

CONVENIO SUBVENCIÓN ENTRE EL AYUNTAMIENTO DE MADRID Y LA ASOCIACIÓN SIN ÁNIMO DE LUCRO "CLÚSTER DE CIBERSEGURIDAD DE MADRID – CYBERMAD" PARA LA PROMOCIÓN DE LA CIBERSEGURIDAD EN EL TEJIDO EMPRESARIAL DE LA ECONOMÍA MADRILEÑA.

Expte: 511/2023/11250

De una parte,

D^a. Engracia Hidalgo Tena, Delegada del Área de Gobierno de Economía, Innovación y Hacienda del Ayuntamiento de Madrid, en virtud del Decreto del Alcalde de 17 de junio de 2023 por el que se nombra a los miembros de la Junta de Gobierno de la Ciudad de Madrid, a los tenientes de Alcalde, a los titulares de las áreas y a los concejales presidentes de Distrito, y en ejercicio de las competencias atribuidas por el apartado 3º, punto 1.8 del Anexo del Acuerdo de 29 de junio de 2023 de la Junta de Gobierno de la Ciudad de Madrid, de organización y competencias del Área de Gobierno de Economía, Innovación y Hacienda.

Y, de otra,

Don Damián Ruiz Soriano, en nombre y representación de la ASOCIACIÓN SIN ÁNIMO DE LUCRO "CLÚSTER DE CIBERSEGURIDAD DE MADRID – CYBERMAD", como Presidente de la misma, nombrado para ese cargo en el punto 3º del Acta Fundacional de la Asociación, de fecha 22 de julio de 2020, y en base a lo dispuesto en los estatutos de la asociación, en su artículo 20, epígrafes a) y g), así como en el mandato otorgado por la Junta Directiva.

Reconociéndose las partes mutua y recíprocamente la competencia y capacidad legalmente necesarias para formalizar el presente convenio y quedar obligadas en la representación en que efectivamente intervienen.

EXPONEN

- I. El presente ejercicio 2023 está siendo particularmente intenso en eventos globales con efectos económicos y sociales muy profundos. Nunca como hasta ahora, en éstos últimos años, los procesos de cambio tecnológico - y en particular la digitalización - se han estado desarrollando con tanta intensidad, generando enormes crecimientos en determinados sectores y poderosas mejoras de la competitividad. Pero, a la vez, pocas veces se ha visto tal acumulación de incertidumbres y amenazas (crisis económicas, guerras como la invasión de Ucrania o los recientes ataques terroristas en oriente medio...) que generan enormes niveles de inestabilidad e inseguridad en el ámbito internacional.
- II. En este contexto, la seguridad en general, y la ciberseguridad en particular, que ya albergaba un carácter estratégico desde hace años, reviste una importancia creciente. Su carácter a la vez urgente y estratégico se deriva justamente de esa conjunción de dos factores; por un lado, el peso creciente del "ciberespacio": en las comunicaciones entre personas o empresas, en el ocio, en las transacciones comerciales o financieras, en el conjunto de telecomunicaciones civiles, pero también en el ámbito de la seguridad militar, la ciberdefensa, o en el funcionamiento de infraestructuras críticas



interconectadas y sensibles. Por otro lado, un escenario internacional incierto y volátil, con múltiples agentes privados o públicos que están utilizando los ciberataques unas veces como arma comercial o fuente de ingresos espurios, otras veces con carácter militar u ofensivo, pero siempre con un enorme potencial de daño. En efecto, el auge de la digitalización (implementación de técnicas de teletrabajo, Internet de las cosas (IoT) en procesos industriales, uso más intensivo de redes, de datos, de conexiones por internet y/o en la nube) no puede llevarse a cabo sin una paralela implementación de la ciberseguridad. En caso contrario, sin seguridad, las mejoras en la productividad y competitividad que vienen de la mano de la digitalización podrían tener como contrapartida un impacto negativo bajo la forma de mayores ciber-vulnerabilidades.

- III. De manera más precisa, se entiende por Ciberseguridad el conjunto de tecnologías, procesos y buenas prácticas destinados a proteger redes, aparatos electrónicos y de proceso de datos, así como sus programas e información almacenada, de ataques, daños o accesos no autorizados, así como la protección de información sujeta a la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales y diversas normativas nacionales y europeas, y los riesgos adicionales que se irán presentando con los nuevos desarrollos tecnológicos (como por ejemplo las redes móviles con quinta generación de tecnologías y estándares de comunicación inalámbrica o "5G", el IoT o Internet de las cosas, tanto en el ámbito doméstico como industrial, la movilidad conectada y los vehículos autónomos, etc.), o la protección de infraestructuras críticas con alto nivel de dependencia de la digitalización (suministros de agua, electricidad, telecomunicaciones, redes de transporte o de distribución de mercancías, etc.).

La digitalización segura o cibersegura de las PYMES, que constituyen el 99% de nuestro tejido empresarial, es especialmente importante en las circunstancias actuales, particularmente por sus niveles más altos de vulnerabilidad y su menor resiliencia, por culpa de su menor tamaño. Y esto es así tanto en términos de resistencia a impactos económicos como a su capacidad de respuesta a los ciberataques. Contrariamente a lo que suele opinar la ciudadanía, estos ataques no se centran sólo en las grandes empresas, los hospitales u otras infraestructuras civiles o militares: un porcentaje elevado se dirige a particulares, autónomos y PYMES, y varios estudios de organismos nacionales e internacionales señalan que 2/3 de las PYMES que sufren este tipo de malware pueden acabar cerrando como consecuencia de su impacto en términos de costes, reputacionales, de pérdida de datos, etc.

Madrid debe ser un motor de esta evolución mediante la colaboración público-privada y el apoyo a los sectores mejor posicionados y tecnológicamente punteros: aquellos sectores que potencien la sostenibilidad, la digitalización, y que fortalezcan la resiliencia de la economía y la sociedad y mejoren su posición competitiva. La ciberseguridad es por tanto, más allá de cualquier duda, uno de esos sectores de actividad, ya que aparece como necesidad transversal en todos los ámbitos relevantes de la digitalización. Además, los avatares internacionales ya mencionados, con conflictos bélicos híbridos, acentúan aún más su importancia, más allá de las necesidades inducidas por el teletrabajo, el uso creciente de IoT o Internet de las cosas, 5G u otras tecnologías.



- IV. En este ámbito, el clúster de Ciberseguridad de Madrid – CyberMAD, promovido desde el Ayuntamiento de Madrid y con participación de empresas de distinto tamaño, Universidades y diferentes administraciones, constituye una herramienta poderosa y única en ese empeño.

En efecto, una de las prioridades en materia económica radica en proteger y dar soporte al tejido productivo y social para minimizar el impacto a medio y largo plazo de la crisis y aprovechar y acelerar las oportunidades que abre en el ámbito de la transformación digital, las nuevas tecnologías y en particular – en el caso que aquí nos ocupa – la resiliencia de los sistemas informáticos, de las redes y de los datos, tanto en el ámbito de las empresas como de los particulares en Madrid.

- V. De conformidad con lo previsto en el Decreto de 17 de junio de 2023 por el que se nombra a los miembros de la Junta de Gobierno de la Ciudad de Madrid, a los tenientes de Alcalde, a los titulares de las áreas y a los concejales presidentes de Distrito, el Acuerdo de 29 de junio de 2023, de la Junta de Gobierno de la Ciudad de Madrid, de organización y competencias del Área de Gobierno de Economía, Innovación y Hacienda, establece, entre las que corresponden a esta área de gobierno, las relativas a la promoción económica y el desarrollo empresarial, el impulso del tejido empresarial de la ciudad a través de la realización de actuaciones dirigidas al desarrollo de sectores productivos estratégicos y al impulso de la innovación empresarial, así como el fomento del respeto al principio de desarrollo sostenible en el sector empresarial madrileño.

En relación con ello, una de las principales líneas de actividad es favorecer el desarrollo de algunos sectores de actividad que han sido considerados prioritarios por su valor estratégico, por su peso económico y por su implantación en la ciudad.

El Área de Gobierno de Economía, Innovación y Hacienda está comprometida con la implementación de iniciativas de refuerzo a la competitividad de las empresas localizadas en Madrid y de forma especial a fomentar el impulso y consolidación de los “clústeres” empresariales como organizaciones empresariales claves para la modernización y competitividad de la economía madrileña.

Además, entre las competencias de la persona titular del Área de Gobierno de Economía, Innovación y Hacienda se encuentran:

“1.8. Celebrar convenios con otras Administraciones y entidades públicas y privadas para el desarrollo y ejecución de las competencias del Área de Gobierno o del Área Delegada...”

1.9. Convocar y conceder subvenciones, así como formular la solicitud a otras Administraciones Públicas de aquellas que incidan en su ámbito competencial.”

- VI. Que el Clúster de Ciberseguridad de Madrid “Cyber MAD” (en adelante, CYBERMAD) se constituyó como una asociación sin ánimo de lucro creada con personalidad jurídica propia, patrimonio propio independiente y plena capacidad de obrar, dentro del marco de la legislación vigente, al amparo de la Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación, y normas complementarias, rigiéndose en su funcionamiento conforme a



principios democráticos y de transparencia, tal y como se refleja en sus estatutos debidamente inscritos en el Registro de Asociaciones.

El artículo 1 de sus estatutos establece que CYBERMAD es una "... Asociación, sin ánimo de lucro, con personalidad jurídica propia, patrimonio propio independiente y plena capacidad de obrar, dentro del marco de la legislación vigente. ... [El clúster] reúne a empresas, asociaciones, e instituciones, tanto públicas como privadas, que desarrollan actividades en el área de Madrid, y que se asocian libremente para impulsar el desarrollo del sector de la Ciberseguridad."

Adicionalmente, y según el artículo 3 de los mismos:

"Son fines de la Asociación:

- Sensibilizar y formar a empresas y ciudadanos, en el área de Madrid, en la importancia crítica de la Ciberseguridad.
- Reforzar el sector en el área de Madrid, incluyendo el desarrollo de las empresas ya existentes y de nuevas empresas, y contribuyendo a generar talento en colaboración con las universidades y centros de formación de Madrid.
- Contribuir a posicionar a Madrid como ciudad impulsora de la Ciberseguridad, dentro de España y en el contexto internacional..."

VII. Que esta subvención se enmarca en el ámbito establecido en el artículo 22.2 apartado c) de la Ley 38/2003, de 17 de noviembre, General de Subvenciones. No solo la situación imprevisible y excepcional que fue provocada por la pandemia de la COVID-19, sino la evolución posterior de la economía mundial, española y madrileña en particular, con las ya mencionadas crisis y amenazas sucesivas, así como el carácter estratégico del sector de la ciberseguridad (por su importancia en términos de seguridad y robustez para la actividad económica y social, y por su papel fundamental en la digitalización) hacen de interés público el potenciar un sector plenamente asentado en la Ciudad, que congrega un ecosistema único a nivel mundial, caracterizado por el uso de tecnología y un empleo con una elevada formación, estable, bien remunerado y con mayor resiliencia a situaciones de crisis.

CYBERMAD es el único caso de entidad específicamente dedicada a la promoción de la ciberseguridad en el ámbito de nuestra ciudad, reuniendo además en una asociación sin ánimo de lucro a un número ya muy significativo y creciente de entidades de diverso perfil, empresas de gran tamaño junto con PYMES y *start-ups*, universidades, centros de investigación e innovación, administraciones participantes en su Consejo Asesor, etc.

Sus **características y objetivos**, recogidos más arriba, son mayoritariamente coincidentes con los que se persiguen desde el Área de Gobierno de Economía, Innovación y Hacienda para un crecimiento económico estable, la promoción de la innovación y la creación de empleo. En efecto, CYBERMAD (a) se constituye como una entidad sin ánimo de lucro, de colaboración público-privada; (b) está formado por pequeñas y grandes empresas (tanto de consultoría o especializadas oferentes de servicios de Cybersec, como compañías demandantes de los mismos) y *start-ups*, así como entidades académicas y de investigación, y asociaciones sectoriales y otros participantes institucionales; (c) con el fin de promover la colaboración entre todos los agentes involucrados para fortalecer la formación, la investigación, la innovación y el desarrollo



empresarial y la difusión del sector en nuestra ciudad, y (d) atraer para Madrid talento, empleo e inversión en el sector y en las actividades económicas relacionadas.

Por todo ello, y por el carácter único del clúster de Ciberseguridad de Madrid – CYBERMAD no se considera necesario dar publicidad a esta actuación para promover la concurrencia, ya que no existen a la fecha otras entidades con similares características, objetivos y naturaleza, regulándose en el presente convenio las condiciones y compromisos aplicables de conformidad con la ley.

Por cuanto antecede, ambas partes, reconociéndose mutuamente capacidad suficiente para ello, acuerdan suscribir el presente convenio subvención que habrá de regirse por las siguientes:

ESTIPULACIONES

PRIMERA.- OBJETO DE LA SUBVENCIÓN

El objeto del presente convenio es el de apoyar el esfuerzo de promoción de la ciberseguridad en el tejido empresarial de la economía madrileña, tanto desde el punto de vista de las empresas demandantes de productos y servicios de ciberseguridad, (con particular atención a PYMEs y Autónomos), como a las ofertantes de los mismos, sean éstas empresas de cualquier tamaño, otras entidades y centros de investigación y de docencia, así como otras entidades del ecosistema de la ciberseguridad, usuarios y particulares.

Para tal fin se estipula la concesión de una subvención directa por parte del Ayuntamiento de Madrid al clúster de Ciberseguridad de Madrid – CYBERMAD por importe máximo de CINCUENTA MIL EUROS (50.000 €) en el año 2023, para la financiación de las actividades tendentes a conseguir los objetivos descritos.

Esta labor se desarrollará con un enfoque integral a través de las actividades subvencionables, objetivos y bloques de actuación que se detallan en las Estipulaciones siguientes.

SEGUNDA. - ACTIVIDADES SUBVENCIONABLES EN EL MARCO DEL CONVENIO SUBVENCIÓN ENTRE EL AYUNTAMIENTO DE MADRID Y CYBERMAD PARA LLEVAR A CABO LAS LABORES DE APOYO AL DESARROLLO DEL SECTOR DE LA CIBERSEGURIDAD EN MADRID

CYBERMAD se compromete, a lo largo del ejercicio, a la promoción de su sector de acuerdo con el objeto de este convenio a través de diferentes actividades.

Las actividades se articularán en bloques o paquetes de actividades, según se detalla a continuación y en el Anexo a este convenio, en el que se recogen los indicadores de actividad para cada bloque actuaciones, así como sus metas, las fuentes de acreditación y la forma o soporte documental de la acreditación, y el importe de la subvención para cada bloque.

Las actuaciones tienen un enfoque integral y se sustentan en los bloques de actividad siguientes:



1. BLOQUE DE PROYECTOS TÉCNICOS Y SECTORIALES
2. BLOQUE DE PROYECTO DE CRECIMIENTO DEL ECOSISTEMA CYBER
3. BLOQUE DE COMUNICACIÓN, DIFUSIÓN Y ORGANIZACIÓN INTERNA

2.1.- BLOQUE DE PROYECTOS TÉCNICOS Y SECTORIALES

Uno de los objetivos fundamentales de un clúster de contenido tecnológico, encuadrado en la finalidad última de dinamización de la actividad económica de la ciudad, es el de la contribución al desarrollo de estudios, análisis y **nuevos proyectos que beneficien y potencien el emprendimiento**.

Para ello, el clúster podrá ayudar a promover y presentar proyectos de desarrollo de estudios, análisis, productos, bienes y servicios relacionados con la ciberseguridad, bien en el ámbito del diagnóstico y prevención, bien en el de la defensa frente a ciberataques, la recuperación de datos afectados por éstos últimos, o cualquier otro de carácter preventivo, defensivo, o posterior a los ataques sufridos, de resiliencia y/o recuperación, tanto a nivel transversal como vertical o sectorial.

Los mismos podrán revestir la naturaleza **estudios técnicos, de proyectos singulares, de MDI (Manifestaciones de interés en el contexto de las iniciativas de cara a los Fondos Europeos conocidos como "Next Generation EU") u otros** vehiculados a través del clúster, o seleccionados o presentados a través de los Grupos de trabajo u otros órganos del mismo.

En este sentido, se observa una línea general de actuaciones por parte de la administración con enfoques Sectoriales, así como movimientos orientados a fortalecimientos de Clústeres, HUBs, asociacionismo, y proyectos en la línea del proyecto RETECH (Redes Territoriales de Especialización Tecnológica) que tienen un alto componente de enfoque sectorial. Por todo ello, CyberMadrid desarrollará proyectos que impulsen el desarrollo de soluciones y servicios para mejorar el nivel de ciberseguridad en determinados sectores (salud y logística) con el objetivo de que las empresas de la región implementen esas soluciones y servicios, apoyándose para ello en una activa colaboración público-privada.

En las actividades relativas a este bloque de Desarrollo de Proyectos Técnicos y Sectoriales, se llevarán a cabo 5 actuaciones en total, entre actuaciones propias del Clúster, proyectos inter-clúster y acciones de gestión de Proyectos internos.

La definición de proyectos en este apartado es enunciativa, no exhaustiva ni limitativa, dada la necesaria flexibilidad en su ejecución en función de la evolución de las necesidades del sector, de la disponibilidad de recursos técnicos y profesionales, etc. Se propone una lista tentativa de actuaciones o proyectos enunciando los siguientes proyectos posibles, incluyendo una breve descripción de sus diferentes contenidos:

- **Ciberseguridad en el sector de la salud:**



Tal y como señala la Agencia de la UE para la Ciberseguridad "ENISA" en su informe "ENISA THREAT LANDSCAPE: HEALTH SECTOR – July 2023":

"...only 27% of organizations surveyed in the health sector have a dedicated ransomware defense program, and 40% of the original equipment suppliers (OES) surveyed have no security awareness program for non-IT staff. In another recent survey by the NIS cooperation group, 95% of the health organizations surveyed face challenges when performing risk assessments, while 46% have never performed a risk analysis."

Esto significa que el sector de la salud, tanto público como privado (o público de gestión privada o concesional), a pesar de tener una "superficie de exposición elevada" a ciberataques por el manejo de información sensible (i.e., historiales médicos), maquinaria costosa y cada vez más conectada (vía IoT / 5G), y sistemas de gestión (citas, gestión de listas de espera, contabilidad, etc.) altamente informatizados, carecen en muchos casos de las herramientas de protección suficientes.

Esto ha quedado de manifiesto por ejemplo en los múltiples ciberataques y *ransomware* recientemente sufridos por varios hospitales españoles o de otros países de nuestro entorno. Mejorar la ciberseguridad global o, al menos inicialmente, la de determinados subsectores de la salud en nuestra ciudad y región es así un objetivo primordial. El mismo se enmarca en proyectos como por ejemplo el de RETECH presentado por la Comunidad de Madrid, que se realizará en un marco de colaboración con otras Comunidades autónomas y el INCIBE.

El clúster CyberMad persigue tener un papel muy activo en varios de los proyectos vinculados al mismo, bien de carácter global, bien en subsectores específicos de la salud con fuerte presencia en la ciudad (clínicas dentales, FIV, hospitales y clínicas privadas en general, o de carácter público local (CMS, etc.), e incluso participando junto con algunos de sus socios y miembros en la gobernanza del mismo. Además, el proyecto reviste fuerte potencial de colaboración con otros clústeres promovidos por el Ayuntamiento, como el de e-Health.

- Ciberseguridad en el ámbito empresarial (pymes, empresas, corporaciones...)

En el "PLAN DE DIGITALIZACIÓN DE PYMES 2021-2025" del gobierno de España se señala que en nuestro país "... las empresas de menos de 50 trabajadores, micropymes y autónomos, suman el 98,99% del total de empresas y el 49,58% del empleo..." y como añade el mismo informe, "España, que presenta una evolución positiva de los principales indicadores internacionales de digitalización en los últimos años, ... no ha avanzado de la misma manera en la dimensión de Integración de Tecnología Digital por parte de las empresas", con un desfase además particularmente grave entre las PYMES. Este retraso en la digitalización conlleva déficits importantes no solo en términos de productividad del tejido empresarial, sino también en seguridad y ciber-resiliencia de las pequeñas empresas.

En ese contexto, el citado Plan de digitalización detalla varios objetivos y actuaciones, y tras el primero (el conocido "Kit Digital"), y las inversiones en conectividad para PYMES, señala un 3er objetivo, "PROTEGE TU EMPRESA (CIBERSEGURIDAD)" con acciones de sensibilización, concienciación, educación y formación en ciberseguridad, dirigido específicamente a la PYME y microempresa, ya que el nivel de protección de las mismas es notoriamente bajo.



En esta línea, el clúster ha remitido una MDI – Manifestación de Interés, denominada PYME 3D Secure, para facilitar que las PYMEs, particularmente madrileñas, sean capaces de abordar sus proyectos de digitalización asegurando unas condiciones mínimas de ciberseguridad, con varias actuaciones a desarrollar: Proporcionar soluciones de ciberseguridad específica para las Pymes; Fomentar la Ciberseguridad de las mismas mediante posibles ayudas directas para su implantación; establecer un mapeo o directorio de Empresas especialistas en Ciberseguridad y sus productos y servicios; el desarrollo de un centro de empleabilidad Ciber y el fortalecimiento de la formación profesional en ciberseguridad; otras actuaciones de *mentoring* y fomento del emprendimiento en Ciberseguridad.

Este proyecto, por su dimensión y ambición, no podría desarrollarse en una única fase de ejecución, y reclamaría el patrocinio de varias entidades privadas y/o públicas a lo largo de varios ejercicios, empezando necesariamente con un mapeo de la PYME madrileña desglosada en sus principales sectores, desde el análisis de sus niveles de digitalización, niveles actuales de ciberseguridad y vulnerabilidades, etc.

- Proyecto de análisis y diagnóstico de la ciberseguridad para empresas

Este proyecto sería complementario del anterior (pudiendo constituir un módulo dentro del mismo), aunque tiene entidad propia al poder estar: (a) dirigido al conjunto de las empresas madrileñas, sea cual sea su tamaño, y (b) orientado específicamente al diagnóstico de las vulnerabilidades en términos de ciberseguridad de las empresas, mediante el desarrollo de herramientas específicas (cuestionarios, herramientas on-line, etc.) para el análisis individual de cada empresa. Si bien existen ya herramientas en el mercado (algunas gratuitas, otras con esquema “freemium”), las mismas son susceptibles de mejora, o necesitan completarse con productos que permitan gestionar la transición entre el mero diagnóstico y la mejor implementación posible de las medidas de protección, herramientas de recuperación, etc.

Este proyecto se incardina además con otro, transversal (al incluir colaboración con otro de los clústeres promovidos desde el Ayuntamiento, como el de MadFintech – Madrid Capital Fintech), de desarrollo de ciberseguros específicos, un producto que necesita obligatoriamente de herramientas de diagnóstico previo.

- Ciberseguridad en las Administraciones Públicas

La modernización y digitalización de las Administraciones Públicas es un proceso continuo y, por definición, siempre inacabado. A título de ejemplo, el Ministerio de Política Territorial y Función Pública, en colaboración con el Ministerio de Asuntos Económicos y Transformación Digital, instaron en 2021 a los miembros de la Conferencia Sectorial de Administración Pública a presentar propuestas a encuadrar en cinco líneas estratégicas: Administración orientada a la ciudadanía; Operaciones inteligentes; Gobierno del dato; Infraestructuras digitales y Ciberseguridad.

En esa línea, el clúster puede colaborar con las administraciones territoriales (el propio Ayuntamiento de Madrid, el IAM, la Comunidad, con su Agencia de Ciberseguridad de la Comunidad de Madrid, el propio INCIBE, etc.) para incidir en la dimensión de la ciberseguridad en las mismas, ya que presentan perfiles similares a los del mencionado sector de la salud: manejo de datos sensibles de los



ciudadanos y de las empresas, gestión de infraestructuras y servicios esenciales (salud, transportes, suministro de agua...).

- Proyecto de colaboración en la mejora en formación en ciberseguridad

El clúster ya ha colaborado en iniciativas de formación del Ayuntamiento de Madrid, como por ejemplo la denominada "Escuela de talento", que impartió en su programa piloto formaciones específicas en dos áreas: programación en Python, y Ciberseguridad.

El clúster puede seguir colaborando con las administraciones y con centros docentes (tanto públicos como privados, al tener ya entre sus socios a varias universidades como la Politécnica de Madrid o la Universidad Antonio de Nebrija) para, junto con las empresas privadas (que conocen las necesidades de formación de sus profesionales, y los déficits o dificultades de obtención de determinados perfiles en el mercado) ayudar a diseñar mejor los contenidos teóricos o los recorridos en prácticas de los distintos niveles, desde la FP hasta las carreras STEM.

A tal efecto, el clúster ha puesto en marcha entre sus 4 grupos de trabajo, uno específico de "Formación y empleabilidad" con esa misma finalidad.

2.2. BLOQUE DE PROYECTO DE CRECIMIENTO DEL ECOSISTEMA CYBER

Con el fin de posicionar a Madrid como centro de referencia nacional e internacional en el ámbito de la Ciberseguridad, y lograr una colaboración estrecha entre los distintos agentes del ecosistema del sector en nuestra ciudad, el crecimiento del clúster y la agregación al mismo del mayor número de socios, colaboradores, empresas y entidades que aporten valor, la captación de socios y la dinamización de su colaboración constituyen un objetivo fundamental.

A tal fin, se marcan objetivos alcanzables de crecimiento del clúster, medido particularmente en el número de socios o de entidades colaboradoras del mismo, principalmente de entidades con sede, actividad o centros de producción en Madrid.

Además, el crecimiento del Clúster ha de llevarse a cabo de manera coordinada con otras instituciones públicas, entidades privadas, entidades sin ánimo de lucro y organizaciones vinculadas al propio Ayuntamiento de Madrid y Comunidad de Madrid en coherencia con los objetivos relacionados en sus estatutos. Por tal razón, según sus estatutos el clúster cuenta con un Consejo asesor que, entre otras funciones, da el visto bueno a los nuevos miembros - Consejo en el que participan, además del Ayuntamiento de Madrid, otras administraciones e instituciones, como la Comunidad de Madrid o el INCIBE.

A tal efecto, en este bloque de crecimiento orgánico del clúster, y del conjunto del ecosistema Cyber, se desarrollarán actuaciones de captación y seguimiento de nuevos socios, de atención al Socio ya incorporado (canal del asociado, documentación, facturas, consultas...), y se desarrollará, según, el Plan de Alianzas Estratégicas mencionado anteriormente, el modelo relacional con otras Instituciones, Empresas y Organismos (acuerdos, colaboraciones con otras asociaciones y clústeres, - tanto del Ayuntamiento de Madrid como de otros territorios - para generar sinergias horizontales; desarrollo de un marco estratégico de relaciones, etc.).



En las actividades relativas a este Bloque de Crecimiento del ecosistema Cyber, se llevarán al cabo 125 actuaciones en total, incluyendo las relacionadas con la atención al socio (canal del asociado, documentación, facturas, consultas, etc.), actuaciones de captación y seguimiento y aquellas vinculadas al Modelo relacional con Instituciones, Empresas y Organismos (acuerdos con terceras entidades, vinculaciones de colaboración, etc.)

En particular:

Canal del asociado: unas 100 actuaciones en relación con la interactividad de los asociados con el Clúster (consultas, emisión de facturas, etc.).

Captación y seguimiento de nuevos socios: 12 y búsqueda de patrocinios: 5
Modelo relacional con otros clústeres, Instituciones, Empresas y Organismos: 8 actuaciones (reuniones, acuerdos y colaboraciones).

Así, el total de actividades de este Bloque 2 de Crecimiento del ecosistema Cyber será de 125 actuaciones.

2.3. BLOQUE DE COMUNICACIÓN, DIFUSIÓN Y ORGANIZACIÓN INTERNA

Este bloque comprenderá todas las actividades relacionadas con la comunicación de conceptos, técnicas y productos relacionados con la Ciberseguridad, la necesidad de su implementación en las empresas, entidades y consumidores, y la difusión de las actividades del propio clúster, así como de las actividades de otras entidades relacionadas con el sector y el Clúster.

Estas actividades se plasmarán en la elaboración y divulgación de documentos públicos o publicables como por ejemplo: una *newsletter* propia (en formato digital), notas de prensa y artículos de prensa, folletos o documentos sintéticos, etc.

Por otro lado, el mero crecimiento cuantitativo del clúster, medido como aumento del número de socios, es condición necesaria pero no suficiente para la dinamización del sector de la ciberseguridad en nuestro país. Su dinamismo deberá traducirse a la postre en su capacidad para difundir y organizar, en su caso, eventos de divulgación, evangelización, formación, dinamización empresarial y en general cualesquiera contenidos que contribuyan a ampliar la actividad económica del sector en la ciudad – ya que el objetivo último del clúster, y del presente convenio, es el de atraer talento, inversión, empleo y actividad empresarial ligados a este sector en la ciudad de Madrid.

Para conseguir estos fines, por tanto, el Clúster de Ciberseguridad de Madrid deberá desarrollar una organización interna transparente, eficaz y con órganos de decisión colegiados que representen adecuadamente a las entidades del ecosistema Cyber que sean miembros del mismo, y que sirvan para dar proyección al sector y a la ciudad.

Por ello, en este bloque se recogen tanto la organización de las diferentes reuniones internas (tales como la Junta Directiva, el Consejo Asesor, reuniones con la Dirección, la Asamblea General o los diferentes Grupos de Trabajo del clúster) como también los diferentes eventos que pudiera organizar el Clúster no relacionados directamente con la presentación de proyectos del bloque 1 y las reuniones externas y /o eventos (con terceros, con empresas no madrileñas que proyecten instalarse en Madrid, con homólogos internacionales, etc.), incluyendo tanto la generación de eventos propios en Madrid, como la participación activa en eventos de terceros (en la ciudad o fuera



de ella) que permitan dar a conocer el ecosistema de Ciberseguridad de nuestra ciudad y el propio clúster.

La huella que ha dejado la pandemia en la sociedad, impone un modelo de realización de eventos o reuniones de tipo mixto, en el que la opción virtual se complementa con la presencial, lo que por otro lado permite maximizar el número de participantes y contribuir al objetivo de la digitalización.

Dada la importancia de ese entorno virtual se hace imprescindible la utilización de elementos tecnológicos para su organización. Entre las tareas a desarrollar en el ámbito de su preparación destacan: la definición del modelo de evento; perfil de los ponentes y moderadores, aspectos técnicos, visión del evento vía *streaming* o herramientas similares, así como definición de su agenda; Desarrollo en su caso de la contratación con entidades terceras para su organización; Definición de los clientes que son objetivo del evento y de una estrategia de comunicación tanto a nivel de redes sociales como portal web corporativo, de la infografía a utilizar, del modelo de inscripción al evento vía Internet (registro *on line* de asistentes); y por último, las actuaciones posteriores, como el tratamiento de los videos para su publicación en redes o vía portal web, así como las presentaciones de los ponentes y otra información relevante, etc.

- **Comunicaciones periódicas y/o puntuales: Publicaciones y artículos relacionados con la ciberseguridad**

La Ciberseguridad, aunque ya integrada en la cultura de la mayoría de las grandes empresas financieras, tecnológicas o industriales o en las administraciones de mayor tamaño, sigue siendo la gran desconocida entre el público en general, las PYMEs, los autónomos o los ciudadanos (desde los más jóvenes, "hiperdigitalizados", hasta las personas mayores, normalmente poco conocedoras del mundo Cyber).

La pandemia ha hecho explotar el uso de herramientas digitales (por ejemplo, el número de empresas que arbitraron mal que bien el teletrabajo, las reuniones telemáticas, etc., así como la compra vía internet entre los consumidores) y sin embargo, apenas ha habido un esfuerzo en paralelo para facilitar la toma de conciencia entre esos agentes, de los riesgos que conlleva esa creciente digitalización – por no hablar de los desarrollos inmediatos o futuros tales como el IoT o la conectividad 5G.

Una de las labores del clúster será la de participar en esa labor de "evangelización" y comunicación mediante la publicación en su página web de Notas de Prensa y Artículos de Prensa, que recojan contenidos tanto sobre la necesidad de la ciberseguridad como sobre la actividad y novedades del sector. Por otro lado, el Clúster realiza una *newsletter* electrónica de periodicidad mensual que recoge las novedades de la asociación, puesta en marcha de diferentes proyectos, eventos e iniciativas junto con noticias destacadas de nuestros asociados y del Sector.

Todo ello se enmarca en una Estrategia de comunicación coherente complementada con material específico de mensajes diseñados ad hoc según los distintos públicos objetivo.

- **Comunicación permanente o "no periódica": Página web, y herramientas colaborativas**

El Clúster, con una trayectoria todavía corta en el tiempo, ha de consolidarse, darse a conocer entre las entidades madrileñas y nacionales, profundizar en su imagen de



marca mediante su presencia en redes sociales, Internet, etc. que permita la captación de nuevos socios para ampliar la base de entidades que componen el Clúster de acuerdo con los criterios establecidos en sus estatutos.

Así, adicionalmente a las publicaciones mencionadas en el punto anterior, el clúster continuará con su labor de comunicación mediante su página web donde se recogerá toda la información y publicaciones anteriores una vez editadas, acceso a información estatutaria del clúster para terceros y/o candidatos a la membresía, con su permanente actualización de contenidos y mantenimiento; cuentas de correo corporativas; dominios con su correspondiente registro oficial, y otras herramientas colaborativas que permitan la mejor interacción on-line de los socios del clúster, de sus grupos de trabajo, o de cara a terceros.

La página web será publicitada y divulgada para que pueda ser un instrumento de consulta de ciudadanos, empresas, otras instituciones y agentes sociales interesados en la ciberseguridad, así como para contribuir de manera general a la difusión de la imagen del sector y de la ciudad.

En las actividades relativas a este Bloque de Comunicación y Difusión, se llevarán al cabo 15 actuaciones, incluyendo actuaciones relacionadas con las comunicaciones periódicas y/o puntuales (Publicaciones y artículos relacionados con la ciberseguridad, Elaboración *newsletter*, Notas de Prensa y Artículos de Prensa, *clipping* de prensa etc.) y 4 actuaciones de mantenimiento y actualizaciones de la página web y las comunicaciones por Internet (además del mantenimiento de la Página web, dominios, cuentas de correo, apps de socios u otras herramientas colaborativas).

En las actividades relativas a Organización Interna (eventos, reuniones etc.), se llevarán al cabo 6 actuaciones en total, entre las relacionadas con la Organización de reuniones internas (Junta Directiva, Consejo Asesor, Asamblea, Grupos Trabajo) y organización de eventos o reuniones con terceros (clústeres, asociaciones, Admón., etc.).

Así, el total de actividades de este Bloque 3 de Comunicación, Difusión y Organización Interna será de 25 actuaciones.

TERCERA.- DESTINATARIO DE LA SUBVENCIÓN

El destinatario de la subvención es el Clúster de Ciberseguridad de Madrid - CYBERMAD, que realizará las acciones contempladas en la estipulación Segunda del presente convenio y en su Anexo.

CUARTA. - OBJETIVOS ESTRATÉGICO Y OPERATIVO

El **objetivo estratégico** de las actuaciones previstas en el presente convenio es el de fomentar la actividad económica y el empleo en la Ciudad de Madrid, impulsándolos a través de la mejora de su capacidad productiva y el refuerzo de su competitividad empresarial, mediante acciones, entre otras, orientadas a potenciar los clústeres de determinados sectores, como CYBERMAD.

Este objetivo estratégico se materializará a través del **objetivo operativo** de apoyo a la promoción de la Ciberseguridad en el tejido empresarial de la economía madrileña.



QUINTA.- PRESUPUESTO TOTAL DEL PROYECTO

El presupuesto total del proyecto dirigido a financiar las actividades que realiza CYBERMAD asciende a CINCUENTA MIL EUROS (50.000 euros), de los cuales son aportados por el Ayuntamiento de Madrid como subvención CINCUENTA MIL EUROS (50.000 euros) a recibir por CYBERMAD en el año 2023.

Dicha subvención es compatible con la recepción de otras subvenciones, ayudas, ingresos o recursos para la misma finalidad, procedentes de cualesquiera otras administraciones o entes públicos o privados, nacionales, de la Unión Europea o de organismos internacionales, tal y como se contempla en el artículo 65.3 apartado c) del Real Decreto 887/2006, de 21 de julio, por el que se aprueba el Reglamento de la Ley 38/2003, de 17 de noviembre, General de Subvenciones.

El solicitante deberá declarar todas las ayudas que haya solicitado u obtenido, tanto al iniciarse el expediente administrativo como en cualquier momento del procedimiento en que ello se produzca.

SEXTA.- COSTE ECONÓMICO

El coste económico que se deriva de este convenio subvención asciende a un importe máximo de CINCUENTA MIL EUROS (50.000 euros) en 2023, y estará destinado exclusivamente a subvencionar la realización de las actividades descritas en la estipulación segunda y en el Anexo del presente convenio, de la siguiente manera: hasta el 100% de los costes de las actividades recogidas en cada uno de los epígrafes 2.1, 2.2, y 2.3 de la Estipulación Segunda.

Las distribuciones de las cantidades previstas en cada epígrafe quedan recogidas en el Anexo del presente convenio.

Esta cantidad tiene la consideración jurídica de subvención que se concede como subvención directa, al amparo de lo previsto en el artículo 22.2 c) de la Ley 38/2003, de 17 de noviembre y en el artículo 30.3 de la Ordenanza de Bases Reguladoras Generales para la concesión de Subvenciones por el Ayuntamiento de Madrid y de su Organismos Públicos de 30 de octubre de 2013.

El gasto se imputará con cargo a la aplicación presupuestaria 001/140/433.07/489.01 "Otras transferencias a instituciones sin fines de lucro" del Presupuesto General del Ayuntamiento de Madrid para 2023, del programa "Estrategias de desarrollo económico y análisis de la economía de Madrid" de la Dirección General de Economía.

En ningún caso la subvención directa concedida excederá, aislada o en concurrencia con otras subvenciones procedentes de entidades públicas o privadas, el coste de la actividad subvencionada.

SÉPTIMA.- FORMA DE PAGO

Con base en lo dispuesto en el artículo 34.4 de la Ley 38/2003, de 17 de noviembre, el pago de la subvención se realizará mediante un pago anticipado del 100% del importe con posterioridad a la firma del convenio por ambas partes y dentro del ejercicio presupuestario de 2023.



Dado el contenido del proyecto a desarrollar, de indudable interés para Ayuntamiento de Madrid, en aras de sumar esfuerzos en la tarea de modernizar el tejido productivo de la ciudad, por su espacio temporal actual, el carácter que tiene la entidad firmante, "Asociación sin ánimo de lucro", así como la carencia de recursos suficientes para financiar las actividades subvencionadas, dada la todavía insuficiente capacidad de autofinanciación de la entidad a través de sus cuotas y aportaciones, es necesario el pago anticipado.

El importe final de la subvención y para este caso, del reintegro que proceda, por tratarse de subvenciones de pago anticipado, dependerá de la realización de las actividades previstas en la estipulación Segunda y su justificación, y no sobrepasará la cantidad de CINCUENTA MIL EUROS (50.000 €).

De acuerdo con lo dispuesto en el artículo 22.2 de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones, en relación con lo establecido en el artículo 42.2 del Reglamento de la Ley 38/2003, de 17 de noviembre, al ser CYBERMAD una entidad sin ánimo de lucro, así como por el objeto de la actividad subvencionada, no se considera preciso que preste garantía alguna por el pago de la subvención con carácter anticipado a la realización de dichas actividades.

OCTAVA.- GASTOS SUBVENCIONABLES

Los gastos que podrán ser financiados con la subvención serán los directamente relacionados con la realización de las actividades objeto del convenio, que se describen en la estipulación Segunda, y cuya distribución concreta aparece detallada en el Anexo del presente convenio regulatorio de la subvención.

En cuanto a los costes indirectos asociados a la realización de las actividades objeto del convenio, de acuerdo con lo establecido en el artículo 51 de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones, se acuerda que será subvencionable el importe correspondiente al 8% del importe justificado de la subvención concedida a CYBERMAD de las actividades recogidas en los epígrafes 2.1, 2.2, y 2.3, de la estipulación segunda "Actividades Subvencionables", en concepto de costes indirectos. En todo caso, y tal y como determina el mencionado artículo 51 de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones, precisarán de la certificación del responsable de la entidad, no siendo necesaria la aportación de los justificantes de gasto.

En ningún caso la aportación municipal podrá destinarse a gastos de inversión, garantía bancaria, equipos o bienes inventariables y a impuestos personales sobre la renta. Tampoco se podrá destinar la aportación municipal a gastos de representación (como, por ejemplo, gastos de comida, viajes, alojamiento o manutención) u otros gastos no relacionados con los bloques de actividad mencionados en la Estipulación Segunda, ni a gastos de personal, si los hubiere.

El importe imputado a las actuaciones subvencionables y, en su totalidad del convenio, en ningún caso podrá ser de tal cuantía que supere su presupuesto.

Para desarrollar las actividades subvencionables recogidas en la estipulación Segunda en materia de subcontratación se estará a lo dispuesto en el artículo 31 de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones.



- Si la subcontratación se concierta con empresas o entidades vinculadas con el beneficiario, de acuerdo con lo establecido en el artículo 68.2 del Reglamento de la Ley 38/2003, de 17 de noviembre, será necesario que la contratación se realice de acuerdo con las condiciones normales de mercado y se obtenga la previa autorización del órgano concedente. A estos efectos, el beneficiario solicitará dicha autorización por escrito con carácter previo a la celebración del contrato, no pudiendo celebrarse éste hasta que la misma fuera otorgada. Si en el plazo de un mes no se hubiera dictado resolución al respecto, los interesados podrán entender desestimada su solicitud por silencio administrativo. Las actividades que se subcontraten con personas o entidades vinculadas con el beneficiario y que no cuenten con la preceptiva autorización, no se considerarán gastos subvencionables. En particular, no se considerarán gastos subvencionables aquellos que el beneficiario subcontrate, en su caso, con empresas que pertenezcan a la Junta Directiva de CYBERMAD.

Para obtener la preceptiva autorización, el beneficiario deberá solicitar como mínimo tres ofertas de diferentes proveedores, con carácter previo a la prestación del servicio o la entrega del bien, salvo que por sus especiales características no exista en el mercado suficiente número de entidades que los realicen, presten o suministren, o salvo que el gasto se hubiere realizado con anterioridad a la concesión de esta subvención pero siempre dentro del período definido como subvencionable.

La elección entre las ofertas presentadas, que deberán aportarse en la justificación, o, en su caso, en la solicitud de subvención, se realizará conforme a criterios de eficiencia y economía, debiendo justificarse expresamente en una memoria la elección cuando no recaiga en la propuesta económica más ventajosa.

- Cuando la actividad concertada con terceros exceda del 20 por ciento del importe de la subvención y dicho importe sea superior a 60.000 euros, la subcontratación estará sometida al cumplimiento de los requisitos establecidos en el artículo 29.3 de la Ley 38/2003, de 17 de noviembre, en relación con lo dispuesto en el apartado 5 del artículo 31 de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones.

El contrato deberá celebrarse por escrito y la celebración del mismo se autorizará previamente por el órgano concedente de la subvención, para lo cual el beneficiario solicitará dicha autorización por escrito al citado órgano con carácter previo a la celebración del contrato, no pudiendo celebrarse éste hasta que la misma fuera otorgada. Si en el plazo de un mes no se hubiera dictado resolución al respecto, los interesados podrán entender desestimada su solicitud por silencio administrativo. Las actividades que se realicen con terceros superando los límites anteriores y que no cuenten con la preceptiva autorización no se considerarán gastos subvencionables. A estos efectos, no podrá fraccionarse un contrato con el objeto de disminuir la cuantía del mismo y eludir el cumplimiento de los requisitos exigidos.

Cuando el importe del gasto subvencionable supere las cuantías establecidas en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, por la que se transponen al ordenamiento jurídico español las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, para el contrato menor, se estará a lo establecido en el artículo 32.2 de la Ordenanza de Bases



Reguladoras para la Concesión de Subvenciones, el beneficiario deberá solicitar como mínimo tres ofertas de diferentes proveedores, con carácter previo a la contratación del compromiso para la prestación del servicio, salvo que por sus especiales características no exista en el mercado suficiente número de entidades que los realicen, presten o suministren, o salvo que el gasto se hubiere realizado con anterioridad a la concesión de esta subvención pero siempre dentro del período definido como subvencionable, o que ya exista un contrato marco formalizado por el beneficiario que cubra la totalidad o parte de los servicios necesarios para el desarrollo de las actividades del presente convenio. La elección entre las ofertas presentadas, que deberán aportarse en la justificación, o, en su caso, en la solicitud de subvención, se realizará conforme a criterios de eficiencia y economía, debiendo justificarse expresamente en una memoria, la elección cuando no recaiga en la propuesta económica más ventajosa. Cuando con cargo a la subvención concedida se realicen contratos que cumplan los requisitos establecidos en el artículo 23 en la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, a dichos contratos se les aplicarán las normas previstas en la citada Ley respecto de los contratos subvencionados.

Los tributos son gasto subvencionable cuando el beneficiario de la subvención los abona efectivamente. En ningún caso se consideran gastos subvencionables los impuestos indirectos cuando sean susceptibles de recuperación o compensación ni los impuestos personales sobre la renta.

A los efectos de realización de las actuaciones descritas en la estipulación Segunda, el período subvencionable abarca desde la fecha de la firma hasta el primer aniversario de la misma, ambos inclusive.

No obstante, se podrán subvencionar gastos anteriores al inicio del periodo subvencionable, en los que haya incurrido el beneficiario para el desarrollo inicial o arranque de los proyectos mencionados en los bloques recogidos en la Estipulación Segunda, siempre que los citados gastos se hayan devengado entre el 1 de septiembre de 2023 y la fecha de la firma del presente convenio.

NOVENA. - EVALUACIÓN DE LA ACTIVIDAD SUBVENCIONADA

El Ayuntamiento de Madrid, durante el período de ejecución y a la finalización del presente convenio, evaluará el desarrollo de las actividades propuestas y su vinculación con el objetivo estratégico programado, a través de los indicadores, metas y fuentes de verificación que se establecen en el Anexo de este convenio y mediante la cumplimentación de los documentos que en el mismo se relacionan.

Así pues, se establece para este convenio un sistema de pago por resultados que medirá la diferencia entre el resultado inicialmente previsto y el definitivamente conseguido, sirviendo la diferencia para modular el importe definitivo de la subvención y cuantificar el correspondiente reintegro, si así procediera. El reintegro se calculará, en su caso, aplicando la ponderación indicada en el reiterado Anexo.

DÉCIMA. - FORMA Y PLAZO DE LA JUSTIFICACIÓN

A efectos de la justificación de la subvención se estará a lo dispuesto en el artículo 30 de la Ley 38/2003, de 17 de noviembre, en los artículos 72 y siguientes del Reglamento



de la Ley 38/2003, de 17 de noviembre, y en el artículo 35 de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones.

Una vez finalizado el período subvencionable, y en cualquier caso, en los tres meses siguientes al mismo, el beneficiario deberá presentar la justificación de los fondos recibidos a través del registro electrónico del Ayuntamiento de Madrid, accediendo a la sede electrónica <https://sede.madrid.es>.

De conformidad con lo dispuesto en el artículo 35 de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones, la cuenta justificativa deberá contener la siguiente documentación:

- a) **Memoria e Informe de Evaluación de Actividades:** consistirá en una descripción detallada de las actividades subvencionables realizadas contempladas en la estipulación Segunda y en la introducción del dato cuantitativo correspondiente al indicador establecido a fin de medir el grado de consecución (Anexo).

En la memoria deberá hacerse constar expresamente que ha sido cumplida la finalidad para la que se otorgó la subvención conforme al proyecto presentado, evaluando los resultados obtenidos respecto a los previstos.

- b) **Memoria económica:** consistirá en la acreditación económica justificativa del coste de las actividades subvencionables (estipulación Segunda) descritas en la Memoria de Actividades y contendrá, siguiendo el orden numérico, los siguientes apartados:

1. Relación numerada y clasificada de gastos realizados, con identificación del acreedor y del documento, su importe, fecha de emisión y fecha de pago.

Para cada uno de los gastos relacionados se indicará cuál ha sido la fuente de financiación. Cuando se hubiera utilizado más de una fuente de financiación se indicará el porcentaje en el que hubiera participado cada una de ellas.

2. Facturas, recibos, tributos y demás documentos de valor probatorio equivalente, con validez en el tráfico jurídico mercantil o con eficacia administrativa, que respalden las actividades realizadas cuyo importe haya sido abonado a cargo a la subvención concedida. Se indicará expresamente el porcentaje de IVA imputado o la no imputación del mismo, si fuera el caso, así como la documentación acreditativa del pago de los mismos, que se realizará por alguna de las siguientes formas:

- a. Resguardo del cargo de las transferencias bancarias realizadas.
- b. en caso de pago mediante cheque, extracto bancario del cargo en cuenta.
- c. si el pago se realiza en efectivo, sólo se admitirá el pago en metálico en facturas de cuantía inferior a seiscientos euros. Dichos pagos se justificarán mediante factura o recibí firmado por el acreedor indicando fecha de abono.
- d. Certificación del beneficiario del porcentaje de la subvención concedida como costes indirectos asociados a la realización de las actividades



recogidas en los epígrafes 2.1, 2.2, 2.3, 2.4 y 2.5 de la estipulación segunda "Actividades Subvencionables".

Dichos documentos originales deberán estampillarse por el beneficiario para facilitar el control de la concurrencia de otras subvenciones otorgadas para la misma finalidad, debiendo reunir la estampilla, como mínimo, los siguientes datos:

Número de expediente administrativo.

Denominación del proyecto subvencionado.

Ejercicio económico de la concesión de la subvención.

Órgano concedente de la subvención.

Porcentaje de financiación imputable a la subvención.

Las facturas y, en su caso, los documentos sustitutivos habrán de reunir los requisitos que exige el Reglamento por el que se regulan las obligaciones de facturación, aprobado por Real Decreto 1619/2012, de 30 de noviembre.

Los originales de dichos documentos quedarán depositados y custodiados por el beneficiario en tanto puedan ser objeto de las actuaciones de comprobación y control.

3. Documentación acreditativa de los rendimientos financieros que se generen por los fondos librados. En el supuesto de que no se hubieran generado rendimientos financieros se aportará declaración responsable al respecto.
4. Relación detallada de otros ingresos o subvenciones que hayan financiado las actividades objeto del presente convenio subvención, con indicación del importe y su procedencia. De no existir otros ingresos o subvenciones, se aportará declaración responsable al respecto.
5. Cuando el importe del gasto subvencionable supere las cuantías establecidas en la Ley 9/2017, de 8 de noviembre, para el contrato menor, el beneficiario deberá solicitar, como mínimo, tres ofertas en los términos establecidos en el artículo 31.3 de la Ley 38/2003, de 17 de noviembre.
6. En su caso, la carta de pago de la devolución voluntaria en el supuesto de remanentes no aplicados, así como de los intereses derivados de los mismos.
7. Declaración responsable de no hallarse incurso en las prohibiciones descritas en el artículo 13 de la Ley 38/2003, de 17 de noviembre.
8. Declaración responsable del cumplimiento de obligaciones por reintegro de subvenciones.
9. Declaración responsable del perceptor de que ha sido cumplida la finalidad para la cual se otorgó la subvención.



10. Declaración responsable acreditativa del importe, procedencia y aplicación de otras subvenciones distintas a la municipal que han financiado actividades objeto del presente convenio, en su caso.

11. Certificado acreditativo, de conformidad con el artículo 22 del Reglamento de la Ley 38/2003, de 17 de noviembre, de hallarse al corriente de obligaciones tributarias y de seguridad social.

A la finalización de los plazos establecidos para la justificación, es decir, en los tres meses siguientes a la terminación del periodo de gasto subvencionable, una vez presentados todos los documentos justificativos de las actividades objeto de subvención, se estudiarán los mismos y, en especial, se atenderá al Informe de Evaluación, para conocer hasta qué punto se han conseguido los resultados que se pretendían.

DECIMOPRIMERA.- OBLIGACIONES DE LAS PARTES

Obligaciones de CYBERMAD:

Esta entidad ostenta el derecho de percibir el importe de la subvención en los términos establecidos en la estipulación Séptima, y queda obligada conforme a las estipulaciones de este convenio a:

1. Cumplir el objeto del convenio que fundamenta la concesión de la aportación.
2. Justificar ante el Ayuntamiento de Madrid el cumplimiento de los requisitos y condiciones, así como la realización de la actividad y el cumplimiento de la finalidad que determinen la concesión de la aportación.
3. Someterse a las actuaciones de comprobación, a efectuar por el Ayuntamiento de Madrid, así como cualesquiera otras de comprobación y control financiero que puedan realizar los órganos de control competentes, tanto nacionales como comunitarios, aportando cuanta información le sea requerida en el ejercicio de las actuaciones anteriores.
4. Comunicar al Ayuntamiento de Madrid la obtención de otras subvenciones, ayudas, ingresos o recursos que financien las actividades subvencionadas. Esta comunicación deberá efectuarse tan pronto como se conozca y, en todo caso, con anterioridad a la justificación de la aplicación dada a los fondos percibidos.
5. Disponer de los libros contables, registros diligenciados y demás documentos debidamente auditados en los términos exigidos por la legislación mercantil y sectorial aplicable al beneficiario, así como cuantos estados contables y registros específicos sean exigidos por este convenio, con la finalidad de garantizar el adecuado ejercicio de las facultades de comprobación y control.
6. Conservar los documentos justificativos de la aplicación de los fondos recibidos, incluidos los documentos electrónicos, en tanto puedan ser objeto de las actuaciones de comprobación y control.
7. Acreditar que se halla al corriente en el cumplimiento de sus obligaciones tributarias, incluidas las municipales y frente a la Seguridad Social, y que no es deudor por resolución de reintegro.



Obligaciones del Ayuntamiento de Madrid:

1. Supervisar el desarrollo de las actividades que debe realizar CYBERMAD y que se describen en la estipulación Segunda.
2. Abonar a CYBERMAD el importe de la subvención en los términos de la estipulación Séptima.

DECIMOSEGUNDA. - RÉGIMEN DE MODIFICACIÓN DEL CONVENIO

De conformidad con lo establecido en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, las partes podrán modificar el convenio en cualquier momento, de mutuo acuerdo y por escrito, previo examen de la Comisión de Seguimiento prevista en la estipulación Decimotercera.

DECIMOTERCERA. - COMISIÓN DE SEGUIMIENTO

Para el seguimiento y desarrollo de las actuaciones contempladas en este convenio, se constituye una comisión de seguimiento con representantes designados por ambas partes en régimen de paridad.

La Comisión de Seguimiento se reunirá, al menos, semestralmente, y siempre que se considere necesario, o cuando lo solicite una de las partes.

Estará formada por:

- La persona titular de la Dirección General de Economía, del Área de Gobierno de Economía, Innovación y Hacienda, o persona en quien delegue.
- La persona titular de la Subdirección General de Análisis Socioeconómicos, de la Dirección General de Economía, o persona en quien delegue.
- Dos representantes del clúster "CYBERMAD", designados por su Presidente.
- La función de Secretaría, que comprenderá la elaboración de las actas de las reuniones, podrá ser encomendada por la Comisión de Seguimiento a uno de sus miembros, o atribuida a un/a funcionario/a representante del Ayuntamiento de Madrid. En este último caso, tendrá voz, pero no voto.

La aprobación de las actas de las sesiones de la Comisión de Seguimiento se someterá a lo establecido en el apartado 2 del artículo 8 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

El Presidente del clúster "CYBERMAD" podrá sustituir a los miembros de la Comisión de Seguimiento designados por parte del clúster, mediante comunicación escrita dirigida a la Dirección General de Economía.

Cuando la Comisión de Seguimiento lo estime necesario, podrá solicitarse la presencia en sus reuniones de personal técnico, con fines de asesoramiento, ya sea propuesto por el Ayuntamiento o por el clúster.

Son funciones de la Comisión mixta de seguimiento:



- a) Resolver las discrepancias que pudieran surgir en torno a la interpretación, desarrollo, modificación, resolución y efectos derivados de la aplicación del presente convenio.
- b) Tomar conocimiento de cualesquiera circunstancias e incidencias que puedan acaecer en el desarrollo del presente convenio.
- c) Velar por el cumplimiento y ejecución del presente convenio.
- d) Autorizar el reajuste de importes asignados inicialmente a cada grupo de actividades como figura en el Anexo al presente convenio, en los términos de la estipulación Sexta.

En ningún caso la Comisión tendrá funciones que, de manera irrenunciable, corresponden a la Administración concedente, como es el caso de la evaluación de las actividades realizadas.

Las decisiones de la Comisión de Seguimiento se adoptarán por mayoría simple.

Para lo no previsto en la presente estipulación, el funcionamiento de esta Comisión se regulará por lo establecido en los artículos 15 y siguientes de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

DECIMOCUARTA. - VIGENCIA Y CAUSAS DE RESOLUCIÓN

La vigencia del presente convenio subvención será de un año, desde el día de su firma, sin posibilidad de prórroga.

Las causas de extinción del convenio, además de por el transcurso del plazo, será el incumplimiento por parte de CYBERMAD de las obligaciones que como beneficiario le impone la Ley 38/2003, de 17 de noviembre, en cuyo caso dará lugar a la iniciación del correspondiente expediente de reintegro de las cantidades percibidas, incluidos los intereses de demora desde la recepción del importe subvencionado, según lo establecido en los artículo 41 y siguientes de la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones y por el artículo 37 de la Ley 38/2003, de 17 de noviembre.

Las partes firmantes del convenio se comprometen a llevar a término las actuaciones que pudieran estar en fase de ejecución a la extinción del convenio.

DECIMOQUINTA. - PROTECCIÓN DE DATOS

El régimen de protección de datos de carácter personal en las actuaciones que se desarrollen en ejecución del presente convenio será el previsto en la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales, así como 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.

La entidad CYBERMAD es responsable directo del tratamiento de datos de carácter personal relativos a los usuarios que atiende, y está obligada al cumplimiento de las prescripciones de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales, comprometiéndose específicamente a:



1. Recabar el consentimiento del interesado para tratar de manera automatizada datos de carácter personal.
2. Utilizar los datos personales para los fines para los que han sido recogidos.
3. Adoptar las medidas de seguridad necesarias que eviten su alteración y tratamiento o acceso no autorizado.
4. Atender las solicitudes de los interesados para ejercitar sus derechos de acceso, rectificación y cancelación de sus datos, en tiempo y forma.

DECIMOSEXTA. - NATURALEZA JURÍDICA

La naturaleza del presente convenio es administrativa, de acuerdo con lo dispuesto en el artículo 28 de la Ley 38/2003, de 17 de noviembre.

Para lo no previsto en el presente convenio, resultará de aplicación, lo dispuesto en la citada de la Ley 38/2003, de 17 de noviembre, en el Reglamento de la Ley 38/2003, de 17 de noviembre, en la Ordenanza de Bases Reguladoras para la Concesión de Subvenciones, en las restantes normas de derecho administrativo, y en su defecto, en las normas de derecho privado que, en su caso, fueran de aplicación.

Serán de aplicación los principios de la Ley 9/2017, de 8 de noviembre, de Contratos del Sector Público, para la resolución de dudas y lagunas que pudieran surgir en la interpretación y aplicación del presente convenio, conforme a lo previsto en su artículo 4.

DECIMOSEPTIMA. - JURISDICCIÓN

Para las cuestiones litigiosas que puedan surgir sobre el cumplimiento del presente convenio serán competentes los juzgados y tribunales de la jurisdicción contencioso-administrativa de Madrid.

Y para que conste a los efectos oportunos y en prueba de conformidad, las partes firman el presente convenio.

Firmado electrónicamente

LA DELEGADA DEL ÁREA DE GOBIERNO
DE ECONOMÍA, INNOVACION Y HACIENDA

Firmado electrónicamente

EL PRESIDENTE DE CYBERMAD

Engracia Hidalgo Tena

Damián Ruiz Soriano



ANEXO: RELACIÓN DE ACTUACIONES 2023 Y SU PRESUPUESTO, INDICADORES Y ACREDITACIÓN

BLOQUE	ACTUACIÓN	IMPORTE ACTIVIDAD	% PONDE- RACIÓN	INDICADORES	META FUENTE DE VERIFICACIÓN	FORMA DE ACREDITACIÓN (*)
PROYECTOS TÉCNICOS Y SECTORIALES	Ciberseguridad en el sector de la salud Ciberseguridad en el ámbito empresarial (pymes, empresas, corporaciones...) Ciberseguridad en las Administraciones Públicas Proyecto de análisis y diagnóstico de la ciberseguridad para empresas Proyecto de colaboración en la mejora en formación en ciberseguridad			Nº de actuaciones, Número de reuniones y grupos de trabajo participados, nº de eventos realizados, nº de publicaciones realizadas vinculadas al proyecto.	5 Proyectos, nº de reuniones	Documentación de proyectos, organización de las reuniones de trabajo para el desarrollo de los mismos, actos o eventos de presentación de resultados y en su caso productos, publicaciones (papel o preferiblemente digitales o en la página web del clúster) ligadas al proyecto, etc...
		25.000	50,0%	ACTUACIONES DEL BLOQUE PROYECTOS TÉCNICOS Y SECTORIALES:		5
PROYECTO DE CRECIMIENTO DEL ECOSISTEMA CYBER	Actuaciones de captación y seguimiento de Socios y Patrocinios, Atención al Socio y Clúster (canal del asociado, documentación, facturas, consultas, promociones,...) Modelo relacional con otros clústeres, Instituciones, Empresas y Organismos (reuniones y grupos de trabajo, acuerdos y colaboraciones)			Número de actuaciones Número de actuaciones Número de reuniones y grupos de trabajo participados, nuevos acuerdos firmados y colaboraciones	17 Alta de socios. Patrocinios. Nº reuniones 100 Bitácora 8 Reuniones preparatorias, Acuerdos, etc	Alta de Socio. Patrocinios. Reuniones Certificación número sobre Bitácora de actividades Actas de reuniones y grupos de trabajo; Acuerdos cerrados
		15.000	30,0%	ACTUACIONES DEL BLOQUE PROYECTO DE CRECIMIENTO DEL ECOSISTEMA:		125
COMUNICACIÓN DIFUSIÓN. ORGANIZACIÓN INTERNA	Elaboración newsletter, Notas de Prensa y Artículos de Prensa. Estrategia de comunicación y material de mensajes. Página web, dominios, cuentas de correo, herramientas colaborativas Organización reuniones internas (Junta Directiva, Consejo Asesor, Asamblea, Grupos Trabajo, Junta de Socios, preparatorias de reuniones estatutarias o de eventos, etc.), Organización de reuniones con terceros. Organización o colaboración en eventos no incluidos en el bloque 1			Nº de actuaciones Número de reuniones	15 Medio publicado 4 Nº total de ámbitos gestionados (web, dominios, correos, streaming) 6 Nº de reuniones	Detalle de contenidos elaborados/publicados Enlace página web, contenido, contratos, Actas/Notas/Correos de Reuniones
		10.000	20,0%	ACTUACIONES DEL BLOQUE COMUNICACIÓN DIFUSIÓN. ORGANIZACIÓN INTERNA:		25
TOTAL		50.000	100,0%	TOTAL ACTUACIONES:		155

1KGLM6JNOOTHCTL6

Información de Firmantes del Documento



FRANCISCO DAMIAN RUIZ SORIANO
ENGRACIA HIDALGO TENA - DELEGADA DEL AREA DE GOBIERNO DE ECONOMIA, INNOVACIÓN Y HACIENDA
URL de Verificación: https://servint.madrid.es/VECSV_WBCONSULTAINTRA/VerificarCove.do

Fecha Firma: 15/12/2023 12:04:29
Fecha Firma: 19/12/2023 12:36:48

CSV : 1KGLM6JNOOTHCTL6

