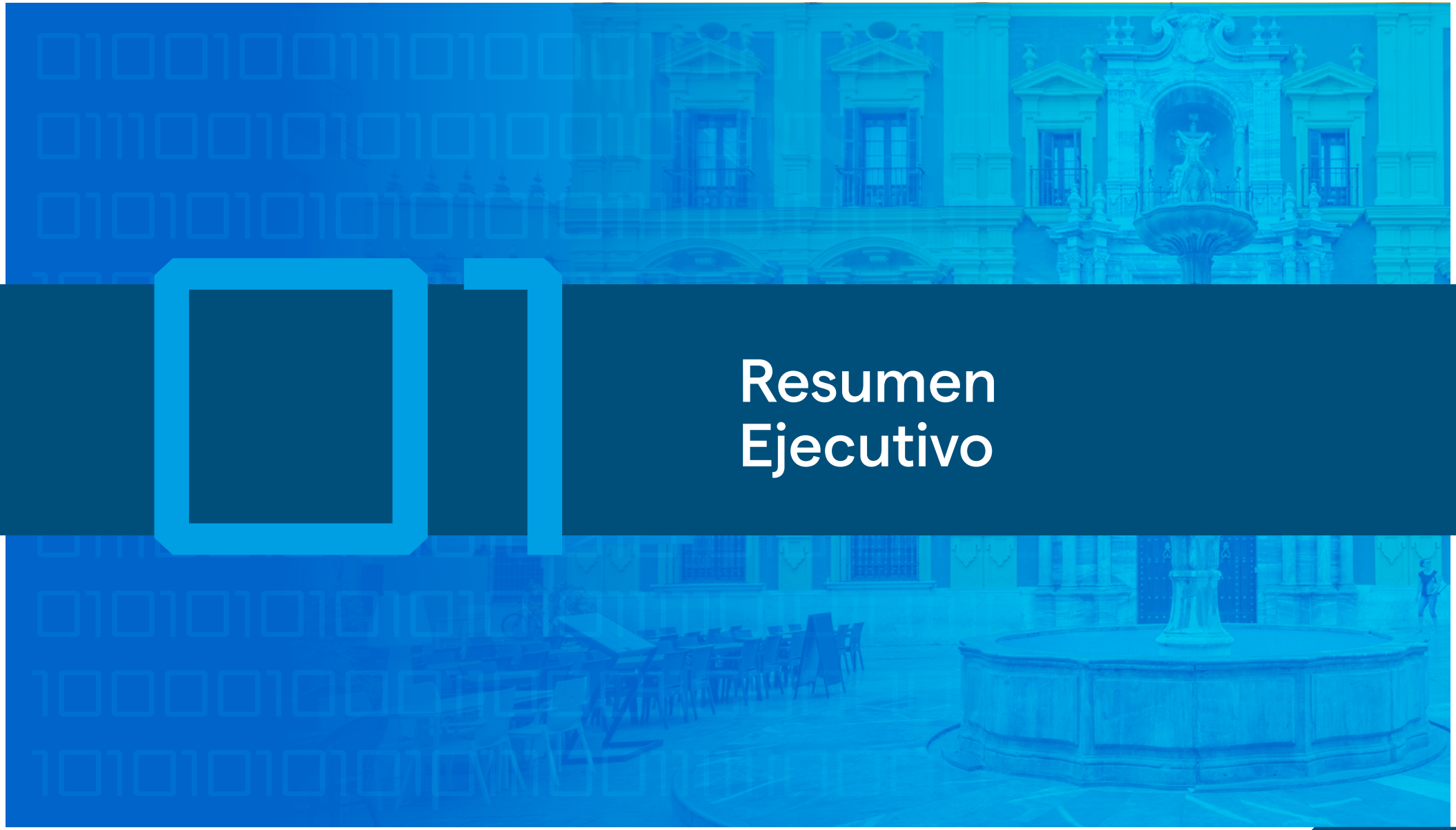
2024-2027

Estrategia de Ciberseguridad

Ciudad de Málaga

Ciudad de Málaga

Índice



01 Resumen Ejecutivo

El mundo se encuentra inmerso en una profunda transformación impulsada por la irrupción de nuevas tecnologías y la digitalización. Este nuevo paradigma da lugar a desafíos emergentes a los que deben dar respuesta todas las organizaciones. En este marco, los Estados, Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y sus organismos vinculados o dependientes deben concentrar sus esfuerzos en desarrollar e implementar estrategias de ciberseguridad que estén alineadas con las principales regulaciones y permitan avanzar hacia una sociedad digital segura y confiable.

El Ayuntamiento de Málaga, consciente del entorno digital actual, donde las ciberamenazas son cada vez más sofisticadas y frecuentes, apuesta por una transformación digital de sus sistemas y servicios. En esta transformación, la ciberseguridad desempeña un papel prioritario para garantizar la protección de los activos digitales y la continuidad de las operaciones críticas, así como para reforzar la confianza de la sociedad malagueña, contribuyendo al posicionamiento de Málaga como territorio líder en materia de ciberseguridad.

Para enfrentar esta realidad, el Ayuntamiento de Málaga, ha elaborado la **Estrategia de Ciberseguridad Ciudad de Málaga 2024-2027** (en adelante, Estrategia).

Este instrumento está diseñado basándose en un conjunto de principios orientados a la integración del liderazgo en materia de ciberseguridad, la colaboración con la sociedad civil, la seguridad desde el diseño y por defecto, la ciberresiliencia, la innovación y digitalización segura en los servicios públicos y la sensibilización y capacitación en ciberseguridad.

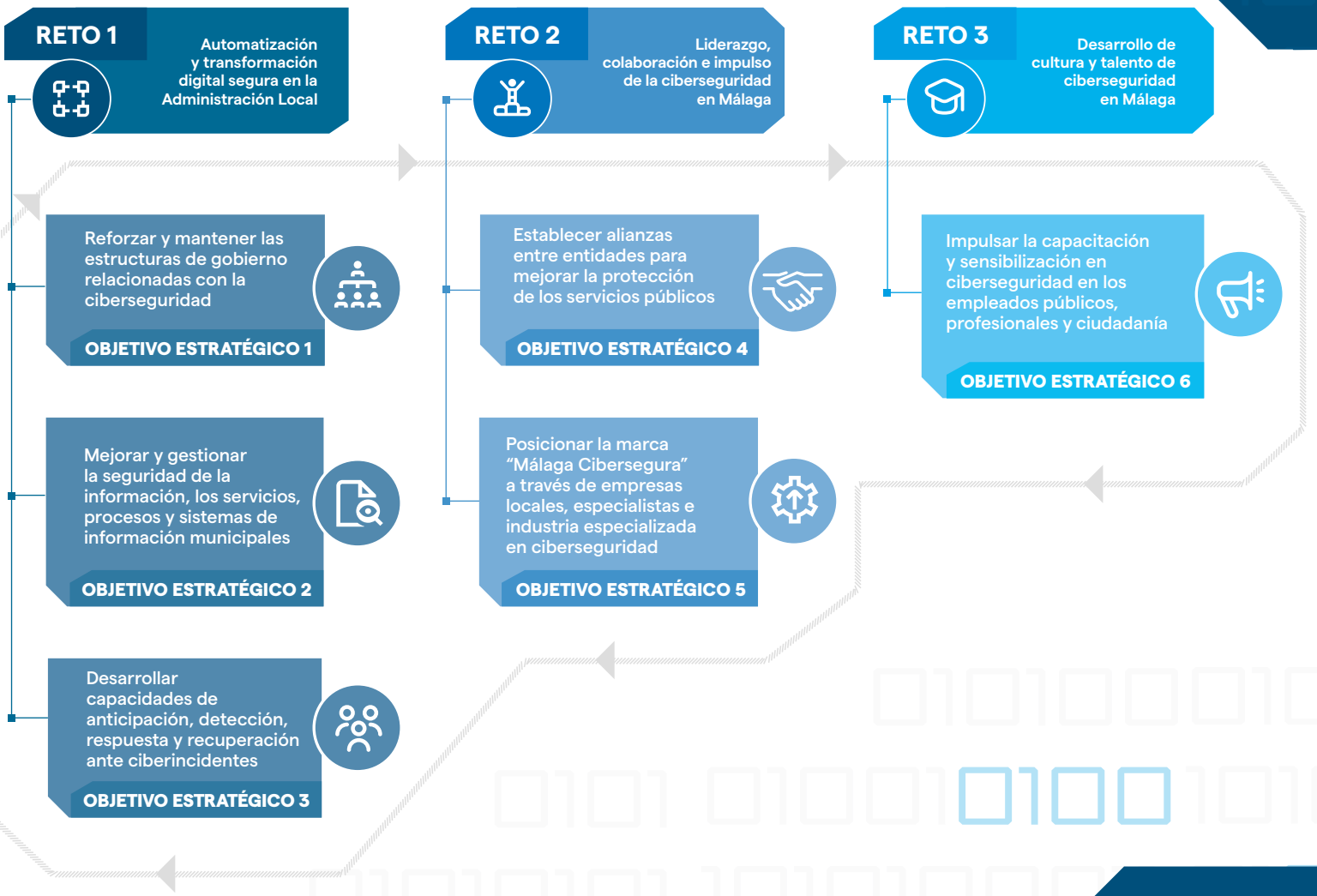
Principios de la Estrategia

1. Liderazgo en ciberseguridad
2. Colaboración con la sociedad civil
3. Seguridad desde el diseño y por defecto
4. Ciberresiliencia
5. Innovación y digitalización segura en los servicios públicos
6. Sensibilización y capacitación en ciberseguridad

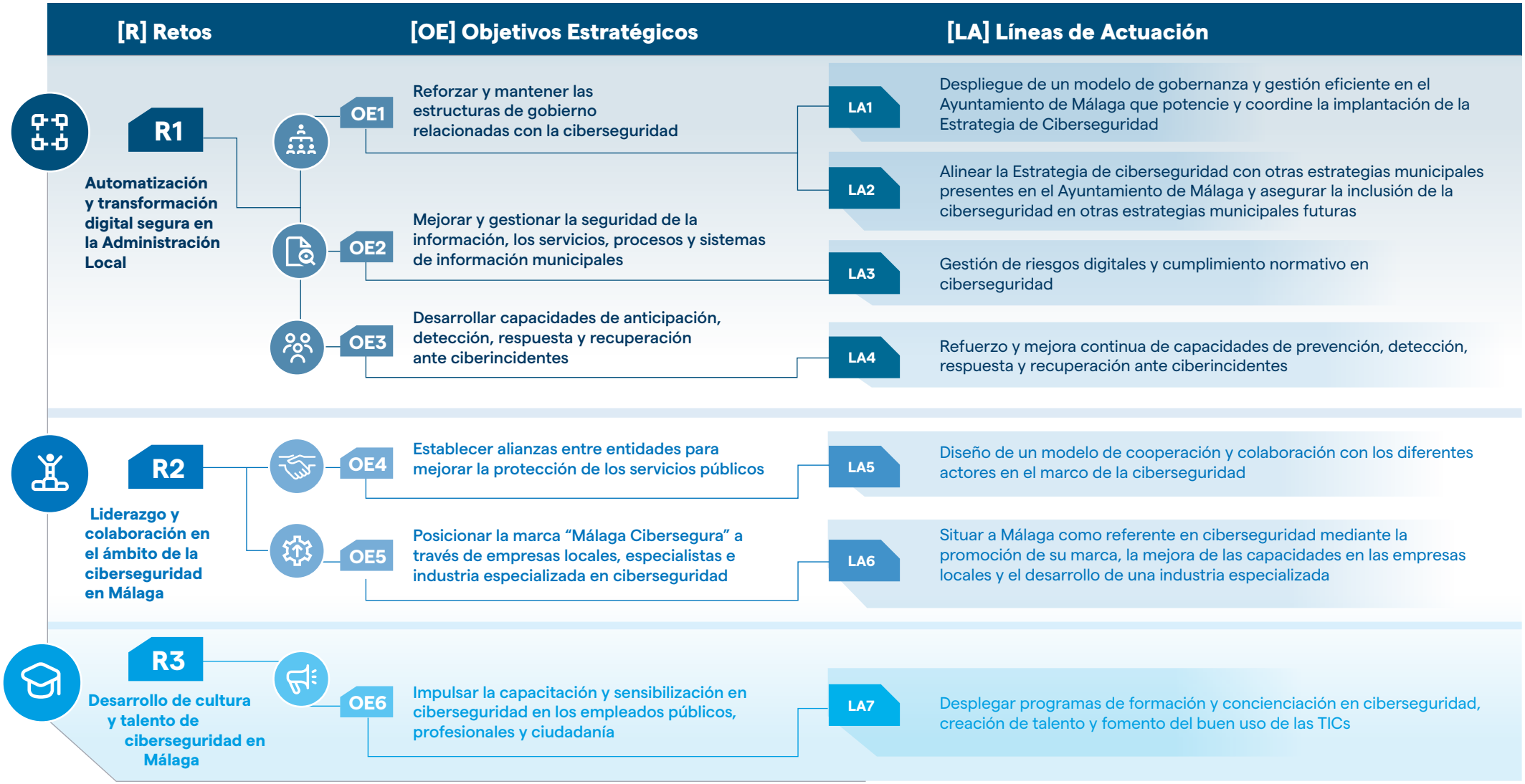
En este contexto, a través de esta Estrategia, se definen los retos, objetivos y líneas de actuación a seguir por el Ayuntamiento de Málaga para los años 2024-2027 en materia de ciberseguridad, involucrando a la Administración, la ciudadanía, el sector privado, las instituciones educativas y las entidades de referencia en este ámbito.

Dicha Estrategia identifica **tres grandes retos** a afrontar por el Ayuntamiento de Málaga, derivados de la digitalización y evolución tecnológica, a los cuales se les pretende dar respuesta para consolidar a Málaga como líder en el ámbito de la ciberseguridad.

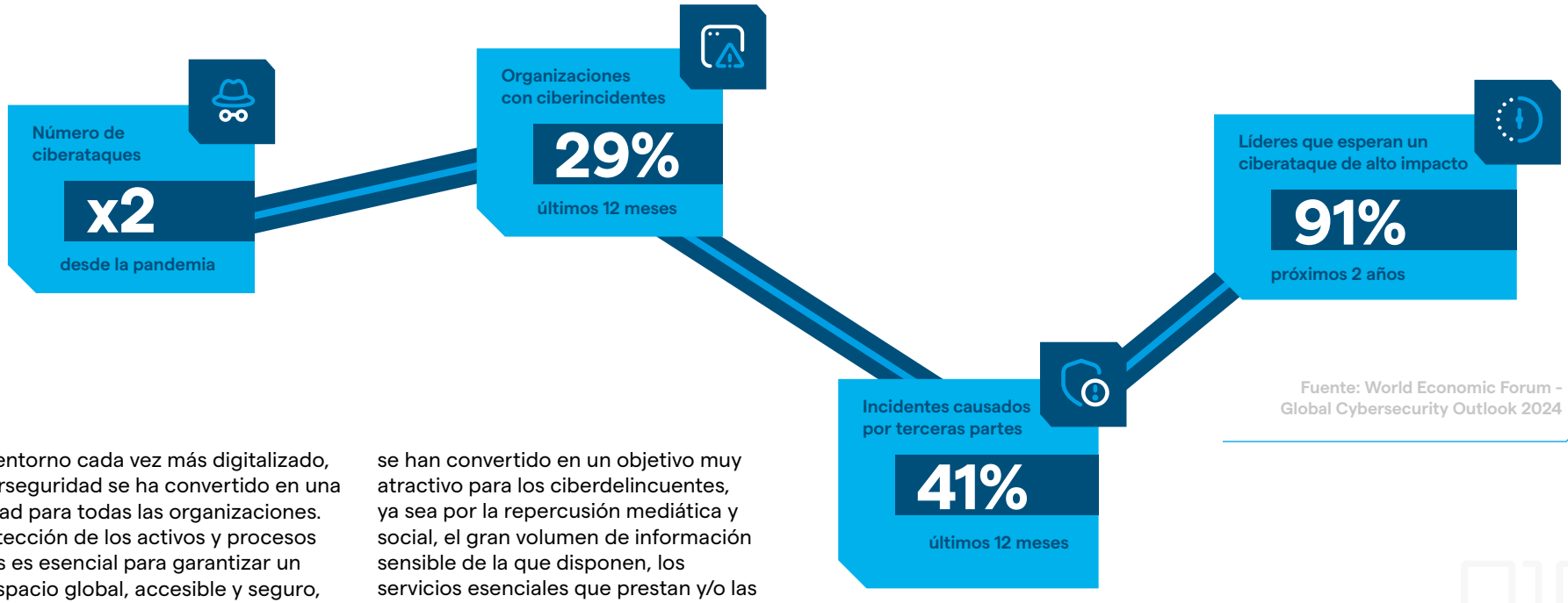
Asimismo, para abordar estos retos, la Estrategia define **seis objetivos** clave que se deben alcanzar durante su período de ejecución.



Alineado con los objetivos estratégicos, se establecen **siete líneas de actuación** que posibilitan su consecución, permitiendo a Málaga avanzar hacia una sociedad digital, segura y confiable, que la posicione como un territorio y economía líder en el sector:



02 Contexto global de la ciberseguridad



Fuente: World Economic Forum - Global Cybersecurity Outlook 2024

En un entorno cada vez más digitalizado, la ciberseguridad se ha convertido en una prioridad para todas las organizaciones. La protección de los activos y procesos críticos es esencial para garantizar un ciberespacio global, accesible y seguro, que sustente el buen funcionamiento de una economía digital y ofrezca garantías y confianza a la sociedad.

Asimismo, la fuerte dependencia en las tecnologías disruptivas y la hiperconectividad digital ha provocado que los ciberataques aumenten exponencialmente en los últimos años, afectando a todas las organizaciones, con un impacto particularmente significativo en las Administraciones Públicas, que se han convertido en un objetivo muy atractivo para los ciberdelincuentes, ya sea por la repercusión mediática y social, el gran volumen de información sensible de la que disponen, los servicios esenciales que prestan y/o las infraestructuras críticas en las que se soportan, lo que resalta la necesidad de fortalecer las medidas de ciberseguridad en todos los niveles.

Esta situación se vio agravada por los efectos de la pandemia que provocó una digitalización acelerada y masiva de los servicios públicos, ampliando así la superficie de exposición a potenciales ciberataques que contribuyen a dificultar la adecuada protección de la información.

De acuerdo con los resultados del informe *"Global Risks Report"*, del "World Economic Forum", a través de las respuestas obtenidas de más de un millar de colaboradores de una amplia red de expertos y líderes de diversas disciplinas y sectores, sobre los riesgos más significativos que el mundo podría enfrentar en el corto, mediano y largo plazo, la ciberseguridad ha pasado de ocupar la octava posición en 2023 a la cuarta en 2024, convirtiéndose en un desafío crítico que requiere una atención y acción concertada a nivel global, debido entre otros motivos, a la fuerte dependencia de la tecnología, el incremento en la frecuencia y severidad de los ciberataques, la evolución de las amenazas y la creciente regulación en torno a la privacidad y la ciberseguridad.

Fuente: World Economic Forum Global Risks Perception Survey 2023-2024

Con el objetivo de enfrentar este desafío, la Unión Europea (UE) ha llevado a cabo diferentes iniciativas en los últimos años, con el fin de adoptar medidas de seguridad para proteger los sistemas y redes, prestando especial atención a los operadores críticos y servicios esenciales.

Entre las más destacadas cabe mencionar la elaboración en 2020 de la denominada "Estrategia de Ciberseguridad de la UE para la Década Digital", cuyas principales líneas de actuación son: "aumentar la seguridad de los servicios esenciales y de los dispositivos conectados, reforzar las capacidades colectivas para responder a los principales ciberataques y cooperar con socios a nivel mundial para garantizar la seguridad internacional y la estabilidad en un ciberespacio global, abierto, estable y seguro, protegiendo los derechos humanos, las libertades fundamentales y los valores democráticos"[1]

A nivel nacional, el Consejo de Seguridad Nacional aprobó en 2019 la "Estrategia Nacional de Ciberseguridad" en la cual se establece la posición de España ante una nueva concepción de la ciberseguridad en el marco de la Política de Seguridad Nacional[2]. Alineada con la europea, esta Estrategia persigue fortalecer la coordinación a nivel nacional e internacional, proteger las infraestructuras críticas, mejorar la prevención y respuesta ante ciberamenazas y promover la cultura de ciberseguridad en la sociedad y las empresas.

Asimismo, en 2021, el Consejo de Ministros aprobó la "Estrategia de Seguridad Nacional"[3], en la que se refleja una visión integral de las amenazas y oportunidades para la seguridad nacional y, se establece un marco para la acción gubernamental en diversas áreas, entre las que se incluye la ciberseguridad.

Alineado con dicha Estrategia, el Departamento de Seguridad Nacional (DSN), elaboró el "Informe Anual de Seguridad Nacional", en el cual realiza una clasificación de los dieciséis riesgos establecidos en la Estrategia de Seguridad Nacional de 2021, ordenados de mayor a menor según la intensidad del riesgo, calculada mediante el producto del grado de probabilidad y el nivel de impacto, siendo 5 el valor máximo para cada uno de ellos. En el informe correspondiente al año 2023, la vulnerabilidad del ciberespacio o ciberseguridad se encuentra en segunda posición, solo por detrás de las campañas de desinformación.

[1] The EU's Cybersecurity Strategy for the Digital Decade. Fecha: Diciembre 2020. Autor: ENISA (https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0).

[2] Estrategia Nacional de Ciberseguridad 2019 Fecha: Abril 2019. Autor: Departamento de Seguridad Nacional. Ministerio de la Presidencia, Relaciones con las Cortes e Igualdad. (https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019).

[3] Estrategia de Seguridad Nacional 2021. Fecha: Diciembre 2021. Autor: Departamento de Presidencia del Gobierno. (https://www.dsn.gob.es/es/documento/estrategia-seguridad-nacional-2021).

Fuente: Departamento de Seguridad Nacional

DSN Informe Anual de Seguridad Nacional 2023	IMPACTO	PROBABILIDAD	INTENSIDAD DEL RIESGO
Campañas de desinformación	3,97	4,39	17,43
Vulnerabilidad del ciberespacio	4,14	4,19	17,35
Flujos migratorios irregulares	3,91	4,34	17,02
Tensión estratégica y regional	3,96	4	15,82
Terrorismo y radicalización violenta	3,90	3,79	14,81
Efectos del cambio climático y de la degradación del medio natural	3,7	3,9	14,74
Inestabilidad económica y financiera	3,76	3,74	14,08
Vulnerabilidad energética	3,80	3,69	14,06
Espionaje e injerencias desde el exterior	3,59	3,73	13,43
Emergencias y catástrofes	3,35	4	13,42
Crimen organizado y delincuencia grave	3,24	3,41	11,07
Amenazas a las infraestructuras críticas	3,58	3,03	10,87
Proliferación de armas de destrucción masiva	3,18	3	9,54
Vulnerabilidad del espacio marítimo	2,95	2,74	8,11
Epidemias y pandemias	3,17	2,54	8,05
Vulnerabilidad aeroespacial	2,89	2,64	7,66

Entre las principales regulaciones de referencia en materia de seguridad a nivel nacional cabe destacar las siguientes: >>

- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (ENS).
- Real Decreto 43/2021, de 26 de enero, por el que se desarrolla el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información (Directiva NIS).
- Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD).
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas (LPIC).
- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

En sintonía con las Estrategias europea y nacional, a nivel autonómico, Andalucía puso en marcha en 2022 su propia Estrategia de ciberseguridad para hacer frente a los retos derivados de la digitalización y evolución de las nuevas tecnologías. La "Estrategia Andaluza de Ciberseguridad" define un marco destinado a proteger los sistemas de información y las infraestructuras críticas, mejorar la prevención y respuesta ante amenazas y promover la cultura de ciberseguridad en la sociedad y las empresas andaluzas.

Igualmente, en el ámbito local, el Ayuntamiento de Málaga ha adoptado medidas para reforzar la ciberseguridad en su territorio, como viene siendo el impulso de la presente "Estrategia de Ciberseguridad Ciudad de Málaga", la cual establece objetivos claros para la protección de las infraestructuras críticas locales y la seguridad de los sistemas de información y servicios esenciales. Esta Estrategia municipal se centra en diversos aspectos esenciales tales como el aumento de las capacidades de ciberseguridad, la cooperación entre entidades públicas y privadas, y la formación y concienciación en ciberseguridad para todos los actores implicados. A su vez, también fomenta la innovación tecnológica y la implementación de medidas preventivas para garantizar un entorno digital seguro y resiliente en todo el territorio malagueño.

En resumen, las estrategias mencionadas con anterioridad convergen en su objetivo de reforzar la ciberseguridad, impulsar la colaboración y fomentar la ciberresiliencia frente a las crecientes amenazas emergentes.

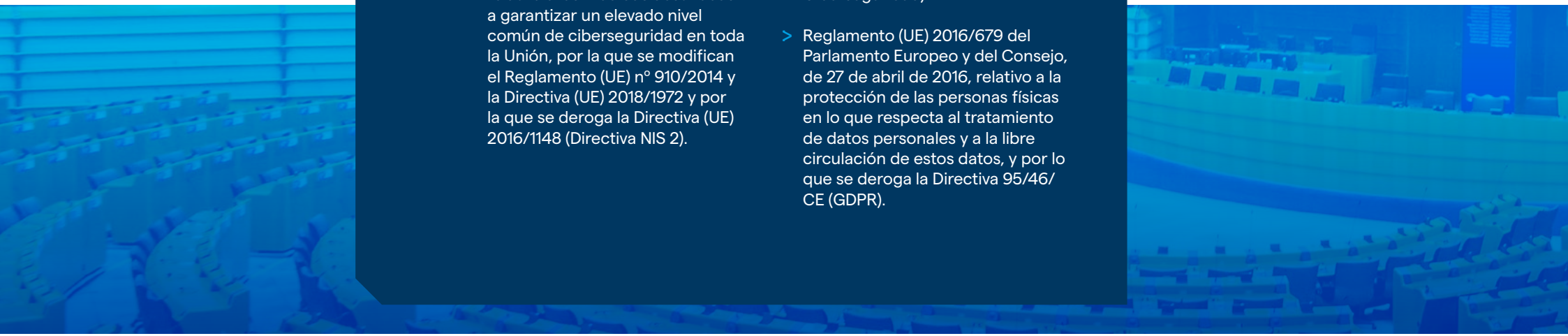
En este ámbito, es importante señalar que tanto el marco regulatorio como las normativas en ciberseguridad, tanto a nivel nacional como internacional, también han evolucionado de manera continua para adaptarse al dinámico entorno digital actual.

Por otro lado, las principales regulaciones de referencia en materia de seguridad en el ámbito de la Unión Europea son las siguientes:

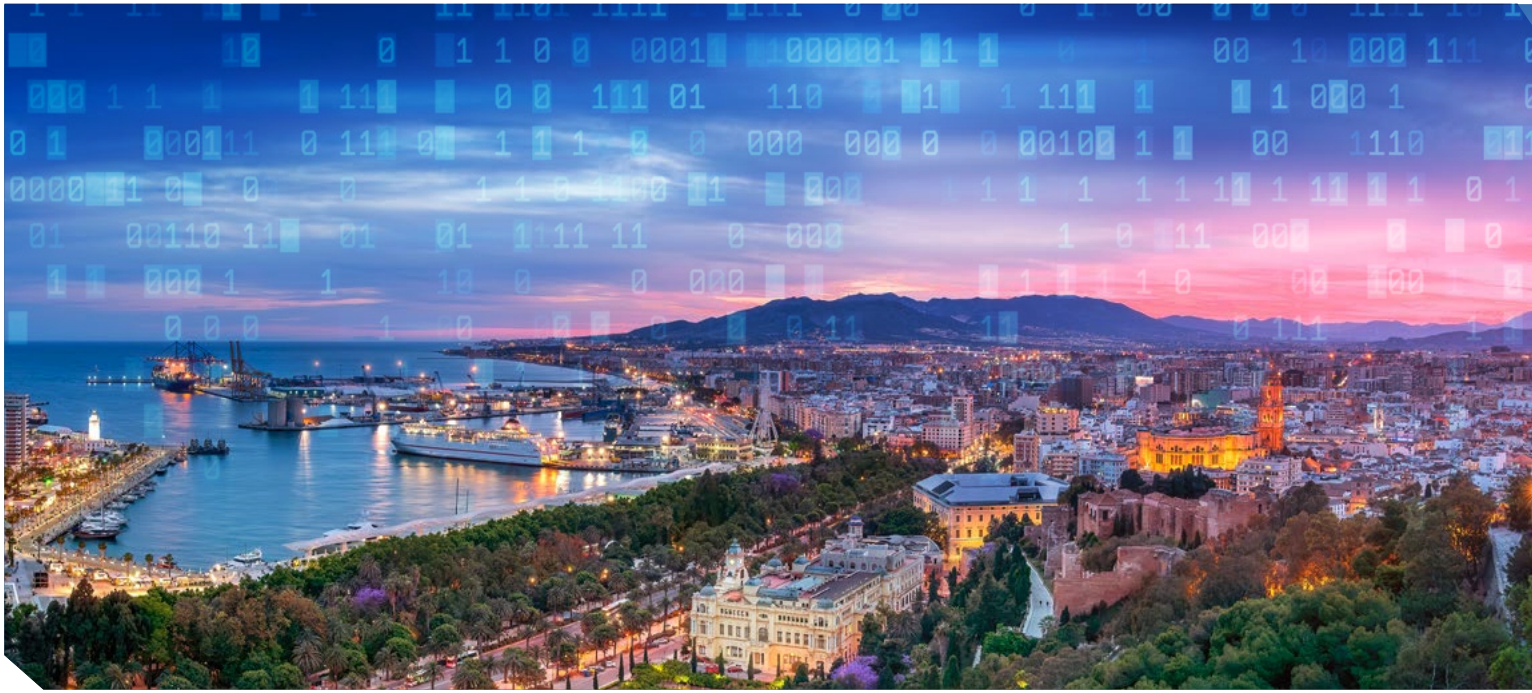
- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, relativo a las medidas para fomentar el desarrollo y la adopción de una IA segura y fiable en todo el mercado único de la UE, por la que se modifican los Reglamentos (CE) nº 300/2008, (UE) nº 167/2013, (UE) nº 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) nº 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva NIS 2).
- Directiva (UE) 2022/2557 del Parlamento Europeo y del Consejo de 14 de diciembre de 2022 relativa a la resiliencia de las entidades críticas y por la que se deroga la Directiva 2008/114/CE del Consejo (Directiva CER).
- Reglamento (UE) 2019/881 del Parlamento Europeo y del Consejo, de 17 de abril de 2019 relativo a ENISA (Agencia de la Unión Europea para la Ciberseguridad) y a la certificación de la ciberseguridad de las tecnologías de la información y la comunicación y por el que se deroga el Reglamento (UE) 526/2013 (Reglamento sobre la Ciberseguridad).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por lo que se deroga la Directiva 95/46/CE (GDPR).

De acuerdo con lo mencionado anteriormente, podemos decir que la sociedad actual se encuentra en medio de una transformación global impulsada por la irrupción de nuevas tecnologías y la digitalización.

Este nuevo paradigma da lugar a nuevos retos y desafíos a los que deben dar respuesta las organizaciones. En este marco, los gobiernos y organismos públicos deben concentrar sus esfuerzos en desarrollar e implementar estrategias de ciberseguridad que estén alineadas con las principales regulaciones, con el fin de garantizar el uso seguro de sistemas, servicios esenciales y redes e infraestructuras críticas, que respalden los sectores estratégicos del mundo actual y, permitan avanzar hacia una sociedad digital segura y confiable.



03 Situación actual de la Ciudad de Málaga



En la transformación digital, la ciberseguridad debe ser en una prioridad crítica para las instituciones públicas y privadas. El Ayuntamiento de Málaga, como entidad gestora de servicios esenciales para la ciudadanía, no es ajeno a esta realidad. La creciente dependencia de tecnologías de la información y la comunicación (TIC) para la Administración Local y la prestación de servicios municipales conlleva un aumento en la exposición a ciberamenazas que pueden comprometer la integridad, disponibilidad y confidencialidad de la información.

En respuesta a estos desafíos el Ayuntamiento de Málaga ha impulsado en los últimos años diversas iniciativas y colaboraciones significativas de partenariado público-privado que han contribuido a consolidar a la ciudad como un referente en el ámbito de la innovación digital y la ciberseguridad. En este contexto, una de las iniciativas más destacadas fue la creación del Málaga TechPark, anteriormente conocido como Parque Tecnológico de Andalucía (PTA).

Este parque tiene como objetivo fomentar la innovación, el desarrollo tecnológico y la colaboración entre empresas, universidades e instituciones públicas y privadas. En consecuencia, Málaga TechPark se ha convertido en un epicentro para la innovación tecnológica en la capital malagueña.

Otra de las iniciativas más relevantes con ubicación en Málaga, impulsada en los últimos años desde la Junta de Andalucía, fue la creación del Centro de Ciberseguridad de Andalucía (CIAN), el cuál nació con el objetivo de coordinar la Estrategia Andaluza de Ciberseguridad y fortalecer la protección digital en la región. Adicionalmente, este centro alberga el Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía, así como diferentes espacios para ofrecer servicios específicos a la ciudadanía, empresas privadas e instituciones públicas en el ecosistema digital andaluz.

Unos meses después de la creación de este centro, se lanzó el Clúster de Ciberseguridad de Andalucía, ubicado también en Málaga. Este clúster integra empresas, asociaciones e instituciones que trabajan para favorecer el desarrollo del ecosistema andaluz en el ámbito de la ciberseguridad, facilitando el intercambio de conocimientos y fomentando la creación de alianzas estratégicas que impulsen el desarrollo de nuevas tecnologías de protección.

En línea con la creación del clúster, cabe mencionar la reciente inauguración en Málaga del *Google Safety Engineering Center* (GSEC), como centro de ciberseguridad de referencia en Europa. Este espacio se ha convertido en un punto internacional de ciberseguridad, en el que colaboran gobiernos, empresas y expertos europeos para mejorar la ciberseguridad a través del desarrollo de habilidades digitales avanzadas, discusiones sobre buenas prácticas, compartición de investigaciones y conocimientos y creación de herramientas que combatan amenazas cibernéticas sofisticadas.

En este contexto, Málaga se posiciona como lugar clave para el intercambio de conocimientos en ciberseguridad mediante la creación de diversas comunidades y foros especializados. En 2024, la ciudad de Málaga fue sede del I Foro de Ciberseguridad ISMS Forum Andalucía, organizado por ISMS Forum, una de las entidades sin ánimo de lucro más relevantes en el ámbito nacional para la promoción de la seguridad de la información y la protección de datos personales. Además, también tuvo lugar el I Foro de Mujeres Cyber-Líderes de Andalucía donde se abordaron temas relacionados con la ciberseguridad y el papel de la mujer en este campo. Este foro se centra en promover la igualdad de género en el sector de la ciberseguridad, fomentando un espacio de intercambio, reflexión y encuentro sobre las necesidades de formación, talento y visibilidad profesional en este ámbito.

Asimismo, cabe destacar el desarrollo de convenios que han permitido colaboraciones con diversas entidades, como la Universidad de Málaga (UMA) y el Instituto Nacional de Ciberseguridad de España (INCIBE), entre otras, para dar lugar a una mejora continua de las capacidades de ciberseguridad a nivel local y nacional con el desarrollo de nuevas técnicas y tecnologías que mejoren la seguridad de los sistemas de información, servicios esenciales e infraestructuras críticas del sector público y privado.

Por último, se debe mencionar la apuesta por la promoción y visualización de la ciberseguridad del Ayuntamiento de Málaga, a través de congresos y eventos en este ámbito, ya sea como organizador, patrocinador o participante de los mismos, con el fin de hacer del territorio malagueño el punto de encuentro de expertos, profesionales e interesados en la ciberseguridad para compartir conocimientos, discutir sobre tendencias y presentar las últimas innovaciones en el campo.

Por todo lo mencionado con anterioridad, podemos afirmar que en los últimos años Málaga ha ratificado su liderazgo en el sector tecnológico y de ciberseguridad, acompañada en este ecosistema por otros enclaves de innovación en el territorio andaluz.

Asimismo, el panorama de la ciberseguridad, tanto en el marco europeo, nacional, autonómico, como en ciudades específicas como Málaga, está marcado por nuevos y complejos desafíos. Para enfrentar esta realidad, el Ayuntamiento de Málaga ha elaborado la Estrategia de Ciberseguridad Ciudad de Málaga para los años 2024-2027.

Este instrumento ha sido diseñado para consolidar la ciberseguridad como un pilar estratégico dentro de la ciudad, asegurando así una protección robusta y eficiente frente a las ciberamenazas emergentes y posicionando la marca Málaga en el ámbito tecnológico y de ciberseguridad.

04 Propósito y principios de la Estrategia

El Ayuntamiento de Málaga, consciente del entorno digital actual, donde las ciberamenazas son cada vez más sofisticadas y frecuentes, apuesta por una transformación digital de sus sistemas y servicios. En esta transformación, la ciberseguridad desempeña un papel prioritario para garantizar la protección de los activos digitales y la continuidad de las operaciones críticas, así como para reforzar la confianza de la sociedad malagueña, contribuyendo al posicionamiento de Málaga como territorio líder en materia de ciberseguridad.

PROPÓSITO

La Estrategia tiene como propósito establecer la ciberseguridad como un pilar fundamental en la Ciudad de Málaga, incluyendo el Ayuntamiento, empresas locales, profesionales independientes y ciudadanía.

Para ello, se ha definido una hoja de ruta que servirá de guía durante los próximos años para proteger eficazmente las infraestructuras y sistemas digitales locales. Se prestará especial atención a los operadores críticos, los servicios esenciales, y los sectores clave del Ayuntamiento, asegurando así la continuidad de los servicios públicos y fortaleciendo la confianza de la ciudadanía. Con esta iniciativa, se busca además situar a Málaga como referente, a nivel nacional e internacional, en el estado del arte de la ciberseguridad y la transformación digital.

Principios de la Estrategia

1. **Liderazgo en ciberseguridad**
2. **Colaboración con la sociedad civil**
3. **Seguridad desde el diseño y por defecto**
4. **Ciberresiliencia**
5. **Innovación y digitalización segura en los servicios públicos**
6. **Sensibilización y capacitación en ciberseguridad**

La Estrategia se fundamenta en seis principios clave, que velan por el desarrollo e implementación efectiva de la misma.

PRINCIPIOS DE LA ESTRATEGIA

1 2 3 4 5 6

Liderazgo en ciberseguridad

El principio de liderazgo en ciberseguridad destaca la importancia de una dirección estratégica y comprometida para establecer un entorno digital seguro y colaborativo que permita garantizar la integridad, confidencialidad y disponibilidad de los activos del Ayuntamiento. Este principio subraya la necesidad de que los líderes impulsen la ciberseguridad como una prioridad, estableciendo un enfoque de gestión de riesgos que permita definir políticas claras, asignar recursos adecuados, implantar tecnologías avanzadas, promover una cultura de seguridad en todos los niveles y desarrollar planes de respuesta y recuperación ante ciberincidentes.

Un liderazgo efectivo en ciberseguridad garantiza que se tomen decisiones informadas con una orientación proactiva para enfrentar y gestionar los riesgos, asegurando así la protección integral de los activos digitales y la continuidad de las operaciones.

1 2 3 4 5 6

Colaboración con la sociedad civil

El principio de colaboración con la sociedad civil pone foco en la importancia de cooperar y coordinar esfuerzos entre diferentes organizaciones, agencias gubernamentales, redes de ciudades y entidades locales para mejorar la ciberseguridad. La sociedad civil incluye entre otros, expertos, ciudadanía, empresas, academias, asociaciones y colegios profesionales. Este enfoque promueve el intercambio de información sobre amenazas, mejores prácticas y recursos, facilitando una respuesta más efectiva ante un ciberincidente y fortaleciendo la protección contra potenciales ataques. Al colaborar con la sociedad civil se puede aprovechar conocimientos colectivos y capacidades complementarias, creando una red de defensa más robusta y adaptativa frente a los retos y desafíos derivados de la digitalización. La colaboración optimiza la capacidad para anticipar, identificar y mitigar riesgos, asegurando una postura de seguridad más sólida y resiliente.

PRINCIPIOS DE LA ESTRATEGIA

1 2 **3** 4 5 6

Seguridad desde el diseño y por defecto

El principio de seguridad desde el diseño y por defecto establece que la seguridad debe estar integrada desde el inicio del ciclo de vida de cualquier proceso, sistema y/o servicio. Este enfoque de la ciberseguridad en primer plano plantea cambiar la perspectiva sobre la seguridad de una postura reactiva a una proactiva. Este cambio es esencial para cualquier entidad que busque no solo proteger sus activos, sino también fomentar la innovación y la transformación digital.

El Ayuntamiento de Málaga, operando bajo un modelo de seguridad por diseño y por defecto, propone en esta Estrategia la construcción de un modelo centrado en la confianza a fin de impulsar proyectos ambiciosos de transformación digital. Este modelo asegura que cada iniciativa esté construida sobre una base segura, permitiendo que la innovación se desarrolle de manera rápida y segura. De este modo se garantiza que la seguridad esté integrada en la arquitectura y funcionamiento del sistema y servicios del Ayuntamiento, abordando posibles vulnerabilidades de manera proactiva y reduciendo el riesgo de brechas de seguridad. Implementar este principio contribuirá a construir soluciones más seguras y ciberresilientes desde el principio, minimizando la necesidad de costosas correcciones y ajustes posteriores.

1 2 3 **4** 5 6

Ciberresiliencia

El principio de ciberresiliencia se centra en la capacidad del Ayuntamiento para anticipar, resistir, responder y recuperarse ante un ciberincidente con el menor impacto posible.

Cabe mencionar que, la ciberresiliencia no solo se enfoca en prevenir ataques, sino también en mantener la continuidad de las operaciones y restaurar la funcionalidad rápidamente en caso de un ciberataque.

Por ello, el Ayuntamiento debe tener planes y procedimientos de gestión de crisis en ciberseguridad bien definidos e implementados periódicamente, sistemas de respaldo robustos, y una estrategia integral que permita adaptarse y recuperarse de manera eficiente ante eventos de seguridad no deseados. Implementar la ciberresiliencia ayudará a garantizar la operabilidad efectiva de los servicios públicos asegurando su disponibilidad para la ciudadanía, minimizando la interrupción de sus actividades y reduciendo el impacto en sus operaciones críticas.

PRINCIPIOS DE LA ESTRATEGIA

1 2 3 4 **5** 6

Innovación y digitalización segura en los servicios públicos

El principio de innovación y digitalización segura subraya la necesidad de actualizar y perfeccionar constantemente los servicios y sistemas públicos para dar respuesta a las necesidades actuales y futuras de la ciudadanía malagueña, mejorando la eficiencia, accesibilidad y calidad de los servicios públicos, así como asegurando al mismo tiempo la protección de los datos y la privacidad de la ciudadanía. Este enfoque promueve la adopción de nuevas tecnologías, como *Cloud Computing*, *Big Data*, hiperautomatización e Inteligencia Artificial (IA) o Internet de las cosas (IoT), entre otras, acompañadas de medidas técnicas y organizativas en el ámbito de la ciberseguridad. No debemos olvidar la importancia de la innovación en Málaga como Ciudad Inteligente (*Smart City*) y de la protección de sus sensores digitales para la mejora de la calidad de vida de su ciudadanía.

La integración de la innovación y digitalización segura implica evaluar regularmente el estado de los servicios, identificar áreas de mejora y aplicar ajustes para abordar potenciales vulnerabilidades. Adoptar este principio asegura que los servicios públicos prestados por el Ayuntamiento de Málaga se mantengan a la vanguardia en términos de calidad y seguridad, proporcionando un valor añadido a la ciudadanía y adaptándose proactivamente a los desafíos emergentes.

1 2 3 4 5 **6**

Sensibilización y capacitación en ciberseguridad

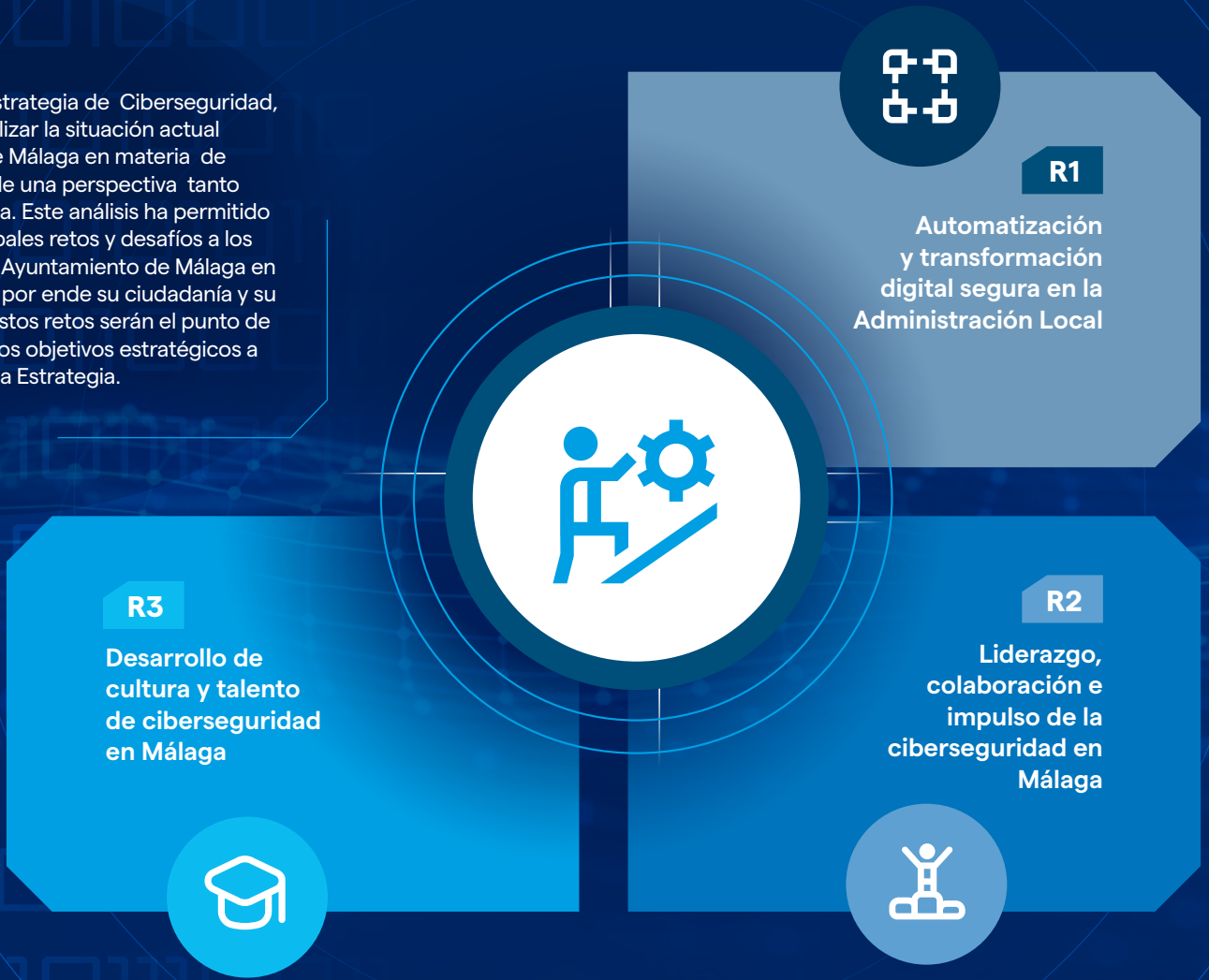
El principio de sensibilización y capacitación en ciberseguridad se enfoca en la creación y/o fortalecimiento de la cultura en torno a la seguridad digital entre la ciudadanía y las organizaciones de la Ciudad de Málaga, así como entre el personal del Ayuntamiento.

Esto implica fomentar la conciencia y la educación sobre la ciberseguridad, promoviendo comportamientos seguros y responsables en el uso de las tecnologías digitales. Fomentar la cultura y formación en ciberseguridad permitirá a la sociedad comprender la importancia de proteger la información y los sistemas digitales contra ciberamenazas, contribuyendo a un entorno digital más seguro y ciberresiliente en todo el territorio malagueño.

05 Retos de la ciberseguridad en la Ciudad de Málaga

RETOS DE LA CIBERSEGURIDAD EN LA CIUDAD DE MÁLAGA

Para desarrollar la Estrategia de Ciberseguridad, es fundamental analizar la situación actual del Ayuntamiento de Málaga en materia de ciberseguridad desde una perspectiva tanto interna como externa. Este análisis ha permitido identificar los principales retos y desafíos a los que se enfrentará el Ayuntamiento de Málaga en los próximos años, y por ende su ciudadanía y su tejido empresarial. Estos retos serán el punto de partida para definir los objetivos estratégicos a abordar a través de la Estrategia.



RETOS DE LA CIBERSEGURIDAD EN LA CIUDAD DE MÁLAGA

R1 Automatización y transformación digital segura en la Administración Local

La automatización y la transformación digital segura en la Administración Local implican la implementación de tecnologías avanzadas y procesos hiperautomatizados para mejorar la eficiencia, la transparencia y la accesibilidad de los servicios públicos. Esto requiere una infraestructura tecnológica actualizada, capacitación continua del personal, y políticas claras que aseguren la privacidad y seguridad de la información ciudadana.

Asimismo, la adopción de estas tecnologías también implica una mayor exposición ante un ciberataque y un aumento de potenciales brechas de seguridad, que pueden poner en riesgo los datos sensibles y la privacidad de la ciudadanía. Por ello, resulta indispensable que el Ayuntamiento, centre sus esfuerzos en la implantación de medidas robustas de ciberseguridad, como, por ejemplo, la encriptación de datos, la autenticación multifactor y la capacitación del personal, con el objetivo de generar confianza en la ciudadanía, empresas malagueñas y entidades locales.

R2 Liderazgo, colaboración e impulso de la ciberseguridad en Málaga

El reto de liderazgo, colaboración e impulso de la ciberseguridad en Málaga radica en la necesidad de coordinar esfuerzos entre múltiples actores, tanto públicos y privados como profesionales independientes y ciudadanía, para crear un ecosistema digital seguro. Este desafío implica que el Ayuntamiento tome la iniciativa en el establecimiento de políticas de colaboración efectivas, mientras que las empresas privadas malagueñas y las instituciones deben participar activamente en el desarrollo e implementación de soluciones innovadoras. La colaboración es importante para compartir información sobre amenazas y mejores prácticas, así como para fomentar la capacitación continua de todos los involucrados.

Por ello, Málaga debe enfrentar estos retos con una visión integradora que promueva la sinergia entre el Ayuntamiento de Málaga, la ciudadanía, el sector privado, el sector educativo y las entidades de referencia en este ámbito, garantizando así la protección de su infraestructura digital y el bienestar de sus ciudadanos en un mundo cada vez más interconectado y vulnerable a las ciberamenazas.

R3 Desarrollo de cultura y talento de ciberseguridad en Málaga

La creciente complejidad de las ciberamenazas y la rápida expansión tecnológica demandan no solo medidas de seguridad para proteger los activos de información, sino también el fomento de una cultura de ciberseguridad integral en el Ayuntamiento, empresas locales, profesionales y ciudadanía.

Este desafío implica la coordinación y apoyo a la implementación de estrategias educativas y formativas desde temprana edad o a sectores específicos de la ciudadanía (por ejemplo. adolescentes) con objeto de concienciar y formar en ciberseguridad fomentando el talento y promoviendo el conocimiento y las competencias necesarias para afrontar las amenazas actuales y futuras. Además, busca establecer alianzas entre instituciones académicas, empresas, organismos públicos y profesionales especializados para facilitar el desarrollo de programas y proyectos innovadores que fortalezcan la capacidad de la ciudad para responder a los retos de la ciberseguridad, posicionando a Málaga como territorio atractivo para la creación y atracción de talento especializado en esta área.

05 Objetivos estratégicos

OBJETIVOS ESTRATÉGICOS

Para abordar los retos identificados, la Estrategia define **seis objetivos** clave que se deben alcanzar durante su período de ejecución. El propósito es que el Ayuntamiento de Málaga se consolide como líder en el ámbito de la ciberseguridad.

RETO 1

Automatización y transformación digital segura en la Administración Local

- Reforzar y mantener las estructuras de gobierno relacionadas con la ciberseguridad
  OBJETIVO ESTRATÉGICO 1
- Mejorar y gestionar la seguridad de la información, los servicios, procesos y sistemas de información municipales
  OBJETIVO ESTRATÉGICO 2
- Desarrollar capacidades de anticipación, detección, respuesta y recuperación ante ciberincidentes
  OBJETIVO ESTRATÉGICO 3

RETO 2

Liderazgo, colaboración e impulso de la ciberseguridad en Málaga

- Establecer alianzas entre entidades para mejorar la protección de los servicios públicos
  OBJETIVO ESTRATÉGICO 4
- Posicionar la marca "Málaga Cibersegura" a través de empresas locales, especialistas e industria especializada en ciberseguridad
  OBJETIVO ESTRATÉGICO 5

RETO 3

Desarrollo de cultura y talento de ciberseguridad en Málaga

- Impulsar la capacitación y sensibilización en ciberseguridad en los empleados públicos, profesionales y ciudadanía
  OBJETIVO ESTRATÉGICO 6

OBJETIVOS ESTRATÉGICOS

R1

Reforzar y mantener las estructuras de gobierno relacionadas con la ciberseguridad

OBJETIVO ESTRATÉGICO 1

Este objetivo se centra en reforzar las capacidades organizativas para gestionar la ciberseguridad de manera efectiva. El fin perseguido es mejorar las estructuras de gobierno que supervisan la ciberseguridad en el Ayuntamiento de Málaga y mantener actualizados los roles y sus responsabilidades asociadas.

El propósito es construir una base sólida de gobernanza para proteger los activos esenciales (información municipal y servicios de negocio), garantizando una respuesta ágil y adecuada ante cualquier posible incidente de seguridad de la información.

OBJETIVOS ESTRATÉGICOS

R1

Mejorar y gestionar la seguridad de la información, los servicios, procesos y sistemas de información municipales

OBJETIVO ESTRATÉGICO 2

Este objetivo se centra en optimizar la gestión de los riesgos asociados con las amenazas digitales, la gestión normativa de ciberseguridad interna y de la cadena de suministro, así como el cumplimiento riguroso de las normativas y estándares vigentes.

El propósito es proporcionar al Ayuntamiento de Málaga un estado de situación actualizado de los riesgos digitales de los diferentes negocios municipales, así como el estado de cumplimiento de los diferentes marcos legales de ciberseguridad de la gestión de la normativa interna de ciberseguridad, de cara a que todos los empleados la conozcan y la entiendan.

R1

Desarrollar capacidades de anticipación, detección, respuesta y recuperación ante ciberincidentes

OBJETIVO ESTRATÉGICO 3

Este objetivo se enfoca en fortalecer las capacidades para anticipar, identificar y gestionar las potenciales ciberamenazas que afectan a los sistemas y servicios públicos digitales, así como aquellas que llegan a materializarse en un incidente en el Ayuntamiento de Málaga y/o sus entes instrumentales.

El fin perseguido es mejorar las medidas de prevención para reducir la exposición a riesgos, optimizar las herramientas y procesos de anticipación y detección para identificar ataques a tiempo, y mejorar las capacidades de respuesta para manejar eficazmente los incidentes y mitigar su impacto.

Ciudad de Málaga

OBJETIVOS ESTRATÉGICOS

R2

Establecer alianzas entre entidades para mejorar la protección de los servicios públicos

OBJETIVO ESTRATÉGICO 4

Este objetivo busca fomentar la cooperación entre el Ayuntamiento de Málaga, la ciudadanía, el sector privado, el sector educativo y otras entidades de referencia para ampliar la capacidad de ciberseguridad. Para ello, se deben establecer alianzas estratégicas que fortalezcan la ciberseguridad en todos los niveles, mejorando simultáneamente las capacidades de protección del Ayuntamiento, así como las del sector privado y la ciudad en general.

La colaboración permitirá compartir recursos, conocimientos y mejores prácticas, asegurando una defensa más eficiente y eficaz ante un ciberataque.

R2

Posicionar la marca "Málaga Cibersegura" a través de empresas locales, especialistas e industria especializada en ciberseguridad

OBJETIVO ESTRATÉGICO 5

Este objetivo se centra en posicionar a Málaga como líder en el ámbito de la ciberseguridad mediante la difusión de logros y éxitos de las empresas y profesionales del sector, definiendo e implementando un conjunto de acciones para fomentar el crecimiento de la industria de ciberseguridad y el fortalecimiento de las capacidades en materia de ciberseguridad de las empresas locales de Málaga.

Para lograr dicho objetivo, el Ayuntamiento de Málaga debe trabajar en crear un ecosistema favorable y de confianza, proporcionando canales de asesoramiento sobre temas de interés, como, financiación, capacitación empresarial, innovación segura y emprendimiento local, permitiendo a las empresas locales y profesionales que mejoren y se adapten a las nuevas demandas del sector.

Esto no solo generará un atractivo entorno económico para la inversión y la innovación dentro de la industria, sino que también aumentará la visibilidad de Málaga.

OBJETIVOS ESTRATÉGICOS

R3

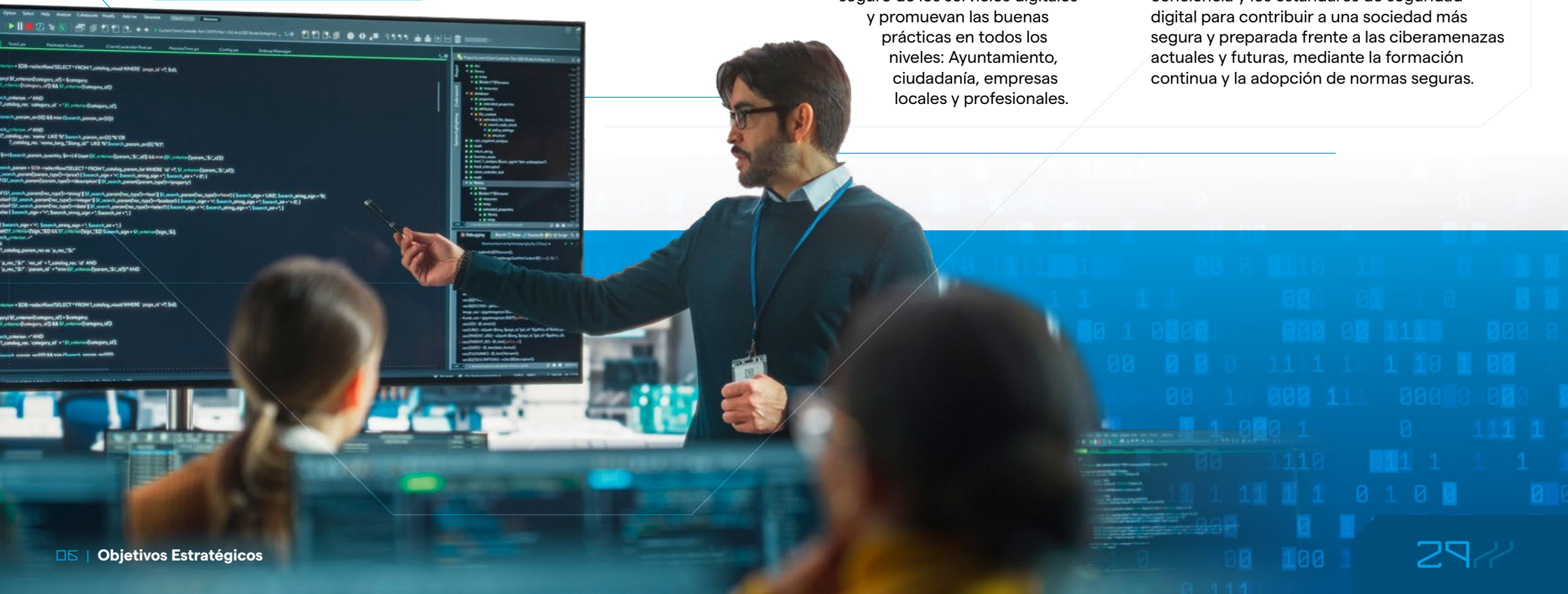
Impulsar la capacitación y sensibilización en ciberseguridad en los empleados públicos, profesionales y ciudadanía

OBJETIVO ESTRATÉGICO 6

Este objetivo consiste en fortalecer las habilidades en ciberseguridad mediante el desarrollo y promoción de planes y programas formativos con contenidos específicos para los distintos perfiles de profesionales y ciudadanía, así como buscar consolidar una cultura de ciberseguridad a través de acciones de concienciación que garanticen el uso seguro de los servicios digitales y promuevan las buenas prácticas en todos los niveles: Ayuntamiento, ciudadanía, empresas locales y profesionales.

Asimismo, se debe fomentar el interés y vocación en ciberseguridad desde edades tempranas para contar con recursos especializados que nos permitan crear talento en ciberseguridad a nivel local.

El fin es mejorar las competencias en ciberseguridad de los empleados públicos, profesionales y ciudadanía, elevando la conciencia y los estándares de seguridad digital para contribuir a una sociedad más segura y preparada frente a las ciberamenazas actuales y futuras, mediante la formación continua y la adopción de normas seguras.



07 Líneas de actuación

LÍNEAS DE ACTUACIÓN

A continuación, se describen las diferentes líneas de actuación que permitirán alcanzar los objetivos estratégicos establecidos. Cabe mencionar que, cada línea de actuación está compuesta por un conjunto de actividades clave diseñadas para enfrentar los desafíos actuales de la sociedad malagueña.

En conjunto, todas las líneas de actuación cubren uno de los objetivos establecidos.

RETO 1

- Reforzar y mantener las estructuras de gobierno relacionadas con la ciberseguridad — **OBJETIVO ESTRATÉGICO 1**
  - Despliegue de un modelo de gobernanza y gestión eficiente en el Ayuntamiento de Málaga que potencie y coordine la implantación de la Estrategia de Ciberseguridad. → **LÍNEA DE ACTUACIÓN 1**
  - Alinear la Estrategia de ciberseguridad con otras estrategias municipales presentes en el Ayuntamiento de Málaga y asegurar la inclusión de la ciberseguridad en otras estrategias municipales futuras. → **LÍNEA DE ACTUACIÓN 2**
- Mejorar y gestionar la seguridad de la información, los servicios, procesos y sistemas de información municipales — **OBJETIVO ESTRATÉGICO 2**
  - Gestión de riesgos digitales y cumplimiento normativo en ciberseguridad. → **LÍNEA DE ACTUACIÓN 3**
- Desarrollar capacidades de anticipación, detección, respuesta y recuperación ante ciberincidentes — **OBJETIVO ESTRATÉGICO 3**
  - Refuerzo y mejora continua de capacidades de prevención, detección, respuesta y recuperación ante ciberincidentes. → **LÍNEA DE ACTUACIÓN 4**

RETO 2

- Establecer alianzas entre entidades para mejorar la protección de los servicios públicos — **OBJETIVO ESTRATÉGICO 4**
  - Diseño de un modelo de cooperación y colaboración con los diferentes actores en el marco de la ciberseguridad. → **LÍNEA DE ACTUACIÓN 5**
- Posicionar la marca "Málaga Cibersegura" a través de empresas locales, especialistas e industria especializada en ciberseguridad — **OBJETIVO ESTRATÉGICO 5**
  - Situar a Málaga como referente en ciberseguridad mediante la promoción de su marca, la mejora de las capacidades en las empresas locales y el desarrollo de una industria especializada. → **LÍNEA DE ACTUACIÓN 6**

RETO 3

- Impulsar la capacitación y sensibilización en ciberseguridad en los empleados públicos, profesionales y ciudadanía — **OBJETIVO ESTRATÉGICO 6**
  - Desplegar programas de formación y concienciación en ciberseguridad, creación de talento y fomento del buen uso de las TICs. → **LÍNEA DE ACTUACIÓN 7**

Ciudad de Málaga

R1 OE1

Líneas de Actuación LA1

Despliegue de un modelo de gobernanza y gestión eficiente en el Ayuntamiento de Málaga que potencie y coordine la implantación de la Estrategia de Ciberseguridad.

> **[LA1.1]** Rediseñar las estructuras organizativas en ciberseguridad dentro del Ayuntamiento de Málaga, identificando los principales roles y funciones, de manera que se articule un ecosistema favorable a la implantación de la Estrategia e iniciativas asociadas. Se debe prestar especial atención a la figura de Responsable de Seguridad de la Información (RSI/CISO), como actor clave en la coordinación y supervisión de la Estrategia, debiendo disponer de capacidad de decisión y de los recursos (económicos y humanos especializados en ciberseguridad) necesarios para gestionar eficazmente la ciberseguridad de los servicios digitales.

> **[LA1.2]** Establecer un catálogo de servicios de negocio digitales prestados por el Ayuntamiento, identificando los marcos legales tecnológicos de aplicación, así como el nivel de criticidad y la caracterización de los mismos, para habilitar una adecuada gestión de riesgos de los sistemas de información.

Ciudad de Málaga

R1 OE1

Líneas de Actuación LA2

Alinear la estrategia de ciberseguridad con otras estrategias municipales presentes en el Ayuntamiento de Málaga y asegurar la inclusión de la ciberseguridad en otras estrategias municipales futuras.

> **[LA2.1]** Asegurar la presencia del CISO, o persona en quien delegue, en las reuniones de definición de nuevos planes estratégicos del Ayuntamiento de Málaga, con objeto de evaluar el impacto en ciberseguridad de dichas estrategias y que la ciberseguridad esté presente en las mismas desde el diseño.

> **[LA2.2]** Asegurar la presencia del CISO, o persona en quien delegue, en los diferentes comités de seguimiento de las respectivas estrategias municipales, para colaborar en su ejecución y aportar soluciones desde la Estrategia de Ciberseguridad y el alineamiento con los objetivos estratégicos.

Ciudad de Málaga

R1 OE2

Líneas de Actuación LA3

Gestión de riesgos digitales y cumplimiento normativo en ciberseguridad de los sistemas de información.

> **[LA3.1]** Definir y desplegar un proceso formalizado de ciberseguridad enfocado en la gestión de riesgos de los sistemas de información (IT, OT e IoT) que dan soporte a los diferentes negocios municipales, con especial atención a los riesgos en la cadena de suministro (proveedores).

> **[LA3.2]** Definir, implantar y supervisar planes de ciberseguridad basados en la gestión de riesgos digitales de los diferentes negocios municipales, en cumplimiento y conformidad con el Esquema Nacional de Seguridad y otras regulaciones vigentes, prestando especial atención a los operadores críticos y servicios esenciales.

> **[LA3.3]** Desarrollar, mantener y actualizar políticas, normas y guías de buenas prácticas que permitan aplicar la ciberseguridad desde el diseño en los sistemas y servicios prestados por el Ayuntamiento de Málaga, debiendo establecer requisitos de ciberseguridad, tanto generales como específicos, según necesidades y requerimientos de los servicios digitales (desarrollados internamente o contratados a terceros).

R1 OE3

Líneas de Actuación LA4

Refuerzo y mejora continua de capacidades de prevención, detección, respuesta y recuperación ante ciberincidentes.

> **[LA4.1]** Reforzar los servicios de ciberseguridad gestionada y optimizar el uso de las herramientas especializadas, los procesos y procedimientos aplicados, y las personas implicadas, en la prevención, detección, respuesta y recuperación con orientación a la identificación de patrones, prevención de potenciales amenazas en tiempo real y monitorización constante. Se debe prestar especial atención a la vigilancia digital continua y a los sistemas de alerta temprana que permitan adelantarse a posibles ciberataques.

> **[LA4.2]** Realizar programas periódicos de auditoría técnica, como pentesting y hacking ético, que permitan el descubrimiento de vulnerabilidades en los entornos tecnológicos del Ayuntamiento de Málaga, garantizando la disponibilidad de los servicios públicos y minimizando la interrupción de sus actividades (especial atención a la gestión de vulnerabilidades y a la gestión de la superficie de exposición).

> **[LA4.3]** Establecer canales de comunicación para poder notificar posibles ciberincidentes o vulnerabilidades en sistemas de información del Ayuntamiento de Málaga.

> **[LA4.4]** Diseñar, planificar y supervisar el plan de gestión de crisis, contingencia y continuidad de negocio donde se establezcan los mecanismos y controles que permitan asegurar las operaciones del Ayuntamiento en caso de producirse un evento no deseado. Dicho plan debe reflejarse en el Plan de Emergencia Municipal.

> **[LA4.5]** Promover la realización periódica de ciber-ejercicios con objeto de probar las capacidades de prevención, detección, respuesta y recuperación ante ciberincidentes, y poder medir la madurez y eficiencia de dichas capacidades de cara a impulsar una mejora continua.

> **[LA4.6]** Promover la realización de simulacros periódicos de ciber-crisis con objeto de probar las actuaciones de los diferentes actores municipales en el caso de que se produjera una crisis ocasionada por un ciber-ataque.

Ciudad de Málaga

R2 OE4

Líneas de Actuación LA5

Diseño de un modelo de cooperación y colaboración con los diferentes actores en el marco de la ciberseguridad.

> **[LA5.1]** Identificar y mantener un mapa de actores clave en el ámbito de la ciberseguridad, tanto a nivel local, nacional como internacional, tales como autoridades competentes, empresas de ciberseguridad, operadores críticos y de servicios esenciales, con los que el Ayuntamiento pueda establecer modelos de colaboración.

> **[LA5.2]** Desarrollar modelos de colaboración (convenios y/o acuerdos) con comunidades, colegios profesionales, asociaciones y organizaciones públicas o privadas que promuevan la ciberseguridad.

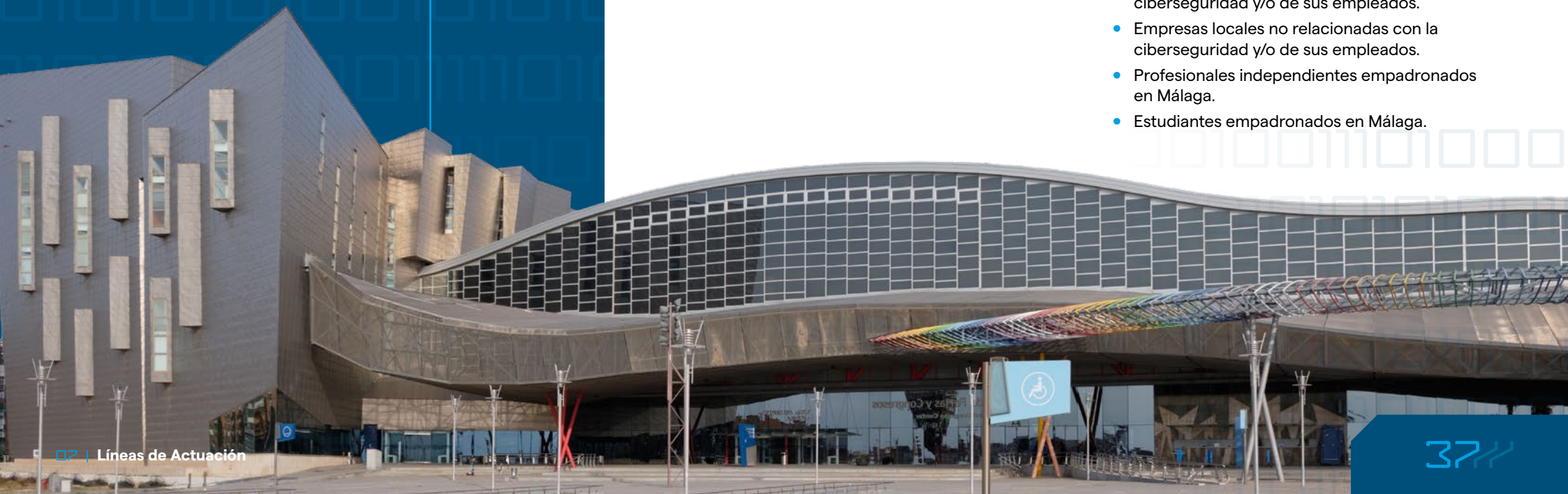
> **[LA5.3]** Identificar y desarrollar protocolos y mecanismos de coordinación y seguimiento para el intercambio de información entre organismos públicos y/o privados, con los que el Ayuntamiento de Málaga tenga acuerdos/convenios en materia de ciberseguridad.

> **[LA5.4]** Promover la colaboración específica, en materia de ciberseguridad, con otras ciudades y redes de ciudades tales como la Red Española de Ciudades Inteligentes (RECI), EuroCities y/o comunidades similares.

R2 OE5

Líneas de Actuación LA6

Situar a Málaga como referente en ciberseguridad mediante la promoción de su marca, la mejora de las capacidades en las empresas locales y el desarrollo de una industria especializada.



> **[LA6.1]** Promover y difundir la marca "Málaga Cibersegura" a nivel local, autonómico, nacional y/o internacional a través de:

- El uso de medios propios y/o de los entes instrumentales pertenecientes al Ayuntamiento de Málaga para recopilar y difundir las certificaciones, reconocimientos, premios y proyectos relevantes de ciberseguridad de la ciudad.
- Patrocinio de eventos y/o congresos de ciberseguridad, en especial a los realizados en el territorio local, regional y nacional.

> **[LA6.2]** Establecer canales de comunicación para recopilar:

- Certificaciones de ciberseguridad.
- Publicaciones en libros o revistas de prestigio en ciberseguridad.
- Ponencias en eventos y congresos de prestigio en ciberseguridad.
- Reconocimientos y premios de ciberseguridad.
- Proyectos relevantes de ciberseguridad.
- Proyectos relevantes que, no siendo específicos de ciberseguridad, usen ciberseguridad.

De:

- El Ayuntamiento de Málaga, sus entes instrumentales y/o de sus empleados.
- Empresas locales relacionadas con la ciberseguridad y/o de sus empleados.
- Empresas locales no relacionadas con la ciberseguridad y/o de sus empleados.
- Profesionales independientes empadronados en Málaga.
- Estudiantes empadronados en Málaga.

Ciudad de Málaga

R2 OE5

Líneas de Actuación LA6

Situar a Málaga como referente en ciberseguridad mediante la promoción de su marca, la mejora de las capacidades en las empresas locales y el desarrollo de una industria especializada.

> **[LA6.3]** Establecer canales de comunicación, a través de las organizaciones locales, regionales y/o nacionales competentes en la materia, con objeto de suministrar asesoramiento para:

- La realización de autodiagnósticos en materia de ciberseguridad, con objeto de que conozcan su nivel de madurez y posibles ámbitos de actuación que necesitan desarrollar como proveedores de productos y servicios.
- La obtención de certificaciones de ciberseguridad, para la mejora de las capacidades de empresas y profesionales.
- Encontrar financiación en el ámbito de la ciberseguridad.

De:

- Empresas locales relacionadas con la ciberseguridad.
- Empresas locales no relacionadas con la ciberseguridad.
- Profesionales independientes empadronados en Málaga.

> **[LA6.4]** Establecer canales de comunicación, a través del Ayuntamiento y sus entes instrumentales, con objeto de promover e impulsar:

- La creación de programas de aceleración específicos para empresas dedicadas a la ciberseguridad.
- La cooperación y transferencia de conocimiento desde universidades y/o centros de innovación malagueños a la industria de ciberseguridad de la Ciudad de Málaga.

Destinado a:

- Empresas locales relacionadas con la ciberseguridad.
- Profesionales independientes empadronados en Málaga.

> **[LA6.5]** Establecer canales de comunicación, a través del Ayuntamiento y sus entes instrumentales, con objeto de promover e impulsar:

- Planes de captación de capital privado destinado a la inversión en empresas de ciberseguridad malagueñas, tanto dentro del territorio como en el extranjero.
- La creación de programas para la atracción de empresas especializadas en materia de ciberseguridad a la Ciudad de Málaga.

Ciudad de Málaga

R3 OE6

Líneas de Actuación LA7

Desplegar programas de formación y concienciación en ciberseguridad, creación de talento y fomento del buen uso de las TICs.

> **[LA7.1]** Establecer canales de comunicación, a través de las organizaciones locales, regionales y/o nacionales competentes en la materia, con objeto de promover y divulgar:

- La inclusión de la programación segura y la cultura de ciberseguridad en la educación desde edades tempranas, con el fin de promover la seguridad digital en Málaga y preparar a la ciudadanía para los retos de la transformación digital.
- Iniciativas y planes de alfabetización sobre los riesgos tecnológicos y de ciberseguridad, incidiendo en aquellos grupos más vulnerables, tales como personas mayores o adolescentes.
- Programas inclusivos y equitativos en materia de ciberseguridad, incrementando la presencia de mujeres e integrando la perspectiva de género en las políticas digitales.
- Programas de formación y reconversión de perfiles ajenos a la ciberseguridad al ámbito de la ciberseguridad.
- Programas de certificación de personas en certificados de ciberseguridad que cubran las necesidades de posibles profesionales del sector.

Destinado a:

- Ciudadanía.

> **[LA7.2]** Establecer, a través del Ayuntamiento y sus entes instrumentales:

- Campañas de ingeniería social, mediante simulacros que permitan a los usuarios identificar y reaccionar ante un posible ataque de suplantación de identidad.

Destinado a:

- Empleados municipales.

Ciudad de Málaga

R3 OE6

Líneas de Actuación LA7

Desplegar programas de formación y concienciación en ciberseguridad, creación de talento y fomento del buen uso de las TICs.

> **[LA7.3]** Diseñar, a través del Ayuntamiento y en colaboración con universidades y/o centros de formación especializados:

- Temarios específicos de ciberseguridad para próximas convocatorias de empleo público especializado de ciberseguridad del Ayuntamiento de Málaga.
- Temas generales de ciberseguridad a incluir en próximas convocatorias de empleo público del Ayuntamiento de Málaga.

Destinado a:

- Selección de personal del Ayuntamiento de Málaga.

> **[LA7.4]** Diseñar, reutilizar y difundir, a través del Ayuntamiento y sus entes instrumentales:

- Campañas de concienciación y sensibilización en ciberseguridad para situaciones específicas, tales como nuevas ciberamenazas o ciberdelitos de actualidad, discriminando los usuarios a las que van dirigidas. Especial atención a usuarios que, por sus responsabilidades y funciones, tienen un mayor riesgo de estar involucrados en un ciberincidente.
- Mejores prácticas para el buen uso de los servicios públicos digitales y la seguridad de las TICs.

Destinado a:

- Empleados públicos.
- Ciudadanía.

> **[LA7.5]** Diseñar, reutilizar y difundir, a través del Ayuntamiento y sus entes instrumentales:

- Alertas de ciberseguridad, que permitan informar de vulnerabilidades existentes, con objeto de que los usuarios administradores de los sistemas puedan remediarlas lo antes posible.
- Contenidos de ciberseguridad en eventos organizados por el Ayuntamiento, tales como foros, congresos o charlas.

Destinado a:

- Empleados públicos.

08 Modelo de gobernanza

Ciudad de Málaga

MODELO DE GOBERNANZA

El impulso y apoyo continuo a la implantación de la Estrategia exige un modelo de gobernanza sólido y bien estructurado, que involucre a todas las partes interesadas dentro del ecosistema de ciberseguridad en el Ayuntamiento de Málaga.

En este sentido, el Ayuntamiento tiene el firme compromiso de crear una estructura que permita impulsar la Estrategia y cumplir con los objetivos estratégicos establecidos para los próximos años. Para ello, los primeros pasos que se deben dar serán:

- Crear el puesto de Responsable de Seguridad de la Información (RSI/CISO), como máxima autoridad en materia de supervisión de la seguridad de la información del Ayuntamiento de Málaga.
- Constituir el Centro de Ciberseguridad Ciudad de Málaga (CC-CIMA), dirigido por el CISO para la protección, coordinación, seguimiento y gestión de la seguridad de la información y servicios digitales del Ayuntamiento y resto de actuaciones indicadas en la Estrategia.

Asimismo, dicha estructura deberá comunicarse de forma bidireccional a través de un comité de seguridad de la información y diferentes grupos de trabajo operativos, por lo que será necesario:

- Constituir el Comité Municipal de Seguridad de la Información (CMSI) como órgano colegiado máximo responsable de proponer, al órgano competente, estrategias de seguridad de la información de los sistemas digitales municipales (ya sean propios o contratados a terceros), sin perjuicio de las competencias que corresponden a los órganos de gobierno municipales. El CMSI se encargará de proponer, al órgano competente, **decisiones estratégicas** relacionadas con el seguimiento e implantación de la Estrategia de Ciberseguridad

Ciudad de Málaga (ECCMA) y resto de cuestiones relacionadas con la ciberseguridad a nivel transversal de toda la Corporación Municipal.

- Los grupos de trabajo de ciberseguridad (GdTC) se crearán una vez aprobada la Estrategia. Son **grupos de trabajo operativo** para el seguimiento más directo de las acciones operativas de la Estrategia de Ciberseguridad.

MODELO DE GOBERNANZA

Adscrito a

- Alcaldía / Presidencia
- Concejalía de innovación, digitalización y transformación

Estructura Organizativa

Comité Estratégico

- Comité Municipal de Seguridad de la Información (CMSI)

- Centro Ciberseguridad Ciudad de Málaga (CC-CIMA)

Nivel Operativo

- Grupos de trabajo ciber (GdT-CIBER)

LA1	Marco de gobernanza unificado de ciberseguridad
LA2	Alinear la Estrategia con otras estrategias municipales
LA3	Gestión riesgos digitales y cumplimiento normativo
LA4	Prevención, detección, respuesta y recuperación ante ciberincidentes
LA5	Modelo de cooperación y colaboración
LA6	Situar a Málaga como referente en ciberseguridad
LA7	Programas formativos y concienciación de ciberseguridad

Frecuencia mínima

- Anual
- 365 Permanente
- Trimestral

MODELO DE GOBERNANZA

A continuación, se identifican los miembros mínimos que deben integrar el Comité Municipal de Seguridad de la Información (CMSI) y los grupos de trabajo, así como sus funciones más relevantes:

Comité Municipal de Seguridad de la Información (CMSI)

Miembros

- Presidente/a: Titular de la Concejalía de Innovación, Digitalización Urbana, Promoción de la Inversión Tecnológica y Empresarial, y Captación de Inversiones del Ayuntamiento de Málaga.
- Vicepresidente/a: Director/a General de Innovación.
- Secretario/a: Titular del órgano de apoyo a la Junta de Gobierno Local.
- Responsable del Centro de Ciberseguridad Ciudad de Málaga.
- Delegado/a de protección de datos.
- Director/a General de Alcaldía.
- Director/a General de Movilidad.
- Director/a General de Medio Ambiente y Sostenibilidad.
- Dirección General de Extinción de Incendios, Protección Civil y Servicios de Emergencia.
- Gerente del Organismo Autónomo de Gestión Tributaria y otros Servicios del Ayuntamiento (GESTRISAM).

Funciones

- Proponer decisiones estratégicas
- Análisis del cumplimiento y actualización de los objetivos de la Estrategia
- Supervisión global de riesgo de ciberseguridad en el Ayuntamiento de Málaga.
- Seguimiento global de las líneas de actuación
- Evaluación de impacto de la Estrategia por grupos de interés
- Análisis global de indicadores relevantes
- Análisis y gestión de presupuestos
- Establecimiento de mecanismos de financiación
- Evolución y adaptación de la Estrategia, según las directrices municipales

Ámbitos de actuación

- Transversal

Periodicidad mínima

- Anual

MODELO DE GOBERNANZA

Grupos de trabajo ciber (GdT-CIBER)

Miembros

- Responsable del Centro de Ciberseguridad Ciudad de Málaga (CC-CIMA)
- Responsables de las diferentes actuaciones identificadas de la Estrategia de Ciberseguridad
- Responsables de los Departamentos Municipales con competencias dentro de cada ámbito de actuación

Periodicidad mínima

- Trimestral

Funciones

- Toma de decisiones operativas
- Planificación de nuevas tareas
- Definición de metodologías de trabajo y acciones operativas
- Medición y mantenimiento de indicadores
- Seguimiento detallado de actividades y tareas asociadas
- Escalado de riesgos
- Análisis de las tareas completadas
- Escalado de problemas
- Ejecución de presupuestos

Cabe destacar, que todos los roles, funciones y Comités identificados en este apartado se detallarán en la Política de Seguridad de la Información del Ayuntamiento de Málaga como parte del desarrollo de la LA1.1.

09 Seguimiento y evaluación

EVALUACIÓN Y SEGUIMIENTO

La Estrategia de Ciberseguridad es un documento vivo que irá cambiando a lo largo del tiempo. Su seguimiento y evaluación permitirá detectar posibles desviaciones de manera temprana y poder tomar decisiones al respecto con objeto de reconducir la situación al estado planificado o adaptar la Estrategia a los nuevos acontecimientos.

Para realizar un seguimiento y evaluación de la Estrategia es fundamental establecer un marco de control que permita medir el progreso, evaluar la efectividad de las líneas de actuación implementadas y ajustar las acciones en función de los resultados obtenidos.

Por ello, deben definirse un conjunto de métricas e indicadores que permitan visualizar el estado actual y esperado de la ciberseguridad, con base en la Estrategia definida, así como el alineamiento y consecución de los objetivos establecidos en la misma para el periodo 2024-2027.

Cabe mencionar que las métricas e indicadores quedan fuera de este documento estratégico que define las políticas a abordar relacionadas con la ciberseguridad durante el periodo 2024-2027. Una vez aprobado el presente documento se procederá a detallar los diferentes proyectos, así como los recursos necesarios, tanto humanos como presupuestarios, junto con las métricas e indicadores que permitan el correcto seguimiento e implantación de la Estrategia.

10 Necesidades presupuestarias

NECESIDADES PRESUPUESTARIAS

Para la correcta implantación de la Estrategia, se debe disponer de un presupuesto adecuado en el Ayuntamiento de Málaga, que permita lanzar las actividades asociadas a las líneas de actuación identificadas, asegurando así el cumplimiento de los objetivos estratégicos en los próximos años.

La asignación del presupuesto de forma responsable puede marcar la diferencia entre el éxito y el fracaso de la implantación de la Estrategia. Por ello, se deben llevar a cabo una serie de pasos una vez aprobada la misma, de cara a disponer de los medios económicos requeridos para dar respuesta a los desafíos de ciberseguridad a los que se enfrenta el Ayuntamiento de Málaga.

Los pasos que se deben seguir serán los siguientes:

- Identificar una partida presupuestaria asignada para ciberseguridad dentro del Ayuntamiento.
- Definir la hoja de ruta a seguir, incluyendo una planificación de recursos y costes.
- Realizar revisiones del estado de la implantación de la estrategia, el presupuesto asignado y el alineamiento con los objetivos establecidos.
- Identificar y trasladar posibles riesgos.
- Reportar de forma clara y transparente el gasto e inversión utilizado para las diferentes iniciativas.

2024-2027

Ciudad de Málaga

Estrategia de Ciberseguridad Ciudad de Málaga