Implementación del sistema de gestión de la red de la Universidad de Granma.

Manuel José Linares Alvaro* (cheche@udg.co.cu)
Javier Iglesias Barbán * (javier@udg.co.cu)
* Universidad de Granma, Bayamo, Cuba

Introducción

- Actualmente, los procesos de chequeo, monitoreo y supervisión, tanto a servicios suministrados a través de las redes como a los equipos y activos de TI, se hacen cada vez más necesarios y adquieren una nueva relevancia, debido al desarrollo sostenido y exponencial que presentan las tecnologías de la información.

Introducción.

- En la actualidad, la gestión en las redes, sobre todo, en aquellas organizaciones medianas y pequeñas resulta en una actividad que se descuida con frecuencia, esto es más común, en países en vías de desarrollo, hecho que conduce, casi siempre, al **deterioro paulatino en la calidad de los servicios** que éstas suministran.

Introducción

- Universidad de Granma.

Introducción. Problema.

- … carencia de un sistema de gestión que permita tener una visión global del estado de la red de la institución (UdG), y conocer en tiempo real y/o diferido, la situación de los servicios de sus principales nodos o centros de datos, su infraestructura y seguridad, el estado de los enlaces y equipos que componen la estructura fundamental de la red y la disponibilidad de los servicios brindados.

Introducción. Objetivos

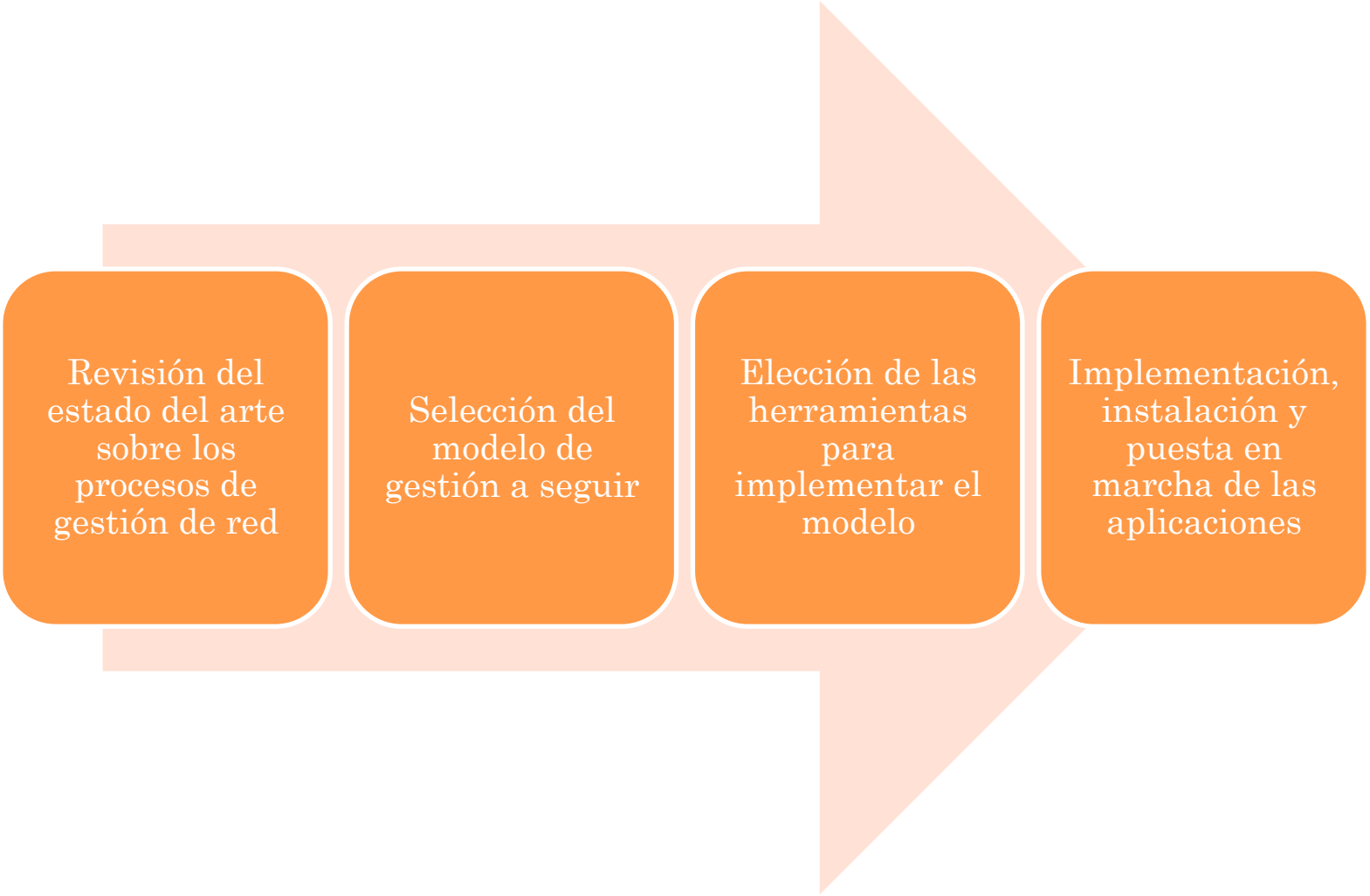
- **General:**
- Implementar un sistema de gestión y monitoreo para la red de la Universidad de Granma.

- **Específicos:**
- Seleccionar un modelo de gestión adecuado para la red de la Universidad de Granma.
- Implementar las herramientas de gestión que complementen el modelo.
- Demostrar, mediante la impementación, la factibilidad del uso de herramientas de gestión basadas en software libre.

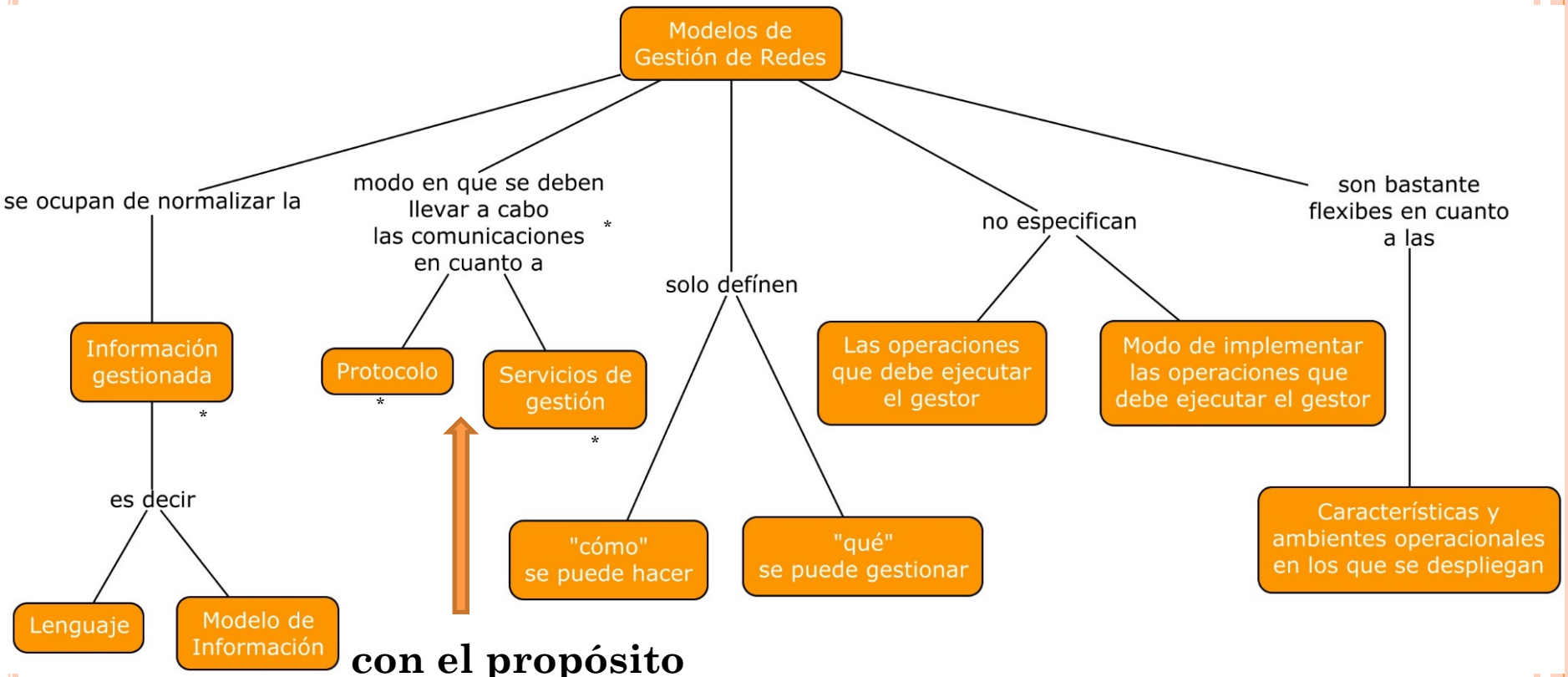
Metodología.

- Desarrollo del sistema de gestión de la UdG data de 2005. Se caracterizaba por:
  - Empleo de herramientas aisladas. (mrtg, nagios)
  - A partir de 2012 que la gestión de la red en la mencionada entidad, comenzó a diseñarse como un sistema organizado e integrador, basado en la aplicación de modelos respaldados por normas internacionales.
  - Todo el proceso de implementación, el cual incluye el perfeccionamiento, la selección y actualización de software, se ha extendido hasta la fecha actual.

Metodología. Etapas de la investigación



Metodología. Modelos de Gestión de redes.



con el propósito de conseguir interoperabilidad entre gestor y agentes

(Pérez, 2013), (Marrero & Hernández, 2016)

Selección del modelo para el sistema de gestión de la red.

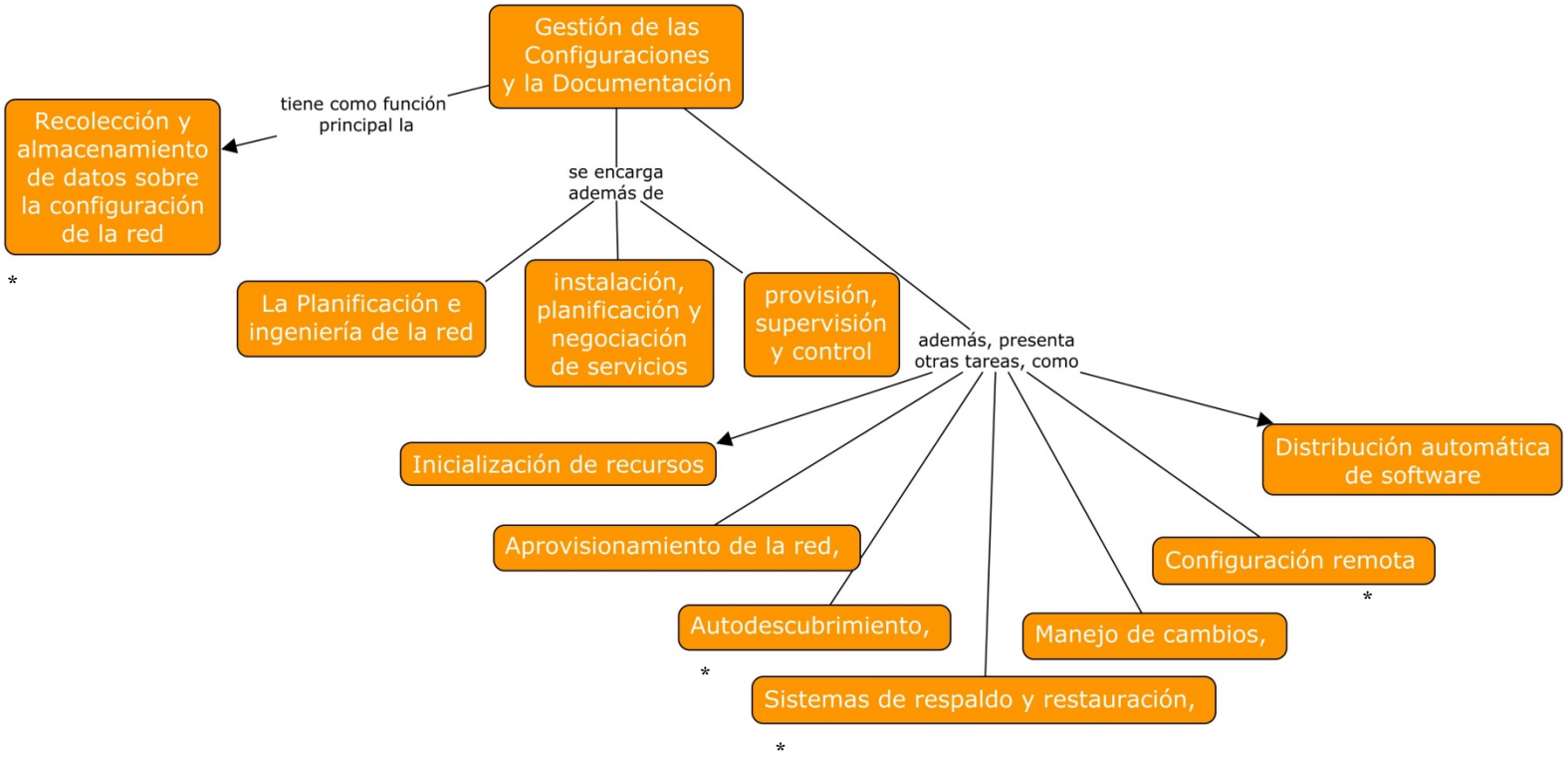
- Se analizaron varios modelos:
  - TMN, FCAPS, eTOM, COBIT e ITIL
- FCAPS, por:
  - facilidades que ofrece para establecer de manera sencilla, rápida y eficiente los diferentes procesos necesarios para implementar un adecuado sistema de gestión de red.
  - Por otra parte, este modelo, constituye uno de los que tiene mayor aceptación y uso. (Gómez & González, 2013)

Fault, Configuration, Accounting, Performance and Security

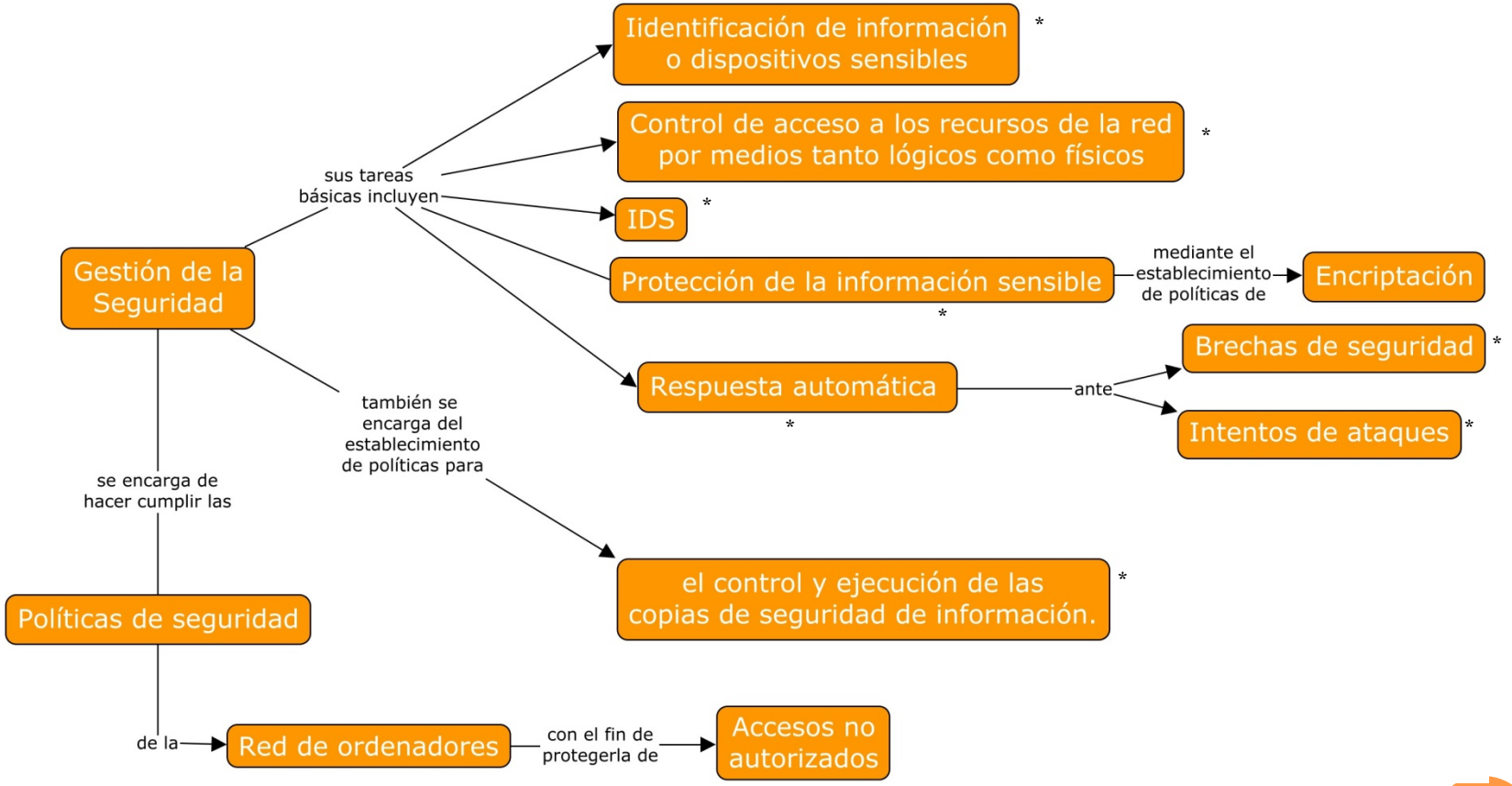
Information Technology Infrastructure Library o Librería de Infraestructura de Tecnologías de Información, conjunto de buenas prácticas de gestión de servicios, desarrollado por el "Office of Government Commerce" del Reino Unido y aceptado en todo el mundo como estándar de facto

División de los procesos de gestión en las redes. FCAPS, normas ISO

Gestión de Configuraciones y Documentación

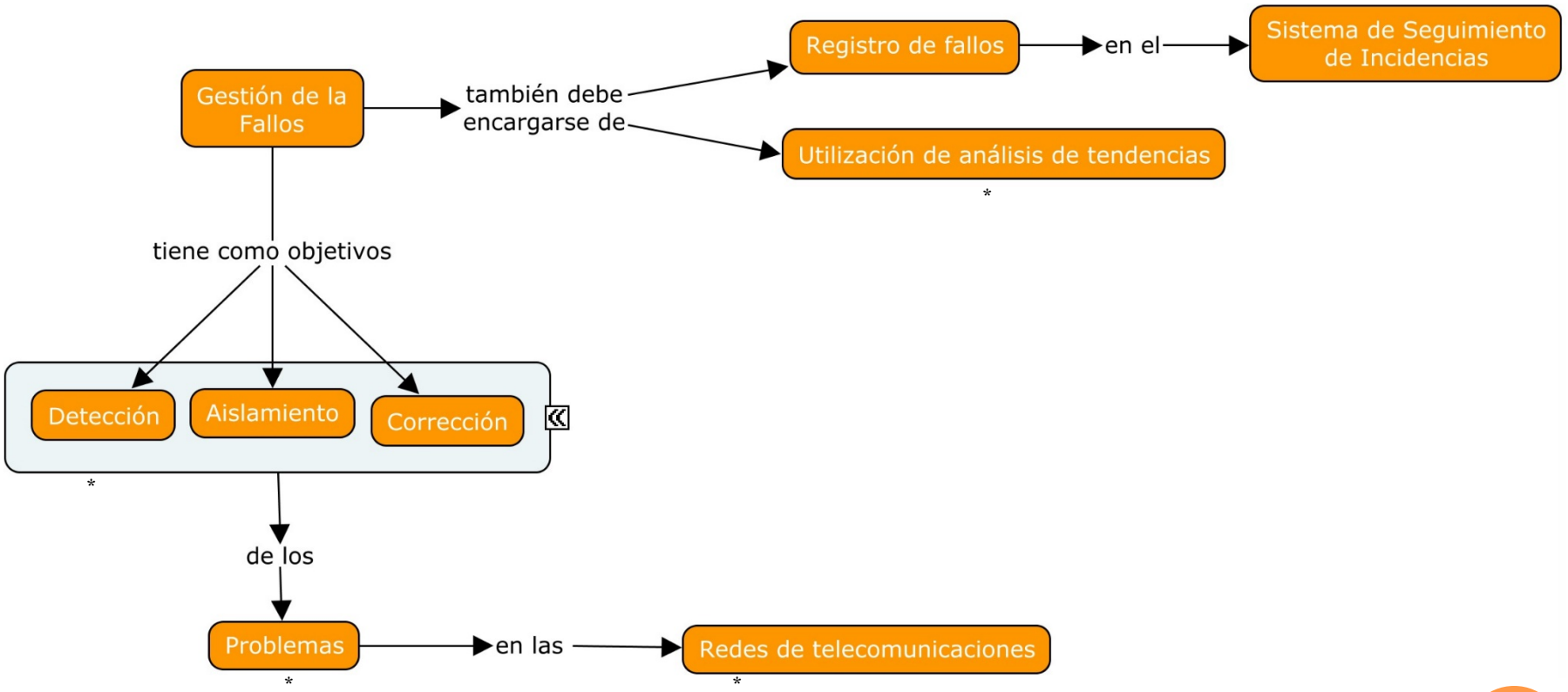


Gestión de seguridad.



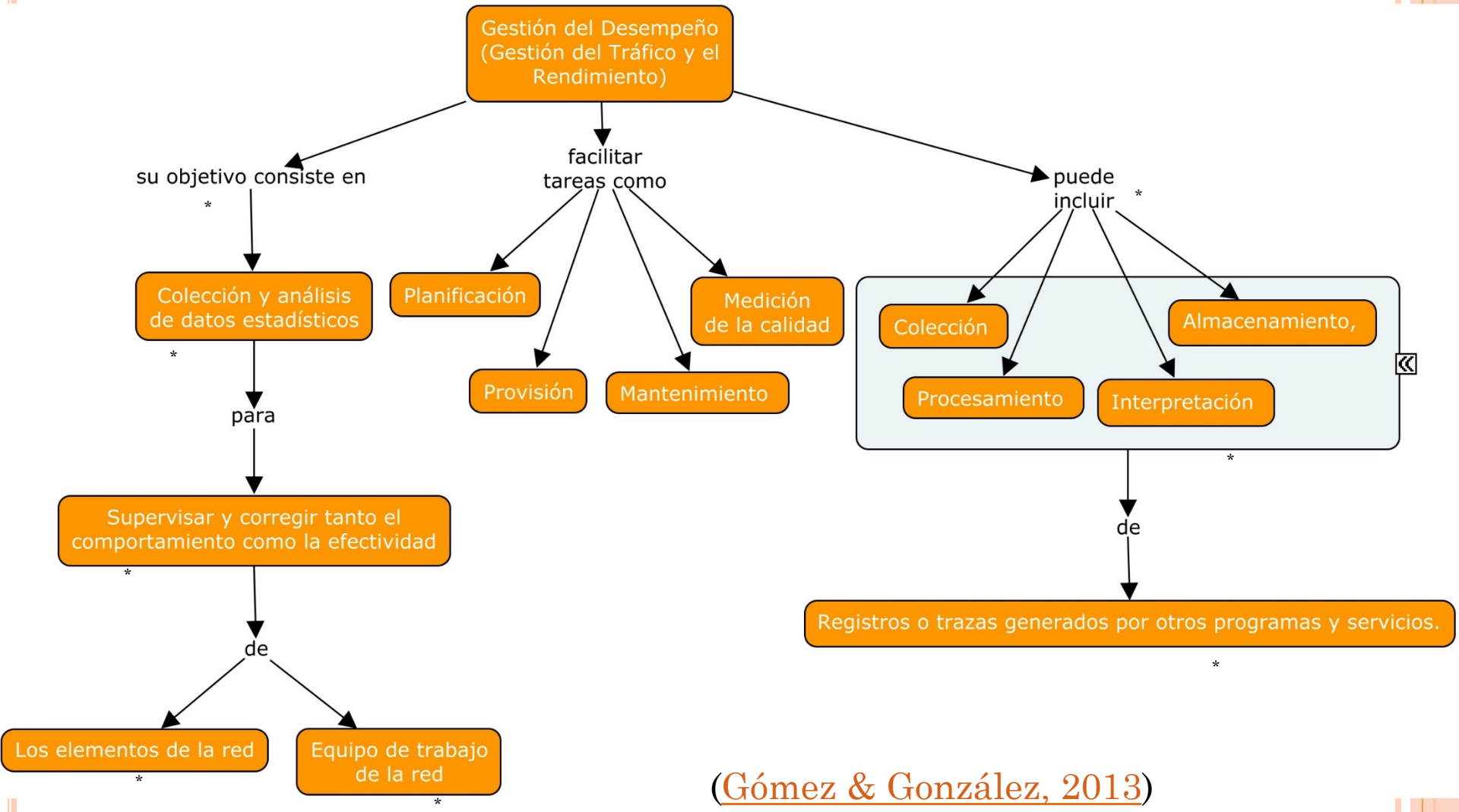
(Gómez & González, 2013)

Gestión de Fallas.



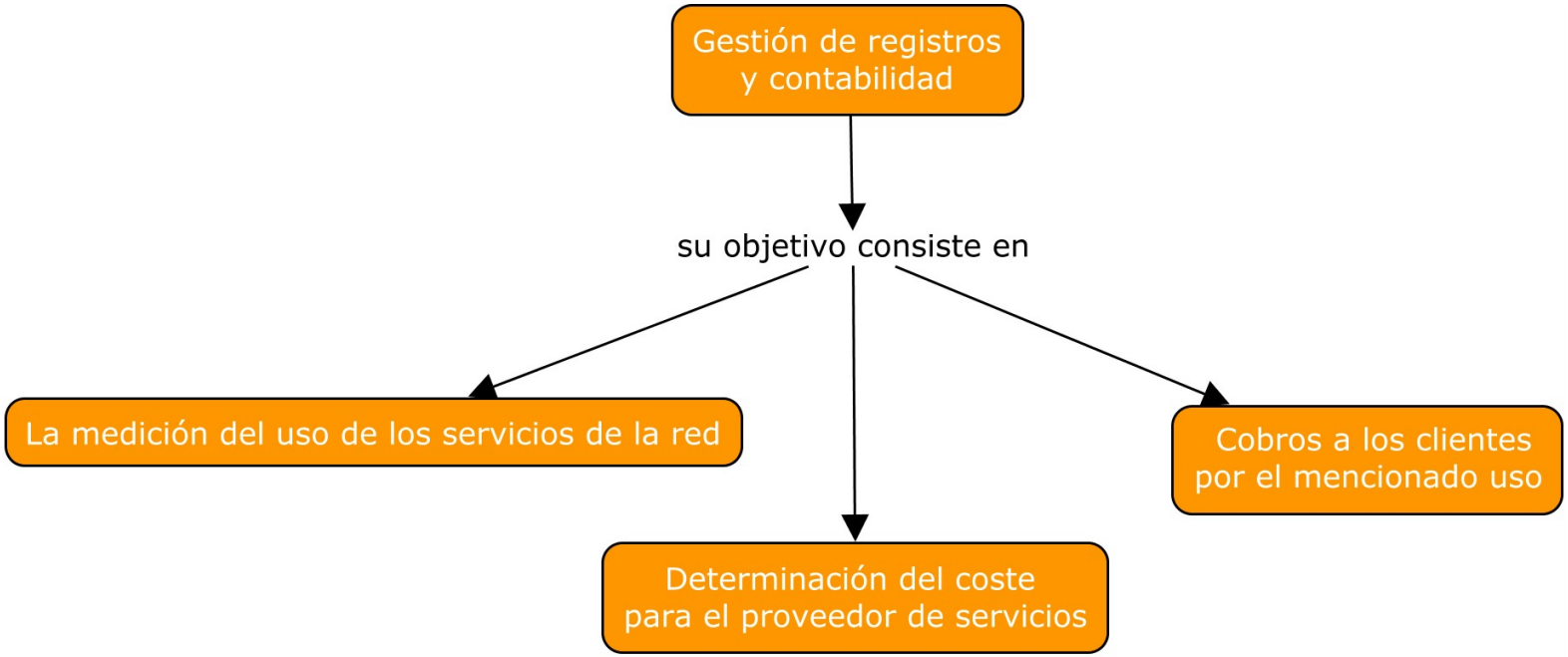
De forma que la red esté la mayor parte del tiempo disponible. (Gómez, 2013)

Gestión de tráfico y rendimiento.



(Gómez & González, 2013)

Gestión o control de los registros y Contabilidad.



last

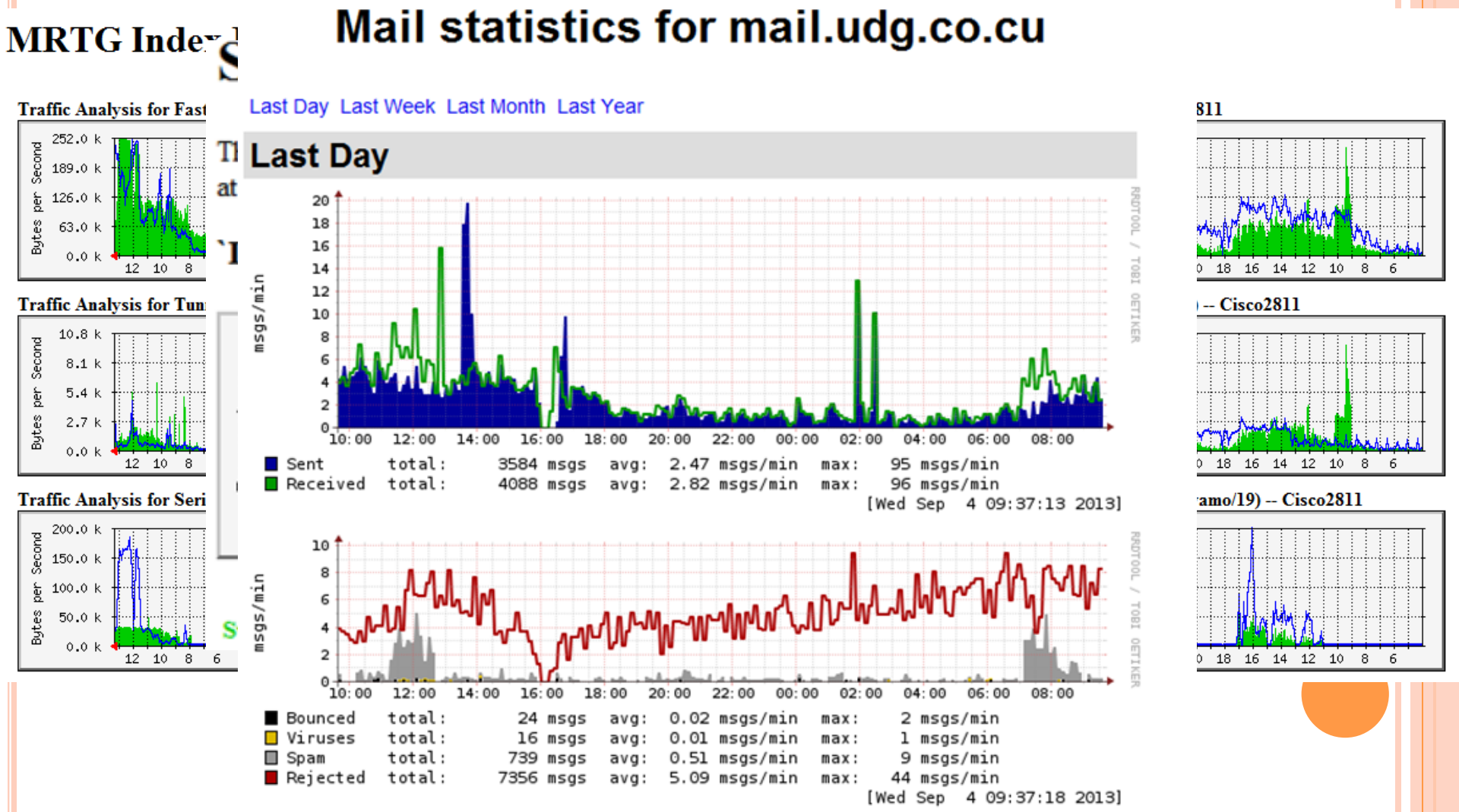
Selección e implementación de las herramientas de gestión. (Requisitos)

- Herramientas basadas Software libre y código abierto.
- Todas las aplicaciones deberían tener una Interface basada en HTML.
- Preferencia por software diseñado para sistemas operativos de tipo Linux.
- El software seleccionado debería contar con un amplio respaldo bibliográfico, con extensa experiencia en su utilización así como un elevado reconocimiento en cuanto a sus prestaciones.

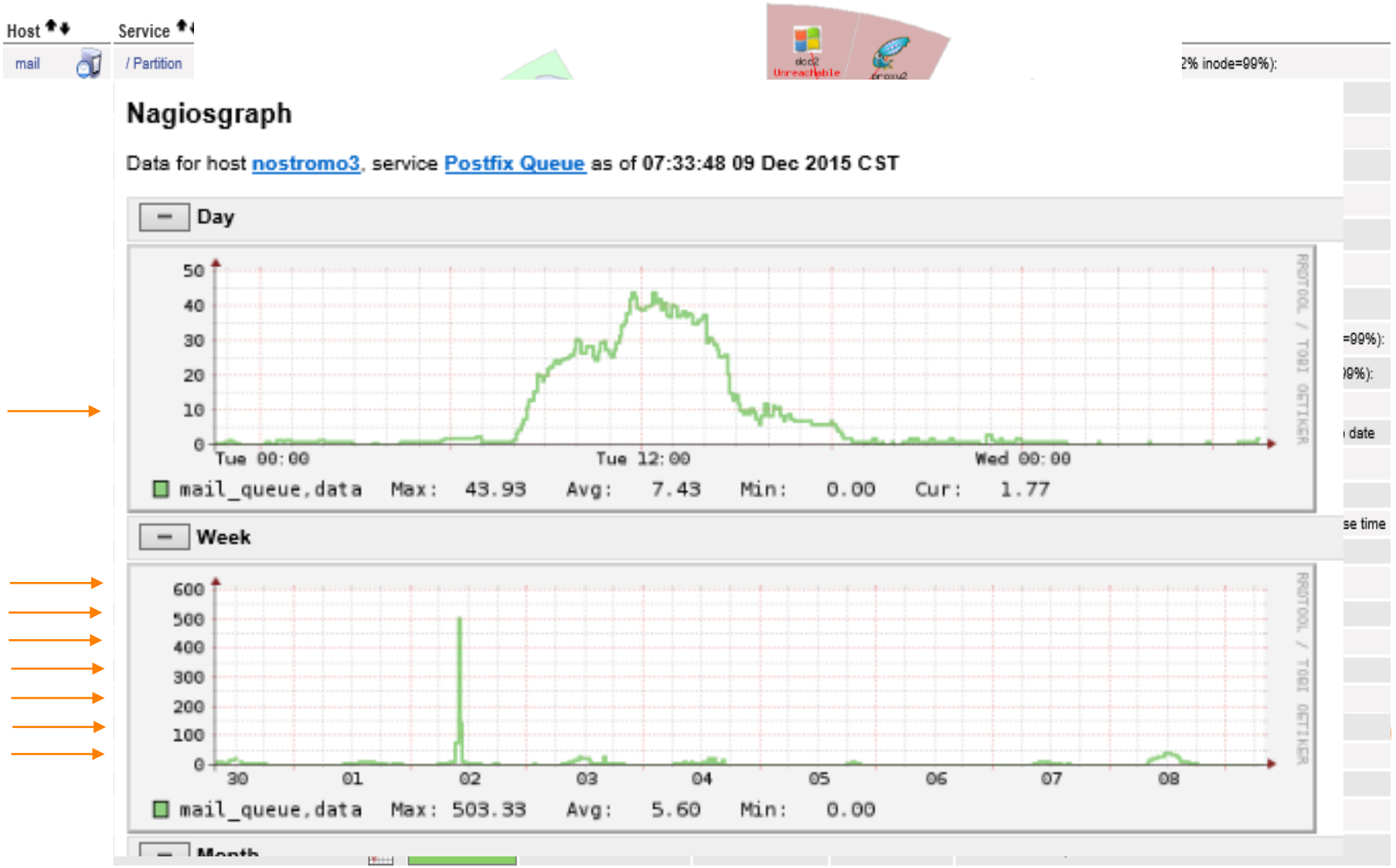
Tabla 1. Categorías en el sistema de gestión implementado, asociadas al software que se emplea para su implementación.

Categorías	Software o Aplicación empleado
Gestión de la configuración	NetDot, Bacula, OCS Inventory y Rancid
Gestión de Fallos	Nagios
Gestión de los registros y contabilidad	LightSquid, SARG, SQStat, FreeSA Webalizer, Sendmail analyzer y OCS Inventory
Gestión del desempeño	MRTG, Cacti, FlowViewer, NFsen+NFsight+SSHCUre, SmokePing, LibreNMS y Nagios
Gestión de Seguridad	NFsen+NFsight+SSHCUre, Flow Viewer, OSSIM, Bacula, SmokePing, MRTG, Cacti, Rancid y Nagios.

Caracterización de las principales aplicaciones seleccionadas.

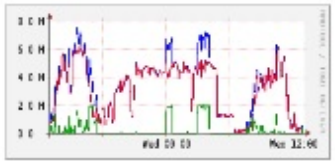


Caracterización de las principales aplicaciones seleccionadas.

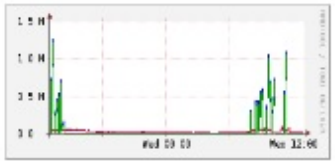


Profile: Internet_In

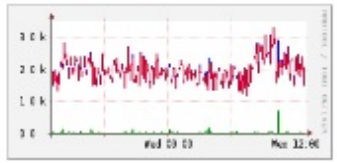
TCP



UDP



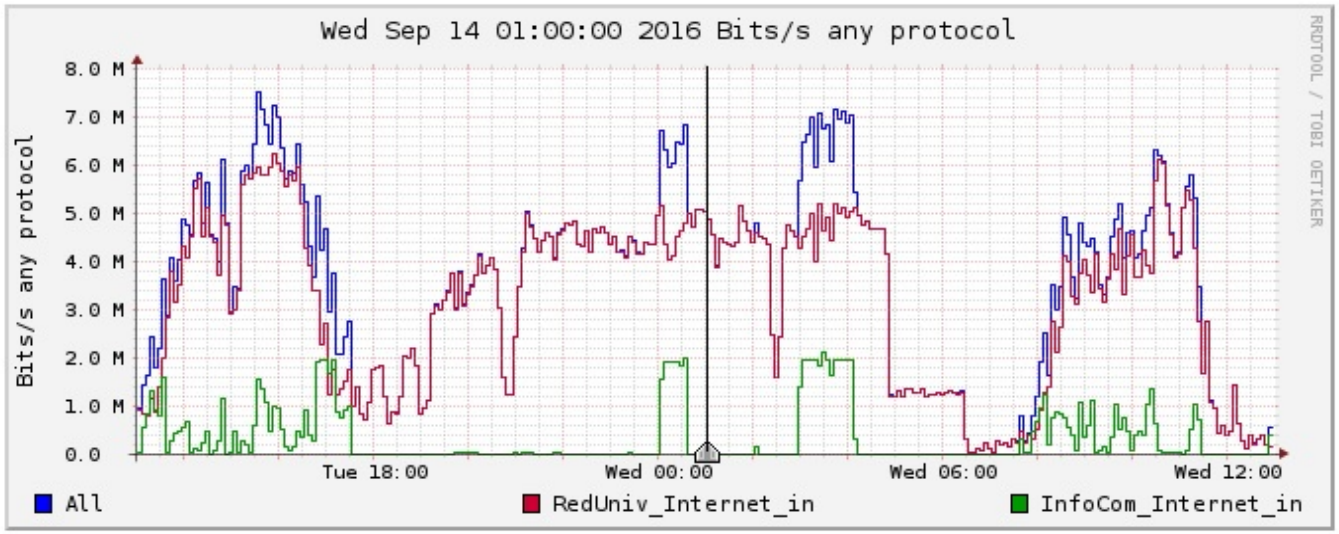
ICMP



other

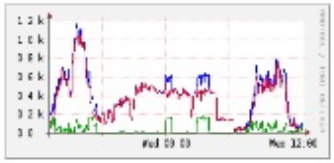
Profileinfo:

Type: continuous / shadow
Max: unlimited
Exp: never
Start: Jan 26 2016 - 14:45 CDT
End: Sep 14 2016 - 13:00 CDT

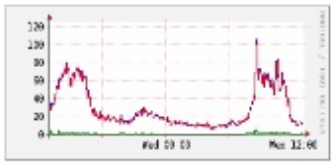


t_{start} 2016-09-14-01-00
t_{end} 2016-09-14-01-00

Packets



Flows



Select Single Timeslot | Display: 1 day | << | < | | | > | >> | >|

◉ Lin Scale ○ Stacked Graph
○ Log Scale ◉ Line Graph

Statistics timeslot Sep 14 2016 - 01:00

Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
☑ All	12.2 /s	2.8 /s	6.7 /s	2.6 /s	0.0 /s	450.6 /s	440.7 /s	6.7 /s	3.0 /s	0.2 /s	4.9 Mb/s	4.9 Mb/s	8.8 kb/s	2.0 kb/s	469.7 b/s
☑ RedUniv_Internet_in	12.0 /s	2.6 /s	6.7 /s	2.6 /s	0 /s	448.8 /s	439.1 /s	6.7 /s	3.0 /s	0 /s	4.9 Mb/s	4.9 Mb/s	8.8 kb/s	2.0 kb/s	0 b/s
☑ InfoCom_Internet_in	0.2 /s	0.2 /s	0.0 /s	0.0 /s	0.0 /s	1.9 /s	1.7 /s	0.0 /s	0.0 /s	0.2 /s	3.3 kb/s	2.8 kb/s	1.9 b/s	1.6 b/s	469.7 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	24.4 /s	5.6 /s	13.4 /s	5.3 /s	0.0 /s	901.3 /s	881.4 /s	13.4 /s	6.0 /s	0.5 /s	9.8 Mb/s	9.8 Mb/s	17.6 kb/s	4.0 kb/s	939.4 b/s

All None Display: ○ Sum ◉ Rate

Profile: Internet_SMTP_IN_OUT

TCP

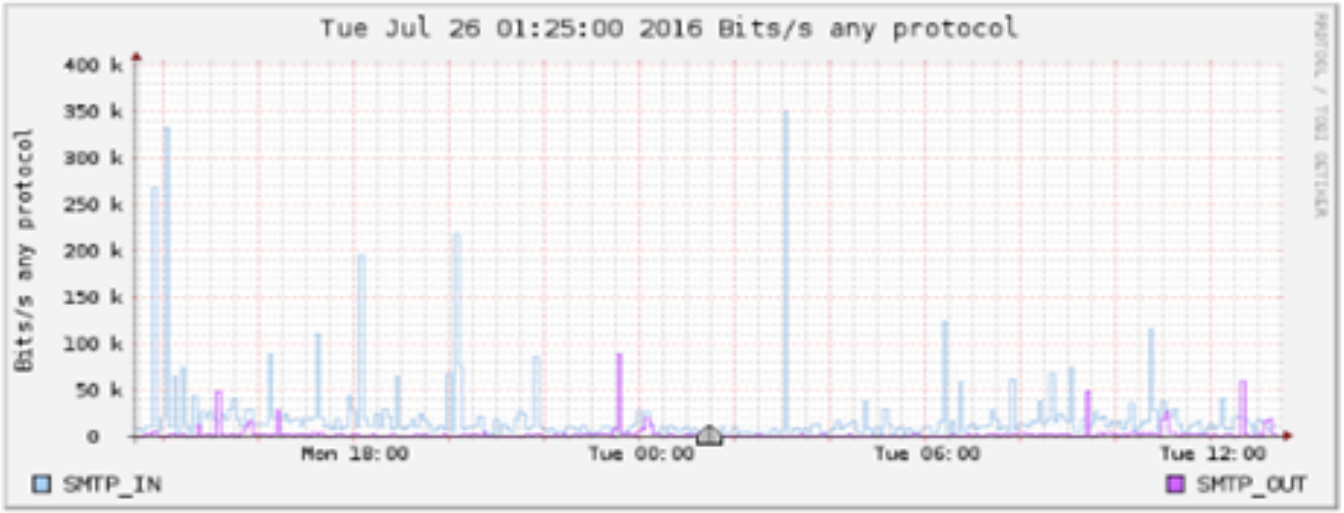
UDP

ICMP

other

Profileinfo:

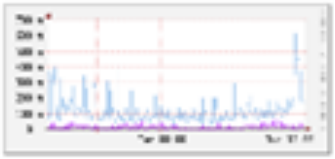
Type: continuous
Max: 256.0 MB
Exp: 60 days 0 hours
Start: May 29 2016 - 16:00 CDT
End: Jul 26 2016 - 13:25 CDT



t_{start} 2016-07-26-01-25
t_{end} 2016-07-26-01-25

Packets

Flows



Select Single Timeslot Display: 1 day << < | ^ > >> >|

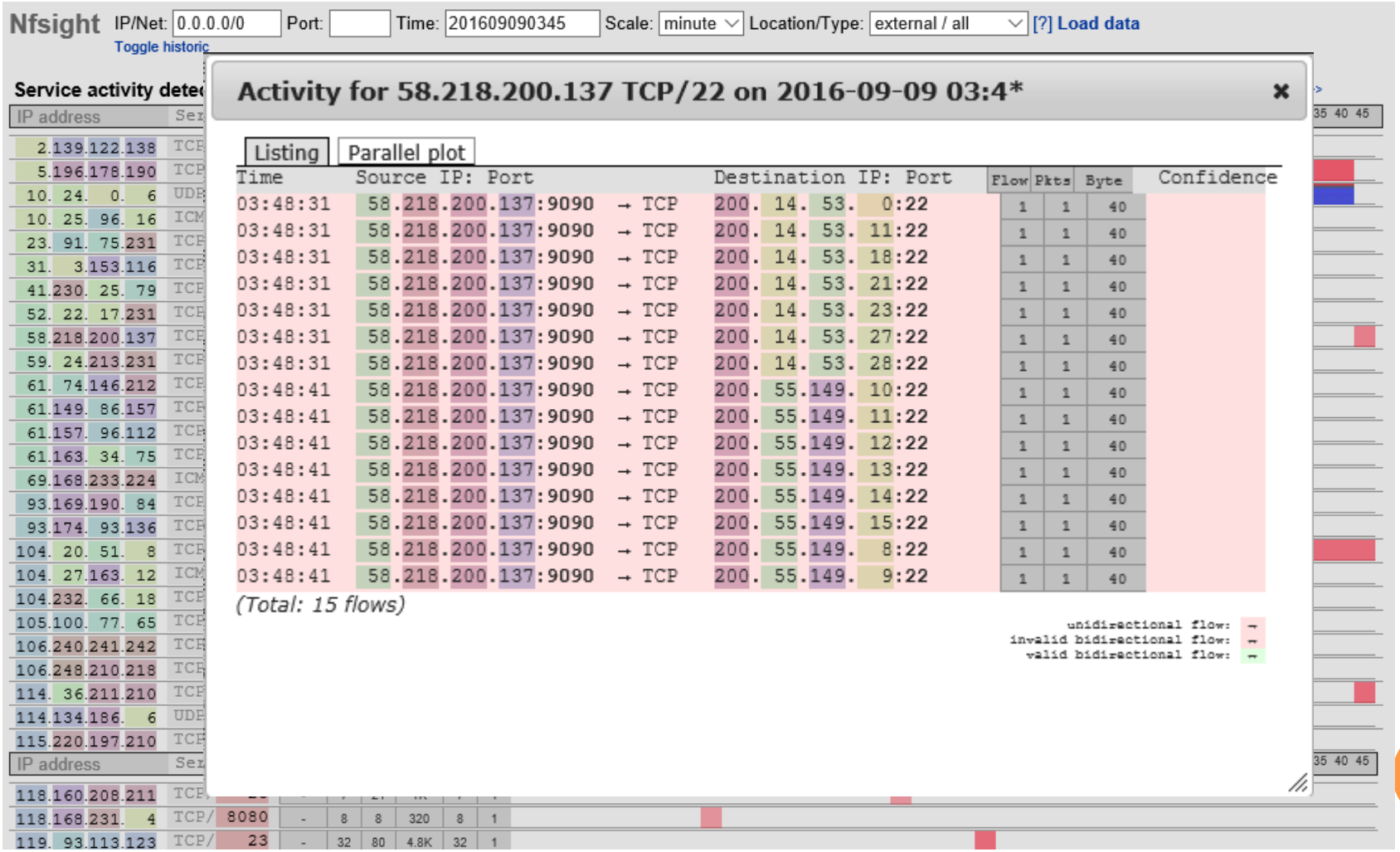
(•) Lin Scale ( ) Stacked Graph
( ) Log Scale (•) Line Graph

Statistics timeslot Jul 26 2016 - 01:25

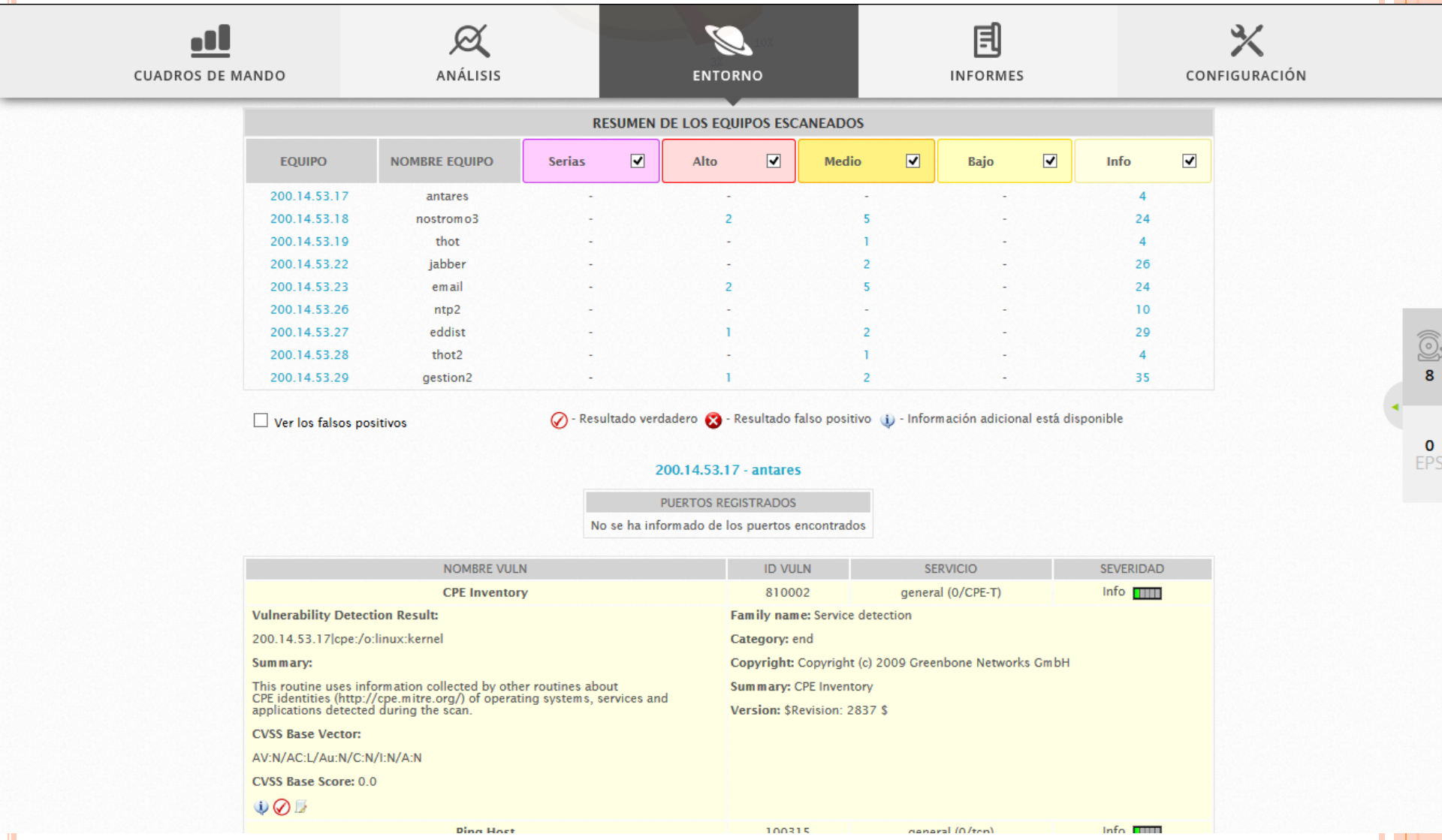
Channel:	Flows:					Packets:					Traffic:				
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
☑ SMTP_IN	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	0.8 /s	0.8 /s	0 /s	0 /s	0 /s	2.6 kb/s	2.6 kb/s	0 b/s	0 b/s	0 b/s
☑ SMTP_OUT	0.0 /s	0.0 /s	0 /s	0 /s	0 /s	0.2 /s	0.2 /s	0 /s	0 /s	0 /s	1.4 kb/s	1.4 kb/s	0 b/s	0 b/s	0 b/s
	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:	all:	tcp:	udp:	icmp:	other:
TOTAL	0.1 /s	0.1 /s	0 /s	0 /s	0 /s	1.0 /s	1.0 /s	0 /s	0 /s	0 /s	4.0 kb/s	4.0 kb/s	0 b/s	0 b/s	0 b/s

All None Display: ( ) Sum (•) Rate

Caracterización de las principales aplicaciones seleccionadas.



CARACTERIZACIÓN DE LAS PRINCIPALES APLICACIONES SELECCIONADAS.



Caracterización de las principales aplicaciones seleccionadas.

Escritorio | Director | Tarea | Pool/Volumen | Cliente | Almacenaje | Logbook | Ayuda

Ultima Actualización: Mon, 25 Jul 2016 10:46:06 -0400
Actualizar cada 300 segundos

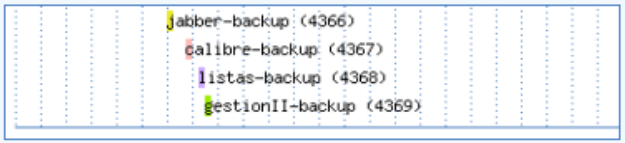
Tareas Programadas (en las próximas 24 horas)

Nivel	Tipo	Prioridad	Programado	Tarea	Volumen
Incremental	Backup	11	25-Jul-16 16:30	antares-backup	nodoBayamoAntares-0113
Incremental	Backup	11	25-Jul-16 16:40	ossim-backup	Ossim-0133
Incremental	Backup	11	25-Jul-16 16:50	eddist-backup	eddist-0027
Incremental	Backup	11	25-Jul-16 17:20	proxy-backup	proxymediaserver-0190
Incremental	Backup	11	25-Jul-16 17:35	mediaserver-backup	proxymediaserver-0190
Incremental	Backup	11	25-Jul-16 17:50	proxy1-backup	UdG-0083
Incremental	Backup	11	25-Jul-16 18:10	www-backup	MailWWW-0188
Incremental	Backup	11	25-Jul-16 18:55	db-backup	db-0134
Incremental	Backup	11	25-Jul-16 19:10	backup-backup	Backup2-0021
Incremental	Backup	11	25-Jul-16 19:30	mailrelayer-backup	MailWWW-0188
Incremental	Backup	11	25-Jul-16 19:45	gestion-backup	gestion-0118
Incremental	Backup	11	25-Jul-16 20:30	backup_udg-backup	UdG-0083
Incremental	Backup	11	25-Jul-16 20:45	nostromo3-backup	Nostromo3-0064
Incremental	Backup	11	26-Jul-16 06:00	jabber-backup	jabber-0153
Incremental	Backup	11	26-Jul-16 06:45	calibre-backup	calibre-0141
Incremental	Backup	11	26-Jul-16 07:15	listas-backup	listas-0174
Incremental	Backup	11	26-Jul-16 07:30	gestionII-backup	gestion-0172

Tareas Terminadas (ejecutadas en las últimas 24 horas)

Id	Tarea	Estado	Nivel	Archivos	Bytes	Errores
4362	calibre-backup	OK	D	0	0	-
4363	listas-backup	OK	D	425	44.5 MB	-
4364	jabber-backup	OK	D	138	124.4 MB	-
4365	gestionII-backup	OK	D	8,135	884.6 MB	-
4366	jabber-backup	OK	I	15	414 KB	-
4367	calibre-backup	OK	I	0	0	-
4368	listas-backup	OK	I	36	110 KB	-
4369	gestionII-backup	OK	I	353	864.8 MB	-

Línea de tiempo para la fecha 2016-07-25



Tareas con errores (últimos 7 días)

Id	Tarea	Estado	Nivel	Archivos	Bytes	Errores	Fin
4273	www-backup	Completado exitosamente	I	93	26.6 MB	2	2016-07-18 18:10:20
4276	mailrelayer-backup	Completado exitosamente	I	34	749 MB	1	2016-07-18 19:31:40
4277	gestion-backup	Completado exitosamente	I	2,196	181.5 MB	48	2016-07-18 19:47:18

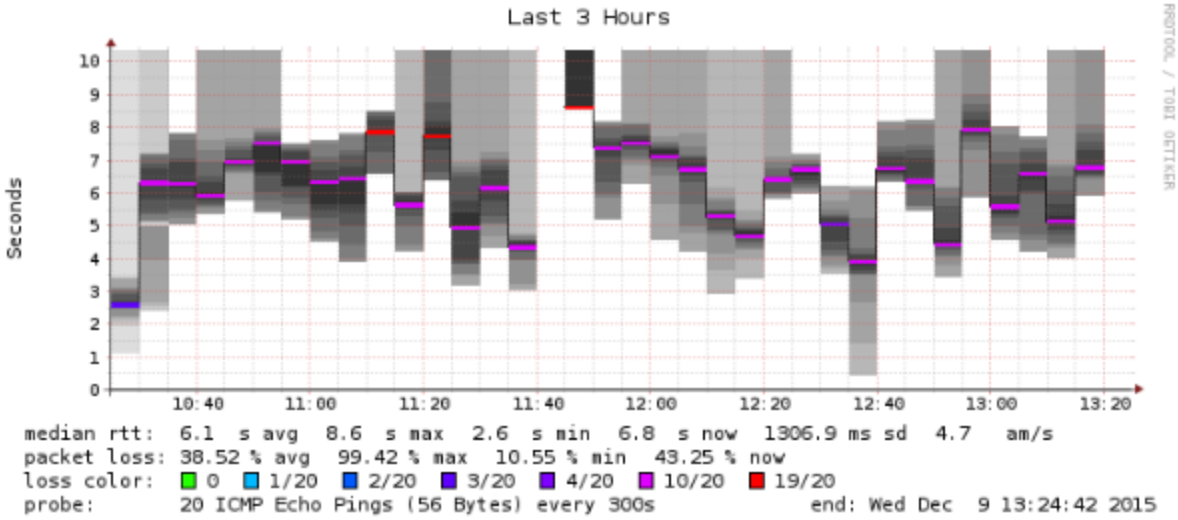
Logged in as Guest

SmokePing Targets:

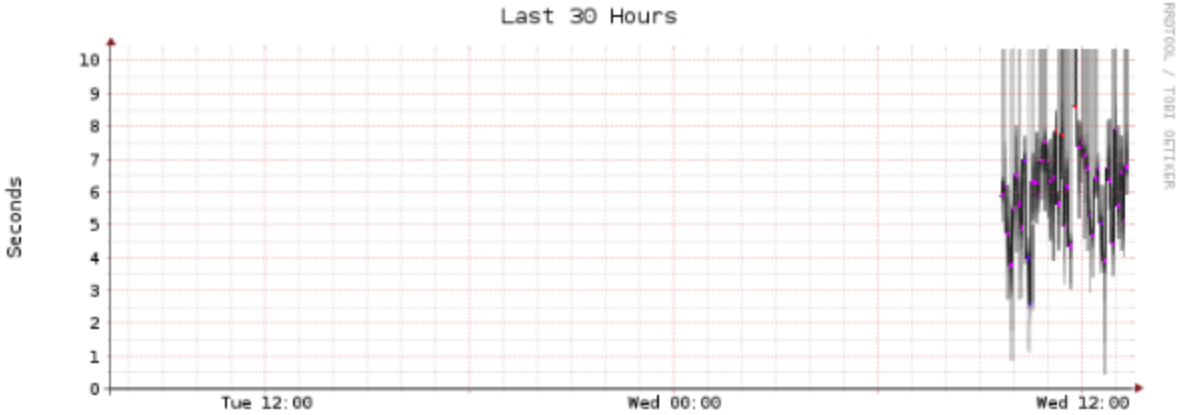
Filter:

- Charts
- Local Network Monitoring and Management
- Servers
- Switches
- Routers
  - SUMs
    - Bayamo
    - EaD
    - Rio_Cauto
    - Cauto_Cristo
    - Jiguani
    - Yara
    - Manzanillo
    - Campechuela
    - Medialuna
    - Niquero
    - Pilon
    - Maso
    - Buey Arriba
    - Guisa
  - cisco2911
  - cisco2811
  - elektra
  - gwcamp2
  - pfomz
  - fces
  - fcf
- Local HTTP Responses
- Remote HTTP Response
- DNS Latency

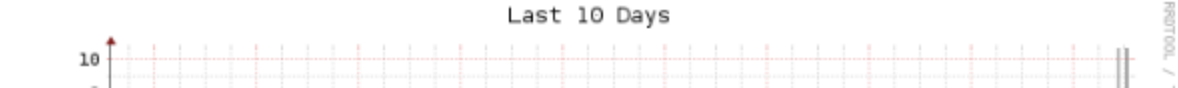
Sede de Yara




```
median rtt:  6.1  s avg  8.6  s max  2.6  s min  6.8  s now  1306.9 ms sd  4.7   am/s
packet loss: 38.52 % avg  99.42 % max  10.55 % min  43.25 % now
loss color:  0  1/20  2/20  3/20  4/20  10/20  19/20
probe:       20 ICMP Echo Pings (56 Bytes) every 300s          end: Wed Dec  9 13:24:42 2015
```



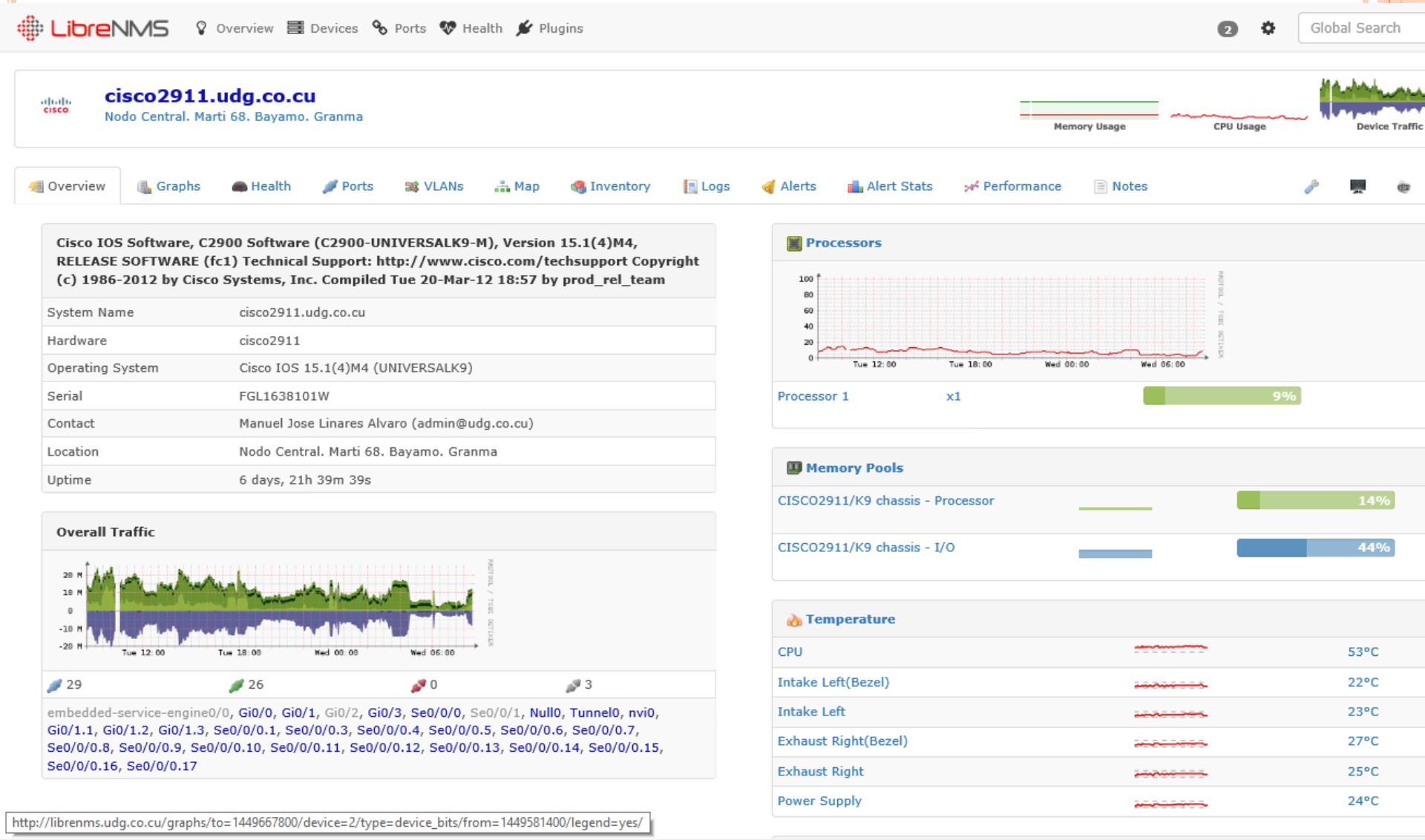

```
median rtt:  6.0  s avg  8.6  s max  2.6  s min  6.8  s now  1259.1 ms sd  4.8   am/s
packet loss: 36.19 % avg  99.42 % max  10.55 % min  43.25 % now
loss color:  0  1/20  2/20  3/20  4/20  10/20  19/20
probe:       20 ICMP Echo Pings (56 Bytes) every 300s          end: Wed Dec  9 13:24:42 2015
```



Caracterización de las principales aplicaciones seleccionadas.

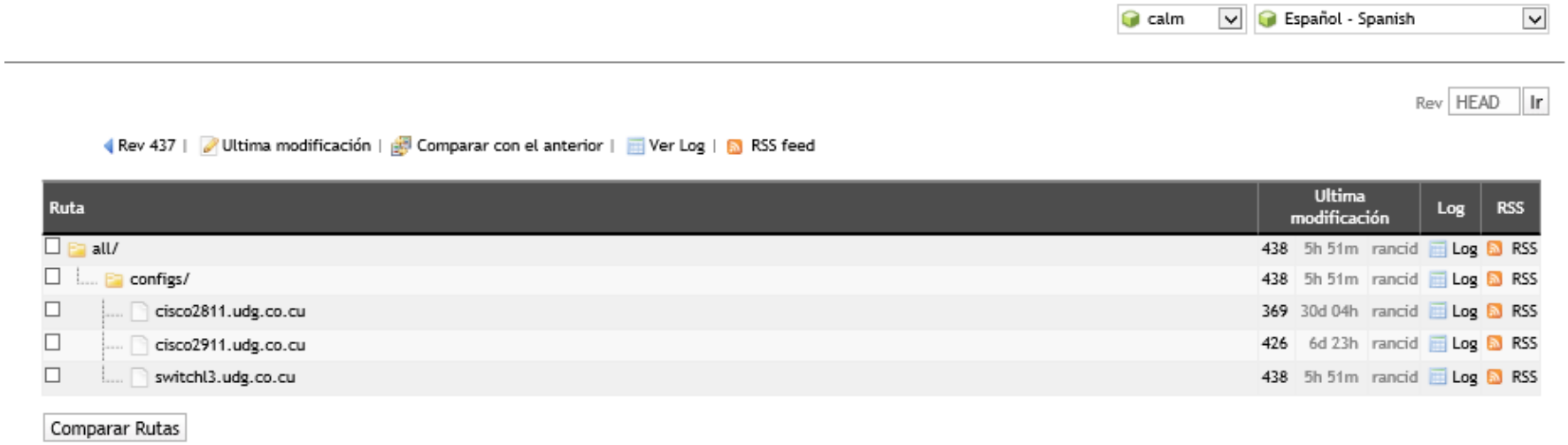
- **Open Computer and Software Inventory Next Generation** (OCS-NG).
- Software libre para gestionar inventarios de los activos de TI.
- Notifica, vía email, sobre cambios en el software y hardware en los equipos monitorizados.
- Actualmente todos los equipos y tecnologías IT de la UdG, se encuentran registrados en este sistema.

Caracterización de las principales aplicaciones seleccionadas.



Caracterización de las principales aplicaciones seleccionadas.

- *Rancid (http://www.shrubbery.net/rancid/) y WebSVN (http://subversion.apache.org/).*



estos. (INSITE, 2018a), (Kinnet, N.A).

CONCLUSIONES.

- [illegible] justifican completamente todas las inversiones que se hagan para preservarla.