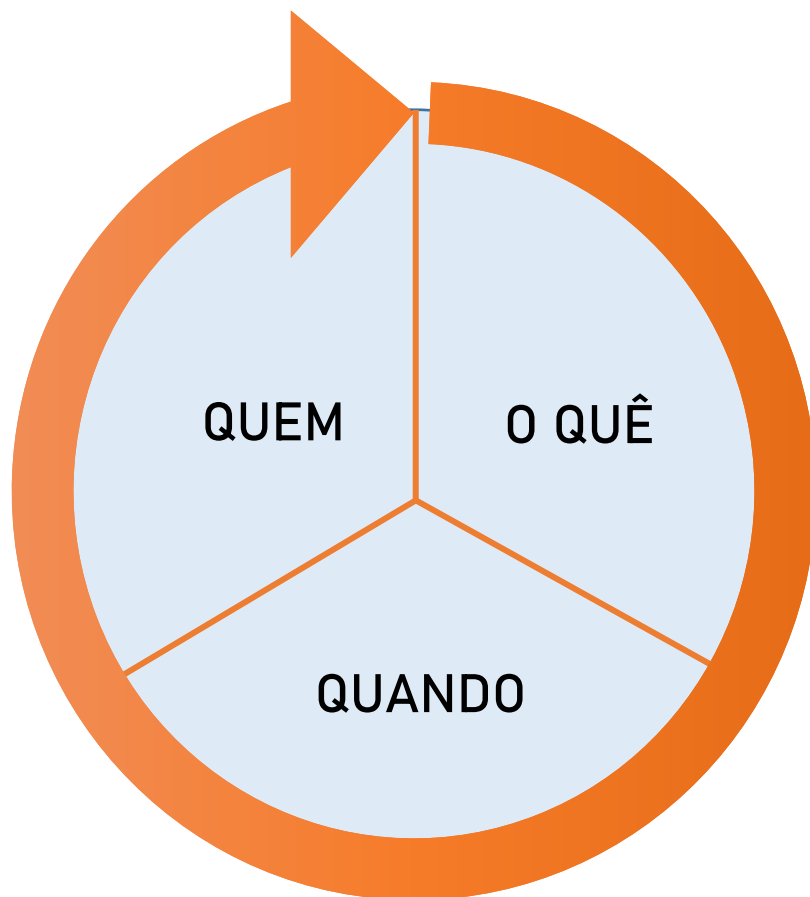


STORM OTRS

TRIAGEM



Evento
Reportado



TRIAGEM

COMO EFETUAR UMA TRIAGEM



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

CLASSIFICAÇÃO



Taxonomias mais populares nos CSIRT:

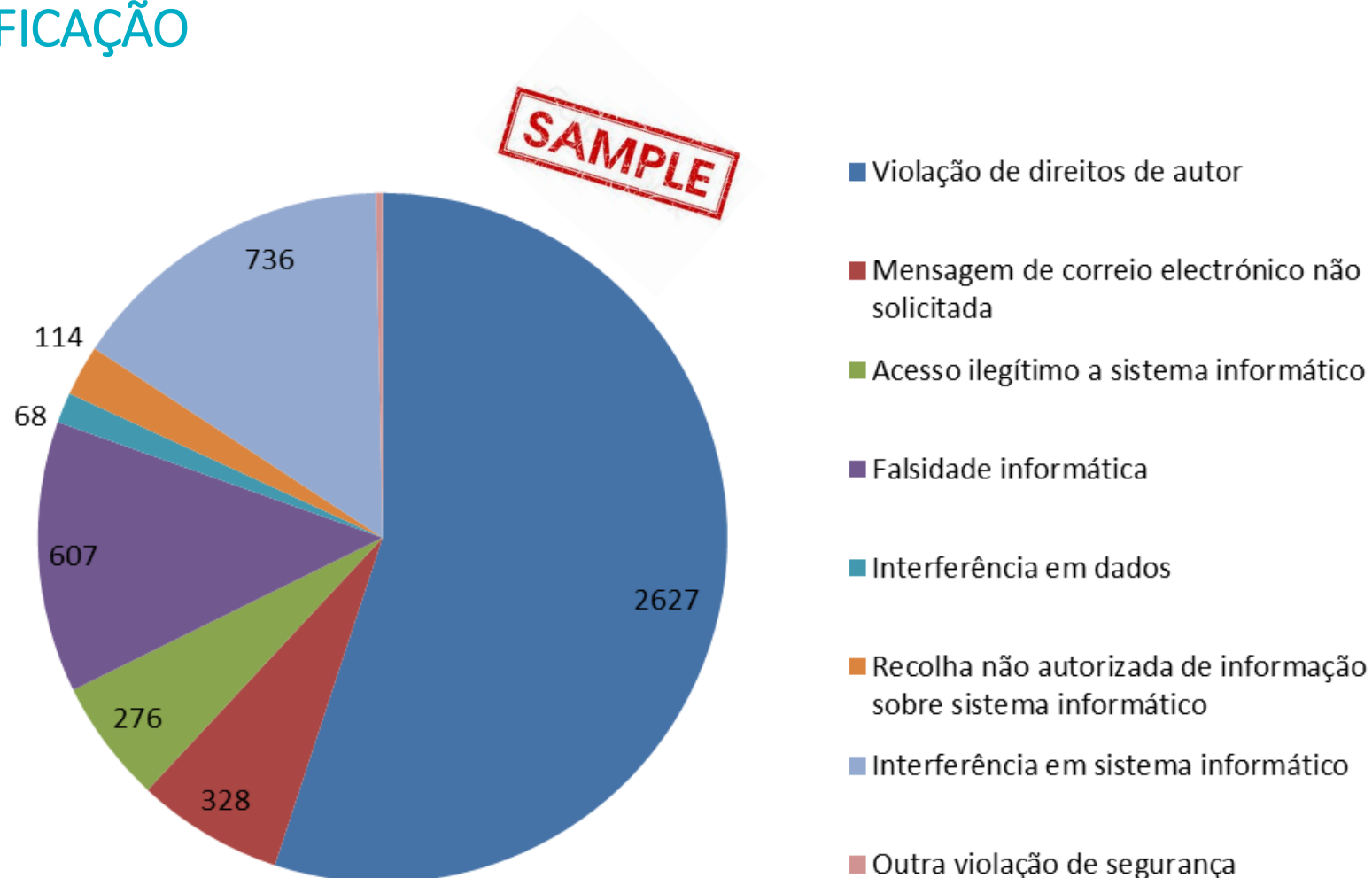
- Common language for incident response
 - By Carnegie Mellon University
- Taxonomia eCSIRT.net
 - Desenvolvida durante o projeto eCSIRT.net
- Taxonomia própria
 - Baseada em experiência

Taxonomia usada na RCTS (e RNCSIRT):

- https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf

TRIAGEM

CLASSIFICAÇÃO



TRIAGEM

CLASSIFICAÇÃO



Classificar incidentes dá-nos a capacidade de:

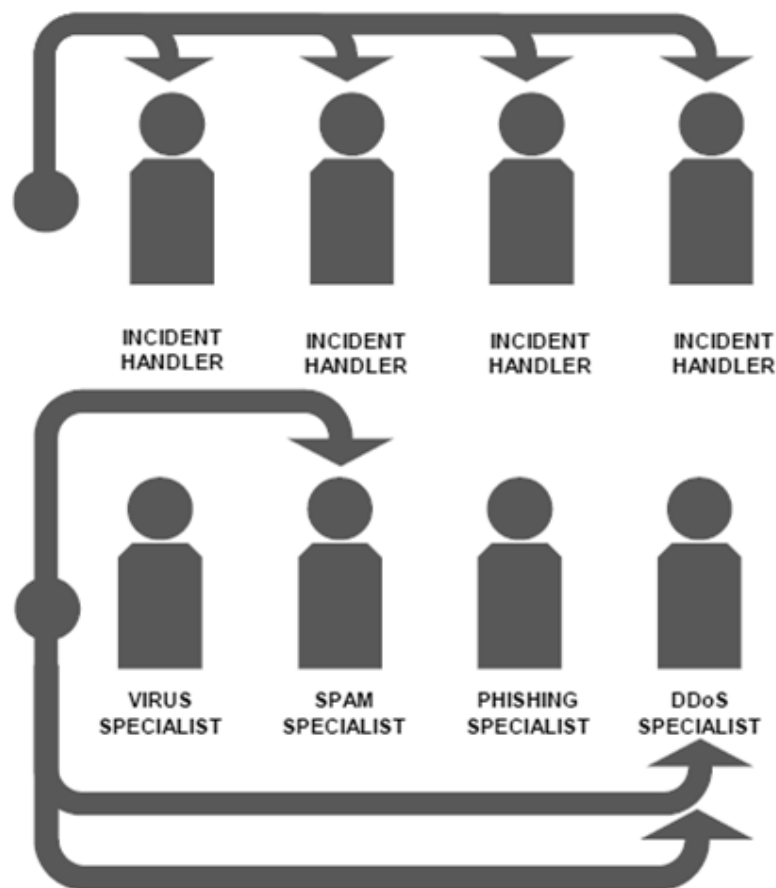
- Reconhecer tendências
- Extrair estatísticas
- Comparar dados
- Ver parte do panorama de ameaças

Desafios:

- Ambiguidades
- Perda de tempo com “sobre-classificações” (demasiados tipos de classificação)

TRIAGEM

ATRIBUIÇÃO

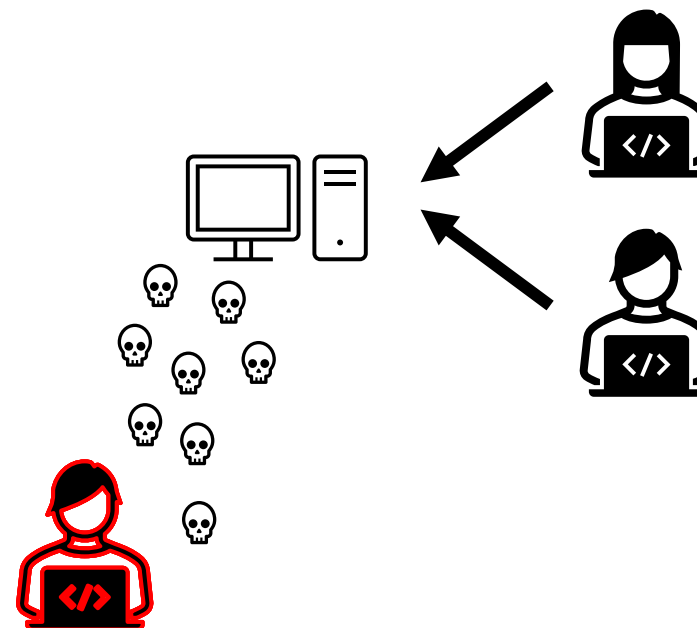
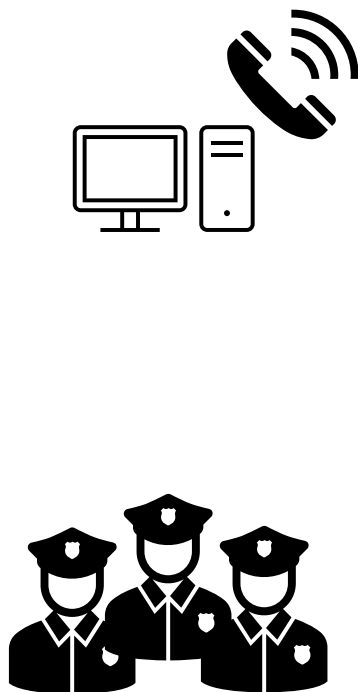


RESOLUÇÃO

COOPERAÇÃO



CERT



RESOLUÇÃO

ANÁLISE



Devem ser analisadas e discutidas as observações e conclusões da resolução do incidente.

Sessões de “brainstorming” são úteis para casos complexos e sofisticados.

Devem ser selecionados os dados que contêm a informação mais importante ou de fontes de maior confiança.



As medidas propostas podem ser diferentes para diferentes intervenientes

Podem-se propor medidas de remediação na fonte.

A influência sobre terceiros é limitada, pelo que as medidas propostas também podem ser, consoante o interveniente.

RESOLUÇÃO

RECOMENDAÇÕES



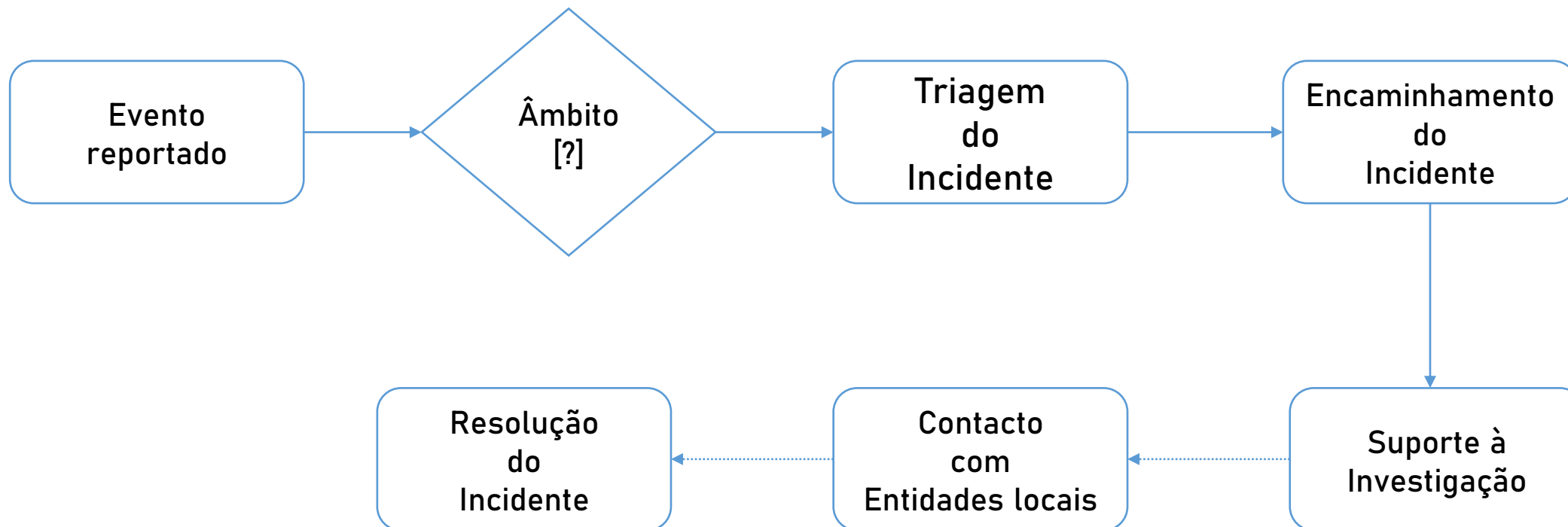
É necessário analisar a anatomia do ataque para aprender como o evitar no futuro

Deve-se tirar partido da informação sobre fragilidades, obtida através do incidente e usá-la para efetuar melhorias

Deve ser partilhada informação relevante frequentemente com a comunidade de CSIRTS

GESTÃO DE INCIDENTES

RESUMO - WORKFLOW



Exemplo de agenda para uma reunião pós-incidente:

- a) Informação estatística das últimas n semanas
- b) Curta apresentação sobre os n incidentes mais interessantes
- c) Análise detalhada de um determinado incidente
- d) Discussão:
 - Lições extraídas
 - Fragilidades conhecidas
 - Propostas de melhoria



EM RESUMO



A resposta a incidentes é um fluxo processual composto por várias fases importantes.



A utilização de uma ferramenta de gestão de incidentes é essencial.



Cada incidente deve ter uma conclusão e um rescaldo, permitindo a aprendizagem contínua.



Obrigado!