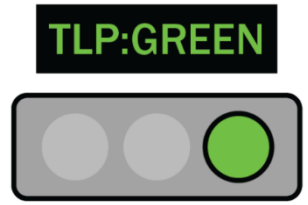


RNEP-GW

MÓDULO

RATING E SITECHECK

fct csirt

RNEP-GW

RELATÓRIOS DE CYBER SEGURANÇA

(RATING)

ÂMBITO

Porque foi criado?

O que faz?

Para quem?

LEITURAS/CATEGORIAS/PERIODICIDADE

CATEGORIA	NOME
incidentes	incidentes
vulnerabilidades	vulnerabilidades
utilização	malware
web	defacements
utilização	ids
csirt	csirt
e-mail	spf
e-mail	dkim
web	cabeçalhos
web	server sig
utilização	blacklists
dns	transferência de zona
dns	dnssec
web	ssl
vulnerabilidades	bases de dados
vulnerabilidades	acesso remoto
utilização	reputação
rpki	dns
rpki	blocos
vulnerabilidades	acesso a ficheiros
web	tls
web	robots.txt
web	security.txt
utilização	direitos autor
e-mail	dmarc

CRON	INPUT	CÁLCULO
daily	inst_id	Soma
weekly	inst_id	Soma
daily	inst_id	Soma
daily	inst_id	Soma
daily	inst_id	Soma
monthly	inst_id	Média
weekly	domain	Média
weekly	domain	Média
weekly	domain	Média
weekly	domain	Média

COMO FUNCIONA

- Leituras
  - Periodicidade
  - Categoria
- Gerar o relatório
  - Fórmula matemática
    - Leitura
      - Média ou soma
- Valor final – Rating

RELATÓRIO FINAL

RELATÓRIO DE CIBERSEGURANÇA - Junho 2025

Fundação para a Computação Científica Nacional

Rating

A

865 / 1000

Número de Incidentes:	Número de IPv4 atribuídos:	Domínio testado:
0	6136	fccn.pt

COMO LER O SCORE

A tabela do lado direito detalha a avaliação de 25 parâmetros realizada com base em diversas leituras levadas a cabo no último mês. Cada linha tem um valor avaliado e um valor máximo possível de atingir com base no peso que o CSIRT FCT atribui a cada parâmetro. Para atingir o valor máximo de 1000 pontos todos os parâmetros terão que ter leituras que reflictam configurações consideradas seguras.

Mais em: https://www.csirt.fct.pt/rating

SERVIÇOS DE SEGURANÇA SUBSCRITOS

Vulnerabilidades	Sim
DNS Firewall	Sim
Auditorias	Sim
Campanhas de Phishing	Sim
IOCaaS	Sim

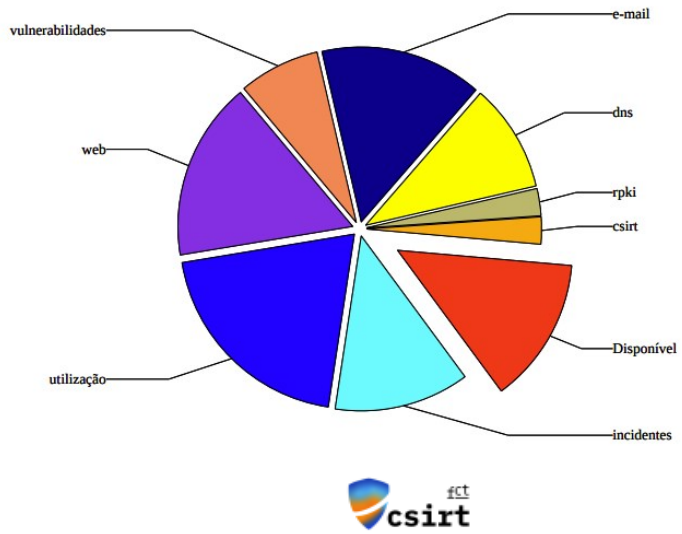
CONTACTOS DE SEGURANÇA

Carlos Friaças	cfriacas@fccn.pt
Pedro Silva	pedro.silva@fccn.pt

csirt - csirt	25 / 25
dns - transferência de zona	50 / 50
dns - dnssec	50 / 50
e-mail - spf	50 / 50
e-mail - dkim	50 / 50
e-mail - dmarc	50 / 50
incidentes - incidentes	125 / 125
rpki - dns	0 / 25
rpki - blocos	25 / 25
utilização - malware	50 / 50
utilização - ids	25 / 25
utilização - blacklists	50 / 50
utilização - reputação	50 / 50
utilização - direitos autor	25 / 25
vulnerabilidades - acesso a ficheiros	25 / 25
vulnerabilidades - vulnerabilidades	0 / 75
vulnerabilidades - bases de dados	25 / 25
vulnerabilidades - acesso remoto	25 / 25
web - defacements	25 / 25
web - robots.txt	25 / 25
web - cabeçalhos	15 / 25
web - server sig	25 / 25
web - ssl	50 / 50
web - tls	25 / 25
web - security.txt	0 / 25
Total	**865** / 1000

RELATÓRIO FINAL

Gráfico Categorias:



Disponível	135	web	165	dns	100		
incidentes	125	vulnerabilidades	75	rpki	25		
utilização	200	e-mail	150	csirt	25		

Incidentes Abertos:

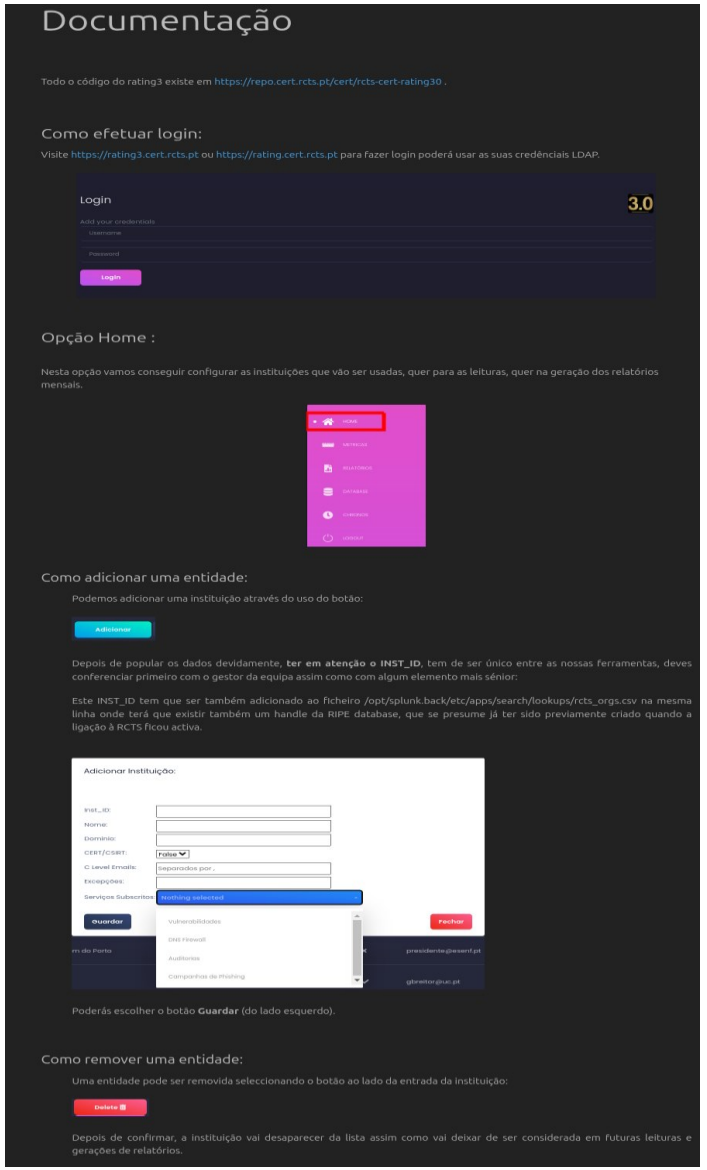
Incidentes	Data	Chave	Taxonomia
487567	2023-10-03		Vulnerable - Vulnerable system
502614	2024-09-08		Fraud - Phishing
506158	2025-01-02		Intrusion Attempts - Exploitation of known vulnerabilities
509187	2025-05-08		Intrusion Attempts - Login attempts
509513	2025-05-22		Intrusions - Unprivileged Account Compromise

DOCUMENTAÇÃO INTERNA

Técnicos

Erros

Passos



Documentação

Todo o código do rating3 existe em https://repo.cert.rcts.pt/cert/rcts-cert-rating30 .

Como efetuar login:

Visite https://rating3.cert.rcts.pt ou https://rating.cert.rcts.pt para fazer login poderá usar as suas credênciais LDAP.

Login 3.0

Opção Home :

Nesta opção vamos conseguir configurar as instituições que vão ser usadas, quer para as leituras, quer na geração dos relatórios mensais.

Como adicionar uma entidade:

Podemos adicionar uma instituição através do uso do botão:

Adicionar

Depois de popular os dados devidamente, **ter em atenção o INST_ID**, tem de ser único entre as nossas ferramentas, deves conferenciar primeiro com o gestor da equipa assim como com algum elemento mais sénior:

Este INST_ID tem que ser também adicionado ao ficheiro /opt/splunk.back/etc/apps/search/lookups/rcts_orgs.csv na mesma linha onde terá que existir também um handle da RIPE database, que se presume já ter sido previamente criado quando a ligação à RCTS ficou activa.

Adicionar Instituição:

Guardar

Fechar

Poderás escolher o botão **Guardar** (do lado esquerdo).

Como remover uma entidade:

Uma entidade pode ser removida seleccionando o botão ao lado da entrada da instituição:

Delete

Depois de confirmar, a instituição vai desaparecer da lista assim como vai deixar de ser considerada em futuras leituras e gerações de relatórios.

DOCUMENTAÇÃO

Rating CSIRT FCT

O Rating CSIRT FCT é um score mensal composto por 25 diferentes parâmetros divididos por oito categorias.

Alguns parâmetros dependem de eventos, que podem variar de mês para mês, consoante dados recolhidos de diversas fontes. Outros parâmetros dependem de configurações que podem assumir a forma considerada correcta ou segura, ou regredir para configurações inseguras (por exemplo no caso de substituição de um sistema).

Sobre estes 25 parâmetros é construído um «score» que pode variar entre 0 e 1000.

Nenhum dos componentes tem um peso inferior a 2,5% e nenhum tem um peso superior a 12,5%.

O «score» em cada mês dá origem a uma categoria, que varia de A (melhor) a F (pior), de acordo com os intervalos da figura abaixo:

A	1000 - 850	B	849 - 700
C	699 - 500	D	499 - 350
E	349 - 200	F	199 - 000

As páginas seguintes deste documento detalham a lógica de cada parâmetro.

Qualquer dúvida sobre o rating ou sobre qualquer um dos parêmetros deve ser dirigida a info@csirt.fct.pt

Categoria «DNS»

2) DNS do domínio principal – Transferência de Zona

A transferência de zona de um domínio DNS é algo que deve estar sempre limitada, uma vez que estando publicamente disponível representará um valioso contributo para qualquer acção de reconhecimento que mais tarde vise o ataque a uma instituição.

Fórmula de cálculo

Se a transferência de zona do domínio principal da instituição estiver inibida serão atribuídos 50 pontos (5% do valor do rating). Se a transferência de zona for permitida serão atribuídos 0 pontos.

O que fazer?

Na configuração de todos os servidores DNS autoritativos para o seu domínio deve estar inibida a transferência de zona. A transferência de zona só deve ser permitida no servidor primário (SOA – Start of Authority) para o servidores secundários (listados nos registos NS do próprio domínio).

SITECHECK

MOTIVAÇÃO

Entender

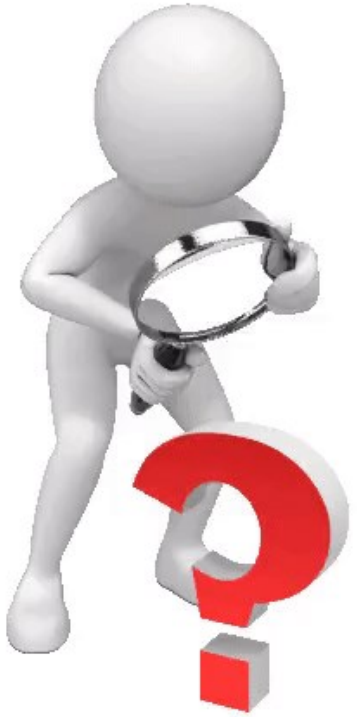
Simples

Ajuda a Proteger

Ajuda a Detetar

Vetores de Ataque

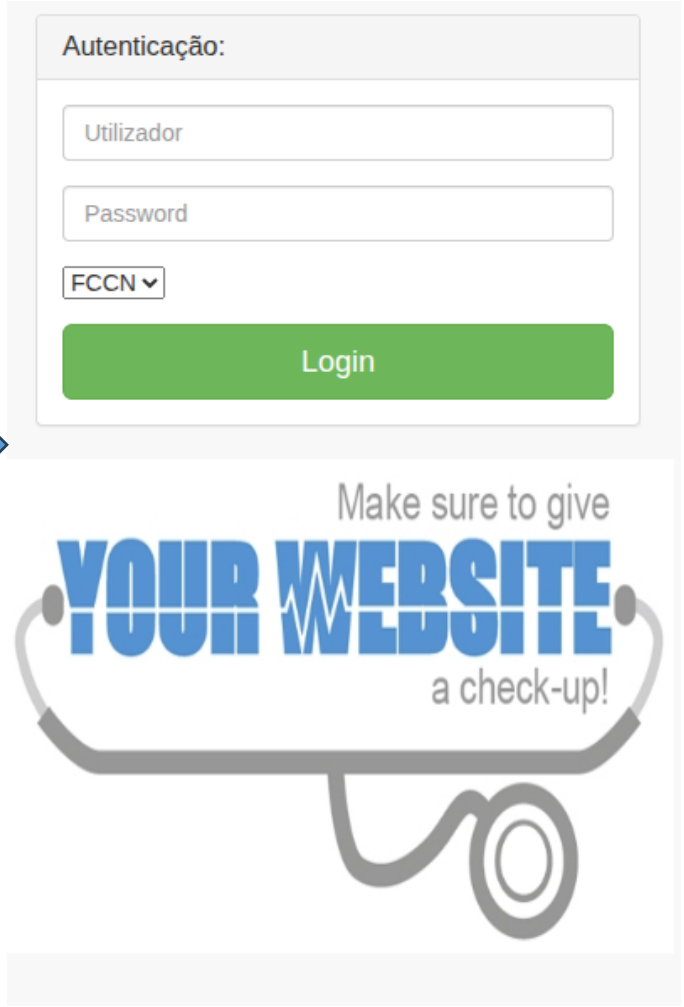
Configurações



COMO ACEDER

https://sitecheck.cert.rcts.pt

https://sitecheck.csirt.fct.pt



GESTÃO DOS URLS

ID	Area	Nome	URL	Admins	Internet NL	Page Speed PC	Page Speed TELM	SSL LABS IPv4	SSL LABS IPv6	X-Frame-Options	X-Content-Type-Options	Content-Security-Policy	Referrer-Policy	SPF	DMARC	DKIM	Data	Check
mskVSMcDPP	ASR	MANAGE RCTSaai	manage.rctsaai.pt	[redacted]	40%	94%	80%	A+	no ipv6	✓	✓	✓	✓	✗	✓	✓	15-07-2025 07:02:52	Re-Check
UJWR8W9Pc5	ASR	PDP RCTSaai	pdp.rctsaai.pt	[redacted]	40%	94%	77%	A+	no ipv6	✓	✓	✓	✓	✗	✓	✓	15-07-2025 07:02:54	Re-Check

https://internet.nl

https://pagespeed.web.dev

https://www.ssllabs.com

Headers

Email

...

CONFIGURAÇÕES

ecommerce.nau.edu.pt

course-certificate.nau.edu.pt

studio.nau.edu.pt

help.myfct.fct.pt

Submit

FAQ

Que significa Internet NL? +

Que significa Page Speed PC? +

Que significa Page Speed TELM? +

Que significa SSL LABS IPv4? +

Que significa SSL LABS IPv6? +

Que significa X-Frame-Options? +

Que significa X-Content-Type-Options? +

Que significa Content-Security-Policy? +

Que significa Referrer-Policy? +

Que significa SPF? +

Que significa DMARC? +

Que significa DKIM? +

Que significa Re-Check? +

FUNCIONAMENTO

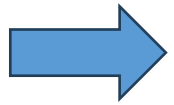
Domingo

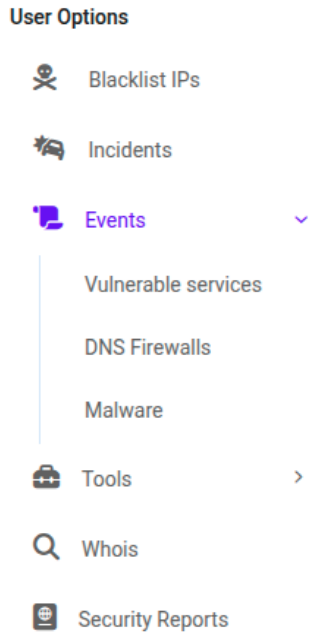
Gestores

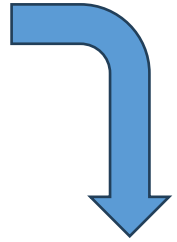
Não é uma Auditoria

info@csirt.fct.pt

SECURITY PORTAL







Done.

Vulnerable Services

Number of hours to search:

72 Search...

CSV Excel Column visibility

Search:

Source Time	Observation Time	Feed Name	Source IP	Accuracy	Identifier
2025-07-08T05:39:17+00:00	2025-07-09T07:36:27+00:00	SSL-POODLE-Vulnerable-Servers	193.137.59.114	100	ssl-poodle
2025-07-08T11:33:38+00:00	2025-07-09T07:34:59+00:00	Open-Portmapper	193.136.60.60	100	open-portmapper
2025-07-08T18:14:41+00:00	2025-07-09T06:32:22+00:00	Accessible-FTP	193.136.60.131	100	accessible-ftp
2025-07-09T20:31:04+00:00	2025-07-10T05:21:51+00:00	Open-Portmapper	193.136.60.50	100	open-portmapper

Showing 1 to 4 of 4 entries

Previous 1 Next

IDEIAS CHAVE

- O sistema de rating integrado em relatórios mensais dá uma ideia da evolução global da cibersegurança de uma organização
- Existem diversas alternativas comerciais para uma avaliação 360º da cibersegurança de uma organização
- Sitecheck foi uma ferramenta desenvolvida internamente para avaliar sites próprios de forma automatizada

Questões?

Obrigado.

csirt.fct.pt/podcast

csirt.fct.pt/mooc

csirt.fct.pt/etc