RedIRIS

Conectando las universidades y la I+D+i española desde 1988

www.rediris.es

SERVICIOS DE SISTEMAS Y SEGURIDAD

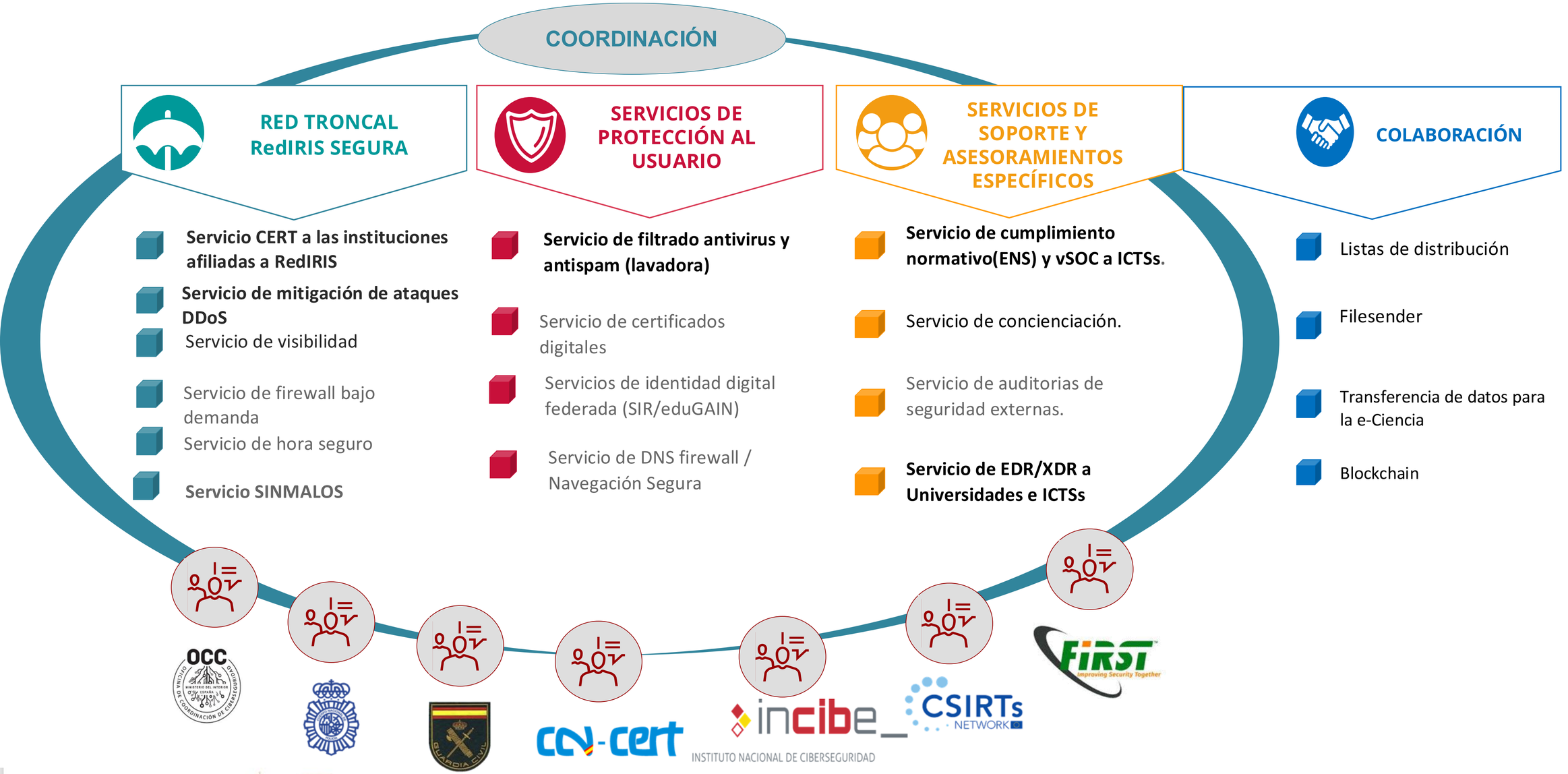
XXXIII Jornadas Técnicas de RedIRIS
Toledo, 20 de mayo de 2025

Equipo


SUBDIRECCIÓN DE SISTEMAS
Y SEGURIDAD
Antonio Fuentes
5
Francisco Monserrat
Enrique De Andrés
Jesús Sanz
Alberto Canales

ÍNDICE

Datos globales del servicio Lavadora



Servicio de Sistemas y Seguridad

RED TRONCAL RedIRIS SEGURA

- Servicio CERT a las instituciones afiliadas a RedIRIS – SOC.
- Servicio de mitigación de ataques DDoS.
- Servicio de visibilidad.
- Servicio de firewall bajo demanda.
- Servicio de sincronización horaria seguro.
- Servicio “Sin Malos”

SERVICIOS DE PROTECCIÓN AL USUARIO

- Servicio de filtrado antivirus y antispam (lavadora).
- Servicio de certificados digitales.
- Servicios de identidad digital federada (SIR/eduGAIN).
- Servicio de DNS firewall / Navegación Segura.

SERVICIOS DE SOPORTE Y ASESORAMIENTOS ESPECÍFICOS

- Servicio de cumplimiento normativo (ENS) y SOC a ICTSs.
- Servicio de concienciación de phishing.
- Servicio de EDR centralizado Universidades.

SERVICIOS TRANSVERSALES INTERNOS

- Sistemas internos de gestión de Seguridad
- Gestión de Infraestructuras y Plataformas horizontales de Sistemas
- Adecuación a la ISO27001/ENS

Adecuación a la ISO27001/ENS

Noviembre 2024. Certificación para el servicio de conectividad, Mitigación de Ataques de Denegación de Servicio (DDoS) y el servicio de identidad IdPnube.

Actualmente, el Servicio de Conectividad de RedIRIS se encuentra inmerso en la fase de auditoria del **Esquema Nacional de Seguridad (ENS).** Estimamos que, en un periodo máximo de un mes, contemos con dicha certificación.

De cara a 2025, se ampliará el alcance para añadir los servicios de Mitigación de Ataques de Denegación de Servicio (DDoS) y el servicio de identidad IdPnube

Gestión de Infraestructuras horizontales de Sistemas

SERVICIOS INTERNOS DE EXPLOTACIÓN DE SISTEMAS Y SEGURIDAD

ATENCIÓN A USUARIOS

- Gestión de identidad [1]
- Gestión del puesto de usuario

INFRAESTRUCTURA

- Almacenamiento
- Hosting [2,3]
- Housing [3]
- Gestión de infraestructura
- Backup
- Monitorización interna
- Balanceo de carga
- Bases de datos
- Red fuera de banda
- Virtualización
- Gestión CMDB [4]

SEGURIDAD

- Incidentes de seguridad
- Gestión de eventos y correlación
- Seguridad perimetral
- Monitorización de seguridad[7]
- Seguridad en el endpoint
- Gestión de acceso[8]
- Sistema de gestión de la seguridad de la información (ENS e ISO27K)

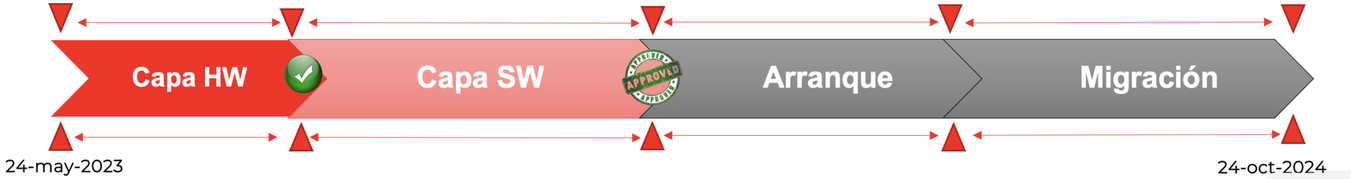
OTROS

- Gestión ITSM
- Gestión de directorio [5]
- Gestión de indicadores
- Correo electrónico y colaboración (buzones, listas, antispam, ...)

Apagón eléctrico

Todos los servicios de RedIRIS siguieron funcionando con normalidad

Primera Fase

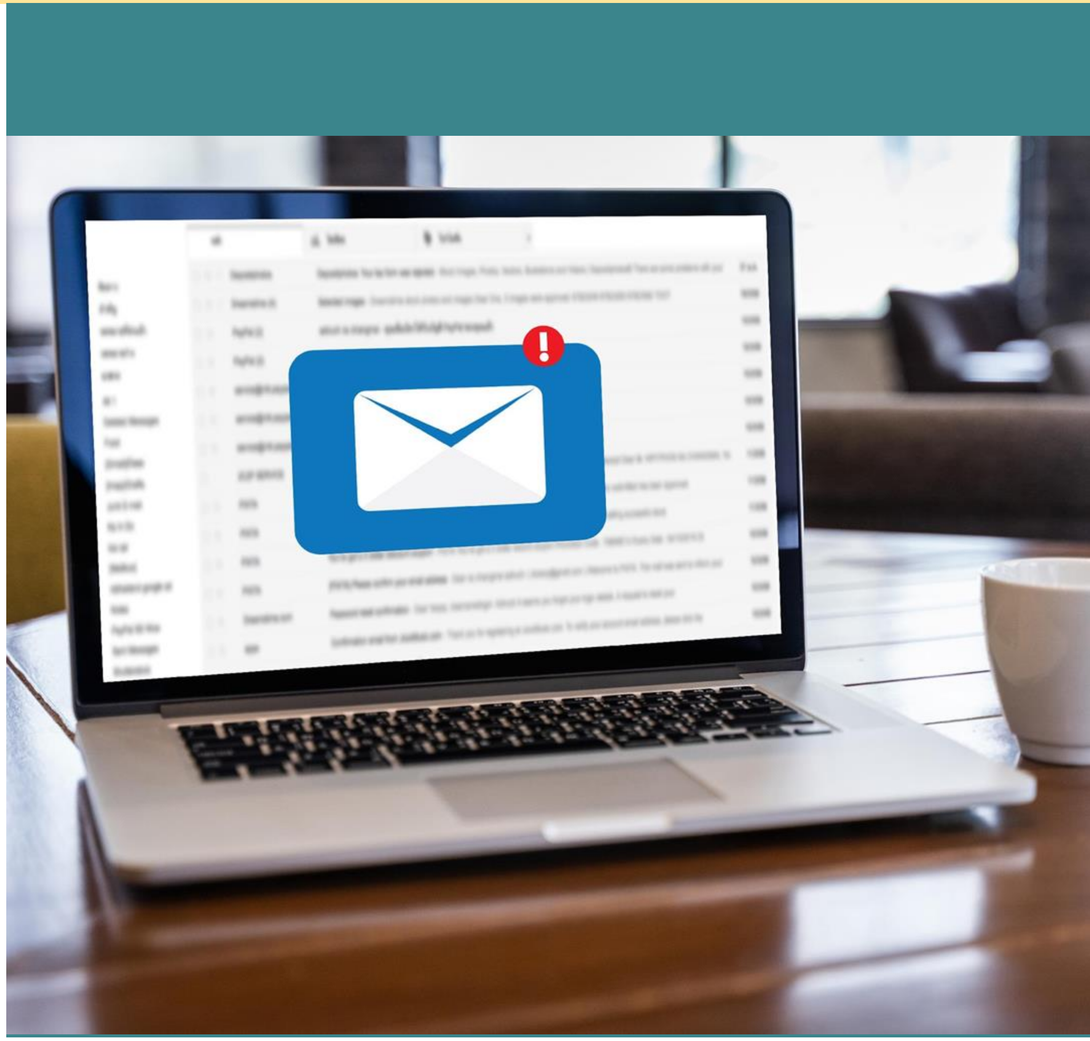


Captura

Servicio de filtrado antispam (Lavadora)

¿Qué ofrecemos?

RedIRIS ofrece a las instituciones afiliadas la posibilidad de pasar su **correo electrónico** por un **sistema de filtrado antispam y antivirus**, antes de entregárselo “limpio” a la institución (de ahí lo de “lavadora”).

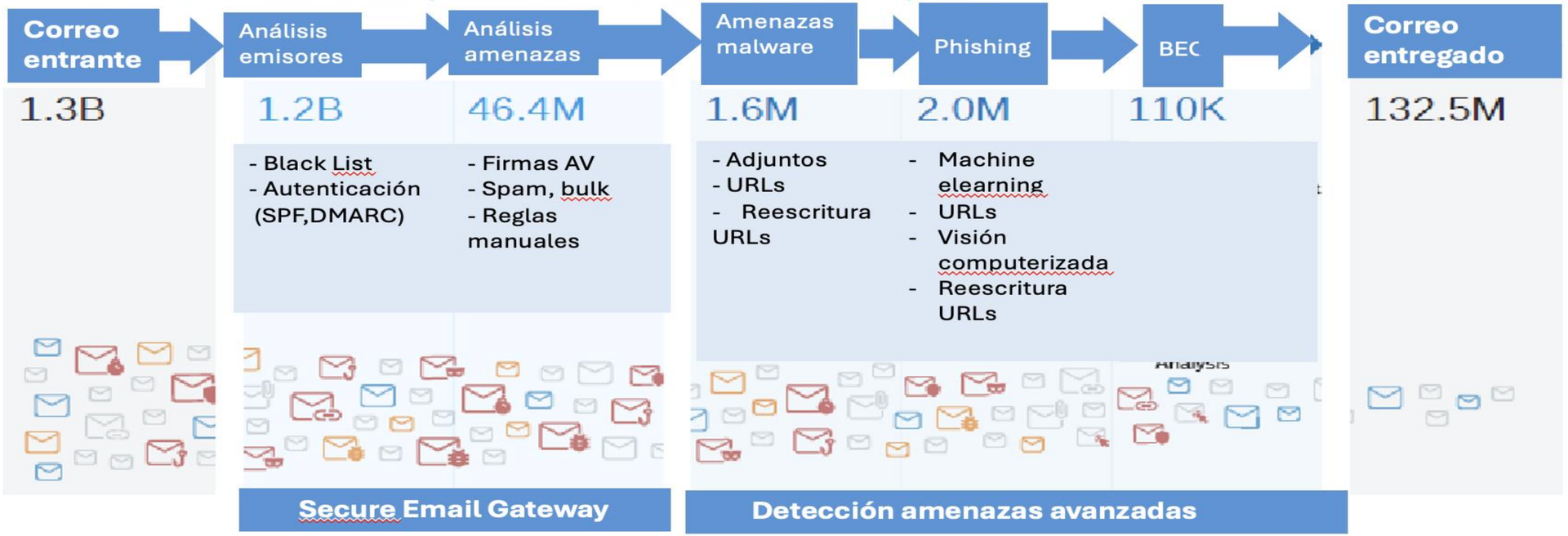


- Numero organizaciones: 100
- Numero dominios: 1000
- Numero de buzones protegidos: 2.200.000 usuarios (1.800.000 registrados)
- Numero de correos entrantes: 260 millones/mes
- Numero de correos clasificados peligrosos: 230 millones/mes (87%)
- Migración de organizaciones a DMARC reject: 6

Servicio de filtrado antispam (Lavadora)

Datos Globales del primer trimestre de 2025

- 1.3B de correos han entrado a la plataforma
- 132.5 M de correos han llegado hasta el usuario
- 1.246 B de correos han sido detectados y descartados por la plataforma (reputación y filtros tradicionales)
- 3.7 M de correos detectados por filtros avanzados de Proofpoint



90% de todos los correos electrónicos entrantes han sido clasificados como «no deseados», lo que significa que no son comunicaciones genuinas deseadas por el destinatario

Servicio de filtrado antispam (Lavadora)

Resumen de Correo Entrante

178.9* M de correos entrantes de usuarios externos a usuarios y dominios internos

Total Inbound	Total Blocked	Total Delivered
178,915,258	46,433,261 26.0%	132,481,997 74.0%
↑ 22.9% vs Previous Quarter	↑ 92.8% vs Previous Quarter	↑ 9.1% vs Previous Quarter

Bulk – son aquellos mensajes de correo que se envían a un gran número de destinatarios quienes activa o pasivamente han permitido recibir las comunicaciones de remitente o remitentes.

Others – otros clasificadores de Spam y reglas personalizadas.

Total Blocked by Category

Category	% of Total Inbound	Messages	vs Previous Quarter
Threats	2.4%	4,252,955	+ 40.8%
Spam	11.3%	20,207,871	+ 28.7%
Bulk	1.5%	2,703,223	+ 28.2%
Others	10.8%	19,269,212	+ 492.3%
Total Blocked	26.0%	46,433,261	+ 92.8%

***178.9 M** - la cifra consiste en descontar del total de correo entrante a la plataforma – **1.3B** - el total de correo descartado por el filtro de reputación – **1.2** (cálculo aproximado debido a las altas cifras)

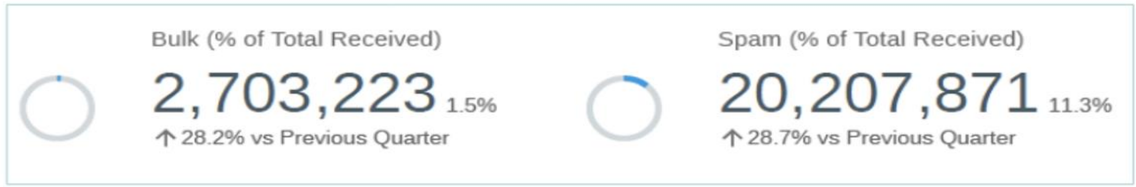
SPAM en los Dominios Principales

Estos son los Top 10 dominios receptores de correo (entre los top 50)

Envelope Receiving Domain	Messages(% of Total Inbound)	vs Previous Quarter
ugr.es	25,714,827 (14.4%)	+ 107.8%
educa.madrid.org	18,178,563 (10.2%)	+ 12.9%
uv.es	12,319,849 (6.9%)	+ 16.9%
unizar.es	9,797,670 (5.5%)	+ 12.7%
um.es	7,582,422 (4.2%)	+ 17.9%
uvigo.es	5,870,060 (3.3%)	+ 0.4%
upm.es	5,556,579 (3.1%)	+ 10.1%
uca.es	5,501,005 (3.1%)	+ 35.4%
uam.es	5,003,314 (2.8%)	+ 21.1%
uco.es	4,449,389 (2.5%)	+ 19.3%

Servicio de filtrado antispam (Lavadora)

SPAM en los dominios principales



Los principales dominios receptores de SPAM

Envelope Receiving Domain	Messages(% of Total Spam)	vs Previous Quarter
ugr.es	6,004,070 (29.8%)	+ 76.7%
uv.es	1,366,991 (6.8%)	+ 6.3%
unizar.es	1,235,966 (6.1%)	+ 21.7%
correo.ugr.es	917,146 (4.6%)	+ 115.5%
um.es	775,595 (3.9%)	+ 14.3%

Los principales dominios receptores de BULK

Envelope Receiving Domain	Messages(% of Total Bulk)	vs Previous Quarter
unizar.es	1,552,101 (58.0%)	+ 28.6%
santpau.cat	246,662 (9.2%)	+ 21.6%
ciemat.es	113,358 (4.2%)	+ 34.0%
uhu.es	103,695 (3.9%)	+ 29.1%
isciii.es	81,696 (3.1%)	+ 25.1%

Simulación de phishing (SIMULPHISHING)

¿Qué ofrecemos?

El objetivo de este servicio, además de concienciar a los usuarios que participan, es **concienciar a las organizaciones** para que dispongan de un servicio permanente de concienciación y formación en ciberseguridad

- Prepara 2021 se contrató un servicio de concienciación (simulphishing) para realizar durante 3 campañas anuales a diferentes organizaciones con un total de 12000 usuarios
- Las instituciones reciben sus correspondientes informes mensuales, trimestrales y anual de la evolución de concienciación de los usuarios
- Instituciones que ha usado el servicio durante estos 3 años: 30 instituciones
  ción de campañas de phishing personalizadas

EGIDA. Mitigación de ataques de DDoS

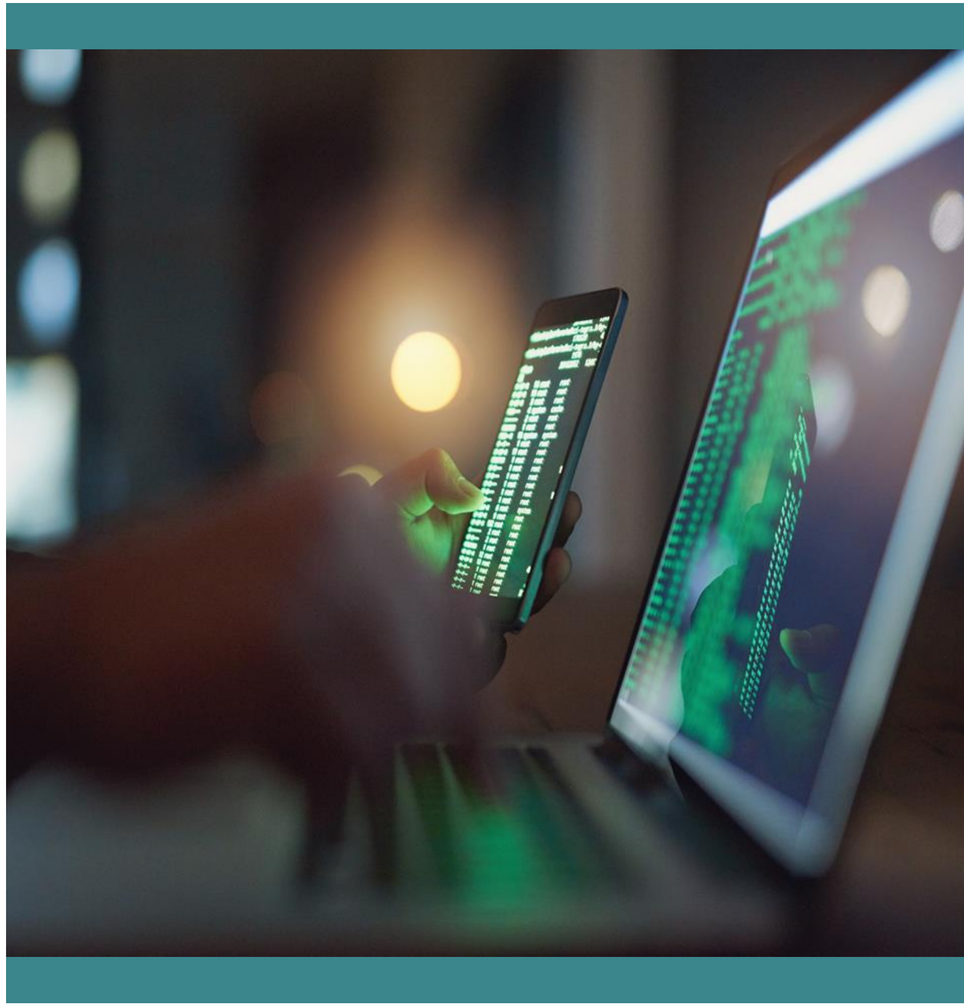
¿Qué ofrecemos?

RedIRIS proporciona **servicios** para ayudar a las instituciones afiliadas a **identificar** y **mitigar** los **ataques de denegación de servicio** o **saturación**, conocidos coloquialmente como ataques **"DDoS"** (*Distributed Denial of Service attacks*)

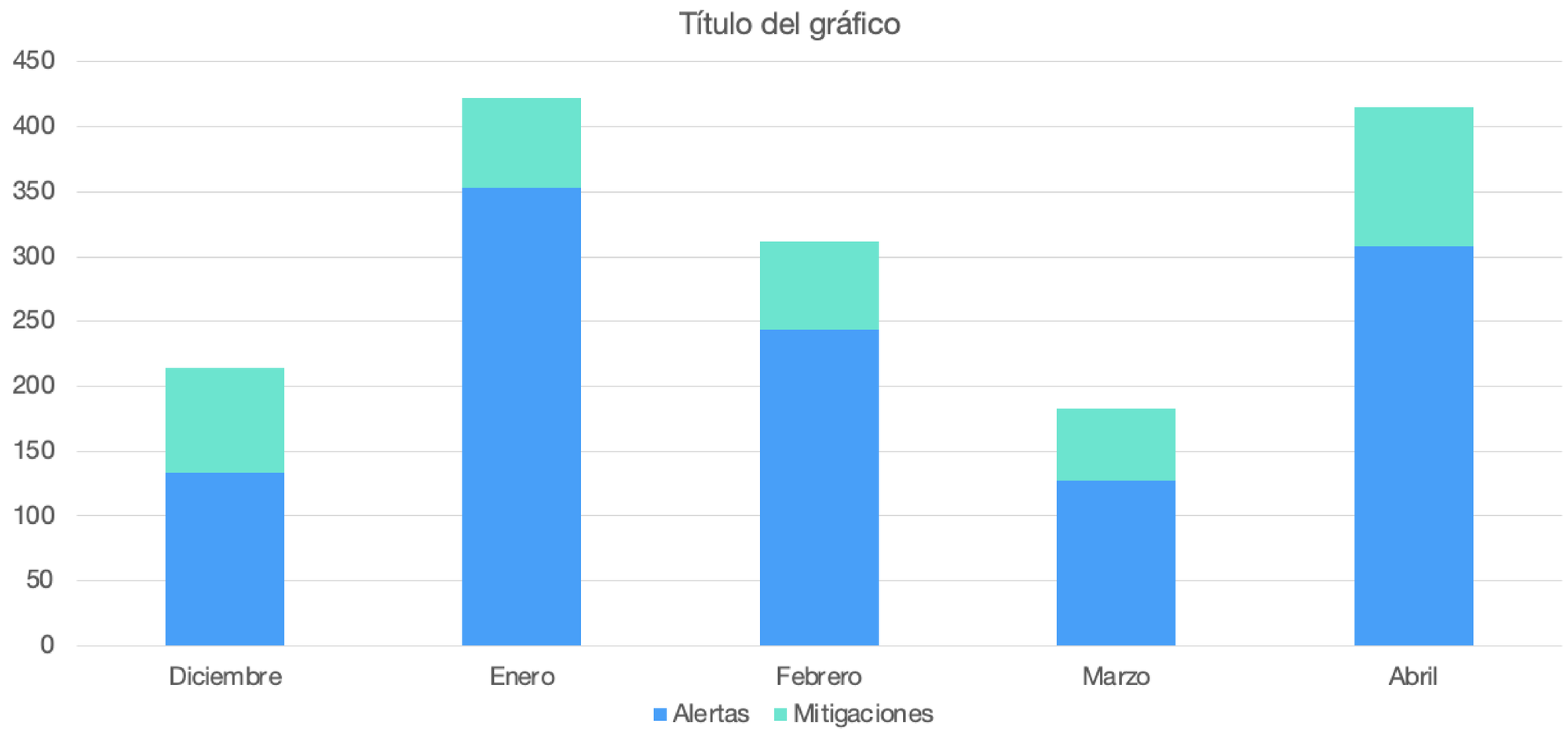
Ventajas de nuestro servicio

- **Protección básica**
  - Todas las instituciones conectadas están monitorizadas y protegidas 24x7
  - Rangos IP que se protegen son los oficiales que están encaminados el troncal de RedIRIS por el NOC
  - Revisión de alarmas por el SOC de mitigación en modo 24x7 y mitigación básica.
  - Notificación en jornada laboral.

- **Protección avanzada**
  - Mitigaciones a medida en base a la definición de servicios y equipos
  - Mitigación inmediata de ataques incluyendo la opción de mitigación permanente.
  - Procedimiento de escalado telefónica y por email por institución.
  - Posibilidad de contactar con el SOC por teléfono o vía mail en modo 24x7/365
  - Tiempo medio de activación de la mitigación en 30 segundos.



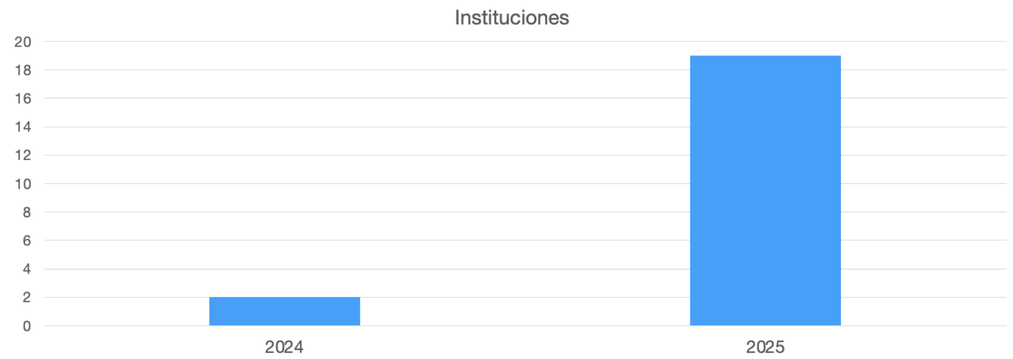
EGIDA. Mitigación de ataques de DDoS



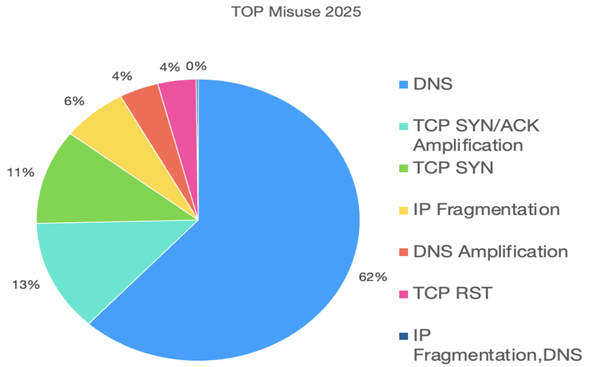
EGIDA. Mitigación de ataques de DDoS

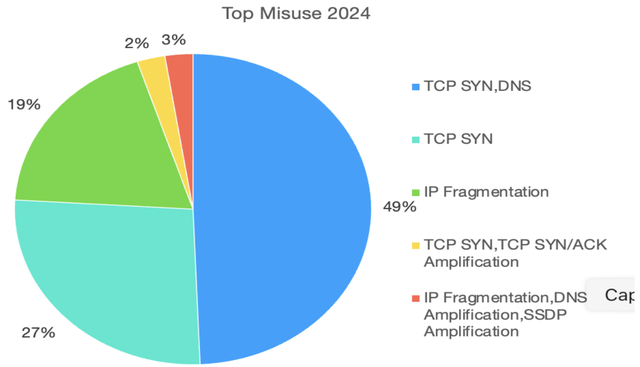
EGIDA. Mitigación de ataques de DDoS

Instituciones en PORTAL

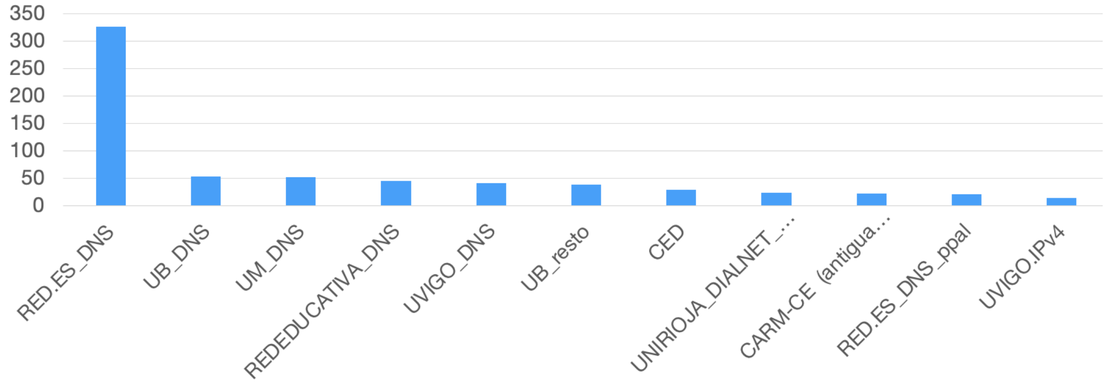


Tipología de los ataques

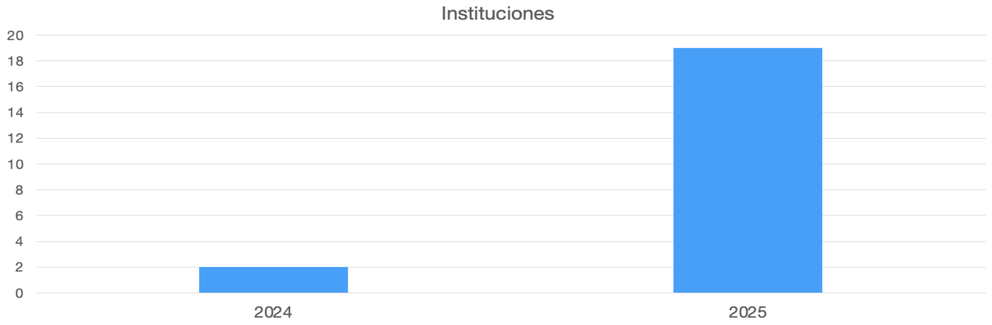




Ataques objetos



Instituciones en PORTAL

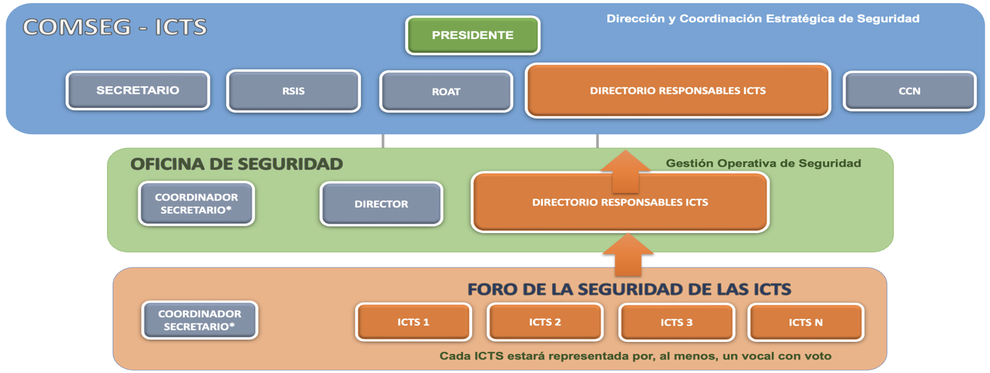


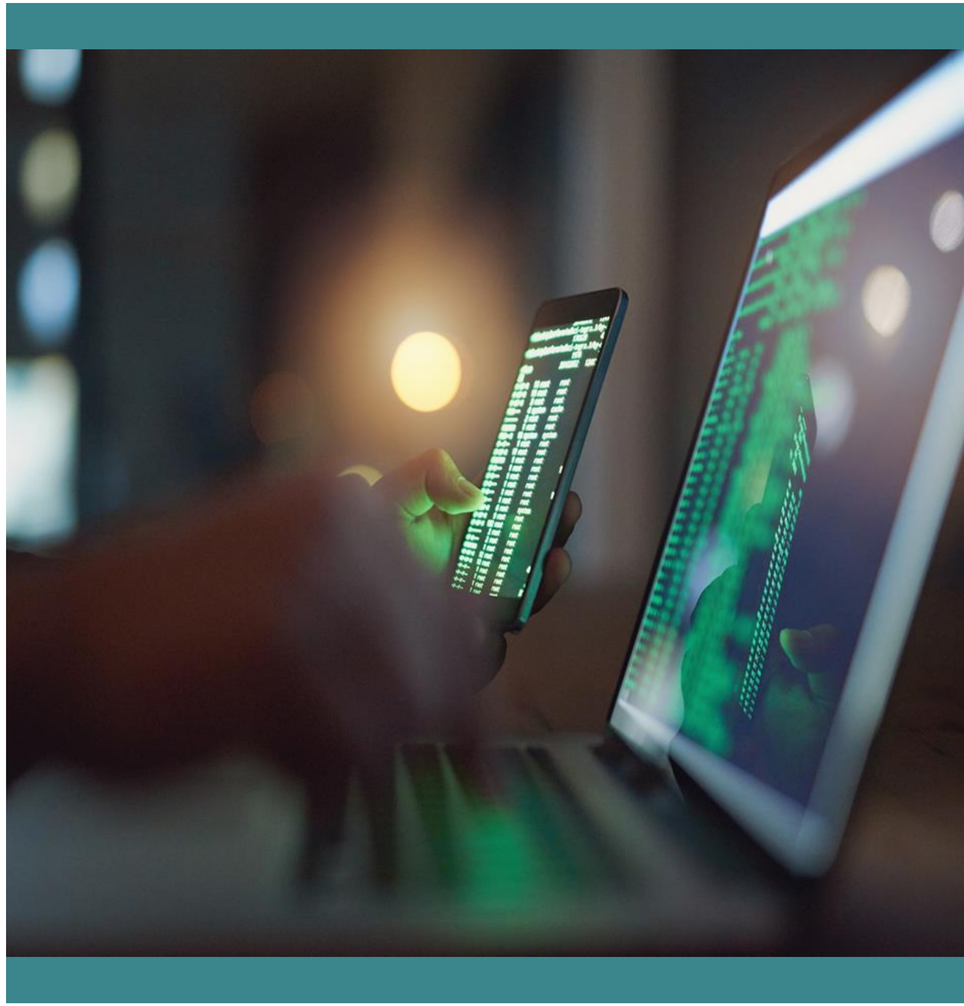
Adecuacion al ENS y servicios de seguridad a ICTSs

Esquema Nacional de Seguridad (ENS), de aplicación a todo el Sector Público.

EL ENS es el framework que establece la **política de seguridad para la protección adecuada de la información** tratada y los servicios prestados a través de un planteamiento común de **principios básicos, requisitos mínimos, medidas de protección y mecanismos de conformidad y monitorización.**

Incluye a los proveedores tecnológicos del sector privado que colaboran con la Administración.





SinMalos

¿Qué es?

SinMalos es un esfuerzo de la comunidad de seguridad de RedIRIS para generar ciberinteligencia adaptada a las redes académicas.

¿Qué ofrece?

Se trata de una herramienta que permite analizar y agrupar la información en tiempo real de cada una de las fuentes registradas para **bloquear el tráfico malicioso**.

¿Quién son los participantes?

CONSUMIDOR: Institución que tiene acceso a los feeds generados por el proyecto para su consumo en FWs, MTAs, SIEMs, etc.

PRODUCTOR: Institución que genera información de ciberseguridad propia y que la aporta a SinMalos. Por supuesto, un productor también puede ser consumidor.

** 2.024: inversión de 2 M€ en una actualización de Sin Malos*

Nº de instituciones que proporcionan información a SinMalos: **12**

Nº de instituciones que usan SinMalos: **92**

Nº de direcciones IP (promedio) reportadas por SinMalos **40 mil**

Las listas de información de SinMalos se comparten con la Red Nacional de SOCs del CCN-CERT

Llegó la orquesta

39 instituciones consumiendo feeds de Minemeld

38 instituciones consumiendo feeds de XSOAR

Instituciones en SinMalos

92

¿A DÓNDE VAMOS? | Feeds

SinMalos-MultiSource-HC

https://sinmalos.rediris.es/SM-MultiSource-HC

SinMalos-ALL

https://sinmalos.rediris.es/SM-ALL

REYES-CCN-CERT-Inbound

https://sinmalos.rediris.es/REYES-CCN-CERT-Inbound

REYES-CCN-CERT-outbound

https://sinmalos.rediris.es/REYES-CCN-CERT-Outbound

ELSA-CCN-CERT-inbound

https://sinmalos.rediris.es/ELSA-CCN-CERT-Inbound

Futuras mejoras que están por llegar

- SinMalos 2.0
- Retro-hunting
- Oráculo del malware
- Listas adicionales
- Enriquecimiento de indicadores
- Mejora continua

Soporte de SinMalos

Soporte 24x7

Administración

Monitorización

Interlocución con las instituciones

Automatización

Informes

Integración

Asesoramiento

Documentación

IRIS-Cert - Gestión de incidentes de seguridad

IRIS-Cert

Evolución de IRIS-CERT a un Servicio de Operaciones de Ciberseguridad para las instituciones públicas afiliadas a RedIRIS en coordinación con el CCN-Cert e integrado en la Red Nacional de SOC.

Histórico

2013

El servicio de notificación lo asume INCIBE.
Reorganización y división de funciones y servicios.

2024

Asumir el servicio de notificación de incidentes a instituciones públicas que actualmente cuya gestión está delegada INCIBE.

Desplegar las herramientas necesarias para la integración en la Red Nacional de SOC.

Creación de un servicio de CiberInteligencia que:

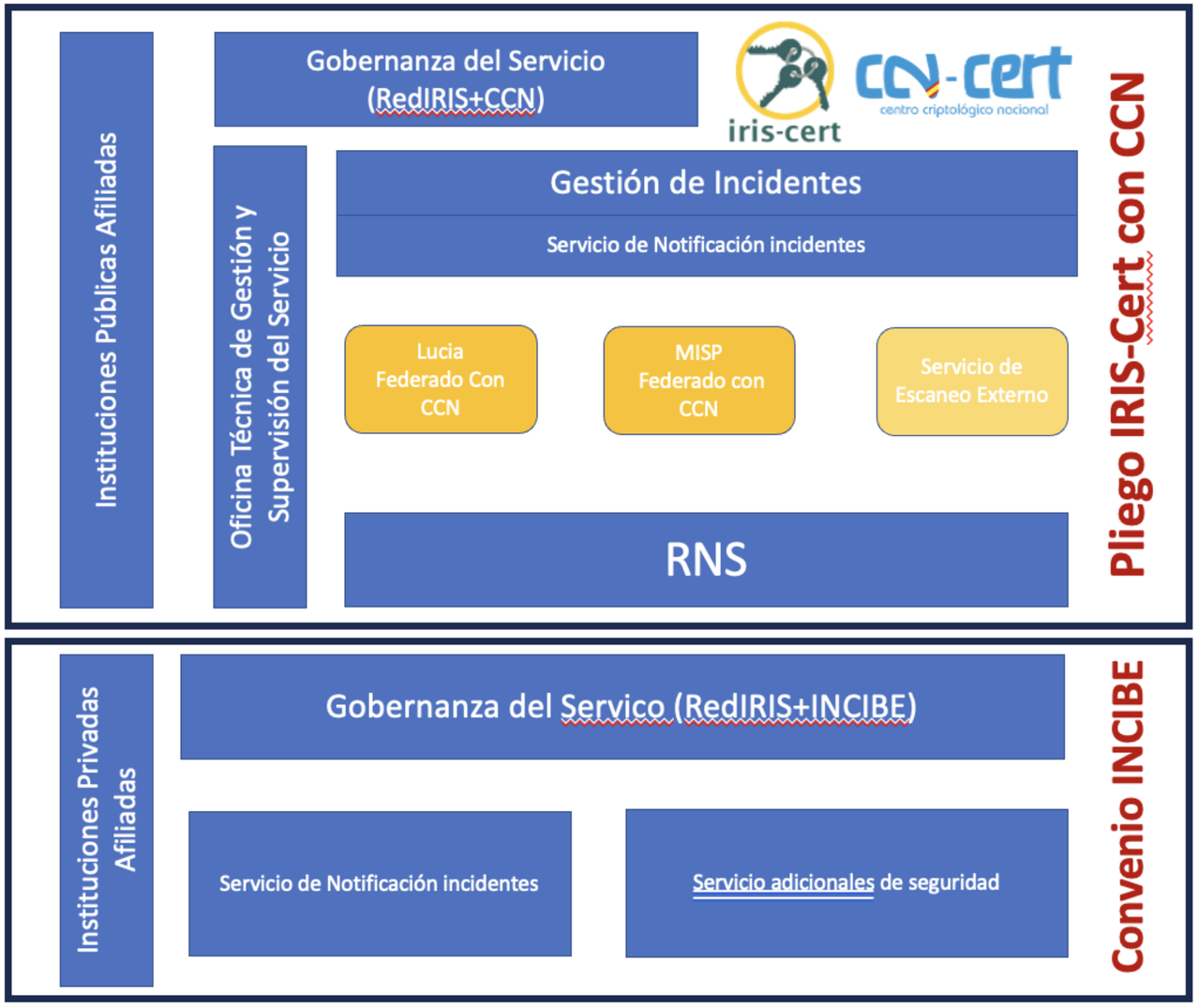
Gestione e integre la información de diferentes fuentes.
Vigile y detecte incidentes de seguridad en la comunidad.
Proporcione información en tiempo real que contribuya a mejorar el escudo de las instituciones afiliadas a RedIRIS.
Comparta esta información con la RNS.

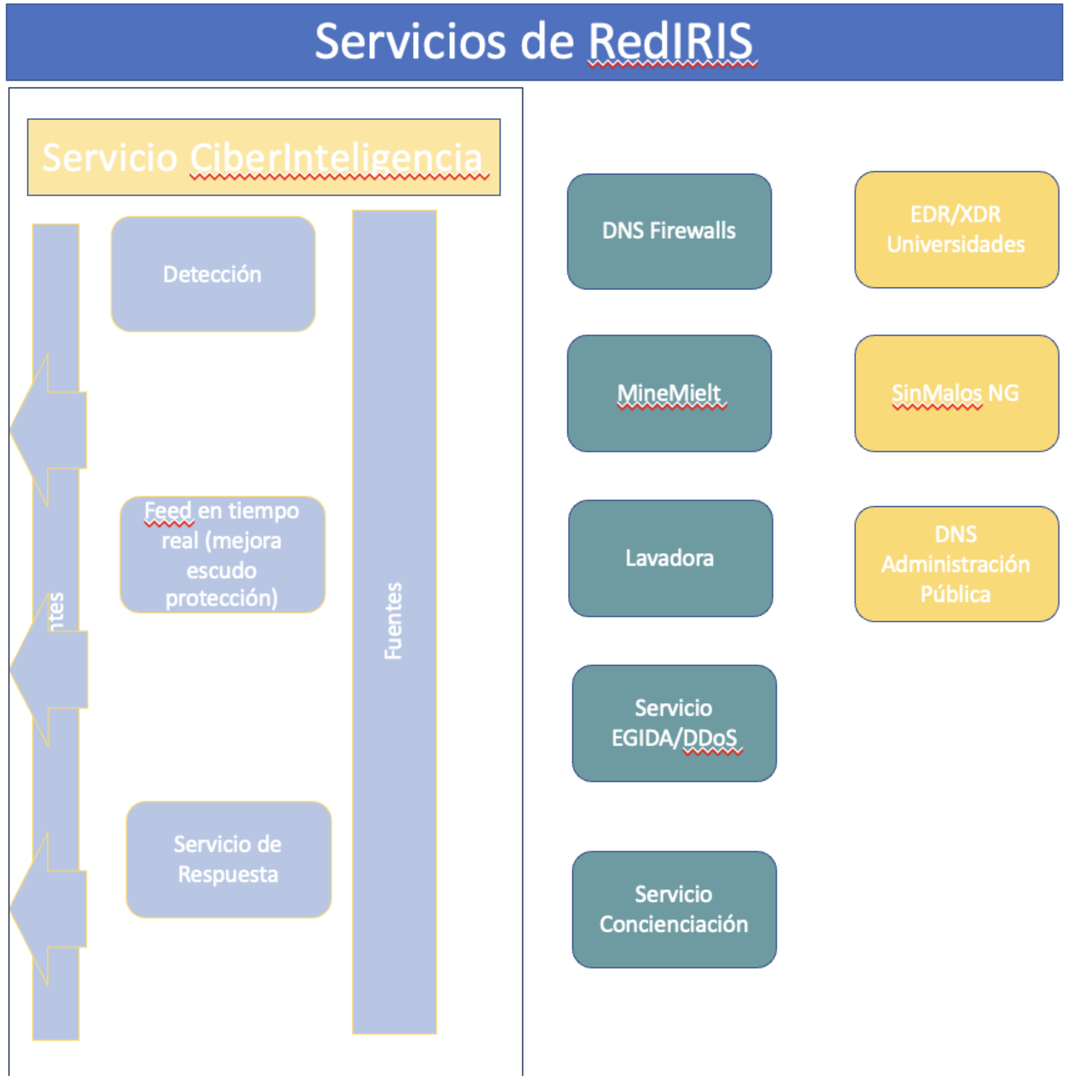
Crear un servicio de respuesta a incidentes que ayude a las instituciones.

Foro de Ciberseguridad 2025

iris-cert

IRIS-Cert - Gestión de incidentes de seguridad





¡Muchas gracias!