crue Universidades Españolas

Digitalización

Ciberseguridad y realidad actual en universidades

Francisco José Sampalo Lainz

Coordinador del GT de Seguridad y Auditorías de

la Sectorial Digitalización de Crue Universidades Españolas

Responsable de Seguridad de la Universidad Politécnica de Cartagena

Universidad Politécnica de Cartagena

MIEMBRO DE EUT+ EUROPEAN UNIVERSITY OF TECHNOLOGY

La voz de las universidades españolas

crue Universidades Españolas

¿Qué es Crue Universidades Españolas?

- Crue Universidades Españolas, constituida en el año 1994, es una asociación sin ánimo de lucro formada por un total de **76 universidades españolas**: 50 públicas y 26 privadas.
- Crue Universidades Españolas es el principal interlocutor de las universidades con el gobierno central y desempeña un papel clave en todos los desarrollos normativos que afectan a la educación superior de nuestro país.
- Promueve iniciativas de distinta índole con el fin de fomentar las relaciones con el tejido productivo y social, las relaciones institucionales, tanto nacionales como internacionales, y trabaja para poner en valor a la Universidad española.

Crue Digitalización. Comisión Sectorial de Tecnologías de la Información y las Comunicaciones

Crue – TIC nace en el año 2007

- **Asesorar y proponer** a Crue Universidades Españolas cuantos temas se consideren oportunos en el ámbito de las tecnologías de la información y las comunicaciones para mejorar la calidad, la eficacia y la eficiencia de las universidades españolas.
- **Estudiar las necesidades y aplicaciones de estas tecnologías** en la gestión, la docencia y la investigación, proponiendo actuaciones y proyectos conjuntos.
- **Fomentar, promover y liderar** la cooperación entre las universidades.

Pinceladas sobre ciberseguridad y universidades

Nuestro entorno: factores de riesgo y posibles vulnerabilidades

- Las universidades son organizaciones muy enfocadas a las operativas abiertas y colaborativas ("Open Science" o "Ciencia abierta").
- Entornos descentralizados en su gestión y con una gran superficie de exposición:
  - Servidores departamentales
  - Proyectos de investigación
  - BYOD y redes wifi
  - Diferentes tipologías de usuarios.
- Infraestructuras potentes y conectividad de banda ancha.
- Gestión de la continuidad: Análisis de impacto, planes de recuperación y cibercrisis.
- Poco personal dedicado en exclusiva a la ciberseguridad.
- Bajo nivel de certificación en el ENS: 7 universidades certificadas (nivel MEDIO)

Nuestro entorno: factores de riesgo y posibles vulnerabilidades

A modo de ejemplo se han detectado en algunas de nuestras universidades las siguientes circunstancias que pudieran ser explotadas por los atacantes si no se aplican políticas y filtros que eviten estas prácticas:

- Hay universidades en las que la configuración software de los puestos de trabajo y servidores no está estandarizada y la responsabilidad sobre el bastionado recae sobre el propio usuario.
- En las redes universitarias se instalan equipos y servicios accesibles desde Internet sin la supervisión o conocimiento de los Servicios Informáticos.
- La introducción de dispositivos conectados (Arduino, Raspberry, dispositivos de control industrial y en general dispositivos IoT), cuyas actualizaciones de sistema operativo y parches no se aplican.
- Uso de direccionamiento IP público en la conexión de los puestos de trabajo de los usuarios (PDI, PAS, Aulas)

Colaboración y ciberseguridad en las universidades

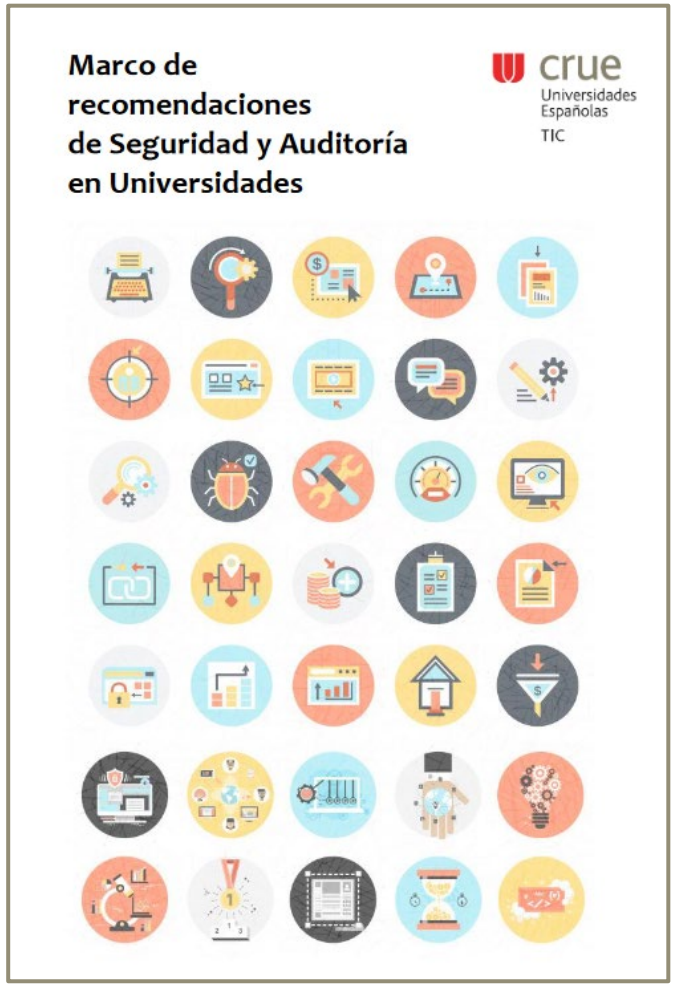
Grupo de trabajo de Seguridad y Auditoría TI de CRUE-Digitalización

- Nuestro objetivo es **coordinar y promover acciones y buenas prácticas para el gobierno y la gestión de la Seguridad de la Información en las universidades españolas**, así como desarrollar recomendaciones y guías para el cumplimiento normativo, especialmente en el ámbito del ENS.
- También actuamos como **interlocutores del conjunto de universidades** con otras entidades con competencias en ciberseguridad: GT Seguridad de la CSAE, CCN-CERT, Foro Nacional de Ciberseguridad, INCIBE, RedIRIS.
- El grupo está compuesto por personal de las universidades con responsabilidades de seguridad de la información (de gestión y/o técnicas) en las universidades (públicas y privadas).
- **NO SOMOS UN SOC**.
- Uno de nuestros pilares básicos es el trabajo colaborativo: reuniones mensuales, documentación compartida, canal de chat, webinars.
- **Actualmente somos 96 personas de 54 universidades.**

Guías y publicaciones

https://tic.crue.org/publicaciones/

2018



2020

Guías y publicaciones

universitic 2022

Aumenta la preocupación por la ciberseguridad y por la continuidad de los servicios

- 3 de cada 4 equipos de gobierno ya han aprobado una **Política de Seguridad** de la Información (se ha incrementado un 20% desde 2020)
- 3 de cada 4 equipos de gobierno han nombrado a un **responsable de seguridad**, diferente y no dependiente del responsable de sistemas, sobre el que va a recaer la responsabilidad de implementar el nuevo modelo de tratamiento de la seguridad
- El 60% de los equipos de gobierno **conoce los riesgos y decide sobre el nivel aceptable** para su institución (16% más que en 2020) y solo 1 de cada 3 ha aprobado un **Plan Integral de Seguridad** de la Información

= plan de seguridad integral

▲ 17% auditoría de seguridad

10%	11%	se ha realizado una auditoría externa y se ha obtenido la certificación
22%	20%	se ha realizado una auditoría externa pero aún no se ha obtenido la certificación
45%	35%	se ha realizado una auditoría interna
22%	35%	no hemos hecho nada al respecto

100%

▲ 15% estrategia de continuidad de servicios críticos

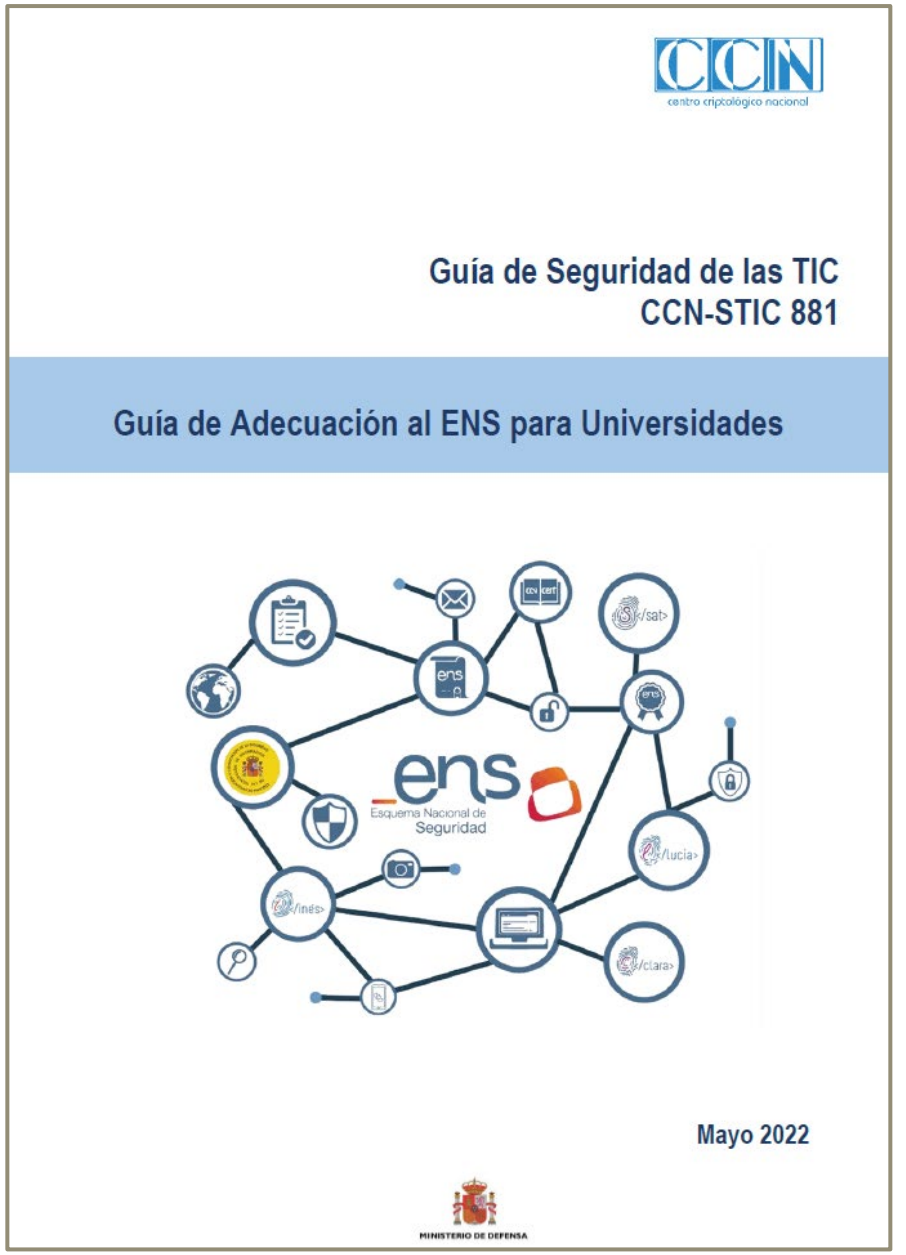
= procedimientos de recuperación de servicios críticos

6%	14%	existen procedimientos para la recuperación de todos los servicios en el mínimo tiempo posible
30%	22%	existen procedimientos para la recuperación de los servicios más críticos
57%	48%	pero hay protocolos de recuperación de los servicios más críticos
7%	16%	no existen procedimientos

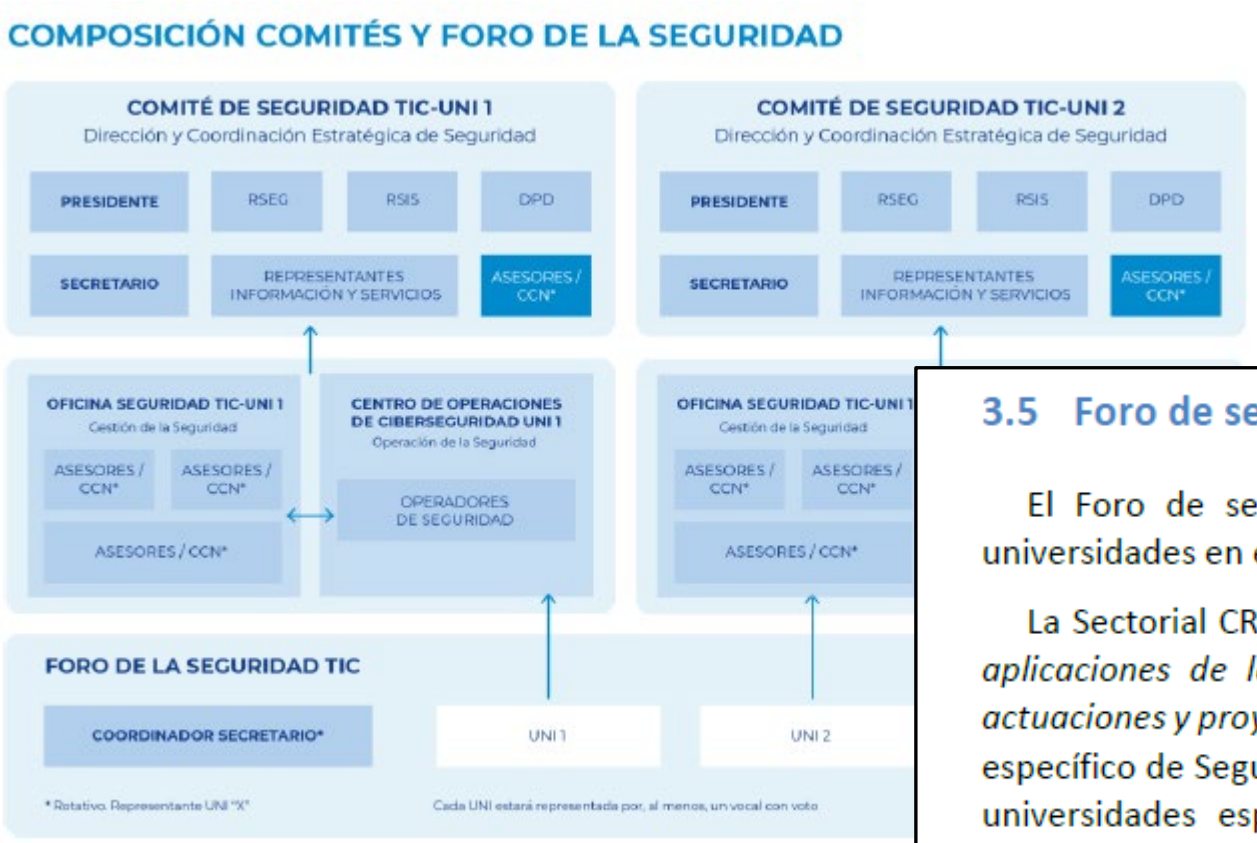
100%

Guías y publicaciones

Guía CCN-STIC 881: Perfil de cumplimiento y Guía de adecuación al ENS para universidades.



Guías y publicaciones



3.5 Foro de seguridad TIC de las Universidades

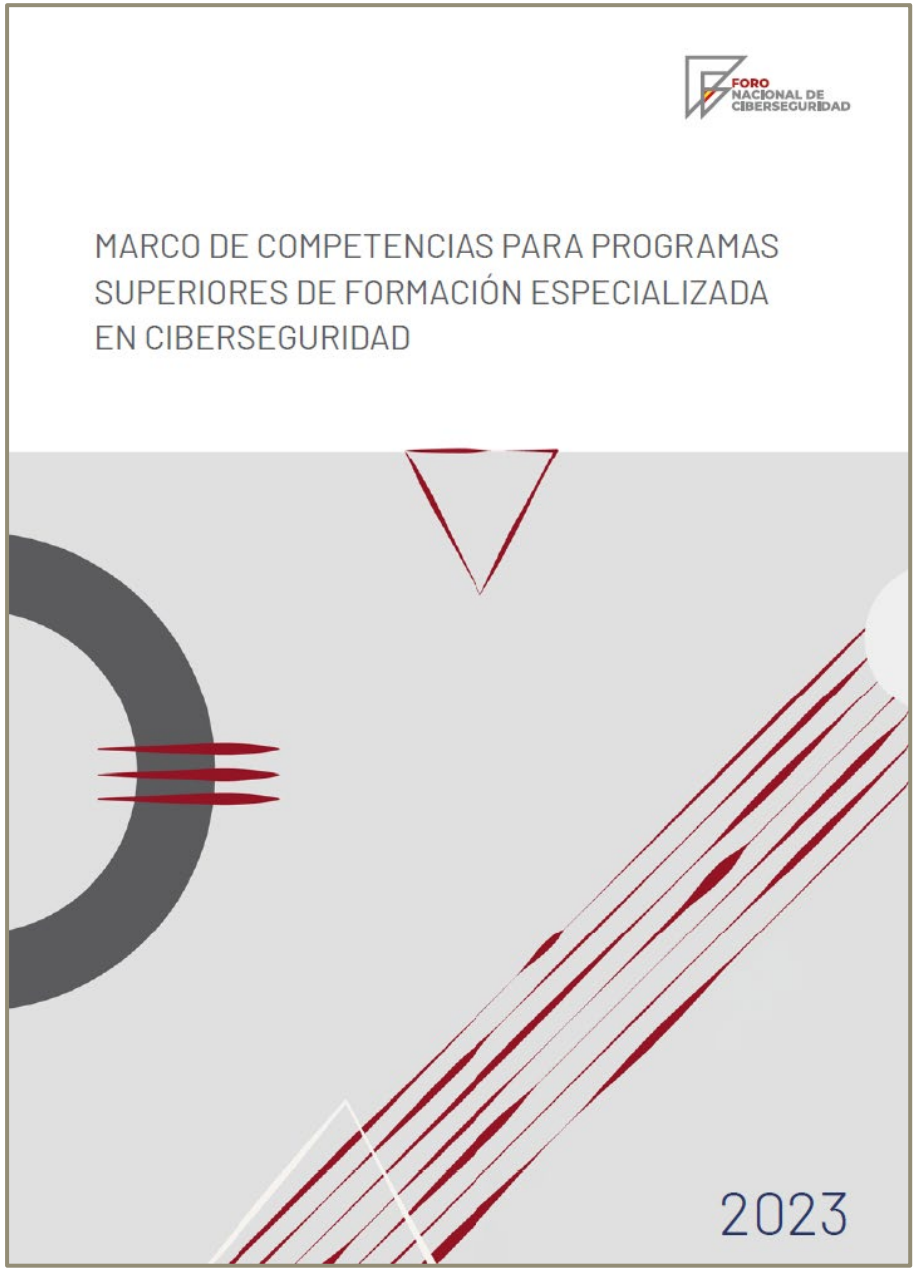
El Foro de seguridad TIC, se constituye como un punto de encuentro de las universidades en el ámbito del Esquema Nacional de la Seguridad.

La Sectorial CRUE-TIC6, entre cuyas misiones está la de "*Estudiar las necesidades y aplicaciones de las TIC en la gestión, la docencia y la investigación, proponiendo actuaciones y proyectos conjuntos a las Universidades*", dispone de un Grupo de Trabajo específico de Seguridad y Auditoría TI. En dicha Sectorial están representadas todas las universidades españolas, tanto públicas como privadas. Dicho Grupo de Trabajo constituye el marco ideal para ser el Foro de Seguridad TIC para universidades. Debido al carácter sectorial de mundo universitario, será de gran ayuda en el ámbito de la Gobernanza en ciberseguridad.

Guías y publicaciones (Foro Nacional de Seguridad)

Documento que tiene como objeto definir un marco de competencias que sirva como referencia para el diseño de programas superiores de formación especializada en ciberseguridad en España.

1. Análisis de los marcos de competencias en ciberseguridad en el ámbito internacional
2. Estudio de la implantación del marco curricular de referencia (ACM/IEEE) en España
3. Propuesta de marco de competencias y caso práctico de uso



Coordinación con otros organismos

CCN-CERT centro criptológico nacional

20 ANIVERSARIO Centro Criptológico Nacional

El CCN-CERT proporciona a las universidades (públicas) las herramientas y servicios para prevención, detección y recuperación.

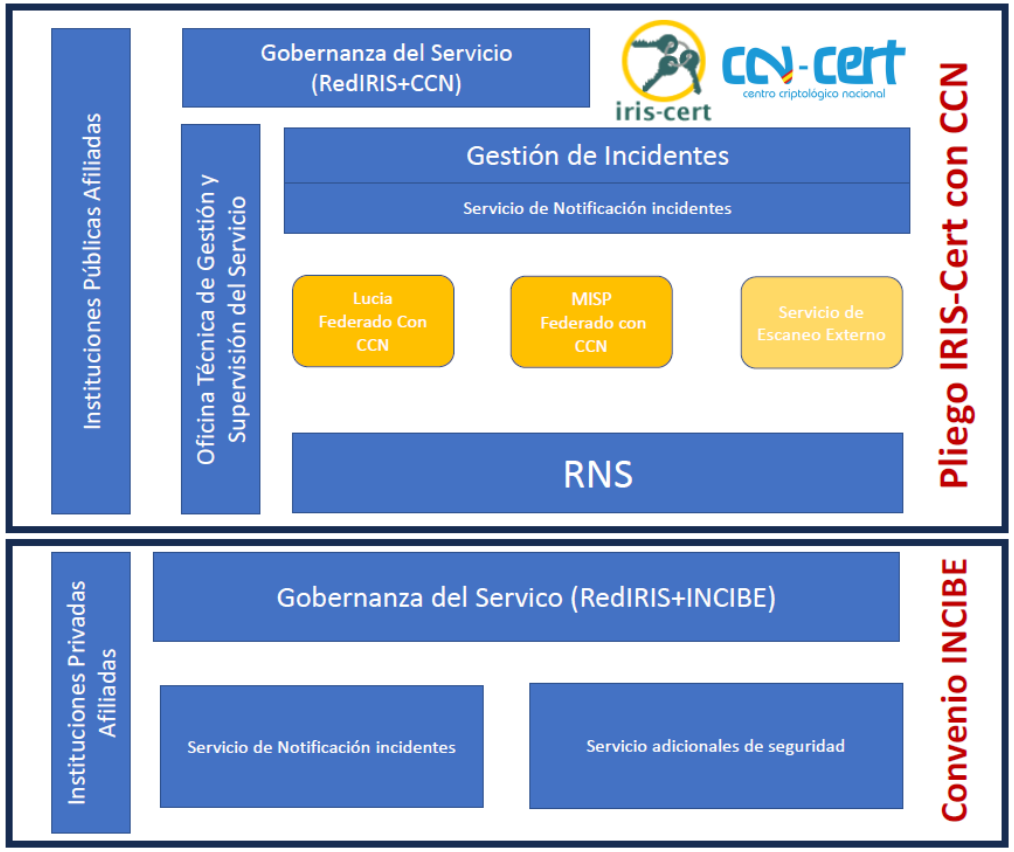
Cursos específicos para el entorno universitario.

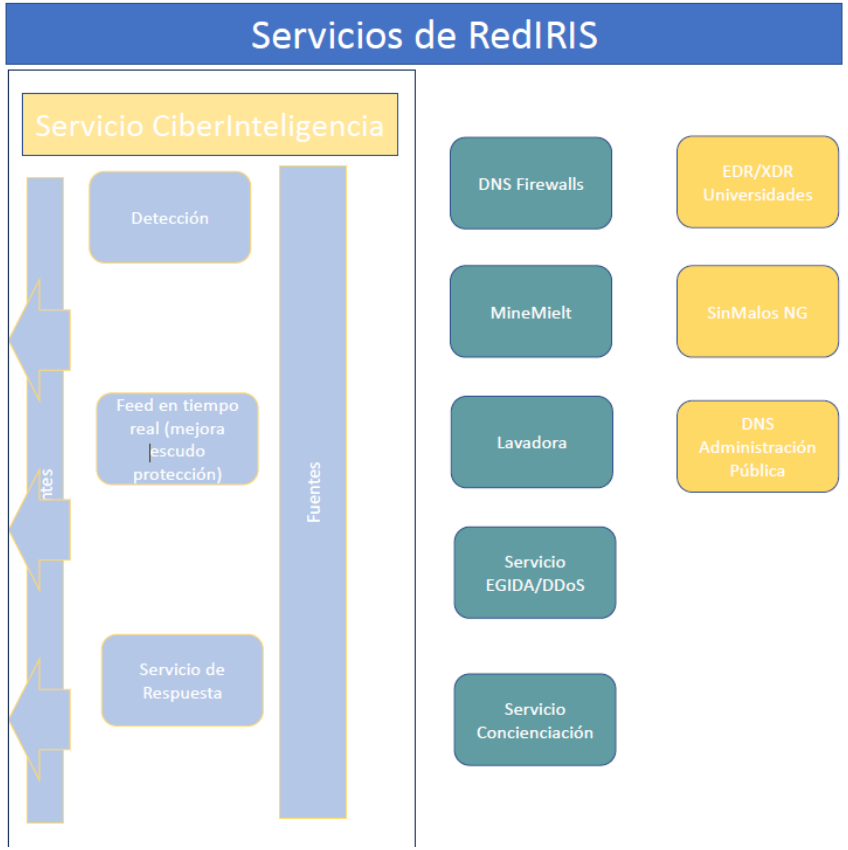
Reporte de incidentes

25 universidades federadas, reportando a LUCIA

RedIRIS

Servicios de Seguridad de RedIRIS





RedIRIS

- LAVADORA: seguridad y filtrado en el correo electrónico.
- EGIDA: Mitigación de ataques DDoS
- DNS-Firewall.
- IRIS-CERT: Notificación de incidentes de ciberseguridad.
- SinMalos: ciberinteligencia compartida entre universidades y organismos de investigación.
- EDR/XDR compartido y soporte a resolución de incidentes graves.

https://www.rediris.es/servicios/seguridad/

Gracias por su atención

Francisco José Sampalo Lainz
Coordinador del GT de Seguridad y Auditorías de la Sectorial Digitalización de Crue Universidades Españolas