CSIRT 101

Carlos Friaças

João Machado

RCTS CERT

Agenda

Situação Actual

Recursos

RFC2350

SIM3, TLP & PGP

Taxonomia

Serviços

Capacidades Mínimas

Situação Actual

A RAC é a Rede Académica de CSIRTs

- RCTS CERT @FCCN [RFC2350]
- CSIRT.UPorto @Universidade do Porto [RFC2350]
- CSIRT.UMINHO @Universidade do Minho [RFC2350]
- CSIRT.UTAD @UTAD [RFC2350]
- CSIRT.UBI @Universidade da Beira Interior [RFC2350]
- CSIRT.UEVORA @Universidade de Évora [RFC2350]
- CSIRT@UA @Universidade de Aveiro [RFC2350]
- CSIRT.IPB @Instituto Politécnico de Bragança [RFC2350]
- CSIRT.UALG @Universidade do Algarve [RFC2350]
- CSIRT ISCTE-IUL @ISCTE – Instituto Universitário de Lisboa [RFC2350]

Situação Actual

www.redecsirt.pt

54 membros

4 reuniões/ano

RCTS CERT

COMUNIDADE
Rede RCTS e organismos do Ministério da Educação e Ciência

DATA DE ADESÃO
21 de Janeiro de 2008

EMAIL
report@cert.rcts.pt
cert@cert.rcts.pt

CSIRT ISCTE-IUL

DATA DE ADESÃO
16 de Março de 2022

EMAIL
csirt@iscte-iul.pt

Recursos

Uma ou mais pessoas

Dedicação exclusiva vs. parcial

Diferentes capacidades, experiência e backgrounds

Ética (Código de Conduta)

RFC2350

A definição da equipa CSIRT

- Ponto de partida
- Exemplos: cert.rcts.pt/pt/rede-academica-de-csirts/

Documento «Charter»

- Como Segundo passo

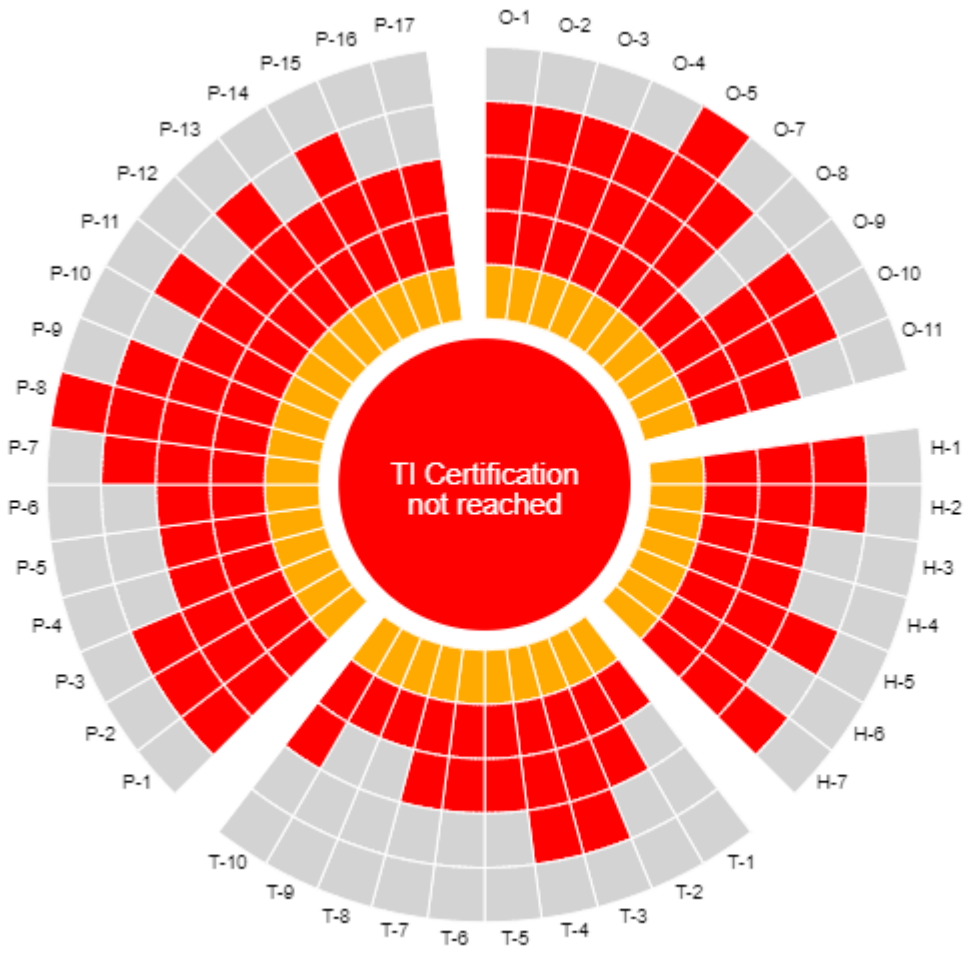
SIM3

Quatro eixos

- Organizacional
- Humano
- Ferramentas
- Processos

Ferramenta de auto-avaliação

- sim3-check.opencsirt.org



powered by OpenCSIRT SIM3-check

Open CSIRT Foundation SIM3 Self Assessment Tool

Traffic Light Protocol (TLP)

Partilha de Informação

Baseado em cores

- TLP-RED
- TLP-AMBER
- TLP-GREEN
- TLP-WHITE

www.first.org/tlp

cncs.gov.pt/pt/certpt/tlp

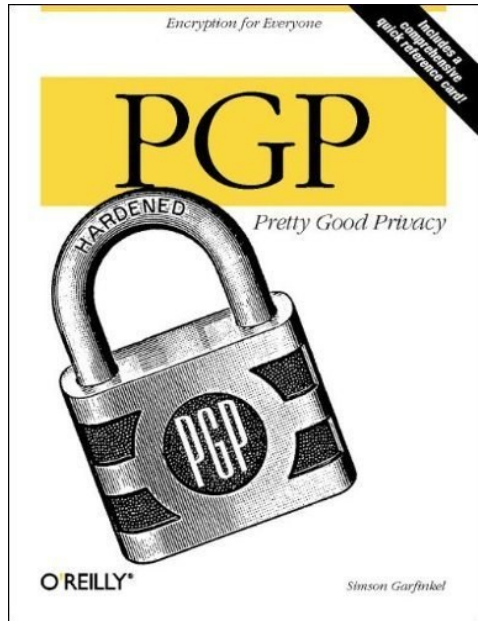
Pretty Good Privacy (PGP)

Outras alternativas também são válidas

PGP é baseado em chaves públicas e chaves privadas

Repositórios de chaves públicas

Novo membro >> Criação de novo par



Taxonomia

Classificação de Incidentes

Classe e Tipo

Comunicação inter-equipas

www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.0.pdf

Classe de Incidente *Classification*	**Tipo de Incidente** *Incident Examples*	**Descrição / Exemplos** *Description / Examples*
Conteúdo Abusivo *Abusive Content*	Spam *Spam*	Spam ou "email em massa não solicitado", significa que o destinatário não concedeu permissão verificável para o envio da mensagem e que a mensagem é enviada como parte de uma colecção maior de mensagens, todas com conteúdo funcionalmente comparável. Este IOC refere-se a recursos da infra-estrutura de SPAM, tais como verificadores e/ou colectores de endereços, URL em emails de spam, etc. *Or 'Unsolicited Bulk Email', this means that the recipient has not granted verifiable permission for the message to be sent and that the message is sent as part of a larger collection of messages, all having a functionally comparable content. This IOC refers to resources, which make up a SPAM infrastructure, be it a harvesters like address verification, URLs in spam e-mails etc.*
	Discurso Nocivo *Harmful Speech*	Individualização ou discriminação de alguém, p. ex. através de ciber perseguição, racismo ou ameaças, contra um ou mais indivíduos. *Discretization or discrimination of somebody, e.g. cyber stalking, racism or threats against one or more individuals.*
	Exploração sexual de menores, racismo e apologia da violência *(Child) Sexual Exploitation/Sexual /Violent Content*	Exploração Sexual de Menores, conteúdo sexual, glorificação da violência, e outros conteúdos proibidos por lei. *Child Sexual Exploitation (CSE), Sexual content, glorification of violence, etc.*

Serviços

Resposta a Incidentes

Segurança Preventiva (opcional)

Treino/Conscencialização de Utilizadores (opcional)

Gestão de Risco (opcional)

Auditorias (opcional)

Reacção a Incidentes: Capacidades Mínimas

www.cncs.gov.pt/pt/roadmap

Cinco graus de maturidade

Fornece listas de:

- acções
- entregáveis
- registos a manter
- requisitos para servidores

Obrigado

info@cert.rcts.pt