AGENCIA DE CIBERSEGURIDAD
centro demostrador

Cyber Demonstration Center

Financiado por la Unión Europea
NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE TELECOMUNICACIONES E INFRAESTRUCTURAS DIGITALES

Plan de Recuperación, Transformación y Resiliencia

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

Comunidad de Madrid

About the center

It is a reference environment for testing and demonstrating cybersecurity solutions in realistic scenarios through use cases and laboratory-based activities.

The Demo Center is managed by the Cybersecurity Agency (ACCM), which operates under the Ministry of Digitalization of the Community of Madrid.

Its activities are structured through a comprehensive service portfolio and complemented by ecosystem engagement initiatives aimed at **promoting adoption, raising awareness and maximizing the impact of cybersecurity across the healthcare sector.**

Visit the Cybersecurity Demonstration Centre website
www.centrodemostrador.comunidad.madrid

Join the **ACCM WhatsApp Channel** for the latest cybersecurity updates

Strategic Fundamentals

Mission

To advance cybersecurity through a **practical approach** to enhances training, awareness and sector capabilities, **strengthens digital trust and delivers measurable impact across both public and private organizations.**

Vision

To become the **leading** national and international **reference environment** for demonstrating and accelerating the **adoption of cybersecurity solutions** applied to the healthcare sector.

Goals

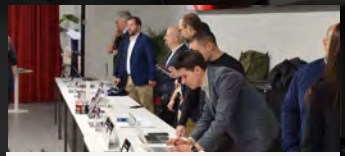
Consolidating **the Demonstration Center** as a **leading hub** through a sustainable model driven by lab environments, use case demos, strategic advisory, and ecosystem engagement (including research, partnerships, and events).

Objectives

To **generate** a **tangible impact**: enhancing professional preparedness, strengthening public awareness, and promoting continuous advancement in cybersecurity throughout the sector.

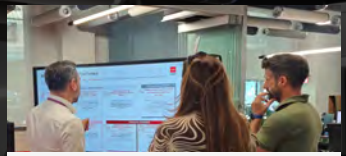
A Centre with the capabilities to Inform, Demonstrate, Advise and Train

Demonstration
Centre Services



Cybersecurity ecosystem

Cybersecurity observatory

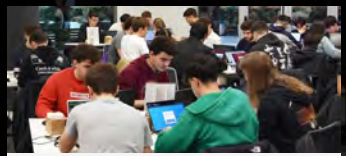


Cybersecurity laboratory

Cybersecurity demonstrations

Advisory and consulting services

Promotion and awareness-raising



Training and certifications

Cybersecurity ecosystem

Positions the Centre as a meeting point for the healthcare and technology ecosystem in the field of cybersecurity. It promotes collaboration and knowledge transfer among public institutions, companies, startups and specialized cybersecurity providers. It also coordinates and facilitates committees, forums and working groups while managing relationships among key stakeholders across the sector.

Cybersecurity observatory

Keeps the healthcare and technology ecosystem up to date on cybersecurity matters. It disseminates information on emerging trends, relevant incidents and cyberattacks, sector reports and studies, regulatory and compliance developments, as well as proprietary content generated by the Centre and a periodic cybersecurity newsletter.

Cybersecurity laboratory

Provides a secure laboratory/ sandbox environment for the validation and assessment of technology and cybersecurity solutions. Activities include proof-of-concept (PoC) exercises, functional testing and controlled simulations tailored to each organization's specific scenarios, with no impact on production systems.

Cybersecurity demonstrations

Showcases cybersecurity use cases specifically designed for healthcare environments through practical demonstrations. Featured solutions address medical device security (IoMT/OT), data protection, identity and access management (IAM), regulatory compliance, cyber defence, digital resilience and cybersecurity awareness.

Further details are provided below.

Advisory and consulting services

Provides specialized cybersecurity support through rapid needs assessments, technical and compliance recommendations, assistance with the interpretation and implementation of regulatory frameworks — including ENS, NIS2 and GDPR — as well as guidance on best practices and sector-specific cybersecurity technologies.

Promotion and awareness-raising

Brings cybersecurity closer to healthcare organizations and society through conferences, events, webinars, awareness sessions and practical activities such as cyber exercises and hackathons. It also disseminates the outcomes and lessons learned from Centre initiatives to strengthen awareness, knowledge and cyber resilience capabilities.

Training and certifications

Promotes cybersecurity talent development and culture through structured learning pathways and professional certifications. Delivered in collaboration with ISMS Forum, the programme is organized into Basic, Intermediate and Advanced levels tailored to different professional profiles.

Explore and enrol in our available **training and certification** programmes

The Demonstration Centre offers 16 training programmes

The courses are structured across **three levels**, targeting **citizens with no prior knowledge** as well as **students, professionals, and specialized profiles.** They are conducted in collaboration with ISMS Forum, a Spanish non-profit association whose primary objective is to **promote information security in Spain**

Basic Level

- *Cybersecurity Awareness Training Certification* (6 hours)
- *Data Privacy Basic Training Certification* (3 hours)
- *Cloud Cybersecurity Governance Basic Training Certification* (6 hours)
- *NIS2 Basic Training Certification* (5 hours)
- *Supply Chain Basic Training Certification* (5 hours)

Intermediate Level

- *Cyber Security Basic Training Certification* (10 hours)
- *Cyber Compliance Basic Training Certification* (7 hours)
- *Artificial Intelligence Basic Training Certification* (10 hours)
- *CNDP (Certified in New Developments in Data Protection)* (5 hours)
- *CESP (Certified Expert in IT Risk Management in the Supply Chain)* (20 hours)
- NIS2PC (NIS2 Regulatory Framework: Understanding and Implementation) (10 hours)

Advanced Level

- *CCGP (Certified Cloud cybersecurity Governance Professional)* (45 hours)
- CCSP *(Certified Cyber Security Professional)* (35,5 hours)
- *CDPP (Certified Data Privacy Professional)* (60 hours)
- *CAIP (Certified Artificial Intelligence and Information Security Professional)* (30 hours)
- *CPCC (Certified Professional Cyber Compliance)* (30 hours)

15 Use Cases to Experience Real-World Cybersecurity Solutions, Organized into 4 Categories

6 Use Cases

Medical Device **Protection** and **IoMT/IoT Security**

5 Use Cases

Cyber Incident Preparedness and Response

2 Use Cases

Identity and Access Management

2 Use Cases

Data Protection and **Regulatory** Compliance

Medical Device Protection and IoMT/IoT Security

6 Use Cases Focused on Asset Discovery, Network Segmentation, Anomaly Detection, Critical Device Protection, and Securing Access and Communications Across Connected Healthcare Environments

1

Healthcare Ecosystem Protection

Enables passive discovery and inventory of connected assets within clinical environments. Enhances visibility, reduces risk exposure, and supports more secure management of the organization's attack surface.

2

Secure Medical Network

Demonstrates intelligent segmentation and protection of IoMT devices and healthcare networks. Helps control communications, detect anomalies, and strengthen operational security.

3

From Alert to Action

Shows how to detect anomalies in connected medical devices and trigger real-time alerts. Enhances early response capabilities to address failures, tampering attempts, or abnormal behavior.

4

Protected Patient

Addresses the protection of critical legacy medical devices within healthcare environments. Enables the identification of vulnerabilities, implementation of mitigation measures, and reduction of risks associated with obsolete assets.

5

Secure Remote Access for IoMT

Demonstrates how to control, monitor, and audit third-party remote access to medical devices. Improves traceability and reduces risks associated with insecure external connections.

6

Connected Emergency Vehicles

Provides a secure communications environment for ambulances and mobile healthcare units. Ensures reliable connectivity, real-time data transmission, and enhanced operational response capabilities in mobile scenarios.

Cyber Incident Preparedness and Response

5 Use Cases Focused on Enhancing Detection, Incident Response, Business Continuity, and Decision-Making Capabilities in Healthcare Cybersecurity Environments

7

Threat Modeling

Enables the analysis of critical healthcare applications to identify attack vectors, vulnerabilities, and cybersecurity risks. Supports the definition of security controls and promotes a security-by-design approach.

8

PhisAware

Simulates phishing campaigns to assess employee awareness and response capabilities. Helps reduce the risk of credential theft and other common cyber threats through targeted awareness and training exercises.

9

Ransomware

Recreates a ransomware incident within a controlled environment to train response teams. Strengthens practical skills in investigation, containment, recovery, and decision-making during real-world cyber incidents.

10

Digital Shield

Demonstrates how a Security Operations Centre (SOC) monitors, detects, and manages cybersecurity incidents within healthcare environments. Centralizes alerts and security events to improve visibility, threat detection, and incident response effectiveness.

11

Digital Resilience in Smart Health

Demonstrates how to design, activate, and manage business continuity and contingency plans. Supports faster recovery and improved coordination when cybersecurity incidents impact critical healthcare services.

Identity and Access Management

2 Use Cases Focused on Digital Identity Protection and Access Control to Ensure Secure Access, Improve Traceability, and Safeguard Sensitive Information

12

Intelligent Access Control

Implements role-based access control to ensure that each user profile can only access the information and resources required for their responsibilities. Enhances traceability, protects sensitive data, and supports regulatory compliance.

13

Healthcare Identity 4.0

Explores a healthcare identity and authorization model based on digital wallets and verifiable credentials. Aims to ensure secure access, patient consent management, interoperability, and an improved user experience.

Data Protection and Regulatory Compliance

2 Use Cases Focused on Data Protection, Risk Management, and Regulatory Compliance to Improve Traceability, Reduce Risk Exposure, and Strengthen Information Security

14

Data Anonymization

Demonstrates how to anonymize, pseudonymize, or encrypt clinical data to safeguard patient privacy. Reduces the risk of re-identification while preserving data usability for operational and research purposes.

15

Governance for Protection

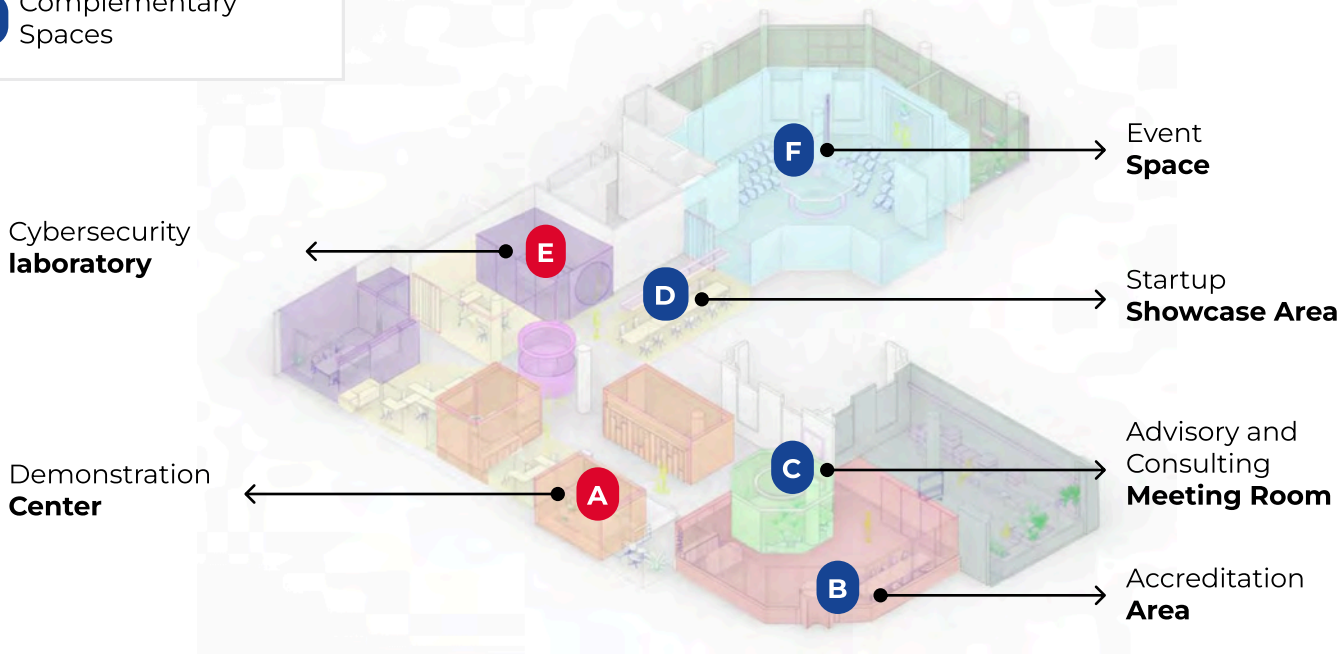
Demonstrates how a Governance, Risk, and Compliance (GRC) platform supports the management of risks, controls, and regulatory compliance requirements. Enhances traceability, visibility, and cybersecurity decision-making within healthcare organizations.

The Demonstration Centre: A Space to Test, Validate, and Showcase Cybersecurity Solutions

3D Interactive Map

Demonstration Centre Areas

- Demonstration Center
- Complementary Spaces



Driving Public-Private Collaboration to Strengthen Capabilities and Connect the Cybersecurity Ecosystem

We work with a network of partner organizations to expand the capabilities of the Demonstration Centre and enhance the value delivered to the cybersecurity ecosystem.

The Centre is supported by an ecosystem of organizations that contribute to strengthening its value proposition, enhancing demonstration capabilities, and fostering connections among startups, innovative SMEs, large enterprises, universities, and investors. This collaborative approach promotes real-world cooperation, facilitates pilot projects and technology validation initiatives, and creates new opportunities for innovation and growth.

Public-Private Collaboration

Our Differentiation Strategy Is Structured Around **Three Core Levels**

Operational Partners - Responsible for the delivery and day-to-day operation of the Centre's services.

accenture | Deloitte.

Associated Companies - Provide support and collaboration in service delivery, operational activities, and ecosystem engagement initiatives.

CREMADES & CALVO-SOTELO ABOGADOS | SCC | AIRBUS | isms FORUM

Strategic Alliances - Act as key partners in the execution, optimization, and continuous improvement of the Centre's operations and services.

ARCHER | aritium | evolutio | F24

FORTINET | imprivata | Namirial | NOZOMI NETWORKS

THALES | Teldat | ThreatModeler + IriusRisk

Our Strategic Agreements that Enhance Visibility, Strengthen Positioning, and Drive the Centre's Activity

The Ministry for Digitalisation and the Demonstration Centre are developing a framework of **strategic agreements** designed to **promote public-private collaboration for the benefit of the cybersecurity ecosystem.**

Network of Collaboration Agreements to Expand **the Centre's Capabilities**

Working group bringing together **CISOs from municipalities, critical infrastructure operators, and local entities across the Community of Madrid.**

Expert advisory committee that helps ensure alignment with emerging trends, challenges, and cybersecurity sector needs.

CIONET · CYBER MADRID · CyberLideria · fundación para el conocimiento madrid · isms forum · ISACA · paloalto NETWORKS · Roche · WOMEN 4CYBER · zscaler

Interested in Collaborating with the Demonstration Centre?
We are open to establishing new cooperation agreements and strategic partnerships.

AGENCIA DE
CIBERSEGURIDAD
centro demostrador

Located within the Digitaliza Madrid Innovation Centre, C/ Embajadores, 181.
Opening hours:
Monday to Thursday: 09:00 – 17:00
Friday: 09:00 – 14:00
Visits are by appointment only

accm_centrodemostrador@madrid.org +34 919 43 99 70