

MÓDULO: COORDENAÇÃO E COLABORAÇÃO

Carlos Friaças
RCTS CERT





AGENDA



Whois

Traffic Light Protocol (TLP)

WHOIS



WHOIS



WHOIS é o protocolo usado para determinar a quem pertence um determinado recurso

Os Regional Internet Registries são a fonte autoritativa (AFRINIC, APNIC, ARIN, LACNIC, RIPENCC) para os blocos/endereços IP

Existem portanto 5 fontes autoritativas, com campos diferentes

WHOIS



Contacto de abuse não é uniforme nos 5 Regional Internet Registries

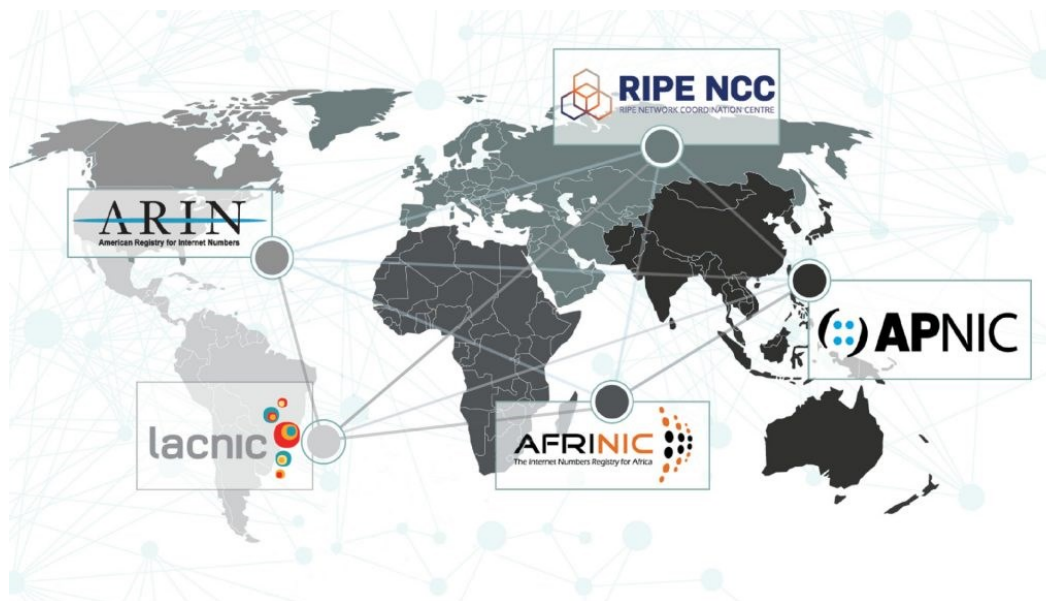
Servidores WHOIS: `whois.<afrinic|apnic|arin|lacnic|ripe>.net`

`whois <ip>`

`whois <bloco/máscara>`

`whois <asn>`

`whois <...>`



WHOIS (PESQUISAS HISTÓRICAS)

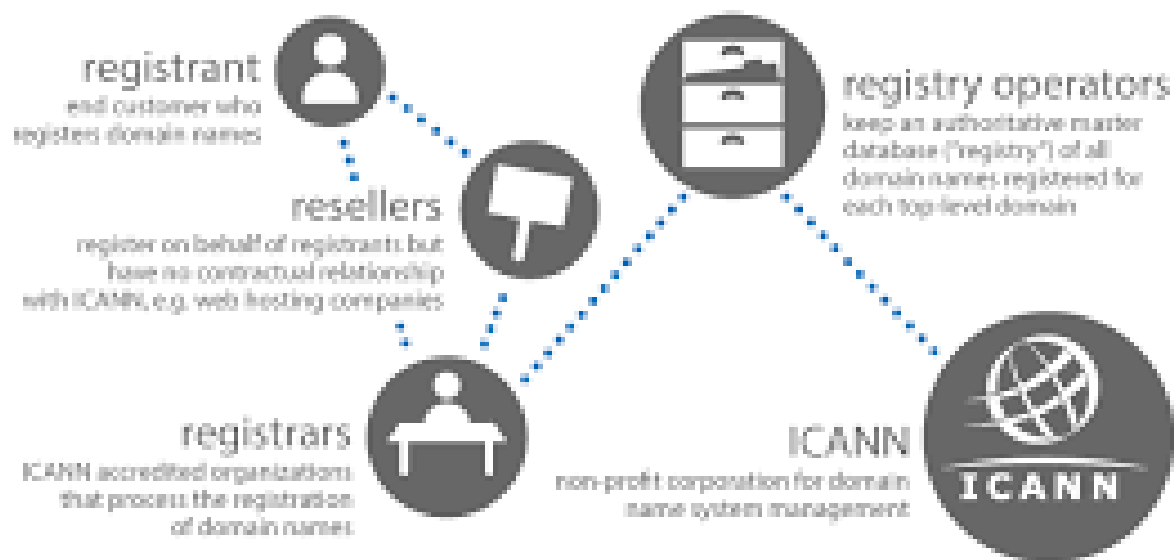


`whois <...> --list-versions`

`whois <...> --show-version <#>`



WHOIS: DOMÍNIOS



domain registry process

O protocolo também é usado para registo de domínios

A opacidade da informação disponível publicamente aumenta

TRAFFIC LIGHT PROTOCOL (TLP)



PROTOCOLO DE CLASSIFICAÇÃO DE INFORMAÇÃO



Versão 2.0

Actualizado em Agosto de 2022

Existe um SIG (Special Interest Group)
que o desenvolve e actualiza



DEFINIÇÕES DO TLP



TLP:RED	Para conhecimento estrito dos recipientes individuais, informação não deve ser partilhada.
TLP:AMBER TLP:AMBER+STRICT	Os recipientes da informação podem partilhar a informação apenas com membros da própria organização e clientes. Se a informação for restrita apenas a membros da própria organização, o TLP:AMBER+STRICT deve ser usado.
TLP:GREEN	Partilha limitada, recipientes podem partilhar a informação dentro da sua comunidade. Informação pode ser partilhada com colegas e organizações parceiras dentro da sua comunidade, mas não por canais publicamente acessíveis.
TLP:CLEAR	Não existem restrições para a divulgação da informação.



É possível ir à fonte autoritativa para determinar a quem pertence um determinado IP/bloco



Quando se partilha informação é importante classificá-la para que quem a recebe saiba a quem a pode redistribuir



Obrigado!