



I CyberSecurity Healthcare & Pharma Congress

SAVE THE DATE



23 DE NOVIEMBRE 2023

**Escuela Técnica Superior de
Ingenieros de Telecomunicación**
Universidad Politécnica de Madrid



www.cybermadrid.org



Con el apoyo y participación institucional de



Colaboran





I CyberSecurity Healthcare & Pharma Congress

PATROCINADORES

PLATINUM



GOLD



SILVER



BRONZE



¿Por qué organizar este Congreso?



ELMUNDO España Opinión Economía Internacional Deportes Cultura
España Elecciones Madrid Andalucía Baleares Castilla y León Cataluña

CATALUÑA · 'Dark web'

Nueva filtración de los datos robados en el ciberataque al Hospital Clínic de Barcelona por los piratas informáticos RansomHouse

GERARD MELGAR
Barcelona

Actualizado Martes, 4
julio 2023 - 23:05



Comentar



→ La **ciberseguridad aplicada al sector sanitario** se ha convertido en una cuestión de la **máxima relevancia** como estamos viendo con casos tan recientes como el del Hospital Clínic de Barcelona.

→ Hay una **enorme superficie de exposición y vulnerabilidad** de los **datos y procesos esenciales** gestionados por el sector **Salud (sanitario y farmacéutico)**

→ La **seguridad de los pacientes** es una de las **principales preocupaciones de la comunidad sanitaria**

→ Los **datos** analizados ponen de manifiesto la **necesidad acuciante** de que las **organizaciones sanitarias** apliquen **prácticas de ciberseguridad**



¿Por qué organizar este Congreso?

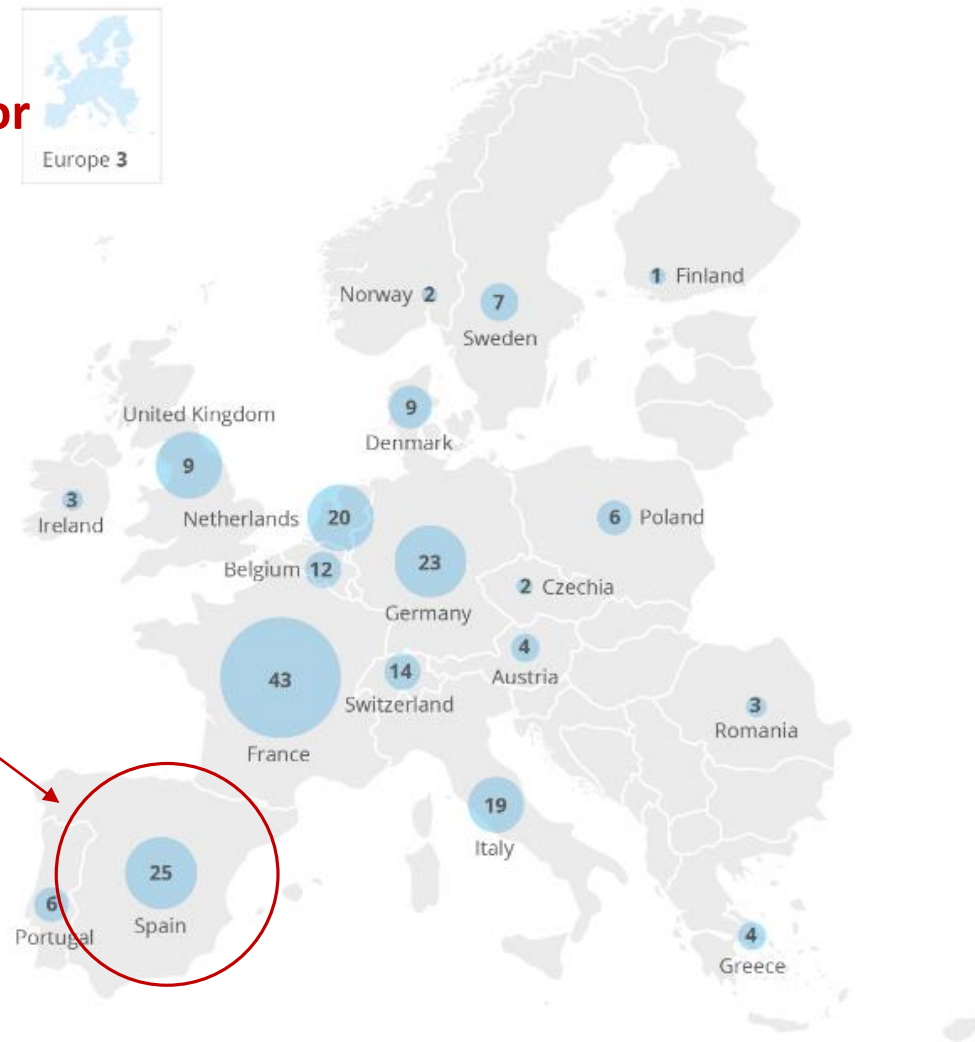
- El proceso de **transformación digital** que está experimentado el sector hace que los **servicios clínicos y hospitalarios dependan fuertemente de las infraestructuras digitales.**
- La **automatización** alcanza a:
 - **servicios de gestión del paciente**
 - **servicios de soporte** (logística, contabilidad y finanzas, compras, etc.)
 - **equipos clínicos y de laboratorio**
- Los **dispositivos médicos conectados** están transformando la forma en que funciona el sector, tanto dentro de los hospitales como entre los diferentes actores de la industria de la salud.
- El **aumento de los flujos de información dentro y fuera de los hospitales y las clínicas** conlleva **riesgos** importantes que necesitan ser abordados.
- Algunos de los riesgos comprenden **daños a la seguridad del paciente o pérdida de información personal**, que puede ser causados por acciones maliciosas, por errores humanos, del sistema o de terceros, y por fenómenos naturales. A medida que la superficie de ataque aumenta con la introducción de nuevos dispositivos conectados, la probabilidad y el posible impacto de los ataques **crece exponencialmente.**



Objetivos del Congreso

- **Impulsar la ciberseguridad** en el sector **salud**, mejorando el posicionamiento y la especialización inteligente de las **empresas**, incentivando la **innovación**, la **formación** y la **concienciación** y la **divulgación**.
- Impulsar el **desarrollo de nuevas soluciones, productos y servicios**, específicamente diseñados para su utilización en el entorno clínico-hospitalario, **aumentando la oferta de soluciones y servicios de las empresas**.
- **Fomentar la participación activa** de nuestras **empresas asociadas** orientando nuestras actividades hacia el **ROI** de las mismas.

Dimensionando la *salud cibernética* del Sector



España ocupa el **2º** puesto en incidentes de ciberseguridad en el sector **Salud** registrados (**25**), después del primer puesto de Francia, con 43 incidentes*.

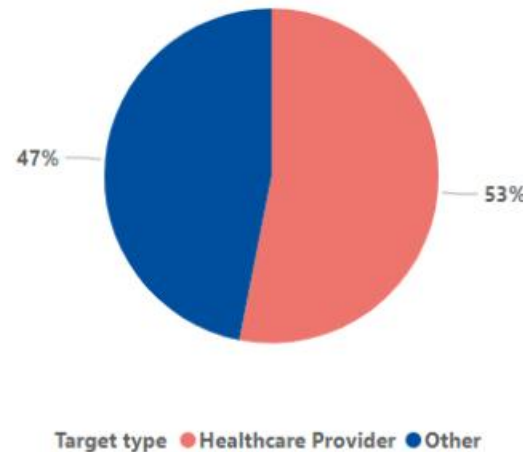
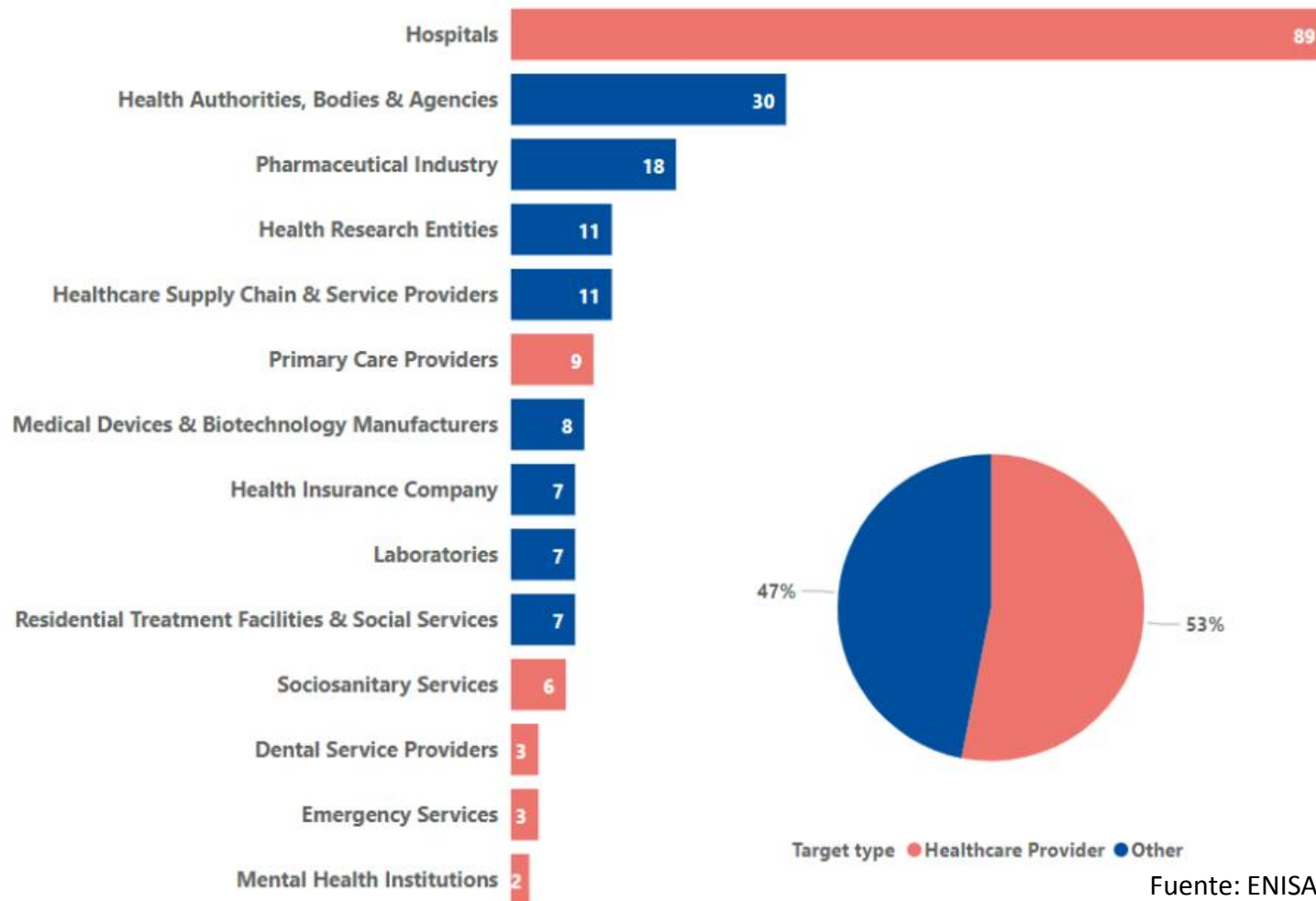
España registra una media de **1.252** incidentes de ciberseguridad a la semana**.

El de **salud**, es el **tercer sector más perseguido por los cibercriminales** en **España**.

*ENISA THREAT LANDSCAPE: HEALTH SECTOR July 2023 (enero 2021- marzo 2023)

** Según el informe global sobre ciberataques de Check Point Research

Dimensionando la *salud cibernética* del Sector



Tipos de organizaciones de salud que fueron objetivo de ataques.

(Enero 2021 – marzo 2023)

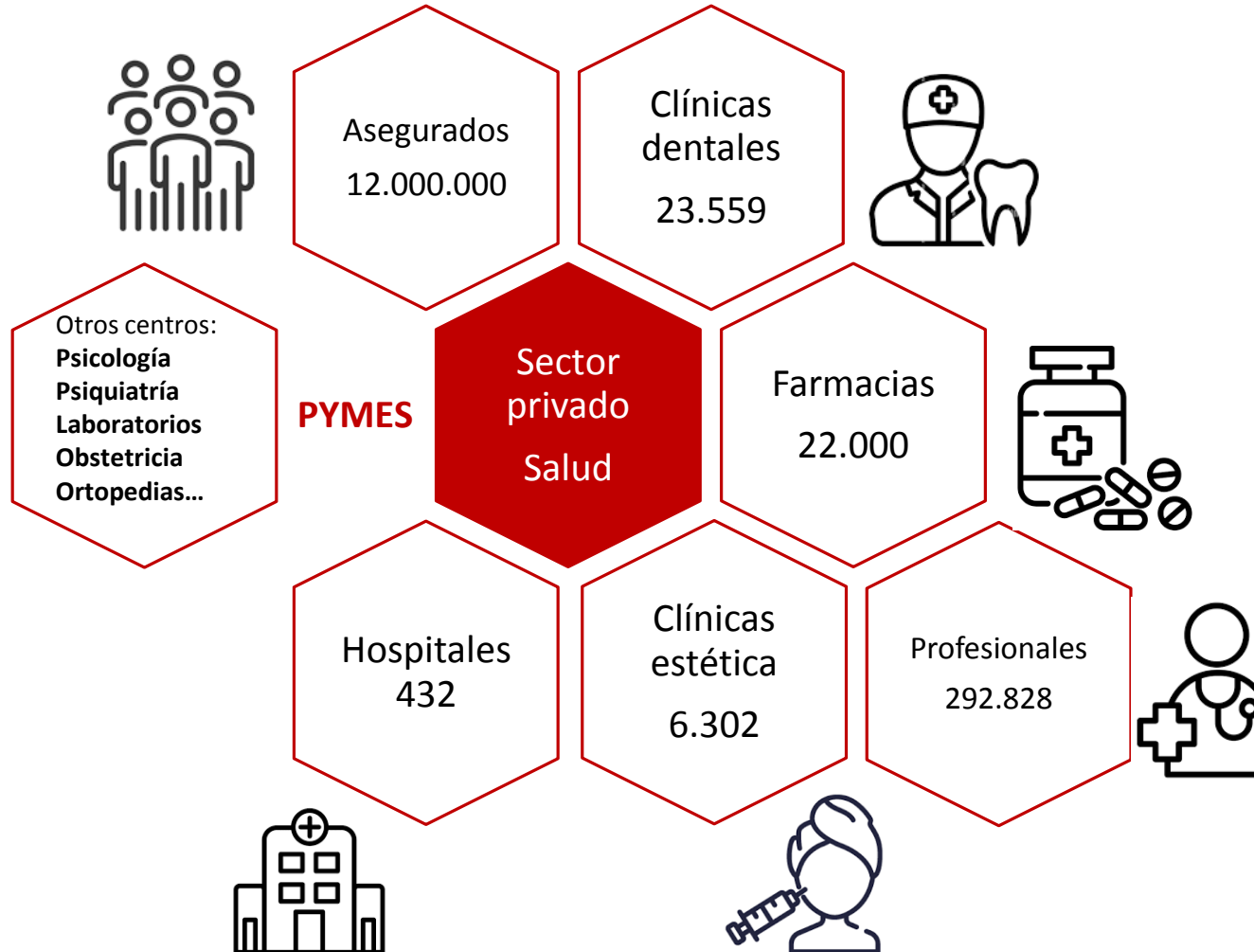
El sector sanitario europeo se enfrentó a un número significativo de incidentes.

- **Proveedores de asistencia sanitaria** de la UE (**53 %** del total de incidentes), y especialmente los **hospitales (42%)** se vieron especialmente afectados.
- También observamos incidentes dirigidos autoridades, organismos y agencias de salud (14%) y ataques a la **industria farmacéutica (9%)**.

Fuente: ENISA THREAT LANDSCAPE: HEALTH SECTOR July 2023 (enero 2021- marzo 2023)

Dimensionando la *salud cibernética* del Sector

Sector privado
España



Dimensionando la *salud cibernética* del Sector

Sector público

España



Conclusiones

- **Sector** en pleno auge que **gestiona información confidencial y muy sensible**
- La **privacidad** y la **disponibilidad** de la información son **factores clave** para un **buen funcionamiento de la actividad y del negocio**
- **Enorme superficie de exposición y vulnerabilidad** de los datos y procesos esenciales gestionados
- **Riesgo** potencial de sufrir **ciberataques**, provocando **pérdidas económicas y una gran alarma social**

Principales amenazas sector Salud

- **Ransomware**
- **Robo y publicación de datos bajo chantaje** dado el **valor de los datos de los pacientes** (historiales médicos electrónicos etc).
- **Ataques contra la cadena de suministro y los proveedores de servicios sanitarios**
- **Vulnerabilidades en software o hardware** de los **sistemas de IT en entornos sanitarios y los dispositivos médicos hiperconectados**
- **Ataques DDoS**

Fuente: ENISA THREAT LANDSCAPE: HEALTH SECTOR July 2023 (enero 2021- marzo 2023)



Público objetivo

200 asistentes

70% capacidad
ejecutiva y de decisión



C- Level/ Owner VP/ President / Chairman | Director | Senior/Manager



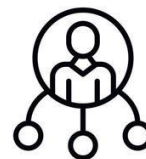
Organizaciones

Pymes y empresas del sector salud,
demandantes de servicios y soluciones de ciberseguridad en los subsectores:

- **Sanitario:** hospitales, clínicas, centros de diagnóstico, seguros médicos, biotech...
- **Farmacéutico:** distribuidores, laboratorios, cadenas farmacéuticas...

Perfiles

- CEO sector sanitario
- COO (Chief Operating Officer)
- Profesionales y Ejecutivos sector salud TIC
 - CISO
 - CTO
 - CIO
 - DPO
 - IT/OT Directors
- Abogados
- Responsables OPD
- Gerentes de asociaciones médicas y pacientes
- Profesionales ámbito académico e investigación



Algunas organizaciones target

CEPYME

CEOE
Empresas Españolas

Cámara
MADRID

ATA
AUTÓNOMOS

ceaje
Confederación Española
Jóvenes Empresarios

Clúster
MAD
e-Health

IDIS

Instituto para el Desarrollo
e Integración de la Sanidad



Ilustre Colegio
Oficial de Médicos
de Madrid



CODEM
Colegio Oficial de
Enfermería de Madrid

**CONSEJO GENERAL DE ENFERMERÍA
DE ESPAÑA**

ASD
ASOCIACIÓN
SALUD DIGITAL

AMYTS
Asociación de Médicos y Titulados Superiores de Madrid

COFM
COLEGIO OFICIAL DE
FARMACÉUTICOS
de MADRID

Farmacéuticos
Consejo General de Colegios Farmacéuticos

COFARES

Sociedad Española de
INGENIERIA BIOMÉDICA

federación española
de empresas de
fenin **TECNOLOGÍA SANITARIA**

**WORLD
COMPLIANCE
ASSOCIATION**

**PLATAFORMA DE ORGANIZACIONES
DE PACIENTES**

**CYBER
MADRID**

Temáticas

Soluciones integrales

- En protección, detección y respuesta con la mayor cobertura de elementos posibles (endpoint, correo electrónico, almacenamiento...)

Soluciones de nicho

- Específicas aplicables para el sector (detección de brechas, etc...)

Ámbitos de Compliance

- En el Sector **Salud** con implicaciones directas en Ciberseguridad

Problemas específicos de la cadena de suministro

Gobierno, privacidad y fuga de los datos

- En Salud. Big Data

Casos de éxito

- De soluciones de ciberseguridad para el sector

Cybersecurity Incident Response

- Casos y simulaciones

Ciberseguros

- En el ámbito **Salud**

Protecciones de elementos IoT



Lugar de celebración y fecha



Jueves, **23 de noviembre** de 2023

**Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad
Politécnica de Madrid** (Campus Ciudad Universitaria). Madrid



Lugar de celebración



Escuela Técnica Superior de Ingenieros de Telecomunicación de la Universidad Politécnica de Madrid.
Edificio C López Araujo. Avenida Complutense nº 30. Ciudad Universitaria (Madrid)



Estructura del Congreso

INTERVENCIONES Y PROGRAMA

• Intervenciones/ponencias institucionales:

- Ayuntamiento de Madrid
- Comunidad de Madrid
- INCIBE
- AEPD
- ENISA: Informe “Threat Landscape: Health sector July 2023”
- CyberMadrid y MAD e-Health
- Patronales y asociaciones de empresarios:
 - CEOE, CEPYME, Cámara de Comercio de Madrid etc.
- Otras



Estructura del Congreso



INTERVENCIONES Y PROGRAMA

- **Keynotes y mesas redondas** en relación a las siguientes temáticas:
 - **Soluciones integrales y de nicho** (Protección, Detección y Respuesta)
 - **Ciberseguros** en el ámbito **Salud**
 - **Compliance** en el Sector **Salud** con implicaciones directas en Ciberseguridad
 - **Cybersecurity Incident Response**
 - **Casos de éxito** de soluciones de ciberseguridad para el sector
 - **Gobierno, privacidad y fuga de los datos** en Salud. Big Data
 - **Problemas específicos de la cadena de suministro**
 - **Protecciones de elementos IoT**
- **Clausura:** personalidad en el ámbito institucional y presidente de CyberMadrid

Empresas asociadas
y patrocinadores



ÁREA DE EXPOSICIÓN Y NETWORKING

- **Área de exposición de patrocinadores**



- **Coffee break | Finger Food**



¿Cómo participar?



- **Las empresas asociadas podrán participar desde el inicio**, en la etapa de diseño del propio Congreso pudiendo aportar tanto **temáticas** como **ponentes**.
- El formato de las intervenciones será **keynote** o **mesa redonda**, y ofrecemos la posibilidad de ser **moderador** o **participante**.
- El congreso ha de tener **contenidos didácticos** y no meramente comerciales, aunque habrá cabida para la **exposición y difusión de producto/servicio**.

Modalidades de patrocinio

¡Ahora con más servicios!

- Tendrán prioridad a la hora de participar, aquellas empresas asociadas y propuestas que ofrezcan un **patrocinio** y sobre este aspecto, las que se postulen por orden cronológico.
- Si tienes alguna otra propuesta de colaboración, **envíanosla!**

Servicio incluido en el patrocinio	Gold	Silver	Bronze
Inclusión del logotipo de la entidad patrocinadora en la web	✓	✓	✓
Inclusión del logotipo de la entidad patrocinadora en la cartelería del evento	✓	✓	✓
Difusión de la participación de la entidad patrocinadora en LinkedIn	✓	✓	✓
Difusión de la participación de la entidad patrocinadora en Twitter	✓	✓	✓
Participar como ponente en una ponencia propia	✓		
Participar como ponente en una ponencia ya constituida	✓	✓	
Ponencia en horario prime time	✓		
Mención expresa en los agradecimientos del discursos inaugural y de clausura por parte del Presidente	✓		
Menciones destacadas en la web oficial, notas de prensa etc.	✓		
Invitaciones al evento	20	10	5
Leads que voluntariamente hayan cedido sus datos en la inscripción al evento	✓	✓	
Inclusión de logotipo en la acreditación del evento	✓	✓	
Patrocinio coffee break	✓		✓
Patrocinio finger food	✓		
Mobiliario zona de expositor	✓	✓	✓
Tarifa (IVA no incluido)	3.000 €	2.000 €	1.000 €



Contacto



Para cualquier duda o consulta, ponte en contacto con nosotros

Charo Pinilla Cabo

manager@cybermadrid.org

+34 689 80 81 16



I CyberSecurity Healthcare & Pharma Congress



¡Te esperamos!



Síguenos en:



Cyber Madrid- Clúster de Ciberseguridad de Madrid

@Cyber_Madrid