REDIRIS · ÁREA DE SISTEMAS Y SEGURIDAD

Actualidad de los servicios

Antonio Fuentes Bermejo Subdirector de Sistemas y Seguridad · RedIRIS

Jt 2026 RedIRIS
A CORUÑA 22-25 JUNIO Universidade da Coruña

AGENDA

Qué vamos a ver

IRISCERT
01

Integración, CERT+SOC y actividad

Detección proactiva
02

HORIZON · FortiRecon

Servicios de correo
03

Lavadora · DMARC con el CCN · SinMalos

Refuerzo a instituciones
04

ICTS y proyecto UniDigital

Cumplimiento y plan
05

ENS/ISO · SLAs · Plan de ciberseguridad

Foro de Ciberseguridad
06

Murcia 2025 y Zamora 2026

IRISCERT

IRIS-CERT coordina y opera los servicios de ciberseguridad de RedIRIS para todas las instituciones. Es a la vez CERT y SOC.

- **Con SOC propio** IRIS-CERT amplifica sus capacidades
- **Sin SOC** IRIS-CERT cubre la capa común
- **Con SOC compartido** IRIS-CERT aporta la coordinación

Recepción de incidentes

Recibe y procesa informes de posibles incidentes remitidos por agentes externos y por los servicios que RedIRIS presta a las instituciones.

IRISCERT

CERT + SOC DE LA COMUNIDAD

AUTOSERVICIO E INTEGRACIÓN

Conecta tu SOC/Institución con IRIS-CERT

SOC de la institución
Sistema de tickets / SOC propio

API / SSO

IRIS-CERT
MISP + LUCIA + HORIZON

API MISP

Inteligencia de amenazas: IoCs y eventos en tus herramientas.
misp.iriscert.es

API LUCIA

Gestión de incidentes integrada en tus flujos de trabajo.
lucia.iriscert.es

API HORIZON

Alta progresiva, iniciada por IRIS-CERT, para todas las afiliadas.
horizon.iriscert.es

IRISCERT

El año de IRISCERT en cifras

La actividad del CERT y SOC de la comunidad, de un vistazo.

300

instituciones bajo cobertura

22

Incidentes gestionados (sistemas internos)

1.573

Incidentes gestionados (sistemas externos)

10.659

Eventos publicados en MISP

3,33 M

IOCs compartidos (3.332.636)

100 %

Tickets resueltos (de 2.556)

Reforzamos la detección proactiva

Sobre los servicios que ya teníamos, este año reforzamos la detección proactiva de IRIS-CERT: ver antes, y desde fuera, lo que un atacante vería.

HORIZON

Gestión de la superficie de exposición externa (ASM): activos, puertos, vulnerabilidades y dominios suplantadores de las instituciones.

FortiRecon (Fortinet)

Protección de riesgo digital y vigilancia en deep & dark web: credenciales filtradas, suplantación de marca y exposición de datos.

Detección temprana: actuar sobre la exposición y las filtraciones antes de que se conviertan en incidente.

Cobertura y superficie expuesta

203
organismos monitorizados

1.076 M
direcciones IP vigiladas

221.328 M
puertos analizados a diario

SUPERFICIE EXPUESTA

33.725
puertos abiertos

1.022
servicios identificados

16.723
recursos web

8.655
tecnologías detectadas

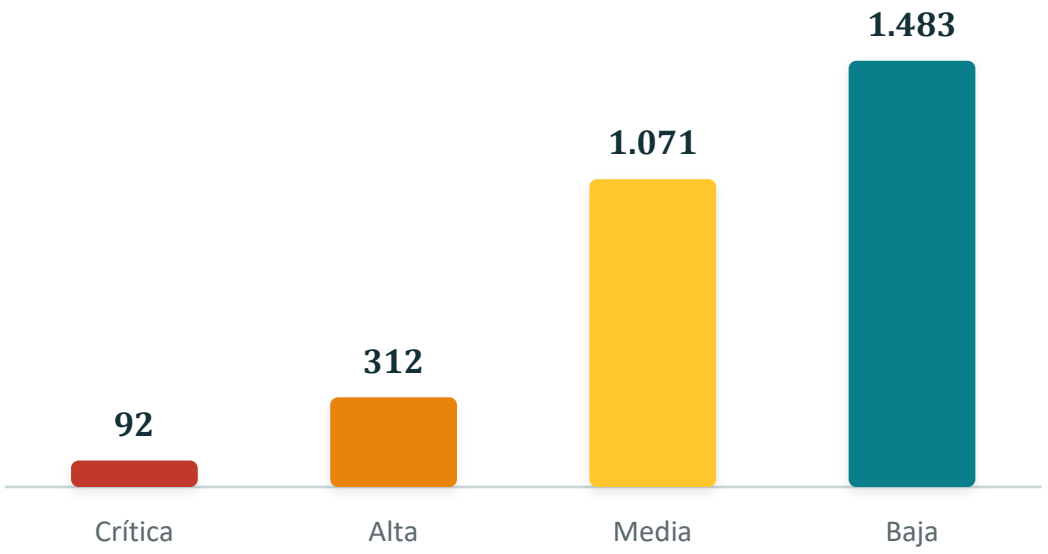
1.833
hosts SSH auditados

1.746
fugas de metadatos

Hallazgos por severidad

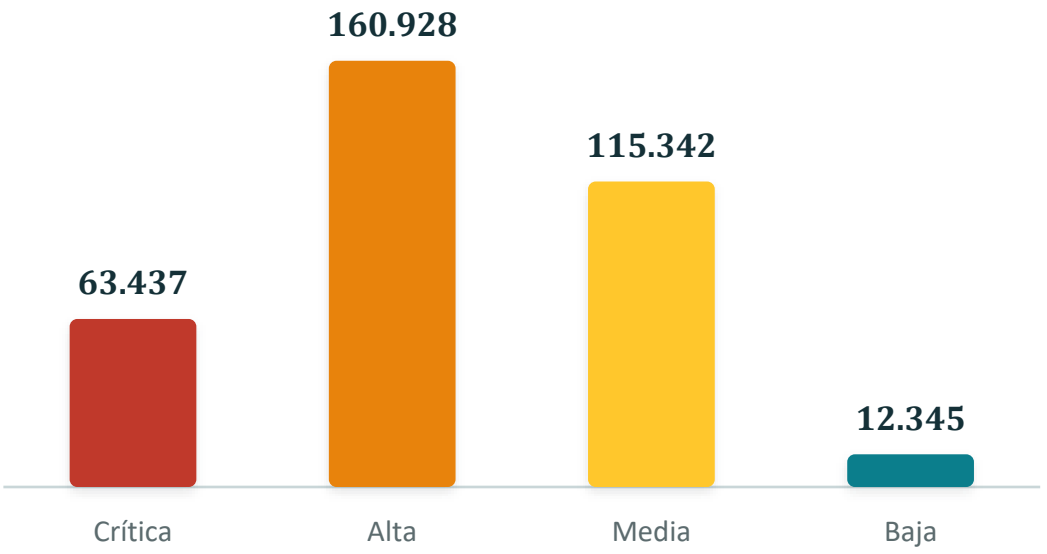
Vulnerabilidades detectadas en el parque, clasificadas por nivel de severidad.

Vulnerabilidades web



1.475 accionables (crítica + alta + media) · 6.052 informativas · 10.524 en total

CVE detectados



352.052 CVE detectados en total

DETECCIÓN PROACTIVA · FORTIRECON

Riesgo digital más allá del perímetro

FortiRecon (Fortinet) es el servicio de Digital Risk Protection que complementa a HORIZON: aporta inteligencia de adversarios y vigilancia en la deep & dark web — la vista de lo que el atacante ve, planea y comparte.

EASM

Superficie externa

Vista «outside-in» de activos expuestos: dominios, subdominios e IPs, vulnerabilidades explotables, certificados SSL, puertos, credenciales filtradas y errores de configuración en la nube.

BRAND PROTECTION

Marca y suplantación

Typosquatting, phishing (marca de agua digital), suplantación de marca y logos, apps móviles fraudulentas y perfiles falsos en redes — con servicio de takedown.

ACI

Inteligencia de adversarios

Deep & dark web curada por FortiGuard Labs: ransomware, credenciales y datos filtrados, vulnerabilidades explotadas in-the-wild y riesgo de proveedores y cadena de suministro.

SINMALOS · SERVICIO · NIS2

Inteligencia de amenazas compartida

Plataforma para compartir inteligencia de amenazas entre instituciones, con procesamiento previo a su publicación y un oráculo de malware que analiza ficheros por correo.

Plataforma de inteligencia compartida

- Comparte inteligencia entre instituciones
- Procesamiento previo a su publicación
- Detección y reporte de actividad maliciosa
- Soporte por correo electrónico y tickets

Oráculo de Malware

Análisis de archivos sospechosos a través de email.

89
emails procesados

17
instituciones atendidas

14
instituciones productoras · SinMalos 1.0

7
instituciones productoras · SinMalos 2.0

106
instituciones consumidoras

SINMALOS · FEEDS

Catálogo de listas e indicadores

Feeds activos por origen, con su volumen aproximado de indicadores.

CCN-CERT

FUENTES EXTERNAS

REYES-Inbound
~1K indicadores

REYES-Outbound
~2K indicadores

ELSA-Inbound
200 indicadores

SinMalos 1.0

LISTAS PROPIAS

SM-MultiSource-HC
~20–30K indicadores

SM-Lite-HC
~5–10K indicadores

SinMalos 2.0

NUEVAS LISTAS

SM-Scanners
~5–10K · IPs de escaneos

SM-Threats
~5–10K · IPs de ataques

Evolución y próximos pasos

26/01/26 — Apagado de Minemeld. **95 % de los consumidores migrados a XSOAR.**

Estado del servicio

- Optimización del procesado de indicadores
- Filtrado y exclusión de redes públicas en las listas
- Mejoras en monitorización y alertas de estado
- +500 tickets de soporte gestionados

Próximos pasos

- Publicación de nuevos feeds
- Mejoras en el oráculo de malware
- Automatización de la clasificación de alertas y reportes
- Nuevas instituciones consumidoras y productoras

De 531 millones, solo 135 llegan al buzón

La gran mayoría del tráfico de correo se descarta antes de llegar al buzón del usuario.

530,9 M correos recibidos

395,9 M descartados por la plataforma

135,0 M entregados al usuario

74,6 %

de los correos entrantes se clasifican como «no deseados»

De los descartados, 8,2 M *los detectaron los filtros avanzados de Proofpoint · primer trimestre de 2026.*

Amenazas avanzadas en el correo

Amenazas detectadas por los filtros avanzados (Proofpoint) en el primer trimestre de 2026.

5,5 M

malware avanzado

2,6 M

phishing dirigido

151 K

BEC · fraude del CEO

URL Defense

3.485 clicks reescritos analizados: 2.231 bloqueados (64 %) y 1.254 permitidos.

Malware principal

404 Keylogger, GuLoader y Tsundere Bot entre las familias más detectadas.

Técnicas de evasión

Geofencing, headers fencing y 404 TDS para esquivar el análisis.

EN COORDINACIÓN CON EL CCN-CERT

DMARC: blindaje del correo de la comunidad

EN MARCHA · 2026

Junto con el CCN, vamos a implantar DMARC en los dominios de la comunidad, acompañando a cada organización hasta la política estricta (p=reject). Tutorización, soporte de especialistas y panel de monitorización. Sin coste para la institución.

Bloqueo del fraude

Correos fraudulentos en nombre de la institución, bloqueados.

Anti-spoofing

Elimina el riesgo de suplantación y phishing sobre el dominio.

Cumplimiento

Alineado con el ENS y los estándares de la UE.

Entregabilidad

Mejora la reputación: los correos críticos llegan al buzón.

El 99 % de la suplantación, eliminada — sin afectar al correo legítimo. Una vez configurado, vale para siempre.

INFRAESTRUCTURA DE SISTEMAS

Datacenter en alta disponibilidad

Pliego en ejecución para reforzar la infraestructura de sistemas de RedIRIS y dotar al centro de datos de alta disponibilidad.

Alta disponibilidad

Configuración activo-activo con failover automático y sin punto único de fallo, para garantizar la continuidad del servicio.

Recuperación ante desastres

Plan de continuidad con objetivos de RTO/RPO definidos, replicación de datos y copias, con pruebas de recuperación periódicas.

Ampliación de capacidad

Ampliación de servidores, almacenamiento absorber el crecimiento de los servicios de la comunidad.

Refuerza la continuidad y la disponibilidad de los servicios, en línea con las exigencias del ENS.

CALIDAD Y CUMPLIMIENTO

ENS Medio e ISO 27001 en los servicios

Llevamos los servicios del área a un marco común de seguridad gestionada y certificada.

ISO/IEC 27001

Certificado · AENOR, nov-2024

Conectividad, Mitigación DDoS, identidad (IdPnube).

ENS nivel MEDIO

Certificado

Sistema de información de todos los servicios de RedIRIS

Adecuación → **Implantación** → **Auditoría** → **Certificación ENS Medio**

REFUERZO A INSTITUCIONES

Acompañamiento a ICTS y UniDigital

Refuerzo a las ICTS

Acompañamos a las Infraestructuras Científico-Técnicas Singulares en su ciberseguridad y en el cumplimiento del ENS, con apoyo del equipo de IRISCERT.

Proyecto UniDigital

Refuerzo de las capacidades de ciberseguridad de las universidades en el marco de UniDigital.

Acercar capacidades de ciberseguridad a las instituciones.

COMUNIDAD

Foro de Ciberseguridad de RedIRIS

fcs 2026 RedIRIS

PRÓXIMA EDICIÓN

XV Foro · Zamora 2026

Campus Viriato · Universidad de Salamanca

26–29 de octubre de 2026

jt 2026 RedIRIS

A CORUÑA
22-25 JUNIO Universidade da Coruña

red.es | RedIRIS | IGTS | UNIVERSIDADE DA CORUÑA

HOJA DE RUTA 2026

Próximos pasos

Apoyo a las ICTSs

Acompañamiento en ciberseguridad y cumplimiento ENS a las infraestructuras singulares (ICTS) y servicios SOC

Mejora de los servicios

Evolución continua de los servicios según las necesidades de la comunidad.

Consolidar el cumplimiento

CENS Medio e ISO 27001 en los servicios

Ampliar la detección proactive y ciberinteligencia

Más cobertura con HORIZON y FortiRecon e implantación de DMARC con el CCN.

Resiliencia de la infraestructura

Alta disponibilidad y continuidad de los servicios.

Automatización e IA

Triaje y enriquecimiento asistido para centrar al equipo en lo que más aporta.

¡Muchas gracias!