MADRID

Cybersecurity **Strategy**

City Council of Madrid

The city of Madrid has immersed itself in a major digital transformation process. For this reason, the City Council of Madrid wishes to integrate this global process of digital transformation which affects affects all government areas in the regulatory and legislative framework and also its services, taking into account the security and cybersecurity information requirements which they are subject to.

The digital transformation processes of organisations are clearly showing the dependency that their corporate services and processes, whether critical or not, have on information and communications systems. In addition, this digital transformation process has been accelerated by the economic context and especially by the global context caused by COVID-19, which has further accelerated this digital transformation process.

Thousands of new "digital citizens" joining the digital society and an incessant technological innovation that is revolutionising daily processes, are causing the digital risk to increase significantly, and the great dependence on technology in all these changes means that the impact of this digital risk will skyrocket.

In addition, we are also in a growing context of interconnectivity of the different technological environments (IT, OT, IoT, CT, etc.), which only increases the probability of an incident occurring.

In turn, the current context of constant increase in cybersecurity incidents that affect all types of organisations, regardless of their size, is one of the main risk factors for the operation of the City Council of Madrid.

It is in this global context in which the different national and European bodies and institutions are carrying out regulatory activity aimed at minimising this impact and probability as much as possible, in order to guarantee the operational resilience of organisations in general, and those that provide essential and/or critical services in particular.

The transposition into the Spanish legislation of the European NIS directive through Royal Decree 12/2018 and its implementing Regulations approved by Royal Decree 43/2021, the recent update of Royal Decree 311/2022 of the National Security Scheme or the revision of the NIS directive itself do nothing other than verify the concern that at a European and Spanish level this risk poses for the national and European economy, and they come to focus on the protection of essential services for the functioning of the countries that make up the European economic area, essential services among which are those provided by the Public Administrations.

Therefore, guaranteeing compliance with the regulatory framework and the regulatory framework on cybersecurity is a fundamental objective for the City Council of Madrid. However, it is not a mere compliance objective, instead it is about protecting the services they provide. It is therefore necessary to define a Security Governance model that identifies the needs of the City Council of Madrid from the point of view of corporate information, technology, processes and people.

The result is the design of the Cybersecurity Strategy of the City Council of Madrid, a set of initiatives aimed at improving the level of corporate Cybersecurity in the IT environment, thus increasing the capacity for management, operation, surveillance and action against possible cyberthreats.

As part of this Strategy, City Council of Madrid IT, the body responsible for digital technologies, has created the "Cybersecurity Center of the City Council of Madrid"

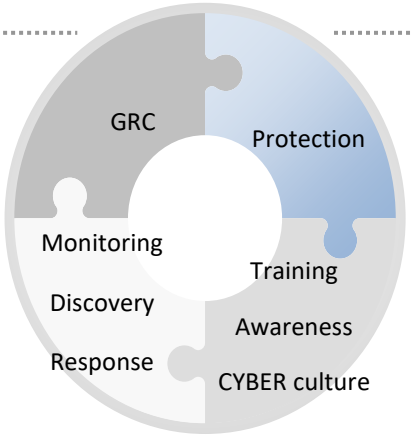
as the backbone of the City Council's capacities for prevention, monitoring, surveillance and response to cyber-incidents. aspiring to become an international reference for cybersecurity in large cities (taking into account the new possibilities, but also risks, that the implementation of 5G networks will bring with the millions of connections between machines, IoT), in collaboration with the National Cryptological Center. The Cybersecurity Center extends the scope of action to all municipal infrastructures and companies that provide services and is integrated into the National Network of Cybersecurity Operations Centers in order to increase the confidence of citizens and companies in the city's public services.

Key objectives

CMAD Centro de Ciberseguridad Ayuntamiento de Madrid

1. Develop a Cybersecurity Government, Risk and Compliance model for the City

2. Improve the degree of Protection of City services



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

4. Promote Training, Awareness and promote the CYBER culture of the City

GRC Model

P01.01 — Obligation compliance of ENS, LPIC and R.D.. Law 12/2018
P01.02 — Spread government information security to all areas of the government and OOPP.
P01.03 — Processes and procedures for a continuous cycle of identification and risk processing
P01.04 — Development of an inventory of suppliers for their valuation
P01.05 — Council cybersecurity INTEGRAL control panel
P01.06 — Business continuation plan

Protecting the City

P02.01 — Define protection requirements in IT and OT networks/systems (Baselined)
P02.02 — Security in the lifecycle of systems and developments
P02.03 —Security testing (pentesting and audiotronics)

Monitoring, detection and response

P03.01 — Distribution of advanced cybersecurity capacities (monitorisation, detection and response) in networks/IT systems and OT
P03.02 — Integration in the SOC's national network
P03.03 — CIBERCRISIS management plan by Madrid City Council

Training, awareness and CIBER culture

P04.01 — Training
P04.02 — Raising awareness
P04.03 — Broadcasting and communication of cybersecurity culture
P04.04 — Creation of a public-private ecosystem, around the theme of "Cibersecurity in Smart Cities"