RedIRIS

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

www.rediris.es

SERVICIOS DE SISTEMAS Y SEGURIDAD

Antonio Fuentes Bermejo

XXXII Jornadas Técnicas de RedIRIS
Mallorca, 28 de mayo de 2024

GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
red.es
RedIRIS

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

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, …)

Adecuación a la ISO27001/ENS

En 2023, el servicio de Conectividad de RedIRIS pasó con éxito la certificación **ISO27001 de Seguridad de la Información**.

Actualmente, estamos en proceso para ampliar el alcance de dicha certificación incluyendo el servicio de Mitigación de Ataques de Denegación de Servicio (DDoS) y el servicio de identidad IdPnube.

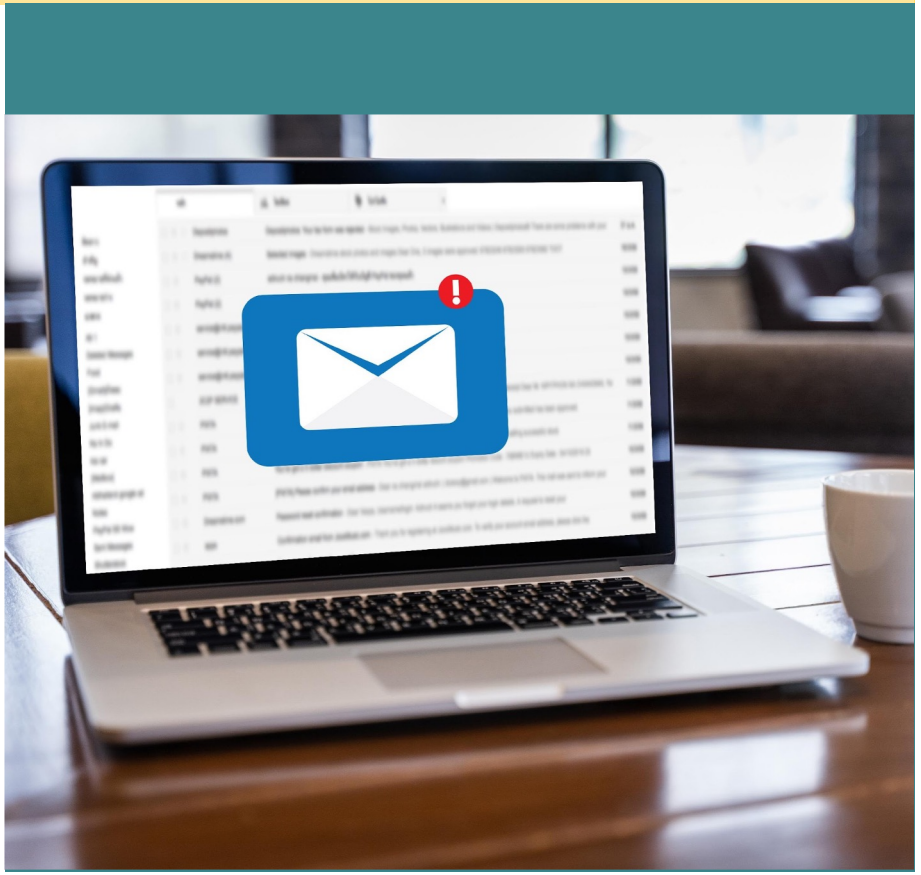
Actualmente, el Servicio de Conectividad de RedIRIS se encuentra inmerso en la fase de auditoria del **Esquema Nacional de Seguridad (ENS).** Estimamos que, en un periodo máximo de un mes, contemos con dicha certificación.

De cara a 2024, se ampliará el alcance para añadir los servicios de Mitigación de Ataques de Denegación de Servicio (DDoS) y el servicio de identidad IdPnube

Servicio de filtrado antispam (Lavadora)

¿Qué ofrecemos?

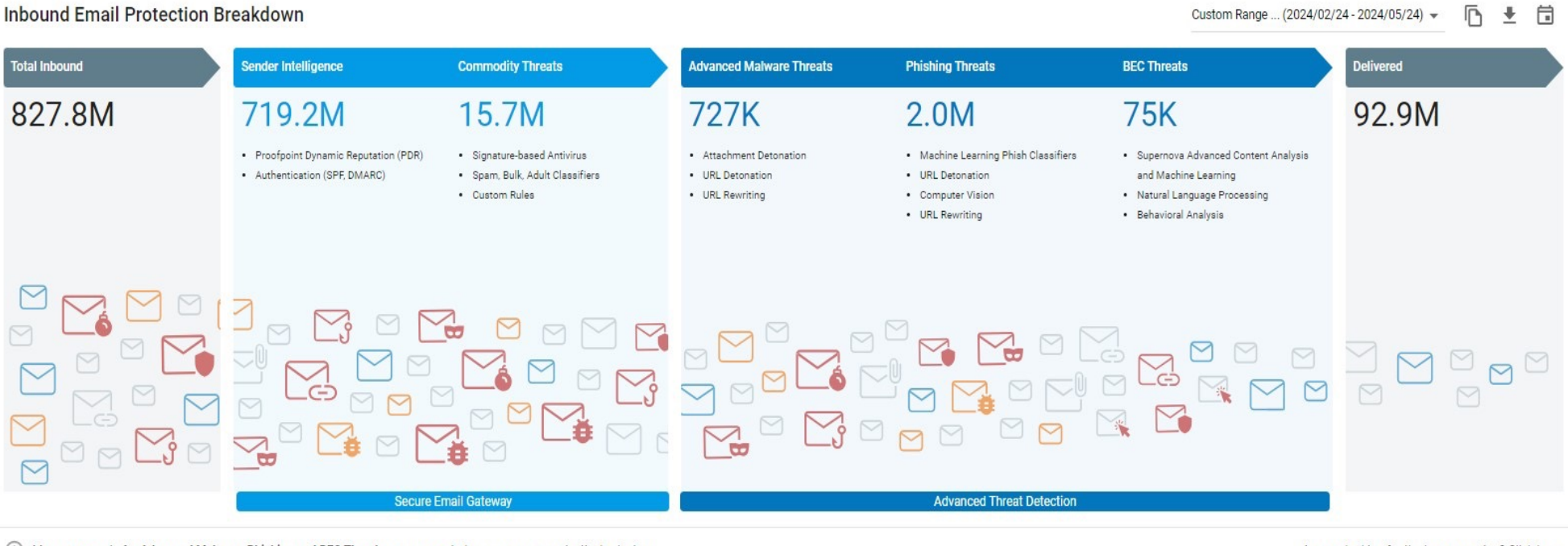
RedIRIS ofrece a las instituciones afiliadas la posibilidad de pasar su **correo electrónico** por un **sistema de filtrado antispam y antivirus**, antes de entregárselo “limpio” a la institución (de ahí lo de “lavadora”).



- 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)

- 827.8 M de correos han entrado a la plataforma
- 92.9 M de correos han llegado hasta el usuario
- 734.9 M de correos han sido detectados y descartados por la plataforma (reputación y filtros tradicionales)
- 778.000 de correos detectados por filtros avanzados de Proofpoint



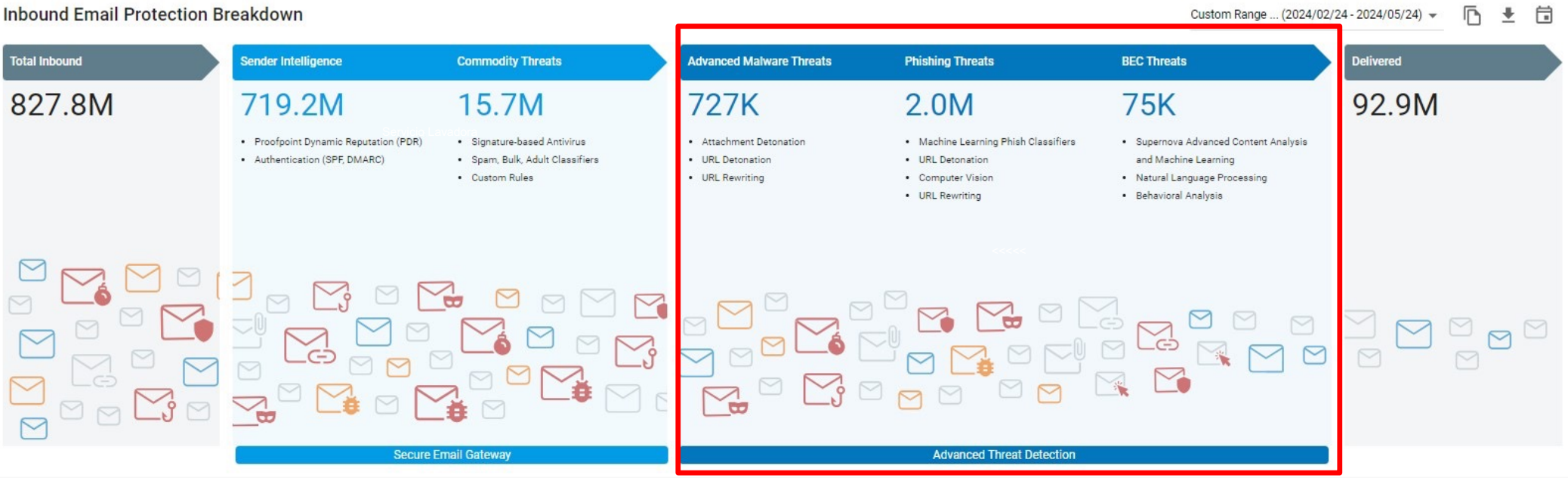
Servicio de filtrado antispam (Lavadora)

ADVANCED THREAT DETECTION – Filtros avanzados de Proofpoint

- *Advanced Malware Threats* – amenazas de malwares detectados de a través de sandboxing en los adjuntos y enlaces

- *Phishing Threats*– amenazas de phishing detectados con los motores AI/ML (inteligencia artificial y machine learning) y sandboxing

- *BEC Threats* – amenazas de ingeniería social detectadas con el motor de análisis de comportamiento de Supernova (Supernova Behavioral Engine)



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 En 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

Simulación de phishing (SIMULPHISHING)

Instituciones

CRG, IAC, INTA, CELLS, PSA, IRAM, UHU, OAN,ITACYL,CIEMAT, CSIC,UBU, ITA, LSC-CANFRANC , CNIC , UMH, UNIRIOJA, UPO, ULOYOLA , CTTC, CLPU, CNIO, UNICAN, UNEX, VHEBRON, UNEBRIJA

Usuarios: 12.000
Cada año 12 simulacros

- La formación es finalizada por un 10% de los usuarios registrados.
- Es necesario motivar a los usuarios en esta actividad de formación
- Se confirma que las instituciones que han seguido la formación han tenido mejor progresión que el resto
- El servicio se prolongará 3 años hasta 2027

TECNIRIS

Grupo de 2123 técnicos de toda la comunidad RedIRIS

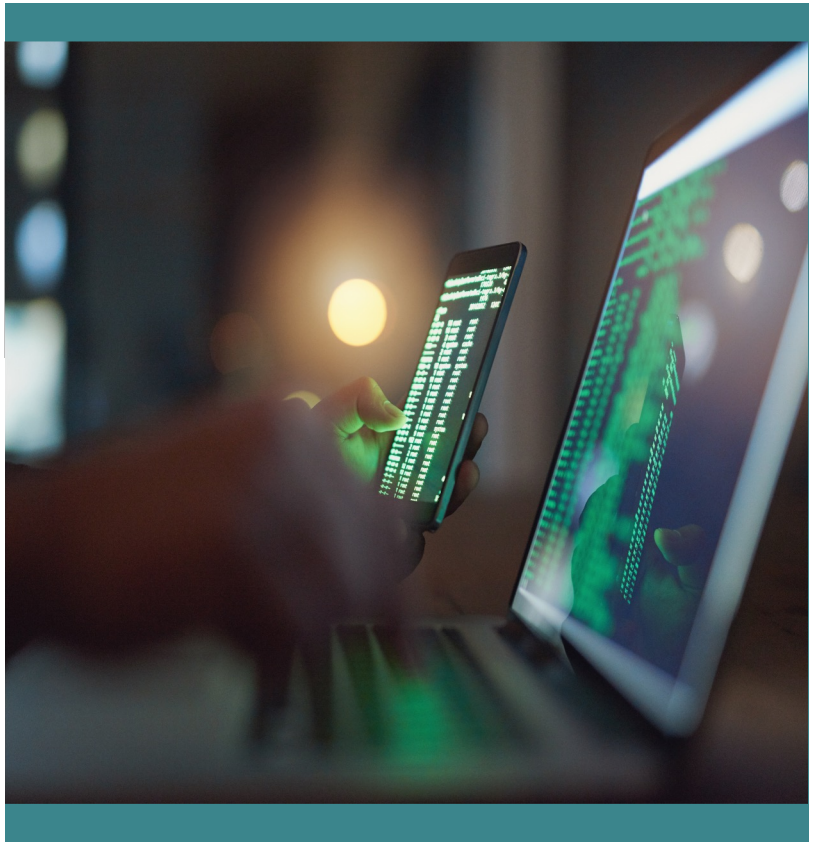
Se organizaron 4 videosesiones:

- Experiencias de plataformas IaaS en nubes locales. Experiencias de EDUCA.MADRID - CSIC - Universidad de Almería y UNILEON . 2 días (6h) 230 asistentes cada día
- Introducción a **plataformas basada en kubernetes**. Experiencias EMBL y UNILEON. 2 días (5h) 200 asistentes cada día
- **Taller de introducción a plataformas basada en kubernetes**. Experiencias de EMBL y UNILEON . 210 asistentes
- **Presentación servicio @firma de RedIRIS**. 160 asistentes

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*)

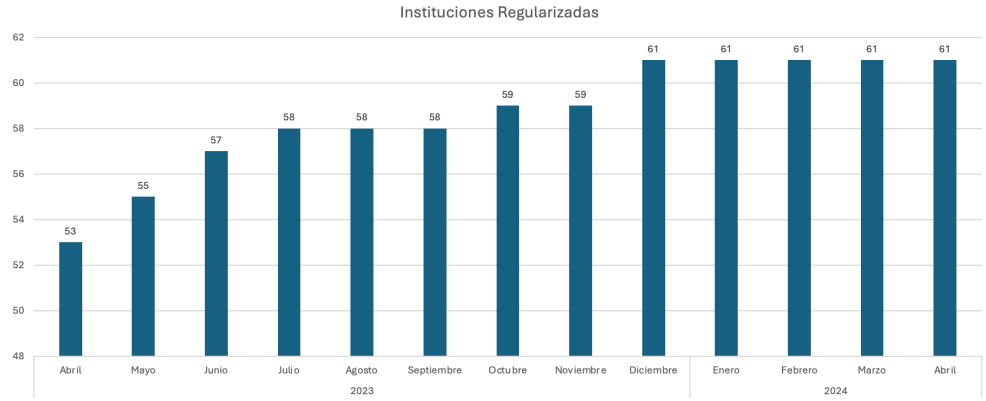


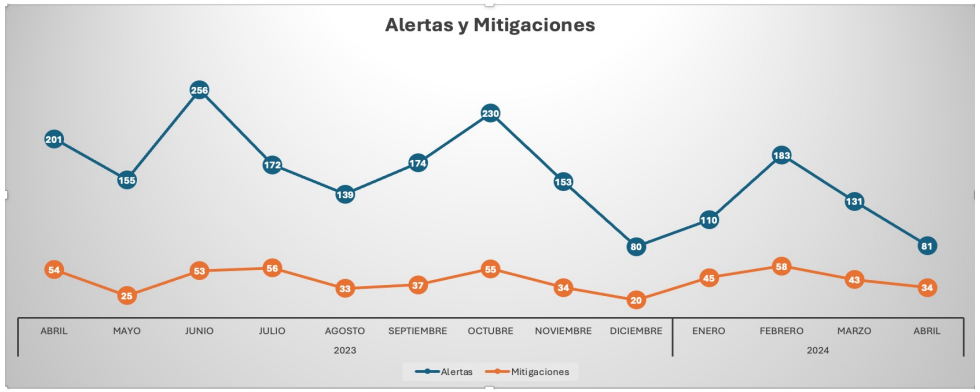
Ventajas de nuestro servicio

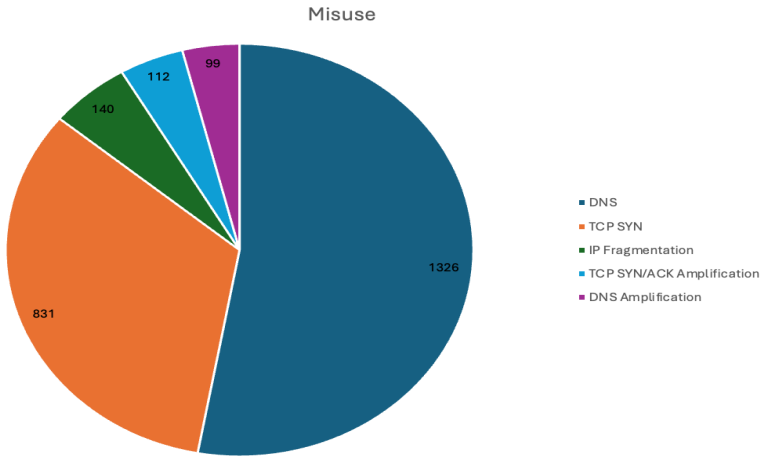
- Protección básica
  - Todas las instituciones conectadas están monitorizadas y protegidas 24x7
  - Rangos IP que se protegen son los oficiales que están encaminados el troncal de RedIRIS por el NOC
  - Revisión de alarmas por el SOC de mitigación en modo 24x7 y mitigación básica.
  - Notificación en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





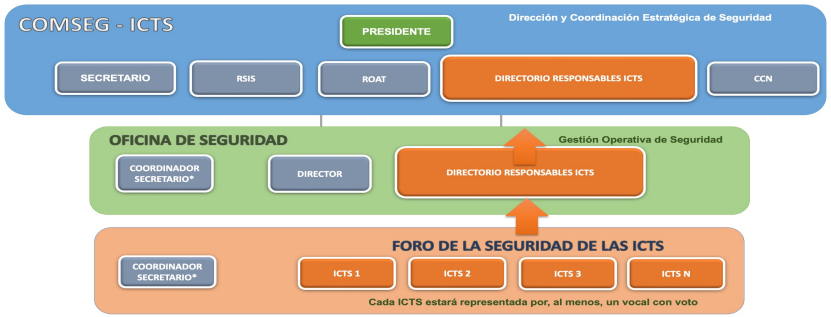


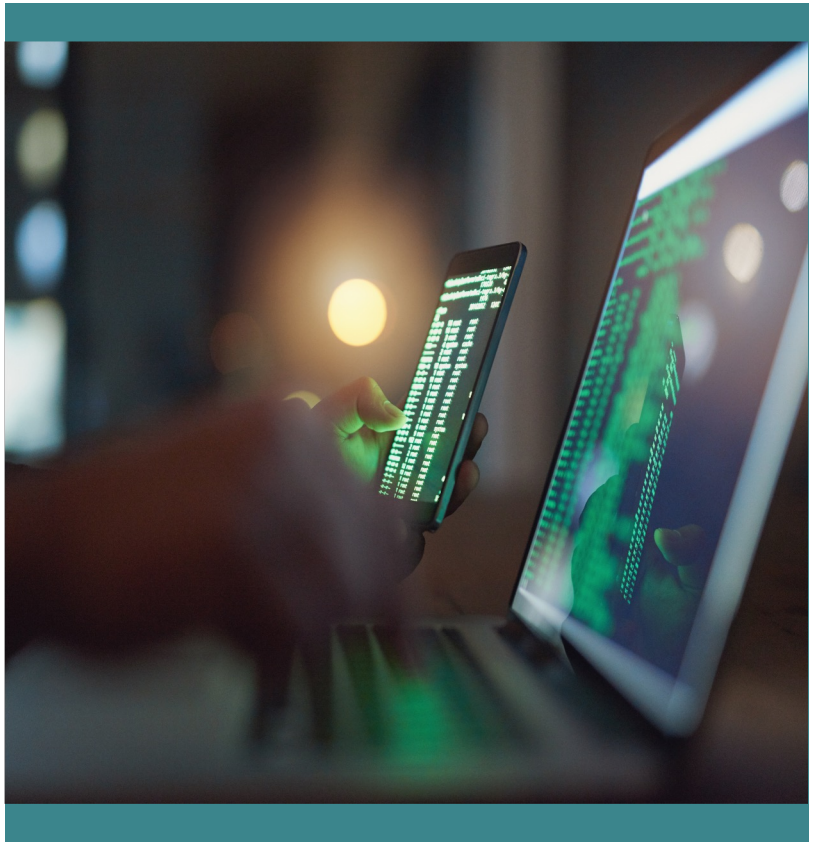
Adecuacion al ENS y servicios de seguridad a ICTSs

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

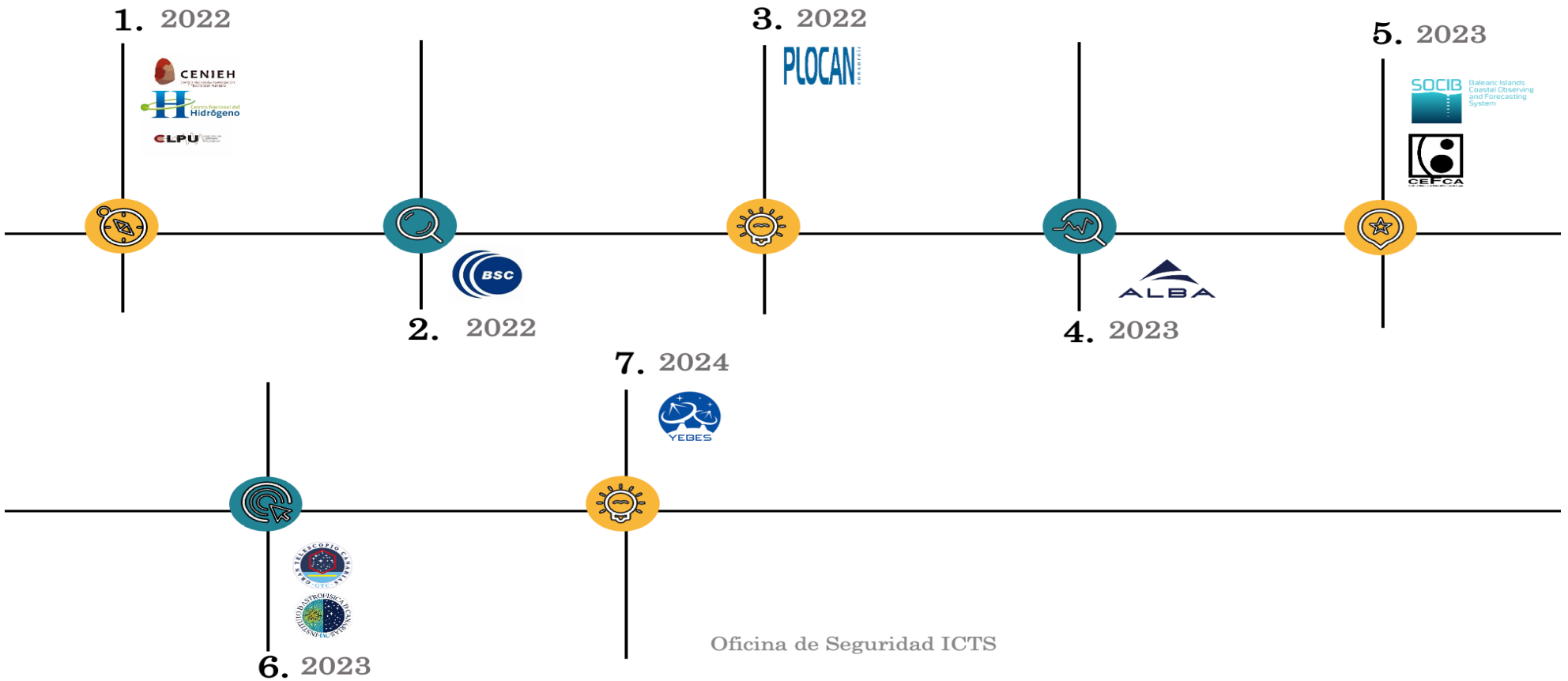
EL ENS es el framework que establece la **política de seguridad para la protección adecuada de la información** tratada y los servicios prestados a través de un planteamiento común de **principios básicos, requisitos mínimos, medidas de protección y mecanismos de conformidad y monitorización.**

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





Adecuacion al ENS y servicios de seguridad a ICTSs



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.

Nº de instituciones que proporcionan información a SinMalos: **6**

Nº de instituciones que usan SinMalos: **66**

Nº de direcciones IP (promedio) reportadas por SinMalos **25 mil**

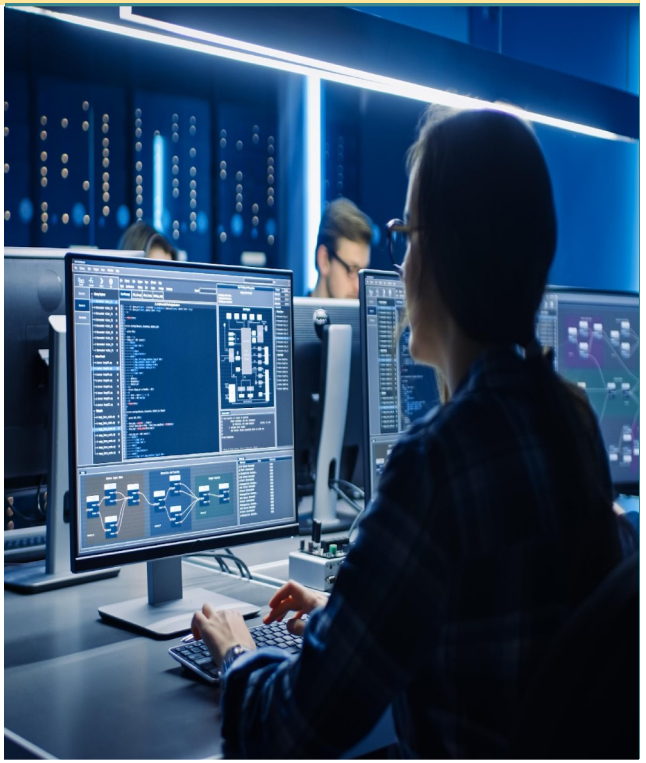
Las listas de información de SinMalos se comparten con la Red Nacional de SOCs del CCN-CERT

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

GOBIERNO DE ESPAÑA · MINISTERIO DE CIENCIA, INNOVACIÓN Y UNIVERSIDADES · MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA · SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

red.es | RedIRIS

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.

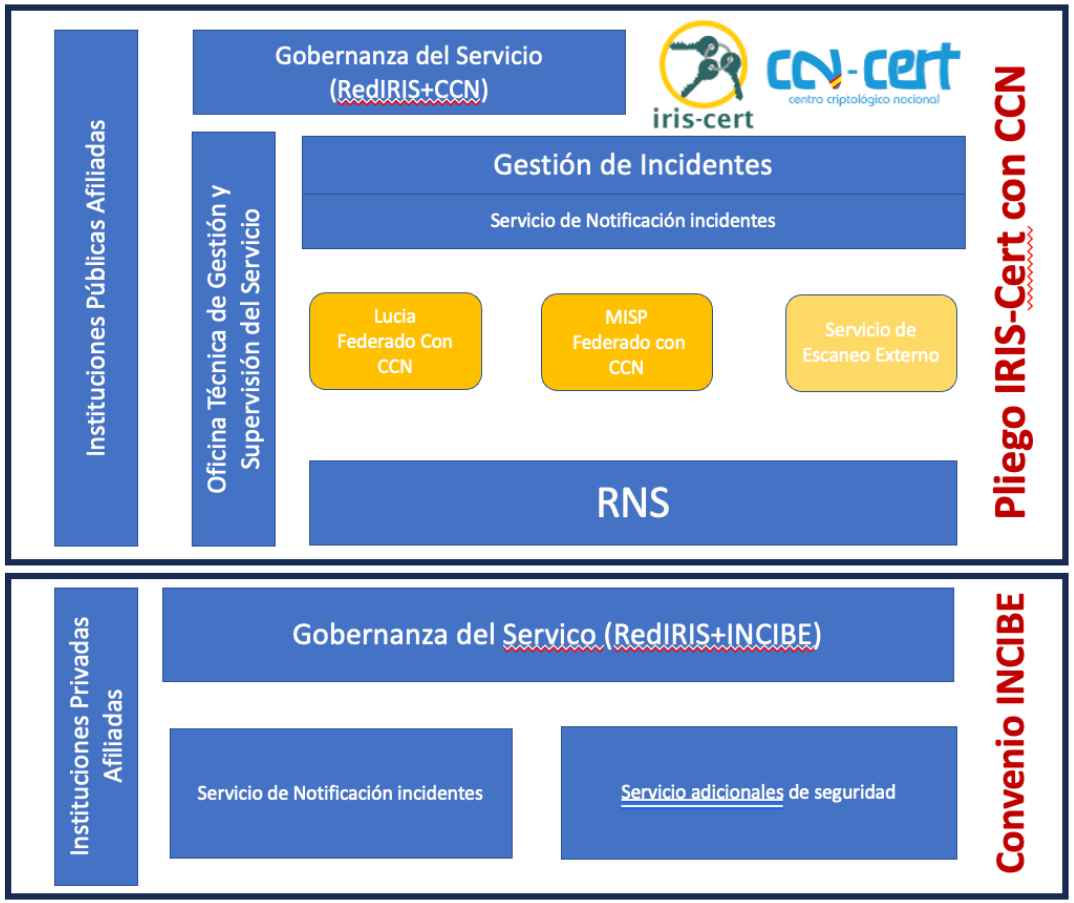
Desplegar las herramientas necesarias para la integración en la Red Nacional de SOC.

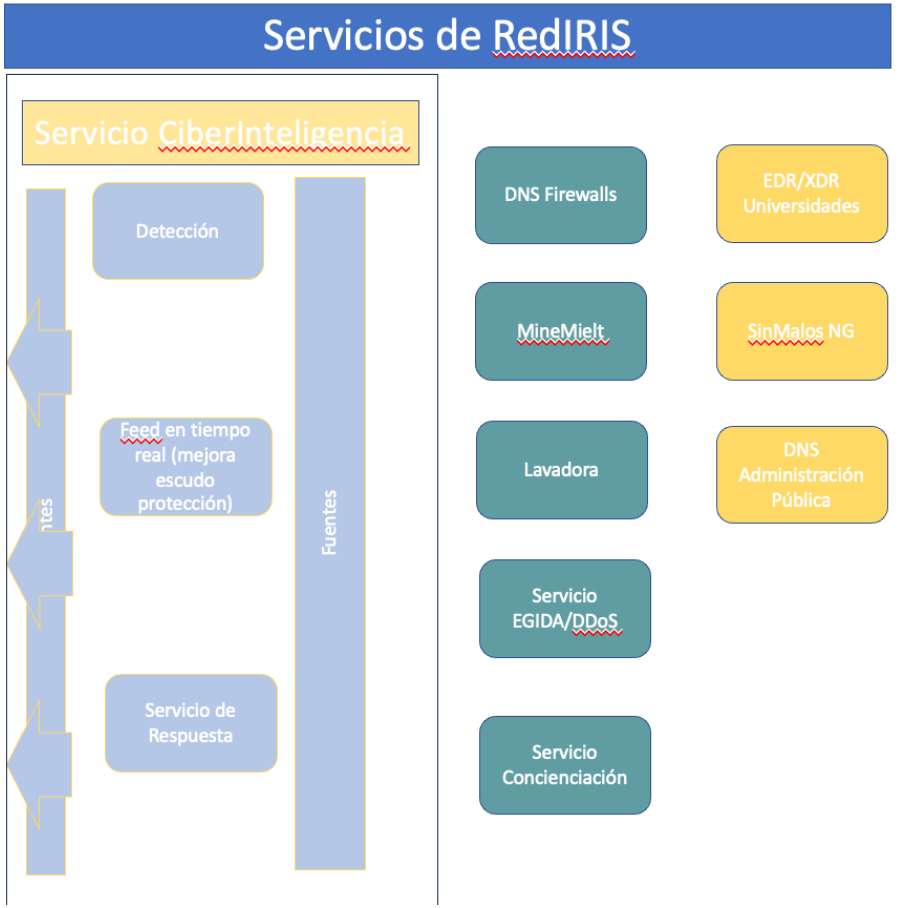
Creación de un servicio de CiberInteligencia que:

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.

IRIS-Cert - Gestión de incidentes de seguridad





¡Muchas gracias!