

Centro Demostrador de Ciberseguridad



¿Qué es el Centro Demostrador?

Es un entorno de referencia para experimentar y demostrar soluciones de ciberseguridad en escenarios realistas, a través de casos de uso y laboratorio.

Está gestionado por la Agencia de Ciberseguridad de la Comunidad de Madrid (ACCM), que se enmarca en la Consejería de Digitalización de la Comunidad de Madrid.

Su actividad se estructura a través de un catálogo de servicios y se acompaña de acciones de dinamización para impulsar **la adopción, el impacto y la concienciación** en el ecosistema sanitario.



Entra en la web del Centro Demostrador
www.centrodemostrador.comunidad.madrid



Únete al canal de **WhatsApp de la ACCM**
para más información sobre ciberseguridad

Fundamentos Estratégicos



Misión

Impulsar la ciberseguridad desde un **enfoque práctico** para incrementar la formación, la concienciación y las capacidades del sector, **fortaleciendo la confianza digital y generando impacto real en el ecosistema público y empresarial.**



Visión

Ser el **entorno de referencia**, nacional e internacional, para demostrar y acelerar la **adopción de soluciones de ciberseguridad** aplicadas al sector sanitario.



Metas

Consolidar **al Centro Demostrador** como **espacio de referencia** mediante un modelo estable basado en laboratorio, demostración de casos de uso, asesoramiento y dinamización del ecosistema (investigación, alianzas y eventos).

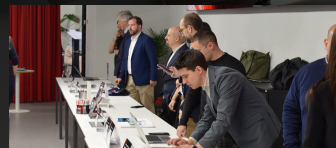


Objetivos

Generar un impacto tangible: mejorar la preparación de los profesionales, reforzar la concienciación ciudadana y fomentar la mejora continua del sector en materia de ciberseguridad.

Un Centro con capacidades para informar, demostrar, asesorar y formar

Los servicios del Centro Demostrador



Ecosistema de ciberseguridad



Observatorio de ciberseguridad



Laboratorio de ciberseguridad



Demostraciones de ciberseguridad



Asesoramiento y consultoría



Impulso y sensibilización

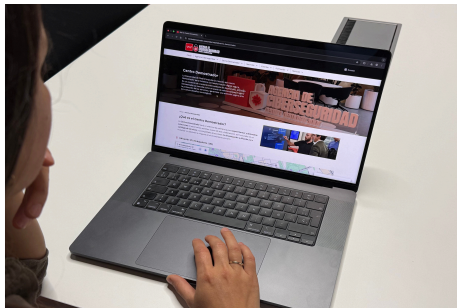


Formación y certificaciones



Ecosistema de ciberseguridad

Posiciona al Centro como punto de encuentro del ecosistema sanitario y tecnológico en materia de ciberseguridad. Impulsa la colaboración y la transferencia de conocimiento entre instituciones públicas, empresas, startups y proveedores especializados. Asimismo, coordina y dinamiza comités, foros y grupos de trabajo y gestiona las relaciones entre los distintos agentes del sector.



Observatorio de ciberseguridad

Mantiene actualizado al ecosistema sanitario y tecnológico en materia de ciberseguridad. Difunde tendencias, incidentes y ciberataques relevantes, informes y estudios sectoriales, novedades normativas y regulatorias, así como contenidos propios del Centro y una newsletter periódico con información de interés.



Laboratorio de ciberseguridad

Ofrece un entorno técnico seguro tipo laboratorio/sandbox para la validación y análisis de soluciones tecnológicas y de ciberseguridad. Su actividad se basa en pruebas de concepto (PoC), pruebas funcionales y simulaciones controladas, adaptadas a escenarios específicos de cada organización y sin impacto sobre sistemas reales.



Demostraciones de ciberseguridad

Expone casos de uso de ciberseguridad aplicados al ámbito sanitario mediante demostraciones prácticas. Se muestran soluciones orientadas a la seguridad de dispositivos médicos (IoMT/OT), la protección del dato, la gestión de identidades y accesos, el cumplimiento normativo, la ciberdefensa, la resiliencia digital y la concienciación en ciberseguridad.

Se especifican más adelante.



Asesoramiento y consultoría

Ofrece acompañamiento especializado en ciberseguridad mediante diagnósticos rápidos de necesidades, recomendaciones técnicas y de cumplimiento, apoyo en la interpretación y aplicación normativa —ENS, NIS2, RGPD, entre otras— y orientación sobre buenas prácticas y tecnologías aplicadas al sector.



Impulso y sensibilización

Acerca la ciberseguridad al sector sanitario y a la sociedad mediante jornadas, eventos, webinars, sesiones divulgativas y actividades prácticas, como ciberejercicios y hackathones. Además, difunde los resultados y aprendizajes generados desde el Centro con el objetivo de reforzar la concienciación, el conocimiento y las capacidades de respuesta ante ciberamenazas.



Formación y certificaciones

Impulsa el talento y la cultura de ciberseguridad con itinerarios formativos y certificaciones. La oferta, desarrollada con ISMS Forum, se organiza en niveles básico, intermedio y avanzado para distintos perfiles.



Conoce e insíbete en nuestras **formaciones y certificaciones** disponibles

El Centro Demostrador ofrece 16 programas formativos

Los cursos se distribuyen en **tres niveles dirigidos** tanto a **ciudadanos sin conocimientos previos** como a **estudiantes, profesionales y perfiles especializados**. Se realizan en colaboración con ISMS Forum, asociación española sin ánimo de lucro, cuyo principal objetivo es **fomentar la seguridad de la información en España**.



Básico

- Curso de Concienciación en Ciberseguridad (6 h) *Cybersecurity Awareness Training Certification*
- Curso base de Protección de Datos (3 h) *Data Privacy Basic Training Certification*
- Curso de iniciación a la Ciberseguridad en la Nube (6 h) *Cloud Cybersecurity Governance Basic Training Certification*
- Punto de partida Directiva NIS2 (5 h) *NIS2 Basic Training Certification*
- Primeros pasos para la Gestión de la Cadena de Suministro (5 h) *Supply Chain Basic Training Certification*



Intermedio

- Curso de conceptos básicos sobre Ciberseguridad (10 h) *Cyber Security Basic Training Certification*
- Curso introductorio al marco normativo de Ciberseguridad: Cyber Compliance (7 h) *Cyber Compliance Basic Training Certification*
- Curso de introducción a la Ciberseguridad de la IA (10 h) *Artificial Intelligence Basic Training Certification*
- Novedades en el Marco Regulatorio de Protección de Datos (5 h) *CNDP (Certified in New Developments in Data Protection)*
- Curso Gestión de riesgo IT en la Cadena de Suministro (20 h) *CESP (Certified Expert in IT Risk Management in the Supply Chain)*
- Curso NIS2 Conoce y aplica el framework regulatorio de ciberseguridad (10 h) *NIS2PC*



Avanzado

- Curso de gobierno de Ciberseguridad en la Nube (45 h) *CCGP (Certified Cloud Cybersecurity Governance Professional)*
- Curso de Especialización en Ciberseguridad (35,5 h) *CCSP (Certified Cyber Security Professional)*
- Curso de Especialización en Protección de Datos (60 h) *CDPP (Certified Data Privacy Professional)*
- Curso de IA para profesionales de Ciberseguridad y Privacidad (30 h) *CAIP (Certified Artificial Intelligence and Information Security Professional)*
- Curso Cyber Compliance: adecuación al nuevo marco normativo de la Ciberseguridad (30 h) *CPCC (Certified Professional Cyber Compliance)*

15 casos de uso que permiten experimentar con soluciones reales, **agrupados en 4 familias**



6 Casos de uso

Protección de dispositivos médicos y seguridad **IoMT/IoT**



5 Casos de uso

Preparación y respuesta ante **ciberincidentes**



2 Casos de uso

Gestión de **identidades y accesos**



2 Casos de uso

Protección y cumplimiento normativo

Protección de dispositivos médicos y seguridad IoMT/IoT

6 casos de uso orientados a identificar activos, segmentar redes, detectar anomalías, proteger dispositivos críticos y reforzar accesos y comunicaciones en entornos sanitarios conectados.

1

Protección del Ecosistema Sanitario

Permite descubrir e inventariar de forma pasiva los activos conectados en entornos clínicos. Mejora la visibilidad, reduce riesgos y facilita una gestión más segura de la superficie de ataque.

2

Red Médica Segura

Orienta la segmentación y protección inteligente de redes y dispositivos IoMT. Ayuda a controlar comunicaciones, detectar anomalías y reforzar la seguridad operativa.

3

De la Alerta a la Acción

Muestra cómo detectar anomalías en dispositivos conectados y activar alertas en tiempo real. Refuerza la capacidad de respuesta temprana ante fallos, manipulaciones o comportamientos anómalos.

4

Paciente Protegido

Aborda la protección de dispositivos legacy críticos en entornos sanitarios. Permite identificar vulnerabilidades, aplicar mitigaciones y reducir la exposición de activos obsoletos.

5

Acceso Remoto Seguro para IoMT

Demuestra cómo controlar, monitorizar y auditar accesos remotos de terceros a dispositivos médicos. Mejora la trazabilidad y reduce el riesgo asociado a conexiones externas no seguras.

6

Vehículos Conectados

Plantea un entorno de comunicaciones críticas y seguras para ambulancias y unidades móviles. Busca garantizar conectividad, transmisión en tiempo real y mayor capacidad de respuesta en movilidad.



Preparación y respuesta ante ciberincidentes

5 casos centrados en identidad digital y control de acceso para garantizar accesos seguros, reforzar la trazabilidad y proteger datos sensibles.

7

Modelado de Amenazas

Permite analizar aplicaciones críticas del sector salud para identificar vectores de ataque y riesgos. Ayuda a definir controles de seguridad y mejorar la protección desde el diseño.

8

PhisAware

Simula campañas de phishing para medir el nivel de concienciación y respuesta del personal. Contribuye a reducir el riesgo asociado al robo de credenciales y otras amenazas frecuentes.

9

Ransomware

Recrea un incidente de ransomware en un entorno controlado para entrenar la respuesta. Refuerza habilidades prácticas de investigación, actuación y toma de decisiones ante un caso real.

10

Escudo Digital

Muestra cómo opera un SOC en la monitorización, detección y gestión de incidentes en sanidad. Centraliza alertas y eventos para mejorar la visibilidad y la respuesta ante amenazas.

11

Resiliencia Digital en Smart Health

Demuestra cómo diseñar, activar y gestionar planes de continuidad y contingencia. Ayuda a mejorar la recuperación y coordinación ante incidentes que afecten a servicios críticos.

Gestión de identidades y accesos

2 casos de uso orientados a mejorar la **detección, respuesta, continuidad y toma de decisiones** ante incidentes de ciberseguridad en el **ámbito sanitario**.

12

Control de Acceso Inteligente

Aplica control de acceso basado en roles para que cada perfil acceda solo a lo necesario. Refuerza la trazabilidad, protege datos sensibles y mejora el cumplimiento normativo.

13

Identidad Sanitaria 4.0

Explora un modelo de identidad y autorización sanitaria basado en wallet y credenciales verificables. Busca garantizar acceso seguro, consentimiento, interoperabilidad y mejor experiencia de usuario.



Protección y cumplimiento normativo

2 casos de uso centrados en **la protección del dato, la gestión de riesgos y el cumplimiento normativo**, con foco en mejorar la trazabilidad, reducir riesgos y reforzar la seguridad de la información.

14

Anonimización

Demuestra cómo anonimizar, seudonimizar o cifrar datos clínicos para proteger su privacidad. Reduce el riesgo de reidentificación manteniendo la utilidad del dato.

15

Gobernar para Proteger

Muestra cómo una herramienta GRC ayuda a gestionar riesgos, controles y cumplimiento normativo. Mejora la trazabilidad, la visibilidad y la toma de decisiones en ciberseguridad sanitaria.

El Centro Demostrador, un espacio para probar, validar y demostrar

Mapa 3D

Espacios del Centro Demostrador

 Centro Demostrador

 Espacios Complementarios

Laboratorio
de ciberseguridad

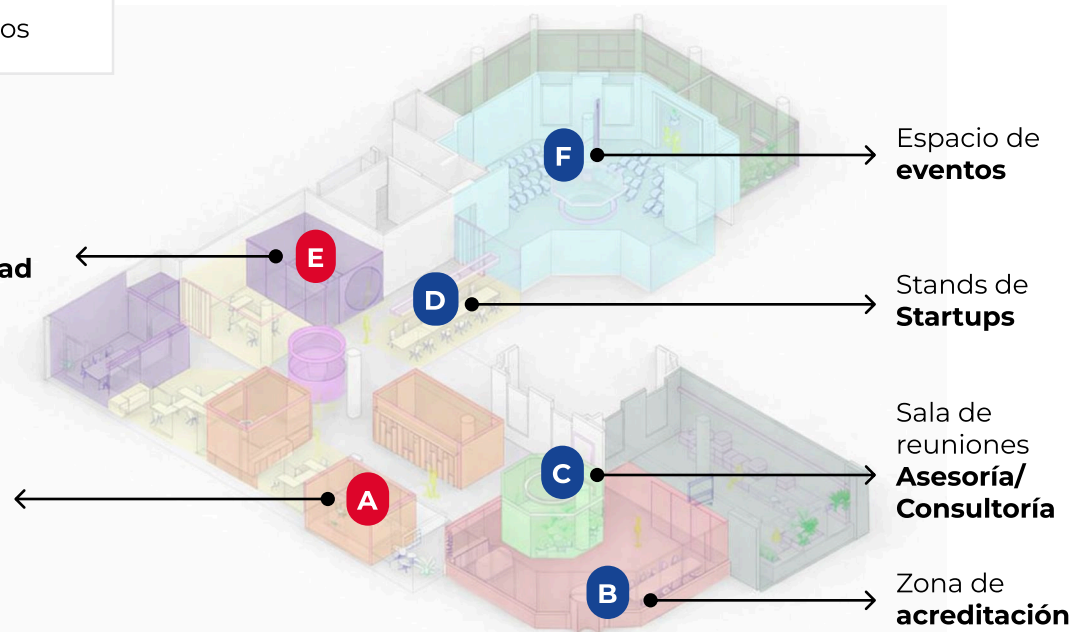
Centro
Demostrador

Espacio de
eventos

Stands de
Startups

Sala de
reuniones
**Asesoría/
Consultoría**

Zona de
acreditación



El Centro Demostrador impulsa la colaboración público-privada para ampliar capacidades y conectar el ecosistema ciber

Seguimos un modelo de innovación abierta orientado a **facilitar la colaboración entre empresas, startups y otros agentes del ecosistema**, con acompañamiento técnico y desarrollo de pilotos de validación tecnológica.

Trabajamos con una red de empresas colaboradoras para ampliar las capacidades del Centro

El Centro se apoya en un ecosistema de empresas que contribuyen a enriquecer su propuesta de valor, reforzar las capacidades de demostración y conexión entre startups, pymes innovadoras, *corporates*, universidades e inversores para generar colaboración real y facilitar proyectos piloto, validación tecnológica y nuevas oportunidades de desarrollo.

La estrategia de diferenciación se estructura en **tres niveles fundamentales**

Operativo - Aseguran la ejecución y operación de los servicios

 **accenture**

Deloitte.

Empresas asociadas - Aportan apoyo y colaboración en las actividades de soporte / operación de servicios

CREMADES & CALVO-SOTELO
ABOGADOS

 **SCC**

AIRBUS

isms
FORUM

Alianzas estratégicas - Actúan como socios de referencia en la ejecución y optimización operativa.

 **ARCHER**

aritim
the APT company

evolutio

F24

FORTINET.

 **imprivata**

 **Namirial**

 **NOZOMI**
NETWORKS

THALES
Cybersecurity

 **Teldat**

 **ThreatModeler** + **IriusRisk**

Nuestros convenios estratégicos facilitan la visibilidad, mejoran el posicionamiento y fomentan la actividad del Centro Demostrador

La Consejería de Digitalización y el Centro Demostrador están desarrollando un **conjunto de convenios** que facilitan la **colaboración público-privada en beneficio del ecosistema ciber**.



Red de protocolos para ampliar las capacidades del Centro



Grupo de trabajo con **CISOs de ayuntamientos, infraestructuras críticas y entidades locales de la Comunidad de Madrid**



Comité de expertos para estar actualizados según las tendencias y necesidades del sector



¿Quieres colaborar con el Centro Demostrador?

Estamos abiertos a establecer nuevos convenios y alianzas estratégicas

Nuestras alianzas



Ubicado en el **Centro de Innovación Digitaliza Madrid, C/ Embajadores, 181.**
Puedes visitarnos de **lunes a jueves de 9 a 17 h** y **viernes de 9 a 14 h.**
Es necesario concertar cita previa

✉ accm_centrodemostrador@madrid.org ☎ +34 919 43 99 70

