

## CONVENIO ENTRE LA AGENCIA DIGITAL DE ANDALUCÍA Y EL EXCMO. AYUNTAMIENTO DE MÁLAGA EN MATERIA DE CIBERSEGURIDAD.

### REUNIDOS

De una parte, el Excmo. Sr. D. Francisco de la Torre Prados, en nombre y representación del Excmo. Ayuntamiento de Málaga, en su calidad de Alcalde-Presidente, elegido como tal en la Sesión Especial de Constitución celebrada en Pleno, con fecha 17 de junio de 2023, en la que se procedió a constituir la Corporación Municipal surgida de las elecciones del día 28 de mayo de 2023, conforme a la normativa aplicable, y que queda recogida en el Acta Número 9/23 de 17 de junio de 2023, actuando para este acto conforme a su competencia de representación del Ayuntamiento prevista en el artículo 124.4.a) de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local.

De otra parte, el Ilmo. Sr. D. Raúl Jiménez Jiménez, en su calidad de Director Gerente de la Agencia Digital de Andalucía, nombrado mediante Decreto 140/2021, de 13 de abril, de la Consejería de la Presidencia, Administración Pública e Interior (BOJA núm. 71, de 16 de abril de 2021), que actúa en su nombre y representación y en uso de las facultades conferidas en el artículo 14.3.f) de los Estatutos de la Agencia Digital de Andalucía, aprobados por Decreto 128/2021, de 30 de marzo, (BOJA núm. 65, de 8 de abril de 2021), modificado por Decreto 572/2022, de 27 de diciembre.

Las partes, en el concepto en que respectivamente intervienen, aseguran la vigencia de las representaciones con las que actúan y se reconocen recíprocamente la capacidad legal suficiente y necesaria para suscribir el presente convenio (en adelante, el Convenio), y a tal efecto,

### EXPONEN

- I. El Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía, modificado por el Decreto 70/2017, de 6 de junio, indica en su artículo 12 que la Consejería competente en materia de coordinación y ejecución de las políticas de seguridad de los sistemas de información y telecomunicaciones desarrollará acciones centralizadas de prevención, detección y respuesta a incidentes en el ámbito de la Administración de la Junta de Andalucía a través del centro especializado AndalucíaCERT. Este Decreto resulta de aplicación a la Administración de la Junta de Andalucía y a sus entidades instrumentales, así como a los consorcios a los que se refiere el artículo 12.3 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía.
- II. El Comité de Seguridad TIC de la Junta de Andalucía aprobó en la reunión celebrada el día 2 de noviembre de 2017 el carácter obligatorio para todos los organismos y entidades incluidos en el ámbito subjetivo de aplicación del Decreto 1/2011, de 11 de enero, para formar parte del grupo atendido de AndalucíaCERT.
- III. Mediante Acuerdo de 18 de octubre de 2022, el Consejo de Gobierno, aprueba la Estrategia Andaluza de Ciberseguridad 2022-2025, la cual contiene los retos, objetivos y líneas de actuación en materia de ciberseguridad para los años 2022-2025, involucrando a la Administración Pública de Andalucía, la ciudadanía, el sector privado y las entidades más representativas del sector. La Administración Autonómica debe afrontar cuatro grandes retos,

Código Seguro De Verificación	Estado	Fecha y hora
Firmado Por	Firmado	27/10/2025 14:54:40
Observaciones	Página	1/31
Uri De Verificación		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).	

derivados de la digitalización y evolución tecnológica de la sociedad, a los cuales se les pretende dar respuesta a través de un escenario objetivo que permita a Andalucía convertirse en un territorio de referencia en materia de ciberseguridad.

En el marco de su línea de actuación dedicada al “fortalecimiento y desarrollo de marcos de cooperación y colaboración en diferentes ámbitos, tanto a nivel autonómico, nacional e internacional” se precisa desarrollar la extensión y capilaridad de la Red Nacional de SOCs mediante una Red Andaluza de SOC, para ampliar la coordinación y la cooperación entre el sector público y privado, así como con los organismos competentes en materia de ciberseguridad, utilizando cuando sea posible modelos federados de herramientas comunes y compartidas, y con ello, reforzar los modelos de relación, coordinación y colaboración en materia de ciberseguridad entre las distintas Administraciones Públicas (Ayuntamientos, Diputaciones Provinciales y otros entes públicos) y fomentar su integración en los modelos de relación nacionales. El modelo que se propone a través de este Convenio es por tanto el recomendado por el Centro Criptológico Nacional (CCN) a través de su iniciativa Red Nacional de SOCs. <https://rns.ccn-cert.cni.es/images/descargas/SOC-v5.pdf>

La colaboración entre entidades públicas en el ámbito de la ciberseguridad persigue, como fin último, el intercambio de información ágil y efectivo entre las distintas Administraciones Públicas (AGE, Comunidades Autónomas y Entidades Locales) para mejorar, de esta forma, las capacidades de defensa, detección y respuesta a posibles ciberincidentes. Además, se busca la optimización en la inversión destinada a la ciberseguridad, evitando duplicidades en el gasto e infraestructuras y potenciando así la sostenibilidad de las mismas en el tiempo.

Por ello, la Administración de la Junta de Andalucía, con el objetivo de cooperar y colaborar en aras de extender la capacidad de protección de la Administración Autonómica Andaluza, así como mejorar las capacidades de ciberseguridad, debe promover la colaboración y cooperación con las entidades e instituciones públicas a fin de reforzar los mecanismos de alerta temprana de amenazas y de prevención de incidentes, a través del uso de herramientas específicas de notificación y compartición de datos, de modo que se contribuya a la mejora del nivel de ciberseguridad y de las capacidades de protección del conjunto de entidades del sector público andaluz, como diputaciones provinciales, ayuntamientos y otros entes públicos.

Además, la Agencia Digital de Andalucía participa en el Proyecto Red-Argos, de la iniciativa Retech, que tiene como finalidad impulsar y fortalecer el ecosistema nacional de ciberseguridad a través del trabajo en Red de Nodos de Ciberseguridad regionales y la generación de capacidades especializadas en ámbitos estratégicos o polos específicos. En el caso de Andalucía, uno de los ámbitos de especialización ha sido las Smart Cities. En dicho proyecto se va a trabajar en la mejora de la ciberseguridad de los proyectos de Smart Cities implantados en Andalucía, por lo que se van a desarrollar varias acciones en colaboración con los Ayuntamientos, desde mejoras en la metodología a la hora de abordar estos proyectos, ayudas a los Ayuntamientos para la elaboración de auditorías técnicas sobre los proyectos de Smart Cities y la elaboración de planes directores de seguridad. La inclusión de las Administraciones Locales en el SOC permitiría una colaboración aún más estrecha en el ámbito del Retech, retroalimentando la información que disponemos de estos proyectos lo que nos permitiría medir de primera mano la eficacia de las medidas adoptadas y trabajar conjuntamente con las AALL para el mejor desarrollo de la ciberseguridad en el ámbito de las Smart Cities.

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	2/31
<b>Uri De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

- IV. Al Ayuntamiento de Málaga, entidad local encargada del gobierno y la administración autónoma de su municipio, conforme al artículo 57 de la Ley 7/1985, de 2 de abril, Reguladora de las Bases de Régimen Local, le corresponde la:

“La cooperación económica, técnica y administrativa entre la Administración local y las Administraciones del Estado y de las Comunidades Autónomas, tanto en servicios locales como en asuntos de interés común, se desarrollará con carácter voluntario, bajo las formas y en los términos previstos en las leyes, pudiendo tener lugar, en todo caso, mediante los consorcios o los convenios administrativos que suscriban”.

y tiene atribuidas entre otras, las competencias relativas a la “Promoción en su término municipal de la participación de los ciudadanos en el uso eficiente y sostenible de las tecnologías de la información y las comunicaciones”, de conformidad con el artículo 25.2. ñ), estando encuadrada la tipología del proyecto englobado en el Convenio a las materias cuya competencia en municipal.

El Ayuntamiento, además de abordar de forma decidida su modernización, y la de su sector público dependiente, ha establecido, como una prioridad para su actuación, la modernización y la garantía de seguridad en materia de tecnologías de la información y de las comunicaciones.

- V. La Agencia Digital de Andalucía, conforme a lo dispuesto en el artículo 6.2) de sus Estatutos tiene entre sus fines:

a) La definición y ejecución de los instrumentos de tecnologías de la información, telecomunicaciones, ciberseguridad y gobierno abierto y su estrategia digital, en el ámbito de la Administración de la Junta de Andalucía, sus agencias administrativas y sus agencias de régimen especial.

Asimismo, conforme al artículo 6.3) de sus Estatutos, para el ejercicio de sus fines corresponden a la Agencia las siguientes funciones y competencias:

o) La gestión de los recursos comunes para la prevención, detección y respuesta a incidentes y amenazas de ciberseguridad en el ámbito de la Administración de la Junta de Andalucía y del sector público andaluz.

- VI. Que la Agencia Digital de Andalucía, entre dichos recursos comunes, cuenta con el Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía, formado por un conjunto de personas, procesos y herramientas orientados a dar apoyo en tres ámbitos: Prevención, detección y respuesta a ciberincidentes; gobernanza, gestión del riesgo y cumplimiento normativo; y formación y concienciación.
- VII. Que es voluntad de ambas partes reforzar y garantizar la seguridad tecnológica, así como la eficacia y la eficiencia de las Administraciones públicas, mediante el ahorro de costes y de racionalización de recursos.
- VIII. Que la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, establece en su artículo 3 que la Administración de la Junta de Andalucía se organiza y actúa de acuerdo con el principio de colaboración y cooperación en su relación con otras Administraciones Públicas.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	3/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

- IX. Que en el marco normativo establecido por la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector, los convenios se consideran un instrumento, de uso generalizado, que se ha acreditado como especialmente eficaz para la gestión de los recursos públicos desde la perspectiva de su aprovechamiento racional, la búsqueda de sinergias y la coordinación de esfuerzos, de lo que, en general, se sigue naturalmente una economía de medios.
- X. Por ello, teniendo en cuenta la coincidencia de objetivos de las dos entidades, en el marco de sus fines y competencias, consideran de interés establecer una colaboración para el desarrollo conjunto de acciones en el marco de la ciberseguridad.

Por todo lo anterior, bajo el principio de la colaboración mutua que debe presidir las relaciones entre las Administraciones públicas, reconociéndose ambas partes, en la representación que ostentan, el Ayuntamiento y la ADA acuerdan suscribir el presente Convenio que se regirá por las siguientes

## CLÁUSULAS

### Primera. Objeto del Convenio

El objeto del presente Convenio consiste en fijar los términos y el alcance de la colaboración entre el Ayuntamiento de Málaga (en adelante, Ayuntamiento) y la Agencia Digital de Andalucía (en adelante, ADA) en materia de seguridad de los sistemas, servicios, y redes TIC de la Administración, que procesan, almacenan o transmiten información en formato electrónico, a través de la extensión de las actuaciones del Centro de Operaciones de Seguridad (SOC) de la Junta de Andalucía.

Se busca con ello contribuir a una mejora de la ciberseguridad en Andalucía a través de un modelo basado en la colaboración y el intercambio de información entre Administraciones. El proceso se fundamentará en el modelo federado formulado por el Centro Criptológico Nacional (CCN) buscando una mayor eficiencia y ahorro económico para las Administraciones participantes.

### Segunda. Ámbito subjetivo del Convenio

El ámbito subjetivo de aplicación del presente Convenio será el de las entidades que se reflejan en el Anexo III.

Este ámbito incluirá al Ayuntamiento de Málaga, como entidad adscrita principal, así como las empresas públicas municipales y otros entes del sector público dependientes del Ayuntamiento que se estimen oportunos, siempre que cumplan con los requisitos establecidos en esta cláusula y estén incluidas en el Anexo III (entidades adscritas secundarias). Las entidades adscritas secundarias deberán estar integradas en la red corporativa de la entidad adscrita principal y tener salida unificada a Internet, para poder acceder a los servicios del Convenio.

A lo largo de la vigencia del Convenio, las partes podrán acordar, mediante modificación del Anexo III, la incorporación o exclusión de entidades del ámbito subjetivo, siempre que se cumpla el procedimiento establecido en la Cláusula Novena para la modificación del Convenio. Esta modificación deberá ser formalizada por escrito y contar con la aprobación expresa de ambas partes.

Todas las entidades incluidas en el ámbito subjetivo del presente Convenio ya sean principales o secundarias, recibirán la denominación de "entidades adscritas".

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	4/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

### Tercera. Objetivos y actuaciones susceptibles de la colaboración

En el marco de los convenios de extensión de los servicios del SOC de la Junta de Andalucía, éste ofrece a las entidades adscritas al mismo una serie de actuaciones, agrupados en módulos, que se describen en el Anexo I de este Convenio.

De entre dichos módulos de actuaciones, la suscripción a los dos primeros módulos es requisito obligatorio para la suscripción al resto.

Para cada uno de estos módulos se especifican en el Anexo I las actuaciones a realizar por cada una de las partes y el coste anual del mismo, en base a su dimensionamiento. Este dimensionamiento se realiza por tramos, en base a unos parámetros específicos para cada módulo de actuaciones. El último de los módulos de actuaciones agrupará aquellas actividades que se ejecuten bajo demanda, y por tanto el coste asociado se reflejará por unidad de utilización.

Independientemente de estos módulos de actuaciones, y en el marco general de este Convenio, se podrán abordar por las dos partes, previo acuerdo de la Comisión de seguimiento de este Convenio, actuaciones específicas para el intercambio de información, la colaboración en actuaciones de difusión, formación y concienciación en materia de ciberseguridad u otras actividades que fomenten la ciberseguridad de los sistemas del Sector Público Andaluz.

### Cuarta. Suscripción de módulos

El Ayuntamiento de Málaga, por el presente Convenio, suscribe con la Agencia Digital de Andalucía los módulos de actuaciones que se indican en el Anexo II, con el nivel de dimensionamiento indicado en el mismo para cada uno.

En dicho Anexo II se calcula también el importe anual fijo de dichos módulos de actuaciones suscritos, en base al dimensionamiento y a los costes reflejados en el Anexo I. Para el último módulo, compuesto por actuaciones que se prestarían bajo demanda, se indica el coste por unidad de utilización de la actuación.

### Quinta. Obligaciones de las partes

Por ambas partes:

Para el desarrollo y ejecución de las actividades previstas en el Convenio, ambas partes adquieren las siguientes obligaciones de carácter general:

- Velar por la correcta ejecución de las actuaciones, llevando a cabo cuantas acciones sean necesarias para la buena marcha del Convenio.
- Difundir, utilizando los medios a disposición de cada parte, todas aquellas actuaciones e iniciativas que se realicen en el marco del Convenio, bajo las directrices que en materia de comunicación y difusión se acuerden.
- Poner a disposición del Convenio los recursos humanos necesarios, designando cada parte en el marco de la Comisión de Seguimiento a un responsable técnico del sector público.
- Facilitar e intercambiar cuanta información técnica y jurídico-administrativa se considere útil.
- Coordinar las acciones y actividades derivadas del Convenio, así como elaborar la documentación técnica, económica y/o administrativa necesaria para el correcto desarrollo del mismo.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	5/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

- f. Compartir cualquier otra información de interés acerca de las actividades que se realicen o impacten en el ámbito local de actuación.
- g. Aquellas otras que se acuerden entre las partes en el seno de la Comisión de Seguimiento y que indudablemente se deriven del objeto del convenio.

Por parte de la Agencia Digital de Andalucía:

Para el desarrollo y ejecución de las actividades previstas en el Convenio la Agencia Digital de Andalucía adquiere las siguientes obligaciones específicas durante la vigencia del mismo:

- a) Proveer las actuaciones suscritas indicados en el anexo II.
- b) Realizar actividades de promoción, comunicación y difusión.
- c) Disponer de los recursos humanos propios para el desarrollo de las actuaciones previstas.

Estas obligaciones podrán ser prestadas por la propia Agencia Digital de Andalucía o por terceros, bajo la modalidad e instrumentos jurídicos que la ADA determine, y en todo caso en el marco de la normativa que resulte de aplicación.

Asimismo, este Convenio no generará, en ningún caso, relación laboral alguna entre la ADA y los profesionales que puedan llevar a cabo la ejecución de las actuaciones que se realicen en ejecución de los objetivos del presente convenio.

Por parte del Ayuntamiento de Málaga:

Para el desarrollo y ejecución de las actividades previstas en el Convenio el Ayuntamiento de Málaga, en función de los módulos a los que se suscriba, adquiere las obligaciones específicas descritas en cada uno de los módulos del Anexo I, así como cumplir con las obligaciones financieras adquiridas con la firma de este Convenio en tiempo y forma, durante la vigencia del mismo.

**Sexta. Financiación y forma de pago**

Los costes que se deriven de la ejecución del presente Convenio, con el alcance inicial indicado en el Anexo II, serán financiados por el Ayuntamiento de Málaga y los mismos tendrán el carácter de costes de compensación para resarcir los gastos a la ADA que genera la actuación de colaboración consistente en la prestación de las actuaciones indicadas del Centro de Operaciones de Ciberseguridad (SOC) de la Junta de Andalucía, para asumir la sostenibilidad funcional y técnica del mismo.

Para el abono de estos costes la Agencia Digital notificará al Ayuntamiento de Málaga las liquidaciones con el importe de los costes de compensación de los módulos a los que se haya adherido. El Ayuntamiento podrá abonar estos importes por uno de los medios de pago disponibles en 'Plataforma Telemática de Pago y Presentación de Tributos y Otros Ingresos de la Junta de Andalucía' o en una de las entidades colaboradoras de la Junta de Andalucía.

La ADA notificará la liquidación **dentro de los dos primeros meses de** cada año natural, e incluirá los importes anuales por los módulos suscritos de actuaciones recurrentes (módulos I a IV), incluidos en el Anexo II y por la totalidad de las entidades incluidas en el Convenio. La cantidad a que ascienda dichas liquidaciones se ingresará por el Ayuntamiento en el modo indicado. Los plazos del

Código Seguro De Verificación	Estado	Fecha y hora
Firmado Por	Firmado	27/10/2025 14:54:40
Observaciones	Página	6/31
Uri De Verificación		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).	

pago en periodo voluntario serán los descritos en el art. 22.2 c) del Decreto Legislativo 1/2010, de 2 de marzo, por el que se aprueba el texto refundido de la Ley General de La Hacienda Pública de la Junta de Andalucía. Las liquidaciones podrán ser trimestrales si así se solicita por el Ayuntamiento a la firma del convenio.

De igual forma se notificará una única liquidación por el importe de las actuaciones bajo demanda descritos en el módulo V del Anexo II solicitados a lo largo del año anterior, con los mismos plazos.

En el caso de que no se produzca el abono en el periodo indicado, se procederá a la reclamación de la deuda mediante los mecanismos legalmente establecidos, según el art. 22.3 del TRLHP, incluido lo dispuesto en la Ley de Presupuesto de la Comunidad Autónoma de Andalucía para el año 2025 en su artículo 44, “Compensación de las deudas de las entidades locales a favor de la Hacienda Pública de la Junta de Andalucía”.

El resto de las actuaciones que se lleven a cabo no generarán coste para las respectivas partes. La financiación del presente Convenio se llevará a cabo por cada parte con cargo a sus propios presupuestos ordinarios de funcionamiento.

#### **Séptima. Justificación del Convenio**

La justificación de las actuaciones del Convenio se realizará por períodos de doce (12) meses, de forma que, una vez finalizado el período anterior a justificar, y en el plazo máximo de dos (2) meses, las partes deberán elaborar y presentar ante la Comisión de Seguimiento, una Memoria de actuación económica-justificativa del cumplimiento de los compromisos acordados, con indicación de las actuaciones realizadas y de los resultados obtenidos.

Con respecto al coste de adhesión al módulo V, al facturarse según el consumo efectivo del Ayuntamiento, y hasta el máximo estimado en el Anexo 2, se explicará en la Memoria el uso real y efectivo del ejercicio. La elaboración y aprobación de dicha memoria de ninguna manera condicionarán los pagos que se hayan acordado en el convenio.

#### **Octava. Mecanismos de seguimiento, vigilancia y control**

Al objeto de impulsar las actuaciones previstas en este Convenio y garantizar su desarrollo integral, de acuerdo con lo establecido en el artículo 49.1.f de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, se crea una comisión de seguimiento, vigilancia y control del Convenio y de los compromisos adquiridos por los firmantes, que ejercerá sus funciones de acuerdo con lo establecido en los artículos 51.2.c) y 52.3 de la citada Ley.

Esta Comisión estará compuesta por cinco (5) miembros: cuatro (4) con voz y voto, dos (2) de ellos nombrados por el Ayuntamiento de Málaga y los otros dos (2) designados por el Director Gerente de la ADA. El quinto miembro, que ostenta las funciones de secretario de la comisión, con voz, pero sin voto, será designado por el Ayuntamiento de Málaga. La Presidencia la ostentará uno de los representantes de la Agencia Digital de Andalucía, con voto de calidad. Los representantes de cada parte podrán designar suplentes, en caso de resultar necesario.

La Comisión de Seguimiento se constituirá en el plazo máximo de un mes, a contar desde la firma del presente convenio. La comisión se reunirá de forma ordinaria, al menos, una vez al año, sin perjuicio de las reuniones extraordinarias que se convoquen. Para la adopción de acuerdos se exigirá que asistan a la reunión la mayoría de los miembros. Los acuerdos se tomarán por mayoría y quedarán debidamente reflejados en acta que será firmada por todos los asistentes.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	7/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

La comisión de seguimiento, vigilancia y control tendrá, entre otras, las siguientes funciones:

- a. Diseño, definición, delimitación, planificación y ejecución de las concretas actividades técnicas derivadas del objeto de las actuaciones de colaboración objeto del presente Convenio.
- b. Evaluación del estado de las infraestructuras TIC gestionadas por las entidades adscritas, en el ámbito dentro de su alcance, con el objetivo de consensuar la evolución de las mismas y adecuar las actuaciones objeto del Convenio a las infraestructuras tecnológicas existentes en cada momento.
- c. Comunicación y seguimiento de la ejecución de las actuaciones de colaboración y de la ejecución económica.
- d. Acuerdos específicos que considere oportunos, que no impliquen modificación del Convenio, para la mejor realización del objeto de éste.
- e. Elaboración conjunta de un informe de conclusiones dentro del primer año de vigencia del presente Convenio.
- f. Propuesta para modificación del Convenio.
- g. Emisión de un informe técnico sobre controversias que puedan surgir entre las partes en relación con la ejecución, interpretación, modificación, efectos o resolución del presente Convenio.
- h. Adoptar las medidas oportunas, en caso de una resolución anticipada del Convenio, para garantizar la finalización de las actividades programadas.
- i. Informar en materia de la actividad de comunicación y difusión de la iniciativa.
- j. Cuantas otras se deriven del presente convenio y se consideren necesarias para su buena ejecución.

Las reuniones de la Comisión de Seguimiento podrán celebrarse por medios telemáticos.

Las cuestiones litigiosas o controversias que puedan surgir entre las partes en relación con la ejecución interpretación, modificación, resolución y efectos del presente Convenio, deberán solventarse por mutuo acuerdo de las partes en la Comisión de seguimiento, vigilancia y control.

#### **Novena. Modificación del Convenio**

El presente Convenio podrá ser objeto de modificación por mutuo acuerdo de las partes, cuando resulte necesario para la mejor realización de su objeto, mediante la formalización de la correspondiente adenda, que será suscrita por el Ayuntamiento de Málaga y la ADA.

Asimismo, mediante adenda se reflejarán, en su caso, los cambios en las actuaciones descritas en el Anexo I y las posibles modificaciones del valor de los mismos, así como los cambios producidos en el Anexo II (suscripciones a los módulos), la adición o eliminación de entidades adscritas incluidas en el Anexo III, así como cualquier cambio en relación a las entidades que se incluyen en el Convenio.

Cuando la modificación propuesta se refiere al contenido de los Anexos II y/o III, será a propuesta del Ayuntamiento de Málaga. El Ayuntamiento elevará la propuesta para modificación del Convenio a la Comisión de seguimiento, que tendrá que convocar reunión extraordinaria para debatirla en el plazo máximo de un mes desde la recepción de la propuesta y aprobarla o

Código Seguro De Verificación	Estado	Fecha y hora
Firmado Por	Firmado	27/10/2025 14:54:40
Observaciones	Página	8/31
Uri De Verificación		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).	

rechazarla en su caso. En el caso en que la modificación implique un aumento de las actuaciones, ya sea por incluir más módulos de los suscritos en el Anexo II o por incluir un mayor número de entidades secundarias en el Anexo III o mayor volumen de usuarios, el Ayuntamiento deberá acreditar la existencia de crédito para hacer frente a los mayores compromisos en la anualidad corriente y/o futura.

Cuando la modificación propuesta se refiera al contenido del Anexo I, será a propuesta de la ADA. Esta propuesta de cambio será como consecuencia de nuevas licitaciones, ya sea por que cambien la naturaleza de las actuaciones, incorporándose nuevas capacidades o porque cambien los costes unitarios o los parámetros de dimensionamiento. En este caso, la ADA elevará la propuesta para modificación del Convenio a la Comisión de seguimiento, que tendrá que convocar reunión extraordinaria para debatirla en el plazo máximo de un mes desde la recepción de la propuesta.

En el caso en que la modificación implique un aumento de los costes, ya sea por incluir más actuaciones o porque los costes se hayan encarecido, la comisión podrá aceptarla o rechazarla. En caso de rechazo por parte de los miembros del Ayuntamiento, no podrá hacerse valer el voto de calidad del presidente y procede extinguir el Convenio, aplicando la cláusula Undécima, apartado b). En el caso de que se apruebe, el Ayuntamiento deberá acreditar la existencia de crédito para hacer frente a los mayores compromisos en la anualidad corriente y/o futura. La ADA comunicará la liquidación complementaria al Ayuntamiento en el plazo de 1 mes y los plazos de pago serán los descritos en la cláusula sexta.

#### **Décima. Vigencia, duración y prórroga**

El plazo de vigencia de este Convenio será de cuatro años desde la fecha de la firma, pudiendo ser prorrogado de forma expresa formalizado por escrito, por un nuevo período de hasta cuatro años conforme a lo dispuesto en el artículo 49, letra h) de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, mediante comunicación previa y por escrito de las partes dentro de los tres meses anteriores a la finalización de su vigencia o de cualquiera de sus prórrogas.

Desde su firma por ambas partes, este Convenio entrará en vigor. La efectiva realización de las actividades se producirá en el plazo máximo de tres meses desde la firma del Convenio, plazo necesario para adaptar los sistemas económicos financieros de la Junta de Andalucía y para la efectiva transferencia de conocimiento hacia el SOC de la Junta de Andalucía por parte del Ayuntamiento. Una vez transcurra dicho plazo, se emitirá la liquidación correspondiente a la anualidad corriente.

#### **Undécima. Extinción**

El presente Convenio se extinguirá según establece el artículo 51.1 de la Ley 40/2015, de 1 de octubre, bien por el cumplimiento de las actuaciones que constituyen su objeto o por incurrir en causa de resolución. Sin perjuicio de lo indicado en el artículo 51 de Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, son causas de resolución del presente Convenio:

- a) El transcurso del plazo de vigencia del Convenio sin haberse acordado la prórroga del mismo.
- b) El acuerdo unánime de todos los firmantes.
- c) El incumplimiento de las obligaciones y compromisos asumidos por parte de alguno de los firmantes. En este caso cualquiera de las partes notificará a la parte incumplidora un requerimiento para que cumpla en un determinado plazo con las obligaciones o compromisos que se consideran incumplidos.

<b>Código Seguro De Verificación</b>			<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente		Firmado	27/10/2025 14:54:40
<b>Observaciones</b>			<b>Página</b>	9/31
<b>Url De Verificación</b>				
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			

Este requerimiento será comunicado al responsable del mecanismo de seguimiento, vigilancia y control de la ejecución del Convenio y a las demás partes firmantes. Si transcurrido el plazo indicado en el requerimiento persistiera el incumplimiento, la parte que lo dirigió notificará a las partes firmantes la concurrencia de la causa de resolución y se entenderá resuelto el Convenio.

La resolución del Convenio por esta causa podrá conllevar la indemnización de los perjuicios causados.

d) Por decisión judicial declaratoria de la nulidad del Convenio.

e) Por cualquier otra causa distinta de las anteriores prevista en otras leyes.

#### **Duodécima. Confidencialidad de la información**

Las partes quedan expresamente obligadas a mantener absoluta confidencialidad y reserva sobre los datos con los que se trabajan con ocasión del cumplimiento del presente Convenio, especialmente los de carácter personal y toda información sensible intercambiada en virtud del presente convenio, incluyendo, sin limitación, datos técnicos, estrategias de ciberseguridad, procedimientos operativos, vulnerabilidades identificadas, informes de auditoría, y cualquier información clasificada como confidencial según la legislación vigente o los términos del presente Convenio. Estos datos no podrán usarse con fin distinto al que figura en el Convenio ni tampoco ceder a otros, ni siquiera a efectos de conservación, sin el previo consentimiento por escrito de la otra parte.

La información intercambiada será clasificada de acuerdo con su nivel de sensibilidad, en conformidad con el Esquema Nacional de Seguridad (ENS) y otras normativas aplicables. Se empleará el Protocolo de Semáforo versión 2.0 (*Traffic Light Protocol*) del *Forum of Incident Response and Security Teams* (FIRST).

La duración de la confidencialidad será indefinida mientras la información ostente tal carácter, manteniéndose en vigor con posterioridad a la finalización del Convenio, sin perjuicio de la obligación de las partes de garantizar una adecuada publicidad de las actuaciones financiadas con cargo a este Convenio.

Las partes informarán a su personal, colaboradores y subcontratistas de las obligaciones establecidas en la presente cláusula de confidencialidad, así como de las obligaciones relativas al tratamiento automatizado de datos de carácter personal conforme a la legislación vigente, recabando un compromiso, por escrito, de éstos sobre el presente extremo.

Una vez cumplidos los fines del convenio o terminada su vigencia, cada parte destruirá o devolverá la información confidencial recibida, garantizando su eliminación segura conforme a estándares internacionales y normativas aplicables.

Las obligaciones recogidas en la presente cláusula no serán de aplicación a aquella información que sea:

1. Conocida por la parte receptora con anterioridad a la revelación.
2. Accesible al público sin culpa de la parte receptora.
3. Conocida por medios legítimos de un tercero sin deber de confidencialidad.
4. Revelada por la parte propietaria de la información a un tercero sin imponer a éste un deber de confidencialidad.
5. Desarrollada de forma independiente por la parte receptora con anterioridad o con independencia a la revelación.

Código Seguro De Verificación	Estado	Fecha y hora
Firmado Por	Firmado	27/10/2025 14:54:40
Observaciones	Página	10/31
Uri De Verificación		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).	

6. Revelada por imperativo legal.
7. Revelada por la parte receptora mediando la previa aprobación por escrito de la parte que revela la información confidencial.
8. Propiedad Intelectual.

### **Décimo tercera. Responsabilidad Patrimonial y Exoneración de Responsabilidad**

#### 1. Exoneración de Responsabilidad de la ADA:

La Agencia Digital de Andalucía no será responsable de los daños o incidentes relacionados con la ciberseguridad que afecten al Ayuntamiento de Málaga o sus entidades adscritas, siempre que las actuaciones realizadas por la ADA se ajusten a lo acordado en este Convenio y no se deban a negligencia o incumplimiento por parte de la ADA. La ADA no será responsable por ciberataques o fallos ajenos a su control.

#### 2. Responsabilidad del Ayuntamiento de Málaga:

El Ayuntamiento asume la responsabilidad de los daños, incidentes o pérdidas en sus sistemas y redes, salvo que se deriven de un incumplimiento de la ADA durante la realización de las actividades acordadas en el Convenio.

#### 3. Colaboración en Incidentes:

En caso de incidente de ciberseguridad, el Ayuntamiento colaborará con la ADA en su resolución, pero sin que ello implique responsabilidad por parte de la ADA, salvo que se demuestre incumplimiento de los servicios acordados.

#### 4. Limitación de Responsabilidad:

La responsabilidad de la ADA se limita a las actividades que se describen en este Convenio y no cubre incidentes fuera de su control, como ciberataques externos o fallos técnicos no atribuibles a la ADA.

### **Décimo cuarta. Protección de datos.**

Las partes se comprometen a cumplir, en los términos que le sean de aplicación, a lo establecido en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y en el 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 el que se deroga la Directiva 95/46/CE (en adelante, RGPD).

Respecto de los tratamientos de datos personales necesarios en desarrollo de las actividades del Anexo II, el Ayuntamiento de Málaga y las entidades adscritas que figuren en el Anexo III, será responsable, cada uno, de los mismos en su ámbito, mientras que la Agencia Digital de Andalucía actuará como encargado de tratamiento, por lo que le serán de aplicación las estipulaciones previstas en el artículo 28.3 del Reglamento General de Protección de Datos y pondrá a disposición del responsable de tratamiento cuantas evidencias esta estime oportuna para la verificación de dicho cumplimiento.

Las obligaciones y prestaciones que se recogen en el Anexo V constituyen el acuerdo de encargo de tratamiento entre la parte responsable del tratamiento y la parte encargada del tratamiento a que hace referencia el artículo 28.3 del RGPD y tendrán la misma duración que la prestación objeto de

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	11/31
<b>Uri De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

este convenio, prorrogándose en su caso por períodos iguales a éste. No obstante, a la finalización del convenio, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del convenio.

#### **Décimo quinta. Cesión de competencias**

El presente Convenio no supone, en ningún caso, la cesión de competencias de una de las partes a la otra, ni tampoco la concesión, expresa o implícita, de derecho alguno respecto a patentes, derechos de autor o cualquier otro derecho de propiedad intelectual o industrial.

#### **Décimo sexta. Régimen de transparencia**

De acuerdo con lo dispuesto en el art. 8.1 b) de la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno ambas partes, darán publicidad activa al convenio, según lo dispuesto en el artículo 18 de la Ley 38/2003, de 17 de noviembre.

Se publicará en el portal de transparencia de la Junta de Andalucía la información relativa a este convenio, conforme establece el artículo 15 de la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía.

#### **Décimo séptima. Régimen jurídico y jurisdicción**

Este Convenio tiene naturaleza administrativa y se regulará por lo establecido en las presentes cláusulas y en la legislación que resulte aplicable.

Está excluido del ámbito de aplicación de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se trasponen al Ordenamiento Jurídico Español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014.

Las cuestiones litigiosas o controversias que puedan surgir entre las partes en relación con la ejecución, interpretación, modificación, efectos o resolución del presente Convenio, de no existir el mutuo acuerdo de la Comisión de seguimiento, serán de conocimiento y competencia del orden jurisdiccional de lo Contencioso-Administrativo, de conformidad con la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Y en prueba de conformidad de cuanto antecede, firman este documento, en lugar y fecha señalada en la última firma electrónica realizada

EL ALCALDE-PRESIDENTE DEL EXCMO. EL DIRECTOR GERENTE DE LA AGENCIA  
AYUNTAMIENTO DE MÁLAGA DIGITAL DE ANDALUCÍA

Fdo.: Excmo. Sr. D. Francisco de la Torre Prados Fdo.: Ilmo. Sr. D. Raúl Jiménez Jiménez

**JIMENEZ**  
**JIMENEZ**  
**RAUL -**  
Firmado digitalmente por  
JIMENEZ  
JIMENEZ RAUL -  
Fecha:  
2025.10.14  
11:50:59 +02'00'

Código Seguro De Verificación	Estado	Fecha y hora
Firmado Por	Firmado	27/10/2025 14:54:40
Observaciones	Página	12/31
Uri De Verificación		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).	

## ANEXO I

### CATÁLOGO DE MÓDULO DE ACTUACION OFRECIDOS POR EL SOC DE LA JUNTA DE ANDALUCÍA EN EL MARCO DE ESTE CONVENIO

Las actuaciones de colaboración entre ambas partes se canalizarán en distintos módulos de actuación. Algunos serán de carácter obligatorio y otros serán potestativos. Los módulos de actuación se detallan a continuación. Para cada módulo se indican las características, los compromisos de cada parte (SOC y entidad adscrita) y el coste anual asociado.

El uso frecuente del concepto “puesto” requiere una clarificación de su significado: se entiende en el contexto de este convenio que un puesto de trabajo digital (abreviado “puesto”) es un equipo informático propiedad de la organización que es usado por uno o más empleados de la misma para la realización de su trabajo. Se incluye también en el concepto “puesto” a los equipos servidores que presten servicios TI a los usuarios del organismo.

#### A) Módulo I (obligatorio): Actuaciones de intercambio de información, notificación, coordinación en respuesta a incidentes y auditorías técnicas

- Federación de instancias de la herramienta LUCIA

La entidad adscrita deberá implementar una instancia propia de la herramienta LUCIA en su infraestructura con medios propios (o adscribirse a la instancia de LUCÍA web del CCN). Esto permitirá la implantación de un modelo federado para la gestión de los flujos de información relacionados con los incidentes de seguridad TIC.

Con independencia de los canales y mecanismos de comunicación e intercambio de información internos que se utilicen en cada ámbito, sobre dicha instancia de LUCIA se notificarán y gestionarán durante todo su ciclo de vida los incidentes de seguridad que afecten a los activos TIC de la propia entidad adscrita.

La instancia de la herramienta LUCÍA de la entidad adscrita deberá federarse a la instancia del SOC de la Junta de Andalucía, que a su vez se encuentra federada con la LUCÍA central del CCN-CERT, cerrándose de este modo los flujos de información de incidentes.

La gestión unificada de información de incidentes de seguridad a través de LUCÍA será condición indispensable y necesaria para la colaboración a tres niveles CCN-CERT / SOC de la Junta de Andalucía / Entidad adscrita en el resto de los módulos.

- Puntos de contacto y canales de comunicación

El SOC de la Junta de Andalucía pondrá a disposición de la entidad adscrita, adicionalmente a la herramienta LUCÍA, puntos de contacto telefónico y por correo electrónico.

Por parte de la entidad adscrita se comunicarán al SOC el POC (puntos de contacto) de notificación de incidentes (habitual y de emergencia) y administrativos.

Para la comunicación por correo electrónico se generarán e intercambiarán claves OpenPGP entre las partes.

- Inventariado de activos

La entidad adscrita comunicará al SOC de la Junta de Andalucía, y mantendrá actualizado, un listado de los activos TIC que gestiona, incluyendo al menos

Código Seguro De Verificación	Estado	Fecha y hora
Firmado Por	Firmado	27/10/2025 14:54:40
Observaciones	Página	13/31
Uri De Verificación		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).	

- Rango de direccionamiento expuesto a Internet.
- Servicios de red expuestos a Internet.
- Dominios de Internet gestionados.
- Dominios de correo electrónico y arquitectura de su prestación.
- Estructura general de la red del organismo y de su interconexión con otras redes y con Internet.
- Ubicación y características de sus principales centros de trabajo y de proceso de datos.
- Tenants y activos alojados en proveedores de servicio en nube.
- Principales tecnologías empleadas en los sistemas de información.
- URLs de los principales sitios web y sistemas de información accesibles vía web.
- Disponibilidad de personal para interlocución y resolución de incidentes en la entidad adscrita

Las entidades adscritas deberán contar con un equipo humano para la interlocución con el SOC de la Junta de Andalucía. El equipo deberá tener capacidad para atender las notificaciones realizadas vía LUCIA, así como para gestionar y resolver los incidentes de seguridad notificados (equipos de técnicos resolutores de seguridad, puesto de trabajo, infraestructuras y operaciones, desarrollo, etc.). Será compromiso de la entidad adscrita el correcto dimensionamiento de este equipo y la asunción de su coste.

- Recepción de incidentes

El SOC de la Junta de Andalucía proporcionará, de forma alineada con la guía CCN-STIC 817, servicios de recepción, análisis, identificación, clasificación, triaje y grabación en LUCÍA de los incidentes comunicados

- internamente desde la entidad adscrita
- internamente desde actuaciones de otros módulos en el marco de este Convenio
- externamente por el CCN-CERT, otras entidades colaboradoras o fuentes externas
- Coordinación de la gestión de incidentes

El SOC de la Junta de Andalucía proporcionará actuaciones de coordinación y asesoramiento para la gestión de los incidentes comunicados.

Las acciones de contención, mitigación y recuperación que deban realizarse sobre infraestructura propia de la entidad adscrita se realizarán por parte de ésta, así como las investigaciones necesarias para la correcta identificación y clasificación del incidente.

- Avisos de alerta temprana

El SOC de la Junta de Andalucía pondrá a disposición de la entidad adscrita, mediante el envío por correo electrónico y otros canales que se establezcan, información sobre vulnerabilidades, campañas de explotación de las mismas y otras actividades de interés para la ciberseguridad.

- Compartición de IOCs

El SOC de la Junta de Andalucía pondrá a disposición de la entidad adscrita la información que recopila y correla de indicadores de compromiso (IoC) sobre amenazas, artefactos y actores que

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	14/31
<b>Url De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

las operan, de modo que puedan ser utilizados como listas negras en los procesos de detección y protección que el Ayuntamiento implemente. Estas listas negras incluyen:

- Hashes de ficheros maliciosos
- Nombres de dominio y URL maliciosas
- Remitentes de correos electrónicos maliciosos
- Direcciones IP empleadas para desencadenar ataques o ejercer de Comando y Control
- ...etc

Para la confección de dichas listas, el SOC de la Junta de Andalucía utiliza la información que el CCN-CERT pone a disposición a través de la herramienta REYES, fuentes públicas, así como indicadores de compromiso extraídos de sus propias investigaciones de incidentes de seguridad.

Dichas listas serán publicadas y accesibles por la entidad adscrita bien a través de la red interadministrativa NEREA, bien a través de otros medios que se establezcan. Se permite al Ayuntamiento la difusión a través de canales seguros (p.e. su red interna) de estas listas a otras entidades adscritas al presente Convenio que pudiesen encontrarse interesadas en su utilización.

- Auditorías técnicas de seguridad

Se planificarán y realizarán auditorías técnicas (pruebas de intrusión) sobre los sistemas e infraestructuras que se determinen.

La entidad adscrita realizará la solicitud, indicando el ámbito de la auditoría, y en colaboración con el SOC de la Junta de Andalucía se establecerán los requisitos, esfuerzo necesario y compromisos por las partes para la realización de la misma.

Por parte del SOC de la Junta de Andalucía se dirigirá la ejecución de la auditoría, y por parte de la entidad adscrita se prestará colaboración en la identificación de interlocutores, la convocatoria de reuniones, la concesión temporal de los accesos y privilegios que se hayan acordado, y el seguimiento y colaboración, en general, con los trabajos.

Se incluye la prestación de esta actuación por un esfuerzo equivalente total de 20 jornadas.

Los hallazgos o alertas que se deriven de la actuación se notificarán a la entidad adscrita a través de los mecanismos establecidos en este Módulo I.

#### Dimensionamiento y coste

<b>Módulo I: Actuaciones de intercambio de información, notificación y coordinación en respuesta a incidentes</b>	<b>Parámetro de dimensionamiento</b>	<b>Coste anual (IVA incluido)</b>
	Hasta 1500 puestos	34.702,65 €
	De 1501 a 3500 puestos	66.919,49 €
	Más de 3500 puestos	99.136,32 €

#### **B) Módulo II (obligatorio): Gestión de la información y eventos de seguridad (SIEM) y detección de incidentes**

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	15/31
<b>Url De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

La monitorización de los eventos de seguridad de la infraestructura de una organización constituye uno de los pilares de la defensa en profundidad. Esta monitorización de eventos permite a los equipos de respuesta ante incidentes conocer, entre otros, el comportamiento en las comunicaciones e identificar acciones fuera de lo habitual, bien sea por tipo de tráfico, por el momento en el que se llevan a cabo, por su volumen... Esto es, la monitorización de los eventos de seguridad permite identificar y eliminar amenazas.

Para llevar a cabo una monitorización efectiva de la infraestructura de una organización se debe realizar un proceso de recolección desde diversas fuentes de información (tráfico de red, flujos, logs de sistemas y aplicativos...), un procesado y almacenamiento de dicha información, así como correlación de la misma, permitiendo de esta forma que un sistema especializado (un SIEM) genere alarmas en base a las anomalías que se produzcan. Dichas alarmas serán tratadas por un equipo de técnicos expertos que se encargará de su análisis, tratamiento y notificación a los responsables de los activos afectados, realizando también un seguimiento de los casos.

Como parte de las actividades de este módulo se incluyen el despliegue de sistemas que permitan realizar una monitorización de eventos de seguridad de la red de la entidad adscrita.

- Configuración de políticas

La entidad adscrita será responsable de configurar y mantener actualizadas y gestionadas las políticas de detección de sus sistemas de seguridad, incluyendo, si se dispone de ellos, sistemas antivirus, EDR, cortafuegos de nueva generación (NGFW), sistemas de detección/prevención de intrusiones (IDS/IPS), cortafuegos de aplicación web (WAF), sistemas de autenticación y control de acceso...

Las políticas se comunicarán al SOC de la Junta de Andalucía.

- Identificación e integración de fuentes, desarrollo de casos de uso

El SOC de la Junta de Andalucía, en colaboración con el personal técnico de la entidad adscrita, analizará la arquitectura de red de la misma, los principales sistemas e infraestructuras que le prestan servicio, los sistemas de seguridad implantados y sus políticas. En base a ello identificará las fuentes de eventos que tengan interés para la detección de incidentes, y sobre las que se puedan desarrollar casos de uso.

Se establecerán flujos para la recolección de los eventos requeridos provenientes de dichas fuentes, y su envío al SIEM del SOC de la Junta de Andalucía para su correlación y análisis.

- Sonda de recolección de eventos

Si así se requiere, el SOC de la Junta de Andalucía desplegará equipamiento en las instalaciones de la entidad adscrita para la recolección local de dichos eventos y su envío al SIEM.

La entidad adscrita proveerá espacio en sus instalaciones, alimentación, conectividad y acceso al personal del SOC de la Junta de Andalucía para el despliegue del equipamiento.

- Capacidad de ingesta en el SIEM del SOC de la Junta de Andalucía

Se habilitará en el SIEM del SOC de la Junta de Andalucía un canal de entrada y almacenamiento para los eventos enviados por la entidad adscrita.

- Monitorización de eventos y reporte de incidentes

El SOC de la Junta de Andalucía llevará a cabo la monitorización 24x7 para la detección de posibles amenazas de seguridad en base a los eventos y alarmas recibidos. Estos incidentes se notificarán a la entidad adscrita a través de los mecanismos establecidos en el Módulo I.

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	16/31
<b>Url De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

- Apoyo en instalación y recepción de incidentes de sonda SAT-INET

El Sistema de Alerta Temprana (SAT) es un servicio desarrollado por el CCN-CERT para la detección en tiempo real de las amenazas e incidentes existentes en el tráfico que fluye entre la red interna de una entidad e Internet. Para su puesta en marcha es necesario el despliegue de una sonda individual en la red de la entidad, que se encarga de recolectar la información de seguridad relevante que detecta y, después de un primer filtrado, enviar los eventos de seguridad hacia el sistema central que realiza una correlación entre los distintos elementos y entre los distintos dominios.

El SOC de la Junta de Andalucía apoyará a la entidad adscrita, en colaboración con el CCN-CERT, en el despliegue una sonda SAT-INET en sus instalaciones para la monitorización del tráfico de su red. Para ello, la entidad adscrita deberá contar con un agregado de tráfico y de los organismos a los que dicha red preste servicio.

Los costes asociados al despliegue de dicha sonda (hardware, licencias, servicios profesionales...) correrán a cargo de la entidad adscrita, siendo el personal del CCN-CERT quien monitorizará los eventos de seguridad generados por dicha sonda.

Los incidentes de seguridad que se detecten a través de la sonda SAT-INET se notificarán a la entidad adscrita por el CCN-CERT de forma conjunta con el SOC de la Junta de Andalucía, a través de los mecanismos establecidos en el Módulo I.

Dimensionamiento y coste

Módulo II: Gestión de la información y eventos de seguridad (SIEM) y detección de incidentes	Parámetro de dimensionamiento	Coste anual (IVA incluido)
	Hasta 1500 puestos	32.023,10 €
	De 1501 a 3500 puestos	55.324,65 €
	Más de 3500 puestos	78.626,20 €

**C) Módulo III (potestativo): Detección y Respuesta en Punto Final (EDR)**

- Agentes EDR y operación de los mismos

El SOC de la Junta de Andalucía proporcionará licencias de una solución de detección y respuesta de amenazas en punto final (*Endpoint Detection and Response*, EDR), basada en agentes de equipo final de usuario y servidor, de última generación, no basada exclusivamente en firmas, con consola de operación en nube pública y caza de amenazas (*threat hunting*) en la nube.

Los agentes recibirán las configuraciones, políticas e indicadores de la consola, ejecutarán las actividades de detección y las respuestas preaprobadas y trasladarán a la consola tanto alertas como telemetría.

Desde la consola se realizará el seguimiento del despliegue, se establecerán centralizadamente configuraciones y políticas, se difundirán indicadores, se recibirán alertas y telemetría y se realizarán acciones de contención inicial y de caza de amenazas.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	17/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

El despliegue de estos agentes se realizará por parte de los organismos adscritos, con sus propias herramientas y personal.

Se prestarán por el SOC de la Junta de Andalucía asistencia en:

- Asesoramiento en la instalación de nuevos agentes.
- Configuración y despliegue de políticas de detección y respuesta automática.
- Gestión de los IOC/IOA (indicadores de compromiso/ataque) del fabricante y de terceros.
- Atención a las detecciones y monitorización de alertas de seguridad, recepción de alertas procedentes del soporte a la caza de amenazas o de otras fuentes.
- Notificación y escalado de las alertas según los procedimientos que se establezcan.
- Los incidentes de seguridad que se detecten se notificarán a la entidad adscrita a través de los mecanismos establecidos en el Módulo I.

#### Dimensionamiento y coste

Módulo III: Detección y Respuesta en Punto Final (EDR)	Parámetro de dimensionamiento	Coste anual (IVA incluido)
	Hasta 1500 puestos	55.317,75 €
	De 1501 a 3500 puestos	123.729,22 €
	Más de 3500 puestos	179.519,35 €

#### D) Módulo IV (potestativo): Vigilancia digital y de superficie de exposición

Se prestarán por el SOC de la Junta de Andalucía asistencia en el análisis de la superficie de exposición y de vigilancia digital.

La entidad adscrita deberá proporcionar y mantener actualizada la información de los activos de interés:

- Direccionamiento público expuesto a Internet
- Objetivos de monitorización: nombres de organismo, dominios de publicación de servicios, dominios de correo electrónico, términos específicos, aplicaciones móviles...

Los hallazgos o alertas que se deriven de la asistencia se notificarán a la entidad adscrita a través de los mecanismos establecidos en el Módulo I.

- Análisis de superficie de exposición

El SOC de la Junta de Andalucía prestará a la entidad adscrita asistencia para el análisis de su superficie de exposición:

- Sondeos periódicos de los activos publicados en Internet, basados en el direccionamiento IP público de la entidad adscrita, para el descubrimiento, la enumeración, la identificación y la caracterización de servicios publicados.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	18/31
Url De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

- Interpretación de los datos obtenidos conforme a las necesidades y características de la entidad adscrita.
- Complementación y contraste de la información obtenida con las vulnerabilidades conocidas por el SOC de la Junta de Andalucía.
- Propuesta de realización de análisis de activos más completos y profundos, incluidos análisis de vulnerabilidades, en caso necesario.
- Emisión de recomendaciones para la reducción de la superficie de exposición y para la eliminación o mitigación de los riesgos que esta pueda suponer.

- Vigilancia digital

El SOC de la Junta de Andalucía prestará asistencia de vigilancia digital para la detección temprana de amenazas mediante la monitorización e investigación de la información disponible sobre activos de la entidad adscrita, así como sobre posibles actividades que pudieran afectar a su seguridad.

La vigilancia digital se realizará sobre activos de distintos tipos: nombres de organismo o marcas, dominios, direccionamientos IP, términos específicos (palabras claves), aplicaciones para dispositivos móviles, aplicaciones y servicios web, cuentas de acceso...

Se utilizarán tanto plataformas propias del SOC de la Junta de Andalucía como herramientas comunes y compartidas del CCN-CERT, como REYES.

Dimensionamiento y coste

Módulo IV: Vigilancia digital y de superficie de exposición	Parámetro de dimensionamiento	Coste anual (IVA incluido)
	Hasta 1500 puestos	24.009,40 €
	De 1501 a 3500 puestos	29.757,58 €
	Más de 3500 puestos	29.757,58 €

**E) Módulo V: Actuaciones bajo demanda**

De forma adicional a las actuaciones ya presentadas, desde el SOC de la Junta de Andalucía se ofrecen algunos otros que pudieran ser de especial interés. Consistirían en un conjunto de actuaciones que se activan bajo demanda de las entidades adscritas y previa autorización de la ADA. Se elaborará un presupuesto previo, que deberá ser aceptado por la entidad adscrita.

Consisten en:

- Auditorías técnicas de seguridad

Con el mismo funcionamiento que la actividad equivalente descrita en el Módulo I, se podrán ampliar las jornadas de auditorías técnicas (pruebas de intrusión).

Los hallazgos o alertas que se deriven de la asistencia se notificarán a la entidad adscrita a través de los mecanismos establecidos en el Módulo I.

- Análisis forense

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	19/31
Url De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

Consiste en la realización de tareas cuyo fin es reconstruir qué ha sucedido en el sistema analizado. Algunos ejemplos típicos son: determinar cómo se ha perpetrado un ataque, esclarecer qué método han usado los cibercriminales para lograr una intrusión o identificar qué usuario modificó unos datos sensibles sin autorización para ello.

Para ello se ofrece asistencia en:

- Peritaje informático: engloba todas aquellas tareas destinadas a la adquisición, conservación, documentación, análisis y presentación de evidencias digitales con validez legal, mediante el uso de procedimientos estandarizados. El análisis forense determinará el origen y las causas de un incidente de seguridad, plasmando todo el procedimiento en un informe pericial informático que podrá ser ratificado ante la autoridad judicial.
- Análisis DFIR: DFIR son las siglas de Digital Forensics & Incident Response. Supone una respuesta rápida ante incidentes para encontrar el origen del problema y aportar una posible solución al mismo. Una de sus características principales es que se suele trabajar sobre sistemas en funcionamiento, mediante el despliegue de algún agente que se encarga de realizar un “triaje” u obtención de información, y no sobre copias clónicas.

Dadas sus características, este proceso suele dejar rastro en los sistemas analizados, contaminando evidencias y dificultando la cadena de custodia de las mismas, por lo que en un análisis DFIR no prima tanto la obtención de pruebas informáticas que sea posible usar en un procedimiento judicial, como el dar una respuesta rápida ante un incidente de seguridad.

- Obtención, certificación y preservación de evidencias digitales.

Durante el análisis de un incidente de seguridad puede ser necesaria la certificación de una evidencia digital, de tal forma que se pueda asegurar, incluso judicialmente, su autenticidad y la no alteración de la misma.

Por ejemplo, en casos de suplantación de identidad puede ser necesario certificar la existencia de perfiles falsos en redes sociales, en casos de difamación puede ser necesario certificar el contenido de una web en un momento determinado, etc.

Con esta asistencia se pretende proveer de un mecanismo que permita la obtención, certificación, sellado de tiempo y preservación de evidencias digitales de diversa naturaleza.

- Análisis de malware.

Durante la gestión de los incidentes de seguridad es posible encontrarse con diversas muestras de malware que deben ser convenientemente analizadas.

Con la presente asistencia se busca la realización de análisis de malware bajo demanda, con el objetivo de identificar las muestras analizadas (familia de malware, autores...), listar sus características y capacidades (método de infección, vía de propagación, daño potencial sobre el sistema...), obtener un conjunto de indicadores relacionados con el malware (servidores C&C con los que contacta, hashes de los ficheros involucrados...), etc.

- Plataforma de concienciación.

Se incluye:

- Envío de píldoras, simulacros, refuerzos y otro material

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	20/31
<b>Url De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

- Acceso a web con contenidos y cuestionarios de concienciación
- Seguimiento individual del progreso
- Configuración, adaptaciones y gestión de la plataforma.

Dimensionamiento y coste

<b>Módulo V: Actuaciones bajo demanda</b>	<b>Coste</b>
	Bajo presupuesto

<b>Código Seguro De Verificación</b>	[Redacted]	<b>Estado</b>	<b>Fecha y hora</b>	
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40	
<b>Observaciones</b>		<b>Página</b>	21/31	
<b>Uri De Verificación</b>	[Redacted]			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			

**ANEXO II**

**MODULOS SUSCRITOS POR LA ENTIDAD ADSCRITA EN EL MARCO DE ESTE CONVENIO**

De los módulos descritos en el Anexo II, y en virtud de este Convenio, la entidad adscrita se suscribe a los que se indican con el valor “Sí” en la columna “suscripción”, con los parámetros de dimensionamiento indicados

Módulo	Suscripción	Parámetro de dimensionamiento	Coste anual
Módulo I: Actuaciones de intercambio de información, notificación y coordinación en respuesta a incidentes	<b>SI</b>	Más de 3500 puestos	99.136,32 €
Módulo II: Gestión de la información y eventos de seguridad (SIEM) y detección de incidentes	<b>SI</b>	Más de 3500 puestos	78.626,2 €
Módulo III: Detección y Respuesta en Punto Final (EDR)	<b>SI</b>	Hasta 1500 puestos	55.317,75 €
Módulo IV: Vigilancia digital y de superficie de exposición	<b>SI</b>	Más de 3500 puestos	29.757,58 €
Módulo V: Actuaciones bajo demanda. Bolsa de horas: - Auditoría técnica de seguridad. - Análisis forense. - Obtención, certificación y preservación de evidencias digitales. - Análisis de malware. Plataforma de concienciación (4000 usuarios).	<b>SI</b>	<b>NO APLICA</b>	100.339,01€ *(estimación)
TOTAL (excepto Módulo V)/12 meses			<b>262.837,85 €</b>
TOTAL (incluyendo estimación Módulo V)/12 meses (**)			<b>363.176,86 €</b>

(\*) Al tratarse de actuaciones bajo demanda, se facturarán a final de año, según el consumo efectivo del Ayuntamiento, y hasta un máximo de 100.339,01 €

(\*\*) Los precios de cada módulo tienen su referencia en los contratos en materia de ciberseguridad que han sido adjudicados por la Agencia Digital de Andalucía, y que se encuentran resumidos en el Anexo IV de este Convenio, según la información publicada en la plataforma de contratación.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	22/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

**ANEXO III**  
**ENTIDADES ADSCRITAS EN EL MARCO DE ESTE CONVENIO**

Entidad adscrita principal:  
Ayuntamiento de Málaga – P2906700F  
Avenida de Cervantes, 4, 29016, Málaga

Entidades adscritas secundarias:

Ninguna

**ANEXO IV**  
**CONTRATOS ADJUDICADOS POR LA AGENCIA DIGITAL DE ANDALUCÍA EN MATERIA DE CIBERSEGURIDAD COMO BASE DEL CONVENIO**

TÍTULO	DESCRIPCIÓN	licitación	ADJUDICACIÓN	FECHA	CPV
SUMINISTRO LICENCIAS Y SERVICIO DE SOPORTE ASOCIADO CIBERSEGURIDAD (EDR)	Suministro de licencias por suscripción y servicio de soporte asociado de una solución para la detección y respuesta a ciberincidentes en equipo final (EDR)	Importe total (con IVA): 17.909.283,45 €	Importe adjudicación (sin IVA): 14.801060,70 €	Fecha de adjudicación: 08/09/2023	48000000-8 - Paquetes de software y sistemas de información
		Importe total (sin IVA): 14.801060,70 €	Importe adjudicación (con IVA): 17.909.283,45 €	Fecha de formalización: 03/10/2023	48200000-0 - Paquetes de software de conexión en red, Internet e intranet. 48730000-1 - Paquetes de software de seguridad de archivos 48730000-4 - Paquetes de software de seguridad 48732000-8 - Paquetes de software de seguridad de datos 48760000-3 - Paquetes de software de protección antivirus
CONTR 2022 0000816345		Valor estimado: 17.761272,84 €			Duración del contrato: 48 meses 48760000-0 - Paquetes de software antivirus
PLATAFORMA DE MONITORIZACIÓN Y DE SERVICIOS RECURRENTE	Plataforma de monitorización y de servicios recurrentes y bajo demanda, para apoyo al Centro de Operaciones de Seguridad de la Junta de Andalucía	Importe total (con IVA): 11.597.446,95 €	Importe adjudicación (sin IVA): 1647.882,00 €	Fecha de adjudicación: 02/04/2024	72000000-5 - Servicios TI, consultoría, desarrollo de software, Internet y apoyo
		Importe total (sin IVA): 9.584.666,90 €	Importe adjudicación (con IVA): 1.993.937,22 €	Fecha de formalización: 19/05/2024	48732000-8 - Paquetes de software de seguridad de datos 32500000-8 - Equipo y material para telecomunicaciones
CONTR 2023 0000642838		Valor estimado: 17.891378,21 €			Duración del contrato: 36 meses
AM SERVICIOS DE CONSULTORIA, OF DE GOBERNO Y SEGUIMIENTO PROYECTOS TIC	Servicios de Consultoría, Oficiana de Gobierno y Segurimenot de Proyectos y servicios en materia de Tecnología de la Información y la Comunicación.	Importe total (con IVA): 58.080.000,00 €	Importe adjudicación (sin IVA): 38.400.000 €	Fecha de adjudicación: 22/02/2024	72240000-1 - Servicios de consultoría en gestión de proyectos
		Importe total (sin IVA): 48.000.000,00 €	Importe adjudicación (con IVA): 46.464.000 €	Fecha de formalización: 25/04/2024	72200000-3 - Servicios de consultoría en sistemas y consultoría técnica 72500000-5 - Servicios de consultoría en planificación de instalaciones informáticas 72220000-7 - Servicios de planificación y revisión estratégica de sistemas de información o de tecnología de la información
CONTR 2022 0001243819		Valor estimado: 96.000.000,00 €			Duración del contrato: 24 Meses 72500000-1 - Servicios de consultoría en auditoría informática y en equipo informático 72230000-0 - Servicios de consultoría en análisis empresarial 79100000-5 - Servicios jurídicos 72230000-4 - Servicios de revisión de las exigencias de tecnología de la información
AUDITORIA CERTIF, AUDITORIA TÉCNICA Y DE FORMAC Y CONC	Acuerdo marco de servicios de Auditorías de Certificación, de Auditorías Técnicas, y de Formación y Concianciación en el ámbito	Importe total (con IVA): 4.500.987,14 €	Importe adjudicación (sin IVA): 1.170.488,26 €	Fecha de adjudicación: 17/11/2024	72500000-1 - Servicios de consultoría en auditoría informática y en equipo informático
		Importe total (sin IVA): 3.719.824,08 €	Importe adjudicación (con IVA): 3.719.824,08 €	Fecha de formalización: 03/12/2024	
CONTR 2023 0000934533		Valor estimado: 3.719.824,08 €	1416.290,79 €		Duración del contrato: 36 Meses

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	23/31
Url De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

**ANEXO V****ACUERDO DE ENCARGO DE TRATAMIENTOS DE DATOS PERSONAL RELATIVOS A LAS ACTUACIONES DE CIBERSEGURIDAD DE LA AGENCIA DIGITAL DE ANDALUCIA****Obligaciones de la Agencia Digital de Andalucía como Encargada de tratamiento****I.- Aspectos Generales.**

La finalidad del tratamiento objeto de encargo a la Agencia Digital de Andalucía será el apoyo a la prevención, detección y respuesta a ciberincidentes mediante herramientas transversales, así como el desarrollo de actividades de formación y concienciación en materia de ciberseguridad

De conformidad con lo previsto en el artículo 28 del RGPD, la parte encargada del tratamiento se obliga a garantizar el cumplimiento de las siguientes obligaciones:

a) Tratar los Datos Personales conforme a lo estipulado en el presente convenio o demás documentos asociados aplicables a la ejecución del convenio, salvo que esté obligado a ello en virtud del Derecho de la Unión o nacional que se aplique a la persona encargada; en tal caso, la persona encargada informará a la persona responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.

b) No utilizar ni aplicar los Datos Personales con una finalidad distinta a la ejecución del objeto del presente convenio.

c) Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso.

En particular, y sin carácter limitativo, se obliga a aplicar las medidas de protección del nivel de riesgo y seguridad detalladas en este Anexo.

d) Mantener la más absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la ejecución del convenio, así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta de la parte encargada del tratamiento, siendo deber de la parte encargada del tratamiento instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la ejecución del convenio o de su desvinculación.

e) Llevar un listado de personas autorizadas para tratar los Datos Personales objeto de este convenio y garantizar que las mismas se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	24/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

debe informar convenientemente. Y mantener a disposición de la parte responsable del tratamiento dicha documentación acreditativa.

f) Garantizar la formación necesaria en materia de protección de Datos Personales de las personas autorizadas a su tratamiento.

g) Salvo que cuente en cada caso con la autorización expresa del Responsable del Tratamiento, no comunicar, ceder ni difundir los Datos Personales a terceros, ni siquiera para su conservación.

h) Nombrar Delegado de Protección de Datos, en los supuestos previstos en el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y comunicarlo a la parte responsable del tratamiento.

La dirección de contacto del delegado de protección de datos de la Agencia Digital de Andalucía es [dpd.ada@juntadeandalucia.es](mailto:dpd.ada@juntadeandalucia.es)

i) Una vez finalizadas la actuaciones objeto del presente convenio, se compromete, según corresponda y se instruya en este Anexo, a devolver o destruir (i) los Datos Personales a los que haya tenido acceso; (ii) los Datos Personales generados por la parte encargada del tratamiento por causa del tratamiento; y (iii) los soportes y documentos en que cualquiera de estos datos consten, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción. La persona Encargada del Tratamiento podrá, no obstante, conservar una copia de los datos durante el tiempo que puedan derivarse responsabilidades de su relación con la persona Responsable del Tratamiento. En este último caso, los Datos Personales se conservarán bloqueados y por el tiempo mínimo que establezcan los plazos de prescripción legal aplicables, destruyéndose de forma segura y definitiva al final de dicho plazo, salvo que se permita o requiera por la normativa de archivos y documentación, hacienda pública, procedimiento administrativo y judicial y el resto de normativa aplicable o por norma de derecho comunitario su conservación.

j) Según corresponda y se indique en este Anexo, a llevar a cabo el tratamiento de los Datos Personales en los sistemas/dispositivos de tratamiento, manuales y automatizados, y en las ubicaciones que a tal efecto disponga la Agencia bajo su control directo.

k) Salvo que se indique otra cosa en este Anexo o se instruya así expresamente por la parte responsable del tratamiento, a tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio que haya sido declarados de nivel de protección adecuado por la Comisión Europea o cuente con las garantías de adecuación establecidas en el RGPD, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subencargados autorizados conforme a lo establecido en este convenio o demás documentos asociados, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	25/31
<b>Uri De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

En el caso de que por causa de Derecho nacional o de la Unión Europea la parte encargada del tratamiento se vea obligado a llevar a cabo alguna transferencia internacional de datos, la parte encargada del tratamiento informará por escrito a la parte responsable del tratamiento de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables al mismo, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

l) De conformidad con el artículo 33 del RGPD, comunicar a la parte responsable del tratamiento, de forma inmediata y a más tardar en el plazo de 24 horas, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia o cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener que ponga en peligro la seguridad de los Datos Personales, su integridad o su disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones obtenidos durante la ejecución del convenio. Comunicará con diligencia la información detallada al respecto, incluso concretando qué interesados sufrieron una pérdida de confidencialidad.

Si no es posible facilitar la información simultáneamente se facilitará de manera gradual sin dilación indebida.

La dirección de contacto del Delegado de Protección de dato es [dpd@malaga.eu](mailto:dpd@malaga.eu)

m) Cuando una persona ejerza un derecho de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable (conjuntamente, los “Derechos”), ante la persona Encargada del Tratamiento, ésta debe comunicarlo a la parte responsable del tratamiento con la mayor prontitud. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del día laborable siguiente al de la recepción del ejercicio de derecho, juntamente, en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud que obre en su poder, e incluyendo la identificación fehaciente de quien ejerce el derecho.

La parte encargada del tratamiento asistirá a la parte responsable del tratamiento, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.

n) Colaborar con la parte responsable del tratamiento en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o las personas interesadas, y (iii) colaborar en la realización de evaluaciones de impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga.

<b>Código Seguro De Verificación</b>	[REDACTED]	<b>Estado</b>	<b>Fecha y hora</b>	
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40	
<b>Observaciones</b>		<b>Página</b>	26/31	
<b>Uri De Verificación</b>	[REDACTED]			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).			

Asimismo, pondrá a disposición del mismo, a requerimiento de este, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en este convenio y demás documentos asociados y colaborará en la realización de auditoras e inspecciones llevadas a cabo, en su caso, por parte del Responsable o auditor autorizado por éste.

ñ) Llevar, por escrito, incluso en formato electrónico, y de conformidad con lo previsto en el artículo 30.2 del RGPD un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de la parte responsable del tratamiento, que contenga, al menos, las circunstancias a que se refiere dicho artículo.

o) Disponer de evidencias que demuestren el cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad proactiva, como certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición la parte responsable del tratamiento a su requerimiento. Asimismo, durante la vigencia del convenio, pondrá a disposición toda información, certificaciones y auditorías realizadas en cada momento.

p) Derecho de información: El encargado del tratamiento, en el momento de la recogida de los datos, debe facilitar la información relativa a los tratamientos de datos que se van a realizar. La redacción y el formato en que se facilitará la información se debe consensuar con el responsable antes del inicio de la recogida de los datos.

## II. Descripción general del tratamiento de Datos Personales a efectuar.

La finalidad del tratamiento objeto de encargo a la Agencia Digital de Andalucía será el apoyo a la prevención, detección y respuesta a ciberincidentes mediante herramientas transversales, así como el desarrollo de actividades de formación y concienciación en materia de ciberseguridad

El tratamiento consistirá exclusivamente en los tratamientos de datos imprescindibles para que la parte encargada del tratamiento lleve a cabo las actividades que le correspondan de conformidad con el presente convenio.

El personal adscrito a la parte encargada del tratamiento, para proporcionar las actuaciones conveniadas establecidas en el Convenio puede tratar Datos Personales. Los Datos Personales se tratarán únicamente por el personal adscrito y al único fin de efectuar el objeto del convenio.

En caso de que como consecuencia de la ejecución del Convenio resultara necesario en algún momento la modificación de lo estipulado en este Anexo, la persona encargada del tratamiento lo requerirá razonadamente y señalará los cambios que solicita. En caso de que el Responsable del tratamiento estuviese de acuerdo con lo solicitado, emitiría un Anexo actualizado, de modo que el mismo siempre recoja fielmente el detalle del tratamiento.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	27/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

### III. Colectivos y Datos Tratados.

Los colectivos de personas interesadas y Datos Personales tratados a las que puede tener acceso el encargado del tratamiento son:

Categorías de Tratamientos en relación a los fines del tratamiento	Principales categorías de interesados	Categorías de Datos Personales del tratamiento a los que se puede acceder
Actuaciones de intercambio de información, notificación y coordinación en respuesta a incidentes	Ciudadanía Personal de las AALL Personas representantes de organismos y empresas públicas de servicio de las AALL Empresas que presten servicios a las AALL	Datos identificativos Datos de contacto Datos profesionales en la entidad representada. Datos técnicos de dispositivos y conexiones
Gestión de la información y eventos de seguridad (SIEM) y detección de incidentes	Ciudadanía Personal de las AALL Personas representantes de organismos y empresas públicas de servicio de las AALL Empresas que presten servicios a las AALL	Datos identificativos Datos técnicos de dispositivos y conexiones
Detección y Respuesta en Punto Final (EDR)	Personal de las AALL Personas representantes de organismos y empresas públicas de servicio de las AALL	Datos identificativos Datos técnicos de dispositivos y conexiones
Vigilancia digital y de superficie de exposición	Personal de las AALL Personas representantes de organismos y empresas públicas de servicio de las AALL Empresas que presten servicios a las AALL	Datos identificativos Datos de contacto Datos técnicos de dispositivos y conexiones
Actividades bajo demanda. - Auditoría técnica de seguridad.	Personal de las AALL Personas representantes de organismos y empresas públicas de servicio de las AALL	Datos identificativos Datos de contacto Datos profesionales en la

Código Seguro De Verificación	[REDACTED]	Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	28/31
Uri De Verificación	[REDACTED]		
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

<ul style="list-style-type: none"> <li>- Análisis forense.</li> <li>- Obtención, certificación y preservación de evidencias digitales.</li> <li>- Análisis de malware.</li> </ul>		entidad representada. Datos técnicos de dispositivos y conexiones
Plataforma de concienciación	Ciudadanía Personal de las AALL Personas representantes de organismos y empresas públicas de servicio de las AALL	Datos identificativos Datos de contacto Datos profesionales en la entidad representada.

#### IV. Elementos del tratamiento

El tratamiento de los Datos Personales comprenderá o podrá contener las siguientes operaciones: recogida, estructuración, conservación, consulta, cotejo, comunicación, supresión y cuantos tratamientos sean necesarios para la realización de las actividades de que se trate

#### V. Disposición de los datos al terminar el Convenio.

Una vez finalice el encargo, la persona encargada del tratamiento debe (marcar según proceda):

(Opción A)

Devolver a la persona responsable del tratamiento los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La devolución debe comportar el borrado total de los datos existentes en los equipos informáticos utilizados por la persona encargada. No obstante, la persona encargada puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

No obstante, la persona Responsable del Tratamiento podrá requerir a la persona encargada para que en vez de la opción a), cumpla con la b) o con la c) siguientes:

(Opción B)

Entregar a la persona encargada que designe por escrito la persona responsable del tratamiento, los datos de carácter personal y, si procede, los soportes donde consten, una vez cumplida la prestación. La entrega debe comportar el borrado total de los datos existentes en los equipos

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	29/31
<b>Uri De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

informáticos utilizados por la persona encargada. No obstante, la persona encargada puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

(Opción C)

Destruir los datos, una vez cumplida la prestación. Una vez destruidos, la persona encargada debe certificar su destrucción por escrito y debe entregar el certificado a la persona responsable del tratamiento.

No obstante, la persona encargada puede conservar una copia, con los datos debidamente bloqueados, mientras puedan derivarse responsabilidades de la ejecución de la prestación.

## VI. Medidas de seguridad.

De acuerdo con la evaluación de riesgos realizada, se deben implantar, al menos, las medidas de seguridad aplicables de conformidad con el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad si se trata de tratamiento de datos automatizado o semiautomatizado.

Las medidas de seguridad que el encargado de tratamiento debe observar, tanto de carácter técnico como organizativo, serán las apropiadas en orden a garantizar un nivel de seguridad adecuado al riesgo asociado al tratamiento de datos (artículo 32 del “Reglamento General de Protección de Datos” RGPD). Estas medidas tomarán como base las incluidas en el Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad (en adelante ENS), tal como requiere la Disposición Adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).

El encargado de tratamiento deberá adaptar las medidas de seguridad implantadas a cualquier modificación normativa del propio ENS, RGPD, LOPDGDD y/o cualquier otro marco normativo aplicable a los servicios que preste. Las medidas de seguridad del ENS se aplicarán tanto a los tratamientos de datos personales como no personales.

El encargado de tratamiento deberá designar un POC (Punto o Persona de Contacto) para la seguridad de la información tratada y el servicio prestado, que cuente con el apoyo de los órganos de dirección, y que canalice y supervise, tanto el cumplimiento de los requisitos de seguridad del servicio que presta o solución que provea, como las comunicaciones relativas a la seguridad de la información y la gestión de los incidentes para el ámbito de dicho servicio. Dicho POC de seguridad será el propio Responsable de Seguridad de la organización contratada, formará parte de su área o tendrá comunicación directa con la misma. Todo ello sin perjuicio de que la responsabilidad última resida en la entidad del sector público destinataria de los citados servicios.

Los productos y servicios de seguridad a contratar deberán estar incluidos en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación del Centro Criptológico Nacional (CCN-STIC-105).

Las medidas de seguridad del ENS a implantar serán, como mínimo, las derivadas de la valoración de los sistemas y del análisis de riesgo que se realice.

Código Seguro De Verificación		Estado	Fecha y hora
Firmado Por	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
Observaciones		Página	30/31
Uri De Verificación			
Normativa	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		

Las medidas de seguridad del ENS podrán ser ampliadas con medidas adicionales a las del ENS en caso de que los análisis de riesgos o evaluaciones de impacto sobre protección de datos realizados sobre los tratamientos de datos personales determinasen la insuficiencia de las medidas del ENS para mitigar adecuadamente los riesgos y/o impactos.

### **Obligaciones del Ayuntamiento de Málaga como Responsable del tratamiento**

1. Entregar, en su caso, al encargado los datos que se necesarios para el objeto del encargo.
2. Realizar una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
3. Realizar las consultas previas que corresponda.
4. Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
5. Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

<b>Código Seguro De Verificación</b>		<b>Estado</b>	<b>Fecha y hora</b>
<b>Firmado Por</b>	Francisco de la Torre Prados - Alcalde Presidente	Firmado	27/10/2025 14:54:40
<b>Observaciones</b>		<b>Página</b>	31/31
<b>Uri De Verificación</b>			
<b>Normativa</b>	Este informe tiene carácter de copia electrónica auténtica con validez y eficacia administrativa de ORIGINAL (art. 27 Ley 39/2015).		