

SIA and the Cybersecurity Centre of the Madrid City Council (CCMAD)

Comprehensive cybersecurity services to reinforce the protection of municipal digital management in the face of the exponential growth of threats in cyberspace.



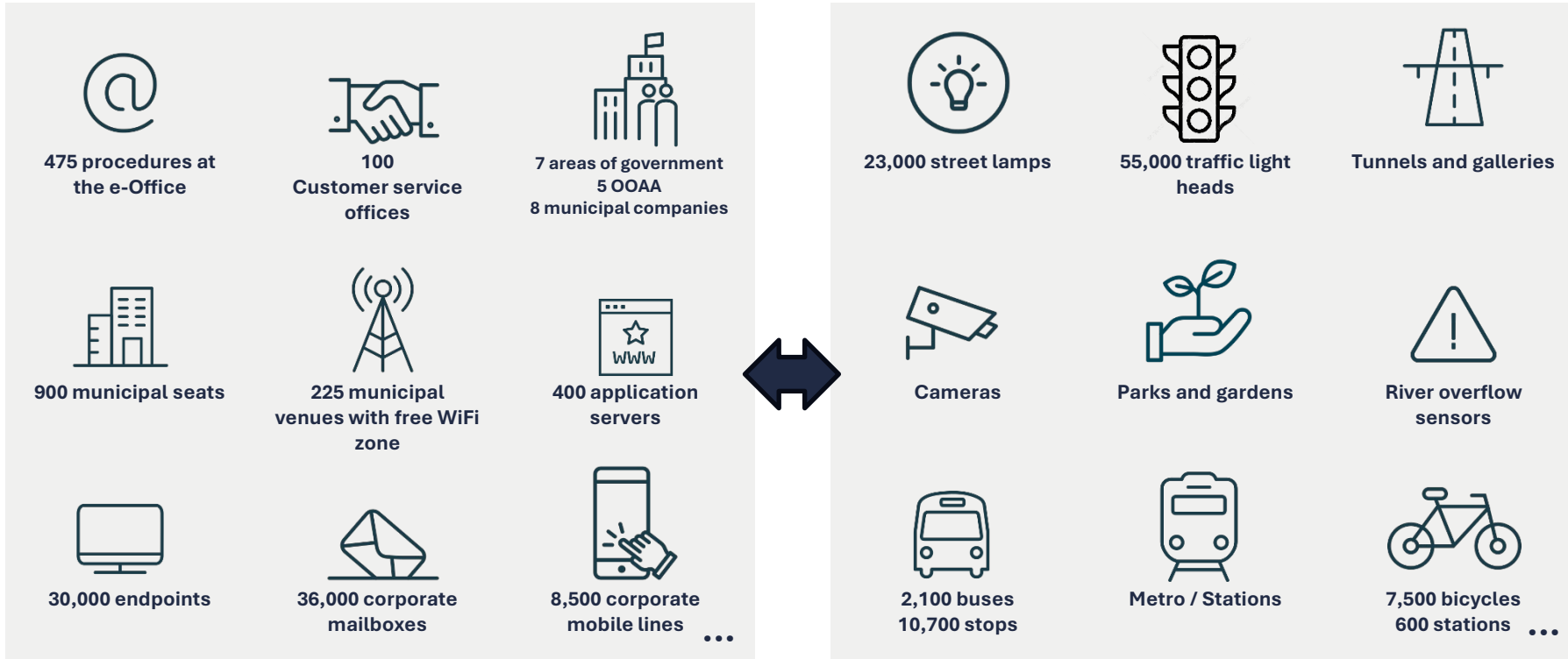
Capital
Digital

01.

Cybersecurity in Madrid City Council



Madrid is a great city with a digitalisation strategy

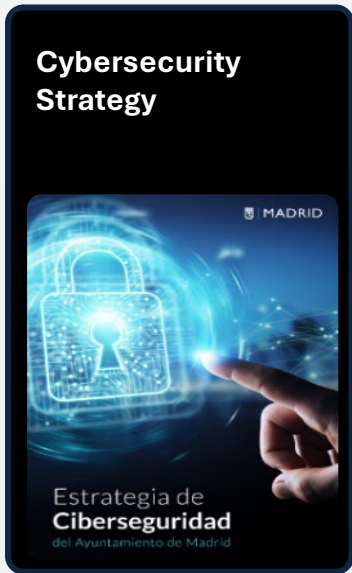


Digital Transformation Strategy 2023-2027



Centre for Cybersecurity (CCMAD)

The **Cybersecurity Centre of the Madrid City Council** is a unit dependent on the Madrid City Council's IT Department (IAM).



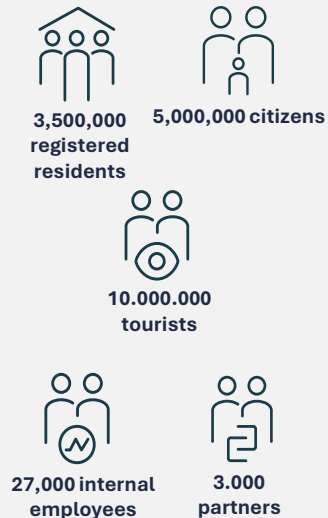
What are its objectives?

- Ensure the cybersecurity of its user community by providing **prevention, detection and response services**.
- **Point of contact** at the City Hall with cyber authorities and researchers.
- Work to disseminate the **culture of cybersecurity** (employees, collaborators and citizens in general).

What services does it provide?

- Digital surveillance
- Monitoring, detection and response to cyber incidents
- Technical vulnerability audits
- Security architectures and technologies
- ICT compliance
- Cybersecurity culture
- Training and awareness
- Digital Identity

To whom?





New advanced cybersecurity services contract

- Focus: **SERVICES** (2 lots):
 - Lot 1: Comprehensive cybersecurity services
 - Lot 2: Targeted cyber-attack service (Red Team)
- Start: 1 September 2023 (2+3)
- Amount: EUR 2 million per year

LOTE 1: Servicios integrales de ciberseguridad

- **Prestación 1 Operaciones de ciberseguridad:**
 - 1.1 Vigilancia digital
 - 1.2 Monitorización y detección de alertas de seguridad
 - 1.3 Respuesta ante incidentes de seguridad
 - 1.4 Búsqueda proactiva de amenazas
 - 1.5 Análisis forense
 - 1.6 Respuesta a ciber crisis
 - 1.7 Operación de herramientas de ciberseguridad
- **Prestación 2 Seguridad en infraestructuras y desarrollo:**
 - 2.1 Asesoramiento tecnológico
 - 2.2 Pruebas integradas en el ciclo de desarrollo
- **Prestación 3 Auditorías técnicas de ciberseguridad:**
 - 3.1 Análisis de vulnerabilidades automatizado
 - 3.2 Auditoría manual de activos
- **Prestación 4 Gobierno y cumplimiento:**
 - 4.1 Planificación estratégica de ciberseguridad
 - 4.2 Información del estado de la seguridad en Madrid
 - 4.3 Asesoramiento en cumplimiento TIC
 - 4.4 Asesoramiento en cumplimiento RGPD y normativa relevante
 - 4.5 Producción normativa
 - 4.6 Gestión de riesgos en terceros
- **Prestación 5 Cultura de ciberseguridad:**
 - 5.1 Concienciación
 - 5.2 Difusión
 - 5.3 Organización de eventos

LOTE 2: Servicios de realización de ciberataques dirigidos (Red Team)

02.

SIA's response to boost
cybersecurity in the city of Madrid



Cybersecurity is not a commodity, is a continuous process

CYBERSECURITY IS A CROSS-FUNCTIONAL...

No digitisation without cyber security

... TO BE CONSIDERED FROM THE DESIGN...

Cybersecurity should be incorporated into processes, from their design, by analysing technological and cyber risks and incorporating measures and controls to mitigate them.

... AND REQUIRES CONSTANT EVOLUTION

Continuous adaptation of processes and tools that support them is necessary to respond to rapidly advancing tactics, techniques and procedures of cybercriminals.

Smart MDR

Advanced, agile and flexible end-to-end SIA solution



An Indra company



Smart MDR: advanced prevention, detection and response

The objective of our services is to **quickly identify and limit the impact of security incidents** on companies, with measurable results that help to continuously improve the resilience of the organisation.

In a 24x7 collaborative work cycle, for continuous improvement...

We bring complementary capabilities that work as a single team and collaborate with IAM to maximise results. We measure key service parameters to improve effectiveness and efficiency.

Governance and cybersecurity reporting / Cyber exercises



An Indra company

... from intelligence information...



We detect threats moving on the Internet (targeted or generic) that can affect IAM and contain them.

Threat Intelligence

... we detect threats...



From automated and orchestrated threat monitoring scenarios

Security Monitoring

Supplemented by proactive threat scanning

Automated and manual threat hunting

And the deployment of simulated environments for the identification of insider attackers.

Deception

... and we respond



We provide context to alerts to drastically reduce the number of false positives, notify, propose containment actions and provide advanced response capabilities if necessary.

- First response
- Crisis management
- Digital Forensic & Incident Response

+ operation, administration and exploitation of security tools

Protecting infrastructures and information in IT / OT / Cloud / On Premise / Hybrid Environments





Complementary services

Governance and Compliance

We identify the rules and regulations that must be complied with (ENS, GDPR, NIS2, Al...) and support how they should be implemented in IAM, including the controls that allow the monitoring of their compliance.

- Strategic cybersecurity planning
- Information on the state of security in Madrid
- ICT compliance advice
- Advice on GDPR compliance and relevant regulations
- Regulatory production
- Third party risk management



Smart MDR



An Indra company



Mission control



Threat Intelligence



Detection



Response

Infrastructure security and development

We introduce security into the software lifecycle from design.

- Technological advice
- Definition of security requirements
- Training
- Integrated testing in the development cycle

Cybersecurity technical audits

We identify the attack surface, communicate new vulnerabilities that may affect IAM, prioritise them and propose how to address them.

- Early warning
- Automated vulnerability management
- Manual audit of assets

Cybersecurity culture

People are the first line of defence in an organisation.

Training and awareness raising is critical.

- Awareness-raising
- Broadcasting
- Organisation of events



Impact

Madrid City Council's Cybersecurity Centre and SIA protect the Spanish capital from cyber-attacks

SIA

An Indra company



Protection

Directly to:

- 7 areas of government
- 5 autonomous bodies
- 27,000 internal employees
- 3,000 employees

Indirectly to

- 3.5 million registered inhabitants
- 5 million citizens
- 10 million tourists



Agility and efficiency in responding to cyber-incidents

Smart MDR alerts incidents in less than 15 minutes and reduces false positives to less than 2%.



A leap in maturity in cybersecurity management

Protection mechanisms and high availability of municipal services are improved, which benefits people who live, work, visit or invest in Madrid.



Responds to the Strategic Plan

The service allows Madrid City Council to advance in its Digital Transformation Strategy 2023-2027, in which cybersecurity has its own strategic plan.

Thank you very much for your attention



Capital
Digital