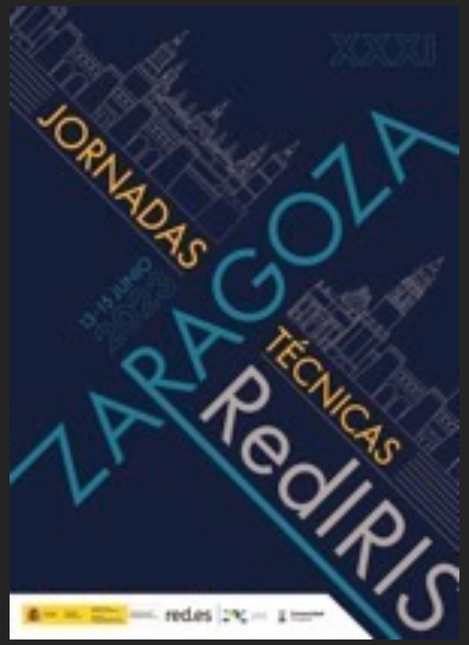
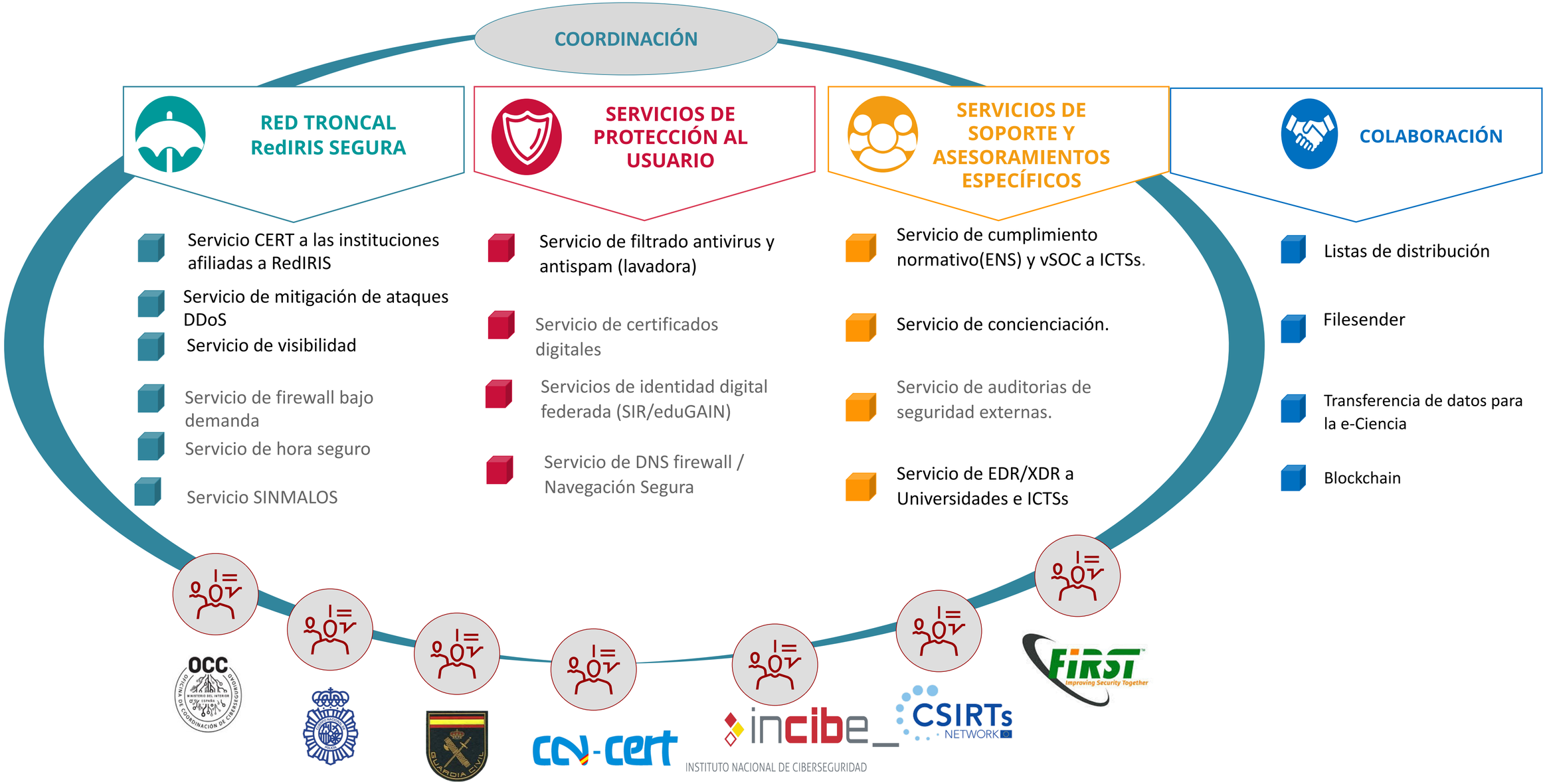


Actualidad de los Servicios de Sistemas y Seguridad de RedIRIS

- RedIRIS
- más que una Red,
- una **Red Segura**


COORDINACIÓN
RED TRONCAL
RedIRIS SEGURA
Servicio CERT a las instituciones afiliadas a RedIRIS
Servicio de mitigación de ataques DDoS
Servicio de visibilidad
Servicio de firewall bajo demanda
Servicio de hora seguro
Servicio SINMALOS
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 vSOC a ICTSs.
Servicio de concienciación.
Servicio de auditorias de seguridad externas.
Servicio de EDR/XDR a Universidades e ICTSs
COLABORACIÓN
Listas de distribución
Filesender
Transferencia de datos para la e-Ciencia
Blockchain
OCC
CCN-CERT
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
CSIRTs NETWORK
FIRST
Improving Security Together

SERVICIOS DE PROTECCIÓN AL USUARIO

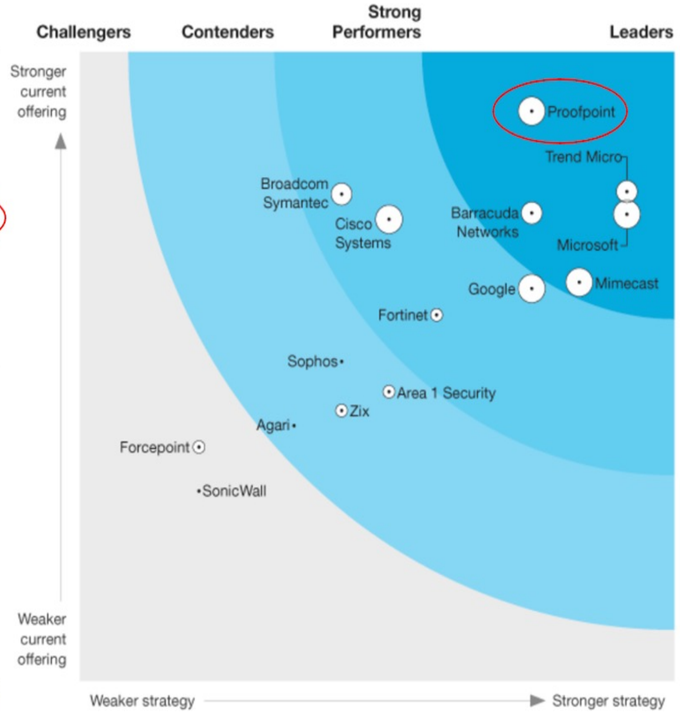
Servicio de filtrado antivirus y antispam (lavadora)

El Servicio LAVADORA de RedIRIS se ofrece de forma gratuita a las instituciones afiliadas y consiste en recoger el correo electrónico de la institución procedente de Internet y, antes de entregarlo a la institución, revisarlo para eliminar el correo basura, virus o mensajes fraudulentos. Es decir, ofrece un relay de correo común que hace las funciones de filtrado de spam así como la detección de virus del correo destinado a los usuarios de la institución que lo utilice.

- Servicio lanzando en 2010
- Migración de la tecnología a través de la cual se presta el servicio a ProofPoint (Noviembre 2022).
- El correo electrónico es el primer vector de ataque a usuarios e instituciones. Los ataques sociales tales como el phishing y las estafas llegan a través del correo electrónico en el 96% de las veces.
- La plataforma Lavadora de seguridad en el correo electrónico bloque el malware, phishing y email fraudulentos.
- Protección a más de 100 , 2000 dominios y 1,5 millones de direcciones de correo

MQ Gartner-Email Security

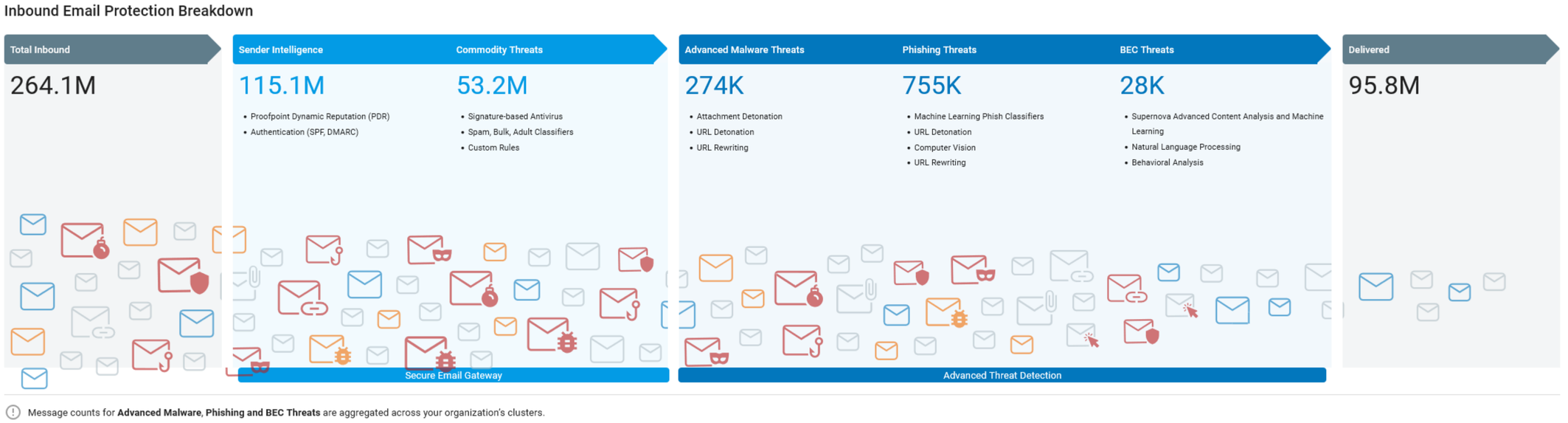
Forrester Wave™: Enterprise Email Security 2021



Contacto: lavadora@rediris.es

Datos Globales

- Perido: 1 de Abril a 12 de Junio de 2023
- 264.1 M de correos han entrado a la plataforma
- 95.8 M de correos han llegado hasta el usuario
- 168.3M de correos han sido detectados y descartados por la plataforma (reputación y filtros tradicionales)



Servicio de simulacros y concienciación

Ejecución de simulacros de phishing por correo electrónico acompañada de formación de usuarios orientada a la concienciación en materias de seguridad a las instituciones académicas y científicas afiliadas a RedIRIS.

SERVICIOS DE SOPORTE Y ASESORAMIENTOS ESPECÍFICOS

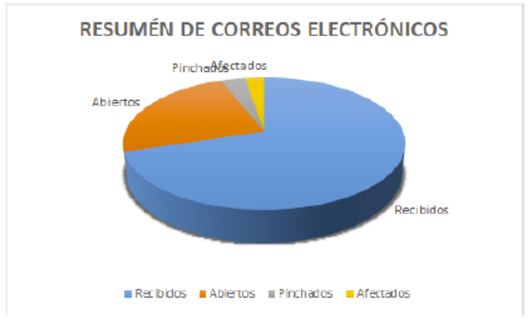
Servicio de simulacros y concienciación

Ejecución de simulacros de phishing por correo electrónico acompañada de formación de usuarios orientada a la concienciación en materias de seguridad a las instituciones académicas y científicas afiliadas a RedIRIS.

- El servicio SIMULPHISHING tiene tres líneas de actuación
  - Simulacros de phishing.
  - Plataforma de concienciación y formación en ciberseguridad
  - Generación y envío de informes de cada simulacro y evolución de formación por usuario
- Detalles del servicio:
  - 4500 usuarios al año de diferentes organizaciones RedIRIS
  - Ejecuta 12 simulacros de phishing al año, 1 al mes
  - Plataforma cloud (Attack Simulator) para formarse y concienciarse en ciberseguridad
- Objetivos
  - Detectar los usuarios mas vulnerables de una institución
  - Cambiar el comportamiento de los empleados: mediante formación basada en amenazas reales, comportamientos y carencias de conocimiento.
  - Reducir la exposición a ataques de una organización mediante usuarios bien formados

Resumen del programa

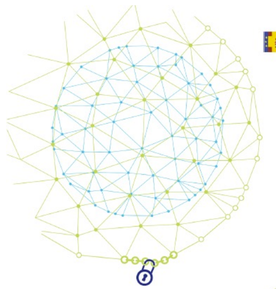
Hasta el momento, se han enviado un total de **568** correos electrónicos, en tres simulaciones diferentes, con el resultado de **193** correos abiertos y **27** enlaces pinchados, por lo que podría haber **21** usuarios afectados.



De los datos anteriores se extrae que de los correos de phishing recibidos, el **33,98 %** son abiertos y el **13,99 %** de estos, consiguen el objetivo de engañar al usuario.

Recibidos	Abiertos	Abiertos %	Pinchados	Pinchados %	Afectados	Afectados %
568	193	33,98%	27	13,99%	21	10,88%

Si comparamos los datos obtenidos con el trimestre anterior, se ha pasado de **71** usuarios con riesgo alto a **66** usuarios, lo que supone un descenso del **7,04 %**. De esos **66** usuarios, **50** son usuarios reincidentes, por lo que se recomienda recordar la importancia de completar el curso de formación.



CENTRO TECNOLÓGICO CARTIF

Informe del Servicio Gestionado para la Concienciación de los Usuarios 2do trimestre

Referencia: R-CARTIF-20220712
Fecha: 12/07/2022

Fdo. Carlos Revilla González

Contacto: simulphishing@rediris.es

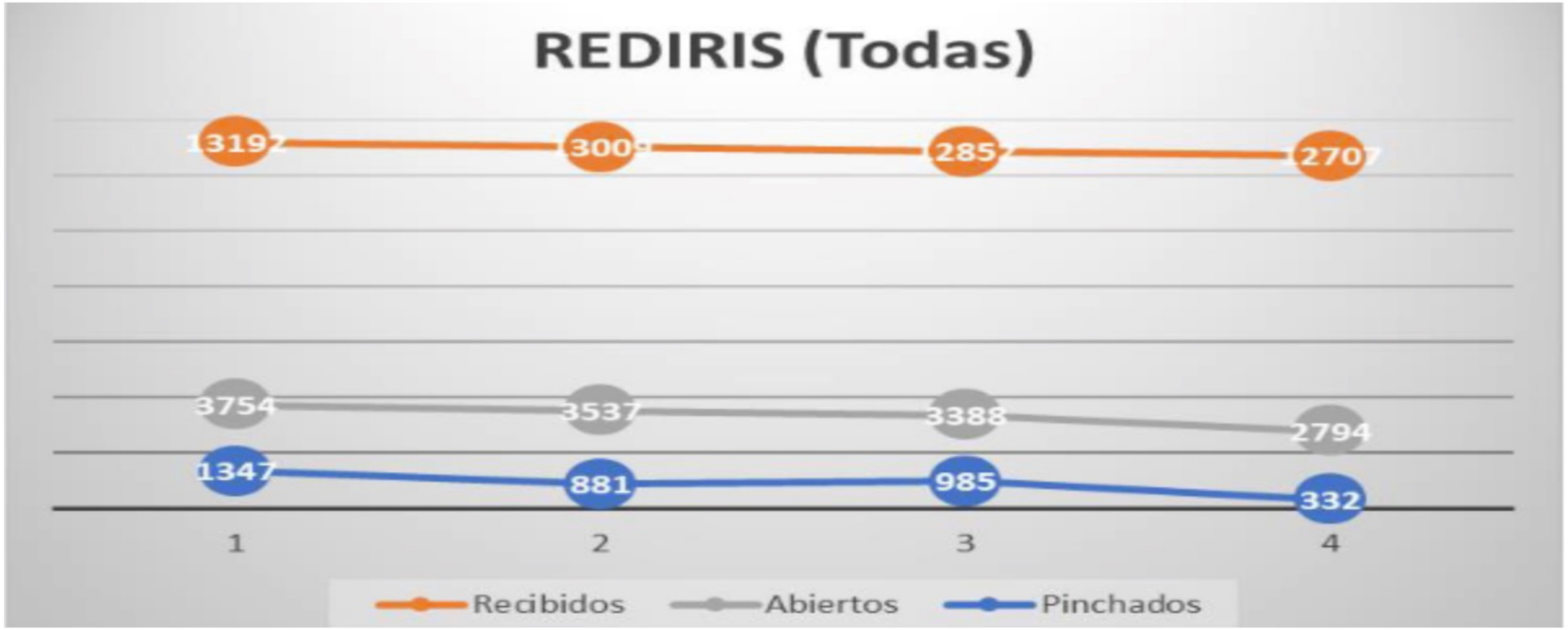
FASES DE EJECUCIÓN DEL SERVICIO

- En 2022 se llevo a cabo una campaña con la plataforma de Attack Simulator para un total de 5000 usuarios de 11 instituciones
- En 2023 están en marcha dos campañas con dos plataformas diferentes (Attack Simulator y Proofpoint) para una total de 10.000 usuarios de 11 instituciones

- Las campañas contemplan:
  1. Página bienvenida y difusión de la actividad
  2. 2. Un examen inicial para todos los usuarios registrados
  3. 3. Un simulacro al mes con posibilidad de formación en ciberseguridad para los usuarios vulnerables detectados en dichos simulacros
  4. 4. Un curso anual formación en ciberseguridad genérico para todos los usuarios registrados.
- Información:

  https://www.rediris.es/formacion/
  https://rediris.es/concienciacion/

Contacto: simulphishing@rediris.es



Efectividad Formacion

En el apartado de la formación, no se han conseguido los objetivos, llegando en el mejor de los casos a un 24,75% de seguimiento en el tercer trimestre.

Finalizaron la formación 294 personas de las 2.573 inscritas.

Contacto: simulphishing@rediris.es

Servicio de cumplimiento normativo (ENS) y vSOC a ICTSs

RedIRIS presta a los consorcios gestores de ICTSs (Infraestructuras Científicas y Técnicas Singulares) que dependen del Ministerio de Ciencia e Innovación un servicio de apoyo y asesoramiento en el cumplimiento de requisitos regulatorios de seguridad, orientado en particular al cumplimiento del Esquema Nacional de Seguridad.

SERVICIOS DE SOPORTE Y ASESORAMIENTOS ESPECÍFICOS

Servicio de cumplimiento normativo (ENS) y vSOC a ICTSs

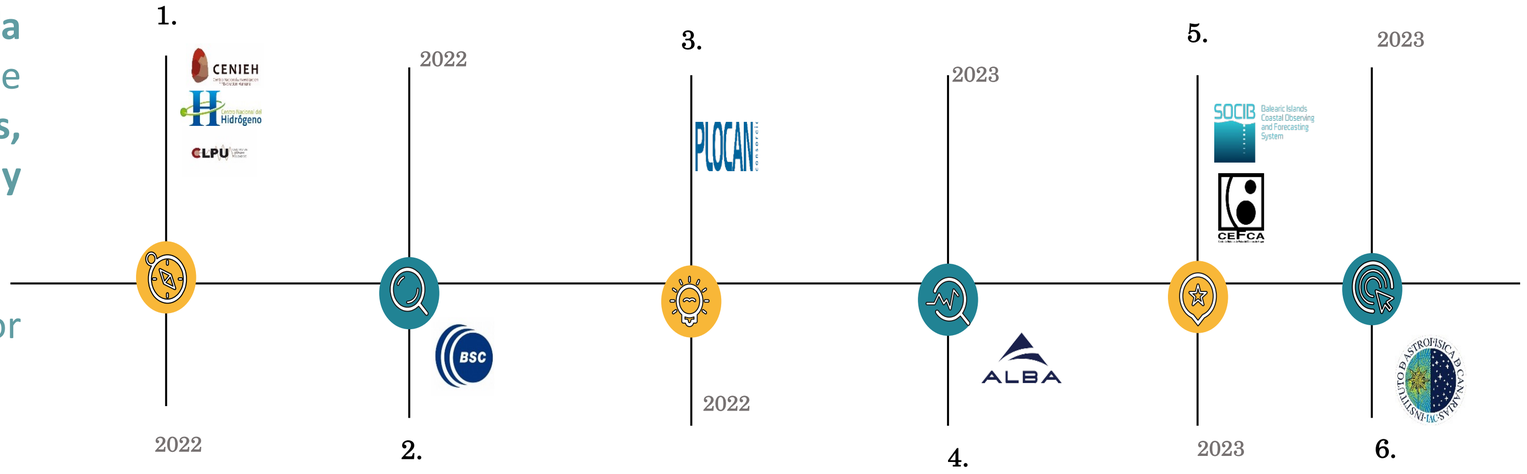
RedIRIS presta a los consorcios gestores de ICTSs (Infraestructuras Científicas y Técnicas Singulares) que dependen del Ministerio de Ciencia e Innovación un servicio de apoyo y asesoramiento en el cumplimiento de requisitos regulatorios de seguridad, orientado en particular al cumplimiento del Esquema Nacional de Seguridad.

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.

INCORPORACIONES



Esquema Nacional de Seguridad

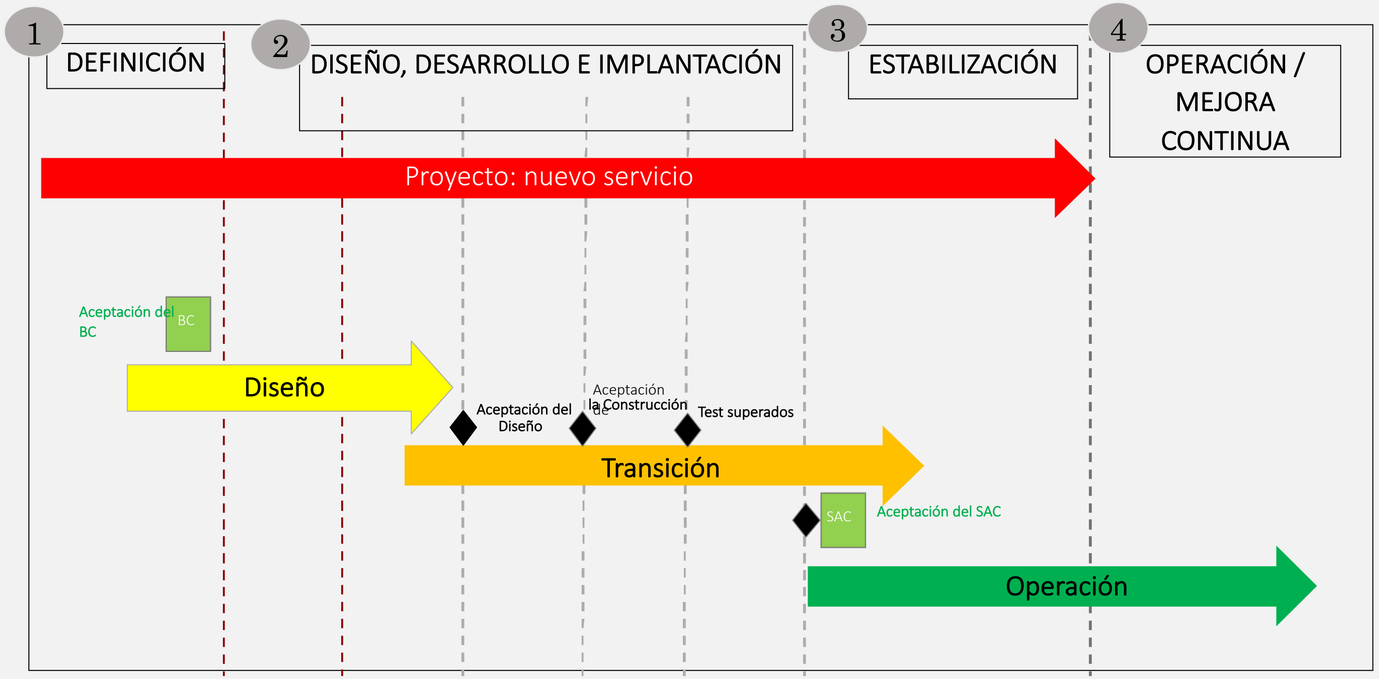
GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

RedIRIS red.es

Infraestructuras Científicas y Técnicas Singulares

FASE DE LOS SERVICIOS

Se han establecido **cuatro (4) fases** que se desarrollan de manera consecutiva junto con **actividades e hitos** que permiten determinar el estado de avance



Alcance determinado para las fases

Definición: Aceptación del Business Case.

Diseño, desarrollo e implantación: Realización del kick off del proyecto e inicio de la estrategia y diseño del proyecto para su respectiva aceptación e inicio de test.

Estabilización: Aceptación de los criterios de aceptación del servicio e inicio de entrega del Servicio.

Operación / mejora continua: Operación del Servicio y cierre del proyecto.

Servicios de Ciberseguridad

- Servicio de protección contra fuga de información.
- Vigilancia digital y bastionado de red
- Evaluación de la superficie de exposición.
- Servicio automatizado de análisis de vulnerabilidades
- Notificación e investigación de incidentes de seguridad
- Servicio de cibervigilancia
- Gestión de la seguridad y mejora continua

Servicio de EDR centralizado para Universidades

Sistema de análisis, detección y prevención de amenazas en End Points. Inicialmente previsto para dar servicio a universidades públicas a través de los fonde Europeos

Servicio de EDR centralizado para Universidades

Sistema de análisis, detección y prevención de amenazas en End Points. Inicialmente previsto para dar servicio a universidades públicas a través de los fonde Europeos

- Proyecto conjunto del Grupo de Seguridad CRUE-TIC y RedIRIS.
- En fase de preparación de las condiciones técnicas específicas para la adquisición de las licencias o subscripciones para la prestación del servicio.
- Modelo descentralizado para la prestación del servicio (Multi-Tenant) con capacidad de visibilidad horizontal con objeto de implementar servicios avanzados.
- Servicio centralizado en RedIRIS de alerta y soporte y apoyo a los equipos de seguridad de las universidades.
- Se orienta a licencias básicas (EDR) principalmente, aunque se podrían incluir licencias avanzadas (XDR).
- Coordinación desde el SOC de IRIS-CERT, integrado en la Red Nacional de SOC (RNS)

SECURE REDIRIS BACKBONE

Servicio “SINMALOS”

El servicio “SINMALOS” es un servicio que se presta en colaboración con la Universidad Autónoma de Madrid. Este servicio proporciona el intercambio de inteligencia de amenazas basado en el software de Minemeld, proporcionando información en tiempo real de IP maliciosas que están atacando a las instituciones afiliadas.

SECURE REDIRIS BACKBONE

Proyecto creado por la Universidad Autónoma de Madrid (Victor Barahona) que se ha implantado en RedIRIS que opera el servicio.

Trabajando en una evolución del servicio utilizando fondos de recuperación y sustitución del software de Minemeld.

- Suministro de nueva plataforma para la sustitución de Minemeld
- Instalación y configuración avanzada de los casos de uso.
- Servicio de soporte y de atención específico a los usuarios.

SECURE REDIRIS BACKBONE

Servicio CERT a las instituciones afiliadas

El servicio de gestión de incidentes de seguridad de RedIRIS (IRIS-CERT) tiene como objetivo coordinar la respuesta ante incidentes de seguridad informática que afecten a la seguridad de las redes de las instituciones afiliadas, como ataques de denegación de servicio, virus, gusanos, troyanos, etc. y realizar una labor preventiva avisando con tiempo a dichos centros de problemas potenciales, ofreciéndoles asesoramiento y facilitándoles soporte complementario

SECURE REDIRIS BACKBONE

Servicio CERT a las instituciones afiliadas

El servicio de gestión de incidentes de seguridad de RedIRIS (IRIS-CERT) tiene como objetivo coordinar la respuesta ante incidentes de seguridad informática que afecten a la seguridad de las redes de las instituciones afiliadas, como ataques de denegación de servicio, virus, gusanos, troyanos, etc. y realizar una labor preventiva avisando con tiempo a dichos centros de problemas potenciales, ofreciéndoles asesoramiento y facilitándoles soporte complementario

- **Servicio IRIS-CERT.**
  - Servicio de notificación externa prestado actualmente por INCIBE.
  - RedIRIS asumirá el servicio de notificación para las instituciones públicas afiliadas a RedIRIS, IRIS-CERT
    - RedIRIS en colaboración con CCN-CERT asumirá el servicio de notificación a instituciones públicas afiliadas a RedIRIS con evolución a SOC.
    - INCIBE coordinado con RedIRIS, seguirá prestando el servicio de notificación para instituciones privadas afiliadas a RedIRIS
  - Trabajando en el pliego para la contratación de los recursos necesario para la atención del servicio.

- **Evolución del servicio IRIS-CERT** a un SOC con capacidades de:
  - Visibilidad horizontal de los servicios de seguridad de RedIRIS.
  - Capacidad de **análisis, detección, atención y notificación**.
  - Servicio de apoyo a incidentes graves.
  - En colaboración con CCN para la definición e implantación del servicio de SOC.
  - Colaboración con el Grupo de Trabajo de Seguridad de CRUE-TIC
  - Integración en la Red Nacional de SOC

SECURE REDIRIS BACKBONE

Servicio de mitigación de ataques DDoS

Previene y mitiga los ataques de denegación de servicio (DDOS) que puedan recibir las instituciones por los enlaces de conexión a RedIRIS. Este servicio esta monitorizado en modo 24x7 y se aplica a todas las instituciones que además pueden aportar información adicional para optimizar la respuesta que se debe dar a determinados ataques.

Contacto: egida (at) rediris.es

SECURE REDIRIS BACKBONE

Servicio de mitigación de ataques DDoS

Previene y mitiga los ataques de denegación de servicio (DDOS) que puedan recibir las instituciones por los enlaces de conexión a RedIRIS. Este servicio esta monitorizado en modo 24x7 y se aplica a todas las instituciones que además pueden aportar información adicional para optimizar la respuesta que se debe dar a determinados ataques.

- 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.

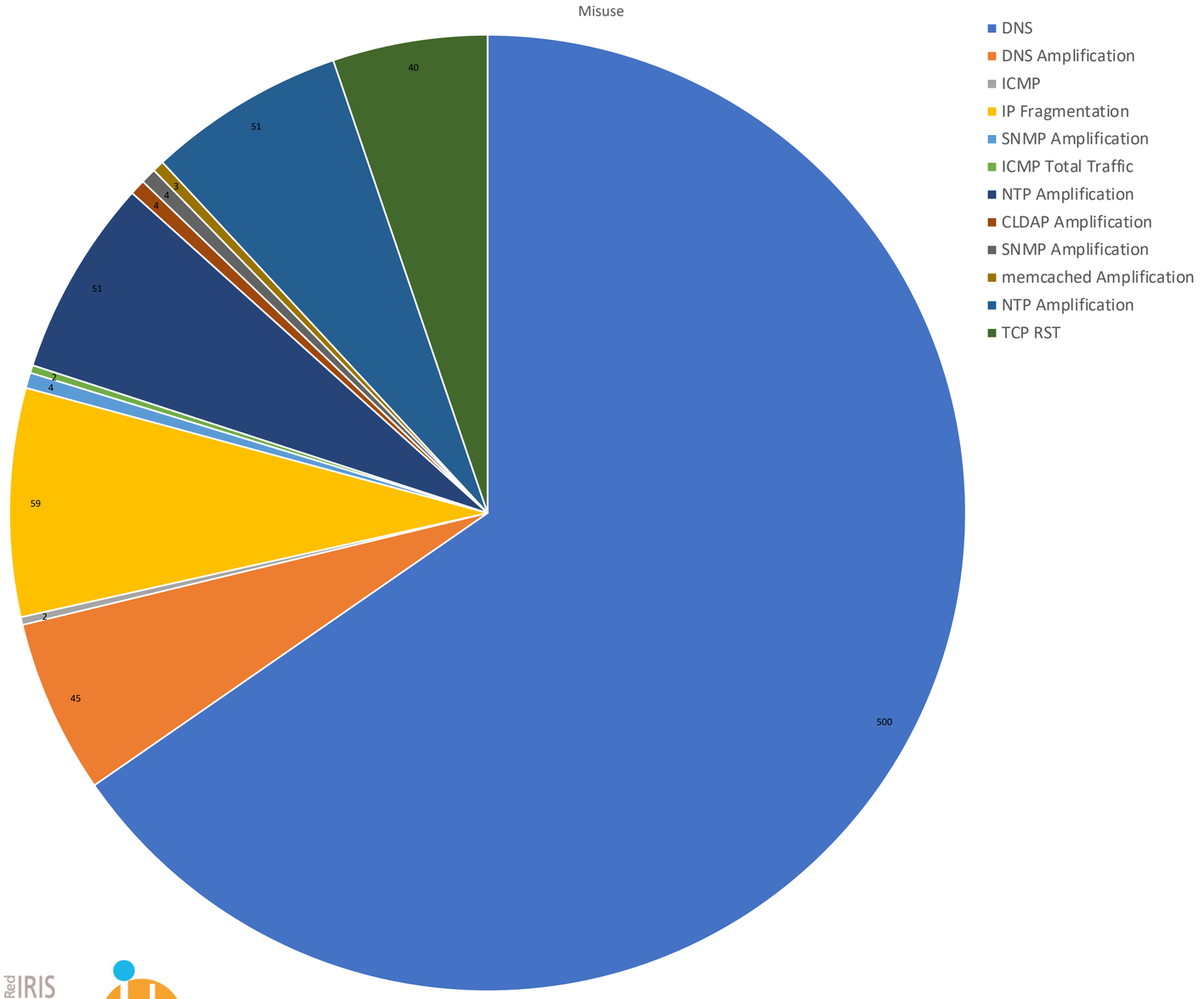
- Protección avanzada
  - Mitigaciones a medida en base a la definición de servicios y equipos
  - Mitigación inmediata de ataques incluyendo la opción de mitigación permanente.
  - Procedimiento de escalado telefónica y por email por institución.
  - Posibilidad de contactar con el SOC por teléfono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

SECURE REDIRIS BACKBONE

Ataques más comunes.

- Amplificaciónes UDP
  - Corta duración.
- Saturación de conexión
  - 2-4 horas

Poca duración de las campañas.



SECURE REDIRIS BACKBONE

Servicio de visibilidad

Proporciona alertas de seguridad relativas al tráfico de las instituciones que circula por el troncal de RedIRIS. El servicio presenta la información que se recoge en los enlaces troncales de RedIRIS de cada institución y permite detectar ataques que se produzcan desde el exterior a las instituciones

Contacto: (próximamente)

SECURE REDIRIS BACKBONE

Servicio de visibilidad

Proporciona alertas de seguridad relativas al tráfico de las instituciones que circula por el troncal de RedIRIS. El servicio presenta la información que se recoge en los enlaces troncales de RedIRIS de cada institución y permite detectar ataques que se produzcan desde el exterior a las instituciones

- Continuidad del servicio de visibilidad.
  - RedIRIS ha adquirido una nueva herramienta de visibilidad. La herramienta es Viewtinet. (https://viewtinet.com/)
  - Trabajando en el despliegue de la herramienta de visibilidad.
  - Capacidad de visibilidad del tráfico, detección y notificación
  - Acceso a todas las instituciones a través de Federación de identidad.
  - Capacidad de búsqueda y filtros avanzados, incluyendo funcionalidades de personalización.
  - Generación avanzada de informes.

- Detección de Ataques
  - Vanilla, Syn ScanXMAs & FIN Scan, FTP Bounce Scan, Sweep Scan
  - DDoS como por ejemplo SYNC floading
  - Anomalías de tráfico.

Type	Description
ack	TCP ack without data flood
ack-data	TCP ack with data anomaly
fin	TCP fin anomaly
frag	Fragmented Packet anomaly
icmp	ICMP flood
ping	Ping (ICMP echo request) anomaly
pong	Pong (ICMP echo reply) anomaly
rst	TCP rst anomaly
syn	TCP syn flood
udp	Outgoing UDP flood

SECURE REDIRIS BACKBONE

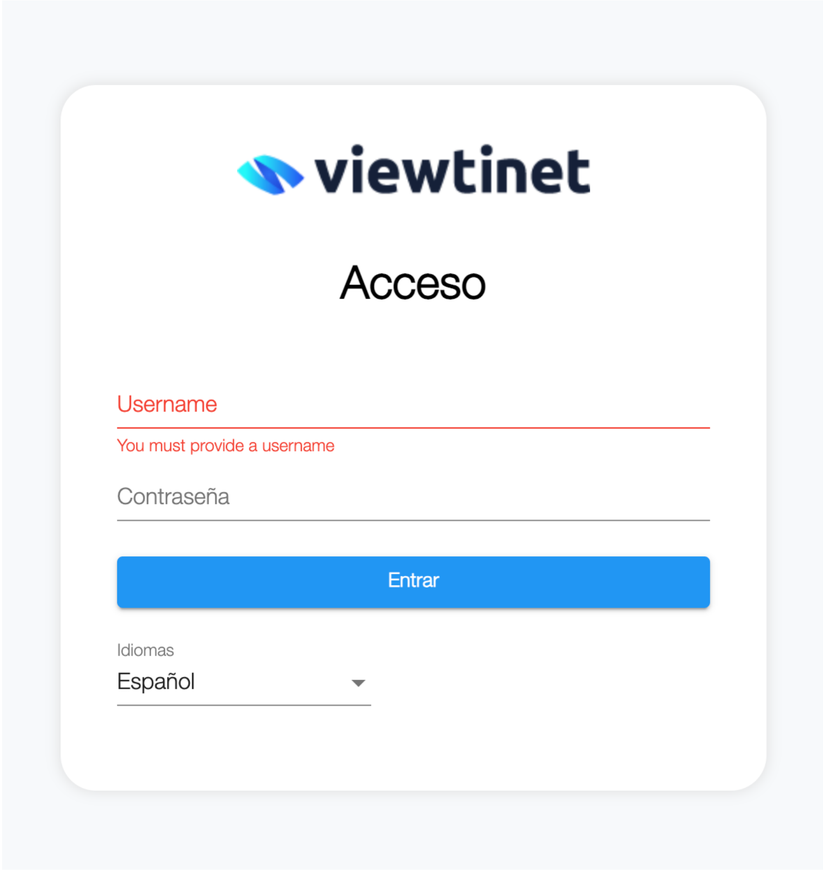
Servicio de visibilidad

Proporciona alertas de seguridad relativas al tráfico de las instituciones que circula por el troncal de RedIRIS. El servicio presenta la información que se recoge en los enlaces troncales de RedIRIS de cada institución y permite detectar ataques que se produzcan desde el exterior a las instituciones

Visibilidad en base al trafico Netflow del troncal

Diversos paneles de visualización configurables por los usuarios

Posibilidad de visualización en monitores externos



GOBIERNO DE ESPAÑA
MINISTERIO DE CIENCIA E INNOVACIÓN
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
RedIRIS red.es
Infraestructuras Científicas y Técnicas Singulares

COLABORACIÓN

Servicio de sincronización horaria

El servicio de sincronización horaria se ofrece a todas las instituciones afiliadas a RedIRIS y consiste en ofrecer un servicio de tiempo de calidad que permitan a las instituciones y usuarios de RedIRIS sincronizar sus dispositivos.

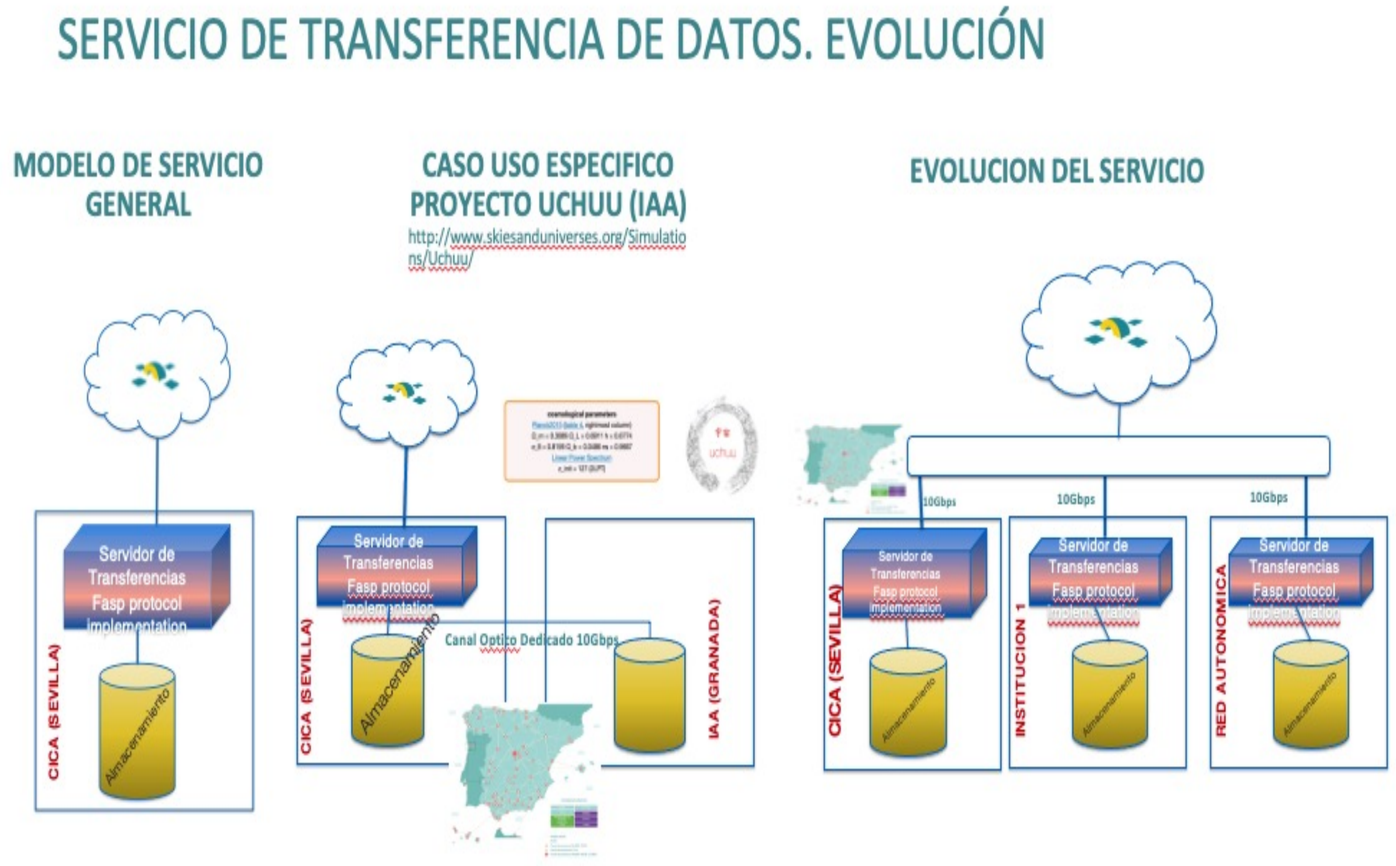
- Mejora del servicio.
- Desplegado la nueva plataforma y en fase de configuración.
- El nuevo servicio ofrecerá:
  - Servicio básico NTP/NTS
  - Servicio de NTP autenticado.
- Coordinación con las instituciones para hacer un listado de servidores de tiempo.
  - Filtrado el protocolo NTP en RedIRIS excepto para los servidores de tiempo registrados.

COLABORACIÓN

Servicio de transferencia de volúmenes de datos

El Servicio de transferencia de volúmenes de datos científicos tiene por objeto mejorar la capacidad de transferencia de los investigadores de las instituciones afiliadas a RedIRIS. Este servicio se ofrece de forma gratuíta a científicos que necesitan transferir grandes volúmenes de datos.

- Mejora del servicio:
  - Aumento de la capacidad de transferencia, que actualmente se situa en 10Gbps.
  - Mejora del backend de almacemiento añadiendo disco SSD a la plataforma de almacenamiento.
  - Mejora del servicio mediante la contratación de servicios de apoyo a la prestación del servicio.



Proceso de adecuación a la ISO27001 y ENS.

- Servicio de conectividad IP y Óptico
- Objetivo de certificación para el área de conectividad a Noviembre de 2023 en ISO27001
- Objetivo de certificación en ENS nivel bajo en Octubre de 2023
- Se irá extendiendo al resto de servicio de RedIRIS

MUCHAS GRACIAS