MADRID

Estrategia de **Ciberseguridad**

del Ayuntamiento de Madrid

La ciudad de Madrid se encuentra inmersa en un importante proceso de transformación digital. Por ese motivo, el Ayuntamiento de Madrid desea integrar ese proceso global de transformación digital que afecta a todas sus áreas de gobierno en el marco normativo y legislativo que afecta a sus servicios, teniendo en cuenta los requisitos de seguridad de la información y ciberseguridad a los que los mismos están sujetos.

Los procesos de transformación digital de las organizaciones están evidenciando de manera patente la dependencia que sus servicios y procesos corporativos, sean críticos o no, tienen de los sistemas de información y de las comunicaciones. Además, ese proceso de transformación digital ha venido a acelerarse por el contexto económico y muy especialmente por el contexto mundial provocado por el COVID-19, lo que ha venido a acelerar aún más ese proceso de transformación digital.

Miles de nuevos "ciudadanos digitales" incorporándose a la sociedad digital y una incesante innovación tecnológica que está revolucionando los procesos cotidianos, están haciendo que el riesgo digital aumente sensiblemente, y la gran dependencia de la tecnología en todos estos cambios hace que el impacto de ese riesgo digital se dispare.

Además, nos encontramos también en un contexto creciente de interconectividad de los diferentes entornos tecnológicos (IT, OT, IoT, CT, etc.), que no hace sino aumentar la probabilidad de ocurrencia de un incidente.

A su vez, el contexto actual de incremento constante de los incidentes de ciberseguridad que afectan a todo tipo de organizaciones, con independencia de su tamaño, supone uno de los principales factores de riesgo para el funcionamiento del Ayuntamiento de Madrid.

Es en este contexto global en el que los diferentes organismos e instituciones nacionales y europeas están desarrollando una actividad normativa dirigida a minimizar en la medida de lo posible ese impacto y esa probabilidad, con objeto de garantizar la resiliencia operacional de las organizaciones en general, y de las que prestan servicios esenciales y/o críticos en particular.

La transposición a la legislación española de la directiva europea NIS a través del Real Decreto 12/2018 y su Reglamento de desarrollo aprobado por el Real Decreto 43/2021, la reciente actualización del Real Decreto 311/2022 de Esquema Nacional de Seguridad o la revisión de la propia directiva NIS no hacen otra cosa que constatar la preocupación que a nivel europeo y español supone este riesgo para la economía nacional y europea, y vienen a poner el foco en la protección de los servicios esenciales para el funcionamiento de los países que integran el espacio económico europeo, servicios esenciales entre los que se encuentran los prestados por las Administraciones Públicas.

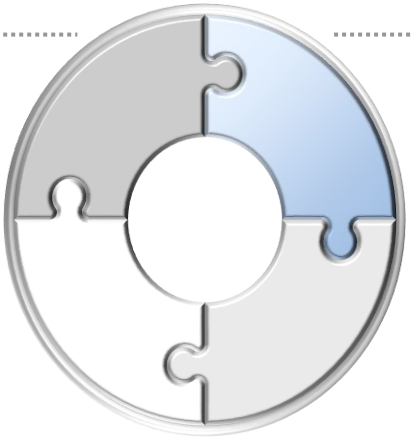
Por tanto, garantizar el cumplimiento del marco normativo y el marco regulador en materia de ciberseguridad es un objetivo fundamental para el Ayuntamiento de Madrid. Pero no se trata, que también, de un mero objetivo de cumplimiento, sino que se trata de proteger los servicios que prestan. Es necesario por tanto definir un modelo de Gobernanza de la Seguridad que identifique las necesidades del Ayuntamiento de Madrid desde el punto de vista de la información corporativa, de la tecnología, de los procesos y de las personas.

El resultado es el diseño de la Estrategia de Ciberseguridad del Ayuntamiento de Madrid, un conjunto de iniciativas orientadas a mejorar el nivel de la Ciberseguridad corporativa en el entorno IT, aumentando así la capacidad de gestión, de operación, de vigilancia y de actuación ante posibles ciberamenazas.

Dentro de esta Estrategia, Informática del Ayuntamiento de Madrid, organismo competente en materia de tecnologías digitales, ha creado el "Centro de Ciberseguridad del Ayuntamiento de Madrid" como elemento vertebrador de las capacidades de prevención, monitorización, vigilancia y respuesta ante ciberincidentes del Ayuntamiento, aspirando a convertirse en referencia internacional para la ciberseguridad en grandes ciudades (teniendo en cuenta las nuevas posibilidades, pero también riesgos, que traerán la implantación de las redes 5G con los millones de conexiones entre máquinas, IoT), en colaboración con el Centro Criptológico Nacional. El Centro de Ciberseguridad amplía el alcance de acción a todas las infraestructuras municipales y empresas que proporcionan servicios y se integra en la Red Nacional de Centros de Operaciones de Ciberseguridad con el fin de incrementar la confianza de la ciudadanía y las empresas en los servicios públicos de la ciudad.

Objetivos clave

CMAD Centro de Ciberseguridad Ayuntamiento de Madrid



1. Desarrollar un modelo de Gobierno, Riesgo y Cumplimiento de la Ciberseguridad de la Ciudad
2. Mejorar el grado de Protección de los servicios de la Ciudad
3. Reforzar las capacidades de monitorización, detección y respuesta de la Ciudad
4. Promover la Formación, Concienciación y fomentar la cultura CIBER de la Ciudad

Modelo GRC

- **P01.01 –** Cumplimiento de las obligaciones de ENS, LPIC y R.D. Ley 12/2018
- **P01.02 –** Extender el gobierno de la seguridad de la información a todas las áreas de gobierno y OOPP.
- **P01.03 –** Procesos y procedimiento para un ciclo continuo de Identificación y Tratamiento de Riesgos.
- **P01.04 –** Desarrollo de un inventario de proveedores de servicios para su valoración
- **P01.05 –** Cuadro de mando INTEGRAL ciberseguridad Ayto.
- **P01.06 –** Plan de continuidad de negocio.

Protección de la Ciudad

- **P02.01 –** Definir requisitos de protección en redes/sistemas IT y OT (Bastionado)
- **P02.02 –** Seguridad en el ciclo de vida de sistemas y desarrollos
- **P02.03 –** Pruebas de seguridad (pentesting y auditorías)

Monitorización, detección y respuesta

- **P03.01 –** Despliegue de capacidades avanzadas de ciberseguridad (monitorización, detección y respuesta) en redes/sistemas IT y OT.
- **P03.02 –** Integración en la red nacional de SOCs
- **P03.03 –** Plan de gestión de CIBERCRISIS del Ayuntamiento de Madrid

Formación, concienciación y Cultura CIBER

- **P04.01 –** Formación
- **P04.02 –** Concienciación
- **P04.03 –** Difusión y comunicación de la cultura de la ciberseguridad
- **P04.04** – Creación de un ecosistema público-privado, en torno a la temática de "Ciberseguridad en Smart Cities"