



# MÓDULO: O MEU CSIRT

Carlos Friaças  
RCTS CERT





# AGENDA

O que é um CSIRT?

O que preciso para criar um CSIRT?

Como avalio a maturidade do meu CSIRT?

Atividade: RFC2350

Atividade: SIM3-CHECK

# O QUE É UM CSIRT?



**EQUIPA DE RESPOSTA A INCIDENTES DE SEGURANÇA INFORMÁTICA**  
**(FORMALIZADA)**

# O QUE É UM CSIRT?



DIFERENTES ORGANIZAÇÕES  
=  
DIFERENTES RESPONSABILIDADES

# O QUE PRECISO PARA CRIAR UM CSIRT?



ORGANIZAÇÃO

PESSOAS

FERRAMENTAS

PROCESSOS

# COMO AVALIO A MATURIDADE DO MEU CSIRT?



0: NÃO EXISTE

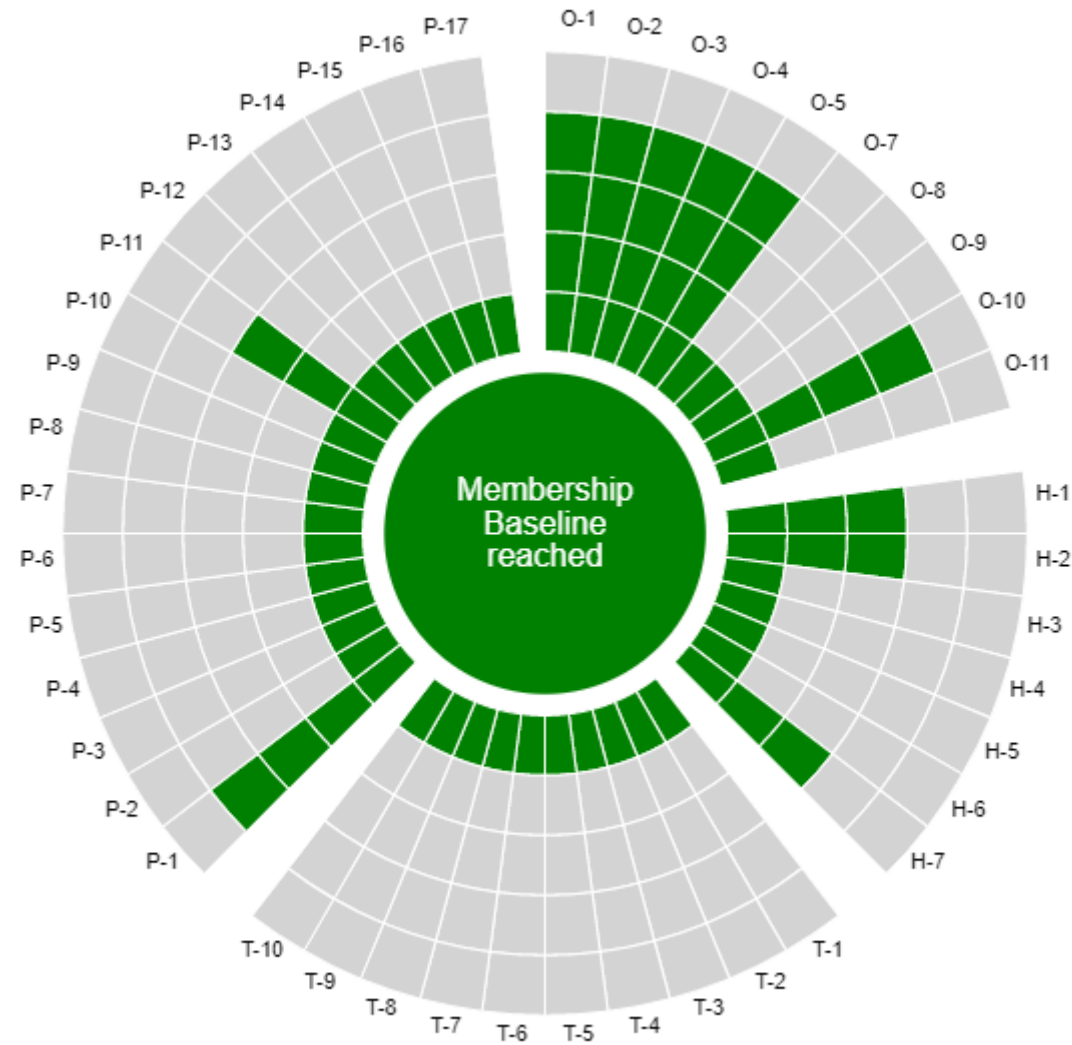
1: IMPLÍCITO

2: ESCRITO MAS NÃO FORMALIZADO

3: EXPLÍCITO & FORMALIZADO

4: AUDITADO

# COMO AVALIO A MATURIDADE DO MEU CSIRT? (EXEMPLO)



# ATIVIDADE: RFC2350



EM GRUPO

EXERCÍCIO DE DEFINIR FORMALMENTE A EQUIPA

(rfc2350-pt-Template.txt)

<https://www.cert.rcts.pt/pt/sobre/rfc2350/>



# ATIVIDADE: SIM3-CHECK



EM GRUPO (POR ORGANIZAÇÃO)

MEDIR «O QUE JÁ TEMOS»

IDENTIFICAR «O QUE PODEMOS MELHORAR»

[sim3-check.opencsirt.org](https://sim3-check.opencsirt.org)



É importante formalizar uma equipa de resposta a incidentes



Pode-se recorrer à framework SIM3 para ver onde é necessário melhorar



Obrigado!