



## DNS.Ar

### Sistema de análisis de servidores y dominios DNS

**Coordinación de Emergencias en Redes Teleinformática de Argentina.**

Oficina Nacional de Tecnologías de Información (ONTI).

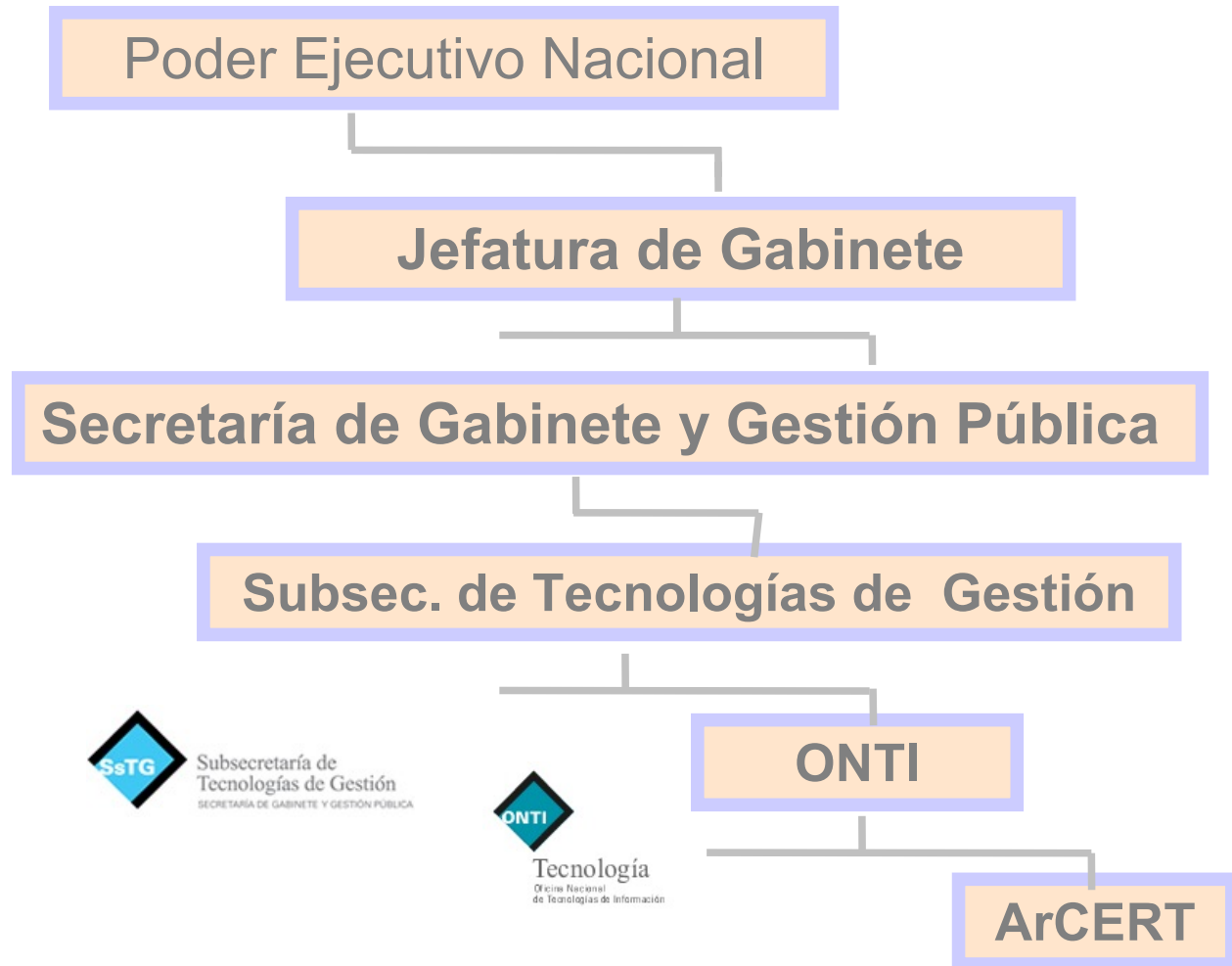
Subsecretaría de Tecnologías de Gestión.

Ing. Marcela Pallero – Equipo ArCERT-

## Temario

- ArCERT
- ¿QUÉ ES DNS.AR?
- OBJETIVO
- SERVICIO BRINDADO
- REPORTES
- RESULTADOS
- CONCLUSIÓN

- Coordinación entre Ministerios
- Coordinación entre entes rectores
- Responsable del uso de TIC en el Estado
- Organismo rector en TICs



### OBJETIVO PRINCIPAL

Incrementar los niveles de Seguridad  
Informática del Sector Público

### OBJETIVOS ESPECÍFICOS

Atención de Incidentes de Seguridad

#### Actividades Preventivas

- Concientización
- Capacitación
- Difusión de Alertas e Información
- Políticas de Seguridad de la Información

#### Servicios

## ¿Qué es?

Herramienta desarrollada por ArCERT, que funciona desde el año 2006 con el objetivo de analizar Servidores y Dominios DNS.

## Objetivo

Detectar y alertar sobre errores de configuración y funcionamiento en los servidores DNS de los dominios de Organismos Públicos.

Mantener una base de datos histórica

Generar información estadística


## Servicio brindado

- El sistema detecta problemas “básicos”.
- Los problemas están clasificados con un nivel de gravedad de 1 a 5. (5 más grave)
- Los nombres internos, la gravedad, la descripción detallada de cada problema, con la solución para algunos casos y la bibliografía se encuentran en el sitio de ArCERT.
- El lanzamiento del servicio se realizó el 19 de diciembre de 2006.

## Servicio brindado

- El sistema se ejecuta cada 3 meses y se envían los reportes en formato PDF.
- Los reportes son enviados a quienes figuran en NIC AR como “Persona Responsable” y en el caso que exista un usuario miembro de ArCERT registrado para ese dominio, se le envía también.
- ArCERT asiste a los organismos para su solución ante consultas puntuales.
- El servicio es gratuito.

»  Versión en Español

»  English Version



» Como deben actuar los Organismos ante un incidente

» Qué es ArCERT

» Información Institucional

» Cómo asociarse

» Noticias

» Productos y Servicios

» Capacitación

» Reportes de incidentes

»  Política de Seguridad para el Sector Público

» Recomendaciones Técnicas

» Lecturas Recomendadas

» Lista de SEGURIDAD

» Manuales de Seguridad

» Enlaces

» CSIRTs

» Alcance y Declinación de Responsabilidad

» Contáctenos

### Detalle de los problemas analizados por DNSAr

En esta sección se detallarán los problemas detectados por DNSAr, mostrando en cada caso una descripción del mismo, su gravedad en cuanto a posibles impactos en la seguridad del mismo y la solución propuesta para dicho problema.

» ALLOW\_RECURSIVE\_QUERIES » » »

» ZONE\_TRANSFER\_ALLOWED » » »

» 2NSS\_PARENT » » »

» NS\_NOT\_RESPONDING » » »

» DOMAIN\_UNRESOLVABLE » » »

» STEALTH\_SERVERS » » »

» DIFF\_SERIAL » » »

» PRIMARY\_MASTER\_NOT\_RESPONDING » » »

» INVALID\_DOMAINNAME\_RFC » » »

» LAME\_DELEGATION » » »

» LESS\_THAN\_2\_MX » » »

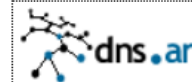
» SOA\_RNAME » » »

» MASTER\_INCLUDE » » »

» PRIVATE\_IP » » »

» WWW\_EXIST » » »

## Servicio brindado



DNSAr

Sistema de análisis de servidores y dominios DNS

» Descripción

DNSAr es un software desarrollado por ArCERT para analizar los servidores y dominios DNS en busca de posibles errores de configuración y funcionamiento.

» Ver

[Más Información del Producto](#)

### :: STEALTH\_SERVERS

<b>Descripción</b>	Existe al menos un servidor de nombre declarado en los servidores de nombre de la zona no está definido en la zona de nivel superior para el dominio.
<b>Gravedad</b>	4 -
<b>Descripción Detallada</b>	Se conoce con el nombre de <i>stealth servers</i> a aquellos servidores de nombres que se encuentran declarados en la zona del dominio y no se encuentran declarados en la zona de nivel superior.
<b>Solución</b>	El responsable del dominio deberá actualizar los datos referentes a sus servidores de nombre en la página de <a href="#">NICar</a> para que aquellos servidores de nombres declarados como <i>stealth servers</i> figuren como servidores de nombres autoritativos para el dominio en la zona de nivel superior. En caso de que no se desee hacer esto, se recomienda reconfigurar los servidores de la zona para que no mencionen a los servidores <i>stealth</i> como servidores autoritativos para el dominio.

- El sistema chequea 30 problemas.

# Glosario



**DNSAr**

Sistema de análisis de servidores y dominios DNS

:: Glosario de Términos

Registros de tipo: A, CNAME, MX, PTR, SOA; AXFR, Resolución de nombre, Respuesta autoritativa, no autoritativa, RTT, Servidores de nombres, primario, secundario, subdominio, Transferencia de zona, URL.

<b>Registro de tipo AXFR</b>	Contiene todos los registros asociados al dominio que corresponda. Este registro será utilizado para realizar Transferencias de Zonas.
<b>Registro de tipo CNAME</b>	Se utiliza para crear nombres de hosts adicionales, o alias, para los hosts de un dominio.
<b>Registro de tipo MX</b>	Define un Mail eXchanger (servidor de correo) para un nombre de dominio.
<b>Registro de tipo NS</b>	Define un servidor de nombres para un dominio.
<b>Registro de tipo PTR</b>	También conocido como 'registro inverso', funciona a la inversa del registro A, traduciendo IPs en FQDNs.
<b>Registro de tipo SOA</b>	Registro de "Start of Authority" para un dominio. Contiene identificadores del servidor de nombres con autoridad sobre la denominación y su operador, y diversos atributos que regulan el funcionamiento general del sistema de nombres de dominio para la denominación, en especial en lo que tiene que ver con períodos de validez de las respuestas emitidas. Todo servidor de nombres de una zona debe responder a una consulta por el registro SOA de esa zona en forma autoritativa.
<b>Resolución de nombres</b>	Genéricamente, traducción de nombres de dominio a direcciones IP y viceversa.
<b>Respuesta Autoritativa</b>	Tipo de respuesta, dada por un DNS a una consulta, en que se indica que el servidor de nombres tiene autoridad sobre el registro por el cual se lo consulta, e implica que es uno de los servidores de nombres del dominio al que pertenece el registro.
<b>Respuesta no Autoritativa</b>	Tipo de respuesta, dada por un DNS a una consulta por cualquier registro, que no está basada en tablas propias, sino que es obtenida consultando a otros servidores de nombres.
<b>RTT</b>	Medida para determinar cuánto tarda un servidor en responder una consulta.
<b>Servidor de nombres</b>	Equipo que efectúa la resolución de nombres para una denominación.

## Problemas detectados:

Problemas relacionados con:

- La zona padre del dominio: Por ejemplo: consultas recursivas, transferencias de zona.
- Los servidores de nombres del dominio.
- Los registros de tipo SOA del dominio, se chequean valores recomendados en RFC's
- Los registros del dominio.
- Los registros de tipo MX del dominio.

## Reporte

## Niveles de gravedad.

### Notas

La implementación del servicio DNS utiliza el protocolo UDP. Este protocolo es sin conexión y no confiable. Debido a esto, es posible que algunos paquetes destinados a consultar los servidores de nombres se pierdan y por lo tanto algunos problemas pueden ser dados de alta de forma incorrecta.

En caso de detectar algún problema en el informe, contactenos a través de [dnsar@arcert.gob.ar](mailto:dnsar@arcert.gob.ar)

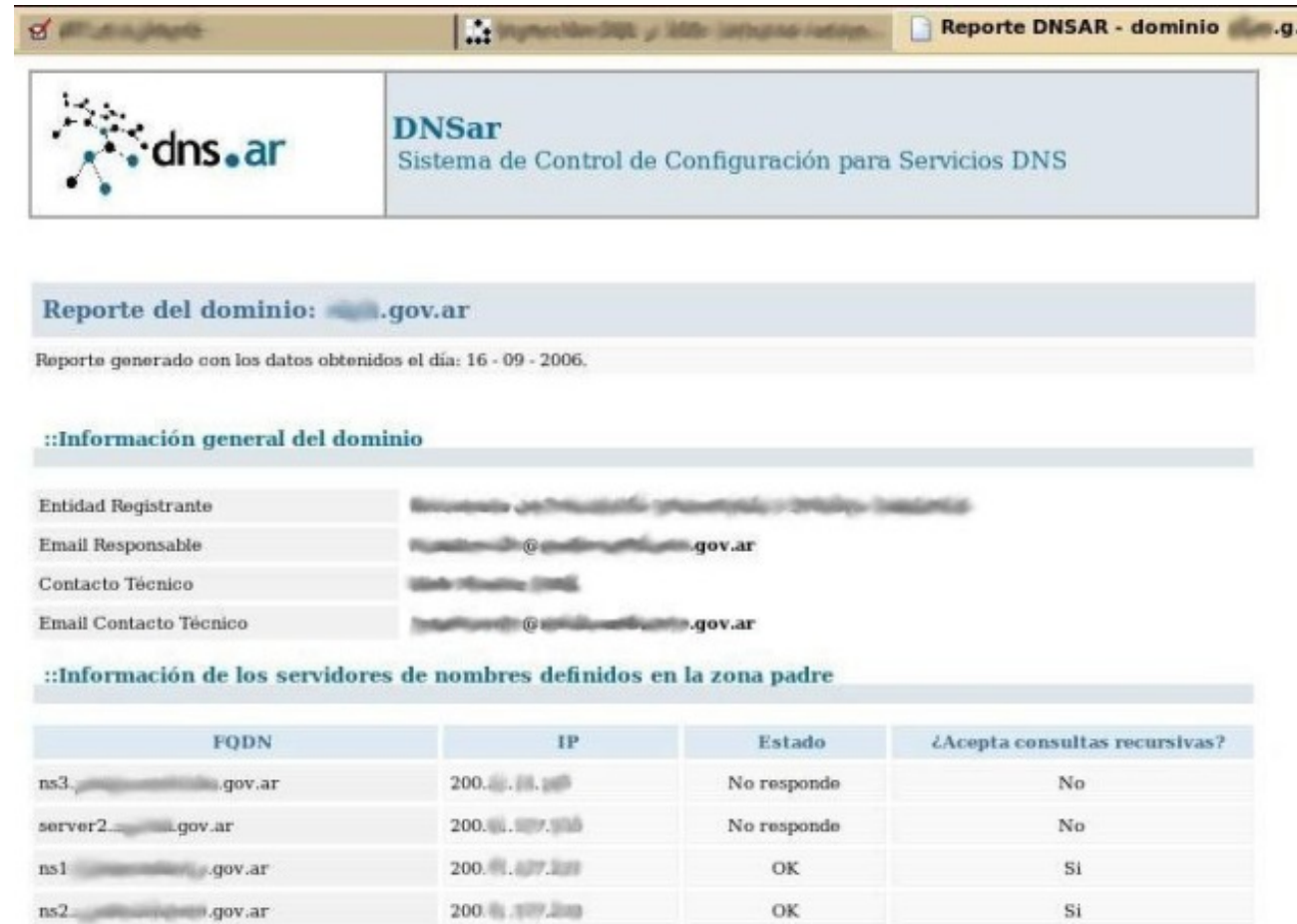
A continuación se detalla el significado de cada nivel de gravedad:

Gravedad	Descripción
5	La resolución del dominio no se puede llevar a cabo. Compruebe que los datos en NICar sean correctos y que sus servidores DNS se encuentren bien configurados para dicho dominio.
4	La configuración de los servidores DNS relacionados con su dominio tienen fallas en configuración que podrían implicar problemas de seguridad, o que los servidores no puedan responder de manera correcta a las consultas.
3	La redundancia de la información en el sistema de resolución se ve comprometida. Esto puede ser por errores de configuración en la zona, ya sea en la declaración del dominio o en los datos que contienen los registros SOA del dominio.
2	No sigue con las normas estipuladas en los RFCs.
1	No sigue con las recomendaciones hechas en los RFCs.
0	Información

## Reporte

Información general del organismo.

Información de los servidores de nombres definidos en la zona padre.



Reporte DNSAr - dominio .gov.ar

**DNSAr**  
Sistema de Control de Configuración para Servicios DNS

Reporte del dominio: .gov.ar

Reporte generado con los datos obtenidos el día: 16 - 09 - 2006.

**::Información general del dominio**

Entidad Registrante: *[Redacted]*  
 Email Responsable: *[Redacted]*@*[Redacted]*.gov.ar  
 Contacto Técnico: *[Redacted]*  
 Email Contacto Técnico: *[Redacted]*@*[Redacted]*.gov.ar

**::Información de los servidores de nombres definidos en la zona padre**

FQDN	IP	Estado	¿Acepta consultas recursivas?
ns3. <i>[Redacted]</i> .gov.ar	200.61.18.100	No responde	No
server2. <i>[Redacted]</i> .gov.ar	200.61.107.100	No responde	No
ns1. <i>[Redacted]</i> .gov.ar	200.61.107.101	OK	Si
ns2. <i>[Redacted]</i> .gov.ar	200.61.107.102	OK	Si

## Información de los reportes:

::Problemas relacionados con la zona padre del dominio:

Problema	Gravedad	Descripción
AT_LEAST_ONE_NS	5	No existen servidores de nombres declarados en la zona de nivel superior que puedan responder por consultas sobre el dominio. Debido a ésto, no se podrá continuar con los controles.

### NOTAS:

- Si bien los reportes informan inconsistencias o incumplimiento de recomendaciones o normativas, existe la posibilidad de que lo informado sea una configuración intencional y debidamente fundada.
- Algunos de los problemas que se informan no implican mal funcionamiento, razón por la cual, en muchos casos no son solucionados rápidamente.

# Reportes

**::Problemas relacionados con los servidores de nombres del dominio:**

Problema	Gravedad	Descripción
NS_NOT_RESPONDING	4	El/los siguiente/s servidor/es de nombres no responden: ns. .... com
ALLOW_RECURSIVE_QUERIES	4	El/Los siguiente/s servidor/es de nombres acepta/n consultas recursivas. Esto significa que cualquier equipo puede consultar a este servidor sobre dominios para los cuales no es autoritativo: ns. .... com
ZONE_TRANSFER_ALLOWED	4	El/Los siguientes servidores de nombre permiten realizar transferencias de zona a un host no declarado como servidor de nombres secundario del dominio: nsl. .... com
STEALTH_SERVERS	4	El/Los siguiente/s servidor/es de nombres declarado/s en los servidores de nombres de la zona no está/n definido/s en la zona de nivel superior para el dominio: ..... com
LAME_DELEGATION	4	El/Los siguiente/s servidor/es de nombres registrado/s en la zona padre son "lame servers", es decir que responden de forma no autoritativa ante una consulta del registro SOA del dominio. dn. .... ar dn. .... ar

# Reportes

### ::Problemas relacionados con los registros del dominio:

Problema	Gravedad	Descripción
WWW_CNAME	1	No se recomienda que la entrada <code>www</code> sea de tipo CNAME.

### ::Problemas relacionados con los registros de tipo MX del dominio:

Problema	Gravedad	Descripción
LESS_THAN_2_MX	1	Es recomendable que existan al menos dos registros de tipo MX para el dominio.

# REPORTE

Problemas relacionados con los registros del tipo SOA del dominio

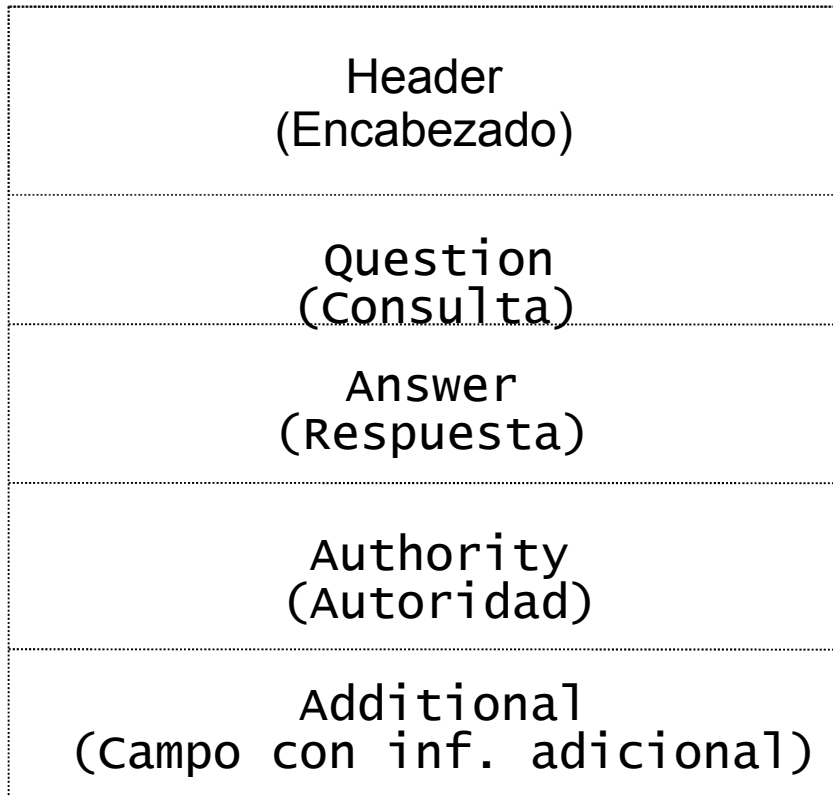
### ::Problemas relacionados con los registros de tipo SOA del dominio:

Los controles de problemas en los registros SOA se realizarán tomando los valores que se especifican a continuación:

Nombre del Campo	Valor	
MNAME	[redacted].b.com	ns.primario.gov.ar (responde c/ aut)
RNAME	[redacted].b.com	mail.dominio.gov.ar
SERIAL	8	AAAADDMMnn
REFRESH	900	e/1200 y 86400
RETRY	600	e/1200 y 86400
EXPIRE	86400	e/ 86400 y 360000
TTL	3600	e/ 3600 y 86400
Servidor DNS consultado	ns.[redacted].com	

Problema	Gravedad	Descripción
MASTER_INCLUDE	2	El servidor de nombres informado en el registro de tipo SOA como servidor primario del dominio no aparece declarado como servidor autorativo para este dominio en la zona de nivel superior.
SOA_SERIAL	1	El valor SERIAL del registro de tipo SOA es correcto pero no coincide con el formato recomendado según RFC 1912.
SOA_REFRESH	1	El valor del campo REFRESH del registro de tipo SOA no se corresponde con los valores recomendados

SOA_RNAME	2	El valor de RNAME del registro de tipo SOA parece ser inválido.
-----------	---	---



Formato de Paquete DNS

### Principales problemas detectados.

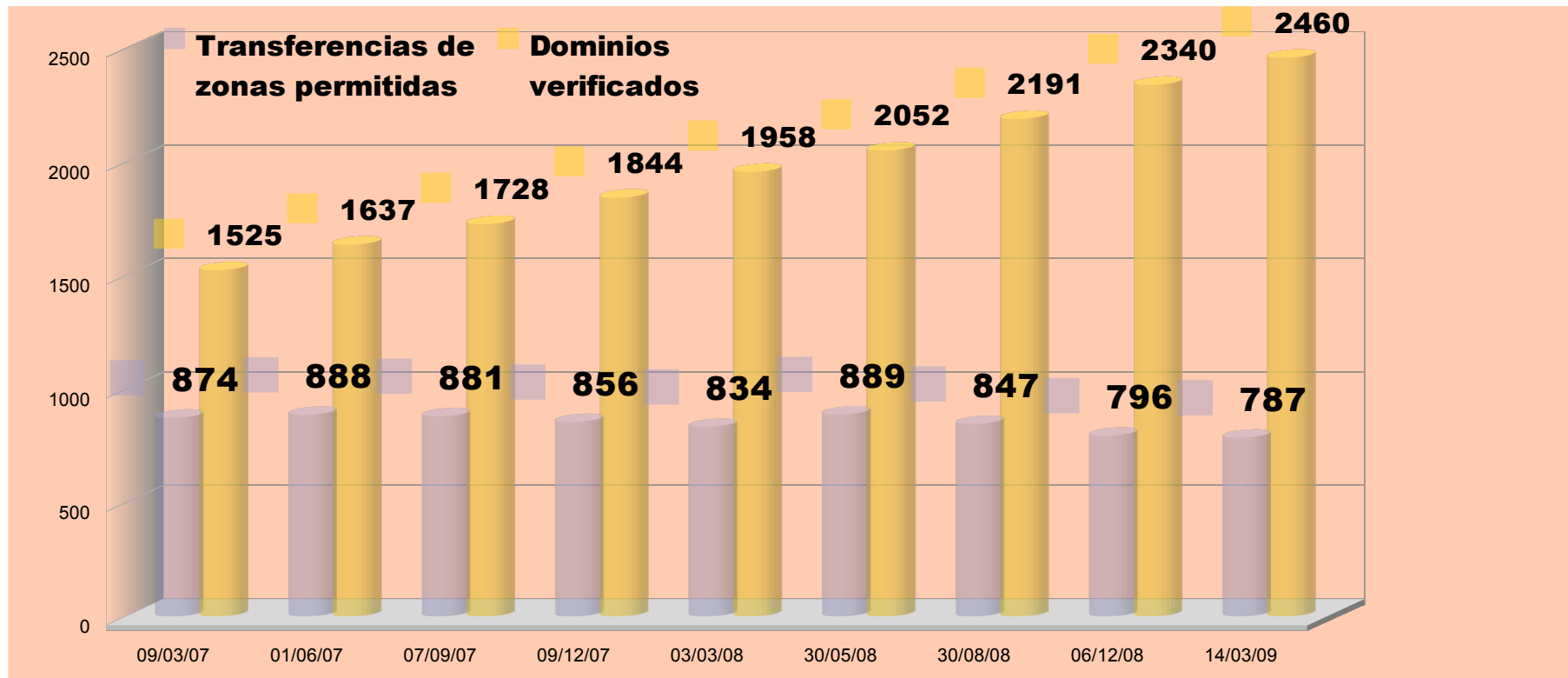
1. Servidores DNS que permiten transferencias de zonas.
2. Equipos que permiten consultas recursivas.
3. Alguno de los servidores que figuran como autoridad no responde.
4. "Lame Delegation"

### No informa sobre:

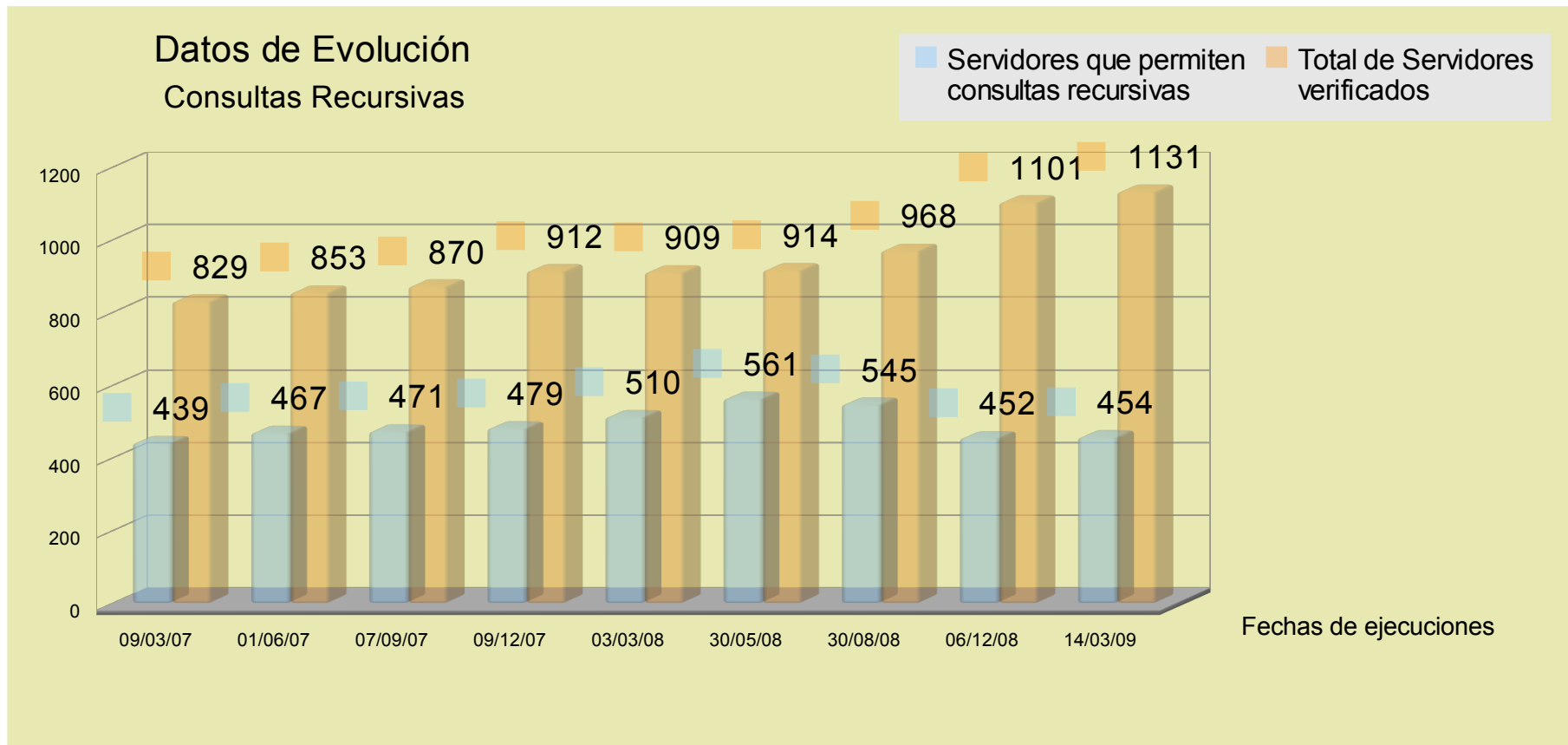
- Aleatoriedad de QID (Id. de la transacción)
- Aleatoriedad del puerto de origen de las consultas


Los problemas relativos a estos 2 puntos fueron testeados e informados por ArCERT por fuera de DNS AR.

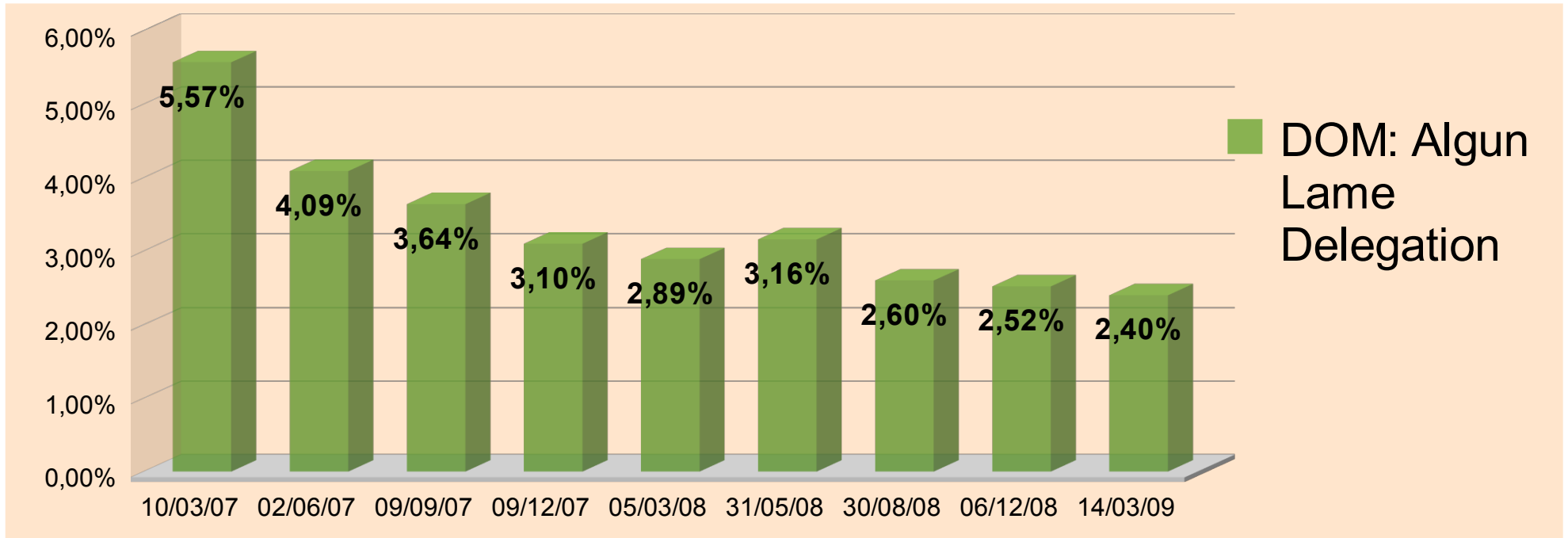
- Datos sobre dominios que permiten transferencias de zona a un equipo no declarado como servidor de nombre secundario del dominio.



### Datos sobre servidores DNS que permiten consultas recursivas



 **Lame delegation:** un servidor DNS tiene este problema cuando, estando registrado en la zona de autoridad de ese dominio, no responde con autoridad para ese dominio.



## Conclusiones:

- DNS AR no es suficiente, pero es necesario.
- Es necesario mejorar los contactos con los administradores de los dominios de organismos públicos para el tratamiento de los Reportes de DNS AR.
- Esperamos poder actualizar, extender y mejorar los chequeos realizados en el corto plazo.

## Próximos eventos de ArCERT:

- El 14 de julio de 2009 : 10° aniversario de ArCERT.
  
- Entre el 23 y el 30 de noviembre de 2009: “Semana de la Seguridad Informática” en Argentina.

**¡Muchas Gracias!**

**ArCERT**

[www.arcert.gob.ar](http://www.arcert.gob.ar)

**Consultas:** [info@arcert.gob.ar](mailto:info@arcert.gob.ar)

**Reporte de incidentes:** [mailinfo@arcert.gob.ar](mailto:mailinfo@arcert.gob.ar)

[www.youtube.com/ seguridadinfoar](http://www.youtube.com/seguridadinfoar)

Marcela Pallero  
[mpallero@arcert.gob.ar](mailto:mpallero@arcert.gob.ar)