Capital
Digital

MADRID

Madrid's Cybersecurity Strategy
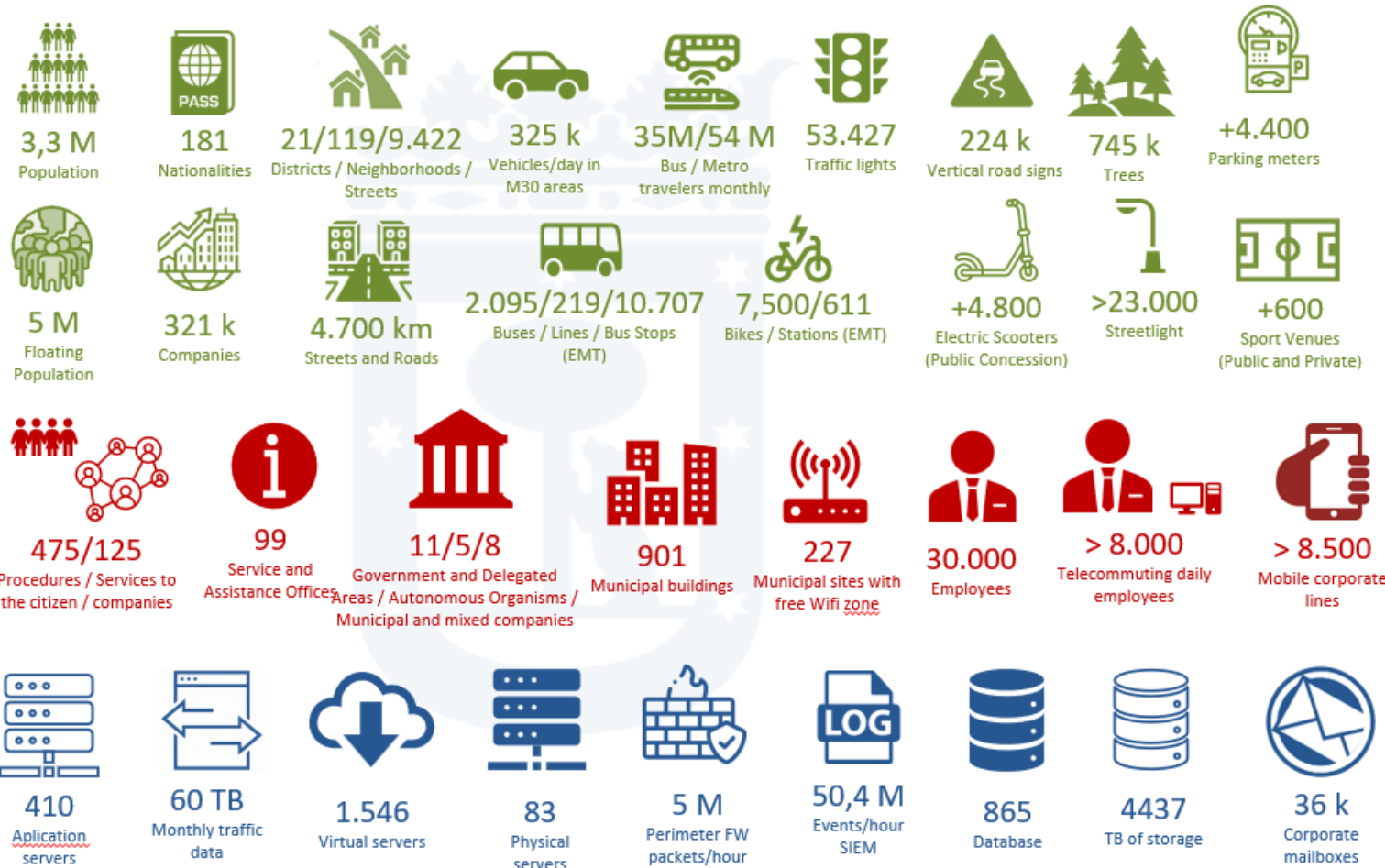
SMART**CITY**
EXPO WORLD CONGRESS

	City		Member state		Official population
1	**Berlin**	🇩🇪	Germany		3,755,251
2	**Madrid**	🇪🇸	Spain		3,332,035
3	**Rome**	🇮🇹	Italy		2,754,719
4	**Paris**	🇫🇷	France		2,087,577
5	**Vienna**	🇦🇹	Austria		2,018,653

20	Croatia	3,862,000
21	Lithuania	2,885,900
22	Slovenia	2,123,900
23	Latvia	1,871,900
24	Estonia	1,374,700
25	Cyprus	933,500
26	Luxembourg	672,100
27	Malta	563.000

3,3 M Population
181 Nationalities
21/119/9.422 Districts / Neighborhoods / Streets
325 k Vehicles/day in M30 areas
35M/54 M Bus / Metro travelers monthly
53.427 Traffic lights
224 k Vertical road signs
745 k Trees
+4.400 Parking meters

5 M Floating Population
321 k Companies
4.700 km Streets and Roads
2.095/219/10.707 Buses / Lines / Bus Stops (EMT)
7,500/611 Bikes / Stations (EMT)
+4.800 Electric Scooters (Public Concession)
>23.000 Streetlight
+600 Sport Venues (Public and Private)

475/125 Procedures / Services to the citizen / companies
99 Service and Assistance Offices
11/5/8 Government and Delegated Areas / Autonomous Organisms / Municipal and mixed companies
901 Municipal buildings
227 Municipal sites with free Wifi zone
30.000 Employees
> 8.000 Telecommuting daily employees
> 8.500 Mobile corporate lines

410 Aplication servers
60 TB Monthly traffic data
1.546 Virtual servers
83 Physical servers
5 M Perimeter FW packets/hour
50,4 M Events/hour SIEM
865 Database
4437 TB of storage
36 k Corporate mailboxes

Digital Transformation Strategy 2023-2027

Rationalisation and simplification shock plan

Artificial Intelligence and Robotisation Strategy
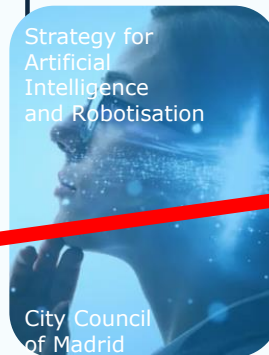
Mobile App Strategy

Cybersecurity Strategy

Madrid GovTech Programme

Digital Administration Plan

5G Agenda

Multicloud Strategy

Data Strategy

Digital Training Plan

CYBERSECURITY STRATEGY UPDATE
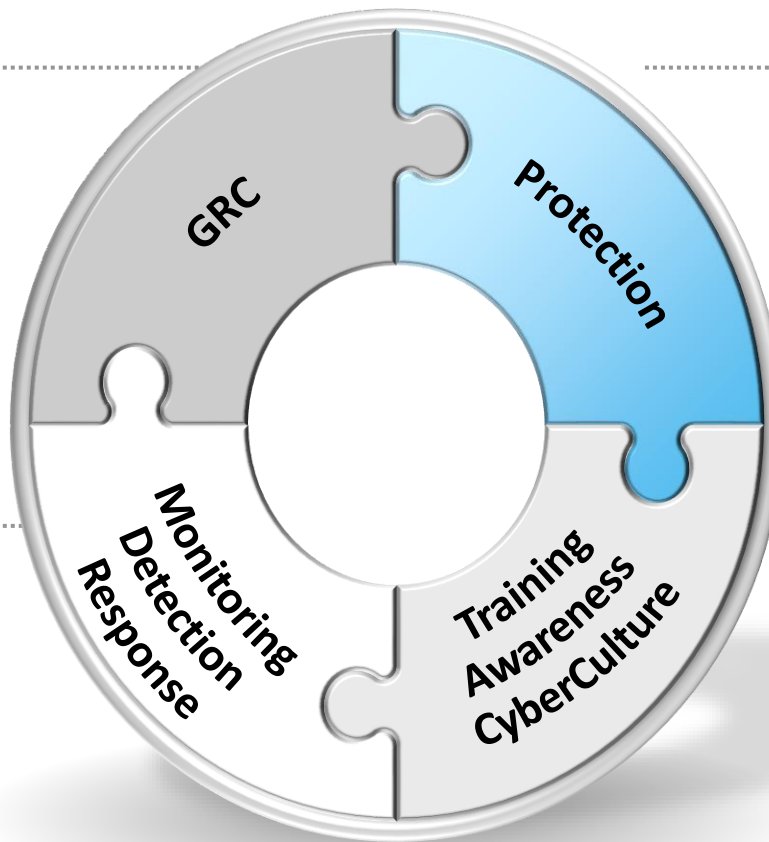

Cybersecurity strategy 2023
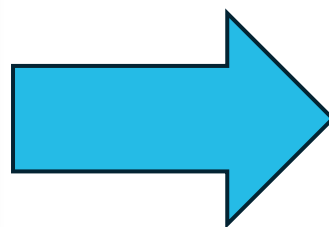
Cybersecurity roadmap Strategic framework

1. Develop a Cybersecurity Governance, Risk and Compliance model for the **City**
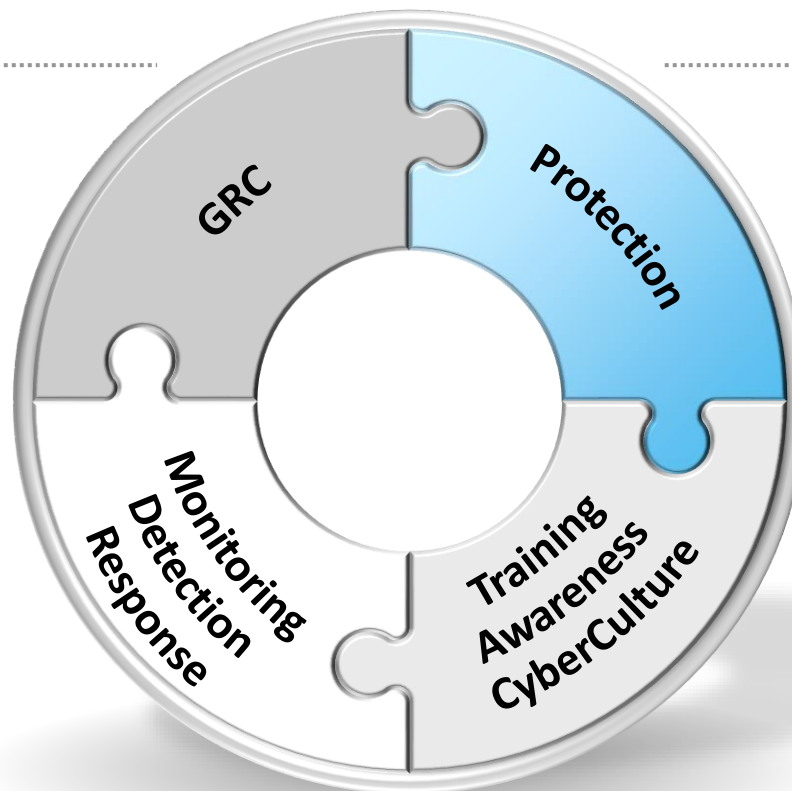
2. Improve the protection of **City** Digital Services

3. Strengthen the **City's** monitoring, detection and response capabilities

4. Promote Training, Awareness and CYBER culture for the **City**

1. **Develop a Cybersecurity Governance, Risk, and Compliance Model for the City**

2. **Enhance the Protection Level of City Services**

3. **Strengthen the City's monitoring, detection and response capabilities**

4. **Promote Cyber Training, Awareness and CYBER culture for the City**

SO1 Develop a Cybersecurity Governance, Risk, and Compliance Model for the City

AL1.1   Compliance with Cybersecurity Regulatory Framework

- o P1 Extend Spanish National Security Schema (ENS) certification to all procedures of the electronic headquarters
- o P2 Obtain certification for CCMAD SOC services (FIRST or EN

AL1.2   Expand Cybersecurity Governance to All Services, Departments, and Agencies

- o P3 Extend information security governance to all government departments: designate delegated security officers
- o P4 Integration of cybersecurity into procurement processes and the monitoring of service delivery by external providers

AL1.3   Coordinate Digital Services Business Continuity Plan with the Citywide Continuity Plan

- o P5 Improve digital services business continuity plans and align them with the city's overall continuity strategy

SO2 Enhance the Protection Level of City Services

AL2.1 Define a security architecture for IoT that enhances the hardening level of urban network infrastructures

- P6 Establish a dedicated urban cybersecurity unit within CCMAD
- P7 Extend the security control lifecycle - encompassing control definition, implementation, continuous monitoring, and ethical hacking audits - from traditional IT environments to OT and IoT infrastructures
- P8 Secure access to the Azca control center (tunnel and lighting control)

AL2.2 Develop Secure and Resilient Information Systems

- P9 Systematically incorporate security testing (pentesting and audits) into OT/IoT environments

SO3 Strengthen the City's Monitoring, Detection, and Response Capabilities

AL3.1 Advanced Security for Comprehensive Protection of the City Council

- P10 Deploy advanced monitoring, detection, and response capabilities for OT/IoT
- P11 Improve and test the Cyber Crisis Management Plan
- P12 Consolidate procedures for managing cyber incident investigation files
- P13 Define and implement a new identity management strategy
- P14 Improve the cybersecurity services dashboard

AL3.2 External Cooperation to Enhance Detection, Monitoring, and Response Processes

- P15 Improve coordination and information sharing with the national SOC network
- P16 Launch "bug bounty" programs to reward ethical hackers for discovering vulnerabilities in municipal systems
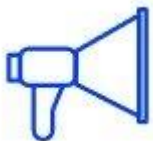
SO4 Promote Cyber Training, Awareness, and Culture in the City

AL4.1 Comprehensive Training for a Cybersecure Future

- P17 Train cyber capabilities through participation in high-level national and international cyber exercises
- P18 Provide training for municipal employees
- P19 Evolve the awareness platform for municipal employees

AL4.2 Cybersecurity Awareness: Outreach and Engagement Initiatives

- P20 Promote cybersecurity culture via intranet and social media (ALMU)
- P21 Participate in the public-private ecosystem focused on "cybersecurity in smart cities"
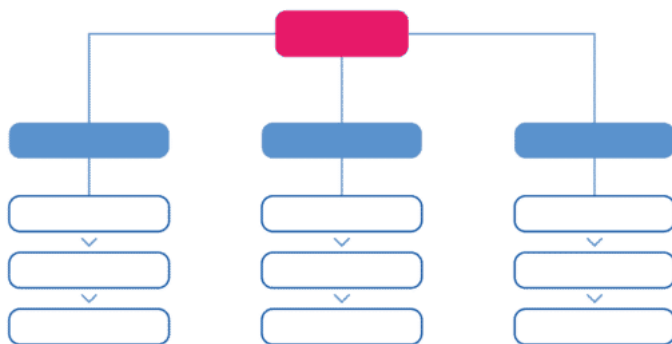- P22 Cooperate with other cities: CoP Cyber Eurocities

ORGANISATION CHART / CISO POSITION
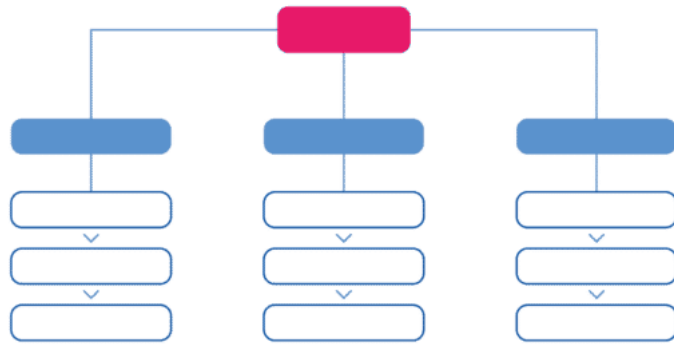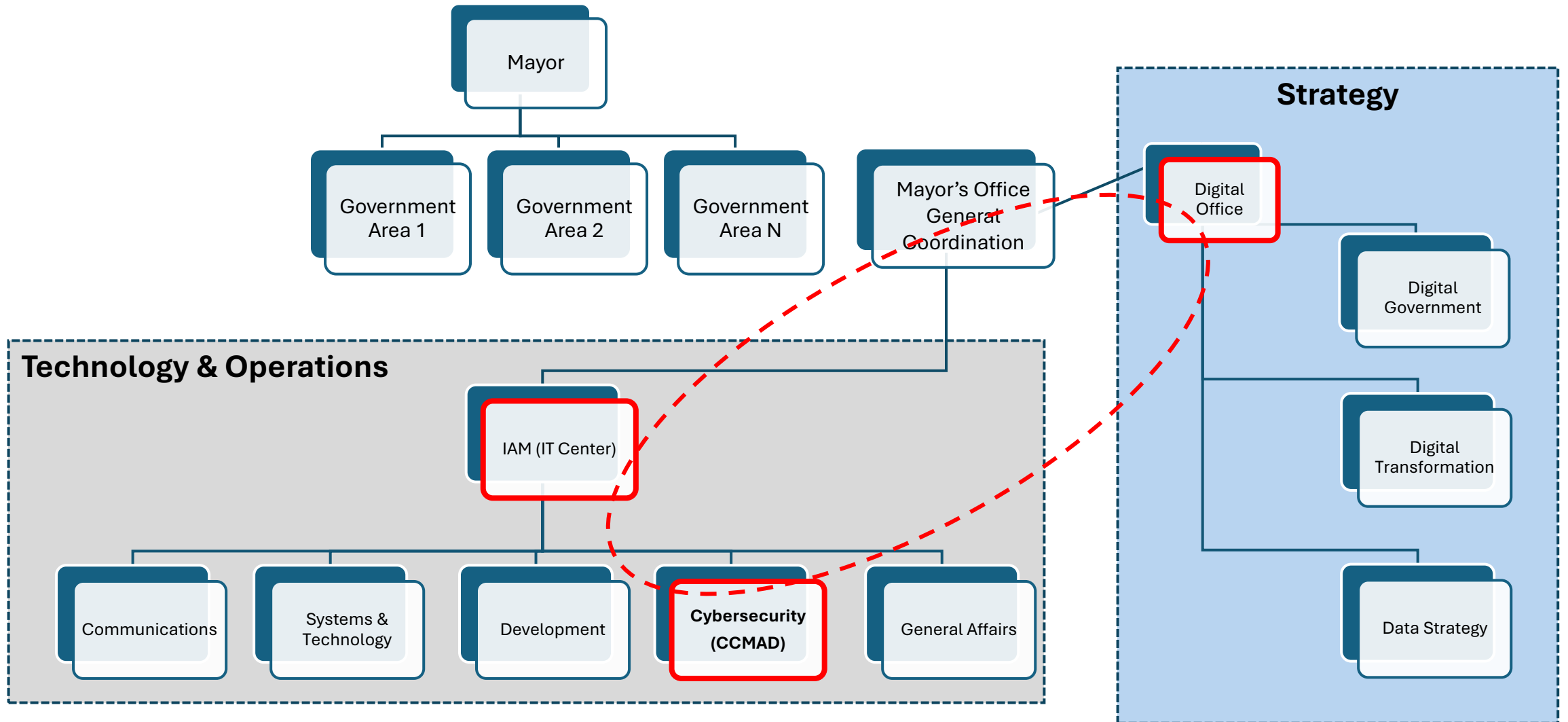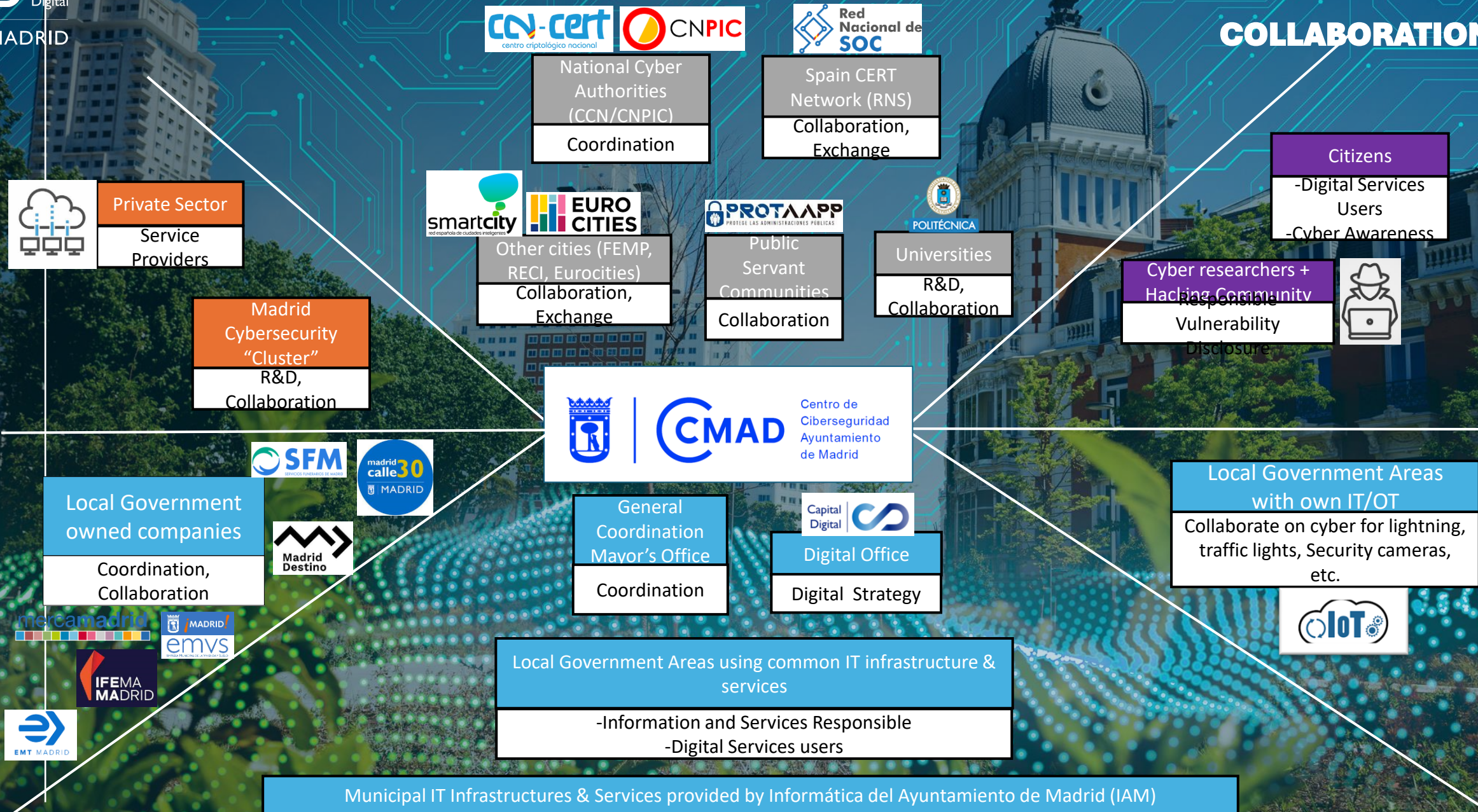
ORGANISATION CHART / CISO POSITION

GRC ONLY?

¡NO!

GRC — Governance, Compliance, Risk management

+

Security Operations Center (SOC)

OWN VS. CONTRACTED STAFF

OUTSOURCING

IN-HOUSE SOLUTION

CCN-CERT
centro criptológico nacional

COCS
Centro de Operaciones de Ciberseguridad

AndalucíaCERT
CENTRO DE SEGURIDAD TIC

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

AGÈNCIA DE CIBERSEGURETAT DE CATALUNYA

Private
Public

ROOTED CON

PROT
AAPP
PROTEGE LAS ADMINISTRACIONES PÚBLICAS

COLLABORATION

Cybersecurity Center of the Madrid City Council

The **Cybersecurity Center of the Madrid City Council** (**CCMAD**) is an organic unit, with the rank of deputy general directorate, attached to the Autonomous Information Technology Agency of the Madrid City Council, which provides cybersecurity services to the Government Areas and Autonomous Agencies of the City Council, with the mission of strengthening the protection of municipal digital management in the face of the exponential growth of threats in cyberspace.

Scope and Services

Cyber surveillance	Threat and Vulnerability Intelligence	Monitoring, detection, and response to cybercriminals	Security Architectures and Technologies
Regulatory compliance	Training, Awareness and Dissemination	Technical Audits	Electronic Identity for municipal personnel and systems

Community of users to whom the services are provided

Directly   Indirectly

- The Government Areas of the Madrid City Council
- The Autonomous Bodies of the City Council
- The more than 27,000 municipal employees and more than 3,000 external workers.

Website and Social Networks

https://madrid.es/ciberseguridad

https://twitter.com/ccmad21

Participating in conferences

CCN-CERT congress

RootedCON

C1b3rwall (National Police School)

Congreso CNIS

Spanish Smart Cities Network (RECI)

Eurocities

Women4cyber

KEY INSIGHTS

1. Cybersecurity strategy ALIGNED with city digital transformation strategy

2. CISO as a senior executive with RESOURCES

3. CISO near the trenches

4. COLLABORATE, COLLABORATE, COLLABORATE