Recursos de Internet

¿Qué son los recursos de Internet? ¿Cómo encontrar quien lo tiene asignado?

Recursos de Internet

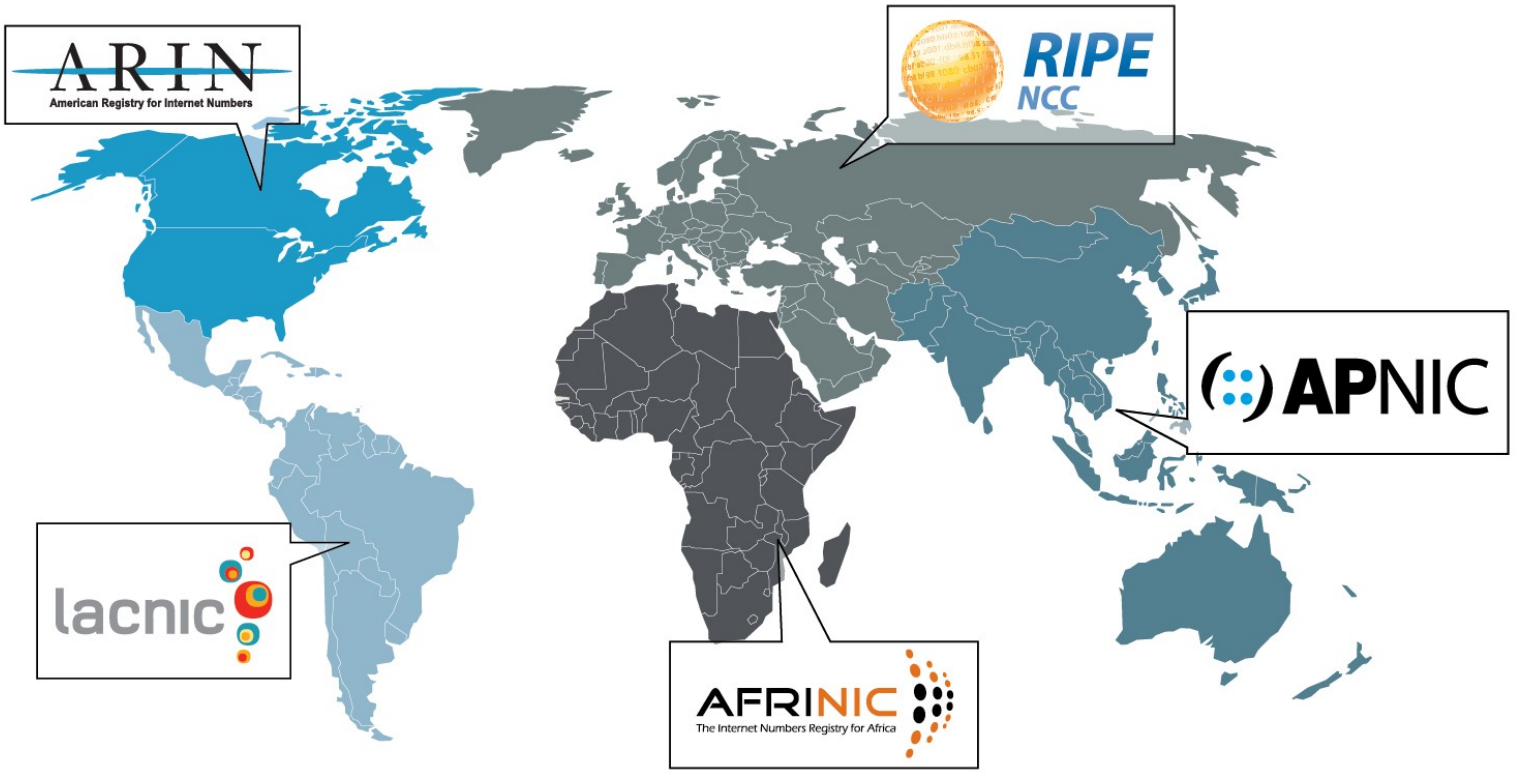
- **Direcciones IP**
  - **IPv4**
  - **IPv6**
- Nombres de dominio

Asignación de direcciones IP

- Los RIRs o Registros Regionales de Internet, son quienes asignan bloques IP a las organicaciones que los requieran.
- Durante el proceso de asignación, la organización que solicita los bloques de Internet, debe completar cierta información de contacto.
- Con esta información, cada RIR, mantiene una base de datos de acceso público sobre los recursos asignados.

Registros Regionales

- Las organizaciones que requieren bloques IP, deben solicitarlo al RIR que opera en la región en la que la organización se encuentra.



Registros Regionales

- American Registry for Internet Numbers (**ARIN**): Canadá, partes del Caribe e islas del Atlántico Norte – http://www.arin.net/
- Asia Pacific Network Information Centre (**APNIC**): Partes de Asia y Regiones de Oceanía – http://www.apnic.net/
- Latin American and Caribbean Internet Addresses Registry (**LACNIC**): América Latina y las regiones del Caribe – http://lacnic.net/
- Réseaux IP Européens (**RIPE**): Europa, Oriente Medio y Asia Central - http://www.ripe.net/
- África Regional Internet Registry (**AFRINIC**): África y algunas regiones del océano Índico - http://www.afrinic.net/

Información sobre recursos asignados

- Cada RIR, mantiene una base de datos de acceso público sobre los recursos IP asignados.
- Para acceder a éstos datos se utilizan dos protocolos de consulta:
  - WHOIS
  - RDAP (Registration Data Access Protocol)

WHOIS vs RDAP

- WHOIS es la base de datos historicamente usada:
  - La información no respeta ningún formato. Texto libre.
  - Complica extraer información de manera automática

- RDAP es el sucesor del protocolo WHOIS:
  - Los datos respetan un formato determinado
  - Adecuado para tareas de procesamiento automático

Información sobre recursos asignados (cont)

Dada una dirección IP, se puede consultar en WHOIS o en RDAP para obtener:

- Bloque IP completo asignado
- Información sobre el poseedor del bloque
  - Nombre, teléfono, dirección postal
- Datos de Contacto:
  - Contacto administrativo
  - Contacto técnico
  - Contacto por incidentes de seguridad

Consulta whois

```
:~$ whois 190.15.133.5
% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2020-09-23 10:33:47 (-03 -03:00)

inetnum:     190.15.128.0/20
status:      allocated
aut-num:     N/A
owner:       CEDIA
ownerid:     EC-CEDI-LACNIC
responsible: NEG redCEDIA
address:     Gonzalo Cordero 2-122 y J. Fajardo, 2-122, Edificio CEDIA
address:     010203 - Cuenca - AZ
country:     EC
phone:       +593  74079300 [400]
owner-c:     CHA2
tech-c:      CHA2
abuse-c:     SCN3
inetrev:     190.15.138.0/24
nserver:     DNS.CEDIA.ORG.EC
nsstat:      20200922 AA
nslastaa:    20200922
inetrev:     190.15.128.0/24
nserver:     DNS.CEDIA.ORG.EC
nsstat:      20200922 AA
nslastaa:    20200922
inetrev:     190.15.137.0/24
```

En verde el comando utilizado.

En violeta, la información del RIR que realizó la asignación del bloque IP en el que se encuentra la dirección IP consultada.

En rojo, información sobre la entidad que tiene asignado el bloque IP en el que se encuentra la dirección IP consultada

Problemas de whois

Algunos temas que se deben considerar cuando se usa WHOIS:

- Los datos no respetan ningún formato. La información buscada, podría:
  - No estar
  - Estar en un comentario (lineas que empiezan con %)
- En un principio la IANA hacia la asignación de recursos. Los RIR fueron posteriores. Esto podría provocar situaciones como la de la UNLP:
  - whois 163.10.5.66

Problemas de whois

```
nico@nico-PORTEGE-Z30-B:~$ whois 163.14.2.2
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '163.13.0.0 - 163.28.255.255'

% Abuse contact for '163.13.0.0 - 163.28.255.255' is 'hostmaster@twnic.net.tw'

inetnum:        163.13.0.0 - 163.28.255.255
netname:        TANET-B
descr:          imported inetnum object for MOEC
country:        TW
admin-c:        TA61-AP
tech-c:         TA61-AP
status:         ALLOCATED PORTABLE
mnt-by:         MAINT-TW-TWNIC
mnt-irt:        IRT-TWNIC-AP
last-modified:  2013-11-27T09:08:01Z
source:         APNIC

irt:            IRT-TWNIC-AP
address:        Taipei, Taiwan, 100
e-mail:         hostmaster@twnic.net.tw
abuse-mailbox:  hostmaster@twnic.net.tw
admin-c:        TWA2-AP
tech-c:         TWA2-AP
auth:           # Filtered
remarks:        Please note that TWNIC is not an ISP and is not empowered
remarks:        to investigate complaints of network abuse.
mnt-by:         MAINT-TW-TWNIC
last-modified:  2015-10-08T07:58:24Z
source:         APNIC
```

Problemas de whois

```
nico@portege-z30-b:~$ whois 163.10.5.66
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '163.0.0.0 - 163.255.255.255'

% Abuse contact for '163.0.0.0 - 163.255.255.255' is 'helpdesk@apnic.net'

inetnum:        163.0.0.0 - 163.255.255.255
netname:        ERX-NETBLOCK
descr:          Early registration addresses
remarks:        ----------------------------------------------------
remarks:        Important:
remarks:
remarks:        Networks in this range were allocated by InterNIC
remarks:        prior to the formation of Regional Internet
remarks:        Registries (RIRs): AfriNIC, APNIC, ARIN, LACNIC and RIPE NCC.
remarks:
remarks:        Address ranges from this historical space have now
remarks:        been transferred to the appropriate RIR database.remarks:
remarks:        If your search has returned this record, it means the
remarks:        address range is not administered by APNIC.
remarks:
remarks:        Instead, please search one of the following databases:
remarks:
remarks:        - AfriNIC (Africa)
remarks:        website: http://www.afrinic.net/
remarks:        command line: whois.afrinic.net
remarks:
remarks:        - ARIN (Northern America)
remarks:        website: http://www.arin.net/
remarks:        command line: whois.arin.net
remarks:
remarks:        - LACNIC (Latin America and the Carribean)
remarks:        website: http://www.lacnic.net/
remarks:        command line: whois.lacnic.net
remarks:
remarks:        - RIPE NCC (Europe)
remarks:        website: http://www.ripe.net/
remarks:        command line: whois.ripe.net
remarks:
remarks:        For information on the Early Registration Transfer
```

1

```
remarks:        http://www.apnic.net/db/erx
remarks:
remarks:        ----------------------------------------------------
country:        AU
admin-c:        IANA1-AP
tech-c:         IANA1-AP
mnt-by:         APNIC-HM
mnt-lower:      APNIC-HM
status:         ALLOCATED PORTABLE
last-modified:  2015-08-28T00:31:35Z
source:         APNIC
mnt-irt:        IRT-APNIC-AP

irt:            IRT-APNIC-AP
address:        Brisbane, Australia
e-mail:         helpdesk@apnic.net
abuse-mailbox:  helpdesk@apnic.net
admin-c:        HM20-AP
tech-c:         NO4-AP
auth:           # Filtered
remarks:        APNIC is a Regional Internet Registry.
remarks:        We do not operate the referring network and
remarks:        are unable to investigate complaints of network abuse.
remarks:        For information about IRT, see www.apnic.net/irt
remarks:        helpdesk@apnic.net was validated on 2020-02-03
mnt-by:         APNIC-HM
last-modified:  2020-02-03T02:04:33Z
source:         APNIC

role:           Internet Assigned Numbers Authority
address:        see http://www.iana.org.
admin-c:        IANA1-AP
tech-c:         IANA1-AP
nic-hdl:        IANA1-AP
remarks:        For more information on IANA services
remarks:        go to IANA web site at http://www.iana.org.
mnt-by:         MAINT-APNIC-AP
last-modified:  2018-06-22T22:34:30Z
source:         APNIC

% This query was served by the APNIC Whois Service version 1.88.15-SNAPSHOT (WHOIS-US4)
```

2

Problemas de whois

```
nico@portege-z30-b:~$ whois 163.10.5.66 -h whois.lacnic.net

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2020-09-30 12:17:18 (-03 -03:00)

inetnum:     163.10.0.0/16
status:      assigned
aut-num:     N/A
owner:       Universidad Nacional de La Plata
ownerid:     AR-UNLP-LACNIC
responsible: Javier Diaz
address:     1900, 50, 115
address:     1900 - La Plata - BA
country:     AR
phone:       +54 221 4236609 [115]
owner-c:     ANB10
tech-c:      ANB10
abuse-c:     CEU
inetrev:     163.10.0.0/16
nserver:     UNLP.UNLP.EDU.AR
nsstat:      20200929 AA
nslastaa:    20200929
nserver:     ANUBIS.UNLP.EDU.AR
nsstat:      20200929 AA
nslastaa:    20200929
created:     19920701
changed:     20100319

nic-hdl:     ANB10
person:      CeSPI UNLP
e-mail:      noc@cespi.unlp.edu.ar
address:     Calle 50 y 115, S/N, 3er. piso
address:     1900 - La Plata - BA
country:     AR
phone:       +54 221 4236609 [1101]
created:     20081104
changed:     20150422

nic-hdl:     CEU
person:      Cert Unlp
e-mail:      abuse@unlp.edu.ar
address:     50 y 115
```

El comando utilizado incluye el servidor WHOIS al que se quiere realizar la consulta

En el recuadro violeta, la información del RIR que realizó la asignación del bloque IP en el que se encuentra la dirección IP consultada.

En el recuadro rojo, información sobre la entidad que tiene asignado el bloque IP en el que se encuentra la dirección IP consultada

Cliente RDAP

- A diferencia de whois, no viene un cliente nativo en los paquetes del sistema

- **nicinfo** es un cliente RDAP realizado por ARIN (American Registry for Internet Numbers)
  https://www.arin.net/resources/registry/whois/rdap/

  Se puede instalar en la VM dada con:

```
sudo apt install ruby
sudo gem update
sudo gem install nicinfo
```

Consulta RDAP

```
nico@portege-z30-b:~$ nicinfo -Q 190.15.133.5
Invalid gemspec in [/usr/share/rubygems-integration/all/specifications/rbnacl-libsodium-1.0.16.gemspec]: invalid date format in specification: "1980-01-02 00:00:00.000000000 Z"
[ NOTICE ] Terms and Conditions
        1 This is the LACNIC RDAP service. Objects are in RDAP format.
      TOS http://www.lacnic.net/web/lacnic/registration-data-access-protocol

[ RESPONSE DATA ]
 1= 190.15.128.0/20
    |--- 1= CEDIA ( EC-CEDI-LACNIC )
    |--- 2= NEG CEDIA ( CHA2 )
    `--- 3= Security CEDIA NREN ( SCN3 )

         [ IP NETWORK ]
                Handle:  190.15.128.0/20
       Object Class Name:  ip network
           Start Address:  190.15.128.0
             End Address:  190.15.143.255
                   CIDRs:  190.15.128.0/20
              IP Version:  v4
                    Type:  allocated
            Registration:  Wed, 19 Jul 2006 12:00:00 -0000
            Last Changed:  Thu, 24 May 2012 03:28:45 -0000
                 Remarks:  -- remarks --
                   Links:  -- for 190.15.128.0/20 --
               Reference:  https://rdap.lacnic.net/rdap/ip/190.15.128.0/20

           [ ENTITY ]
                Handle:  EC-CEDI-LACNIC
       Object Class Name:  entity
             Common Name:  CEDIA
                   Phone:  593  74079300#400 ( voice )
                   Roles:  Registrant
            Registration:  Mon, 10 Apr 2006 12:00:00 -0000
            Last Changed:  Mon, 27 Jul 2020 22:56:53 -0000
                 Address:  -- for CEDIA ( EC-CEDI-LACNIC ) --
              Apt/Suite:  Edificio CEDIA
                  Street:  Gonzalo Cordero 2-122 y J. Fajardo
                    City:  Cuenca
             Postal Code:  010203
                 Country:  EC
                    Kind:  org
                   Links:  -- for CEDIA ( EC-CEDI-LACNIC ) --
               Reference:  https://rdap.lacnic.net/rdap/entity/EC-CEDI-LACNIC
```

En el recuadro verde, el comando utilizado.

En el recuadro violeta, la información del RIR que realizó la asignación del bloque IP en el que se encuentra la dirección IP consultada.

En el recuadro rojo, información sobre la entidad que tiene asignado el bloque IP en el que se encuentra la dirección IP consultada.

RDAP vs WHOIS

```
nico@portege-z30-b:~$ nicinfo -Q 163.10.5.66
Invalid gemspec in [/usr/share/rubygems-integration/all/specifications/rbnacl-libsodium.gemsp
[ NOTICE ] Terms and Conditions
       1 This is the LACNIC RDAP service. Objects are in RDAP format.
      TOS http://www.lacnic.net/web/lacnic/registration-data-access-protocol

[ RESPONSE DATA ]
 1= 163.10.0.0/16
    |--- 1= Universidad Nacional de La Plata ( AR-UNLP-LACNIC )
    |--- 2= CeSPI UNLP ( ANB10 )
    `--- 3= Cert Unlp ( CEU )

         [ IP NETWORK ]
                Handle:  163.10.0.0/16
      Object Class Name:  ip network
          Start Address:  163.10.0.0
            End Address:  163.10.255.255
                  CIDRs:  163.10.0.0/16
             IP Version:  v4
                   Type:  assigned
           Registration:  Wed, 01 Jul 1992 12:00:00 -0000
           Last Changed:  Fri, 19 Mar 2010 20:09:35 -0000
                Remarks:  -- remarks --
                  Links:  -- for 163.10.0.0/16 --
              Reference:  https://rdap.lacnic.net/rdap/ip/163.10.0.0/16

             [ ENTITY ]
                Handle:  AR-UNLP-LACNIC
      Object Class Name:  entity
           Common Name:  Universidad Nacional de La Plata
                 Phone:  54 221 4236609#115 ( voice )
                 Roles:  Registrant
           Registration:  Fri, 06 Mar 2009 15:41:29 -0000
           Last Changed:  Mon, 27 Jul 2020 22:57:06 -0000
                Address:  -- for Universidad Nacional de La Plata ( AR-UNLP-LACNIC ) --
             Apt/Suite:  115
                Street:  1900
                  City:  La Plata
           Postal Code:  1900
               Country:  AR
                  Kind:  org
                 Links:  -- for Universidad Nacional de La Plata ( AR-UNLP-LACNIC ) --
              Reference:  https://rdap.lacnic.net/rdap/entity/AR-UNLP-LACNIC

             [ ENTITY ]
```

```
nico@portege-z30-b:~$ whois 163.10.5.66 -h whois.lacnic.net

% Joint Whois - whois.lacnic.net
%  This server accepts single ASN, IPv4 or IPv6 queries

% LACNIC resource: whois.lacnic.net


% Copyright LACNIC lacnic.net
%  The data below is provided for information purposes
%  and to assist persons in obtaining information about or
%  related to AS and IP numbers registrations
%  By submitting a whois query, you agree to use this data
%  only for lawful purposes.
%  2020-09-30 12:17:18 (-03 -03:00)

inetnum:     163.10.0.0/16
status:      assigned
aut-num:     N/A
owner:       Universidad Nacional de La Plata
ownerid:     AR-UNLP-LACNIC
responsible: Javier Diaz
address:     1900, 50, 115
address:     1900 - La Plata - BA
country:     AR
phone:       +54 221 4236609 [115]
owner-c:     ANB10
tech-c:      ANB10
abuse-c:     CEU
inetrev:     163.10.0.0/16
nserver:     UNLP.UNLP.EDU.AR
nsstat:      20200929 AA
nslastaa:    20200929
nserver:     ANUBIS.UNLP.EDU.AR
nsstat:      20200929 AA
nslastaa:    20200929
created:     19920701
changed:     20100319

nic-hdl:     ANB10
person:      CeSPI UNLP
e-mail:      noc@cespi.unlp.edu.ar
address:     Calle 50 y 115, S/N, 3er. piso
address:     1900 - La Plata - BA
country:     AR
phone:       +54 221 4236609 [1101]
created:     20081104
changed:     20150422

nic-hdl:     CEU
person:      Cert Unlp
e-mail:      abuse@unlp.edu.ar
address:     50 y 115
```

Recursos de Internet

- Direcciones IP
  - IPv4
  - IPv6

- **Nombres de dominio**

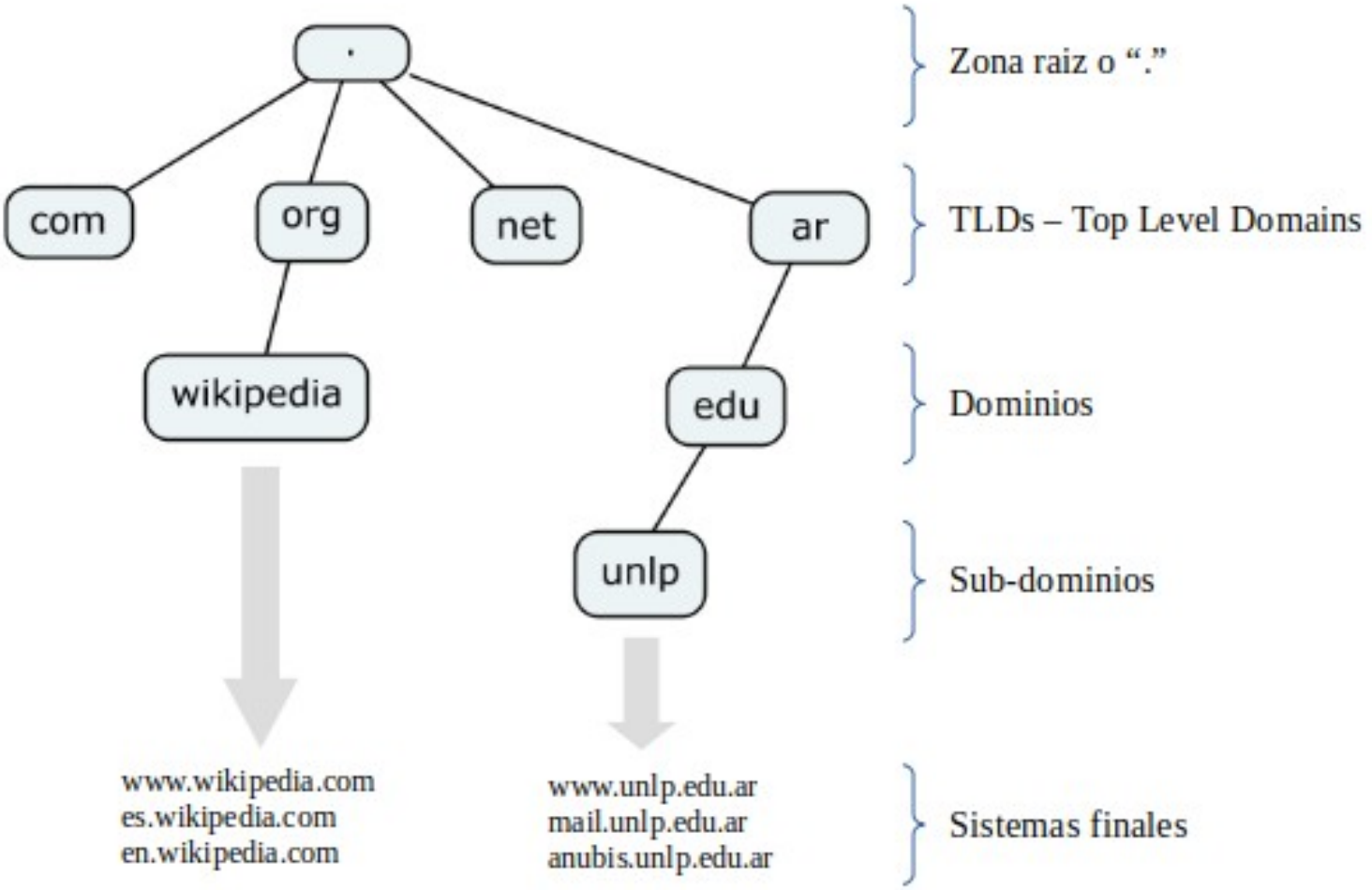
Asignación de dominios

- El sistema de nombres de dominio o DNS es un acrónimo utilizado tanto para referirnos a:
  - Una base de datos distribuida, organizada de forma jerárquica.
  - El protocolo de consulta
- La información de dicho sistema es gestionada de manera descentralizada por diferentes organismos...

Estructura de DNS

- El espacio de nombres de dominio usado en Internet, está organizado de forma jerárquica en distintas zonas:
  - Zona raiz o “.“
  - TLD (Top Level Domains)
    - gTLD (generic TLDs)
    - ccTLD (country codes TLDs)
    - arpaTLD (usado para asociar un nombre a una dirección IP)
  - Dominios y subdominios

Estructura de DNS



Gestión de nombres de dominio

En la gestión de los nombres de dominios, aparecen distintos tipos de actores que es preciso definir:

- **Registry o registros**: repositorio sobre la información oficial de un TLD.
- **Registrar o registradores**: quien vende un dominio.
- **Registrant o registrantes**: cliente que solicita un dominio

Gestión de nombres de dominio

Dado que para un TLD, exite:

- Una organización que mantiene el registro oficial **(registry)**

- Una o muchas organizaciones encargadas de vender dominios en dicho TLD: **(registrars)**

Puede suceder que quien el **registry** también tenga la función de **registrar**:

- NIC Argentina – nic.ar (registro y registrante del ccTLD .ar)
- Verisign (registro del gTLP .com y uno de los registrar posibles)

Información de los registry de distintos TLDs https://www.iana.org/domains/root/db

Información sobre dominios asignados

- Cada **Registry** mantiene una base de datos de acceso público sobre el registrar que asignó un nombre de dominio determinado.
- Cada **Registrar** mantiene una base de datos de acceso público sobre los datos de la organización que compró el dominio.
- Para acceder a éstos datos se utilizan dos protocolos de consulta:
  - WHOIS
  - RDAP (Registration Data Access Protocol)

Consulta whois

- Por ejemplo si quisiera saber sobre www.cualesmiip.com:
  - Si obtengo la IP y utiliza WHOIS o RDAP doy con los datos de un proveedor de hosting.
  - En cambio usando el dominio, voy a poder dar con la organización que hizo el registro del dominio.

```
nico@portege-z30-b:~$ whois cualesmiip.com
   Domain Name: CUALESMIIP.COM
   Registry Domain ID: 94673805_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.dinahosting.com
   Registrar URL: http://www.dinahosting.com/dominios
   Updated Date: 2020-01-29T07:53:55Z
   Creation Date: 2003-02-05T01:41:24Z
   Registry Expiry Date: 2021-02-05T01:41:24Z
   Registrar: Dinahosting s.l.
   Registrar IANA ID: 1262
   Registrar Abuse Contact Email: abuse-domains@dinahosting.com
   Registrar Abuse Contact Phone: +34.981040200
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibite
   Name Server: NS1.DOMMIADNS.COM
   Name Server: NS2.DOMMIADNS.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2020-09-30T17:22:49Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
```

En la primera linea, el comando utilizado.

En el recuadro violeta, la información sobre el registrar que realizó la asignación del nombre de dominio consultado.

Consulta whois (cont)

```
Domain Name: cualesmiip.com
Registry Domain ID: 94673805_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.dinahosting.com
Registrar URL: http://dinahosting.com
Updated Date: 2020-01-29T08:53:55Z
Creation Date: 2003-02-05T01:41:24Z
Registrar Registration Expiration Date: 2021-02-05T01:41:24Z
Registrar: Dinahosting s.l.
Registrar IANA ID: 1262
Registrar Abuse Contact Email: abuse-domains@dinahosting.com
Registrar Abuse Contact Phone: +34.981040200
Domain Status: clientDeleteProhibited (http://www.icann.org/epp#clientDeleteProhibited)
Domain Status: clientTransferProhibited (http://www.icann.org/epp#clientTransferProhibited)
Registrant ID: Redacted by Privacy
Registrant Name: Redacted by Privacy
Registrant Organization:
Registrant Street: Redacted by Privacy
Registrant City: Redacted by Privacy
Registrant State/Province: Barcelona
Registrant Postal Code: Redacted by Privacy
Registrant Country: ES
Registrant Phone: Redacted by Privacy
Registrant Phone Ext:
Registrant Fax: Redacted by Privacy
Registrant Fax Ext:
Registrant Email: https://dinahosting.com/dominios/contacto-whois/dominio/cualesmiip.com
Admin ID: Redacted by Privacy
Admin Name: Redacted by Privacy
Admin Organization: Redacted by Privacy
Admin Street: Redacted by Privacy
Admin City: Redacted by Privacy
Admin State/Province: Redacted by Privacy
Admin Postal Code: Redacted by Privacy
Admin Country: Redacted by Privacy
Admin Phone: Redacted by Privacy
Admin Phone Ext:
Admin Fax: Redacted by Privacy
Admin Fax Ext:
Admin Email: https://dinahosting.com/dominios/contacto-whois/dominio/cualesmiip.com
Tech ID: Redacted by Privacy
Tech Name: Redacted by Privacy
Tech Organization: Redacted by Privacy
Tech Street: Redacted by Privacy
Tech City: Redacted by Privacy
```

En el recuadro rojo, información sobre la entidad que tiene compro el nombre de dominio.

Uno de los servicios (legales) dados por los registrar es poner datos de contactos propios para ser una pasarela y que el cliente no quede tan expuesto.

Consulta RDAP

```
nico@portege-z30-b:~$ nicinfo -Q cualesmiip.com
Invalid gemspec in [/usr/share/rubygems-integration/all/specifications/rbnacl-libsodium.gemspec
[ NOTICE ] Terms of Use
        1 Service subject to Terms of Use.

[ NOTICE ] Status Codes
        1 For more information on domain status codes, please visit https://icann.org/epp

[ NOTICE ] RDDS Inaccuracy Complaint Form
        1 URL of the ICANN RDDS Inaccuracy Complaint Form: https://icann.org/wicf

[ RESPONSE DATA ]
  1= CUALESMIIP.COM ( 94673805_DOMAIN_COM-VRSN )
     |--- 1. Dinahosting s.l. ( 1262 )
     |     `--- 1.  ( (unidentifiable entity 47372469517920) )
     |--- 2. NS1.DOMMIADNS.COM ( NS1.DOMMIADNS.COM )
     `--- 3. NS2.DOMMIADNS.COM ( NS2.DOMMIADNS.COM )

              [ DOMAIN ]
                 Handle:  94673805_DOMAIN_COM-VRSN
        Object Class Name:  domain
              Domain Name:  CUALESMIIP.COM
                   Status:  Client Delete Prohibited, Client Transfer Prohibited
             Registration:  Wed, 05 Feb 2003 01:41:24 -0000
               Expiration:  Fri, 05 Feb 2021 01:41:24 -0000
Last Update Of Rdap Database:  Wed, 30 Sep 2020 09:41:21 -0000
                    Links:  -- for CUALESMIIP.COM ( 94673805_DOMAIN_COM-VRSN ) --
                Reference:  https://rdap.verisign.com/com/v1/domain/CUALESMIIP.COM
        Delegation Signed:  false

              [ ENTITY ]
                 Handle:  1262
        Object Class Name:  entity
              Common Name:  Dinahosting s.l.
                    Roles:  Registrar
                Public ID:  1262 (IANA Registrar ID)

              [ ENTITY ]
        Object Class Name:  entity
                    Email:  abuse-domains@dinahosting.com
                    Phone:  +34.981040200 ( voice )
                    Roles:  Abuse

          [ NAME SERVER ]
        Object Class Name:  nameserver
                Host Name:  NS1.DOMMIADNS.COM

          [ NAME SERVER ]
        Object Class Name:  nameserver
                Host Name:  NS2.DOMMIADNS.COM
```

En verde, el comando utilizado.

En los recuadros violeta y rojo, la información del Registrar que realizó la asignación del nombre de dominio.

Al día de hoy, la información dada por WHOIS para nombres de dominio es más relevante que la dada por RDAP

https://blog.apnic.net/2021/04/02/is-rdap-ready-to-replace-whois/

Usos posibles

La información de contacto brindada por distintos organismos tanto para recursos IP como DNS es utilizada por:

- CSIRTs
  (equipos de respuestas a incidentes de seguridad)

- LEAs
  (Law Enforcement Agencies)

Usos posibles para CSIRTs

Durante la gestión de incidentes de seguridad:

- Dado un recursos IP:
  - Los **RIRs** brindan, vía WHOIS/RDAP, información de contacto sobre la organización que tiene un recurso IP asignado.

- Dado un nombre de dominio
  - Los **registrar** brindan, vía WHOIS/RDAP, información de contacto sobre la personal o la organización que realizó el registro de un dominio determinado.

Usos posibles para LEAs

Durante la investigación de distintas actividades delictivas que se dan a nivel global:

- Dado un recursos IP:
  - Los **RIRs** pueden dar información adicional mediante orden judicial, a la disponible públicamente vía WHOIS/RDAP.
- Dado un nombre de dominio:
  - Los **registrar** pueden dar información adicional mediante orden judicial, a la disponible públicamente vía WHOIS/RDAP.

La información adicional puede ser: datos de contacto y de facturación utilizados en el proceso de asignación.