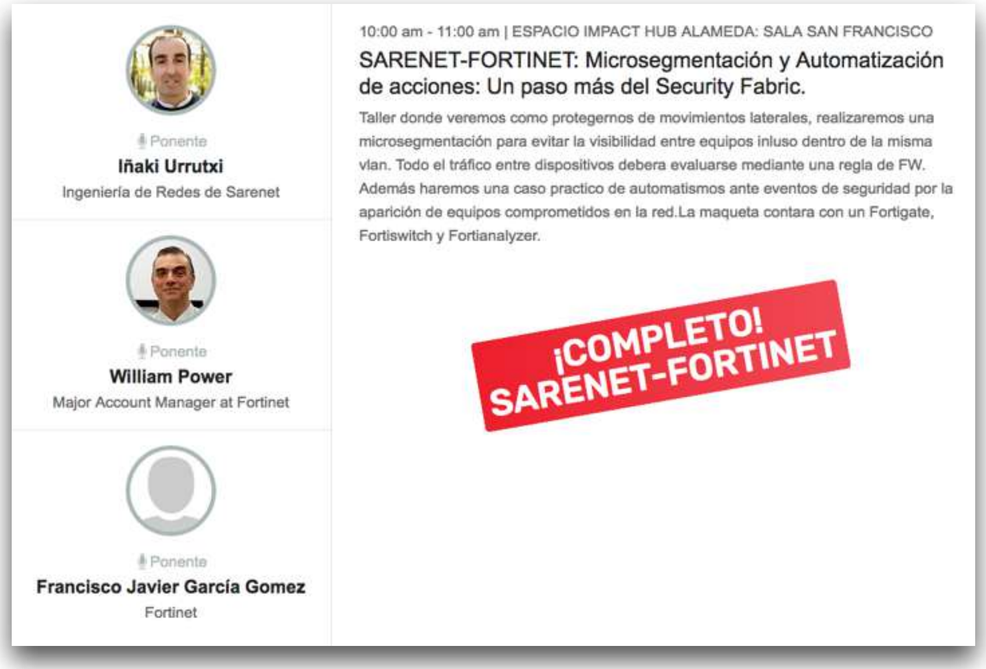
¡Bienvenidos a la primera edición de la Semana de la Ciberseguridad organizada por Sarenet !

sarenet

Agenda de la jornada: talleres prácticos



Ponente
Iñaki Urrutxi
Ingeniería de Redes de Sarenet

Ponente
William Power
Major Account Manager at Fortinet

Ponente
Francisco Javier García Gomez
Fortinet

10:00 am - 11:00 am | ESPACIO IMPACT HUB ALAMEDA: SALA SAN FRANCISCO

SARENET-FORTINET: Microsegmentación y Automatización de acciones: Un paso más del Security Fabric.

Taller donde veremos como protegernos de movimientos laterales, realizaremos una microsegmentación para evitar la visibilidad entre equipos inluso dentro de la misma vlan. Todo el tráfico entre dispositivos debera evaluarse mediante una regla de FW. Además haremos una caso practico de automatismos ante eventos de seguridad por la aparición de equipos comprometidos en la red.La maqueta contara con un Fortigate, Fortiswitch y Fortianalyzer.

¡COMPLETO! SARENET-FORTINET

Ponente
Iñigo Losada
Ingeniería de Clientes y Ciberseguridad de Sarenet

Ponente
Víctor Egido Andrés CISM
Enterprise Sales Engineer at Tenable

10:00 am - 11:00 am | ESPACIO IMPACT HUB ALAMEDA: SALA BOGOTÁ

SARENET-TENABLE: Cómo utilizar el servicio de auditorías contínuas para conseguir un cumplimiento normativo de estándares (GDPR, ISO, CISS, PCI).

Mejores prácticas en la gestión de sistemas.
Ajuste del estado de seguridad de los activos.

APÚNTATE A ESTE TALLER 2 SARENET-TENABLE

Ponente
Karmele Fernández
Ingeniería de Clientes y Ciberseguridad de Sarenet

10:00 am - 11:00 am | ESPACIO IMPACT HUB ALAMEDA: SALA LONDRES

SARENET: Y si todo falla...Veeam Backup

En este taller, aprenderemos a configurar Veeam Backup & Replication para poder crear backups y replicas en la nube, a través del servicio Cloud Connect. Además, aprenderemos algunos trucos para optimizar la configuración de este servicio y otras características de Veeam.

APÚNTATE A ESTE TALLER 3 SARENET-VEEAM

sarenet

Webinars

Lunes
6 de Mayo de 2019
WEBINAR

10:00 - 10:20

Sergio Mendoza Martin
Sophos End-Point y campañas de concienciación

Seguridad avanzada en el puesto y como concienciar a nuestros usuarios

16:00 - 16:20

Aitor Lejarzegi
¿Qué podemos ofrecer a una empresa como la tuya? Casos de éxito y ejemplos

IoT Industrial, ayudas de la SPRI, Segmentación

Miércoles
8 de Mayo de 2019
WEBINAR

10:00 - 10:20

José Ramón Fernández de Alarcón
Auditorías continuas de seguridad

12:00 - 12:20

Egoitz Aurrekoetxea
Seguridad y prevención de problemas en el Correo corporativo

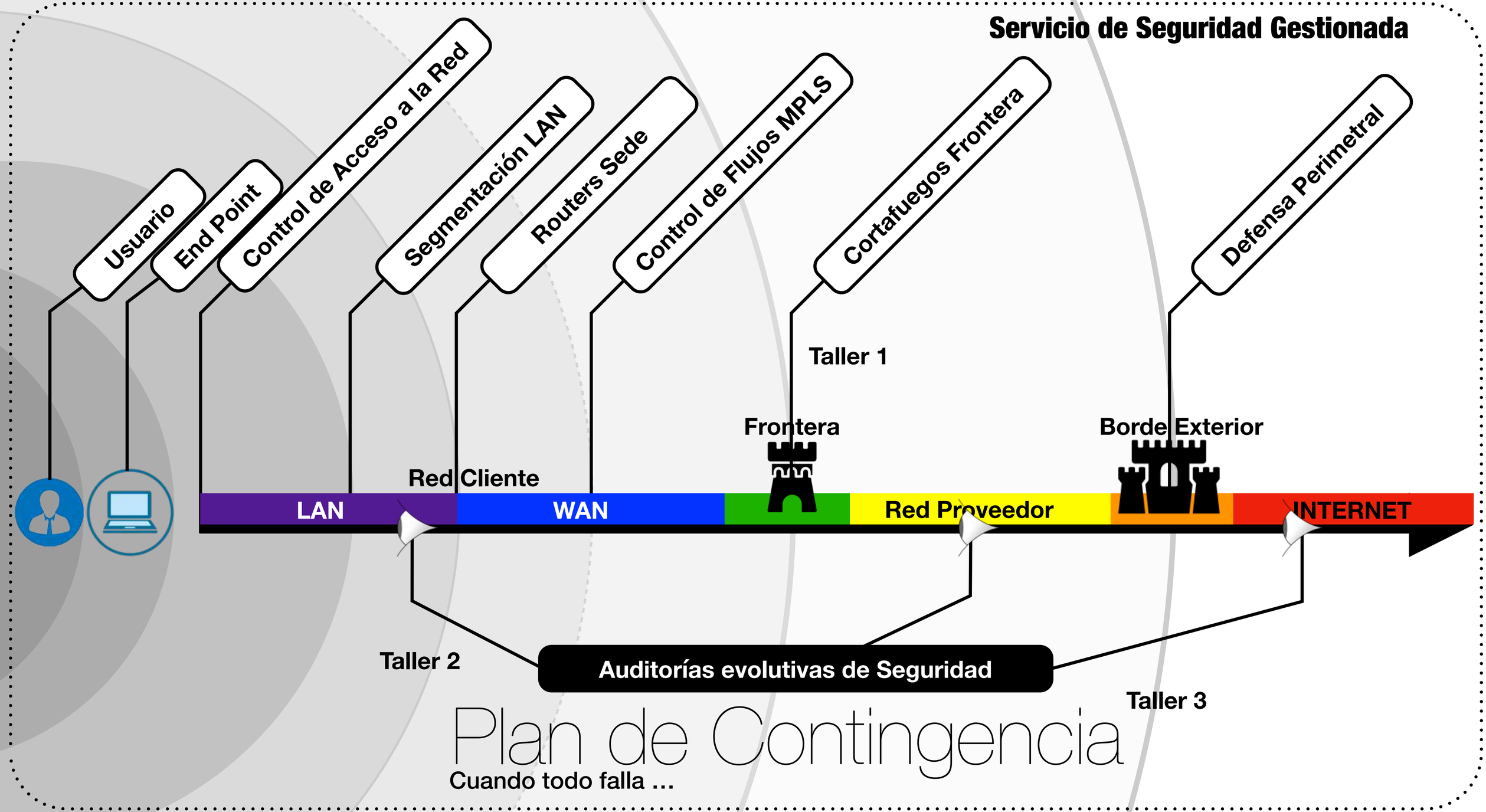
- ✔ Cómo hacer uso de las herramientas para prevenir problemas
- ✔ Nuevos mecanismos de seguridad
- ✔ DMARC, DKIM, Firmas criptográficas

sarenet

Nuestra propuesta integral de ciberseguridad:

Gestión de riesgos por capas

sarenet


Servicio de Seguridad Gestionada
Usuario
End Point
Control de Acceso a la Red
Segmentación LAN
Routers Sede
Control de Flujos MPLS
Cortafuegos Frontera
Defensa Perimetral
Taller 1
Frontera
Borde Exterior
Red Cliente
LAN
WAN
Red Proveedor
INTERNET
Taller 2
Auditorías evolutivas de Seguridad
Taller 3
Plan de Contingencia
Cuando todo falla ...

Riesgo : Contingencia o proximidad de un daño

Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización

Medidas de reducción de probabilidad

De eliminación — Impide que tenga lugar

Preventiva — Reduce las oportunidades de que el suceso ocurra

Disuasoria — Disuade al atacante

De monitorización — Atajan el incidente o aprenden

De detección — Ayudan a actuar rápidamente si el suceso ya a tenido lugar

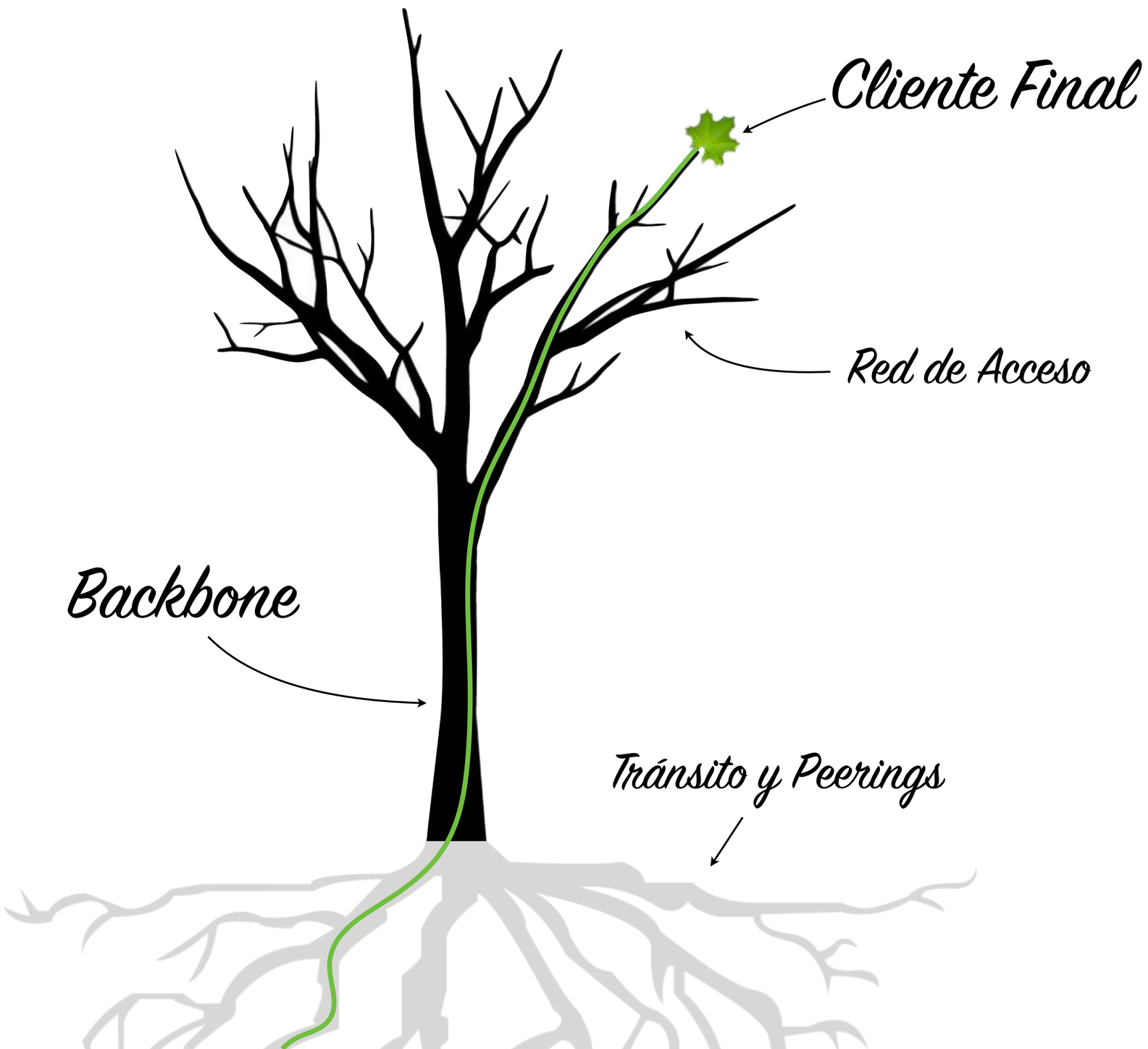
Medidas de reducción de impacto

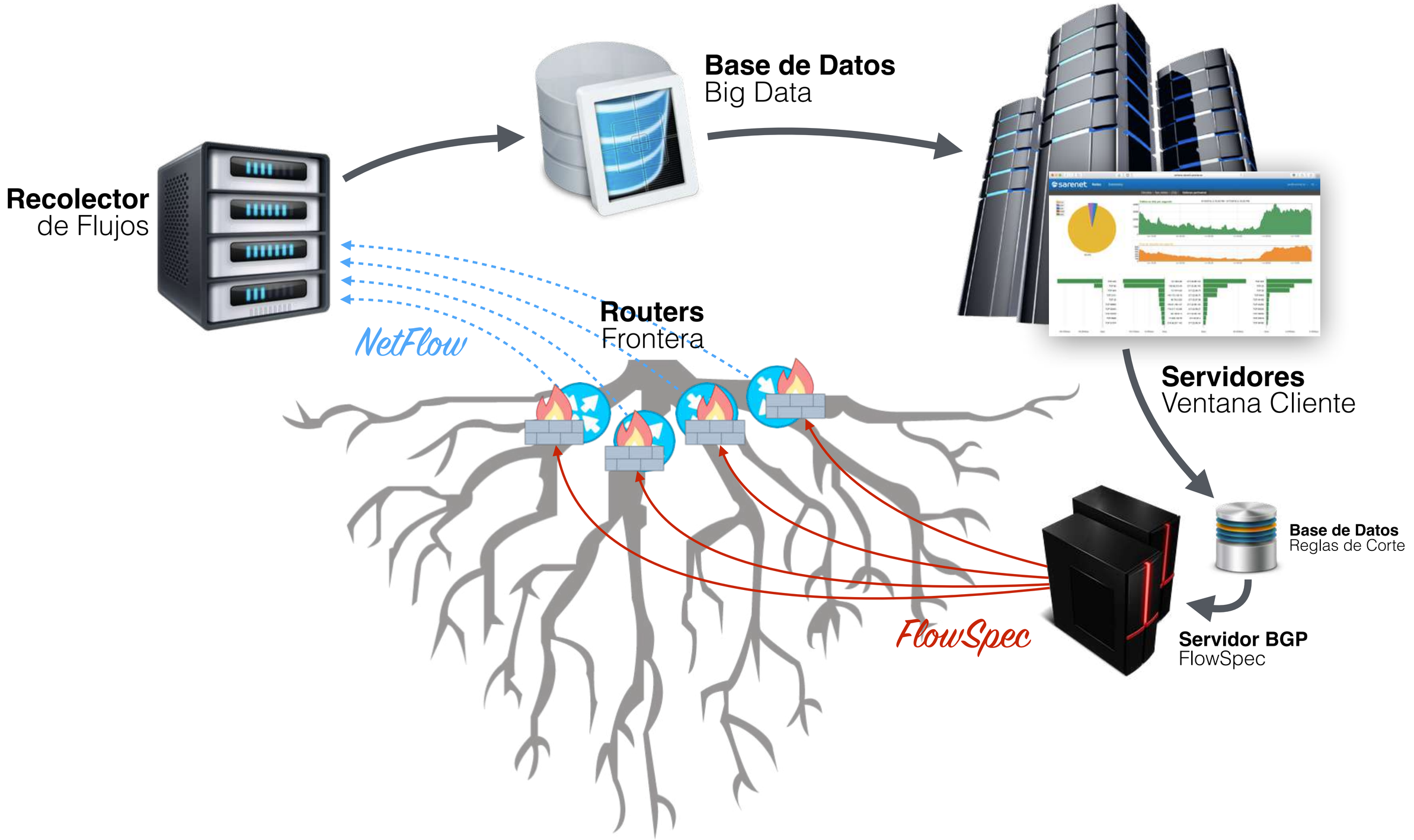
Minimizadoras — Cobertura de un seguro , cumplimiento de la legislación

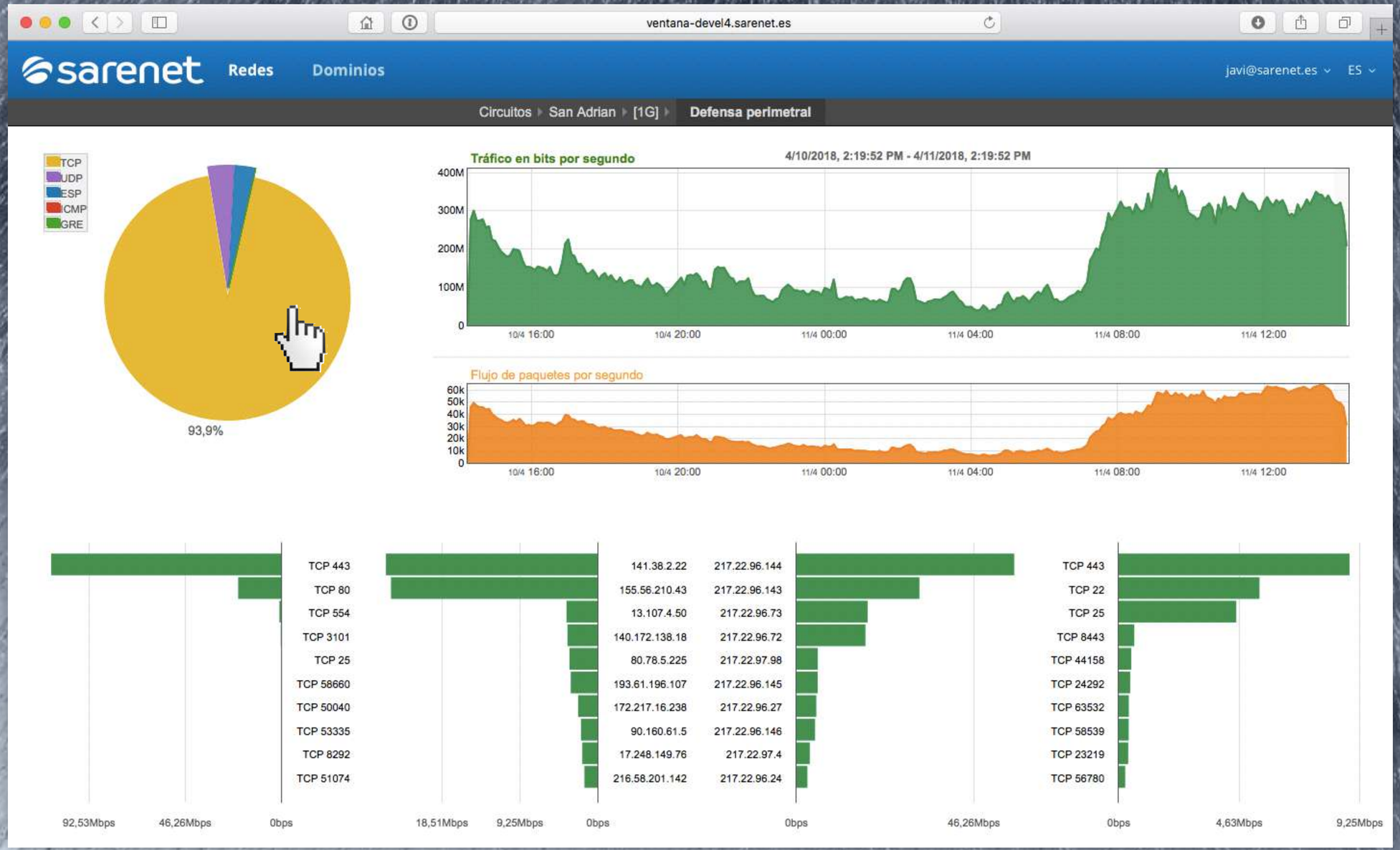
Correctivas o Recuperativas — El incidente ocurre pero lo repara

sarenet

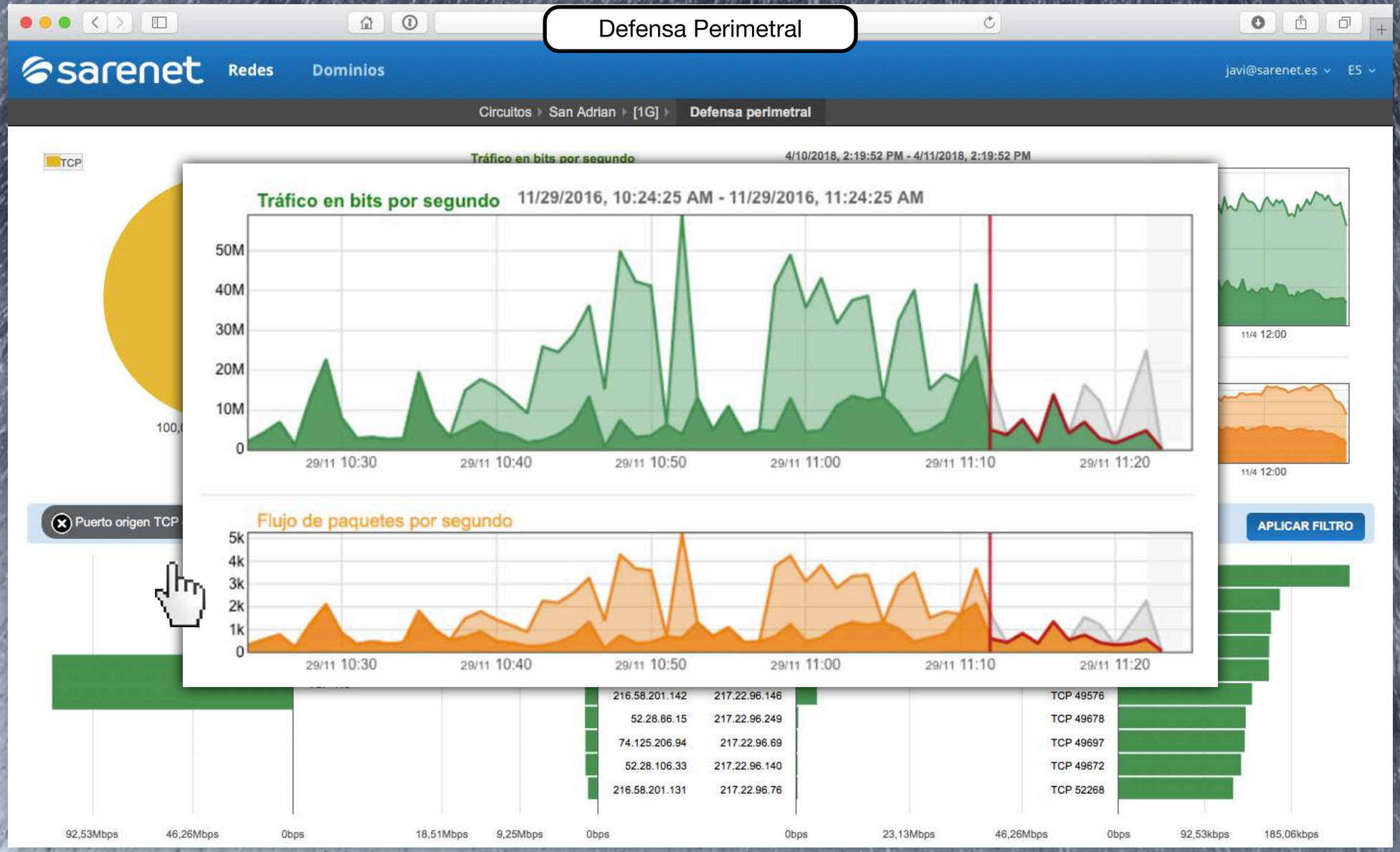
Defensa Perimetral


Cliente Final
Red de Acceso
Backbone
Tránsito y Peerings


Base de Datos
Big Data
Recolector
de Flujos
NetFlow
Routers
Frontera
Servidores
Ventana Cliente
Base de Datos
Reglas de Corte
FlowSpec
Servidor BGP
FlowSpec


ventana-devel4.sarenet.es
sarenet
Redes
Dominios
javi@sarenet.es
ES
Circuitos
San Adrian
[1G]
Defensa perimetral
TCP
UDP
ESP
ICMP
GRE
93,9%
Tráfico en bits por segundo
4/10/2018, 2:19:52 PM - 4/11/2018, 2:19:52 PM
400M
300M
200M
100M
0
10/4 16:00
10/4 20:00
11/4 00:00
11/4 04:00
11/4 08:00
11/4 12:00
Flujo de paquetes por segundo
60k
50k
40k
30k
20k
10k
0
10/4 16:00
10/4 20:00
11/4 00:00
11/4 04:00
11/4 08:00
11/4 12:00
TCP 443
TCP 80
TCP 554
TCP 3101
TCP 25
TCP 58660
TCP 50040
TCP 53335
TCP 8292
TCP 51074
92,53Mbps
46,26Mbps
0bps
141.38.2.22
155.56.210.43
13.107.4.50
140.172.138.18
80.78.5.225
193.61.196.107
172.217.16.238
90.160.61.5
17.248.149.76
216.58.201.142
18,51Mbps
9,25Mbps
0bps
217.22.96.144
217.22.96.143
217.22.96.73
217.22.96.72
217.22.97.98
217.22.96.145
217.22.96.27
217.22.96.146
217.22.97.4
217.22.96.24
0bps
46,26Mbps
TCP 443
TCP 22
TCP 25
TCP 8443
TCP 44158
TCP 24292
TCP 63532
TCP 58539
TCP 23219
TCP 56780
0bps
4,63Mbps
9,25Mbps

Defensa Perimetral



Cortafuegos Frontera

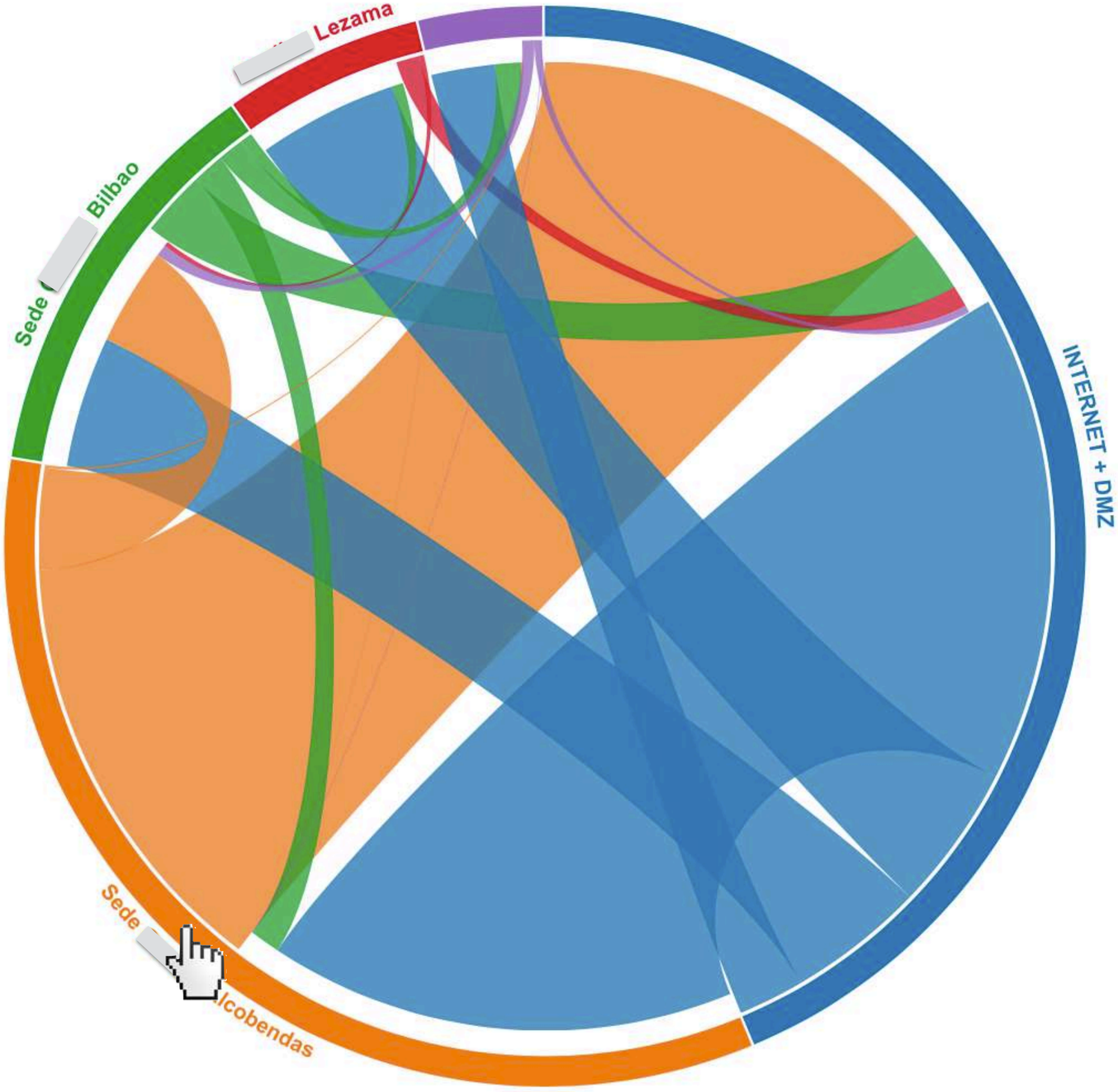
sarenet

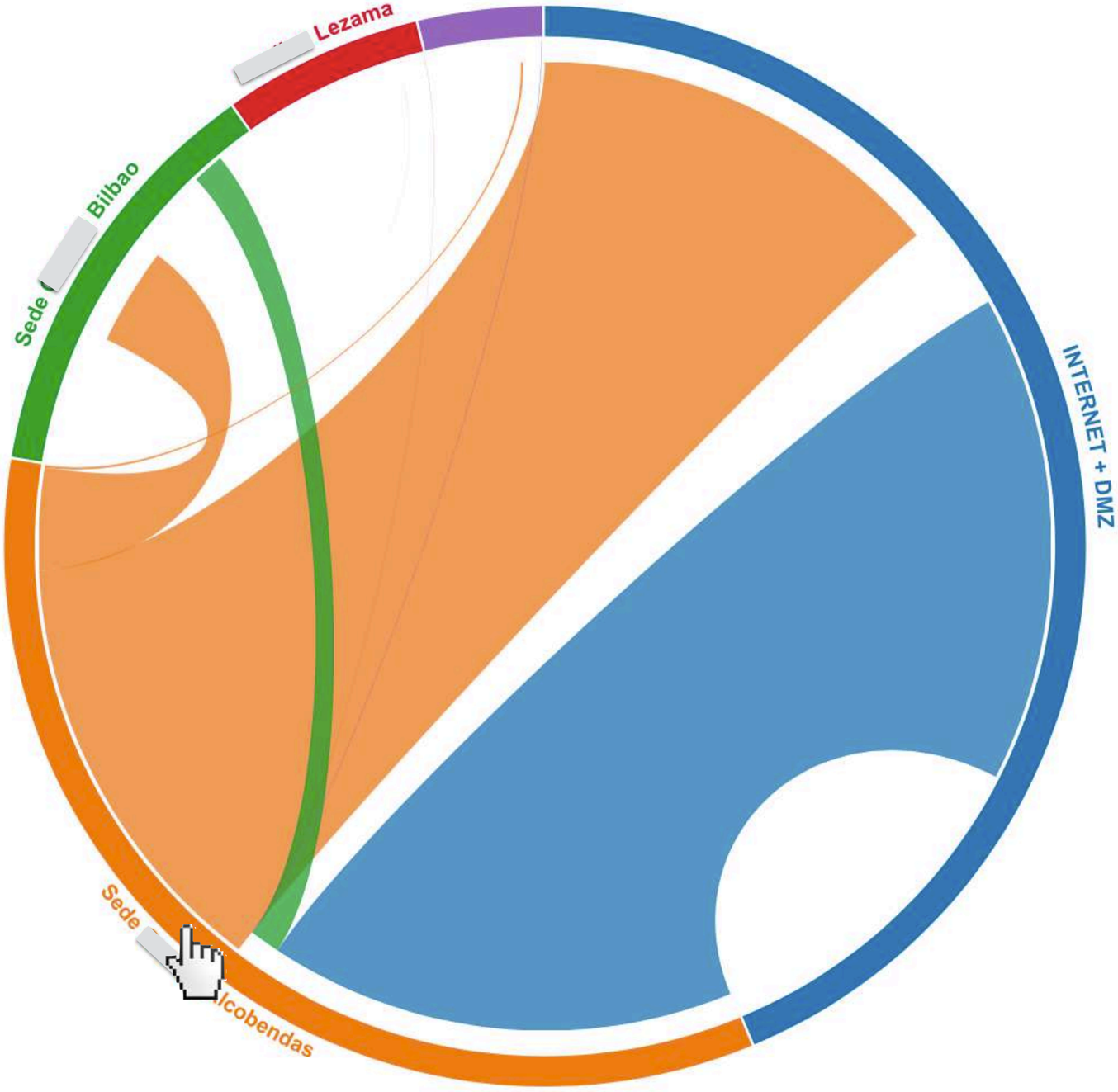
FORTINET

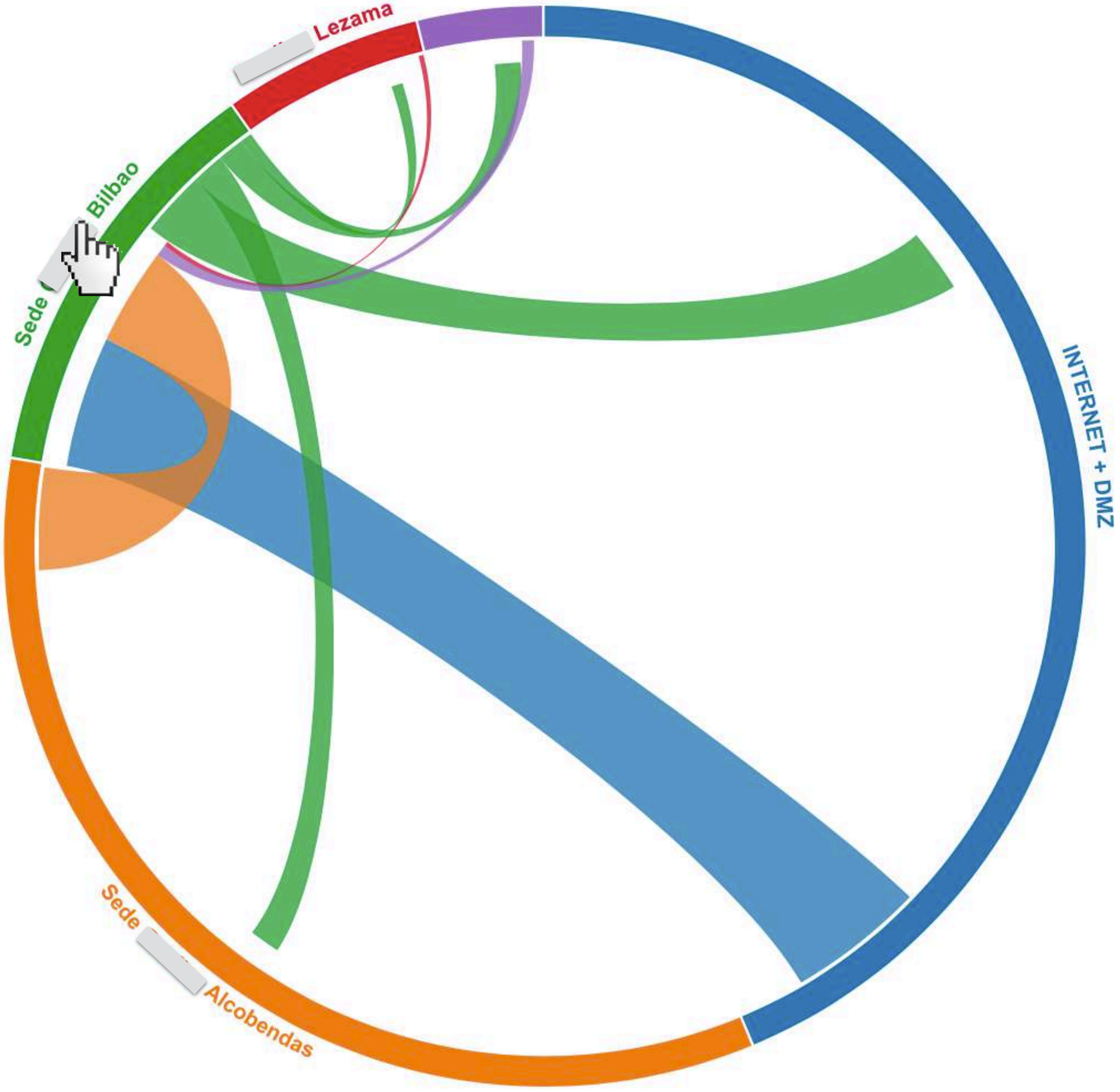
MSSP Partner

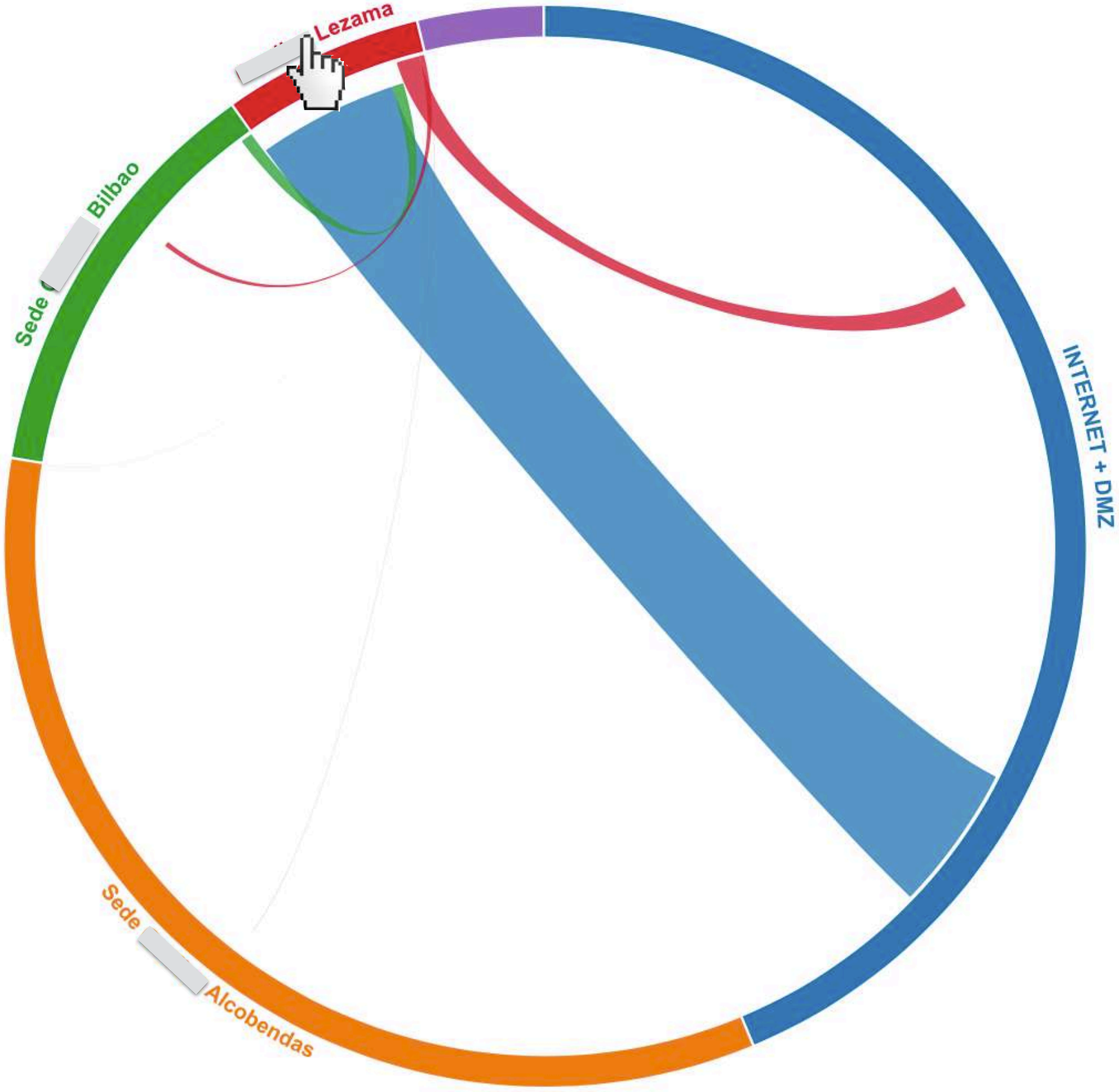
- Anti-botnet
- IP Reputation
- Intrusion Prevention
- Application Control
- Antivirus
- Web Application Security
- Vulnerability Management
- Advanced Threat Protection
- Anti-spam
- Database Protection
- Web Filtering
- Industrial Security Service

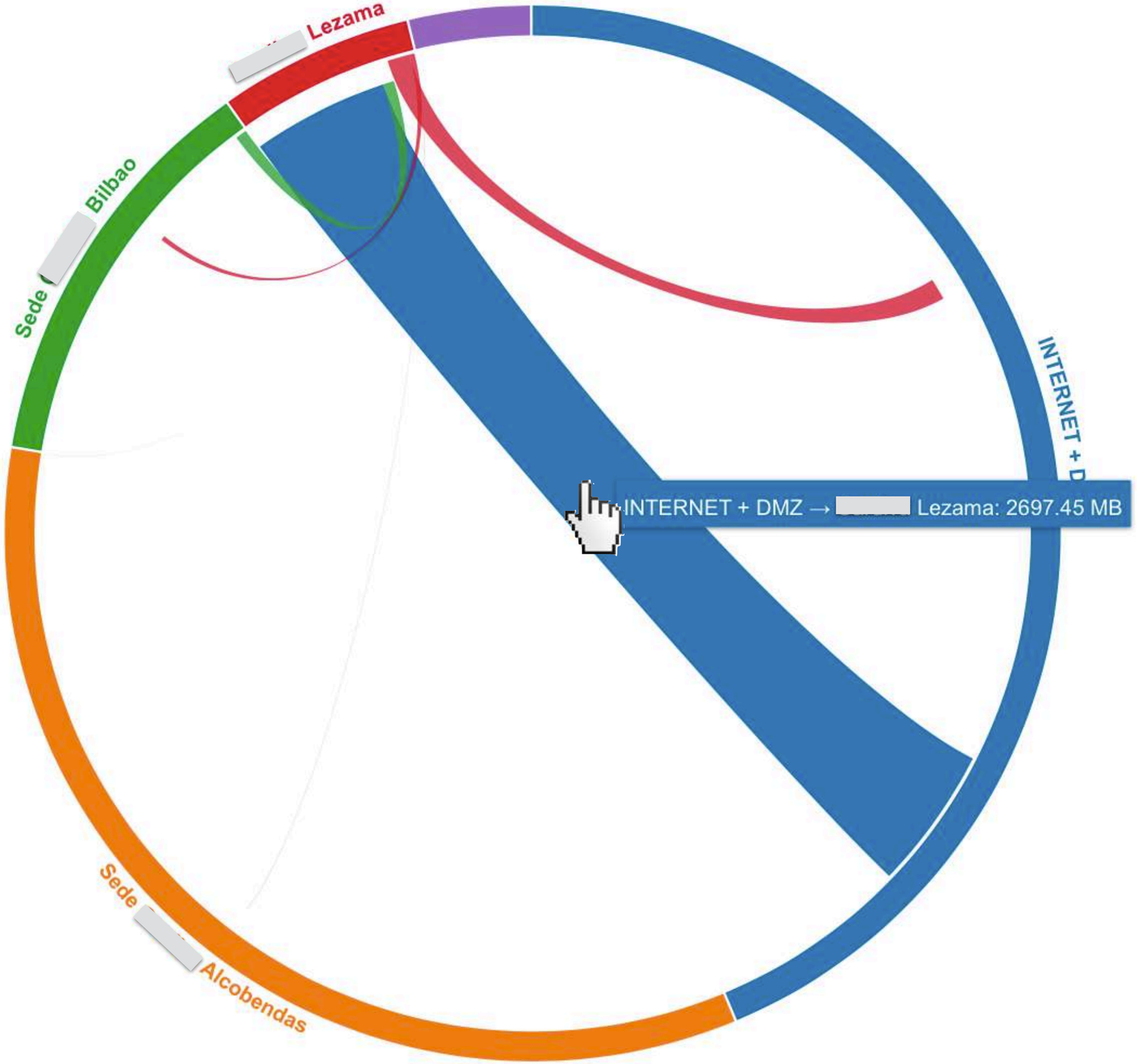
Control de Flujos MPLS

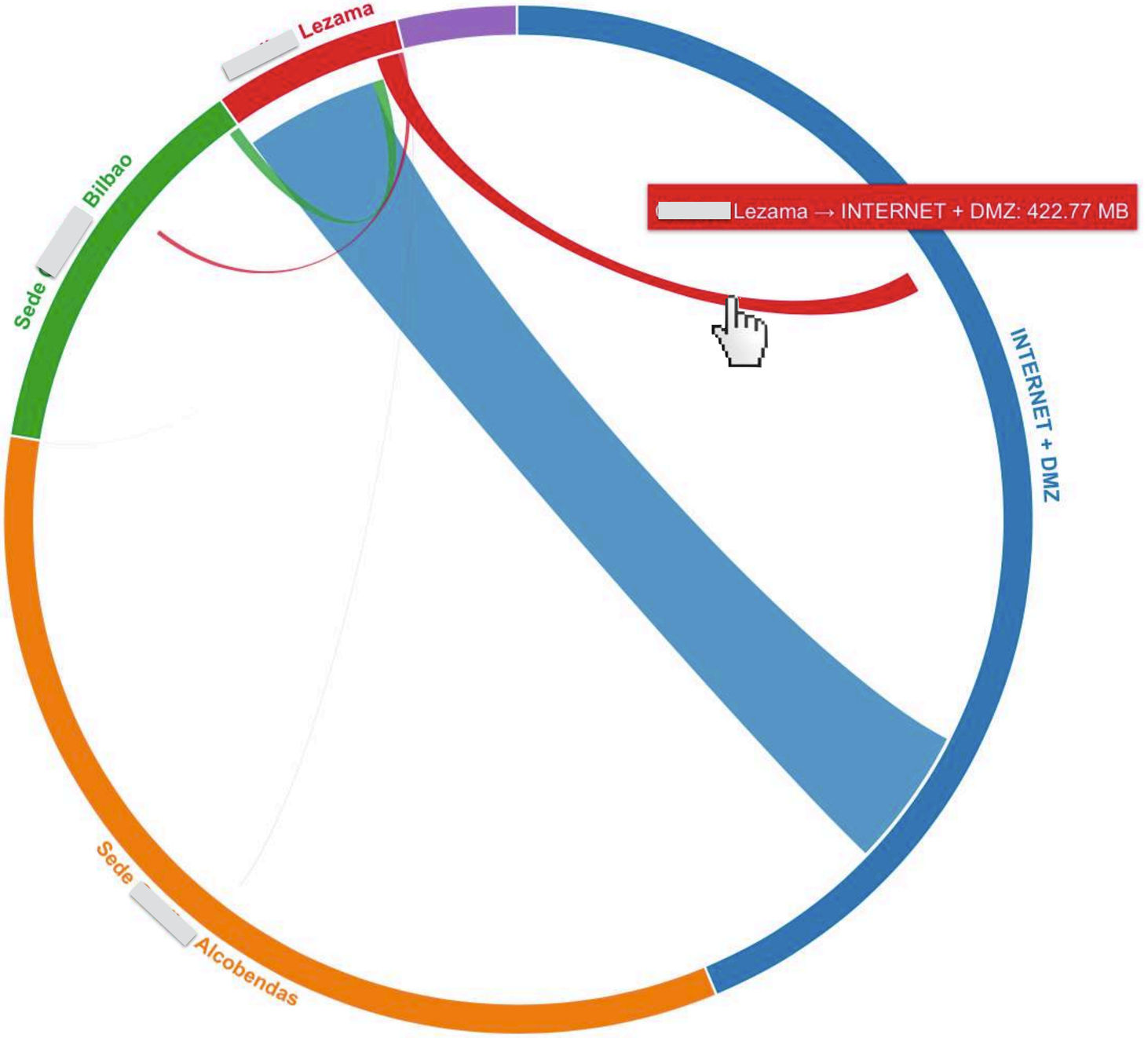

Lezama
Bilbao
Sede
INTERNET + DMZ
Sede
Alcobendas

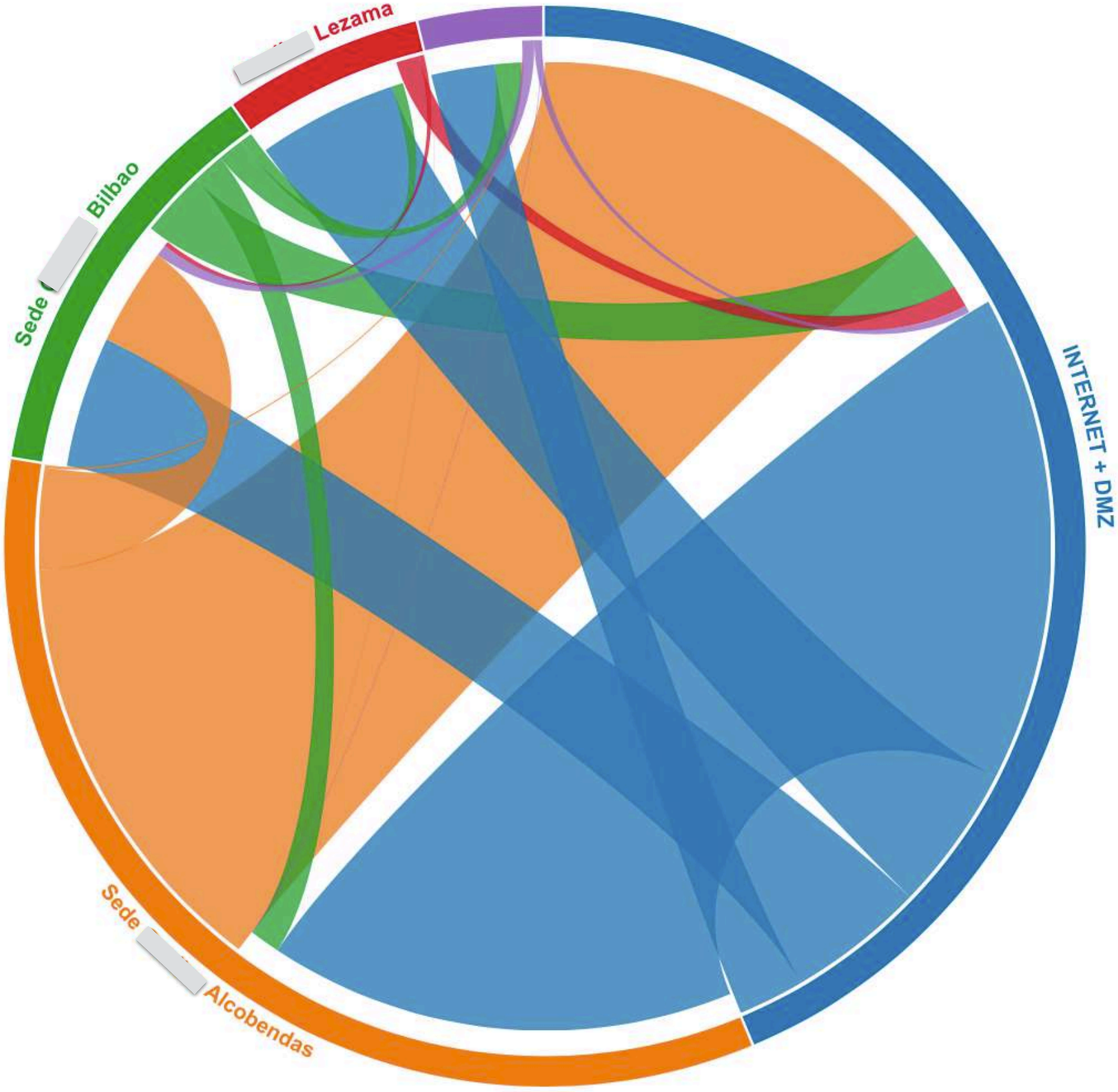

Lezama
Bilbao
Sede
INTERNET + DMZ
Sede
Alcobendas

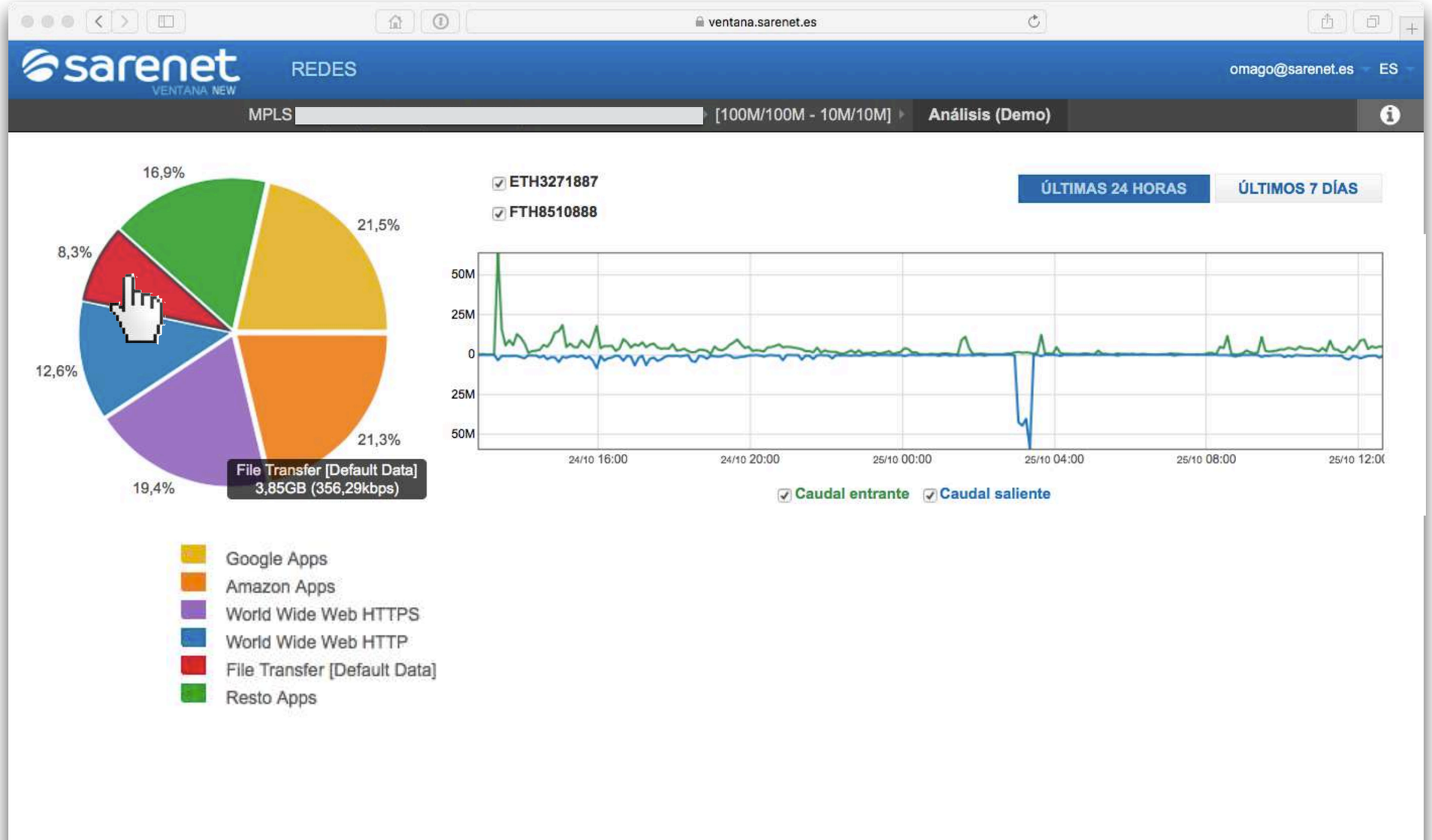

Lezama
Bilbao
INTERNET + DMZ
Alcobendas

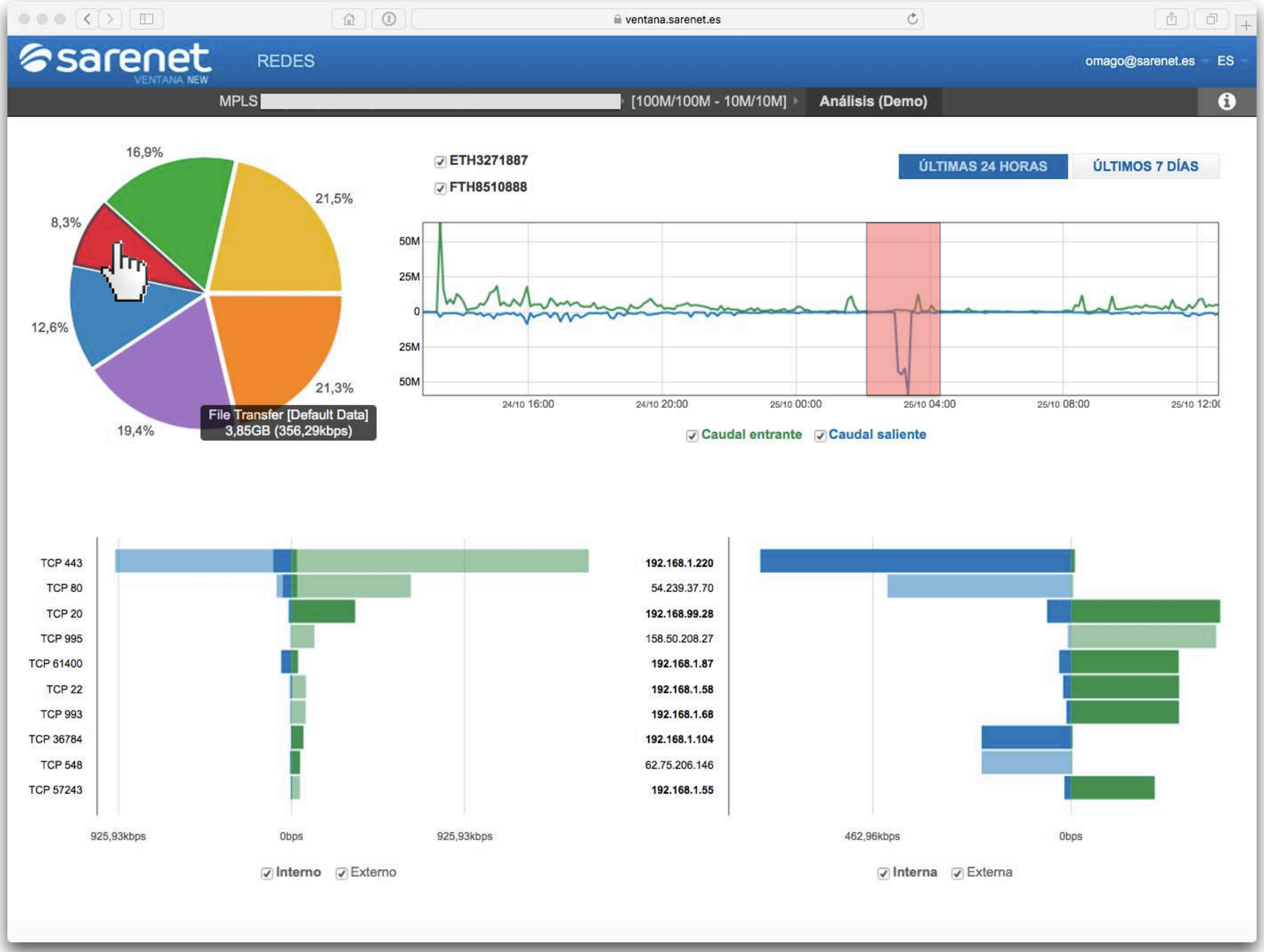

Lezama
Bilbao
Sede
INTERNET + DMZ
Sede
Alcobendas

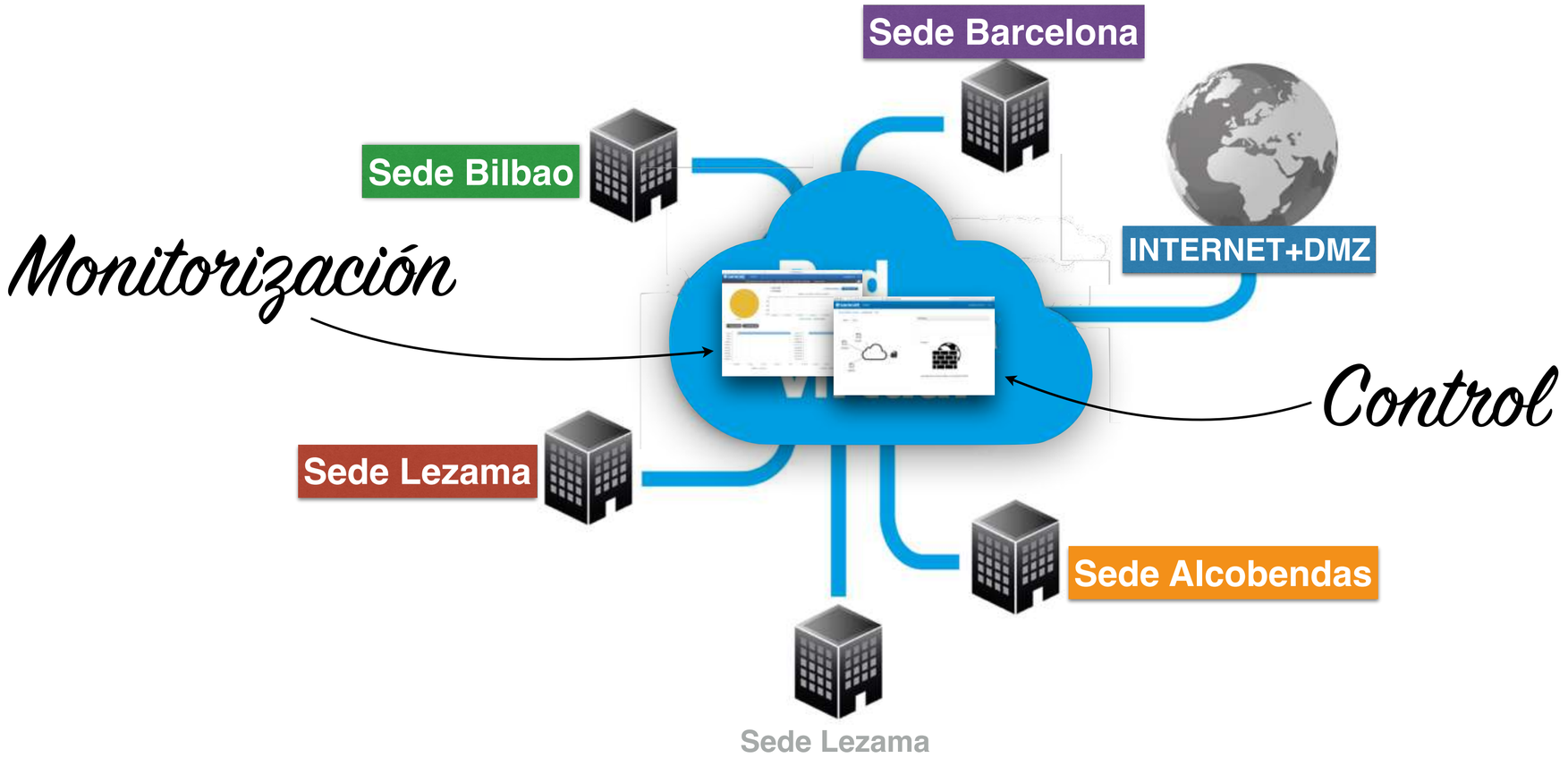

Lezama
Bilbao
Sede
INTERNET + D
INTERNET + DMZ → Lezama: 2697.45 MB
Sede
Alcobendas

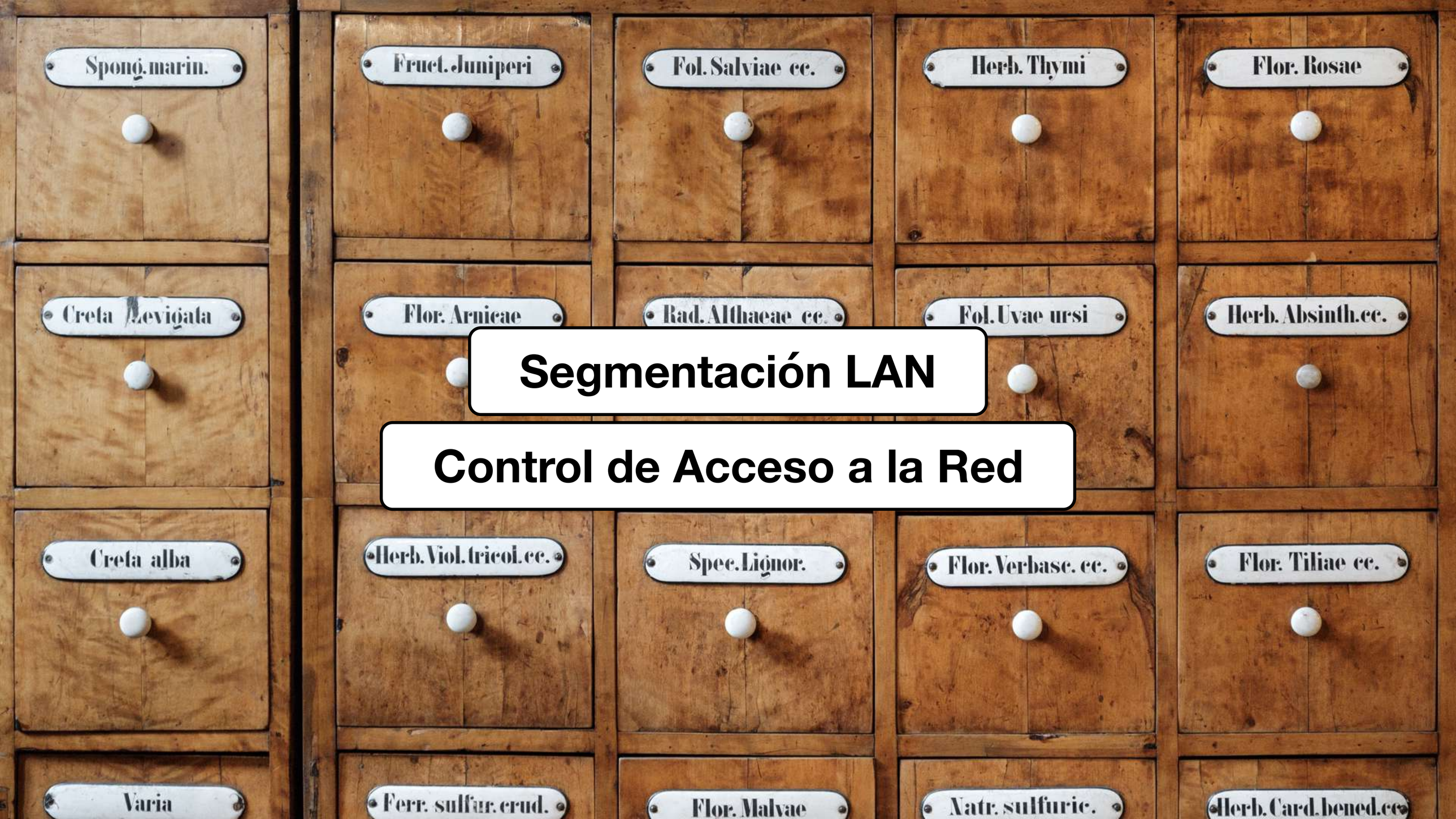

Lezama
Bilbao
Sede
Sede
Alcobendas
INTERNET + DMZ
Lezama → INTERNET + DMZ: 422.77 MB


Lezama
Bilbao
INTERNET + DMZ
Alcobendas


ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
16,9%
21,5%
8,3%
12,6%
21,3%
19,4%
File Transfer [Default Data]
3,85GB (356,29kbps)
Google Apps
Amazon Apps
World Wide Web HTTPS
World Wide Web HTTP
File Transfer [Default Data]
Resto Apps
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
50M
25M
0
25M
50M
24/10 16:00
24/10 20:00
25/10 00:00
25/10 04:00
25/10 08:00
Caudal entrante
Caudal saliente


ventana.sarenet.es
sarenet
VENTANA NEW
REDES
omago@sarenet.es
ES
MPLS
[100M/100M - 10M/10M]
Análisis (Demo)
16,9%
21,5%
8,3%
12,6%
21,3%
19,4%
File Transfer [Default Data]
3,85GB (356,29kbps)
ETH3271887
FTH8510888
ÚLTIMAS 24 HORAS
ÚLTIMOS 7 DÍAS
50M
25M
0
25M
50M
24/10 16:00
24/10 20:00
25/10 00:00
25/10 04:00
25/10 08:00
25/10 12:0
Caudal entrante
Caudal saliente
TCP 443
TCP 80
TCP 20
TCP 995
TCP 61400
TCP 22
TCP 993
TCP 36784
TCP 548
TCP 57243
925,93kbps
0bps
925,93kbps
Interno
Externo
192.168.1.220
54.239.37.70
192.168.99.28
158.50.208.27
192.168.1.87
192.168.1.58
192.168.1.68
192.168.1.104
62.75.206.146
192.168.1.55
462,96kbps
0bps
Interna
Externa


Sede Barcelona
Sede Bilbao
Monitorización
INTERNET+DMZ
Control
Sede Lezama
Sede Alcobendas
Sede Lezama



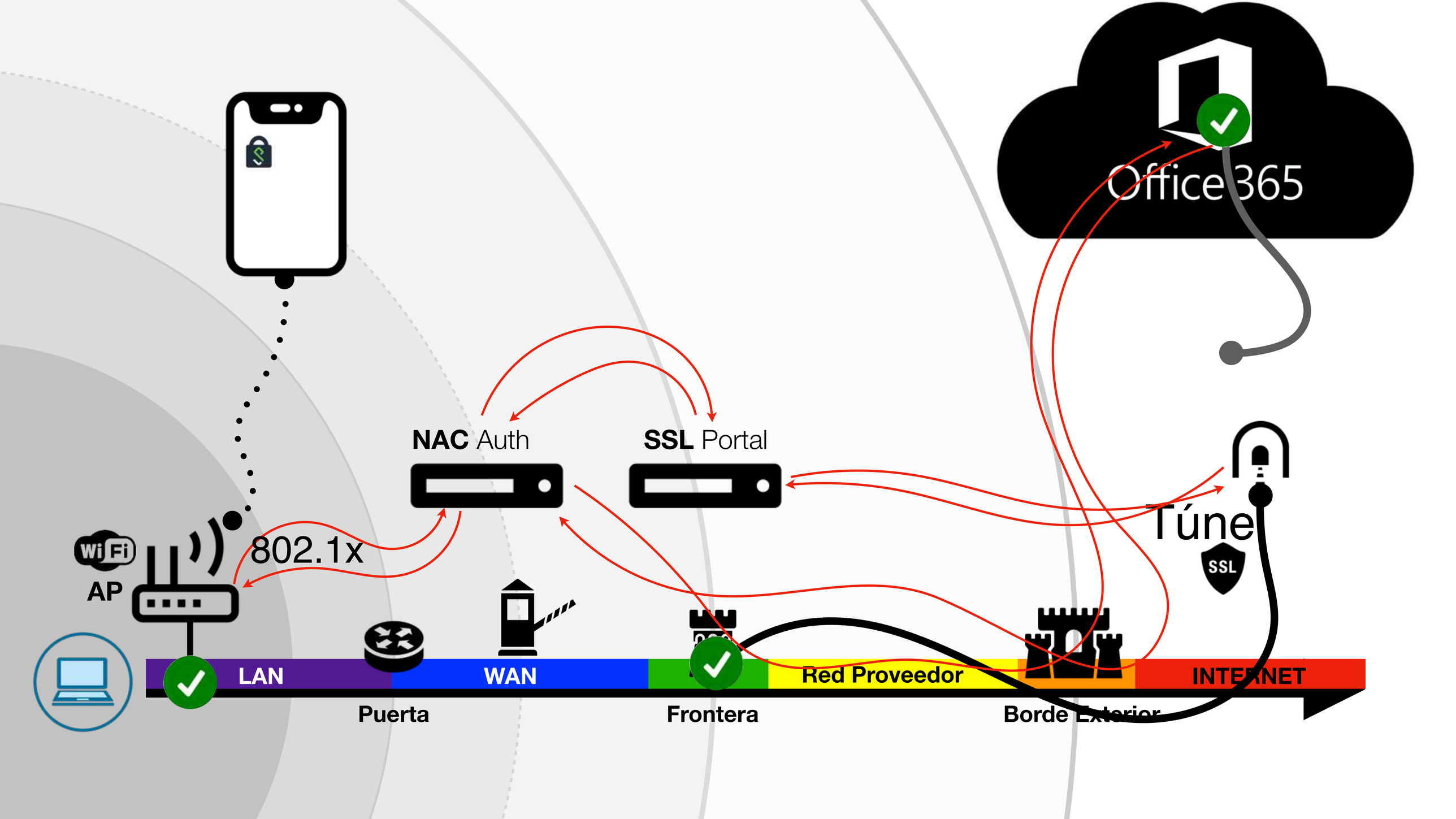
Segmentación LAN

Control de Acceso a la Red

NAC

Control de Acceso a la Red

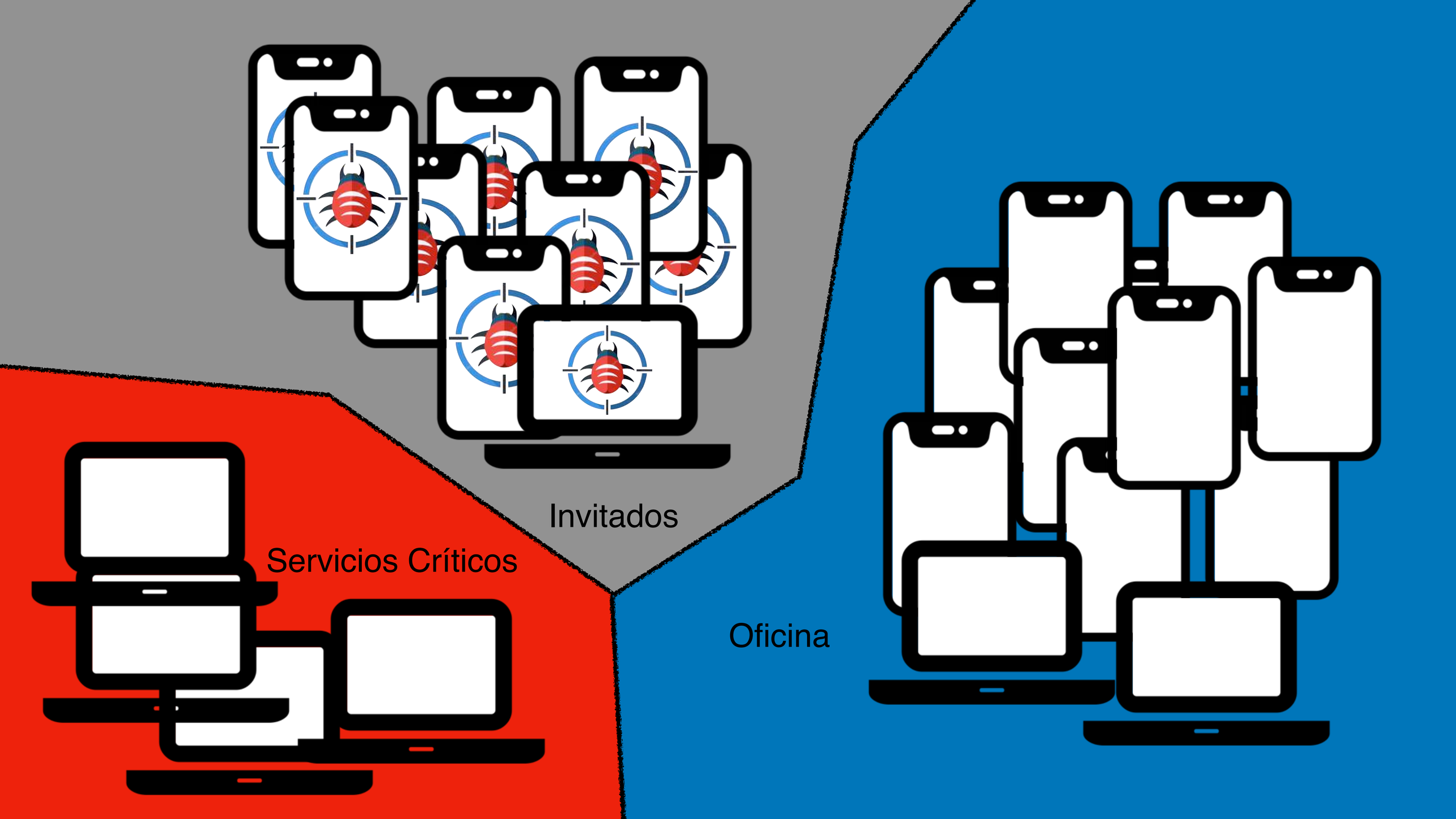
sarenet


Office 365
NAC Auth
SSL Portal
802.1x
AP
Túnel
SSL
LAN
WAN
Red Proveedor
INTERNET
Puerta
Frontera
Borde Exterior

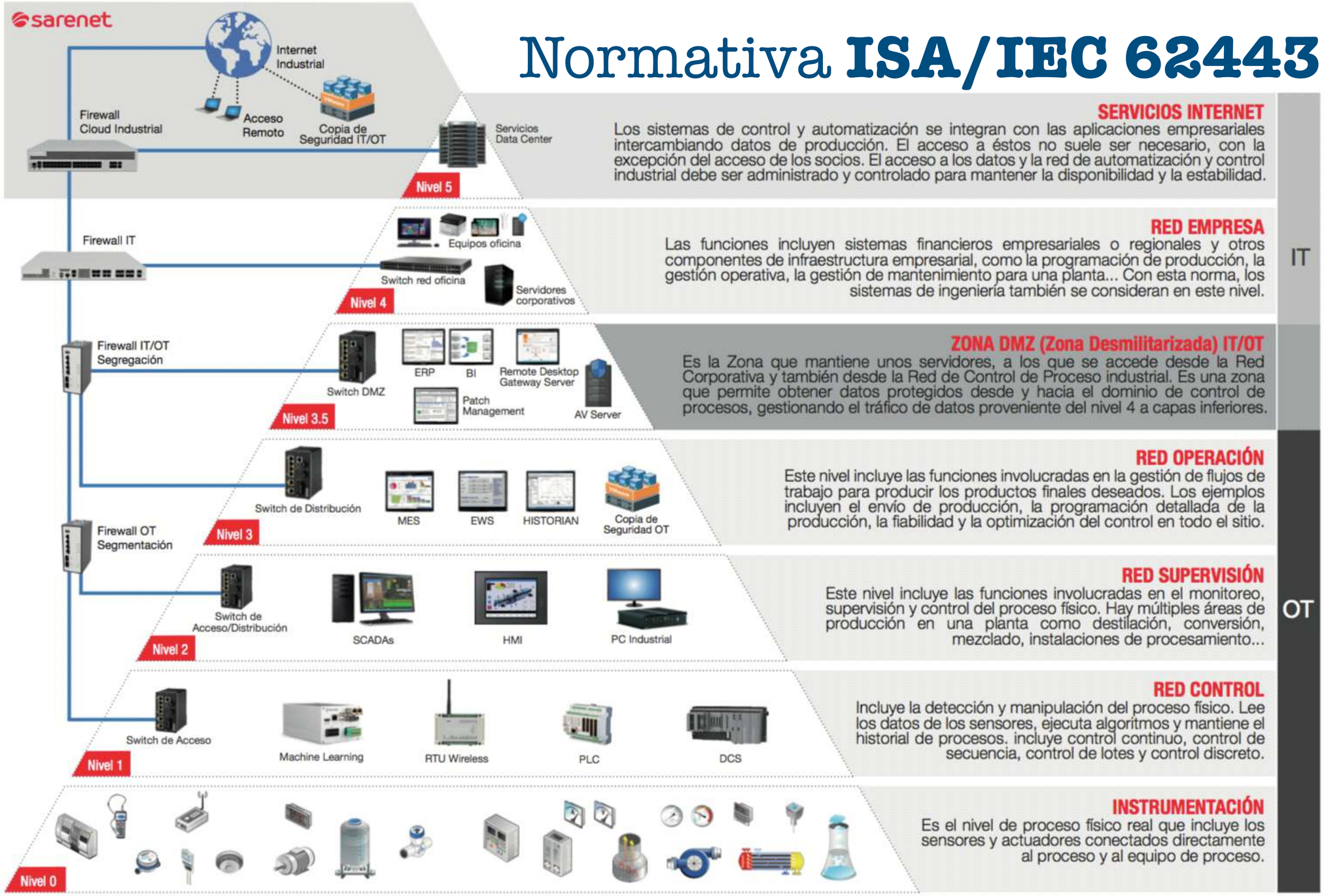
IT/OT

Segmentación LAN

sarenet


Invitados
Servicios Críticos
Oficina

Normativa **ISA/IEC 62443**



SERVICIOS INTERNET
Los sistemas de control y automatización se integran con las aplicaciones empresariales intercambiando datos de producción. El acceso a éstos no suele ser necesario, con la excepción del acceso de los socios. El acceso a los datos y la red de automatización y control industrial debe ser administrado y controlado para mantener la disponibilidad y la estabilidad.

RED EMPRESA
Las funciones incluyen sistemas financieros empresariales o regionales y otros componentes de infraestructura empresarial, como la programación de producción, la gestión operativa, la gestión de mantenimiento para una planta... Con esta norma, los sistemas de ingeniería también se consideran en este nivel.

ZONA DMZ (Zona Desmilitarizada) IT/OT
Es la Zona que mantiene unos servidores, a los que se accede desde la Red Corporativa y también desde la Red de Control de Proceso industrial. Es una zona que permite obtener datos protegidos desde y hacia el dominio de control de procesos, gestionando el tráfico de datos proveniente del nivel 4 a capas inferiores.

RED OPERACIÓN
Este nivel incluye las funciones involucradas en la gestión de flujos de trabajo para producir los productos finales deseados. Los ejemplos incluyen el envío de producción, la programación detallada de la producción, la fiabilidad y la optimización del control en todo el sitio.

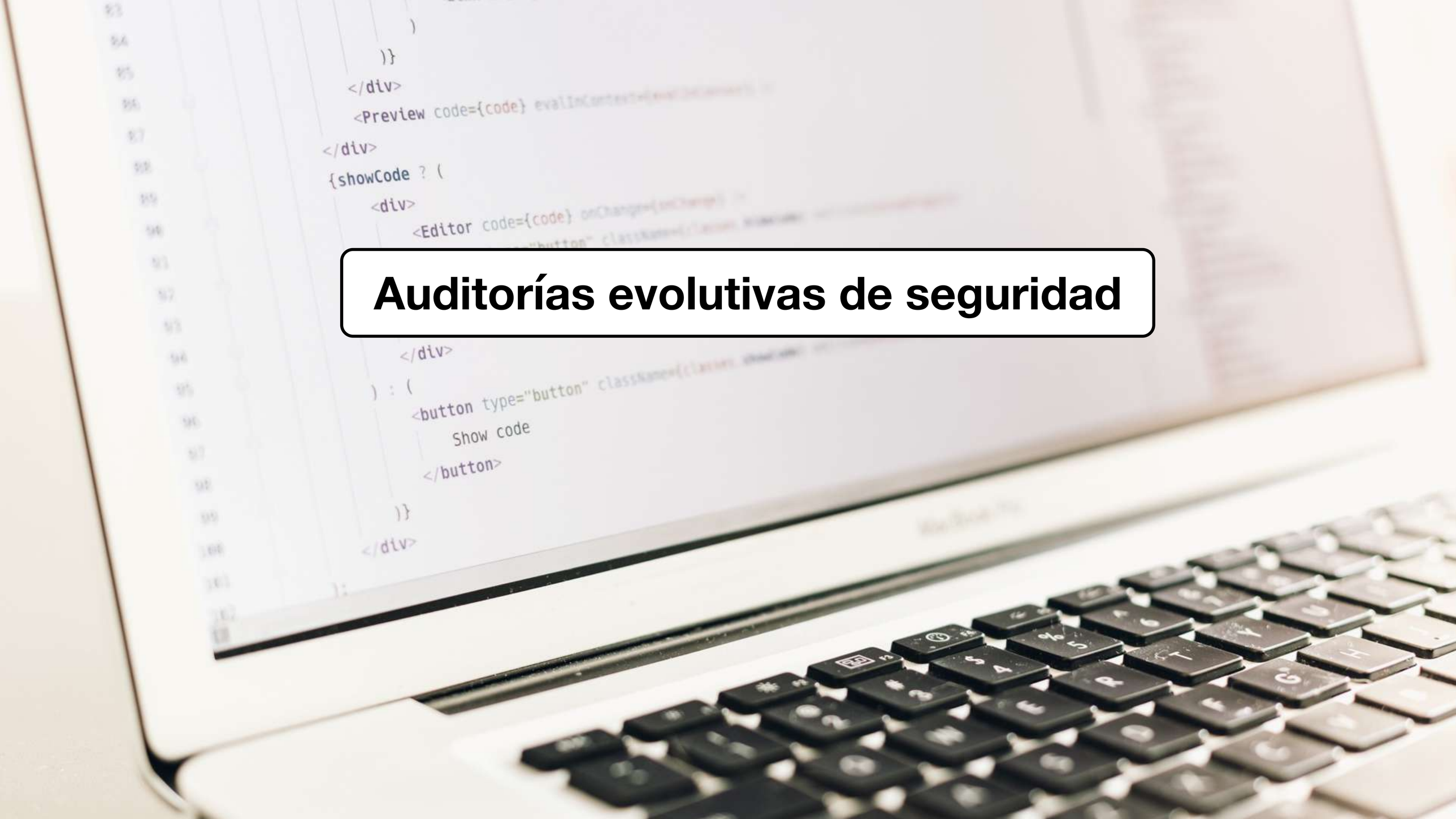
RED SUPERVISIÓN
Este nivel incluye las funciones involucradas en el monitoreo, supervisión y control del proceso físico. Hay múltiples áreas de producción en una planta como destilación, conversión, mezclado, instalaciones de procesamiento...

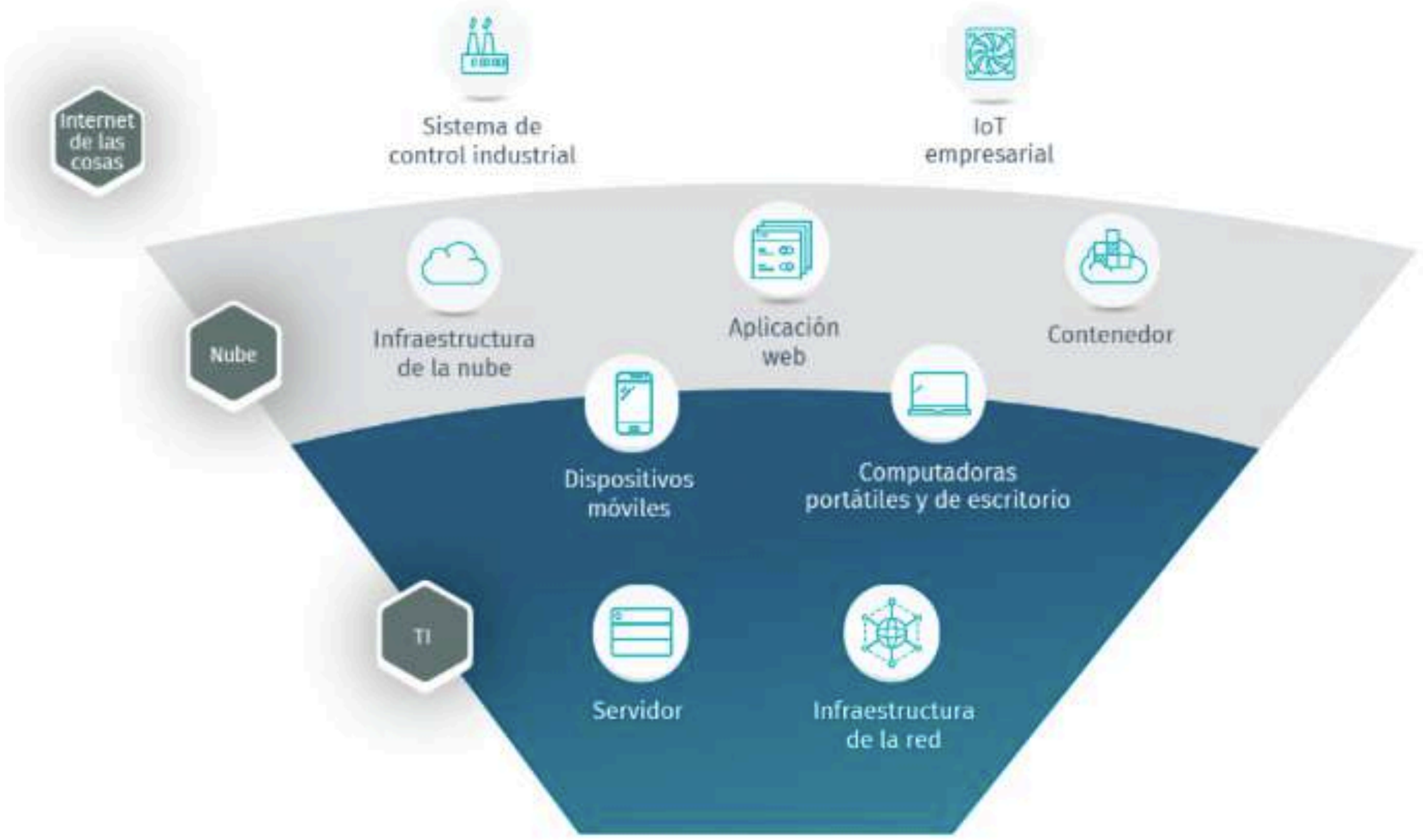
RED CONTROL
Incluye la detección y manipulación del proceso físico. Lee los datos de los sensores, ejecuta algoritmos y mantiene el historial de procesos. incluye control continuo, control de secuencia, control de lotes y control discreto.

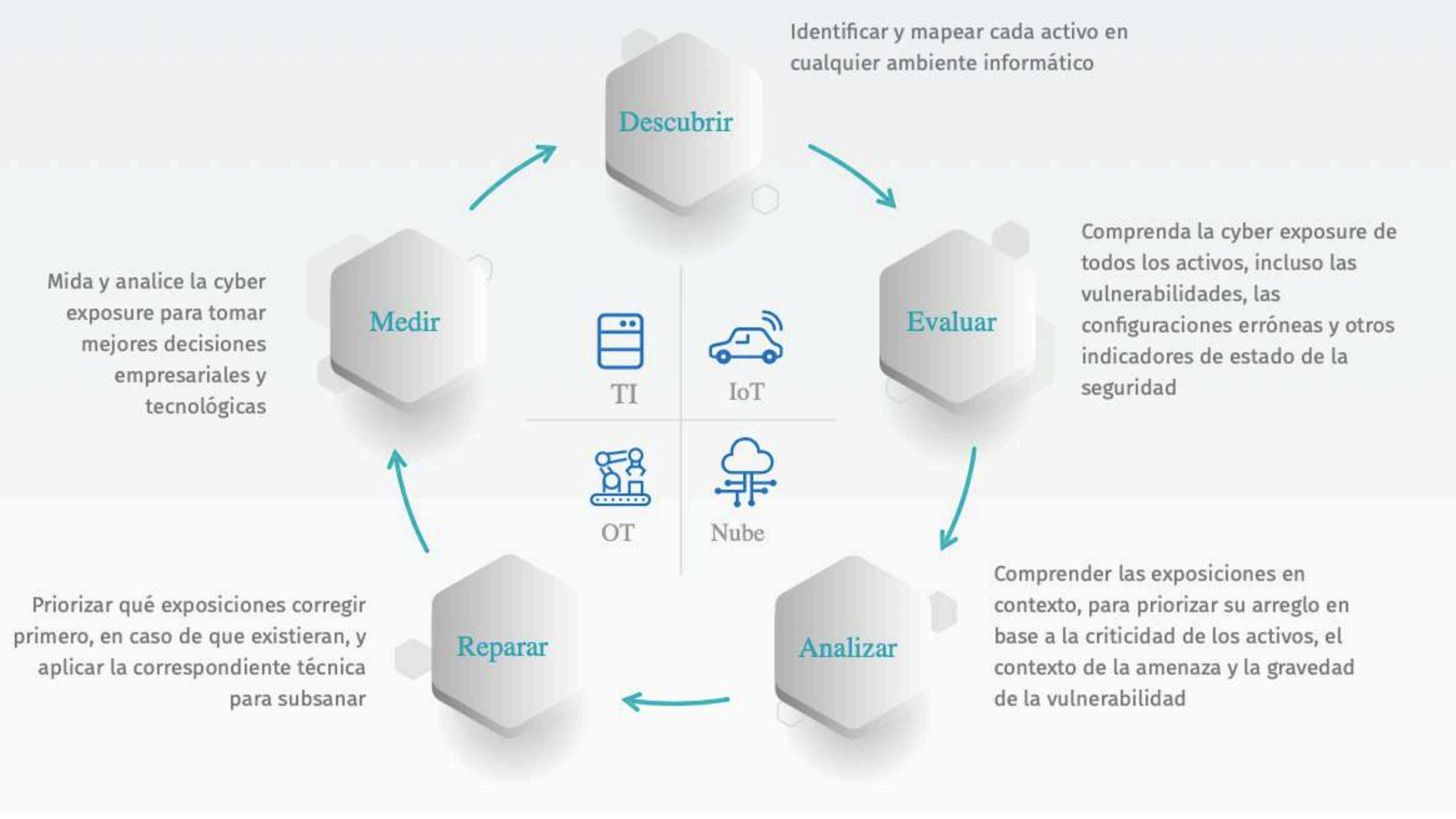
INSTRUMENTACIÓN
Es el nivel de proceso físico real que incluye los sensores y actuadores conectados directamente al proceso y al equipo de proceso.

IT

OT


Auditorías evolutivas de seguridad

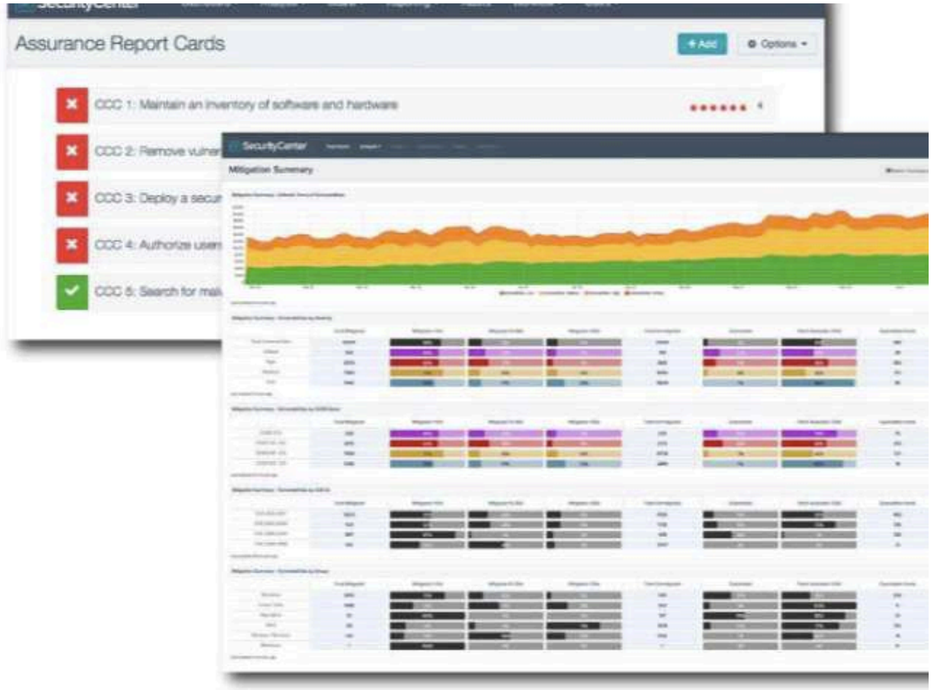

Internet de las cosas
Sistema de control industrial
IoT empresarial
Nube
Infraestructura de la nube
Aplicación web
Contenedor
Dispositivos móviles
Computadoras portátiles y de escritorio
TI
Servidor
Infraestructura de la red


Descubrir
Identificar y mapear cada activo en cualquier ambiente informático
Evaluar
Comprenda la cyber exposure de todos los activos, incluso las vulnerabilidades, las configuraciones erróneas y otros indicadores de estado de la seguridad
Analizar
Comprender las exposiciones en contexto, para priorizar su arreglo en base a la criticidad de los activos, el contexto de la amenaza y la gravedad de la vulnerabilidad
Reparar
Priorizar qué exposiciones corregir primero, en caso de que existieran, y aplicar la correspondiente técnica para subsanar
Medir
Mida y analice la cyber exposure para tomar mejores decisiones empresariales y tecnológicas
TI
IoT
OT
Nube

tenable.sc™

Identifique, investigue y priorice vulnerabilidades de forma precisa.

Capacidades	
Gestión de vulnerabilidades centralizada con múltiples escáneres	☑
Clasificación dinámica de activos (servidor de correo, servidor web, etc.)	☑
Auditoría de configuración basada en políticas	☑
Detección de malware con inteligencia de amenazas integrada	☑
Paneles/informes predefinidos con alimentación automática de Tenable	☑
Respuesta ante incidentes con alertas, notificaciones y tickets configurables	☑
Assurance Report Cards (ARC)	☑



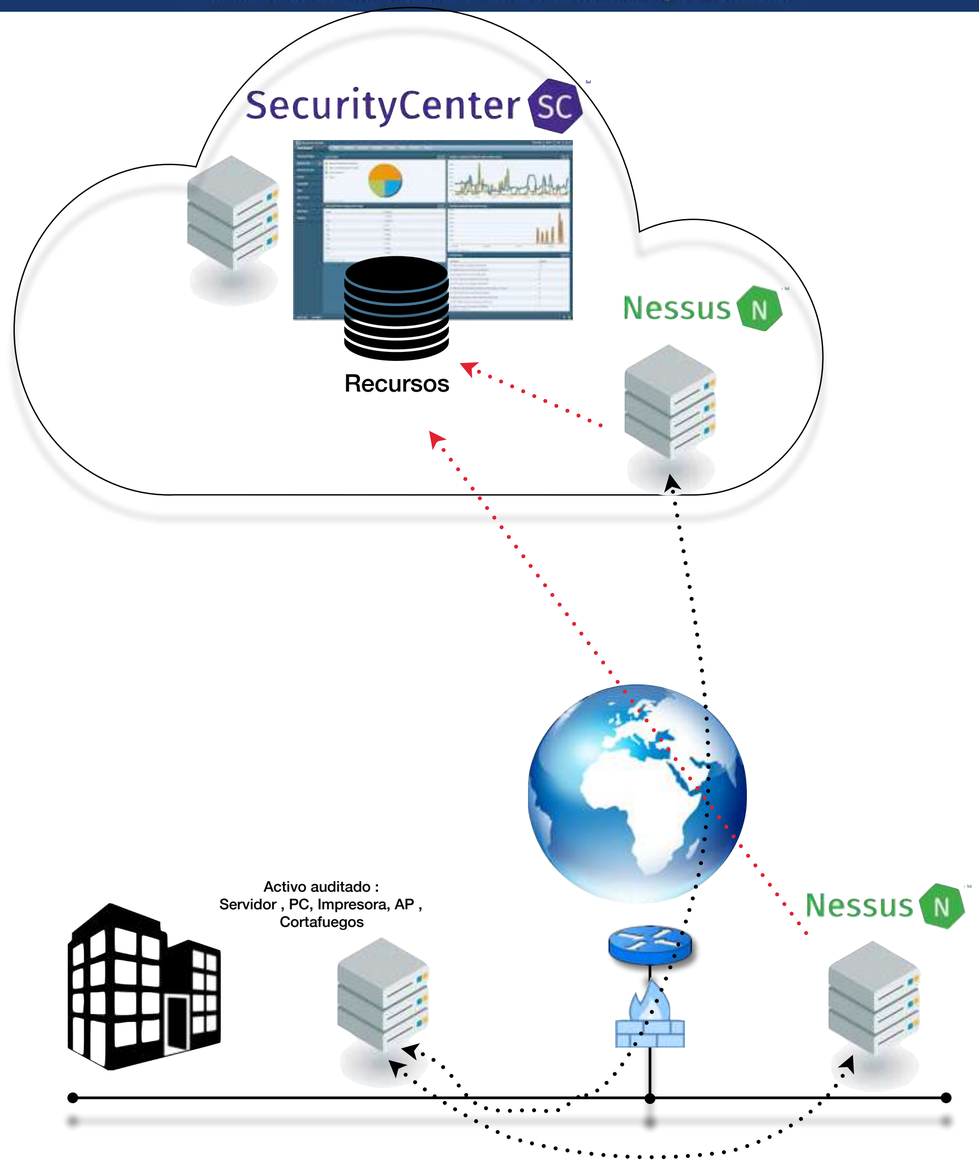
Tenable.sc proporciona análisis de vulnerabilidades, tendenci informes y flujos de trabajo altamente personalizables para adaptarse a las necesidades de su programa de seguridad

tenable

sarenet

tenable.sc™

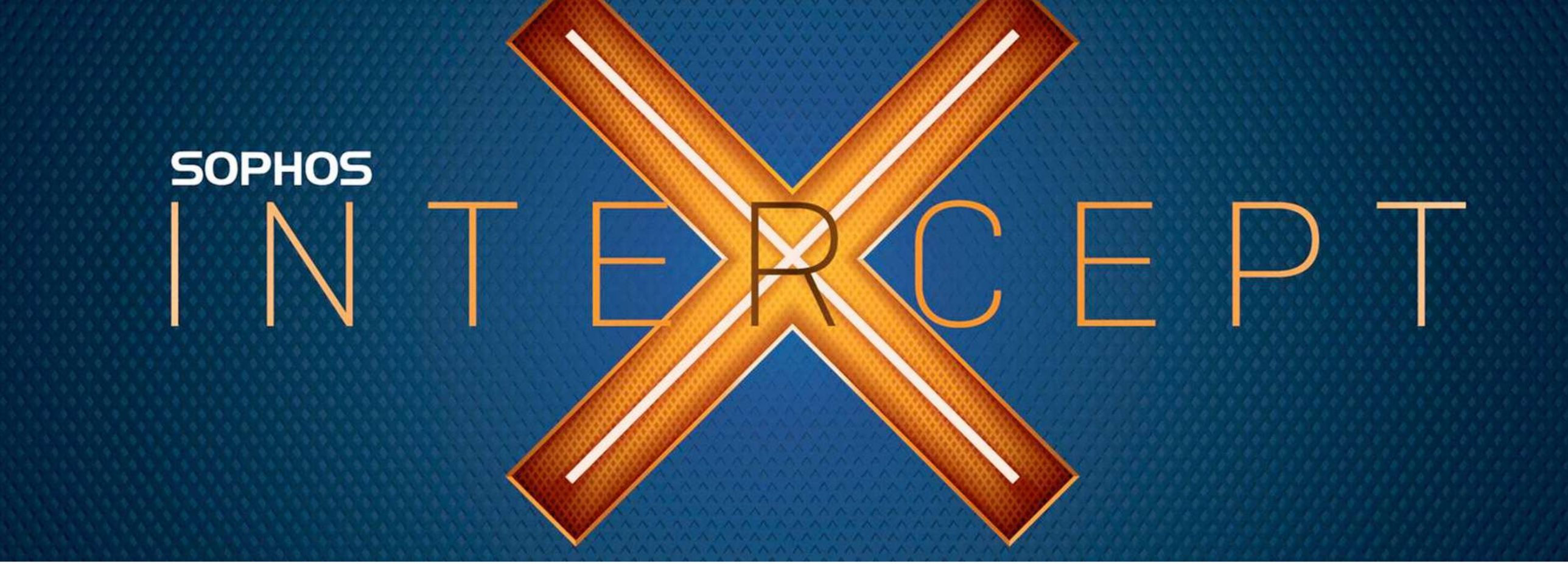
Identifique, investigue y priorice vulnerabilidades de forma precisa.



tenable

sarenet

End Point



Solución Endpoint

Ransomware - Wannacry (ficheros)

Petya - MBR (registro de arranque maestro)

Gartner®

“Leader”

2018 Endpoint Protection Platform Magic Quadrant

Leader in all ten reports since it was first published

One of only 3 leaders

Winner

Security Innovation of the Year

FORRESTER®

“Leader”

The Forrester Wave: Endpoint Security Suites

Off the charts strategy rating

Winner

Innovation Award

Endpoint Security

Gestion Centralizada

1

Control total

Aplique sus políticas de datos, dispositivo, aplicación y web con facilidad, gracias a la perfecta integración en el agente para estaciones y en la consola de administración.

- **Control web** Filtrado web basado en categorías aplicado dentro y fuera de la red corporativa
- **Control de la aplicación** Bloqueo de aplicaciones por categoría o por nombre con solo un clic
- **Control del dispositivo** Acceso controlado a medios extraíbles y dispositivos móviles
- **Control de datos** Prevención de pérdida de datos (DLP) que utiliza reglas preintegradas o personalizadas

Simplicidad sofisticada

Al igual que su aplicación favorita para web o teléfonos inteligentes, Sophos Endpoint Protection ofrece una funcionalidad sofisticada junto con una experiencia de usuario sencilla e intuitiva.

- Despliegue rápido y sencillo desde la nube o de forma local
- Políticas predeterminadas que se configuran para equilibrar la protección, usabilidad y rendimiento
- Eliminación automática de productos de seguridad para estaciones de terceros
- Configuración sencilla de funciones avanzadas tales como HIPS y control de dispositivo, gracias a los datos continuamente actualizados de SophosLabs

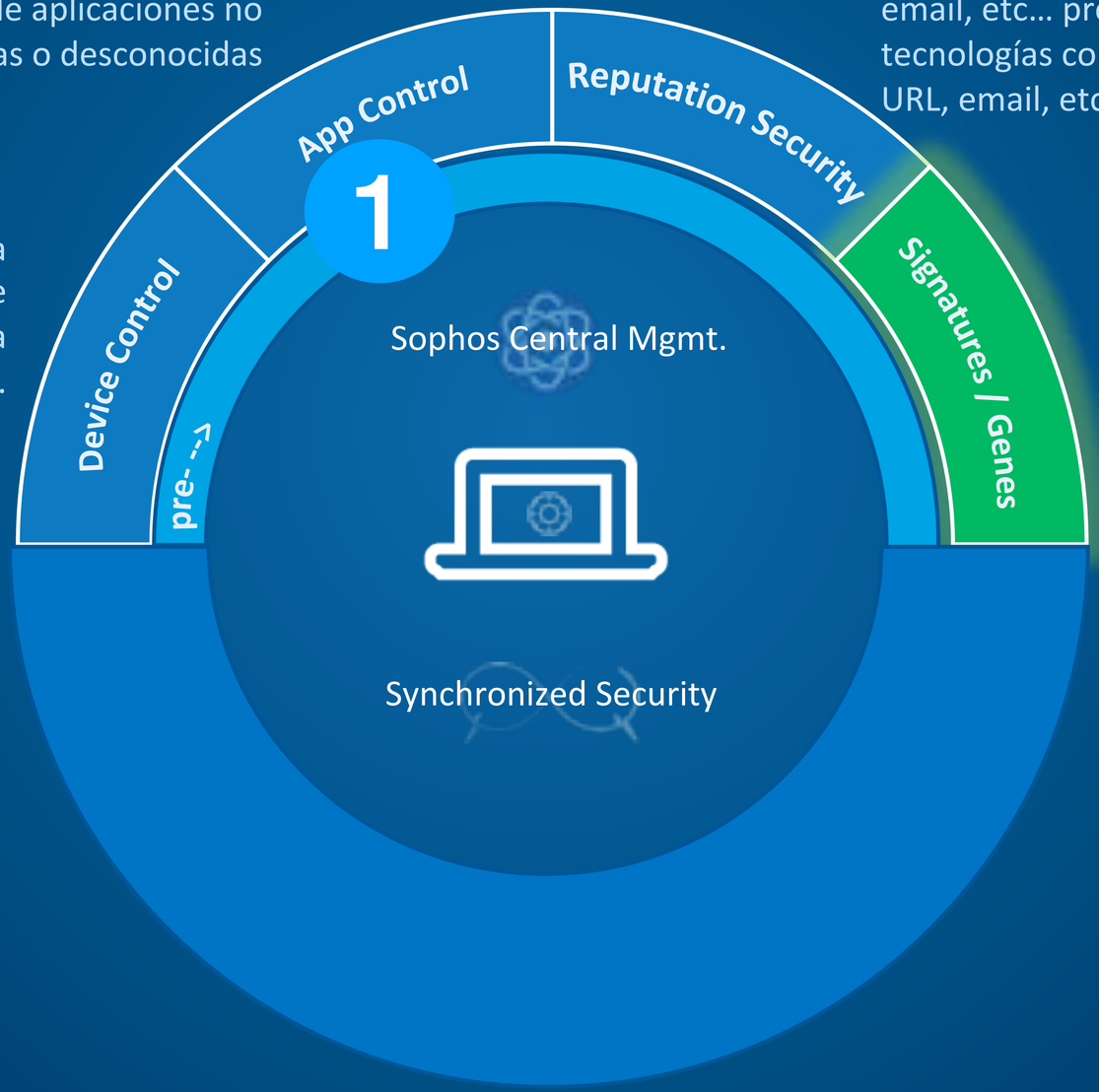
Protección Endpoint Tradicional

Para servidores o puestos, App Control previene de la ejecución de aplicaciones no deseadas o desconocidas

Conociendo el origen/reputación de un fichero, URL, email, etc… previene ataques antes que sucedan. Incluye tecnologías como MTD, reputación de descarga, filtrado URL, email, etc…

Control de políticas para dispositivos extraíbles para que éstos no pongan en riesgo la corporación.

Detección de scripts, macros, documentos y malware como primera línea eficiente de defensa contra variantes conocidas,



- .exe Malware
- Non-.exe Malware
- Script-based Malware
- Phishing Attacks

- Malicious URLs
- Removable Media
- Unauthorized Apps

SOPHOS

sarenet

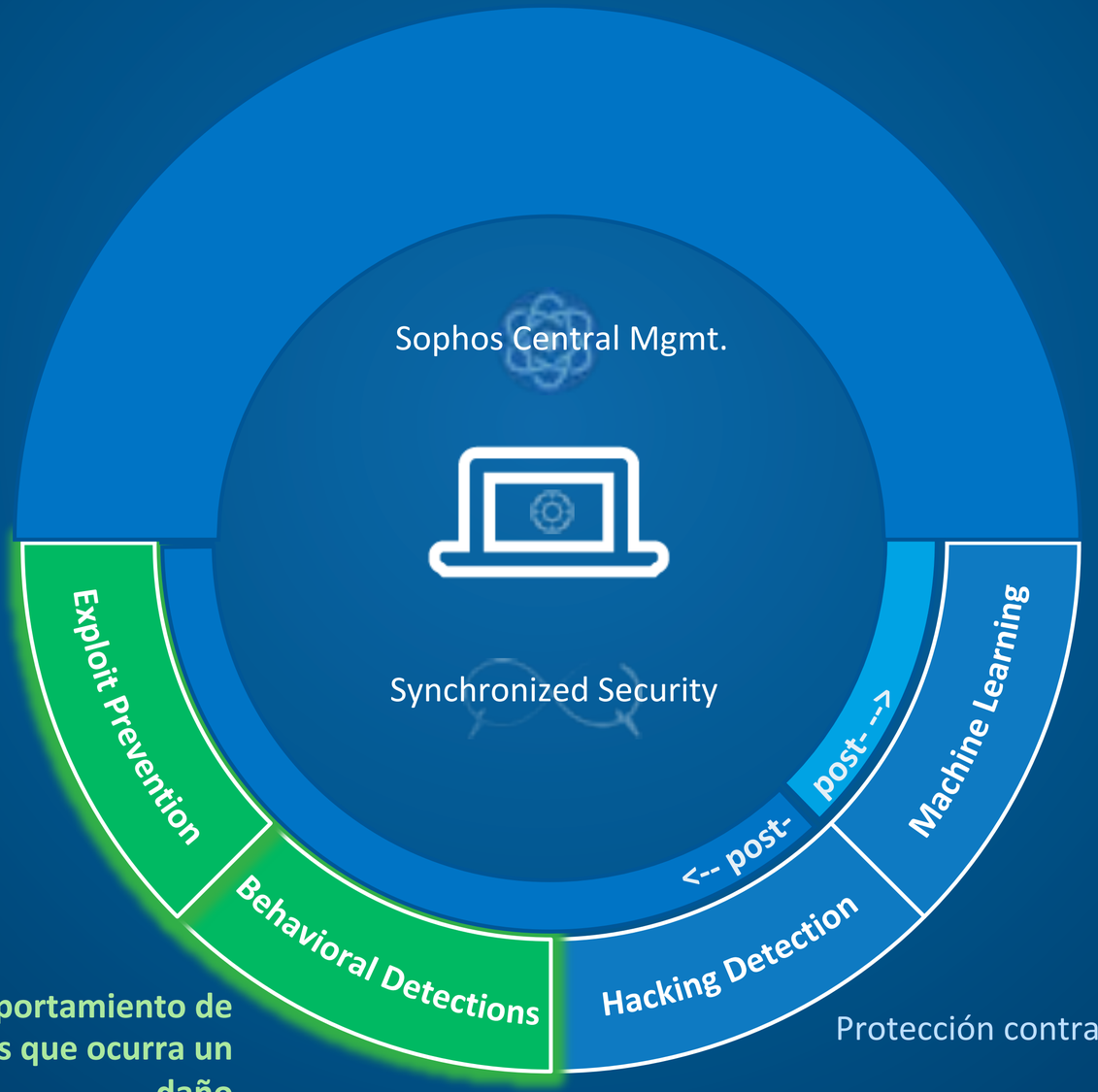
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

Protección contra técnicas post-explotación

SOPHOS

sarenet

Protección incluso cuando ya se ha vulnerado

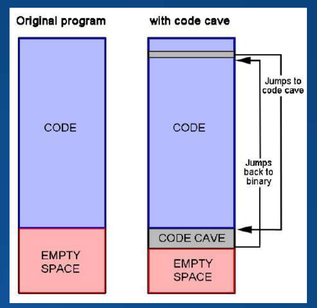
Credential Theft Protection

- Prevent dumping of credentials from memory
- Protect the credential database on Disk and Registry

Additional Registry Protections

- Sticky Key Mitigation
- Application Verifier Protection (Double Agent)

Active Adversary protections



- Code Cave prevention
- Malicious Process Migration
- Process privilege escalation
- APC Filter (prevent Atom Bombing exploit variants)
- Improved Application Lockdown
  - Powershell abuse from browsers
  - HTA apps

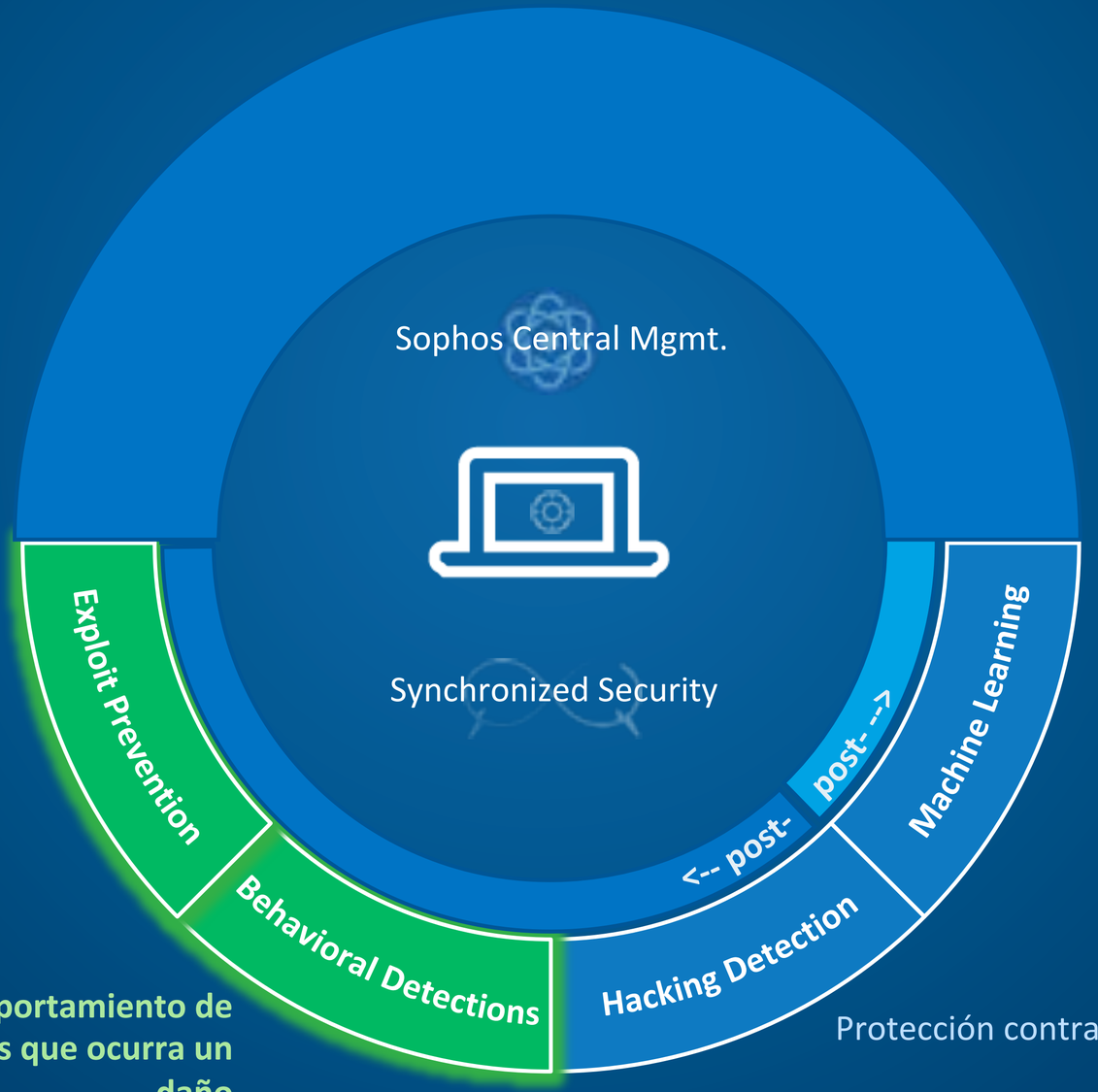
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

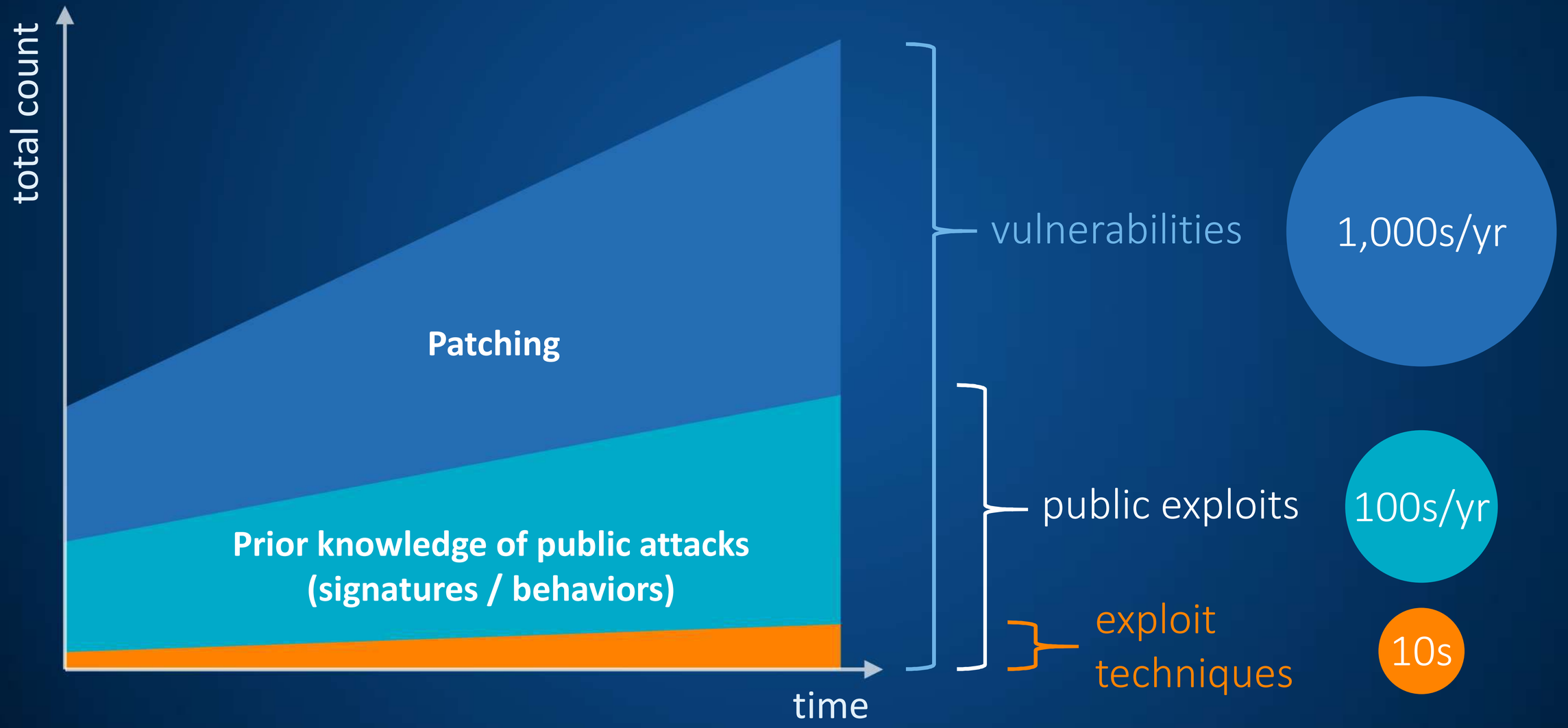
Protección contra técnicas post-explotación

SOPHOS

sarenet

Cómo podemos interceptar un Exploit

Vulnerabilities vs Exploits vs Exploit Techniques



Some of the Exploit and Active Adversary Techniques Stopped by Intercept X

Enforce data execution prevention	Mandatory address space layout randomization	Bottom-up ASLR	Null page deference	Heap spray allocation	Dynamic heap spray	Stack pivot and stack exec (memory protection)
Stack-based ROP (caller)	Structured exception handling overwrite (SEHOP)	Import address table faltering (IAF)	Load library	Reflective DLL injection	Malicious shellcode	VBScript god mode
WOW64	Syscall	Hollow process	DLL hijacking	Squiblydoo Applocker bypass	APC protection (Double Pulsar / Atom Bombing)	Process privilege escalation
	Credential theft protection	Code cave mitigation	MITB protection (Safe Browsing)	Malicious traffic detection	Meterpreter shell detection	

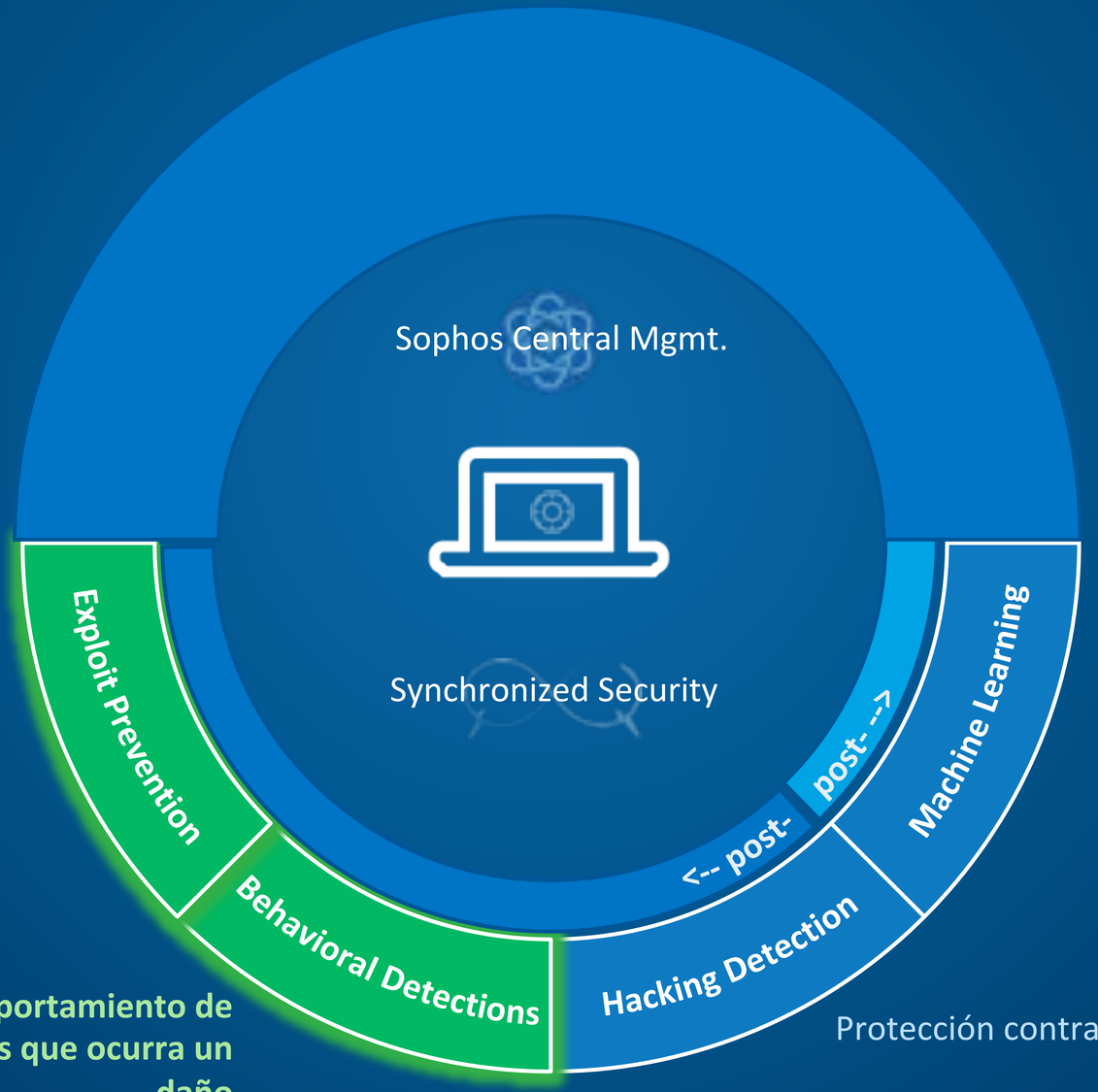
Protección EndPoint de Nueva Generación

Ramsomware

.doc
.xls
.pdf
CodeCaves

Hacking

Detección en tiempo de ejecución contra exploits y ransomware basándose en comportamiento. Proporciona características NextGen con capacidad de análisis forense de Causa Raíz (RCA).



Privilegios

Exploits

Credenciales

Tools

A través de Invincea, en pre-ejecución, detección de amenazas no conocidas gracias a su tecnología líder de ML con baja tasa de falso positivo, haciéndola única.

Detección heurística basada en el comportamiento de ejecución para eludir técnicas evasivas antes que ocurra un daño

Protección contra técnicas post-explotación

SOPHOS

sarenet

InterceptX vs Ransomware = CryptoGuard + WipeGuard

File Protection

Stops Techniques That Encrypt or Compress Files

Disk and Boot Record Protection

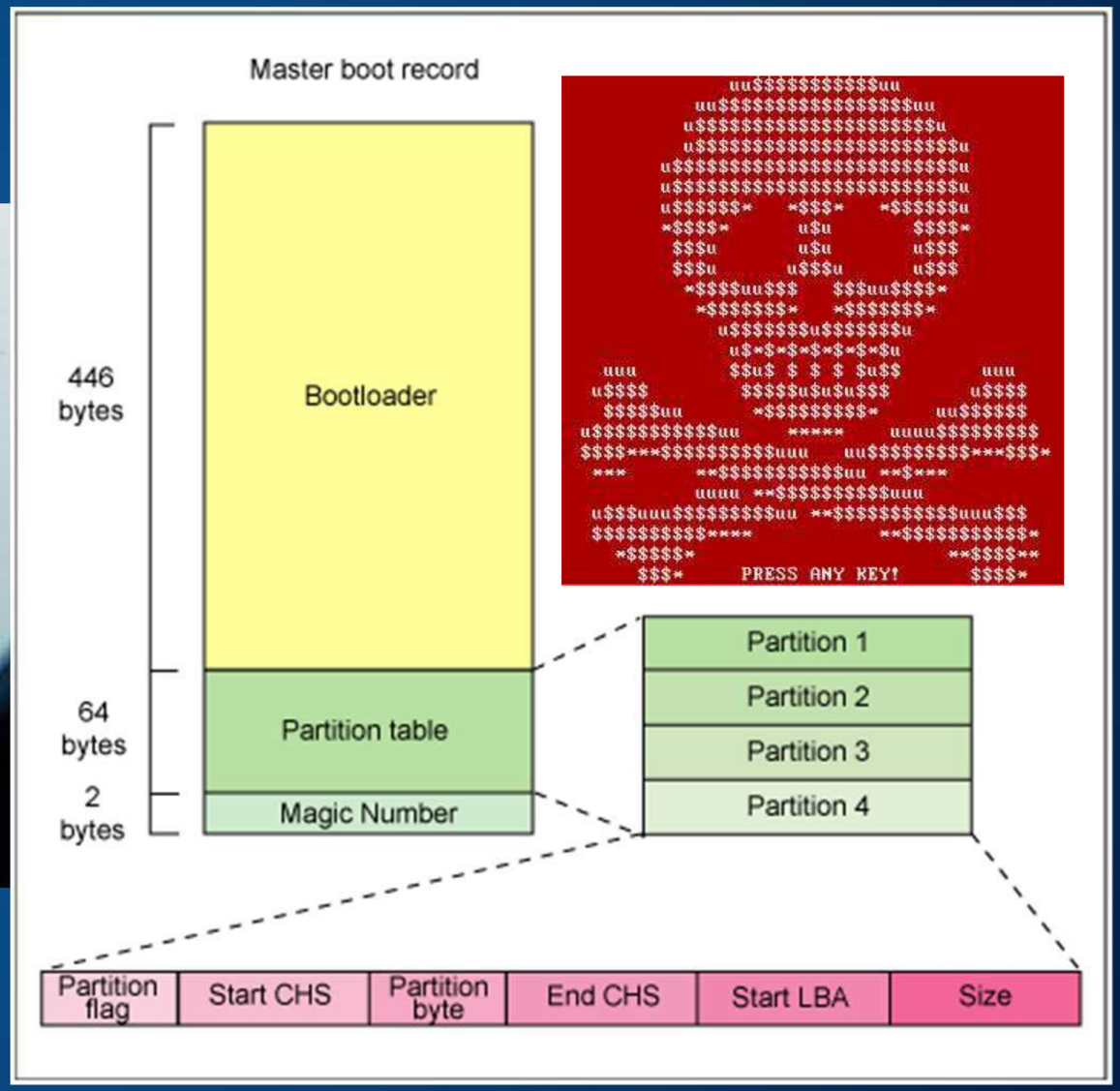
Stops Advanced Attacks that attempt to Lock a device pre-OS

Memory Protection

Stops Memory Exploits From Starting an Encryption Process

CryptoGuard – Interceptando Ransomware

WipeGuard: Modificación MBR



PROTECCIÓN AVANZADA CON APRENDIZAJE MEDIANTE DEEP LEARNING DE TÉCNICAS Y COMPORTAMIENTOS DE ATAQUE				PROTECCIÓN TRADICIONAL CON FICHEROS POR FIRMAS
	Sophos Intercept X Advanced with EDR	Sophos Intercept X Advanced	Sophos Intercept X	Sophos Endpoint Protection
Técnicas base	✔	✔		✔
Deep Learning	✔	✔	✔	
Antiexploits	✔	✔	✔	
Antiransomware de CryptoGuard	✔	✔	✔	
Detección y respuesta para endpoints (EDR)	✔			

SOPHOS

sarenet

RESUMEN DE LAS CARACTERÍSTICAS PRINCIPALES DE LOS ENDPOINT DE SOPHOS

- **Gestión centralizada** desde consola en la nube. 3 niveles de administración (Sarenet, Dpto. IT y usuario)
- Es un **cliente ligero** en cuanto a consumo local de recursos y sus actualizaciones no son de alto volumen
- Pago por uso en base a licencias. **Un usuario es una licencia**. Una licencia es válida para todos los PCS y portátiles del mismo usuario, no así con tablet y smartphone donde hay que ir a los productos de movilidad.
- Hay protecciones **servidor** y protecciones **puestos normales**
- Los procesos de **Deep Learning** se ejecutan en **local**, en el propio equipo, y no se requiere de Internet
- Es un tecnología **compatible con otros fabricantes AV**
- **Multiplataforma : Soporta Windows, Linux y MacOS**
    - Linux desktop consultar, hay muy poco
    - Linux Server soporta. En server se soporta CentOS, Oracle, Suse, Ubuntu
    - Puestos de trabajo Windows a partir de Windows 7
    - Servidores Windows a partir de Windows 8 R2

SOPHOS

sarenet


Usuario

Overview / Phish Threat Dashboard / Campaigns / Aitor

SARENET S.A.U. · Superadministrador del partner

Get Started — Choose Attack — Choose Training — Customize — Enroll Users — Review & Schedule

Choose Training

isk to your organization.

Parque Tecnológico

[IMPORTANTE] Se busca propietario de vehículo

Para: Aitor Jerez,

Responder a: Parque Tecnológico

ATENCIÓN:

Se ha producido un pequeño accidente en el aparcamiento junto a nuestro edificio. Estamos intentando localizar al propietario del vehículo que se ha visto afectado.

Un empleado ha hecho una foto del coche que he adjuntado a este correo electrónico. Si el coche es tuyo, comunícanoslo de inmediato.

PTZ Admon.
Administradores del edificio

DCO100003.jpg.docx

Descripción general de los ataques de phishing — 6 Min

Choose this training

Información personal identificable — 10 Min

Choose this training

Archivos adjuntos de Office — 10 Min

Choose this training

Archivos adjuntos en PDF — 4 Min

Choose this training

Archivos adjuntos zip — 10 Min

Choose this training

Plan de Contingencia

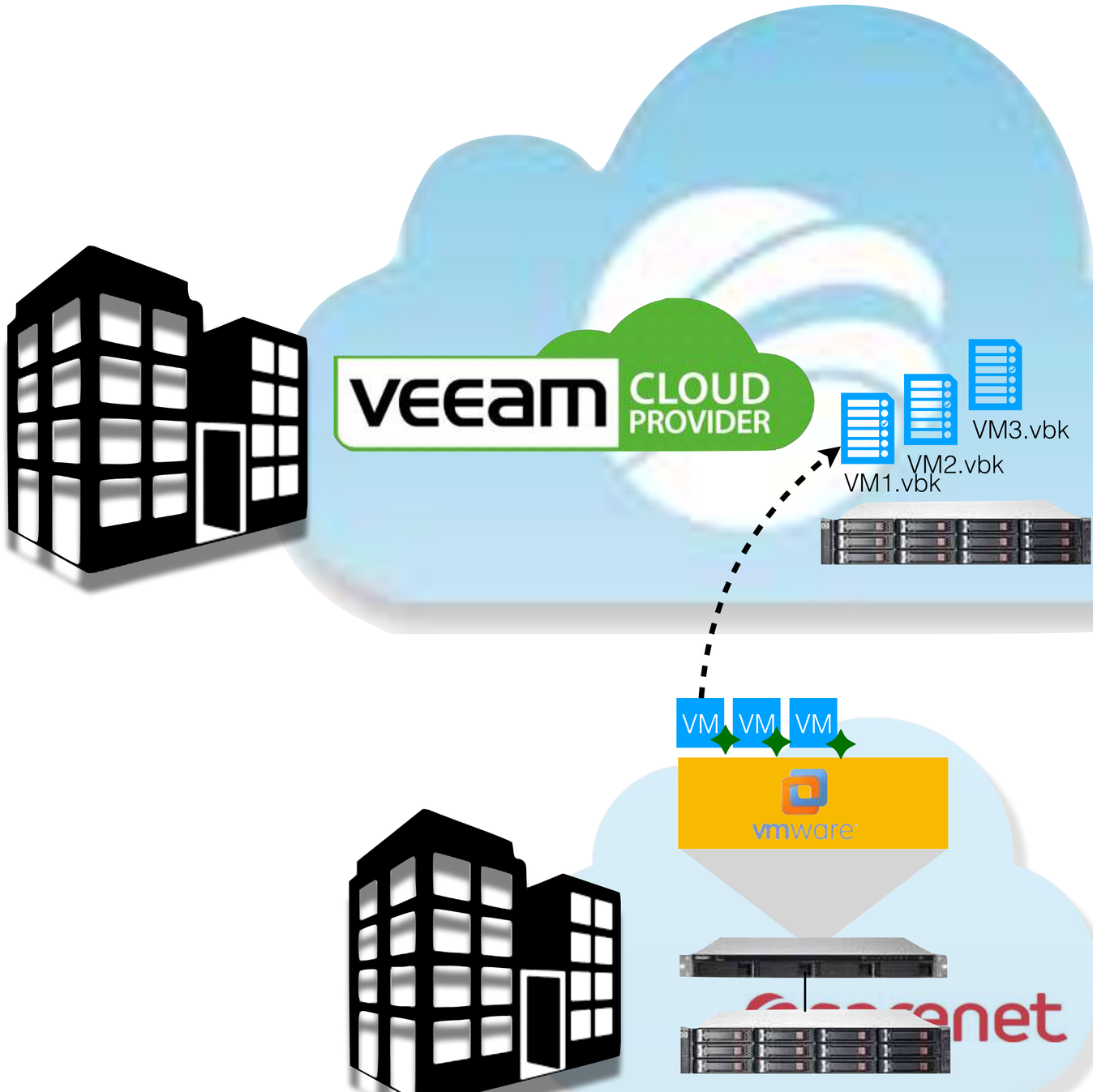
Plan de Contingencia

Veeam Cloud Connect

Veeam Cloud Connect **Backup**

Ahora, además de tener las copias generadas con Veeam en local , puedes almacenarlas fuera de tus instalaciones de forma totalmente segura

Gestiona tu conexión con este almacenamiento desde el propio Veeam y accede a tus copias y restáuralas en local cuando quieras



Plan de Contingencia

Veeam Cloud Connect

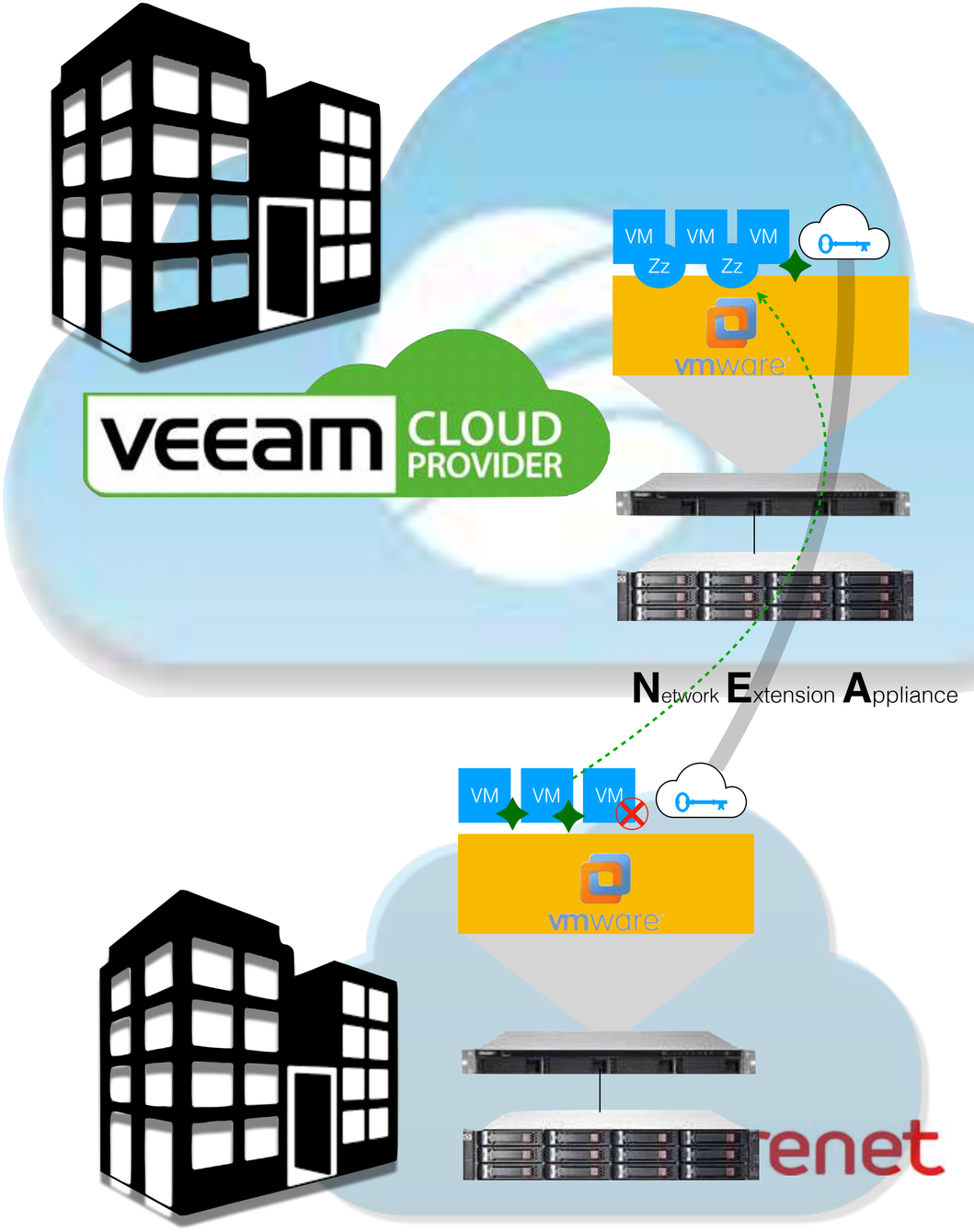
Veeam Cloud Connect **Replication**

Replica tus máquinas virtuales en un entorno externo de forma segura.

Actívalas siempre que lo necesites de forma transparente como si estuvieran en tus instalaciones con el mismo direccionamiento gracias al la tecnología NEA

Gestiona todo este proceso desde el propio Veeam

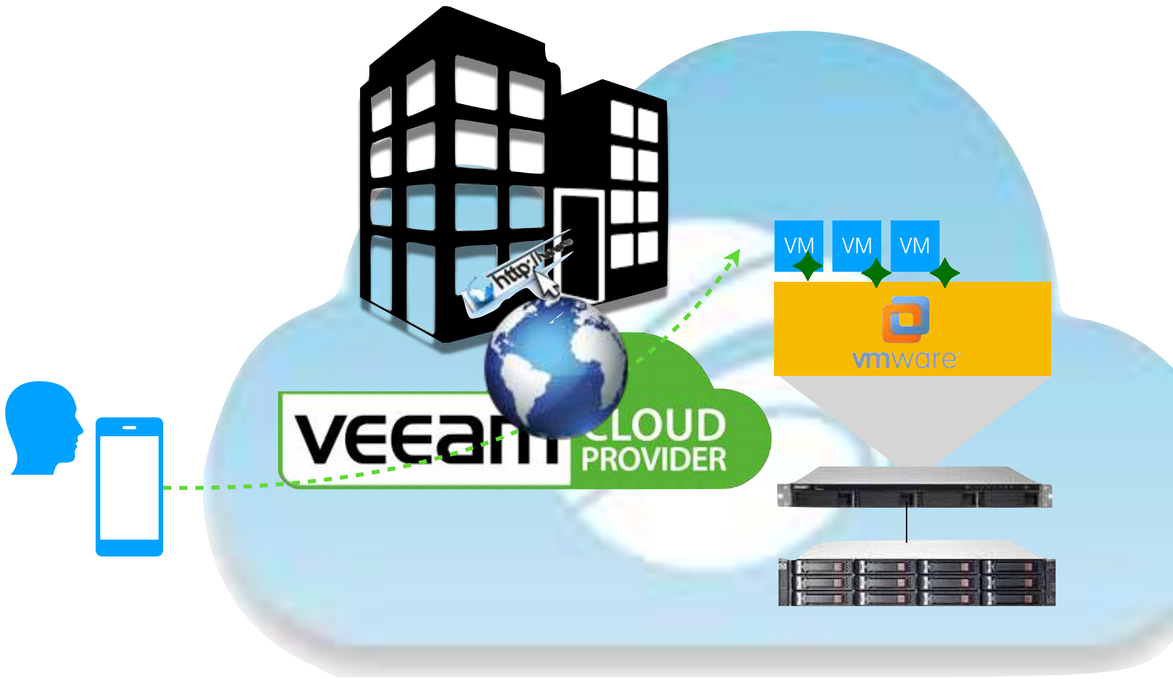
Nota: Versión vmware 5.5 o sup. , Veeam 9 ó sup.



Plan de Contingencia

Veeam Cloud Connect

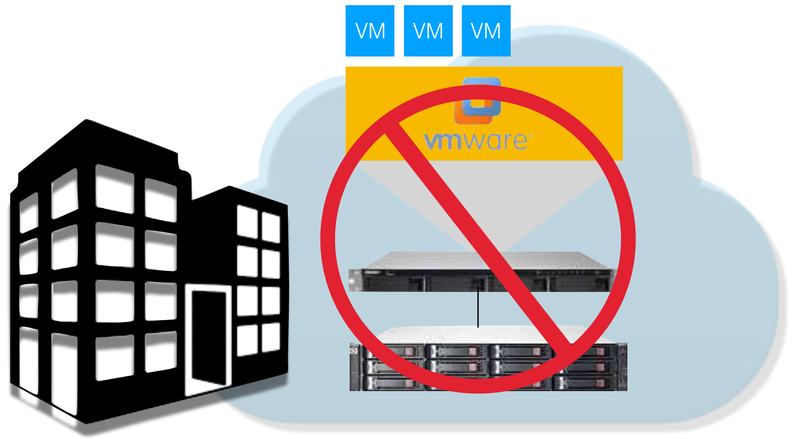
Veeam Cloud Connect Failover Plan



Replica tus máquinas virtuales en un entorno externo de forma segura.

Si tu entorno de virtualización te falla puedes tener un plan alternativo para acceder a tus máquinas por Internet

Gestiona todo este proceso desde un portal que puedes activar desde un smartphone en caso de emergencia



sarenet

Seguridad Gestionada

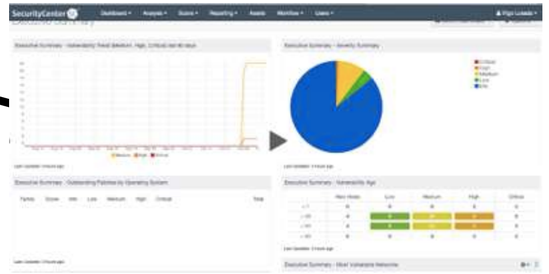
Vigilancia de alertas

Generación de informes

Monitorización de la MPLS

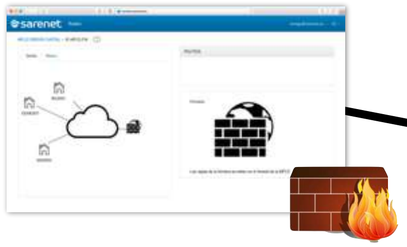
Cortafuegos

Sistema de análisis de vulnerabilidades Security Center



Frontera

Control de flujos

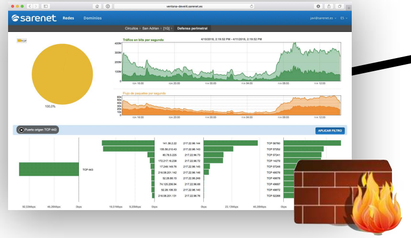


Gestión de redes Wifi

Actuaciones sobre activos

Segmentación y segregación de la red

Perimetral DDoS



Vulnerabilidades en servidores

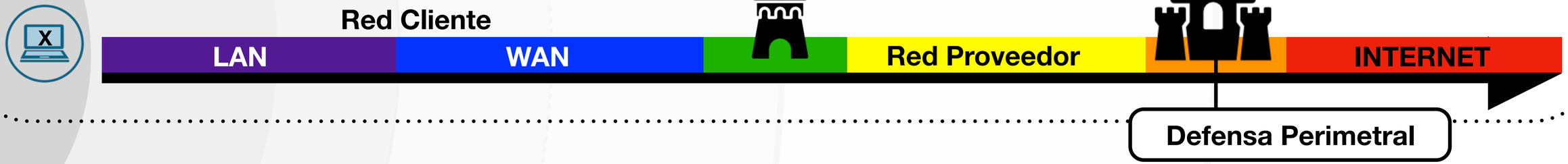
Aplicaciones

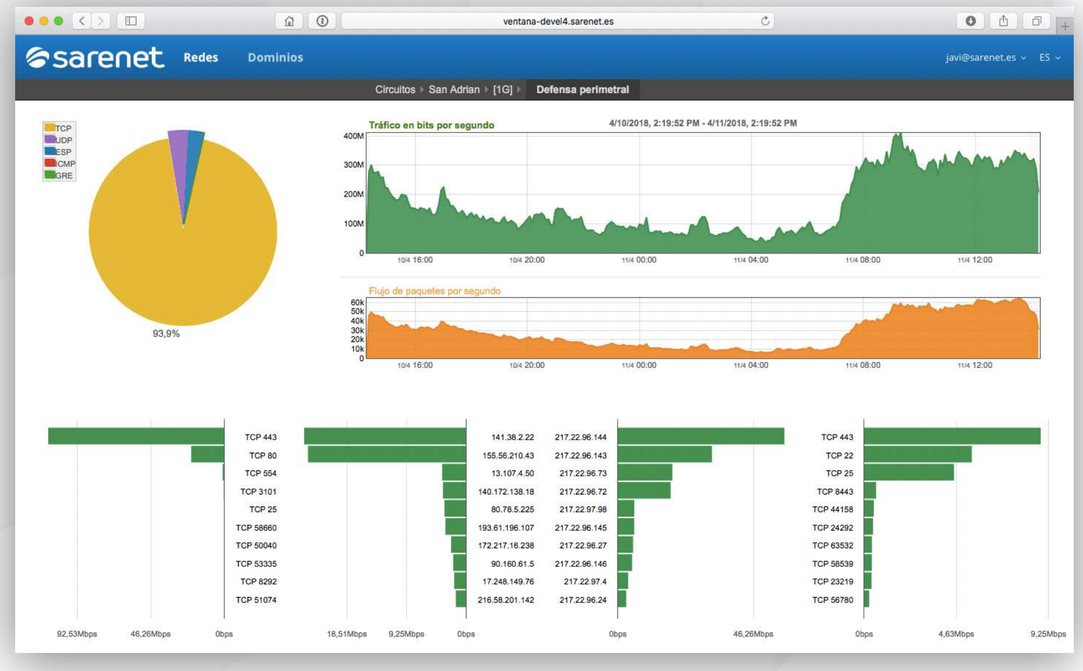
NAC Auth

SSL Portal

Gestión de los dispositivos NAC y control de accesos

Servicio de Seguridad Gestionada



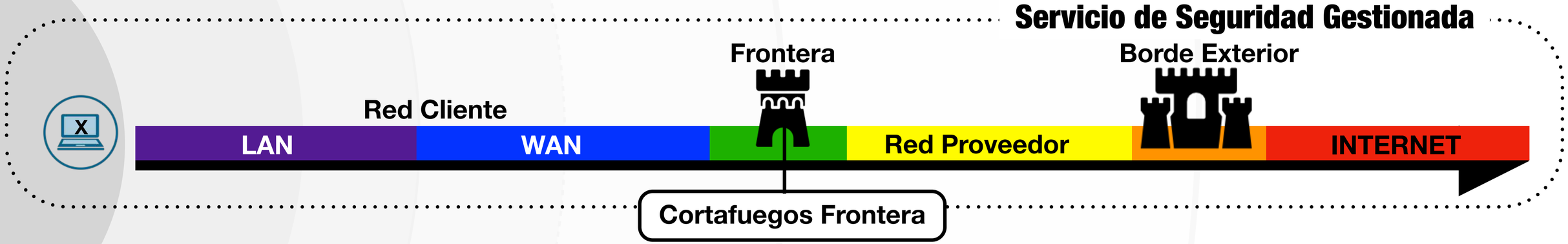


Aplicación Web

Gestión : cliente o Sarenet

Por IP o rango protegido

Desde **150 €/mes**



Alquiler y alojamiento de cortafuegos gestionado

Actualizaciones del Firmware

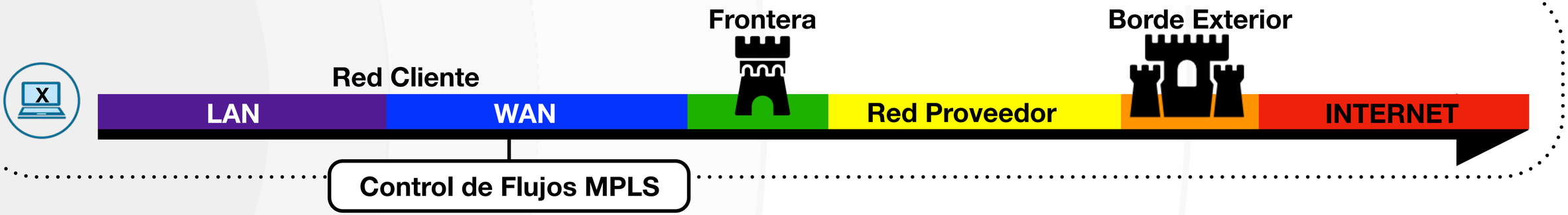
Creación de las políticas de seguridad

Gestión de accesos externos

Atención de las incidencias de seguridad : IPS/IDS, Botnets, virus

Gestión de sistemas de informes : fortianalyzer FAZ

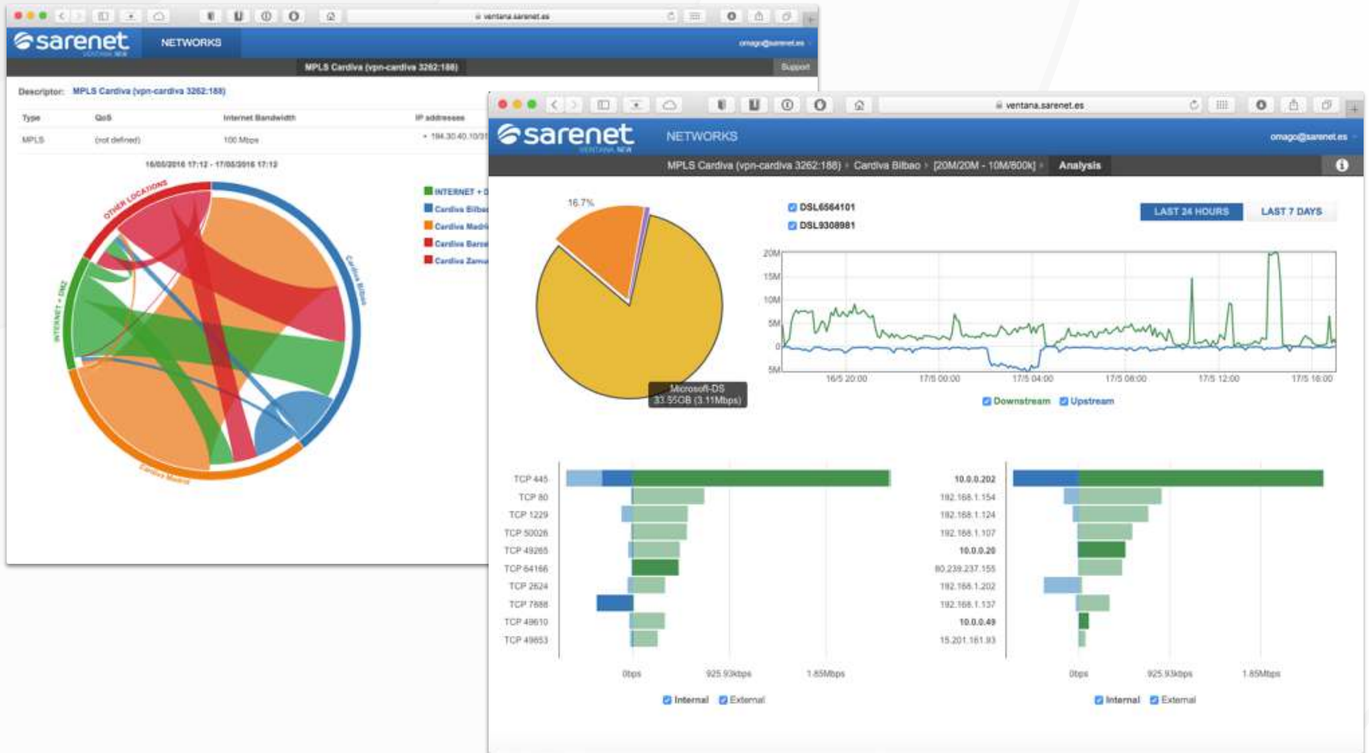
Servicio de Seguridad Gestionada

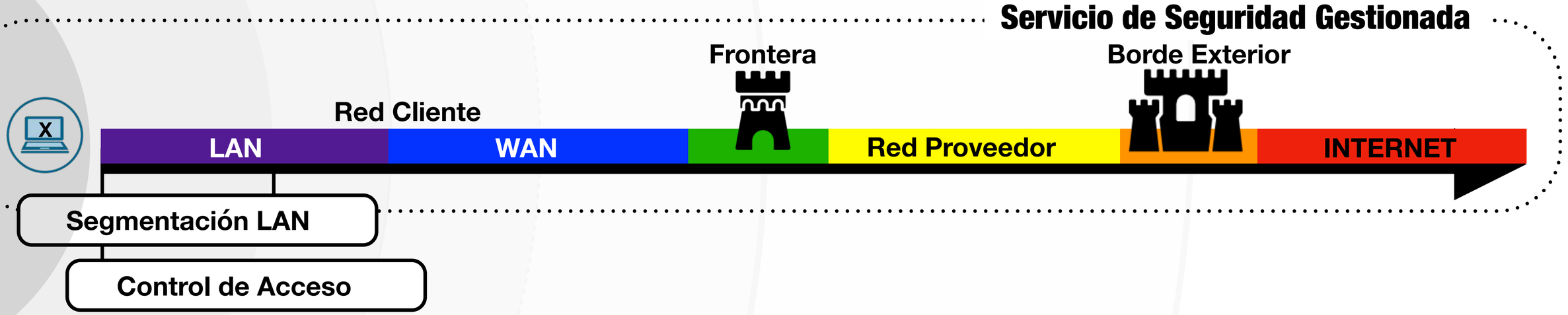


Segundo nivel : 5 €/mes por sede

Control de flujos internos : 10 €/mes por sede

Primer nivel incluido





Inventario inicial de dispositivos en la LAN de cliente

Análisis y diseño de las estrategias para segmentar y segregar las redes

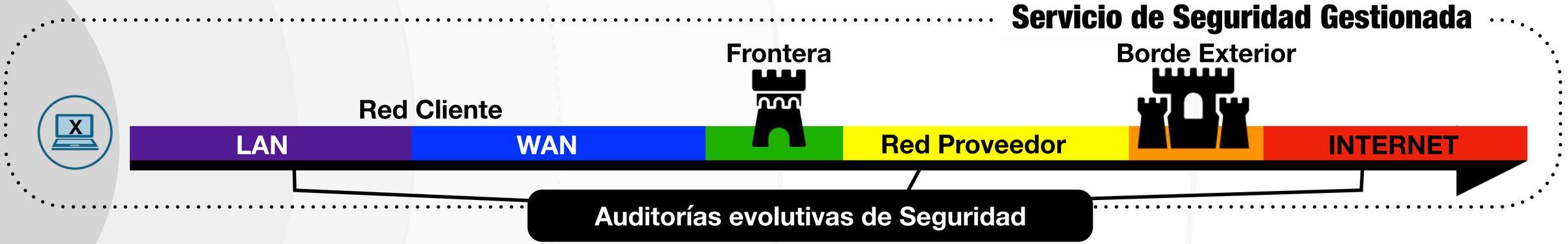
Suministro, instalación y configuración de switches y cortafuegos

Diseño de redes Wifi

Estudio e implementación de sistemas de control de acceso a la LAN

Soporte posterior de toda la implantación

Proyecto a medida con **bolsa de soporte** posterior



Contratación de la herramienta de auditoría evolutiva: 10 IPs, 500 €/año

Detección infraestructura crítica

Monitorización continua

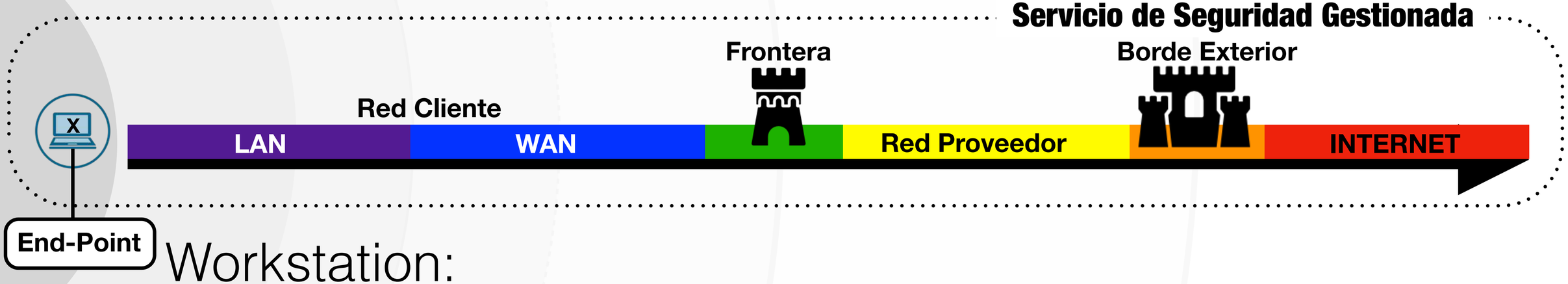
Soporte correctivo

- Alertas y vulnerabilidades

Soporte evolutivo

- Seguimiento continuo : reuniones periódicas y elaboración de informes con recomendaciones de acciones correctoras y de mejoras

Presupuestos a medida en base a fijo mensual : Desde 114 €/mes



Workstation:

Endpoint tradicional - 25 €/año
Intercept X - 35 €/año
Intercept X advanced con EDR - 70 €/año

Servers:

Central Server Protection - 59 €/año
Central Intercept X advanced - 120 €/año

Soporte en base a fijo mensual : Desde 57 €/mes

Plan de Contingencia

Sistemas Seguros de Almacenamiento **Veeam Cloud Connect**

Back-Up:

10€/mes por MV + espacio (ej.: 35€/mes -1TB)

Replication:

MV inactiva: 10€/mes + licencias de MS + almacenamiento

MV activa: 10€/mes + licencias de MS + almacenamiento + CPU + RAM

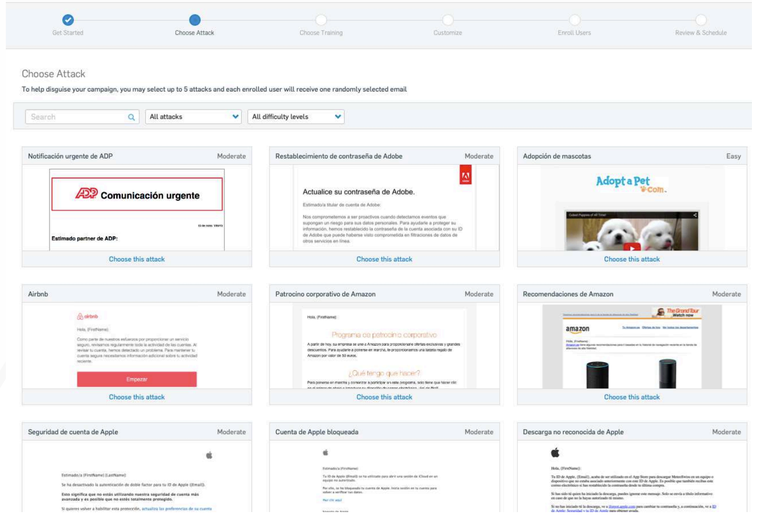
Failoverplan:

Estudio inicial + Costes de Replicación + IPs (10€/mes por IP)

Portal de concienciación: pishing

Alquiler de la herramienta : 100 usuarios, 19 €/año)
Soporte Sarenet : desde 57 €/mes

- Elaboración y análisis de campañas
- Reuniones de seguimiento e informes



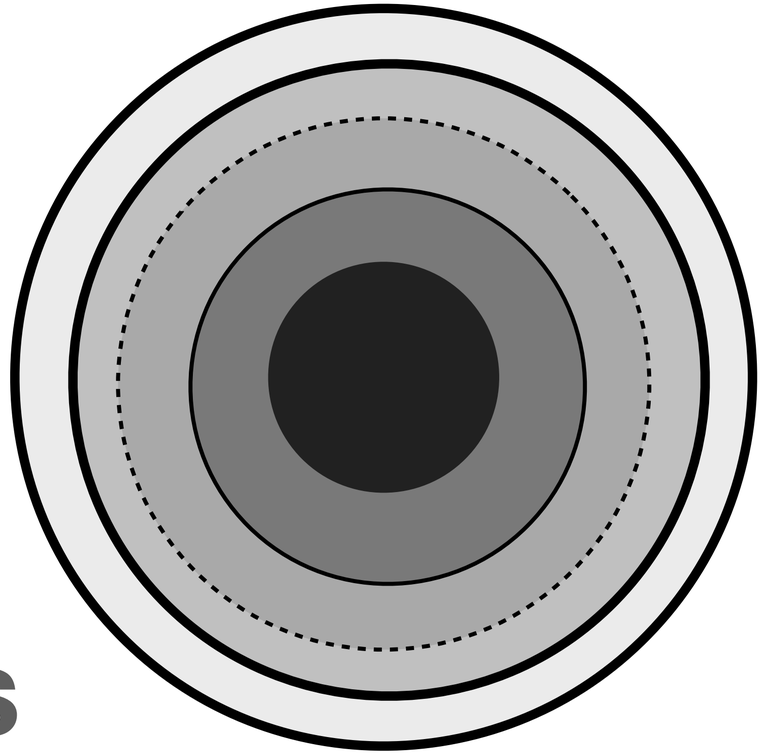
SOC gestionado 24x7

Security Center + SOC Sarenet

- Atención y comunicación de incidentes de seguridad.
- Administración de cambios en elementos de seguridad.
- Administración de respaldo de configuraciones
- Administratición y monitorización de eventos en cortafuegos y FAZ
- Monitorización de la red y de los equipos involucrados
- Monitorización de vulnerabilidades
- Hacking ético : test periódico de robustez de claves, simulación de ataques , etc..
- Generación mensual de informes ejecutivos
- SLA en base a tiempos de respuesta y calidad del soporte.

Seguridad Gestionada

Solución de seguridad integral
para nuestros clientes



Muchas gracias

sarenet