REDCAYLE Estado Actual

Grupos de Trabajo de RedIRIS

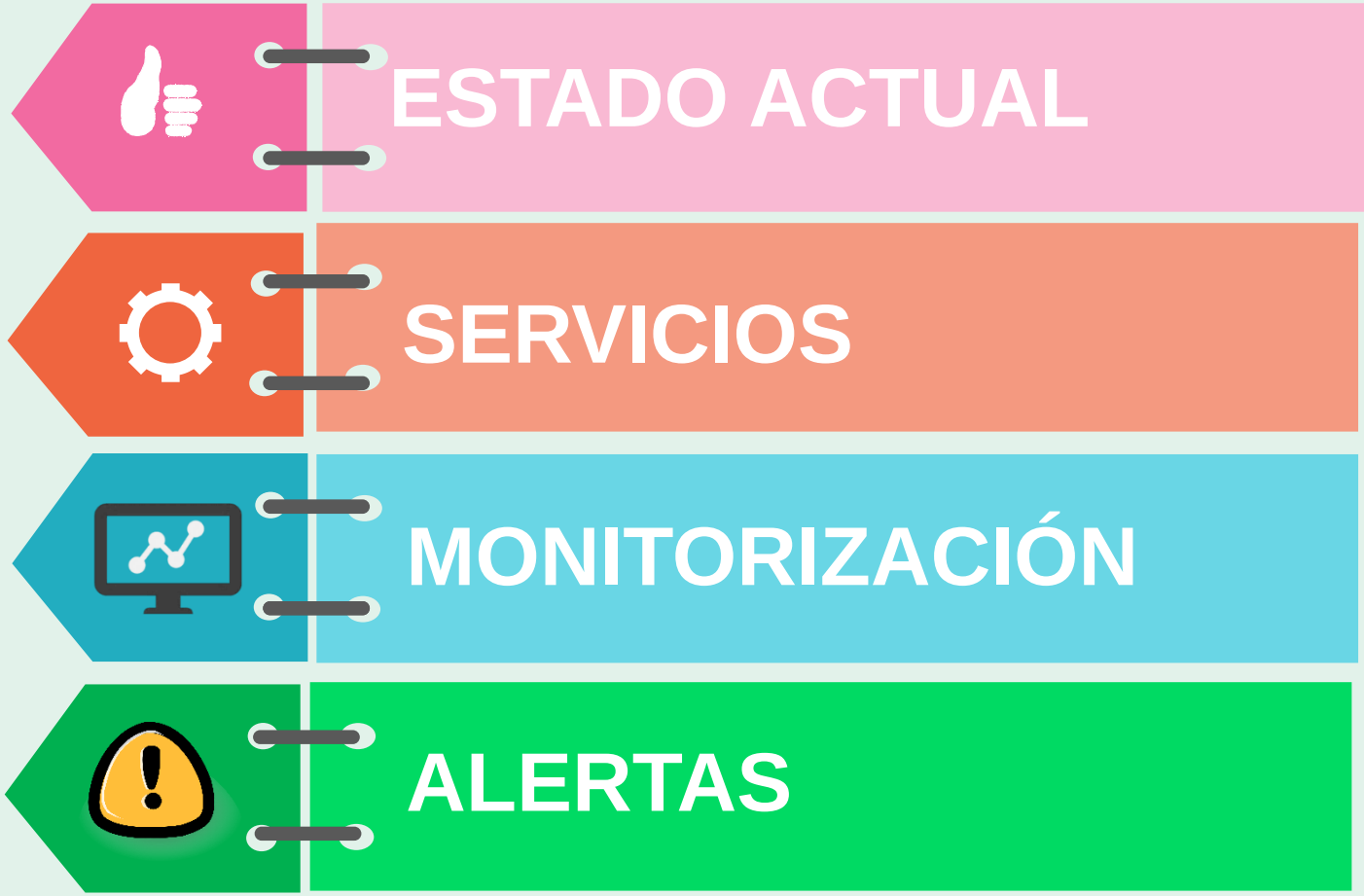
Mariví López López

28 Noviembre 2019
Universidad de Valladolid

RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

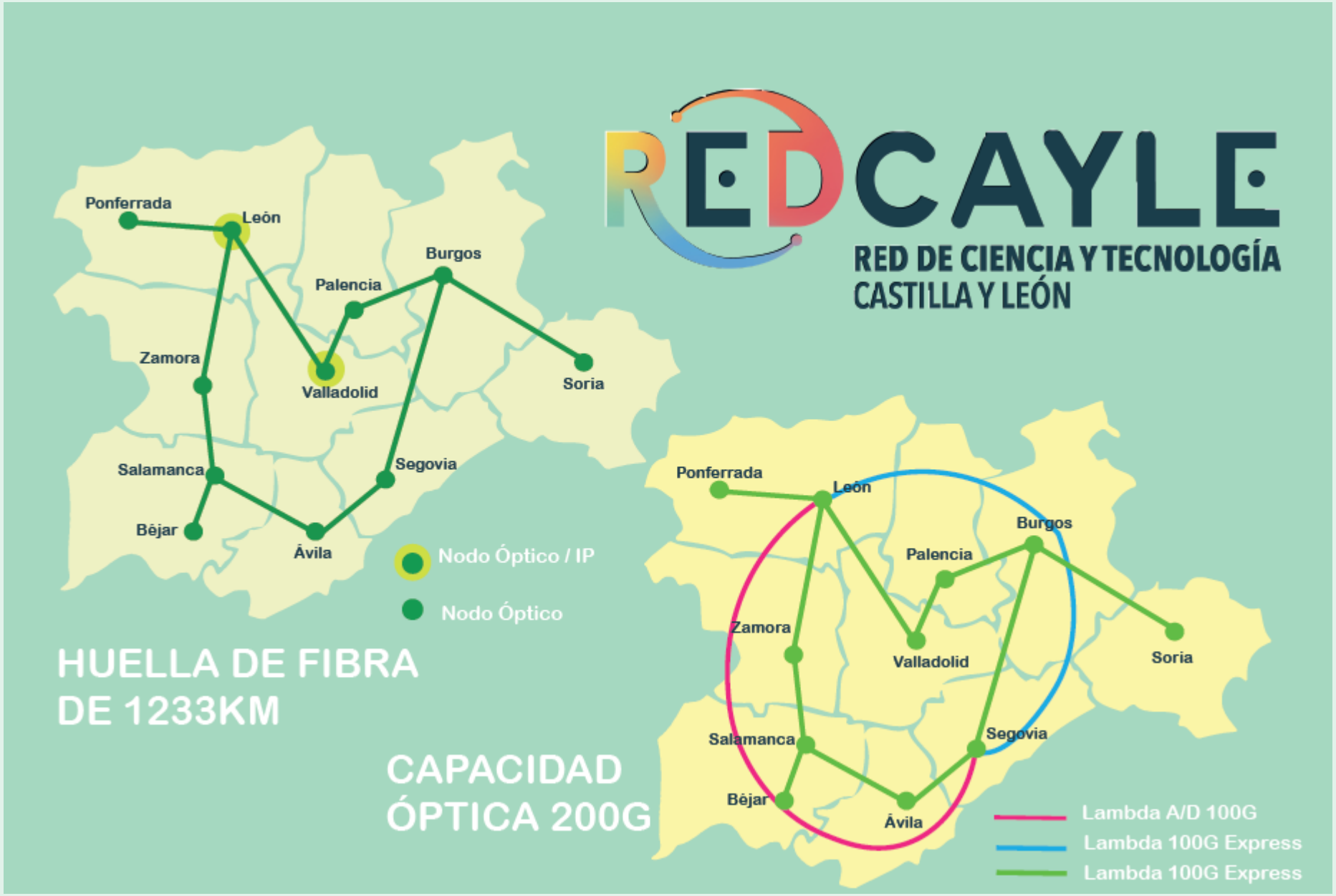
Contenido

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

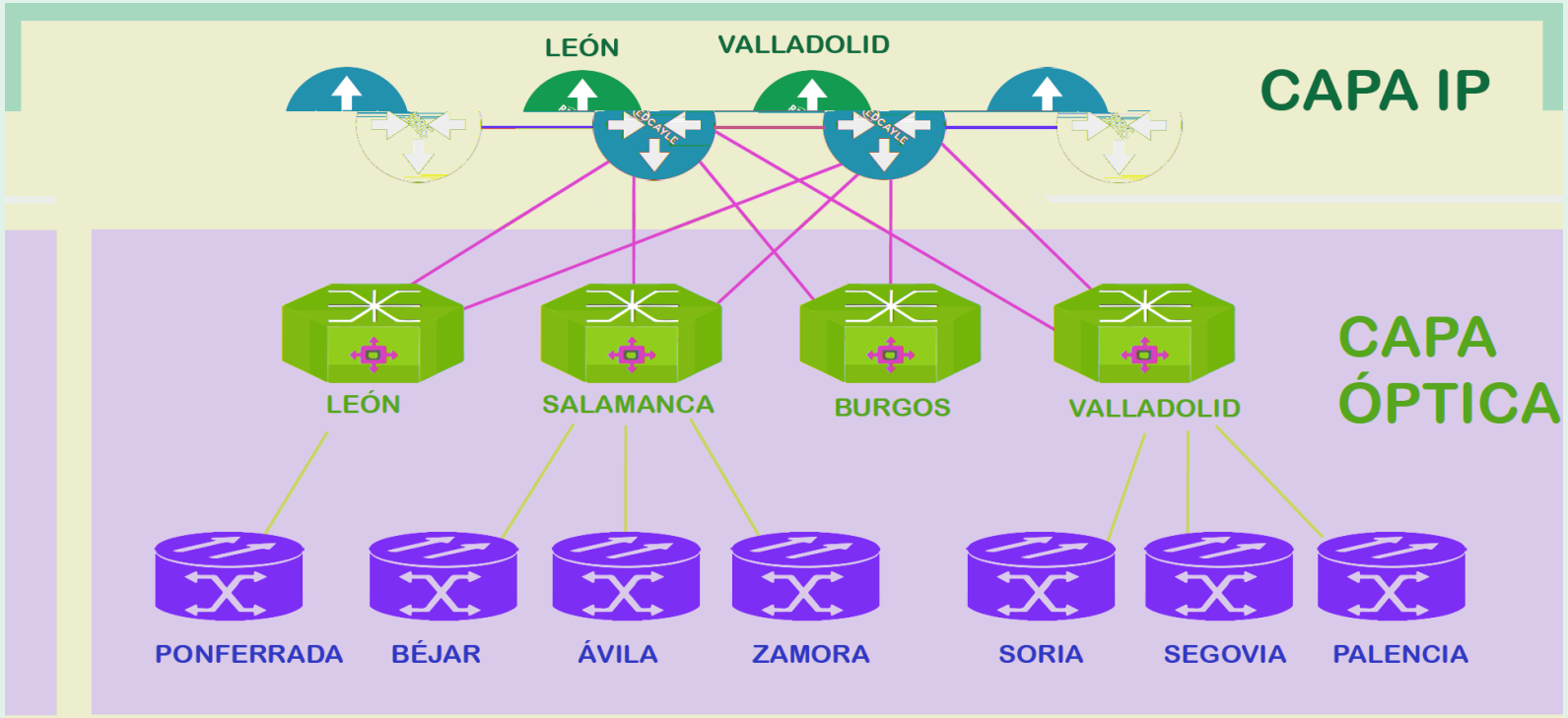


ESTADO ACTUAL

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN



ESTADO ACTUAL



2018 – 2019

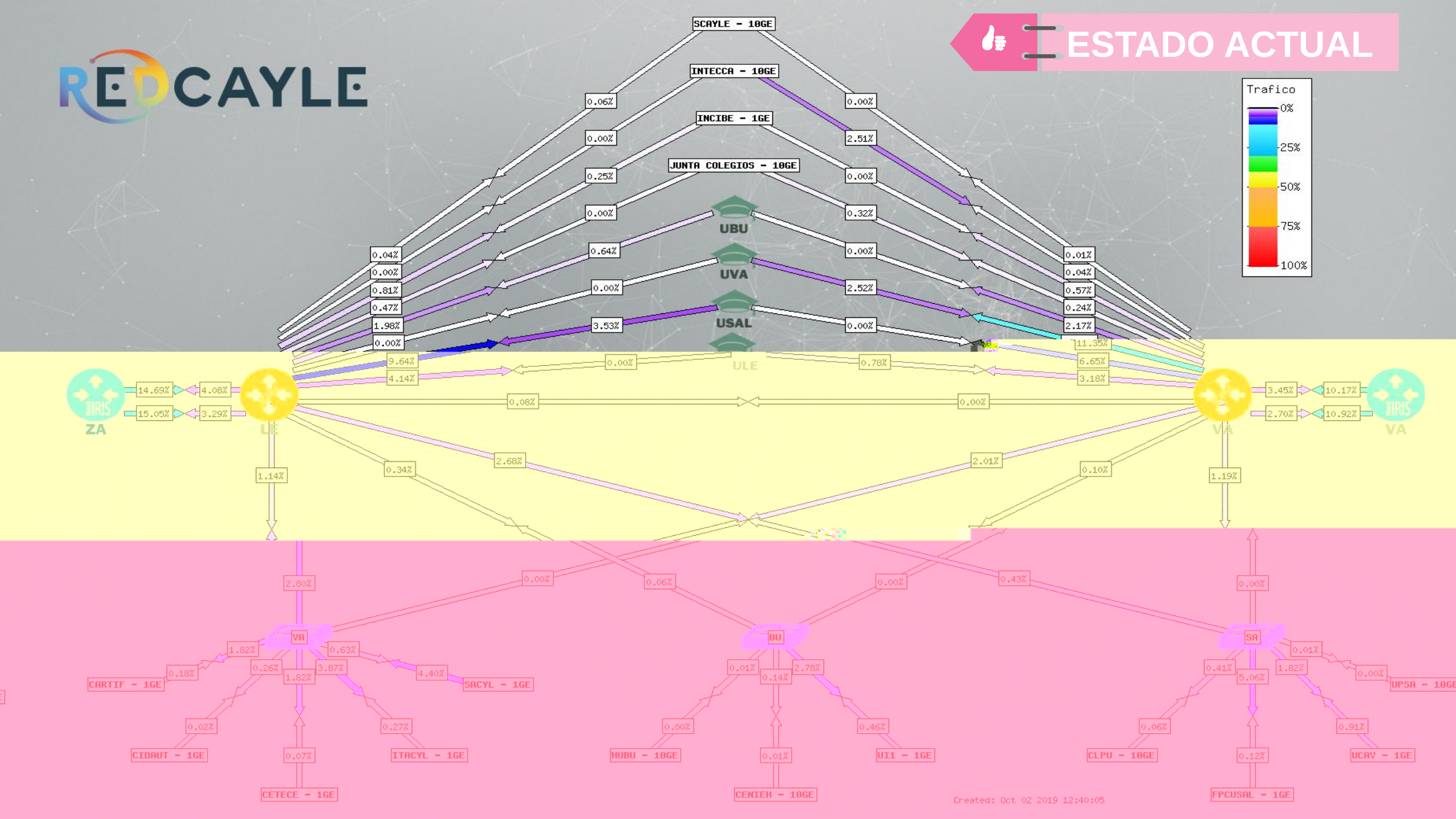
ENTIDADES MIGRADAS 20
AMPLIACION Equipos 120K

Fibra Urbana Hospital Univ. León
CEDER → Último centro conectado!!

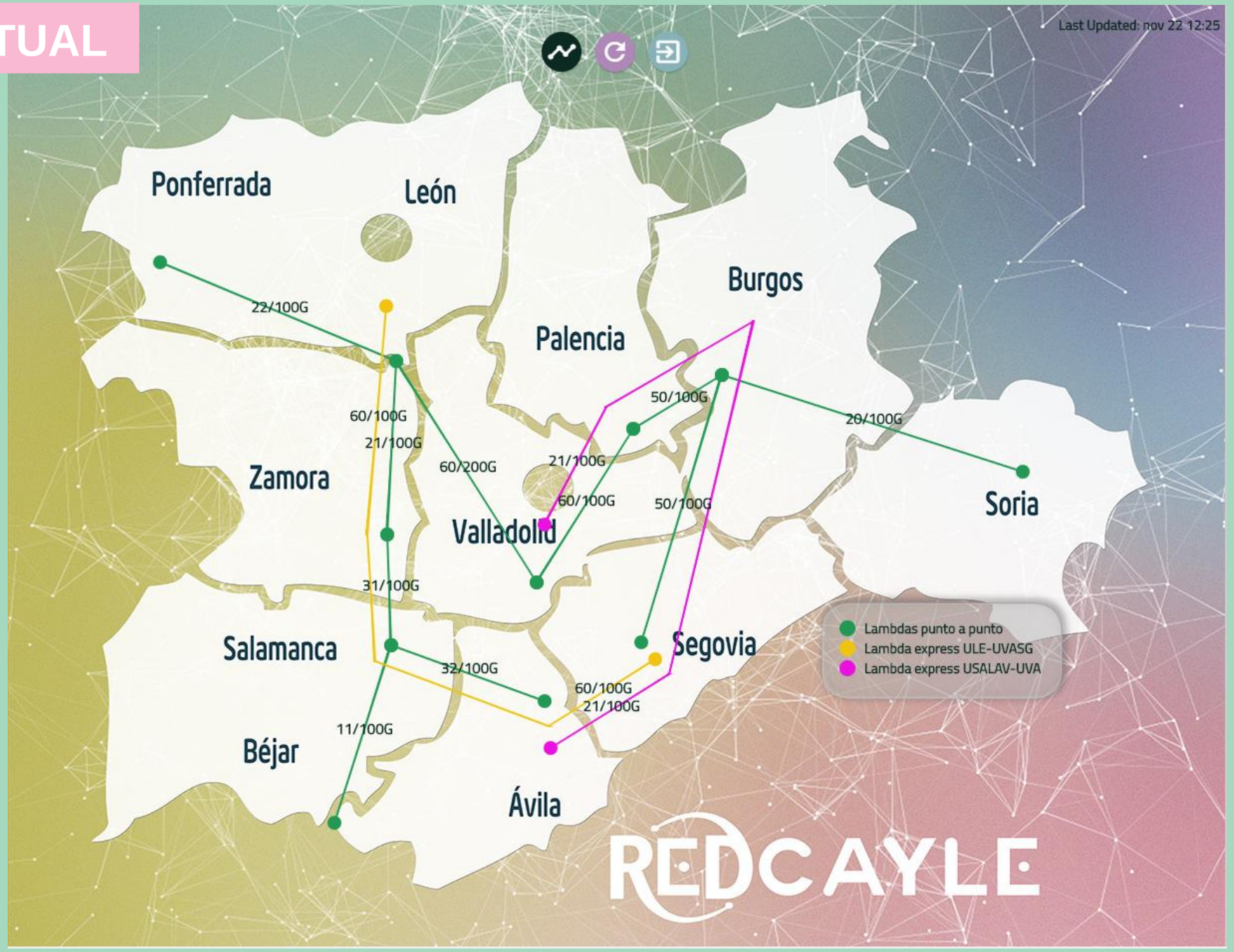
2020 en adelante

ENTIDADES adicionales con posibilidad de conectar 13

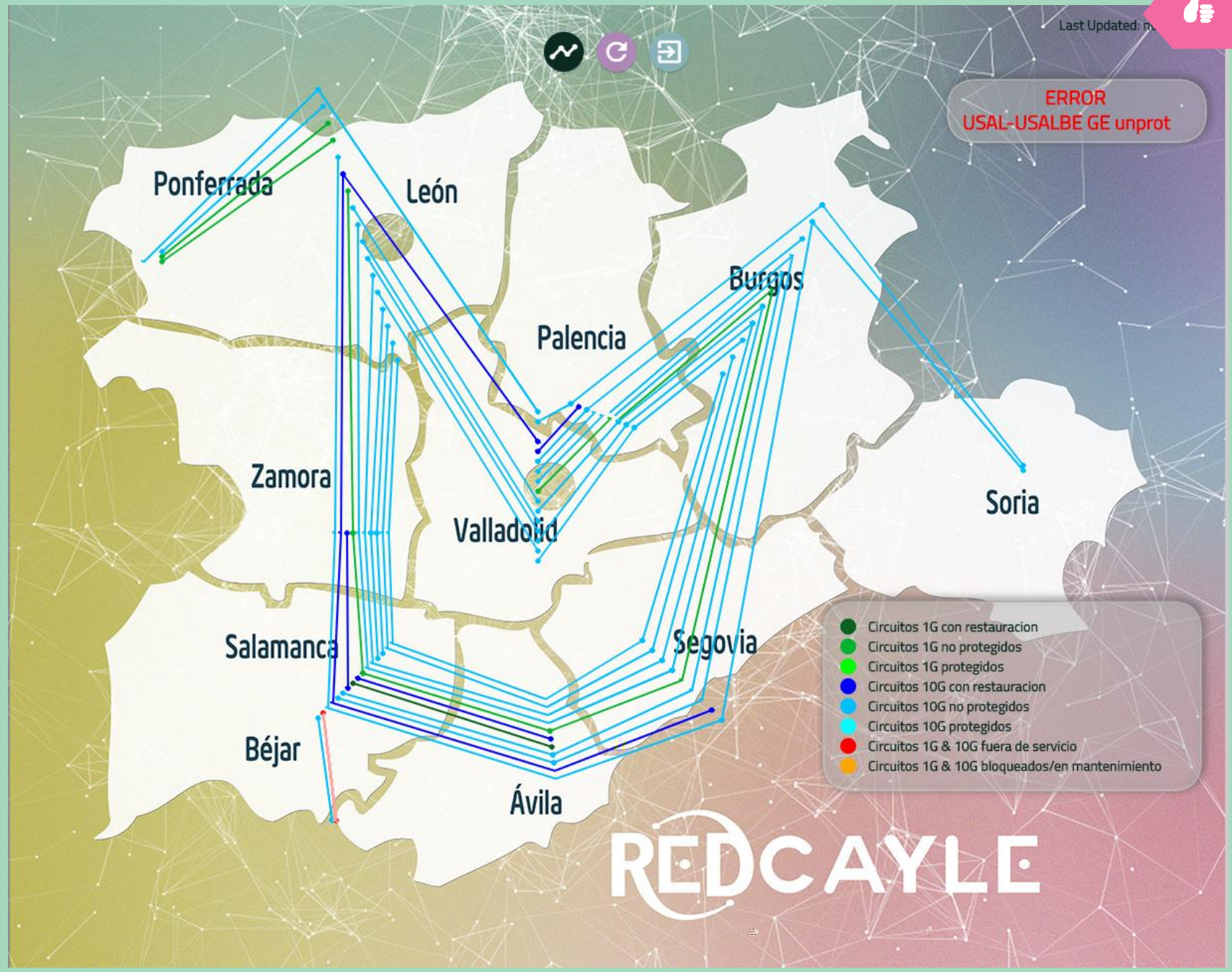
Ampliación de capilaridad urbana


REDCAYLE
ESTADO ACTUAL
SCAYLE - 10GE
INTECCA - 10GE
INCIBE - 1GE
JUNTA COLEGIOS - 10GE
UBU
UVA
USAL
ULE
Trafico
0%
25%
50%
75%
100%
0.06%
0.00%
0.25%
0.00%
0.04%
0.00%
0.81%
0.47%
1.98%
0.00%
0.64%
0.00%
3.53%
2.51%
0.00%
0.32%
0.00%
2.52%
0.00%
0.01%
0.04%
0.57%
0.24%
2.17%
11.35%
6.65%
3.18%
9.64%
4.14%
0.00%
0.78%
0.06%
0.00%
ZA
LE
VA
VA
14.69%
15.05%
4.08%
3.29%
3.45%
2.70%
10.17%
10.92%
1.14%
0.34%
2.68%
2.01%
0.10%
1.19%
2.80%
0.00%
0.06%
0.00%
0.43%
0.00%
VA
BU
SA
1.82%
0.18%
0.26%
1.82%
3.87%
0.63%
4.40%
CARTIF - 1GE
SACYL - 1GE
0.02%
0.07%
0.27%
CIDAUT - 1GE
ITACYL - 1GE
CETECE - 1GE
0.01%
0.14%
2.78%
0.00%
0.01%
0.46%
HUBU - 10GE
CENIEH - 10GE
UI1 - 1GE
0.41%
5.06%
1.82%
0.01%
0.00%
0.06%
0.12%
0.91%
CLPU - 10GE
FPCUSAL - 1GE
UCAV - 1GE
UPSA - 10GE
Created: Oct 02 2019 12:40:05

ESTADO ACTUAL



ESTADO ACTUAL



SERVICIOS Adicionales

Servidores de HORA

tic.redcayle.es
185.179.104.7
Stratum 1 con fuente GPS

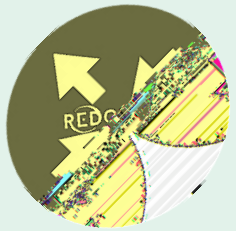
tac.redcayle.es
185.179.104.12
Stratum 1 con fuente GPS

IPERF (previa solicitud al NOC)

MONITORIZACIÓN

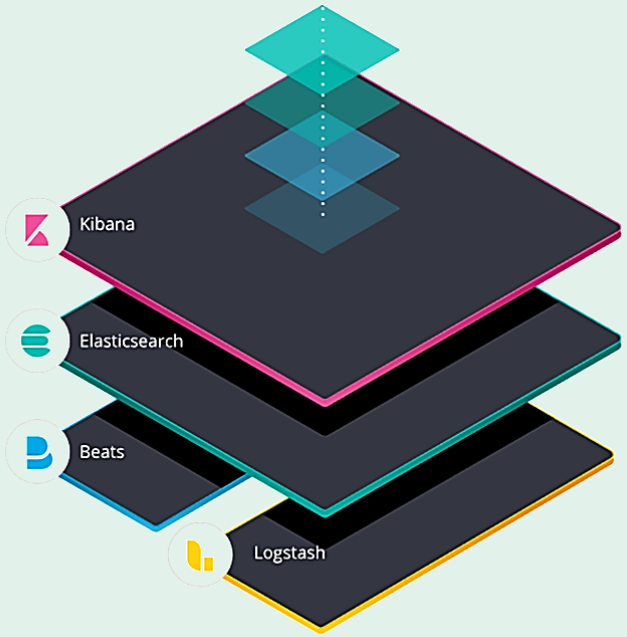
REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

NetFlow



beats → logstash → elasticsearch ← kibana

Data Collection	Data Aggregation & Processing	Indexing & storage	Analysis & visualization



Nagios®

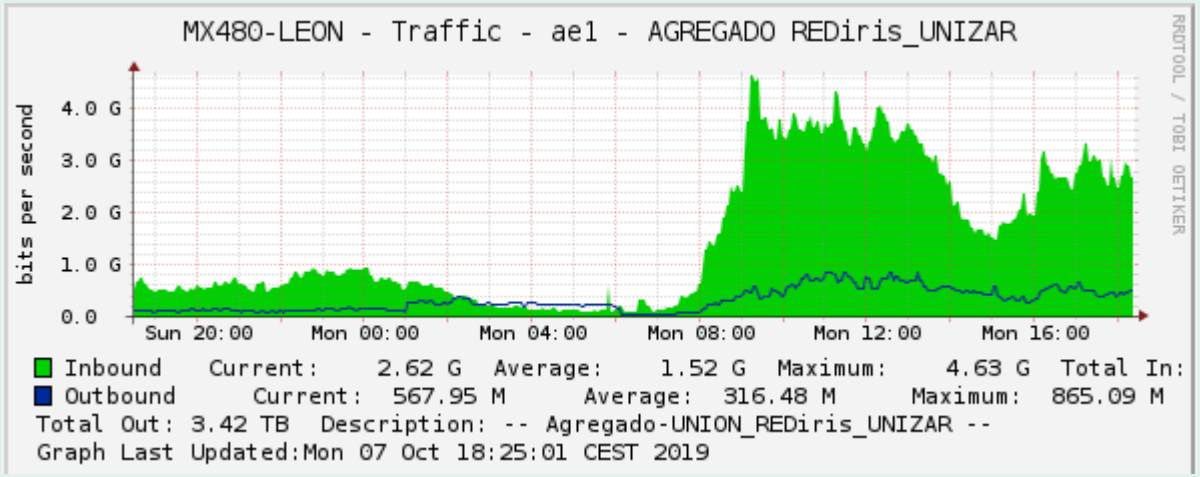
cacti

graylog

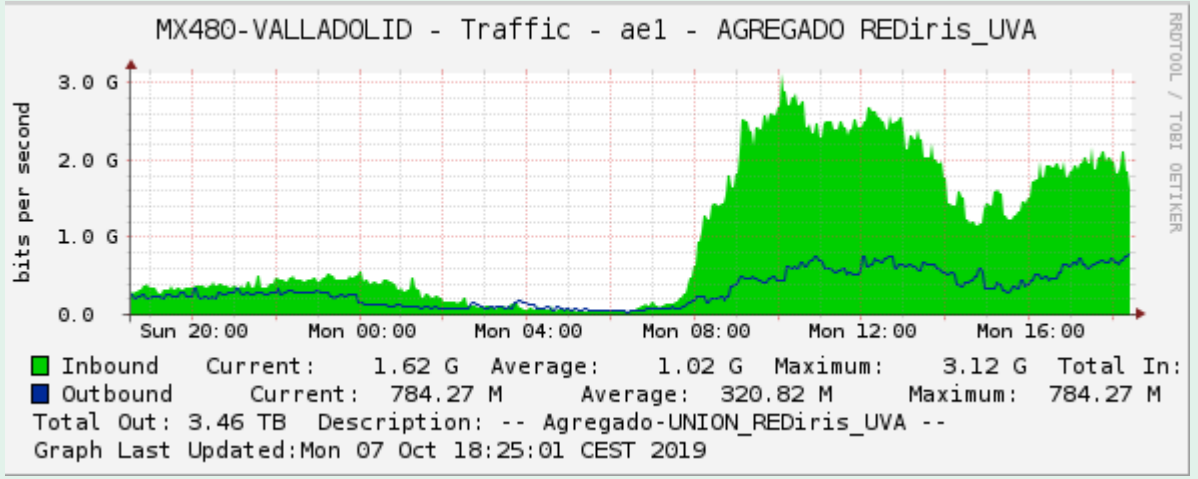
Monitorización - Cacti

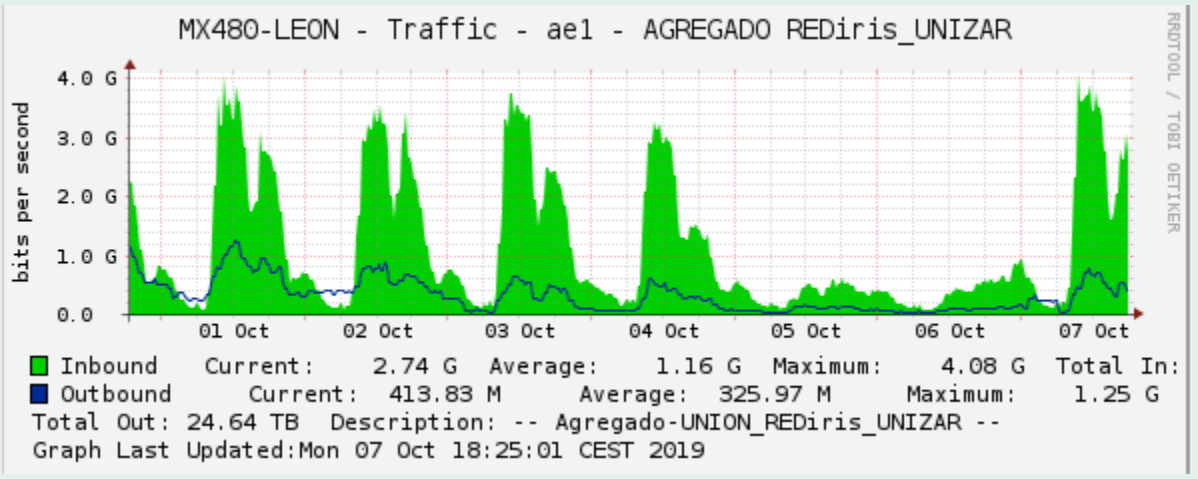
REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

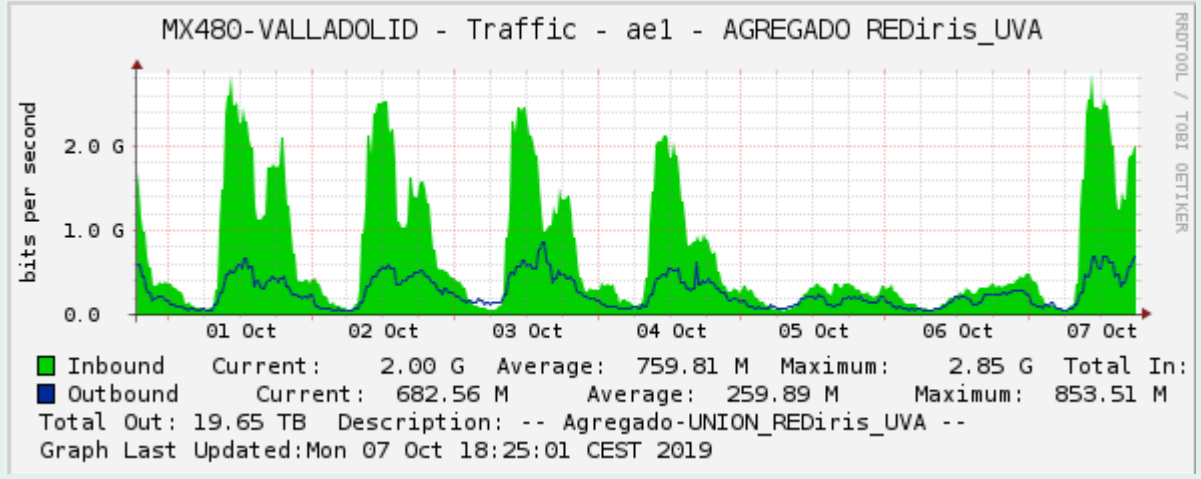
Router LEON Tráfico Agregado con REDIRIS



Router VALLADOLID Tráfico Agregado con REDIRIS





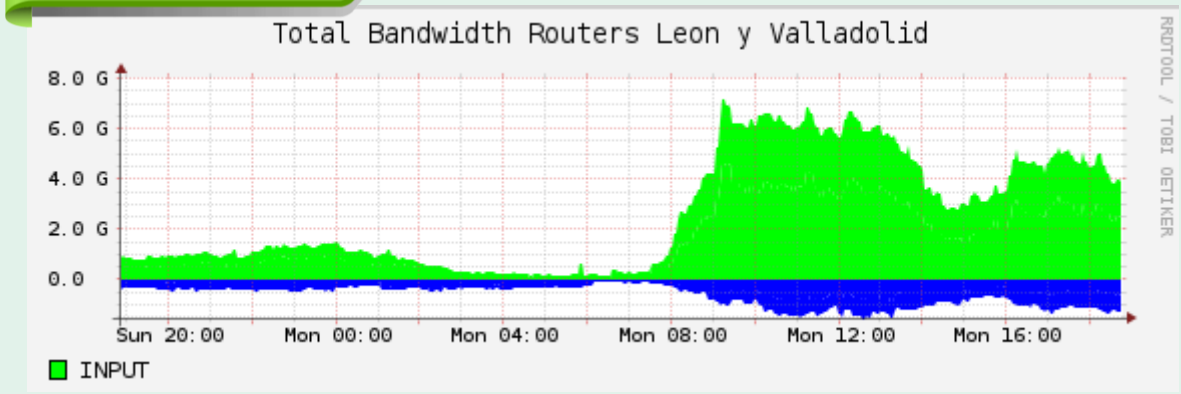


Monitorización - Cacti

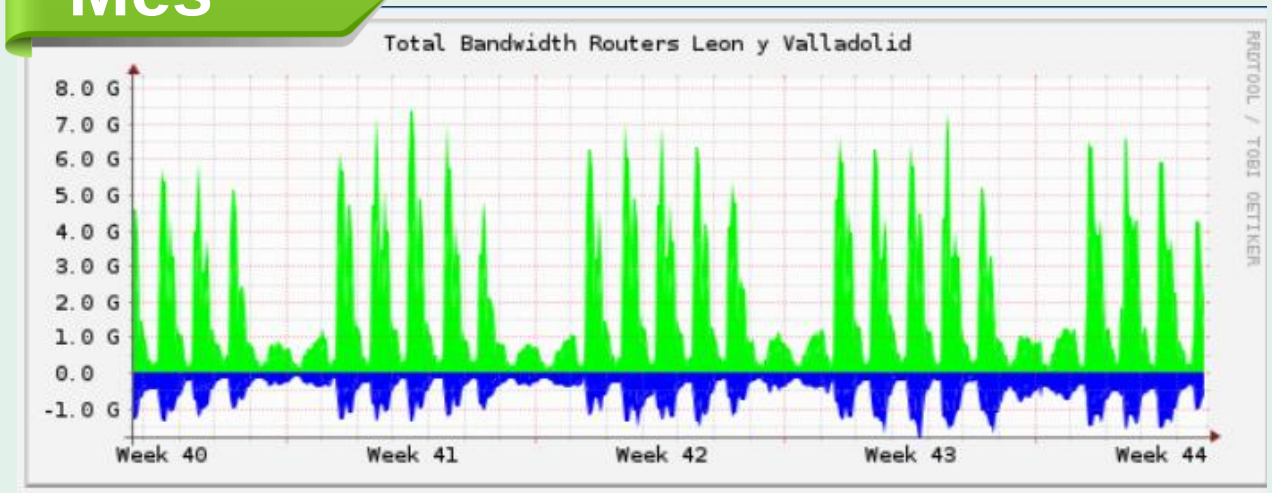
REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

Tráfico Intercambio IP con REDIRIS

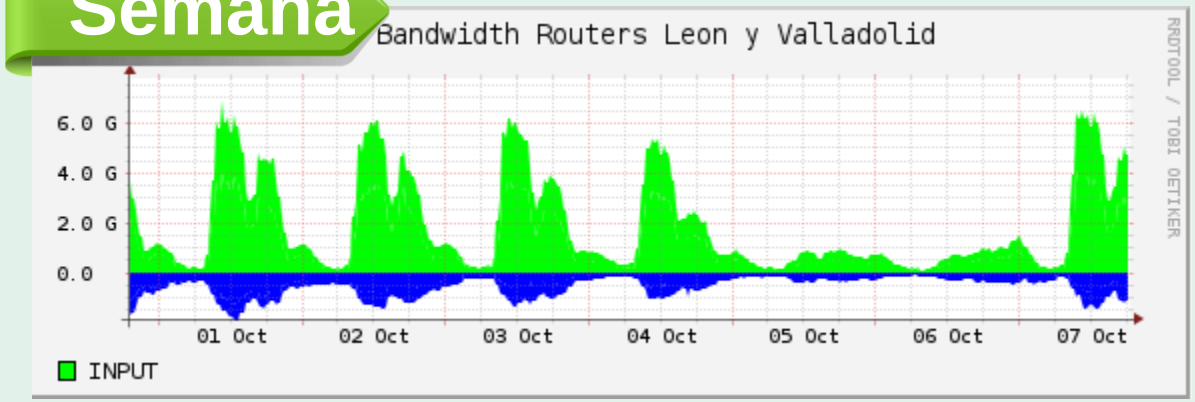
Día



Mes



Semana



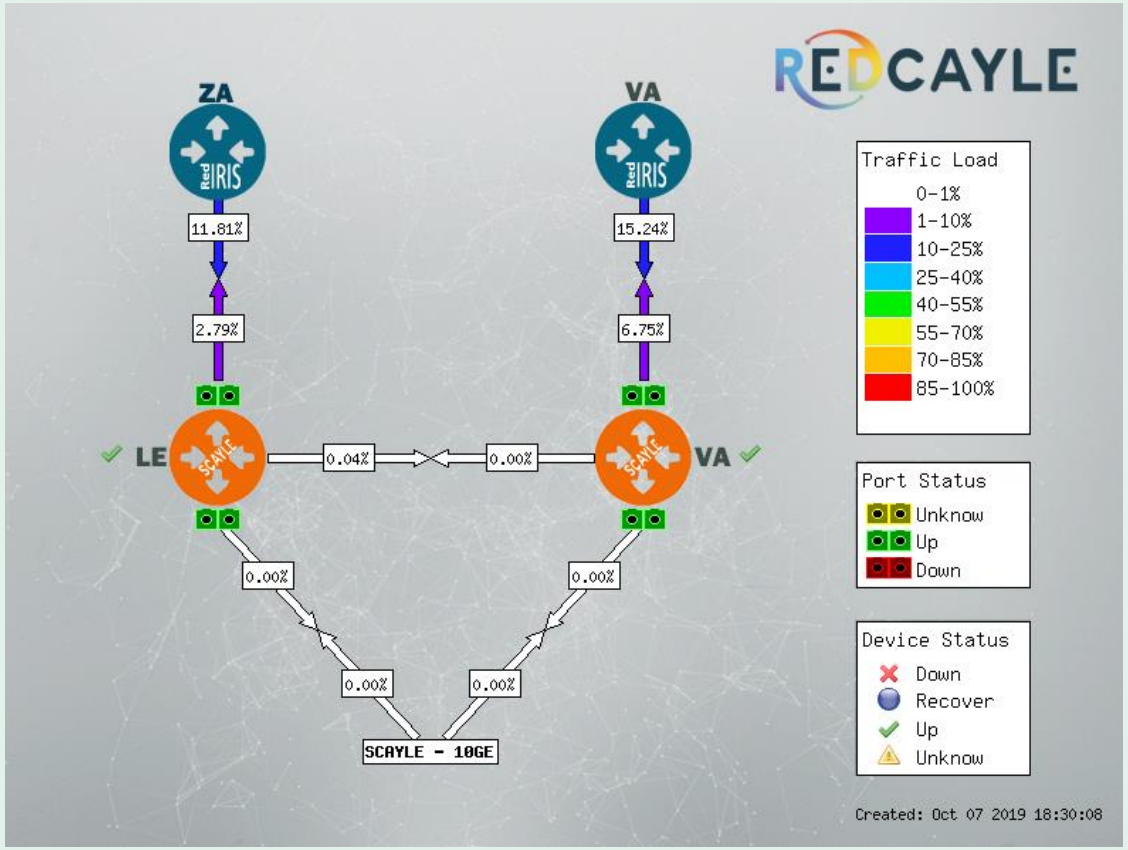
Octubre 677TB

Octubre 205 TB

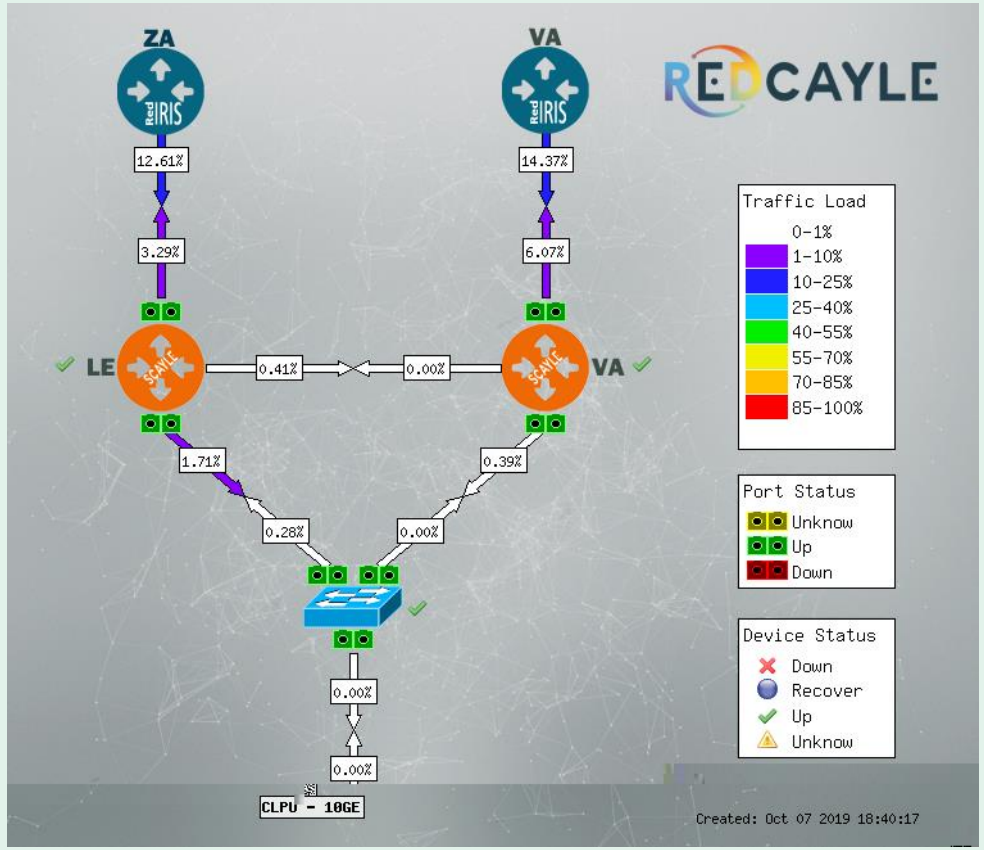
Monitorización - Weathermap

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

TIPO A

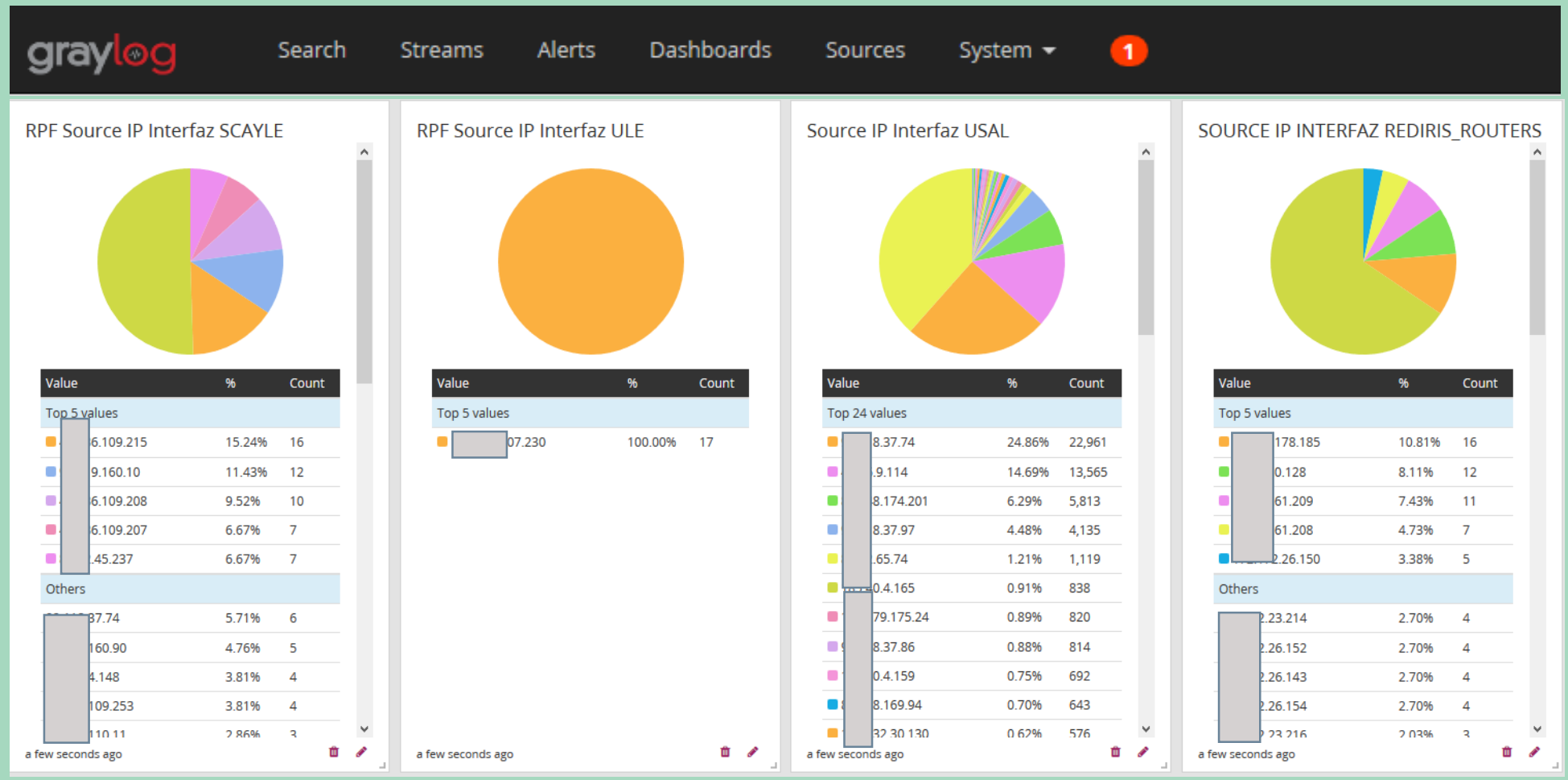


TIPO B

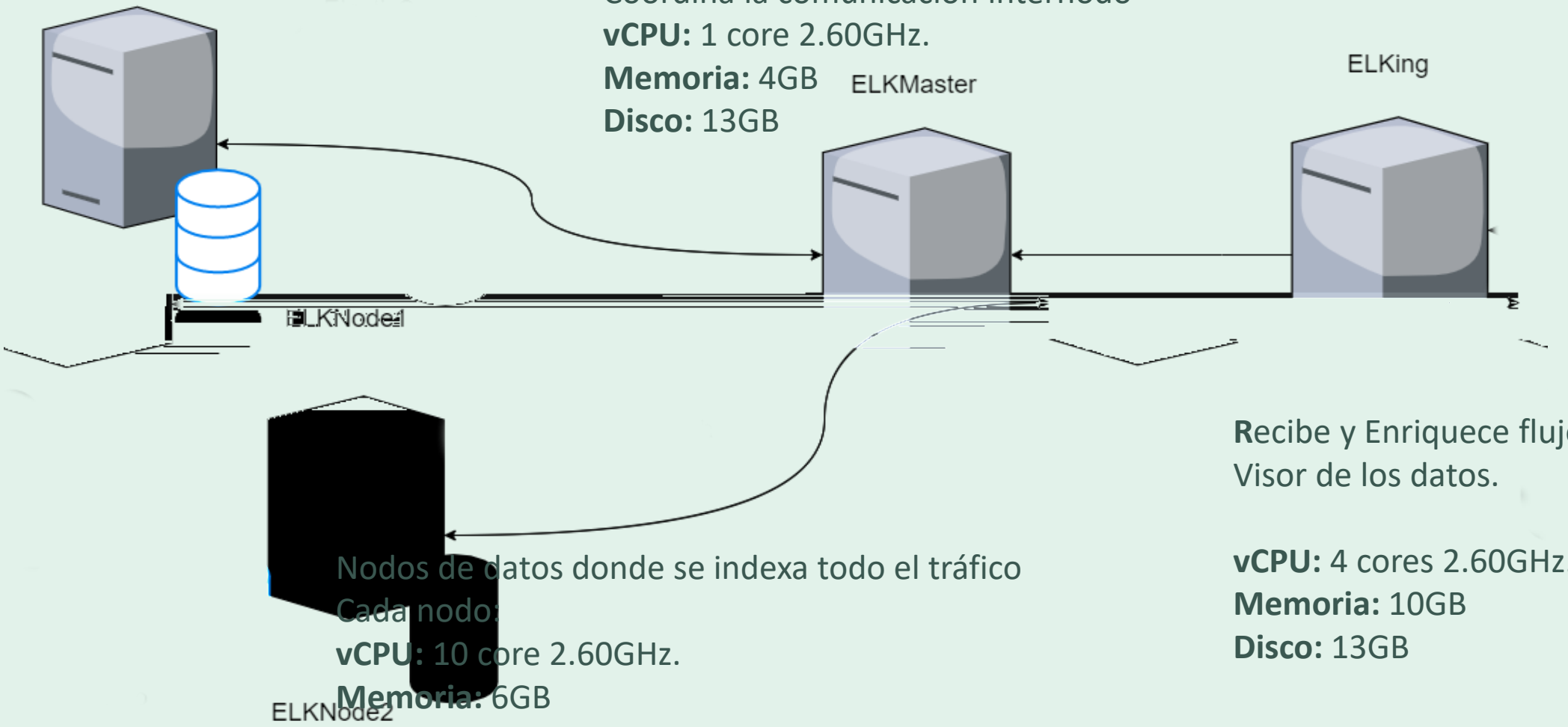


Monitorización - Graylog

EJEMPLO: UNICAST Reverse Path Forwarding (MANRS)



Monitorización - ELK Stack



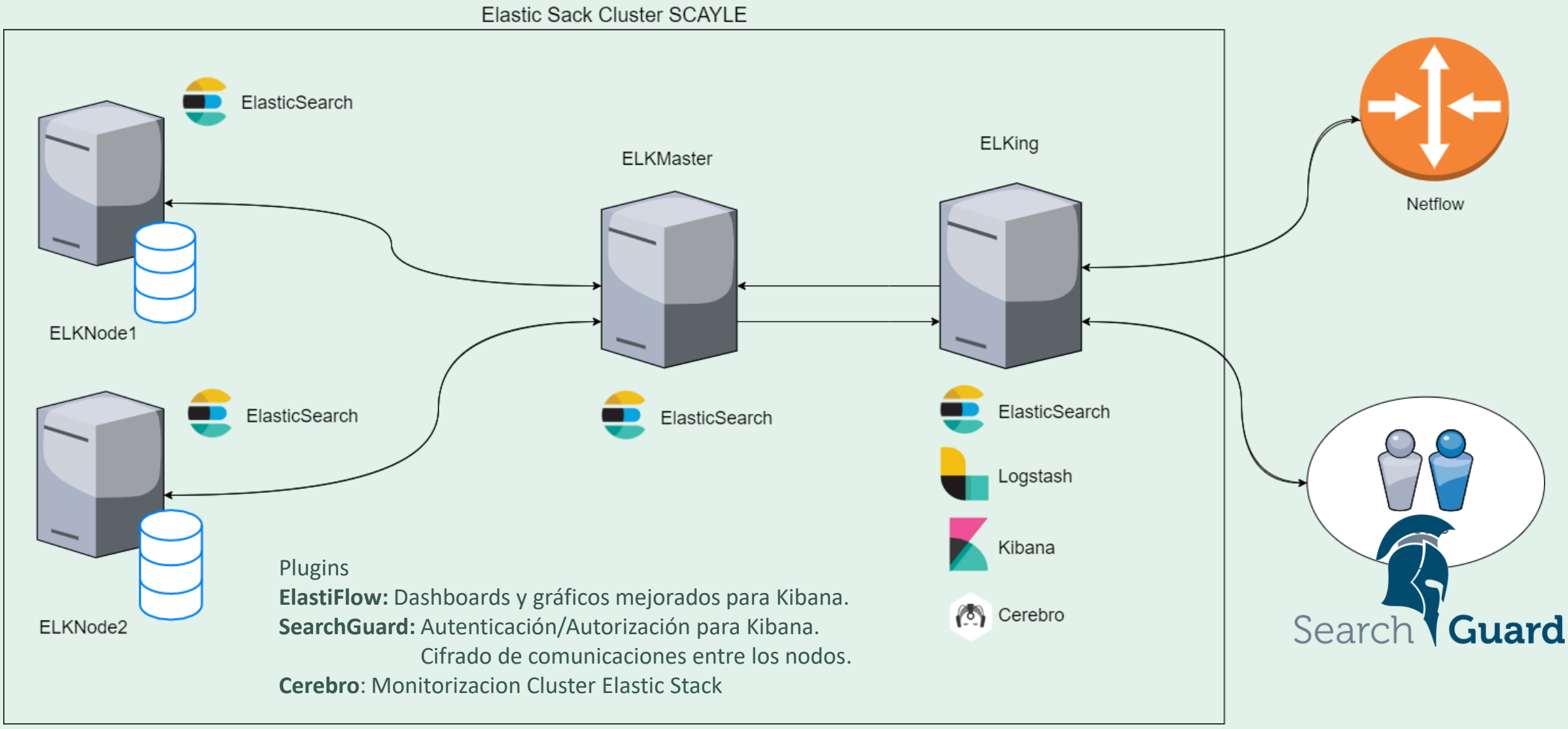
Coordina la comunicación internodo
vCPU: 1 core 2.60GHz.
Memoria: 4GB
Disco: 13GB

Recibe y Enriquece flujos Netflow.
Visor de los datos.

vCPU: 4 cores 2.60GHz.
Memoria: 10GB
Disco: 13GB

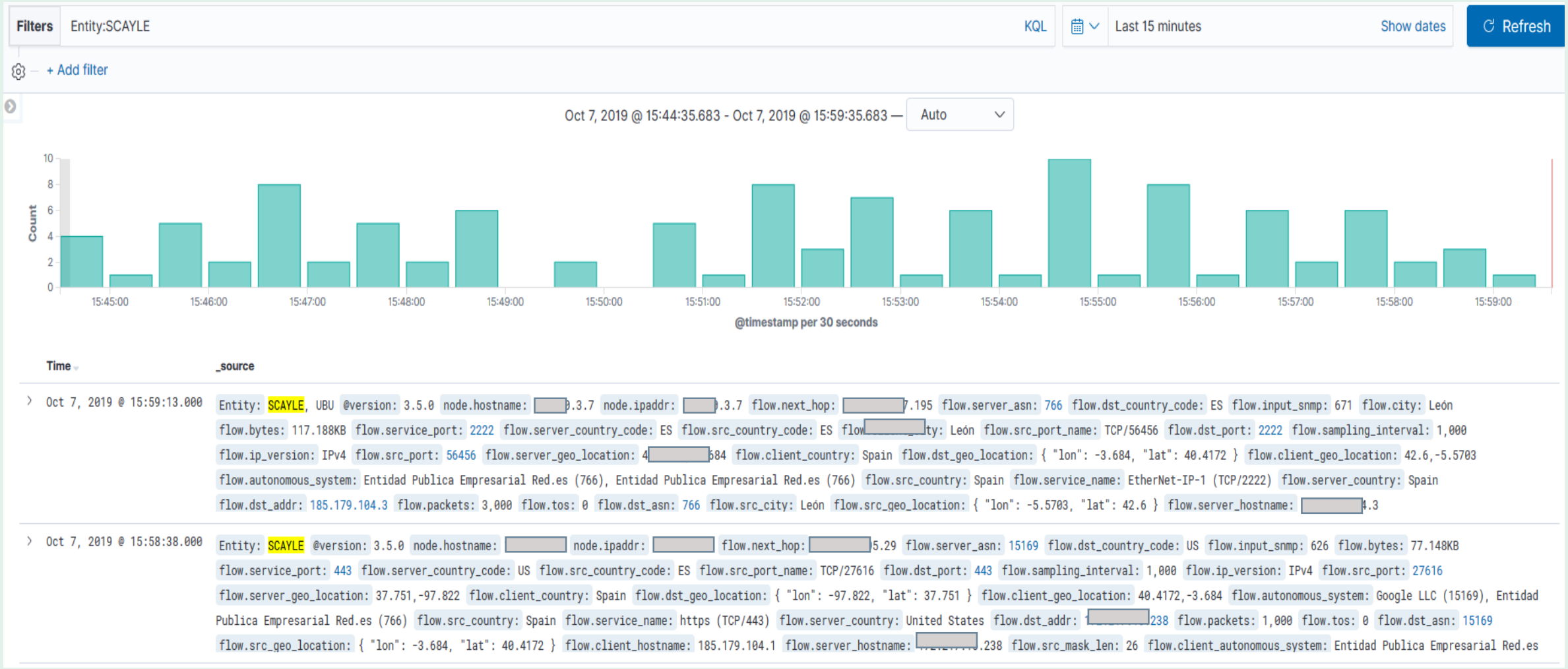
Nodos de datos donde se indexa todo el tráfico
Cada nodo:
vCPU: 10 core 2.60GHz.
Memoria: 6GB
Disco: 200GB

Monitorización - ELK Stack



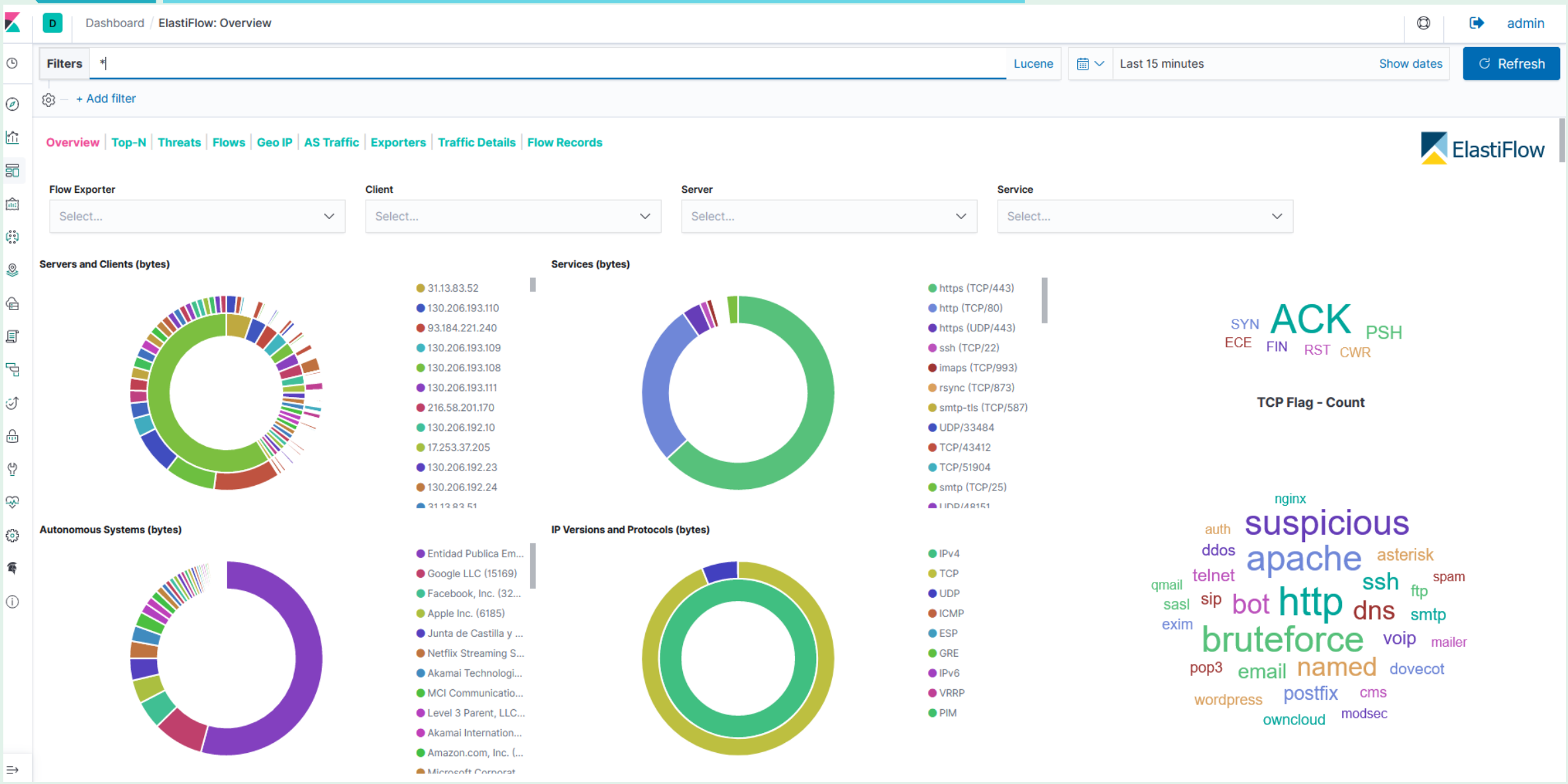
Monitorización - ELK Stack

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN



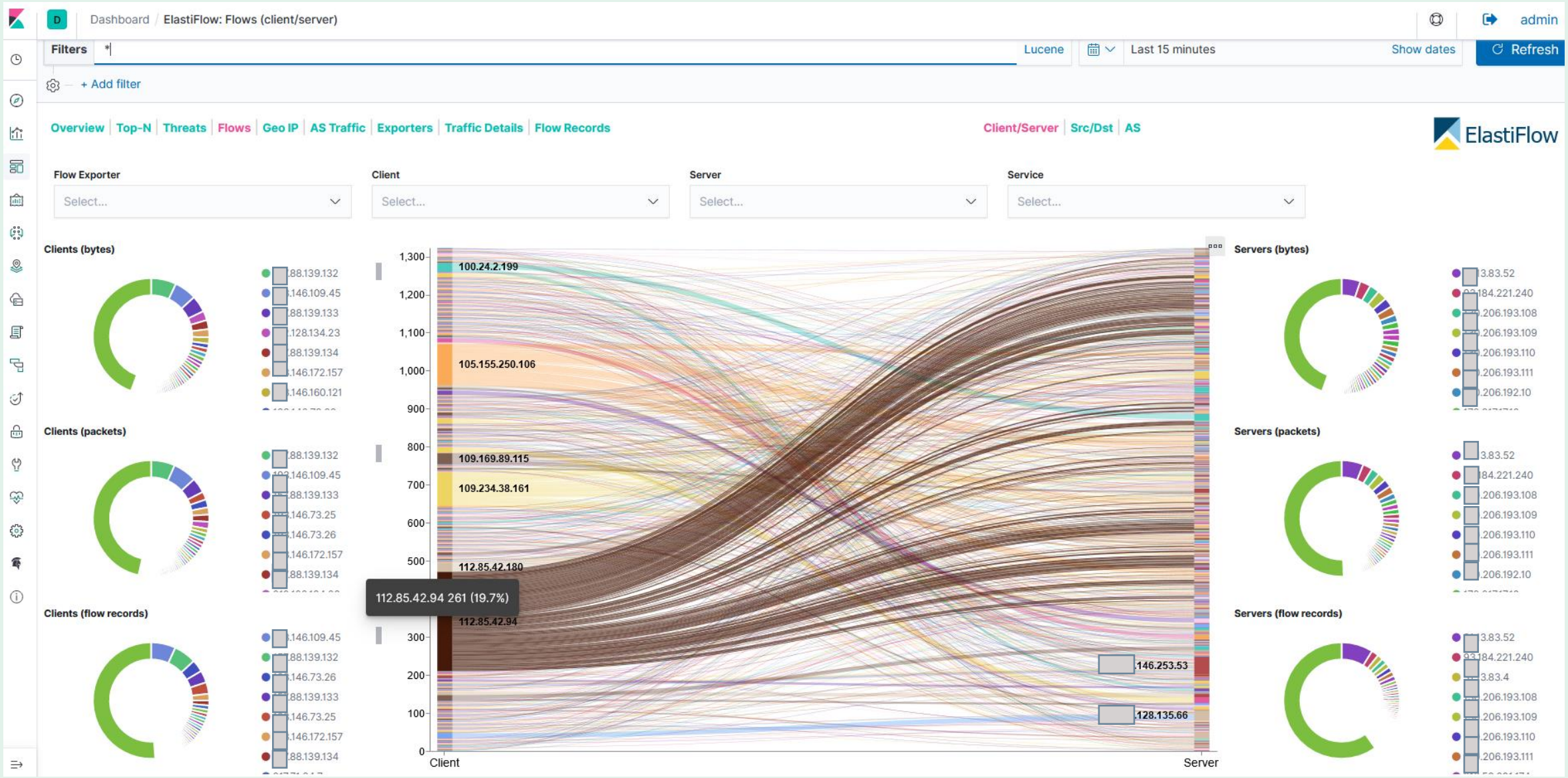
Monitorización - ELK Stack

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN



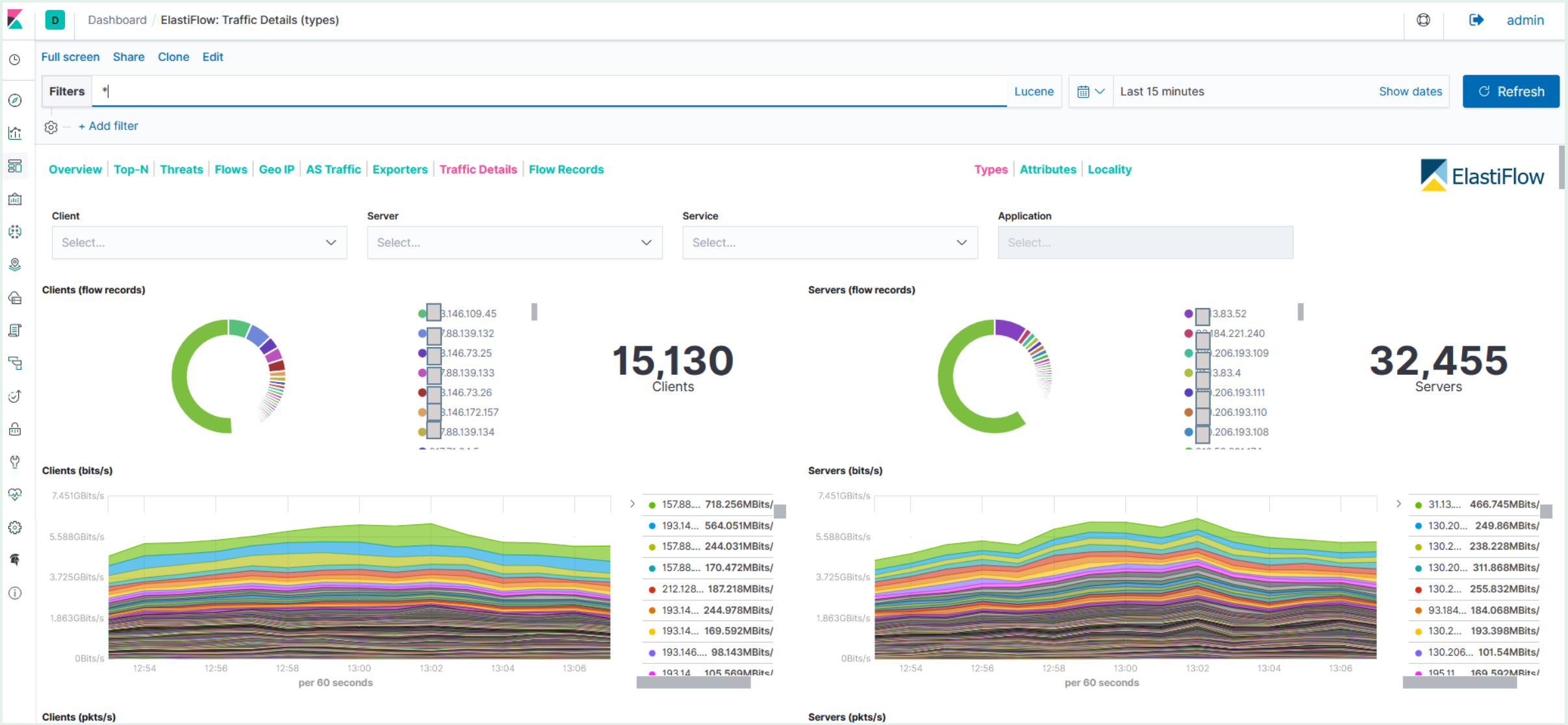
Monitorización - ELK Stack

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

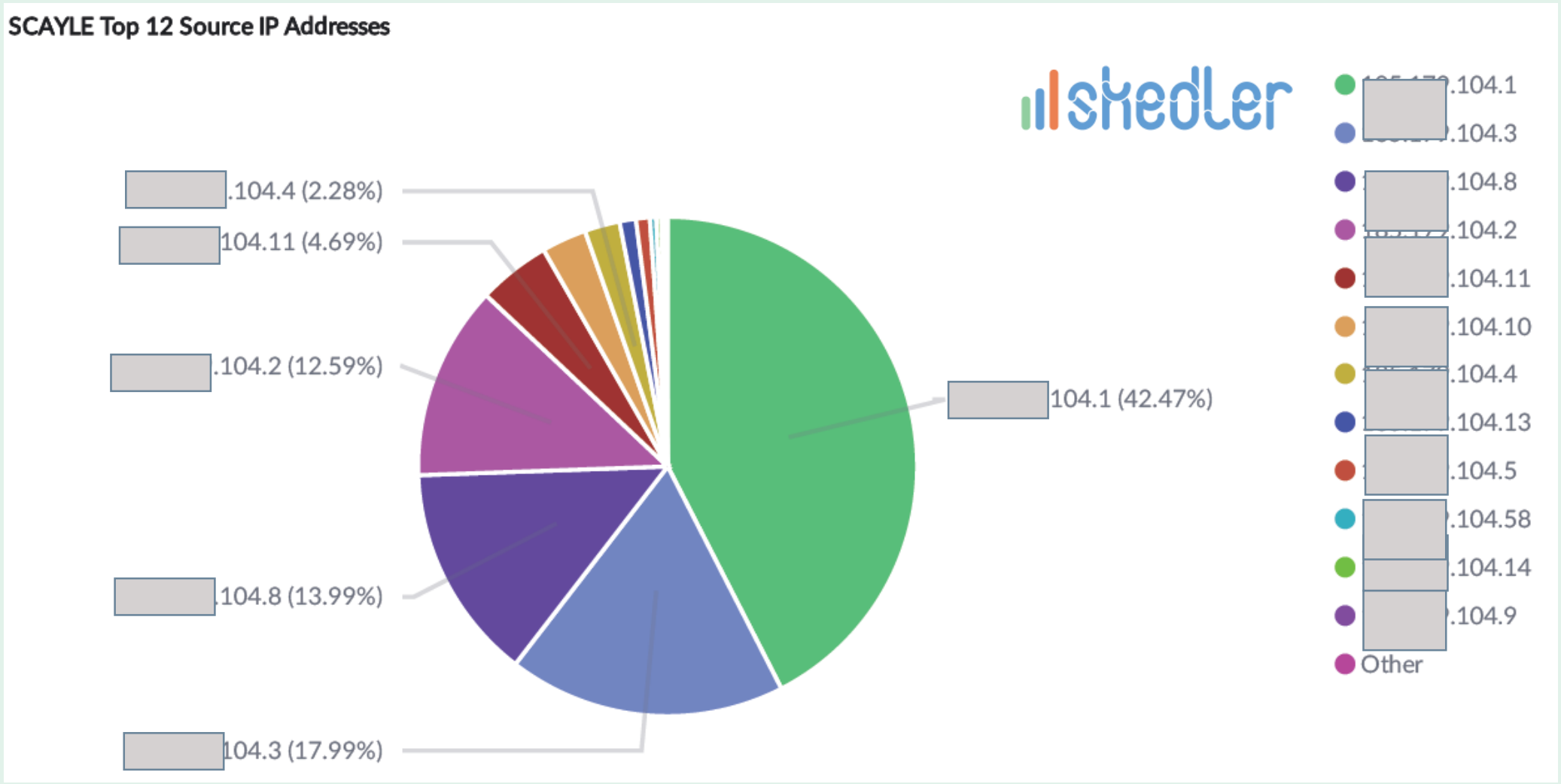


Monitorización - ELK Stack

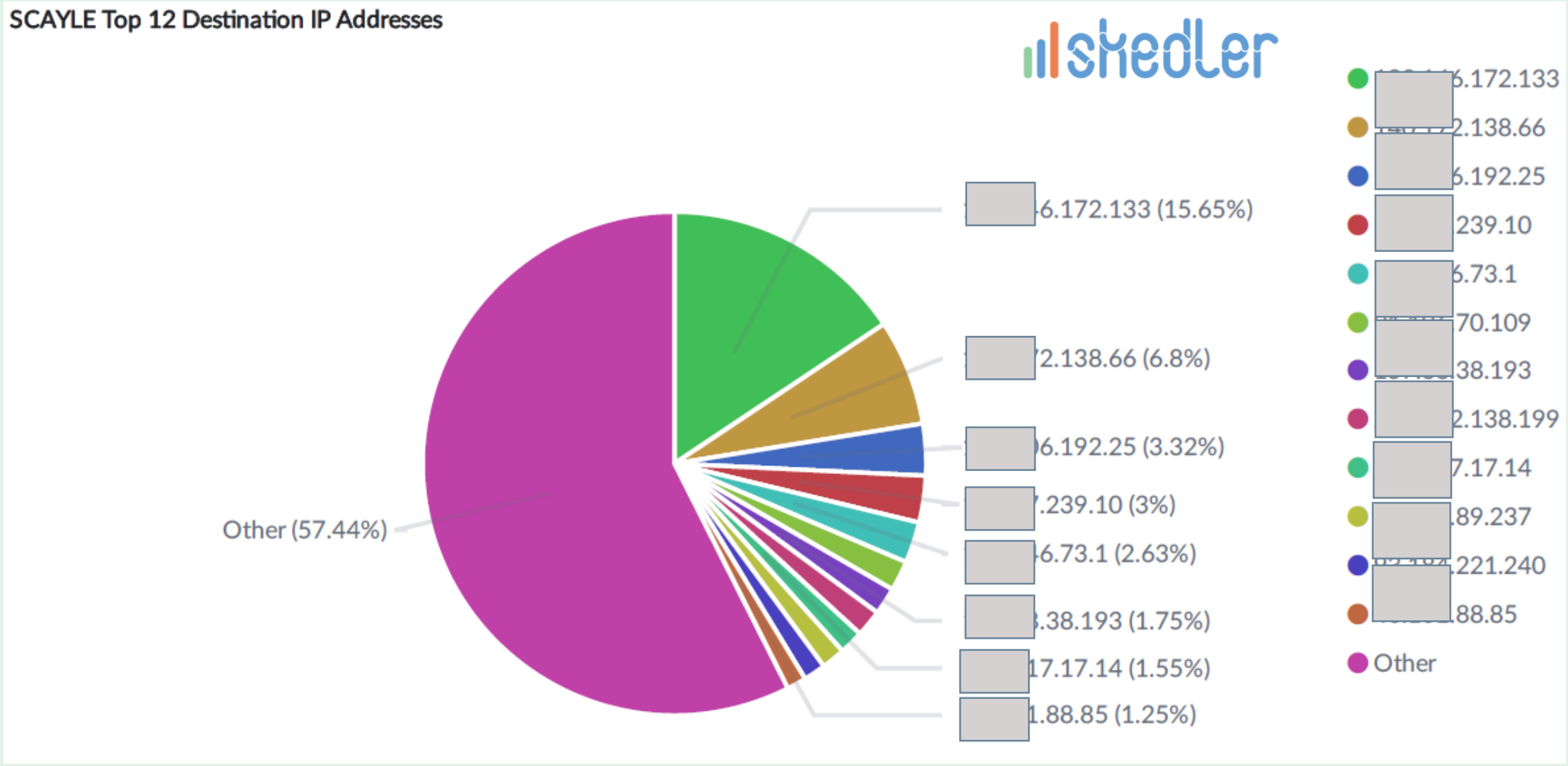
REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN



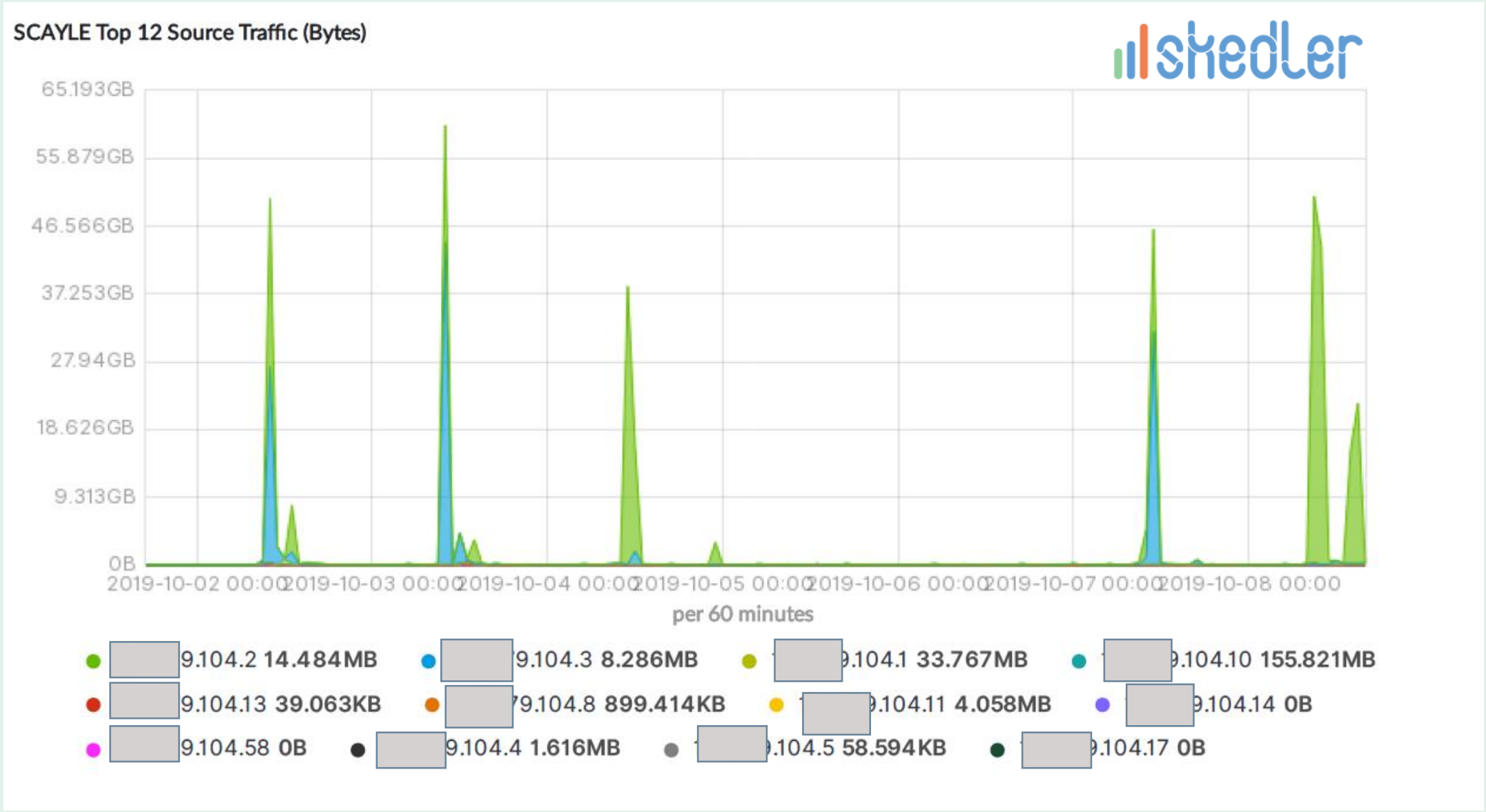
Monitorización - Informes



Monitorización - Informes



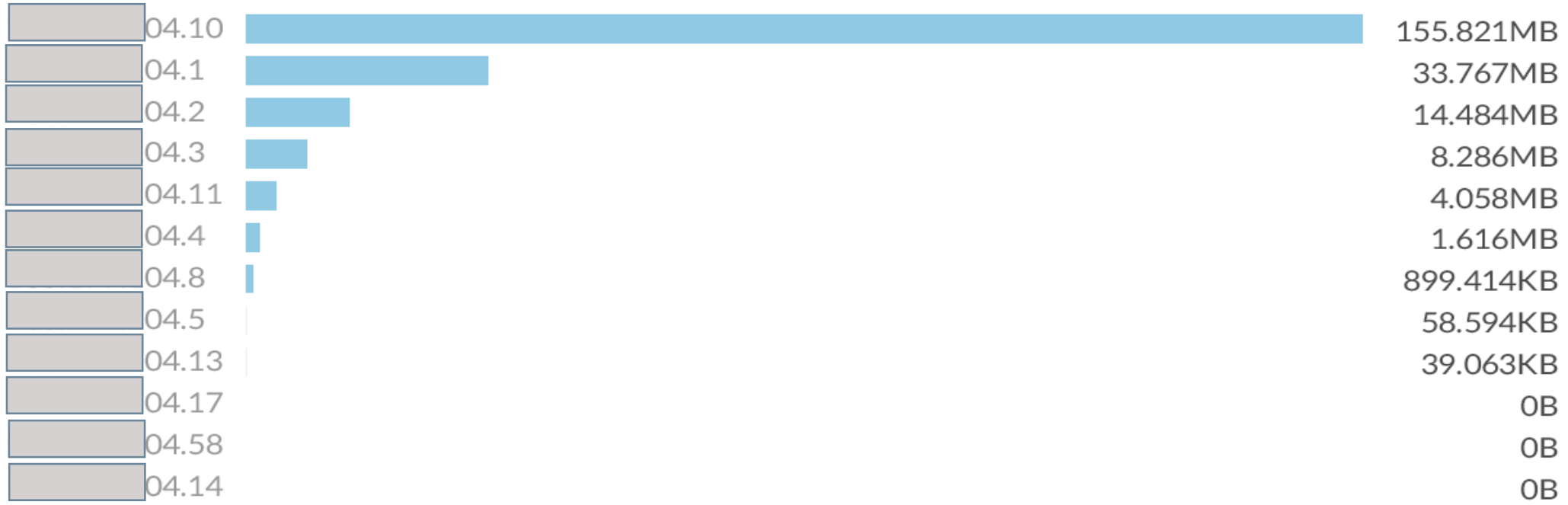
Monitorización - Informes



Monitorización - Informes

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

SCAYLE Top 12 Descending Source Traffic (Bytes)



skedler

Time Window: From: 01-October-2019 05:45:00 pm To: 08-October-2019 05:45:00 pm (Europe/Paris)

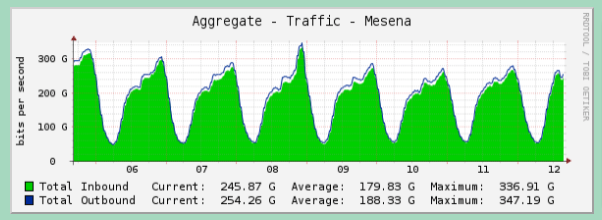
Alertas Proactivas

skedler

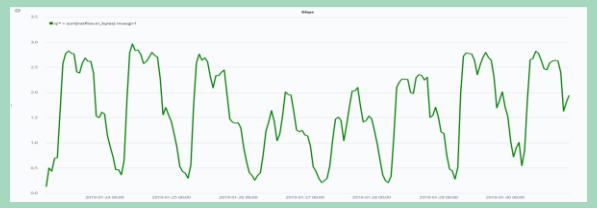
- Alertas + Informes
- ≈10,000$/año

Alertas Proactivas

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN



01 cacti

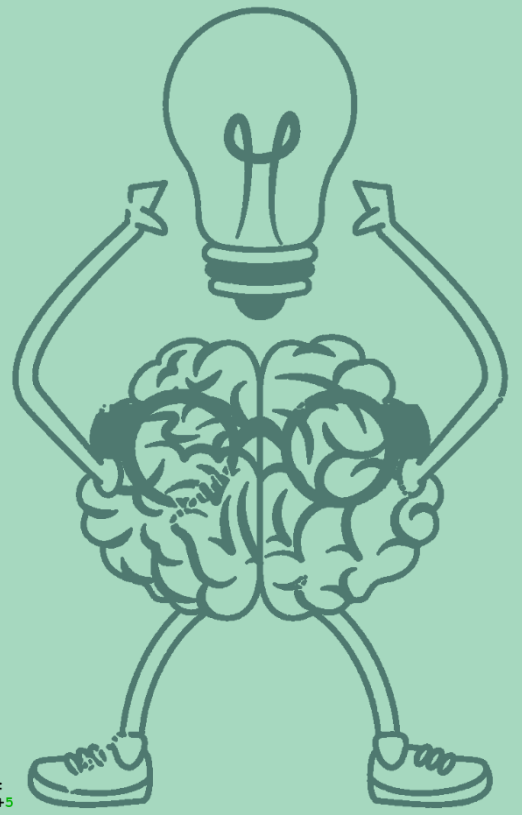


kibana 02

03 NetFlow

elasticsearch 04

05 python



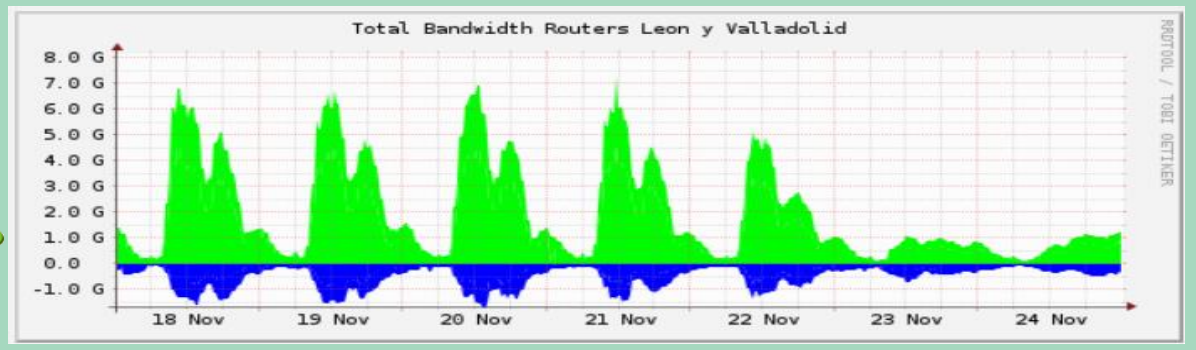
```
def add5(x):
   return x+5

def dotwrite(ast):
   nodename = getNodename()
   label=symbol.sym_name.get(int(ast[0]),ast[0])
   print '    %s [label="%s' % (nodename, label),
   if isinstance(ast[1], str):
      if ast[1].strip():
         print '= %s"];' % ast[1]
      else:
         print '"]'
   else:
      print '"];'
      children = []
      for n, child in enumerate(ast[1:]):
         children.append(dotwrite(child))
      print '    %s -> {' % nodename,
      for name in children:
         print '%s' % name,
```

Alertas Proactivas

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

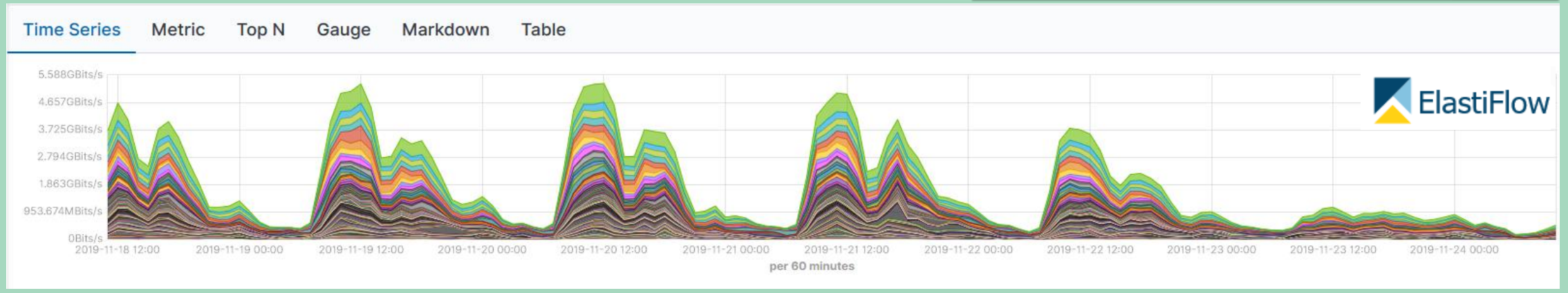
01 TENDENCIAS TRÁFICO

cacti



kibana

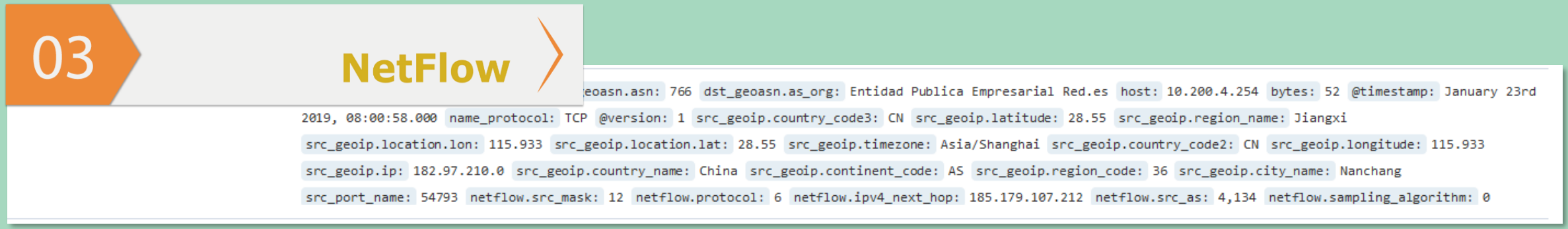
TENDENCIAS TRÁFICO 02



Alertas Proactivas

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

03 NetFlow



elasticsearch 04

Agregación 1

```
"aggs": {
  "2": {
    "terms": {
      "field": "netflow.ipv4_dst_addr.keyword",
      "size": 5,
      "order": {
        "1": "desc"
      }
    },
    "aggs": {
      "1": {
        "sum": {
          "field": "netflow.in_bytes"
        }
      },
```

Agregación 2

```
    },
    "3": {
      "terms": {
        "field": "src_port_name.keyword",
        "size": 5,
        "order": {
          "1": "desc"
        }
      },
      "aggs": {
        "1": {
          "sum": {
            "field": "netflow.in_bytes"
          }
```

Alertas Proactivas

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

05

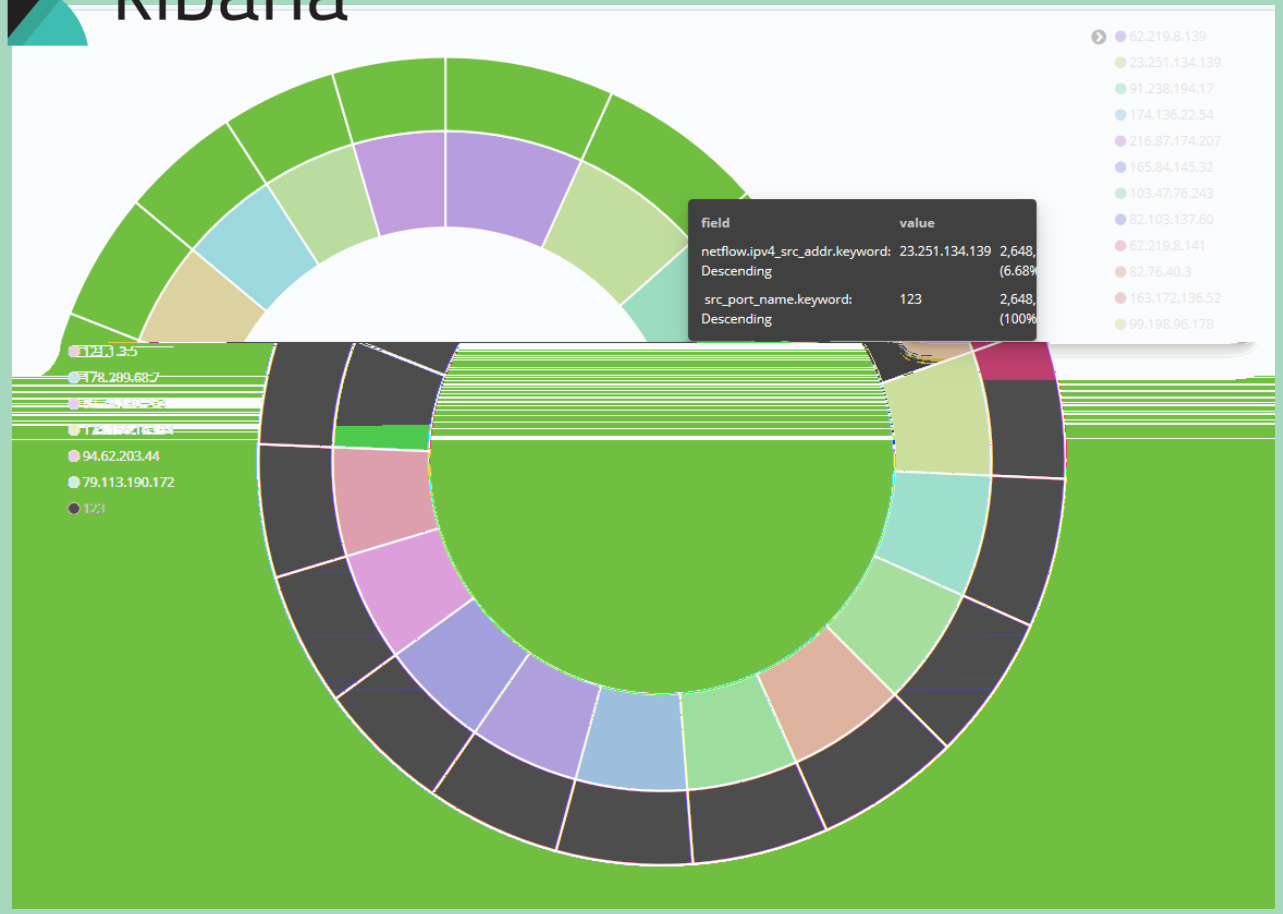
python

```
GLOBAL VARS:

LAST_TOP_IP, LAST_STATE=0, TIME_WINDOW=5m, ALERT_LEVEL=0

MATRIZ TENDENCIA TRAFICO SEMANAL

1. Para TIME_WINDOW
    Obtener los documentos indexados en elasticsearch
    Calcular los bytes/s --> (Gbps)
    Obtener top 5 de host de destinos y puertos y seleccionar ACTUAL_TOP_IP que genera mas del 50% de los Gbps


2.Comparar los Gbps obtenidos con la tendencia de tráfico en esa hora (MATRIZ_TENDENCIA)
    Si los Gbps superan UMBRAL{
        ALERT_LEVEL = 1
        Si LAST_STATE = 1 {     <--- si se ha mantenido durante el TIME_WINDOW anterior
            ALERT_LEVEL = 2
                Si ACTUAL_TOP_IP = LAST_TOP_IP{     <--- si ACTUAL_TOP_IP se mantiene
                    ALERT_LEVEL = 3
                }
        }

        LAST_STATE=1            <--- en el estado actual se ha superado umbral
        LAST_TOP_IP = ACTUAL_TOP_IP  <--- registramos la ip con más actividad
    }
    Si no {
        LAST_STATE = 0          <--- No se registraron anomalías
        LAST_TOP_IP = None
    }

3. Si ALERT_LEVEL != 0  {
    Enviar mensaje correo ALERT_LEVEL
    <--- ALERT_LEVEL 1 : Cuando ha habido anomalía aislada
    <--- ALERT_LEVEL 2 : Cuando ha habido anomalía mantenida desde el ultimo TIME_WINDOW
    <--- ALERT_LEVEL 3 : Cuando ha habido anomalía mantenida desde el ultimo TIME_WINDOW y ACTUAL_TOP_IP = LAST_TOP_IP

}
```

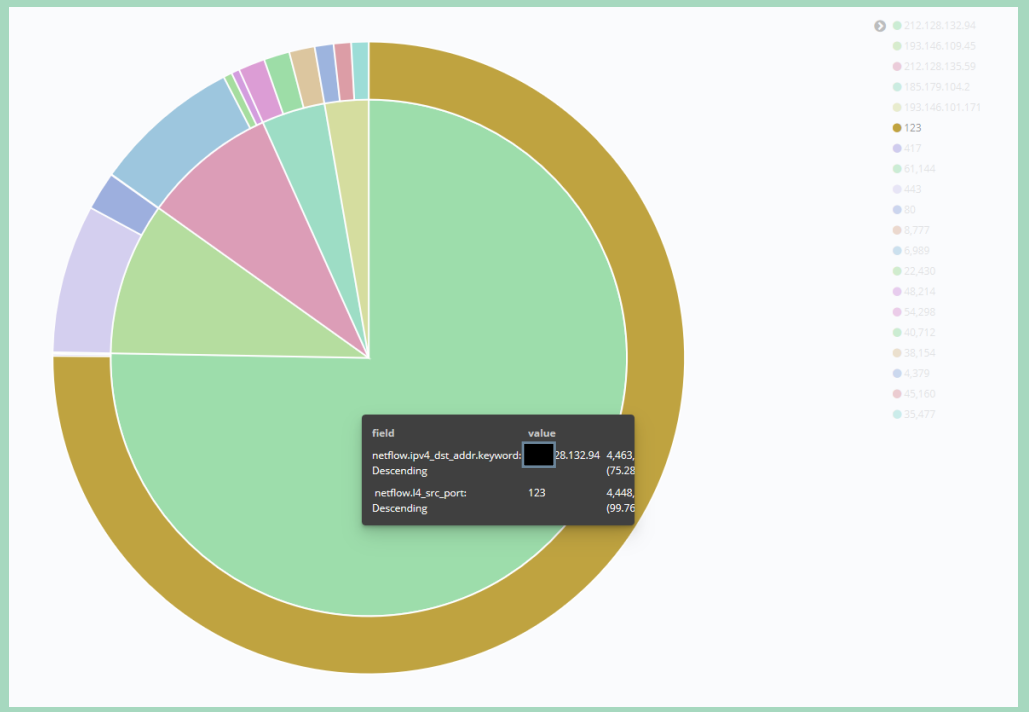
Alertas Proactivas

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

kibana



DDOS amplificación NTP



Alertas Proactivas

REDCAYLE
RED DE CIENCIA Y TECNOLOGÍA
CASTILLA Y LEÓN

05 python

```
root@srv-elk:/home/elk/python_script# python3 script.py
LAST_STATE: 1
LAST_TOPIP: ['[redacted]128.132.94', '[redacted]146.109.45', '[redacted]43.79.232', '[redacted]128.135.105', '[redacted].128.161.136']
[+] Connection: <Elasticsearch([{'host': 'localhost', 'port': 9200}])>
[+] Total flow bytes (in GBps) NO TREATMENT: 514192551.0
[+] Total flow bytes (in GBps): 411.3540408
[+] Total Gbps: 1.371180136
[+][+] TOP_DST_PORTS: 19003
[+][+] TOP_SRC_PORTS: 123
[+] Top 1 destiny IP by bytes: [redacted]128.132.94 with 0.509165897 Gbpsc
[+] Top 2 destiny IP by bytes: [redacted]146.109.45 with 0.000594787 Gbpsc
[+] Top 3 destiny IP by bytes: [redacted]128.135.59 with 0.000364584 Gbpsc
[+] Top 4 destiny IP by bytes: [redacted]128.161.136 with 0.000258483 Gbpsc
[+] Top 5 destiny IP by bytes: [redacted]128.134.24 with 0.000174179 Gbpsc
[+] local ips [[redacted].128.132.94', [redacted].146.109.45', [redacted].128.135.59', [redacted].128.161.136', '[redacted]128.134.24']
ALERT LEVEL 1
ALERT LEVEL 2
ALERT LEVEL 3
```

Gracias !!


SCAYLE
Europa impulsa
nuestro crecimiento
FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)
UNIÓN EUROPEA
universidad de león
Junta de Castilla y León