



# CSIRTamericas.org

**OAS Team**

Junio de 2016

[www.oas.org/cyber/](http://www.oas.org/cyber/)



Organización de los Estados Americanos | Más derechos para más gente

**Descargo de responsabilidades:**

La información y los argumentos de esta presentación no necesariamente reflejan los puntos de vista de la Secretaría General de la Organización de los Estados Americanos (OEA) o de los gobiernos de sus Estados Miembros.

# Agenda

I

- Vista general de los CSIRT nacionales de la región



II

- Problemas detectados en CSIRTs de la region

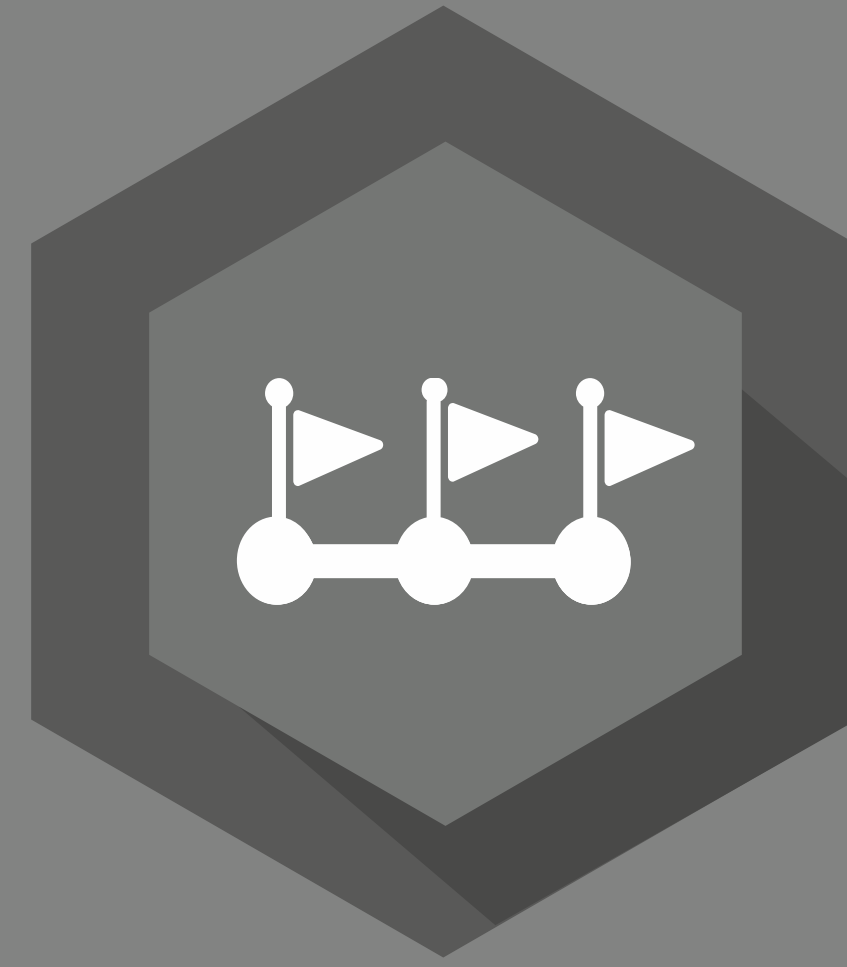


III

- CSIRTamericas.org



CSIRTamericas.org



# Vista General

# CSIRTs en las Américas

(2016) estado actual

○ ICIC CERT

○ CCIRC

○ US-CERT

○ CTIRGov

○ CERT-MX

○ CSIRT Chile

○ CL-CERT

○ ADSIB

○ CSIRTGt

○ PE-CERT

○ SurCSIRT

○ EcuCERT

○ ColCert

○ CSIRT-GY

○ TT-CSIRT

○ JM-CSIRT

○ VenCERT

○ CERT-PY

○ CERTUy

○ CSIRT Costa Rica

○ CSIRT Panama



# I - Vista general de los CSIRT

## Diversidad en las operaciones



 CSIRT Nacional A  
País A

● Experiencia en monitoreo  
CSIRT operativo

 CSIRT Nacional C  
Country C

● Experiencia en incidentes en banca  
CSIRT Operativo

 CSIRT Nacional B  
País B

● Incidentes de gran escala  
CSIRT Operativo

 CSIRT Nacional D  
País D

● Desarrollo de herramientas  
CSIRT Investigación

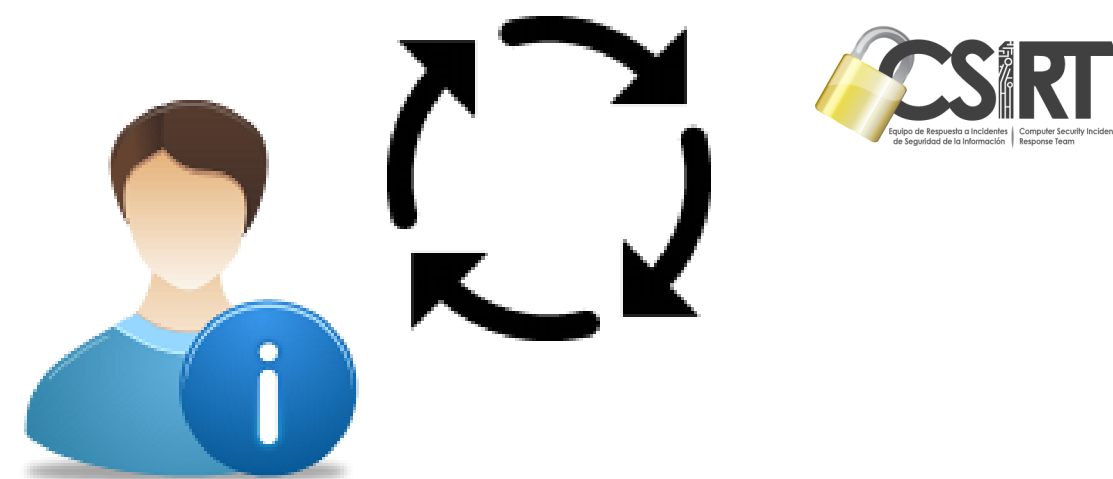


**Problemas detectados**

# Rotacion de personal

**Alta formacion** = Recurso atractivo de irse

**Alto nivel tecnico** = Recurso atractivo de irse



Se pierde la continuidad | se pierde la informacion | empezar de cero muchas veces..



# Limitaciones financieras y logisticas

## Financiero



### Presupuesto para:

- Adquisición de suscripciones
- Adquisición de equipos
- Adquisición de licencias

Monitoreo limitado | respuesta a incidentes disminuida

## Logistico



### Limitaciones internas:

- Para implementar un servicio
- Falta de espacios físicos
- Problemas legales

Retraso en actividades y crecimiento

## II - Problemas detectados

Limitaciones en la respuesta a incidentes (dia a dia)


Confusiones de las actividades del CSIRT desde otras instancias

Por "ejemplo" en

### Respuesta Pasiva

Busqueda de vulnerabilidades 


Tracking de anomalias  

Compartir data &r referencia 

### Respuesta activa


Bloquear origenes o fuentes de ataques  

Bloqueo temporal de cuentas  

Redirigir trafico a honeypots  

(implementación de honeypot)

### Respuesta intrusiva

Considerado un delito en muchos paises. 

Clarificar aspectos legales y funciones de cara a la comunidad 

## CSIRTs y los organismos de aplicacion de ley

Prioridad



Recuperar el servicio o sistema y hacerlo lo menos vulnerable posible ante futuros ataques

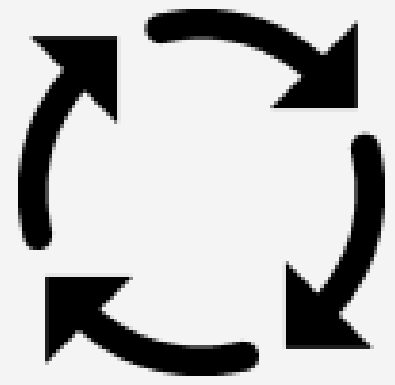
Proteger plataformas tecnologicas de las vulnerabilidades que surgen en sistemas.

Atribuir el ataque y enjuiciar los culpables

Reducir el numero de actores de amenaza



Organismos de Aplicación de Ley



## II - Problemas detectados

# Comunicacion entre instancias regionales

### Institucional



✓ Formal

✓ Uniforme

✓ Segura

No-Colaborativa

Lenta

### Informal



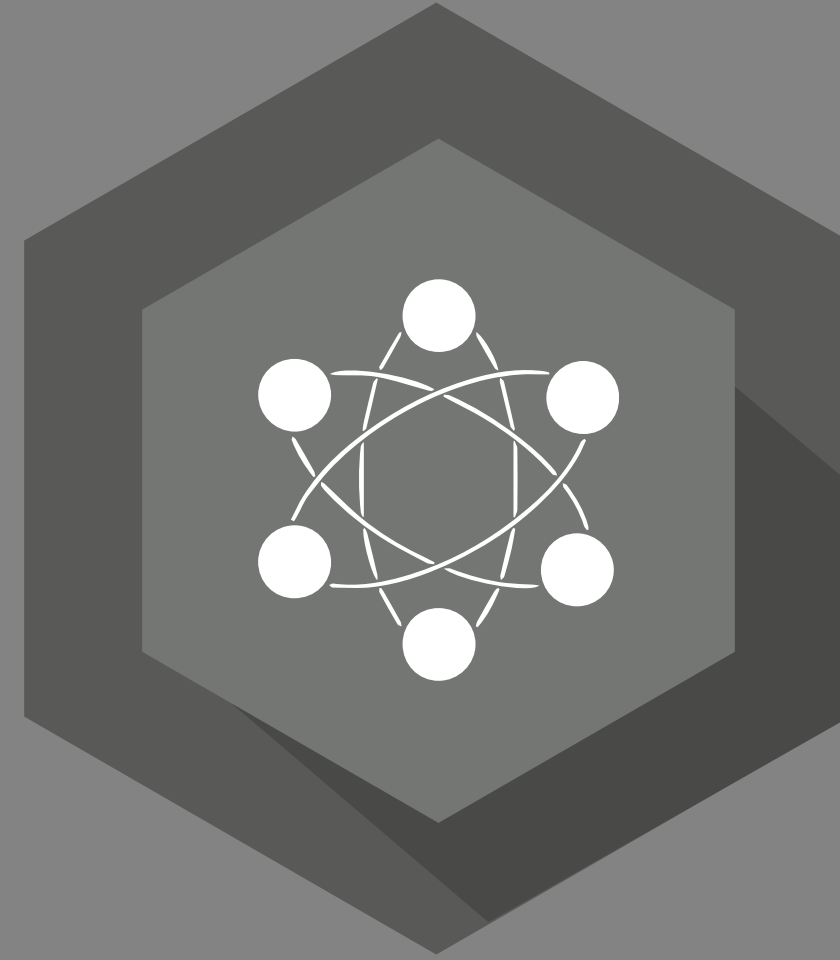
Informal

✓ Colaborativa

No muy segura

✓ Dinamica

No uniforme



**CSIRT**americas.org

Comunicación en tiempo real | Intercambio de información | proyectos colaborativos

## Plataforma tecnológica

Brindar

### Servicios básicos

- Chat y chat grupal
- Foro
- CSIRTs noticias
- Librería digital
- Directorio
- Eventos
- Elecciones

### Servicios especializados

- Early warning systems
- (ftp) – Ejecución de mejora para 2 semestre 2016

### Servicios aliados

- Aliados internacionales

para

## CSIRT de las Americas



**CSIRT Defensa**



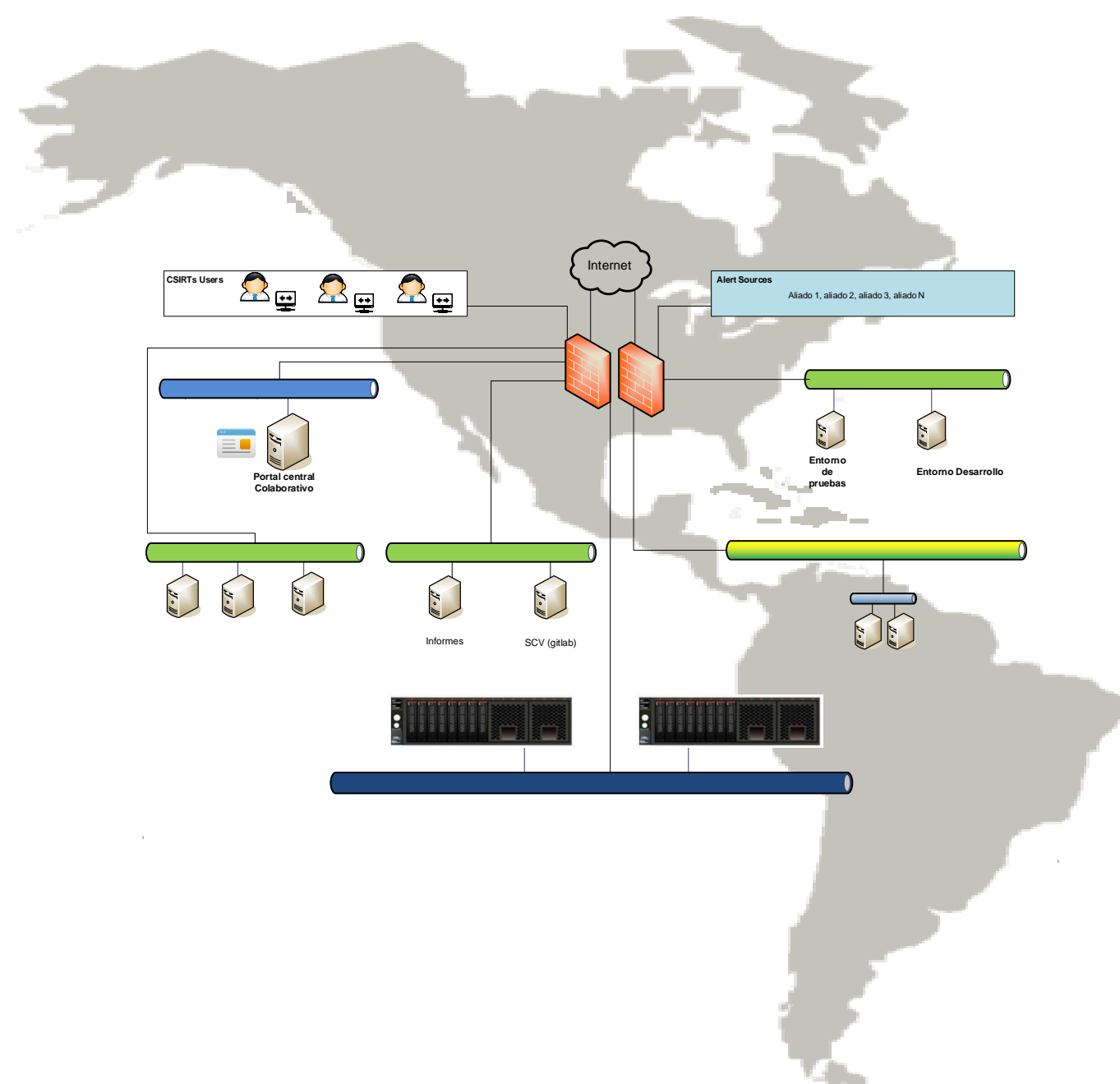
**CSIRT Policia**



**CSIRT gov**



**CSIRT Nacional**



## Servicios Básicos

1 etapa

- ✓ Chat y chat grupal
- ✓ Foro tecnico
  - ✓ Sistemas de tickets, herramientas para pentesting...
- ✓ Noticias orientadas a CSIRTs
  - ✓ Reportes relevantes, entrenamientos
- ✓ Librería digital
  - ✓ Procedimientos, herramientas
- ✓ Directorio
  - ✓ Directorio por skills ( perfil web, perfil de redes,etc)

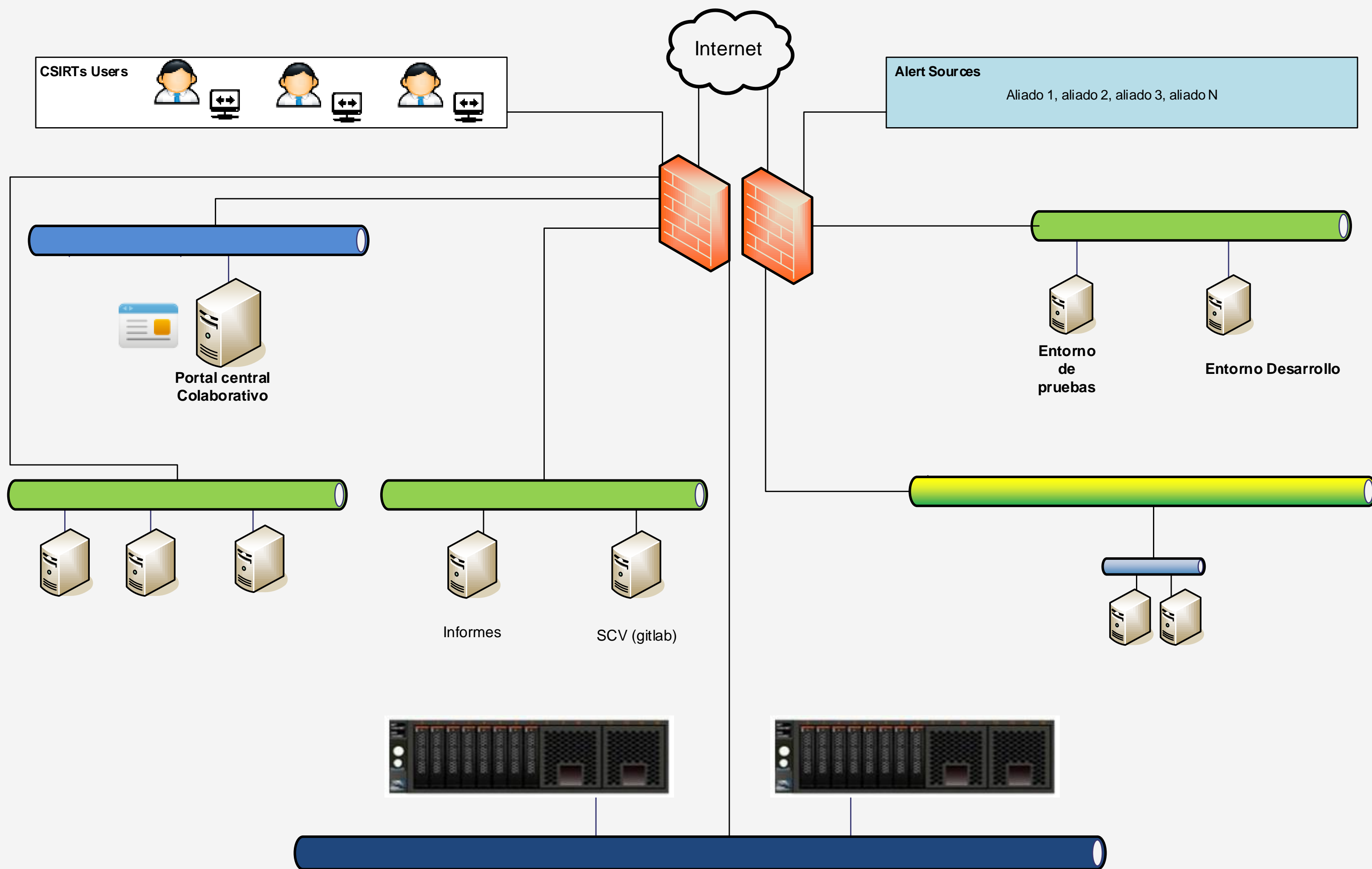
## Servicios especializados

1 etapa

- ✓ Alertas tempranas ( testing)
  - Alertas 7x24
- Control de versiones (svn)

## Servicios de Aliados

- ✓ Servicio aliado 1
- ✓ Servicio aliado 2

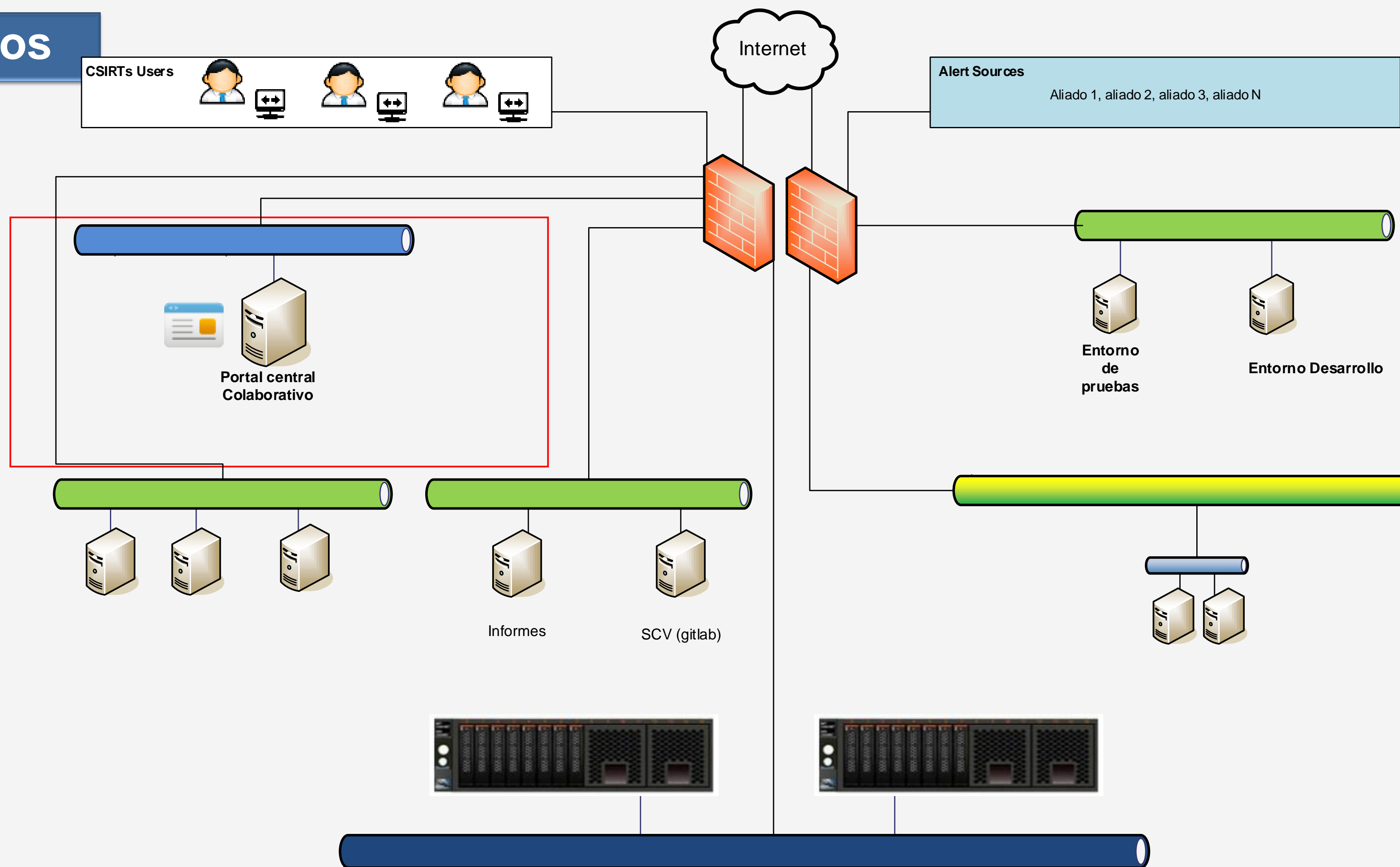




# Servicios Básicos

## Servicios basicos

- ✓ Chat y chat grupal
- ✓ Foro técnico
- ✓ Noticias orientadas a CSIRTs
- ✓ Librería digital
- ✓ Directorio

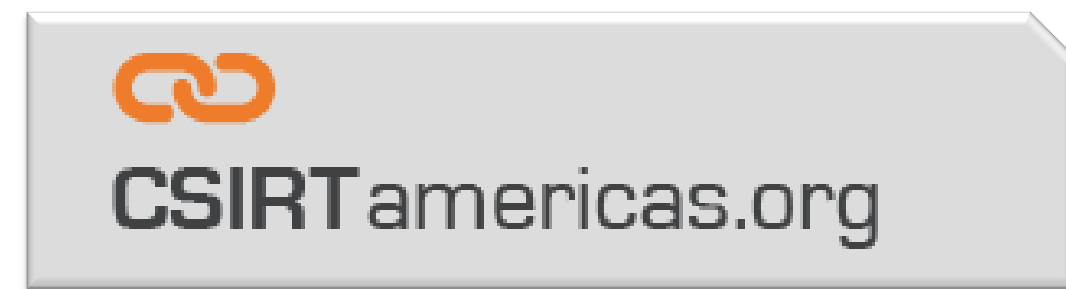
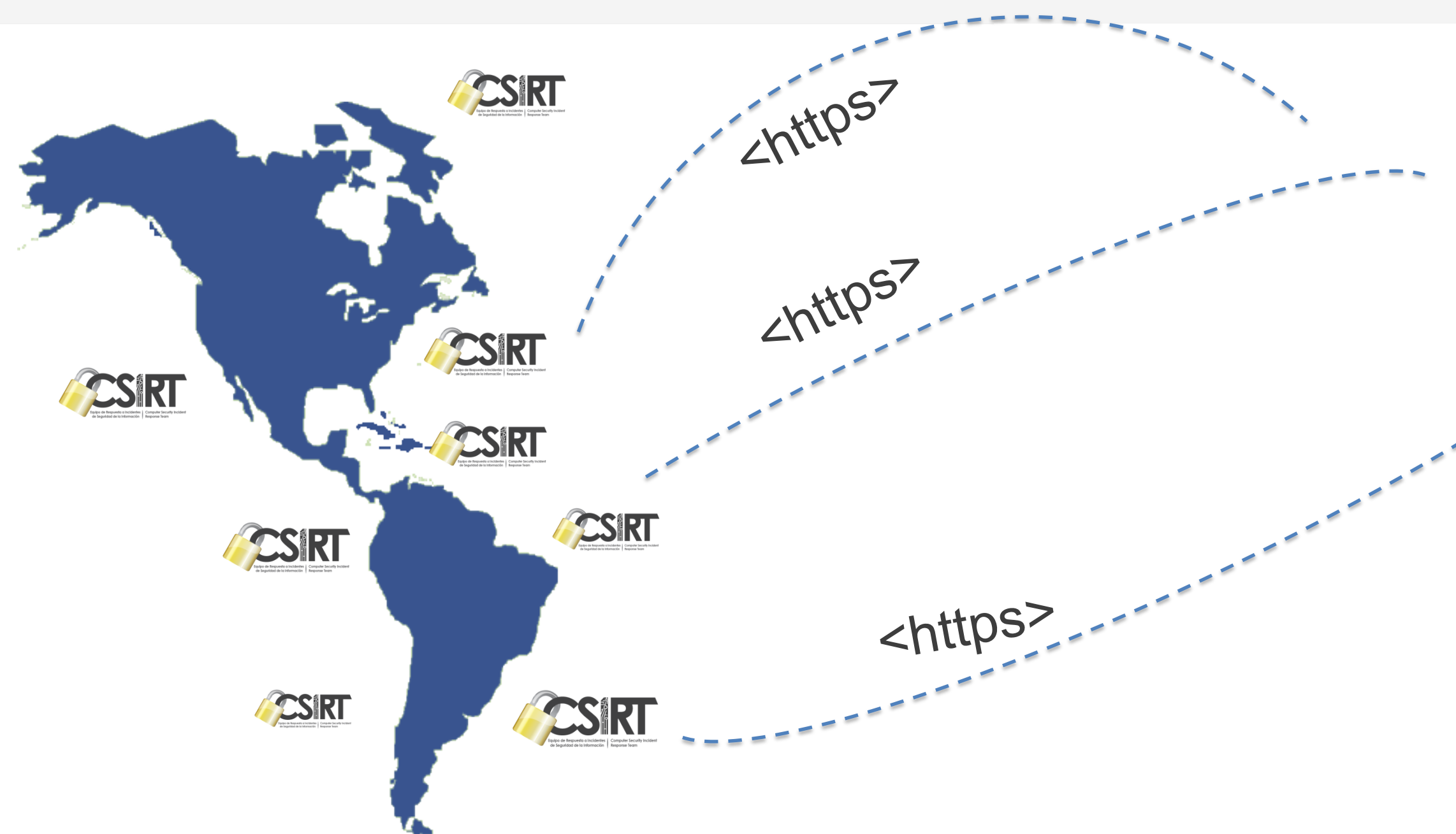


## Servicios Básicos



# El lado #humano

Acceso <https://csirtamericas.org>



Facil acceso para los CSIRTs  
...Pero restringido

- ✓ Directorio
- ✓ Chat y chat grupal
- ✓ Librería digital
- ✓ Foro técnico
- ✓ Noticias orientadas a CSIRTs

## Servicios Básicos

The screenshot displays the OAS Hemispheric Technical NET website interface. At the top, the navigation bar includes the OAS logo, a 'Member states' dropdown menu, and links for 'Services', 'Partners', and 'About'. A 'Logout dsuero' button is visible in the top right corner. The 'Member states' dropdown is open, showing a list of countries with their respective flags and right-pointing arrows. The countries listed are: Antigua and Barbuda, Argentina, Barbados, Belize, Bolivia, Brazil, Canada, Chile, Colombia, Costa Rica, Cuba, Dominica, Dominican Republic, Ecuador, El Salvador, Grenada, Guatemala, Guyana, Haiti, Honduras, Jamaica, Mexico, Nicaragua, Panama, Paraguay, Peru, Saint Kitts & Nevis, Saint Lucia, Saint Vincent & the Grenadines, Suriname, The Bahamas, Trinidad & Tobago, United States of America, Uruguay, and Venezuela.

The main content area is divided into several sections:

- Forum:** A space for the exchanging of ideas and experiences. It features an illustration of two people talking.
- Admin Announcements:** A section titled 'Funcionalidades Basicas'.
- Private messaging:** A section titled 'Private Messages' with a status of 'no new'.
- Latest Forum Posts:** A list of recent forum posts, including:
  - Cursos necesarios para iniciar un CSIRT:** In Main Forum / Education and training, posted 4 months 2 weeks ago.
  - Que opinan de ossim:** In Main Forum / Intrusion Detection.
- Partner Alert:** A section titled 'LACNIC\_Partner' with the heading 'LACNIC ALERTA DE VIRUS'. It contains a post from Tuesday, 03 February 2015 20:13, stating: 'Hemos estado recibiendo varios reportes de nuestros miembros sobre un virus que ...'. Below the text is a 'Read more' link.
- CSIRT\_VENEZUELA:** A section titled 'ESQUEMA DE SEGUIMIENTO'.
- Recent Downloads:** A list of recent forum posts with download counts:
  - Jamaica Strategy!!:** 03 February 2015, 3 downloads.
  - Senal:** 03 December 2014, 3 downloads.
  - Id icon:** 03 December 2014.
  - Ossec rules:** 15 October 2014, 4 downloads.
  - OWASP Testing Guide V4:** 30 September 2014.

## Servicios Básicos



### Foro

- taxonomía
- Ticket Management
- Log Analysis
- ...



### CSIRTs noticias

- Reportes de vulnerabilidades xxx
- Boletines de seguridad xxxx
- Reglas de monitoreo
- ...



### Librería

- Procedimientos de evaluación
- Cursos de CSIRT
- Procedimientos para levantamiento de info
- Herramientas para detección de defacement
- ...



### Directorio

- Web Security skills
- Database skills
- Incident handling
- system administration
- ...



CSIRTamericas.org



CSIRTamericas.org

Servicios especializados


Algunas funciones esperadas

Servicios de alertas

- ✓ Integración en tiempo real con fuentes de alertas (sources privados)
- ✓ Integración en tiempo real con fuentes de alertas generadas por los CSIRT de la región
- ✓ Reportes a la medida por región y por país miembro
- ✓ Generación de alertas tempranas

## Servicios especializados

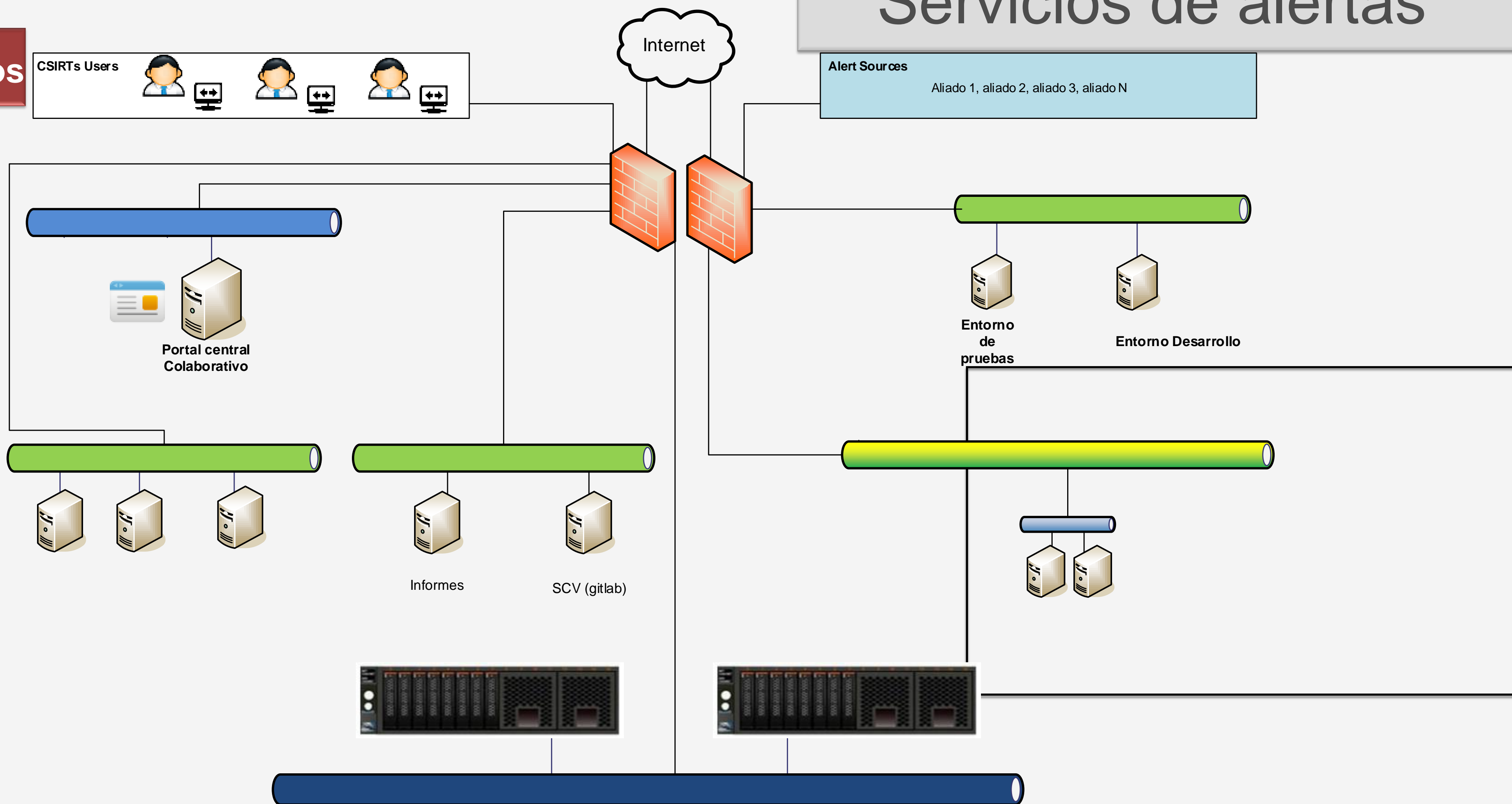
CSIRTs Users



Alert Sources

Aliado 1, aliado 2, aliado 3, aliado N

✓ Alertas tempranas (testing)  
Alertas 7x24



## Servicios especializados

## Visión – caso ejemplo

### Defacement

Prueba piloto

IP | Deface | tec | firma

Múltiples fuentes y formatos

Trending alerts

Aliado regional

Info from Botnets



Possible #Operacion detectada  
IRC, Pastebin, twitter, evidencias

CSIRT xxx

Situación regional



Eventos involucrados con otros países



Eventos que pudieran pasarme

Correlación y distribución

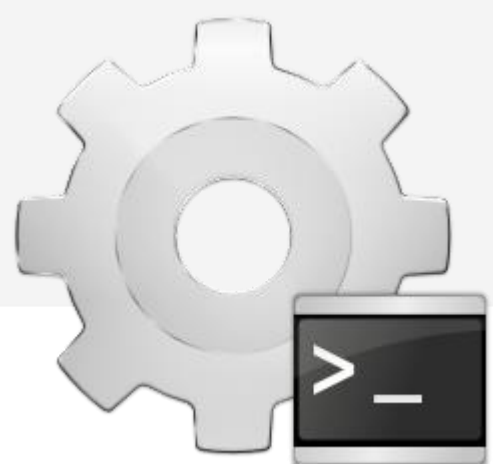


Eventos que me afectan directamente

- CSIRT National A
- CSIRT Gov B
- CSIRT Policia C
- CSIRT Militar C

## Servicios especializados

Acceso



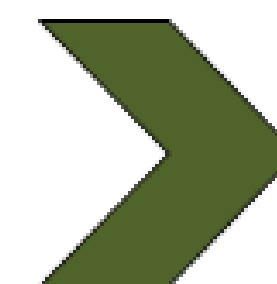
Acceso restringido por CSIRT



## Servicios de alertas

Source A

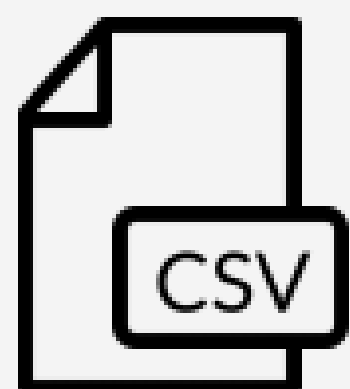
Date	notifier	Domain	Redefacement	Type	OS	mirror
xxxx	hack	www.aa.aa	Redefacement	Government	Linux	http:xxxx
xxxx	hack	www.bb.bb	Redefacement	Government	Linux	http:xxxx
xxxx	hack	www.bb.bb	Redefacement	Government	Linux	http:xxxx



Source A - Files (countries)

Country A Country B Country C  
Country D Country E Country F  
Country I Country H Country N..





## Alertas directas

7x24

Raw text

CSV format

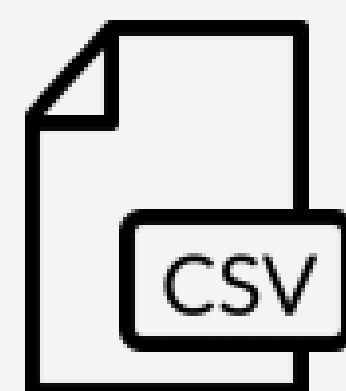
Alertas por país



Defacement  
...  
...

Entregable

Timestamp | notifier name | URL | affected domain IP | OS | Webserver



## Tendencias regionales

7x24

Raw text

CSV format

Tendencias por subregion



Defacement  
...  
...

Entregable

- Total Defacements per month
- Defacement sites: n #
- Sub Region TOP 7 attackers

- Sub region TOP 7 Common paths in affected websites
- Sub region TOP 7 Common methods
- Sub region TOP 7 Webserver affected

## Servicios especializados

[csirtamericas.org/defacement](https://csirtamericas.org/defacement)

directo a cada país

[csirtamericas.org/trending](https://csirtamericas.org/trending)

Trending por mes

- Centro
- Sur
- Norte
- Caribe

# Servicios de alertas

```

2016-05-14 12:00:21 Mr.Rch1 HTTP://trt.web.ve.173.256.171.31.Linux.Apache.Hell...just for fun!.Other Web Application
defaced/2016/05/14/trt.web.ve.mass.yes.published.homepage.26262093
2016-05-14 12:01:01 Mr.Rch1 HTTP://trtca.com.ve/173.236.121.31.Linux.Apache.Hell...just for fun!.Other Web Applicatio
2016-05-14 12:01:01 Mr.Rch1 HTTP://trtca.com.ve/trtca.com.ve.mass.yes.published.homepage.26262092
2016-05-17 01:09:16 langme cakep HTTP://castiblanco.com.ve/castiblanco.com.ve.regular.yes.published.homepage.26274631
2016-05-17 12:31:26 blockid http://www.grupompc.com.ve/148.163.67.131.Linux.Apache.I just want to be the best deface
defaced/2016/05/17/edder.com.ve/x.txt.mass.no.published.secondary.26275227
2016-05-17 12:31:26 blockid http://www.grupompc.com.ve/148.163.67.131.Linux.Apache.I just want to be the best deface
figuration > admin.mistake...defaced/2016/05/17/www.grupompc.com.ve/www.grupompc.com.ve.mass.no.published.homepage:
145
2016-05-17 12:31:26 blockid http://movil.grupompc.com.ve.148.163.67.131.Linux.Apache.I just want to be the best defa
figuration > admin.mistake...defaced/2016/05/17/movil.grupompc.com.ve/movil.grupompc.com.ve.regular.no.not public
homepage.26275446
2016-05-17 19:52:47 incidents HTTP://conatel.gob.ve.159.187.46.4.Linux.Apache.Political reasons.brute force attack.

```

```

# Total Central America Defacements per month | 8 countries | cr,pa,gt,do,ni,sv,h
n,bz
Defacement sites: 27

# Top 7 attackers for Central America
3 PhantomCrews
3 Nofawkx Al
3 Fallaga Team
2 RxR
2 Olive3r.Dark
2 D.R.S Dz Team
1 WILSHERE7

# Top 7 Common paths in affected websites (Certain types of patterns are excluded)
3 lang.tmp
2 drs.htm
2
1 xxx.htm
1 wp
1 wil.htm

# Top 7 Common methods (subjete)
9 known vulnerability (i.e. unpatched system)
5 Not available
3 Other Server intrusion
2 SQL Injection
2 Mail Server intrusion
2 admin.mistake
1 SSH Server intrusion

# Top 7 Common Webserver affected
21 Apache
2 nginx
1 Unknown
1 7.5
1 7.0
1

```

## Servicios especializados

### Alerts

Vulnerability: "jdownloads" | "joomla core"

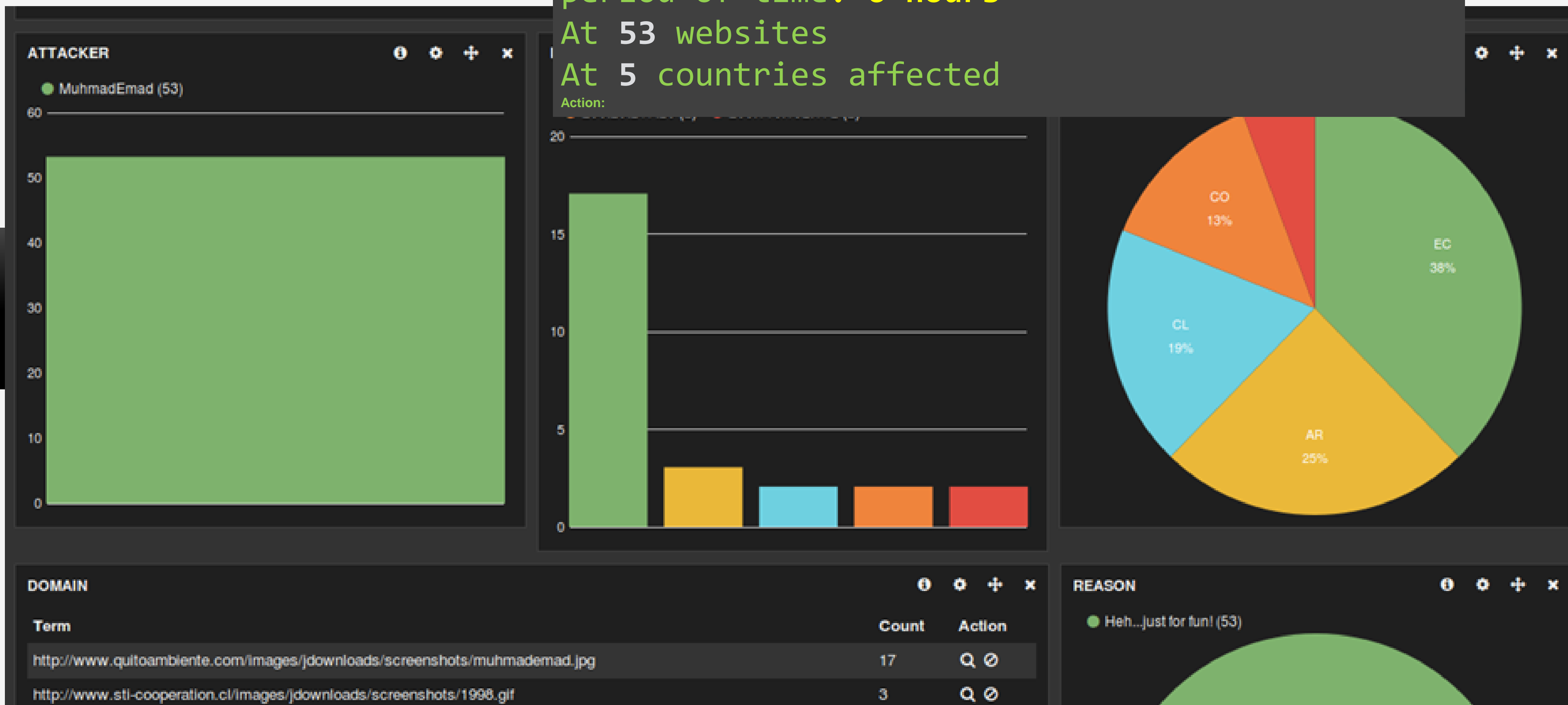
Same attacker : MuhmadEmad

period of time: 6 hours

At 53 websites

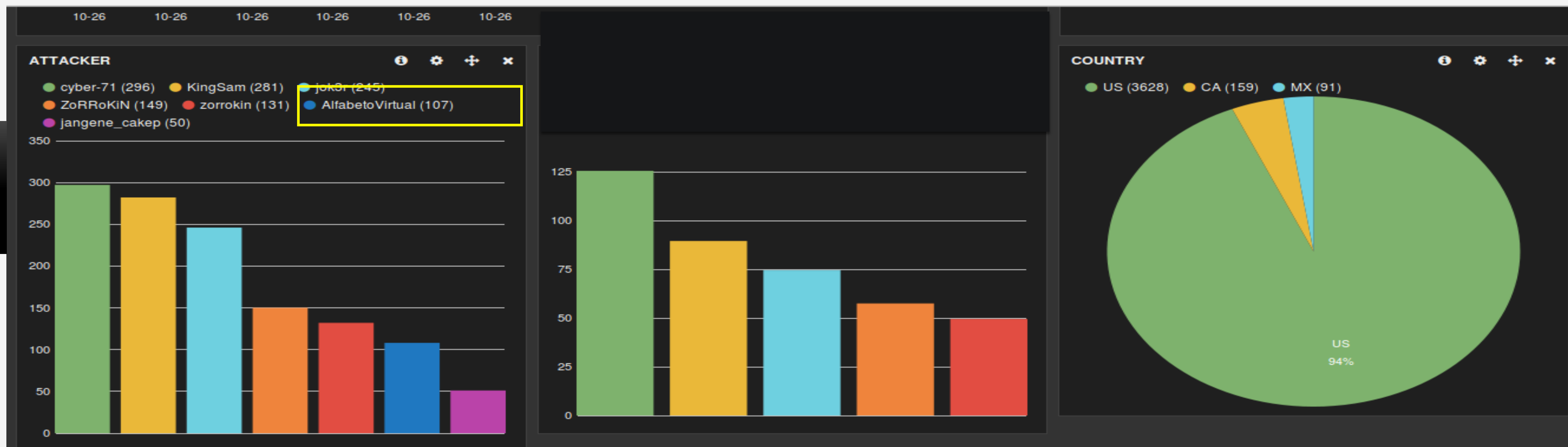
At 5 countries affected

Action:



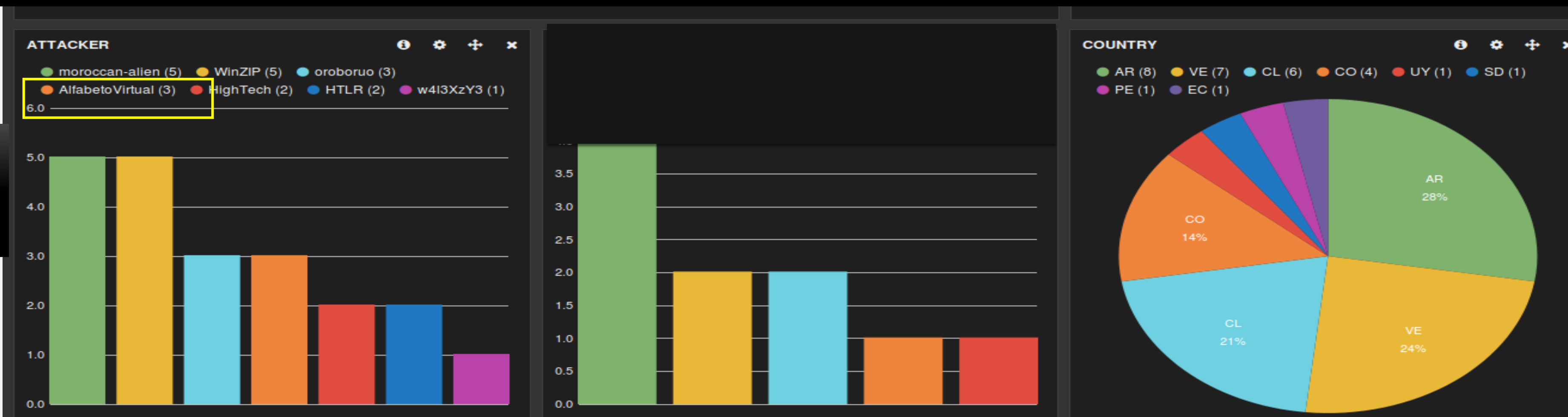
## Servicios especializados

## Norte



AlfabetoVirtual: continued attacks | AR,VE, CL, US, MX | Gov,gob sites

## Sur



# Casos de exito

## Servicios especializados

CSIRTsNET - Importante/Important

## Email



- CERT-MX
- CSIRT-Bolivia
- CSIRT Costa Rica
- CSIRT- Panama
- CSIRT-CL
- PECERT
- ECUACERT
- VenCERT
- CERT-PY
- CERTUy
- OAS
- CSIRT-GY

Estimados,

Varios estados miembros nos han notificado varios incidentes relacionados con la vulnerabilidad de "SQL injection" en portales Joomla "3.4.2 a 3.4.4", por lo que hacemos este aviso preventivo ya que muchas de sus comunidades hacen uso de este CMS.

<https://blog.sucuri.net/2015/10/joomla-3-4-5-released-fixing-a-serious-sql-injection-vulnerability.html>

<https://www.joomla.org/announcements/release-news/5634-joomla-3-4-5-released.html>

<https://www.trustwave.com/Resources/SpiderLabs-Blog/Joomla-SQL-Injection-Vulnerability-Exploit-Results-in-Full-Administrative-Access/>

Saludos Cordiales,

## Ejemplo de algunos CSIRT

### URGENT ALERT FROM GUYANA NATIONAL CIRT



The Guyana National Computer Incident Response Team has been advised by OAS/CICTE Cyber Security Technical Specialists of a serious vulnerability affecting Joomla 3.0 to 3.4.4 platforms.

Joomla is popularly used to manage and develop many websites in Guyana.

Websites within both the private and public sectors in Guyana have been targeted in the recent past and hackers have succeeded in defacing some websites because of exploits such as this.

All are advised to determine whether Joomla is being used within their organisations as Joomla websites (Versions 3.0 to 3.4.4) are vulnerable and require an urgent upgrade.

More details are posted on our [website](#).

# Beneficios

## Servicios especializados

- Totalmente colaborativo
- Construido para los CSIRT de la region
- Soportado por los CSIRT de la region
- OEA participa como supervisor

### OAS Hemispheric Technical NET

#### Individual benefits

Per CSIRT country



#### Reducing Cost



Alerts subscription  
6K per country per year  
Trusted Sources

#### Real time Comparison



Comparative country attacks  
Similar Hacking teams  
Similar behaviors

#### Improve incident Handling



CSIRTs Skill Directory  
Preventive actions  
Knowledge Base

#### Regional benefits

North, Central, South, Caribbean



#### Regional Correlation & Alerts



Same events in countries  
Early warnings  
Hacker team profiles  
Detect regional attacks  
So on..

#### Trending regional incidents



Most active attackers  
Most hack mode  
Most Web Server  
Number of affected sites  
So on...

#### Collaborative Working



Sharing projects  
Sharing incidents handling  
Sharing tools  
Sharing ideas, questions

#### Int'l & Partners benefits

Law enforcement, Int'l communities, private sector



#### Information for investigation



Attackers profiles  
Common vulnerabilities  
Common targets

#### Improve information exchange



Detect needs  
Trends attacks  
Improve Major multi-jurisdiction incidents handling

#### Coordination



Identify & consolidate resources  
Major incidents handling  
Standardized efforts

# Soporte hasta el momento

Ejecutado por:



Organización de los Estados Americanos | Más derechos para más gente

Financiado por:



Foreign & Commonwealth Office



CSIRTamericas.org

Colaboradores:



Subsecretaría del Interior CSIRT

Ministerio del Interior y Seguridad Pública



CyberSeg.com



# Organization of American States

## Diego Subero

Consultor Técnico en Seguridad Cibernética  
Comité Interamericano contra el Terrorismo  
Secretaría Multidimensional de Seguridad  
Organización de los Estados Americanos

1889 F St., NW  
Washington D.C., 20006

T: (202) 370 – 4885

E-mail: [dsubero@oas.org](mailto:dsubero@oas.org)  
Twitter: [@OEA\\_Cyber](https://twitter.com/OEA_Cyber)

[WWW.OAS.ORG/CYBER](http://WWW.OAS.ORG/CYBER)