



# Reacção a Incidentes – Capacidades Mínimas

Kick Off da Rede Académica de CSIRT

**Carlos Friaças**

cfriacas@fccn.pt

2017-04-21

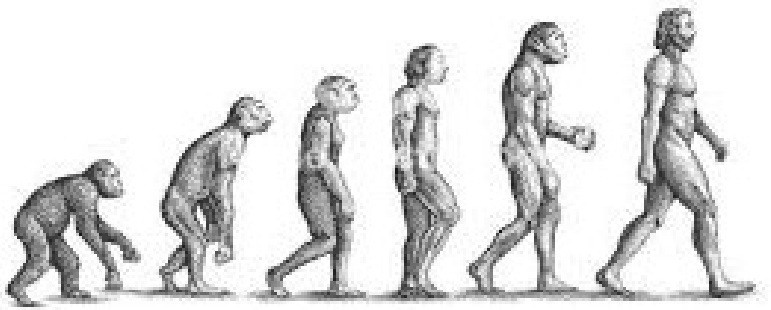
CERT RCTS

# ROADMAP PARA A CRIAÇÃO DE CAPACIDADES MÍNIMAS


https://www.cncs.gov.pt/content/files/roadmap-capacidades-minimas.pdf

# CINCO FASES

- Fase 1: Preparação
- Fase 2: Técnica
- Fase 3: Humana
- Fase 4: Processual
- Fase 5: Organizacional (opcional)



# FASE 1: PREPARAÇÃO


- Definição de ponto de contato e articulação com o CNCS a reação a incidentes de cibersegurança

- Identificação das áreas de atividade e serviços críticos/vitais, realizando gestão de ativos para as mesmas


# FASE 2: TÉCNICA

- Recolha e armazenamento de metadados de comunicações eletrónicas e outros registos necessários para a análise de incidentes

- Dispor de instrumentos técnicos, autónomos ou contratados, para mitigar os ciberataques mais comuns

# FASE 3: HUMANA

- Possuir os recursos humanos com as competências necessárias para realizar grande parte das investigações forenses, articulando com eficácia com o CNCS

# FASE 4: PROCESSUAL

- Existência de procedimentos internos (aprovados) de resposta a incidentes de cibersegurança

- Definição da estrutura e cadeia de responsabilidade, realizando periodicamente simulacros de cibersegurança

# FASE 5: ORGANIZACIONAL (OPCIONAL)


- Possuir um CSIRT
- Colaborar em projetos de desenvolvimento e partilha de informação regular dentro da comunidade nacional de CSIRT
- Participar em exercícios de cibersegurança


# AÇÕES 1/3

| Ação |
| --- |
| A 1.1 – Formalização de Protocolo de Colaboração |
| A 1.2 – Identificação de ECO e levantamento de serviços vitais |
| A 1.3 – Estabelecimento de canais de comunicação |
| A 1.4 – Procedimento de notificação de incidentes |
| A 1.5 – Registo de endereços IP no *Local Internet Registry* (*LIR*) |

| Ação |
| --- |
| A 2.1 – Inventariação de ativos |
| A 2.2 – Produção de um diagrama de rede |
| A 2.3 – Implementação de sistema de recolha e armazenamento de *flows* |
| A 2.4 – Recolha e armazenamento centralizado de registos (*logs*) |
| A 2.5 – Criação de instrumentos de correcção e mitigação de incidentes |

# AÇÕES 2/3

| Ação |
| --- |
| A 3.1 – Formação em análise de artefactos |
| A 3.2 – Formação em análise de tráfego |
| A 3.3 – Formação em resposta a incidentes |
| A 3.4 – Formação em bases legais para reação a ciberincidentes |

| Ação |
| --- |
| A 4.1 – Definição de cadeia de responsabilidade |
| A 4.2 – Definição de procedimentos de reação a incidentes |
| A 4.3 – Treino e sensibilização internos |
| A 4.4 – Realização de simulacro de cibersegurança |

# AÇÕES 3/3

| Ação |
| --- |
| A 5.1 – Definir missão, comunidade servida e portfólio de serviços |
| A 5.2 – Elaborar e fazer aprovar o plano e orçamento para o CSIRT |
| A 5.3 – Montar e anunciar o CSIRT |
| A.5.4 – Afiliação nas comunidades nacionais de CSIRT |
| A.5.5 – Participação num exercício nacional de cibersegurança |

# ENTREGÁVEIS

| |
|---|
| **Fase 1 - Preparação** |
| D 1.1 Manifestação de interesse (partilhado com o CNCS) |
| D 1.2 Estrutura de serviços vitais (partilhado com o CNCS) |
| D 1.3 Procedimento de notificação de incidentes |
| **Fase 2 - Técnica** |
| D 2.1 Inventário de ativos |
| D 2.2 Mapa de rede (Partilhado com o CNCS) |
| **Fase 4 - Processual** |
| D 4.1 Caderno de procedimentos para reação a incidentes |
| **Fase 5 - Organizacional** |
| D 5.1 RFC2350 |

# ANEXOS

- Conjunto mínimo de registos a manter
- Requisitos mínimos para os servidores

JORNADAS FCCN2017

CERT RCTS

report@cert.rcts.pt

cert.rcts.pt