CONVENIO ESPECÍFICO EN DESARROLLO DEL PROTOCOLO GENERAL DE COLABORACIÓN ENTRE LA CONSEJERÍA DE PRESIDENCIA, INTERIOR, DIÁLOGO SOCIAL Y SIMPLIFICACIÓN ADMINISTRATIVA DE LA JUNTA DE ANDALUCÍA Y FUJITSU TECHNOLOGY SOLUTIONS, S.A., PARA EL IMPULSO DEL ECOSISTEMA DE CIBERSEGURIDAD SOCIOSANITARIA EN LA REGIÓN ANDALUZA, EN EL MARCO DEL PLAN DE RECUPERACIÓN, TRANSFORMACIÓN Y RESILIENCIA- FINANCIADO POR LA UNIÓN EUROPEA-NEXT GENERATION EU.

REUNIDOS

De una parte, D. Raúl Jiménez Jiménez, Director Gerente de la Agencia Digital de Andalucía, (en adelante, ADA) con NIF [redacted] y domicilio en Calle Gonzalo Jiménez de Quesada, Edificio Torre Sevilla, 2, 3ª – Sevilla, adscrita a la Consejería de Presidencia, Interior, Diálogo Social y Simplificación Administrativa de la Junta de Andalucía, cargo que ostenta en virtud del Decreto del Presidente 140/2021, de 13 de abril, por el que se dispone su nombramiento como Director Gerente de la Agencia Digital de Andalucía, que actúa en su nombre y representación y en uso de las facultades conferidas en el artículo 14.3.f) del Decreto 128/2021, de 30 de marzo, por el que se aprueban los Estatutos de la Agencia Digital de Andalucía (BOJA núm. 65, de / de abril de 2021).

De la otra parte, Dña. Patricia Urbez, con D.N.I.: [redacted] actuando en nombre de la empresa FUJITSU TECHNOLOGY SOLUTIONS S.A., (en adelante, ***"FUJITSU"***), con domicilio en Madrid, C/ Camino Cerro de los Gamos nº1, 28224- Pozuelo de Alarcón (Madrid), NIF: [redacted] y, encontrándose facultada para este acto según se deduce de la escritura de apoderamiento otorgada ante el Notario D. Juan Ramón Ortega Vidal, el día [redacted] con el número de protocolo [redacted]

Ambas partes, en las representaciones en que intervienen, se reconocen, recíprocamente, representación y capacidad legal suficiente para suscribir la presente adenda, y al efecto:

EXPONEN

PRIMERO. Que con fecha 6 de noviembre de 2023, la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa de la Junta de Andalucía y FUJITSU firmaron un Protocolo General de Actuación para cooperar y colaborar en áreas de mutuo interés, en

particular en materia de iniciativas orientadas hacia el impulso de la ciberseguridad sociosanitaria.

SEGUNDO. Que, conforme a la estipulación segunda del citado Protocolo General, las actuaciones derivadas del objeto de este han de ser desarrolladas y ejecutadas mediante la formalización de Convenios específicos de colaboración.

TERCERO. Que la Consejería de Presidencia, Interior, Diálogo Social y Simplificación Administrativa, a través de la Agencia Digital de Andalucía, de conformidad con sus estatutos aprobados mediante Decreto 128/2021, de 30 de marzo, contempla entre sus fines los relacionados con el desarrollo de la Estrategia Andaluza de Ciberseguridad 2022-2025, aprobada el 18 de octubre de 2022 mediante acuerdo del Consejo de Gobierno. Estrategia que involucra a la Administración Pública de Andalucía, la ciudadanía, el sector privado y a las entidades más representativas del sector.

CUARTO. Que con fecha 12 de febrero de 2021, se aprueba el Reglamento (UE) 2021/241 DEL Parlamento Europeo y del Consejo, por el que se establece el Mecanismo de Recuperación y Resiliencia (en adelante MRR). Seguidamente, mediante Resolución de 29 de abril de 2021, de la Subsecretaría, por la que se publica el Acuerdo del Consejo de Ministros, de 27 de abril de 2021, por el que se aprueba el Plan de Recuperación, Transformación y Resiliencia (en adelante PRTR).

QUINTO. Que el Plan de Recuperación, Transformación y Resiliencia (en adelante PRTR) es el instrumento fundamental para el desarrollo de los fondos europeos de recuperación Next Generation EU. En el desarrollo de dicho Plan, la Agenda España Digital 2026 se constituye como marco para impulsar la transformación digital de España, mediante la conectividad digital, impulso de la tecnología del 5G, el refuerzo de la ciberseguridad, la digitalización de la Administración y de las empresas, el impulso de la producción audiovisual, la garantía de los derechos digitales de la ciudadanía y el desarrollo de la economía del dato y la Inteligencia Artificial. Y que el 14 de julio de 2022 se reunió la Conferencia Sectorial para la Transformación Digital, en la que la Vicepresidenta Primera del Gobierno informó sobre el contenido del programa de Redes Territoriales de Especialización Tecnológica (RETECH). Posteriormente, el 3 de agosto de 2022, la Secretaría de Estado de Digitalización e Inteligencia Artificial publicó en su sede electrónica la “Invitación pública en el impulso de redes territoriales de especialización tecnológica” dirigida a que todas las Comunidades y Ciudades Autónomas pudieran presentar propuestas de proyectos en coordinación, con un mínimo de dos de ellas en cada proyecto, para financiar iniciativas emblemáticas de especialización territorial tecnológica dentro de sus competencias. Como respuesta a dicha invitación, Andalucía

presentó propuesta junto con las Comunidades Autónomas de Castilla-León y País Vasco, con la coordinación del Instituto Nacional de Ciberseguridad (INCIBE).

SEXTO. Que la Junta de Andalucía tiene, en dicho marco, el interés de desarrollar iniciativas tecnológicas que confluyen con el proyecto Argos, adscrito al proyecto de Redes Territoriales de Especialización Tecnológica (RETECH), en concreto en materia de ciberseguridad. En Andalucía el desarrollo de dicho proyecto estará ubicado en el Centro de Ciberseguridad de Andalucía en Málaga y su objetivo es impulsar una industria especializada en el desarrollo de ciberseguridad y la tecnología operativa para el sector de la salud y las smart cities. Gracias a este proyecto Andalucía quiere desarrollar capacidades y conocimientos específicos que contribuyan a la creación de una industria especializada en el diseño de soluciones y servicios de soporte a la securización de tecnologías IoT en los ámbitos salud y smartcity, aprovechando el marco creado por la normativa europea que al efecto se viene desarrollando, y entendiendo esta como una oportunidad para el crecimiento del sector

SÉPTIMO. Que Fujitsu, dentro de sus iniciativas empresariales, ha gestado la reciente creación de un Centro de Excelencia de ciberseguridad sociosanitaria en España, que cuenta con nodos de especialización en diferentes territorios españoles. Y que, en el marco de dicha iniciativa, es voluntad de Fujitsu participar en el impulso de medidas destinadas al fomento de la investigación en el campo de la ciberseguridad sociosanitaria en el tejido empresarial y social Andaluz, con arreglo a las condiciones que se establecen en el presente convenio específico.

OCTAVO. Que con fecha 29 de octubre de 2024, la Dirección General de Planificación de la Investigación emite Resolución por la que se procede a la acreditación de la ADA, como Agente del Sistema Andaluz del Conocimiento, dentro de la categoría de “Entidades del Sector Público Andaluz que gestionan y apoyan la coordinación, promoción o fomento del conocimiento y las tecnologías” prevista en el artículo 3.1.c).1º del Reglamento regulador de la clasificación, acreditación y registro de los Agentes del Sistema Andaluz del Conocimiento aprobado mediante Decreto 223/2023, de 12 de septiembre.

Del mismo modo, la citada Resolución resuelve la inscripción de la entidad en el Registro Electrónico de Agentes del Sistema Andaluz del Conocimiento.

Por lo tanto, en virtud de cuanto antecede, ambas partes acuerdan la suscripción del presente Convenio Específico, que se regirá por las siguientes

ESTIPULACIONES

PRIMERA. OBJETO

El objeto de este convenio es definir los compromisos y las condiciones con arreglo a las cuales se llevará a cabo la colaboración entre la ADA y FUJITSU para la ejecución de la actuación denominada IMPULSO DEL ECOSISTEMA DE CIBERSEGURIDAD SOCIOSANITARIA EN LA REGIÓN ANDALUZA, dedicadas a la Ciberseguridad en el ámbito del Retech de Ciberseguridad, Proyecto Red Argos, que está integrado por el Instituto para la Competitividad Empresarial de Castilla y León, el Departamento de Desarrollo Económico, Sostenibilidad y Medio Ambiente, a través del Grupo SPRI del Gobierno Vasco y la Agencia Digital de Andalucía, coordinados por INCIBE, cofinanciado por la Unión Europea dentro del Componente 15 del Plan de Recuperación, Transformación y Resiliencia C15I7 y por la comunidad Autónoma. La cooperación en la financiación implica que se financiará un mínimo del 25% por la Comunidades Autónomas, con financiación propia o privada.

Este convenio se enmarca en dicho programa Retech.

La colaboración entre FUJITSU y la Junta de Andalucía a través de su Centro de Ciberseguridad en Málaga, en el marco de las actividades del Centro de Excelencia de Ciberseguridad Sociosanitaria de FUJITSU, tiene como objetivo general convertir a Málaga en un referente nacional e internacional en conocimiento, investigación e innovación en ciberseguridad aplicada al ámbito sanitario y de la asistencia social, con especial atención a la seguridad en el Internet de las Cosas Médicas (IoMT) y los dispositivos avanzados de teleasistencia.

Son objetivos específicos de esta colaboración:

- Desarrollo de capacidades de investigación e innovación: Definir y ejecutar servicios orientados a mejorar el conocimiento y la protección de los datos, infraestructuras, dispositivos médicos, teleasistencia y sensores en IoMT e IoT.
- Generación de impacto social positivo: Impulsar iniciativas que beneficien directamente a la comunidad a través de la mejora de los servicios sociosanitarios.
- Fortalecimiento del tejido productivo y emprendedor: Fomentar la colaboración con empresas locales y startups para dinamizar la economía regional en torno a la ciberseguridad.
- Atracción de inversión estratégica: Posicionar Málaga como un polo atractivo para la inversión en tecnologías avanzadas y proyectos de I+D+i.

- Promoción del talento local: Generar oportunidades de formación, empleo cualificado y retención del talento en la región, incrementando las capacidades tecnológicas del entorno.
- Internacionalización del conocimiento: Establecer redes globales de colaboración para transferir tecnologías y posicionar el centro como referente internacional.

SEGUNDA. DESARROLLO DE LAS ACTUACIONES

La participación y desarrollo de las actuaciones conjuntas se articularán, en función de sus características o naturaleza, a través de los instrumentos que, en su caso, resulten de aplicación.

Dada la naturaleza de aplicabilidad en el ecosistema sociosanitario, será crítico para la ejecución de este Convenio de Colaboración hacer uso de acuerdos y alianzas con organizaciones sanitarias en las que aplicar las experiencias obtenidas en dispositivos de electromedicina, como los Hospitales y Centros de Salud del Servicio Andaluz de Salud, y de teleasistencia con instituciones de asistencia social, como la Agencia de Servicios Sociales y Dependencia de Andalucía. Por otra parte, podrán adscribirse mediante Adenda a este Convenio específico, acuerdos con fabricantes de referencia de equipos de electromedicina, (ej. Siemens, General Electric, Agfa, Dräger, Tunstall, …), así como con grupos de investigación o de universidades o centros de investigación referencia en el territorio andaluz, todo ello, previa definición y propuesta de la Comisión de Seguimiento de este Convenio.

En este sentido, los ejes principales de actuación en los que se enmarca este Convenio, sin detrimento de otros que pudieran surgir en desarrollo del Protocolo General de Actuación son los siguientes:

<u>EJE 1. I+D+i ESPECIALIZADO EN CIBERSEGURIDAD EN ENTORNOS SOCIOSANITARIOS</u>

Vivimos en un mundo cada vez más digital y cambiante, en el que los ciberataques son cada vez más sofisticados y destructivos. Ser objeto de un ataque cibernético o una violación de datos tiene implicaciones graves, aún más en un ámbito tan crítico como la sanidad o la asistencia social. Proteger a las personas y sus datos, minimizar el riesgo cibernético y cumplir con unos requisitos normativos cada vez mayores es más importante que nunca. La ciberseguridad es una necesidad y exige actuar con un enfoque inteligente, predictivo y proactivo.

Actualmente, las entidades sociosanitarias gestionan a diario información y recursos sensibles a través de sistemas de información como el Sistema de Información Hospitalaria o Radiológica (HIS/RIS), los Sistemas de Comunicación y Archivo de Imágenes Diagnósticas (PACS), Ensayos clínicos, o servicios avanzados de Teleasistencia, entre otras. Así mismo, vivimos inmersos en el desarrollo de un nuevo paradigma de la gestión de la salud en el que aparecen conceptos novedosos como la Internet de las Cosas Médicas o la Medicina Personalizada donde la tecnología toma un rol principal junto con el tratamiento masivo de información y datos, como por ejemplo en la Genómica y la medicina 5P, incorporando Inteligencia Artificial a los procesos sanitarios tanto de gestión como de apoyo a la decisión médica o la Computación Cuántica para el estudio de procesos probabilísticos como el análisis de proteínas o la optimización de recursos, generándose nuevos riesgos y retos desde el punto de vista de la Ciberseguridad que deben ser estudiados y analizados.

Por ello, este eje se constituye como la principal línea de actuación del Convenio y tendrá foco en el ámbito sociosanitario, en áreas de actividad del mismo que cuenten con escasa regulación, buenas prácticas y metodologías de despliegue, monitorización y análisis en materia de ciberseguridad, como por ejemplo los dispositivos que se localizan en los domicilios de la ciudadanía para la prestación de servicios avanzados de teleasistencia, e incluyendo tecnologías emergentes que puedan tener impacto en el contexto social de la salud.

Su objetivo es la realización de actuaciones para el desarrollo de la investigación en el ámbito de la ciberseguridad que permita identificar, como se ha indicado en el párrafo anterior, necesidades y propuestas regulatorias, conjuntos de buenas prácticas y metodologías de despliegue, monitorización y análisis que permitan ofrecer una respuesta adecuada a los riesgos que supone la implantación de tecnologías disruptivas o novedosas en el ámbito sociosanitario, o que adolezcan de falta de los componentes indicados. Por ejemplo, con el análisis del impacto por la aplicación de sistemas de Inteligencia Artificial o Computación Cuántica en salud, analizando cómo le afecta a la ciberseguridad el desarrollo e implantación de estos entornos y trabajando sobre el análisis de riesgos que pueden presentar frente a la amenaza de la ciberdelincuencia, de forma que se puedan identificar los puntos de ataque, impacto en el sistema sociosanitario e implementar líneas de defensa que se puedan adelantar a los incidentes.

Del mismo modo, es objetivo ayudar a la comprensión de cómo el cumplimiento de normativas y estándares de seguridad, como el Esquema Nacional de Seguridad, la normativa ISO y otras normativas aplicables, puede afectar a estas tecnologías y cómo deben adecuarse

la legislación y normas para poder dar cabida a nuevas necesidades o sistemas tecnológicos que no han sido considerados en su desarrollo.

Para el trabajo en líneas de tecnologías emergentes se podrán establecer colaboraciones tanto con el International Quantum Center de Fujitsu, como con la Cátedra Tecnología para las Personas en el ámbito de la Inteligencia Artificial y Supercomputación de la Universidad de Granada o la Cátedra de Ciberseguridad de la Universidad de Málaga, u otros organismos, entidades o grupos que puedan contribuir a la investigación.

Del mismo modo, y con el objetivo de establecer líneas de investigación operativa centrada en tecnologías que ya están siendo implantadas o son usuales en la sanidad como la IoMT (Internet de las Cosas Médicas), los dispositivos electromédicos, teleasistencia y sistemas de tratamiento de información sanitaria, se propone la colaboración con el Centro de Ciberseguridad de Andalucía, de forma que se facilite la generación de conocimiento e innovación en el campo de la ciberseguridad. Esta colaboración pretende incorporar, como se ha indicado, investigación operativa sobre la aplicación real de las buenas prácticas y metodologías desarrolladas y su impacto en el sistema sociosanitario de forma que se pueda determinar un marco real que permita identificar riesgos actuales y futuros, así como medidas de mitigación adecuadas y adaptadas al ámbito y ecosistema tecnológico de la salud.

El resultado de estas investigaciones y la información generada será accesible y tendrá como destinatarios a organizaciones sociosanitarias, tanto públicas como privadas, así como a fabricantes de dispositivos electromédicos y de teleasistencia, con el fin de que pueda ayudarles en la generación de nuevos productos y servicios que cumplan con los estándares de ciberseguridad y puedan beneficiarse de los descubrimientos e innovación aportada desde el centro, de forma que se consiga mejorar, no sólo la seguridad de los pacientes y de la ciudadanía en general, sino también su confianza en las organizaciones sociosanitarias que custodian sus datos, así como una mejora de la reputación de Málaga, y por tanto de Andalucía, al incorporar I+D+i en ciberseguridad sociosanitaria generando resultados novedosos en ciberseguridad.

EJE 2. DIFUSIÓN DEL CONOCIMIENTO ADQUIRIDO

Las iniciativas enmarcadas en este Eje tienen como objetivo poner a disposición de la sociedad en general, el tejido empresarial y otros centros de investigación los resultados obtenidos del desarrollo de las iniciativas de I+D+i realizadas en el punto anterior. Así mismo, esta difusión servirá como impulso al aumento la concienciación en materia de ciberseguridad para empresas, organizaciones sociosanitarias y centros de formación tanto

Universitarios como de Formación Profesional, de forma que se pueda aportar experiencia y conocimiento con el objetivo de crear cultura de ciberseguridad en general y para el ámbito sociosanitario en particular.

Este Eje se centra en la participación, promoción y patrocinio en foros de ciberseguridad y eventos tanto de nivel científico como de divulgación sobre la ciberseguridad nacionales o internacionales que puedan servir de escaparate a los avances realizados y permitan poner a Andalucía en el centro de la investigación, innovación y desarrollo de la ciberseguridad sociosanitaria. Igualmente, se fomentará la generación de material de investigación publicable en revistas tanto de investigación como de divulgación que permitan una difusión con criterios de calidad científica de los avances y descubrimientos que se vayan realizando.

La puesta en práctica de este Eje sirve de complemento a la formación y concienciación tradicional en ciberseguridad ya que permite incorporar al personal tanto técnico informático como el sociosanitario involucrado en los procesos de salud y de cuidados asistenciales, así como en el tejido empresarial que desarrolla nuevas iniciativas de forma que se puedan trabajar conjuntamente tanto para la investigación como para la publicación de resultados, pero además sin excluir al resto de profesionales o alumnos en formación que puedan estar interesados en complementar sus conocimientos o participar en las actividades que se desarrollen, generando un beneficio que repercuta en una mejora de la seguridad y del conocimiento global en el ámbito de la ciberseguridad sociosanitaria.

Por ello, en línea con este Eje, se incluye la propuesta de colaboración en programas de capacitación y certificación de habilidades científico-técnicas para alumnos de los grados tecnológicos del Sistema Universitario Andaluz. Así mismo, se desarrollarán ciclos de difusión adaptados para alumnos de las Facultades de Medicina, así como para alumnos de grados de formación profesional tanto de ramas técnicas como sociosanitarias. Además, se contempla posibilidad de realización de cursos propios y de especialización universitaria a través de instituciones públicas, de esta forma se consigue potenciar y complementar la oferta formativa y de investigación sobre ciberseguridad en todos los ámbitos y niveles. Para ampliar la capilaridad y facilitar la difusión, se podrá también poner a disposición del Centro de Ciberseguridad de Andalucía el material formativo y de formación de formadores. La participación y desarrollo de actuaciones conjuntas mencionadas en la presente estipulación se podrá articular, en función de sus características o naturaleza, a través de otros instrumentos que, en su caso, resulten de aplicación.

Los resultados de las actuaciones vinculadas al Eje 1 de I+D+i serán en forma de documentación y dosieres informativos que se pondrán a disposición a modo de contenidos de las actuaciones del Eje 2 de difusión del conocimiento.

El Eje 2 tendrá como resultados artículos divulgativos y de investigación, ponencias en eventos sectoriales, formación y/o difusión específica, etc.

Cuantificación del Desarrollo de las Actuaciones

Por parte de Fujitsu:

La valoración de las actuaciones a realizar por Fujitsu en el marco de este Convenio IMPULSO DEL ECOSISTEMA DE CIBERSEGURIDAD SOCIOSANITARIA EN LA REGIÓN ANDALUZA se estima en una totalidad aproximada de 366,5K€ para los dos años de duración del convenio.

Esta cantidad se reparte entre el valor del personal involucrado en el proyecto, servicios de investigación, herramientas y actividades de difusión que se realizarán desde el Centro de Ciberseguridad de Andalucía con el objetivo de contribuir en el desarrollo y en el impulso de la I+D+i y la incorporación de empresas a la Economía Digital en un el sector tan delicado y sensible como el sociosanitario y que favorecerá al desarrollo de la industria de la ciberseguridad situando a Málaga y Andalucía como referente en la investigación, desarrollo y difusión de la cultura de ciberseguridad en el sector sociosanitario.

Este valor se justifica, de forma general y aproximada, en las siguientes partidas:

- 281K€ (76,68%) - Asociados al personal vinculado, aportando un especialista en investigación en ciberseguridad sociosanitaria, adicionalmente a recursos del SOC (Centro de Operaciones de Seguridad) de Fujitsu que colaborarán en las tareas y proyectos vinculadas al Centro. Esta contribución pone a disposición de las instituciones andaluzas el conocimiento y la información relativa tanto a la ciberseguridad que Fujitsu gestiona internamente (al disponer de una red propia de SOC's con 14 centros en el mundo), como referidas a la red nacional CSIRT y al equipo internacional de respuesta ante incidentes FIRST, de las que Fujitsu es miembro.
- 48K€ (13,10%) - Se destina esta cantidad del valor total a la adquisición, licenciamiento y uso de herramientas específicas de ciberseguridad para realizar tareas de investigación y desarrollo para los proyectos que se deriven de la ejecución del Convenio, con el consecuente retorno de información sobre el estado de la ciberseguridad tanto a nivel particular de los participantes como a nivel global de datos consolidados, permitiendo proponer medidas de mejora generales que impulsen la creación en Andalucía de un

ecosistema tecnológico más seguro con un modelo de implantación digital en el ámbito sociosanitario más confiable y menos vulnerable.

- 37,5K€ (10,22%) Finalmente, se destina una partida a la difusión de los resultados obtenidos que permitan la mejora de las competencias digitales en el ámbito sociosanitario a través la participación/organización de cursos, eventos y jornadas impulsadas o realizadas directamente desde el Centro y que permitan la colaboración de otras empresas líderes en el sector de la ciberseguridad. Estas actividades no irán destinadas sólo a la administración pública de Andalucía, sino que también pondrán el foco en el sector privado, PYMES, organizaciones de salud y sociales, centros de formación universitaria y formación profesional y la propia ciudadanía, lo que favorecerá la creación de un ecosistema favorable para impulsar la industria de la ciberseguridad en el sector sociosanitario. Es objetivo del convenio desarrollar, en cooperación con la Universidad de Málaga y con la vocación de extenderse a otras Universidades Andaluzas, una participación activa en forma de cursos y seminarios en los grados tecnológicos y de ciencias de la salud, así como en estudios de posgrado que deseen colaborar, contando con la colaboración de organizaciones empresariales de la región, y organizaciones públicas y privadas sociosanitarias, permitiendo cuando corresponda el acceso libre bajo inscripción y según aforo a la ciudadanía interesada.

Por parte de la Agencia Digital de Andalucía:

La valoración de las actuaciones a realizar por la Agencia Digital de Andalucía, en el marco de este Convenio IMPULSO DEL ECOSISTEMA DE CIBERSEGURIDAD SOCIOSANITARIA EN LA REGIÓN ANDALUZA se estima en una totalidad aproximada de 361.948,72 € para los dos años de duración del convenio.

Esta cantidad se reparte entre el valor del personal involucrado en el proyecto, servicios de investigación, herramientas y actividades de difusión que se realizarán desde el Centro de Ciberseguridad de Andalucía con el objetivo de contribuir en el desarrollo y en el impulso de la I+D+i y la incorporación de empresas a la Economía Digital en un el sector tan delicado y sensible como el sociosanitario y que favorecerá al desarrollo de la industria de la ciberseguridad situando a Málaga y Andalucía como referente en la investigación, desarrollo y difusión de la cultura de ciberseguridad en el sector sociosanitario.

Este valor se justifica, de forma general y aproximada, en las siguientes partidas:

- 150.000€ - Asociados al personal vinculado, aportando la dedicación estimada del personal de la Agencia Digital de Andalucía y de Sandetel destinados en el Centro de

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

FUJITSU

Agencia Digital de Andalucía

Ciberseguridad de Andalucía que se dediquen a las tareas propias de este convenio, así como del personal del SAS que colabore en dicho proyecto.

- 21.948,72€ Puesta a disposición de Fujitsu de un puesto de trabajo en la Sede del Centro de Ciberseguridad de Andalucía u otra sede que se decida. El coste por puesto es de 10.974,36 € anuales.
- 150.000 € Acceso al laboratorio del Retech para el testeo de las soluciones.
- 30.000 € en concepto de difusión del proyecto Retech. El objetivo es la difusión de los resultados obtenidos que permitan la mejora de las competencias digitales en el ámbito sociosanitario a través la participación/organización de cursos, eventos y jornadas impulsadas o realizadas directamente desde el Centro y que permitan la colaboración de otras empresas líderes en el sector de la ciberseguridad.

TERCERA.OBLIGACIONES DE LAS PARTES

Las partes se comprometen al cumplimiento de las siguientes obligaciones:

a) Por parte de la Agencia Digital de Andalucía:

- Nominar a los representantes de la Junta de Andalucía responsables del seguimiento de las actuaciones del Convenio, sus resultados y madurez y dotarlos de capacidad para la toma de decisiones.
- Ceder el uso de un espacio en las instalaciones del Centro de Ciberseguridad de Andalucía en Málaga (CIAN) o de otros espacios disponibles, así como los recursos necesarios, cuando fuera necesario para el desarrollo de las actuaciones del Convenio. En este sentido, el personal que desarrolle alguna actividad en las instalaciones de la otra parte respetará las normas de funcionamiento interno de los centros de trabajo y en ningún caso se alterará su relación jurídica ni adquirirá derechos frente a la otra parte. En concreto, se podrán ceder puestos de trabajo dotados con conectividad de red y salida a internet, además de permitir el acceso supervisado al uso de salas con dotación multimedia para poder mantener reuniones o impartir formación. La colaboración y el trabajo en equipo con los equipos humanos en materia de ciberseguridad de la Junta de Andalucía, especialmente en lo que se refiere al SOC de la Junta de Andalucía, son críticos para la buena marcha de este Convenio.
- Apoyar institucionalmente, y en su caso participar, en la formalización, mediante adendas, de acuerdos de colaboración con otras entidades públicas que resulten de interés para el desarrollo del convenio, entre ellas, el Ayuntamiento de Málaga, el Servicio Andaluz de Salud, la Agencia de Servicios Sociales y Dependencia de

Andalucía y la Universidad de Málaga, o de entidades de investigación, innovación o formación, así como promover los cauces que habiliten una comunicación fluida entre Fujitsu y las distintas entidades que participen en las actuaciones enmarcadas en el presente Convenio.

- Promover la participación en el diseño de las actuaciones previstas en el Convenio mediante la aportación de expertos académicos y operativos propios o, en virtud de su capacidad de convocatoria, de empresas e instituciones del tejido tecnológico andaluz; y apoyar la organización logística de dichas actuaciones, pudiendo facilitar espacios físicos para la formación o eventos y recursos a disposición de la sociedad andaluza.
- Apoyar como administración tractora y dinamizadora en las comunicaciones y actividades de concienciación, formación y difusión que se definan en la comisión de seguimiento del Convenio, mediante la participación en las mismas de representantes de la Junta de Andalucía acordes al nivel institucional de la actividad.
- Dar difusión de los resultados en los eventos de ciberseguridad que se organicen por parte de la Agencia Digital de Andalucía.

b) Por parte de Fujitsu:

- Nominar a los representantes responsables del seguimiento de las actuaciones del Convenio, sus resultados y madurez y dotarlos de capacidad para la toma de decisiones.
- Habilitar los mecanismos para la participación y colaboración con la Junta de Andalucía en relación con los ámbitos de colaboración identificados en el presente Convenio.
- Promover la realización de las distintas actividades planteadas para avanzar conjuntamente en el crecimiento del ecosistema andaluz de ciberseguridad sociosanitaria y, en concreto, de IoMT y dispositivos para los servicios avanzados de teleasistencia, colaborando a su vez con las partes interesadas, como las instituciones académicas o los espacios de emprendimiento y co-creación.
- Proporcionar los recursos humanos, las herramientas tecnológicas y los materiales acordados para el cumplimiento del objeto de la presente Adenda de Convenio de Colaboración y desarrollo de las actuaciones contempladas en esta.
- Establecer las colaboraciones con terceros que sean necesarias para el desarrollo de las actividades objeto del presente convenio.
- Proporcionar informes periódicos de actividad y seguimiento de la planificación, así como documentación asociada a las actuaciones realizadas y generada como resultado de las mismas.

- Respetar las normas de funcionamiento de las instalaciones cedidas por la Junta de Andalucía. El personal que desarrolle alguna actividad en las instalaciones de la otra parte respetará las normas de funcionamiento interno de los centros de trabajo y en ningún caso se alterará su relación jurídica ni adquirirá derechos frente a la otra parte.
- Contribuir a que Andalucía se convierta en un punto de referencia en ciberseguridad sociosanitaria no solo a nivel nacional, sino también a nivel internacional. Para ello, Fujitsu, como multinacional, impulsará la visibilidad y conocimiento del ecosistema andaluz.
- Realizar las siguientes actuaciones en los ejes 1 y 2, así como cualesquiera otras que sean acordadas por la Comisión de Seguimiento:
    - <u>EJE 1. I+D+i ESPECIALIZADO EN CIBERSEGURIDAD EN ENTORNOS SOCIOSANITARIOS</u>
        i. Estudio del impacto en ciberseguridad de las nuevas tendencias tecnológicas en salud junto con la implantación de nuevos procesos sociosanitarias, como la IA, cuántica, Medicina 5p, datalake sanitario, uso primario y secundario de la información, …
        ii. Análisis de normativas y estándares de seguridad (Esquema Nacional de Seguridad, normativa ISO, NIST, etc) para estudiar si contemplan de forma adecuada las nuevas necesidades o sistemas tecnológicos o deben ser modificadas o complementadas para darles cabida
        iii. Diseño de conjuntos de buenas prácticas y de metodologías para el despliegue, la monitorización y el análisis de riesgos, vulnerabilidades y amenazas de los sistemas sociosanitarios.
        iv. Investigación operativa sobre la posibilidad real de aplicación de lo desarrollado y su impacto en el sistema sociosanitario
    - <u>EJE 2. DIFUSIÓN DEL CONOCIMIENTO ADQUIRIDO</u>
        i. Puesta en común en foros especializados de los resultados más relevantes obtenidos del desarrollo de las iniciativas de I+D+i realizadas.
        ii. Colaboraciones formativas con Universidades, Institutos de Formación Profesional y otros centros y entidades formativas.

En cada una de las actuaciones se identificarán los interlocutores más adecuados para maximizar los resultados como, por ejemplo, la participación de universidades, centros de investigación, entidades sociosanitarias públicas o privadas, entidades de protección en ciberseguridad como CCN-CERT, INCIBE o el SOC de la Junta de Andalucía, componentes de la industria, colegios profesionales, etc. Dichos interlocutores serán especificados durante los comités de seguimiento de la ejecución del convenio.

CUARTA. CUANTIFICACIÓN ECONÓMICA DE LAS OBLIGACIONES DE LAS PARTES Y FINANCIACIÓN

1. La aplicación y ejecución de este Convenio, incluyéndose al efecto todos los actos jurídicos que pudieran dictarse en su ejecución y desarrollo, no genera compromisos ni contraprestaciones económicas entre las Partes firmantes, las cuales asumirán los costes que deban realizar con cargo a sus respectivos presupuestos de medios aportados por cada una de las Partes que obran en el expediente.

2. Así, las actuaciones objeto de este convenio suponen un presupuesto total estimado de 728.448,72 €.

La ADA dispone de los recursos suficientes y adecuados con el que hará frente a los gastos derivados de la puesta a disposición del proyecto del uso de un espacio en las instalaciones del Centro de Ciberseguridad de Andalucía en Málaga (CIAN) o de otros espacios disponibles, así como los recursos necesarios, para el desarrollo de sus actuaciones en el Convenio y resto de obligaciones derivadas.

Fujitsu, por su parte, financiará con un presupuesto total de 366.500 € euros, los gastos derivados de la realización de las distintas actividades planteadas para avanzar conjuntamente en el crecimiento del ecosistema andaluz de ciberseguridad sociosanitaria y, en concreto, de IoMT y dispositivos para los servicios avanzados de teleasistencia, colaborando a su vez con las partes interesadas, como las instituciones académicas o los espacios de emprendimiento y co-creación, así como los recursos humanos, las herramientas tecnológicas y los materiales acordados para el cumplimiento del objeto de este Convenio de Colaboración y desarrollo de las actuaciones contempladas en esta.

Cada parte es responsable mancomunadamente de sus propias obligaciones, sin que ninguna de ellas incurra en responsabilidades derivadas de los incumplimientos de la otra parte.

QUINTA. PUBLICIDAD Y DIFUSIÓN.

En cualquier tipo de publicidad que se realice de las actividades que constituyan el objeto del Convenio sobre cualquier soporte técnico o formato, y en cuantas actuaciones de difusión pública se realicen en el desarrollo de las actividades amparadas por este acuerdo, deberán reflejarse las señas de identidad y logos de las Partes, así como los logos relativos al Plan de Recuperación, Transformación y Resiliencia, de conformidad con lo establecido en sus normas sobre Publicidad Institucional.

Asimismo, la información proporcionada a la Comisión de Seguimiento incluirá, en todo caso, los detalles necesarios para documentar la contribución de las actividades y resultados del convenio a los indicadores del Programa RETECH establecidos en el marco del mismo. Esta información servirá para verificar el impacto de las actuaciones en las metas estratégicas del programa, facilitando los mecanismos de seguimiento y acreditación en línea con la documentación oficial aplicable y promoviendo la transparencia y la rendición de cuentas.

SEXTA. PUBLICIDAD ACTIVA.

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

SÉPTIMA. COMISIÓN DE SEGUIMIENTO

Para la puesta en marcha y el control de actividades que se realicen en aplicación de este Convenio, se constituirán una comisión de seguimiento, como órgano de seguimiento y para la resolución de las dudas que pudieran surgir en su interpretación y aplicación, cuya composición y régimen de funcionamiento estará determinado por lo previsto en este convenio y por sus propios acuerdos

En cuanto a su funcionamiento, y en lo no previsto de forma expresa, esta comisión se regirá conforme a lo establecido en el Capítulo VI de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

La Comisión de Seguimiento se constituirá en el plazo máximo de un mes, a contar desde la firma del presente convenio. La Comisión de Seguimiento se reunirá de manera trimestral para el cumplimiento eficaz de sus funciones y estará conformada por los siguientes miembros, sin detrimento de que cuando se considere, los miembros de la comisión podrán asistir acompañados del personal técnico y especializado que consideren en función de las cuestiones a tratar, con voz, pero sin voto. De forma extraordinaria se reunirá cuando lo solicite alguna de las Partes.

Por parte de la Agencia Digital de Andalucía:

- La persona titular de la Dirección Gerencia de la Agencia Digital de Andalucía o, en su caso, la persona que se designe en sustitución de ésta.

- La persona titular de la Dirección General de Estrategia Digital de la Agencia Digital de Andalucía o, en su caso, la persona que se designe en sustitución de ésta.
- La persona titular de la Subdirección con competencias en materia de Ciberseguridad de la Agencia Digital de Andalucía.
- La dirección del Centro de Ciberseguridad de Andalucía (CIAN).

Por parte de FUJITSU:

- El director del Centro de Excelencia de Servicios de Ciberseguridad Sociosanitarios de Fujitsu para Andalucía.
- El director de Ciberseguridad de Fujitsu.
- La directora General de Sector Público de Fujitsu.
- El director de Sector Público de Fujitsu en Andalucía.

Además de estas personas, la Comisión de Seguimiento contará con una Secretaría, que será designada por la parte que, en cada momento, ostente la presidencia de dicha Comisión.

La persona que asuma la Secretaría de la Comisión de Seguimiento levantará acta de las reuniones de esta, a las que asistirá con voz, pero sin voto.

Los acuerdos de la Comisión de Seguimiento se alcanzarán por mayoría simple, salvo en los casos en que las partes, de común acuerdo, dispongan otra cosa.

A la Comisión le corresponden, entre otras, las siguientes funciones:

a) Aprobación de la planificación y calendarización para la puesta en marcha de las actuaciones previstas en el Convenio. La Comisión valorará y aprobará en su caso los proyectos específicos que le sean propuestos por sus miembros. En cada proyecto deberán detallarse los objetivos e indicadores de seguimiento concretos, los compromisos de las partes y sus aportaciones en materia de recursos humanos y materiales necesarios para la consecución de los objetivos descritos, y las condiciones de propiedad intelectual y de uso de los resultados. La Comisión levantará acta del acuerdo y la informará a la Comisión de ámbito operativo del Protocolo General de Actuación.

b) Valoración de la eficacia, resultados e impacto de dichas actuaciones realizadas en el marco del Convenio, así como la satisfacción esperada del servicio, su cumplimiento y adoptar medidas para la mejora continua.

c) Promoción de posibilidades de colaboración en temas de interés común, poniendo de este modo en marcha iniciativas que se plasmarán y regularán de acuerdo con lo pactado en el Convenio.

d) Supervisión de la ejecución del Convenio, así como su interpretación, en caso de dudas suscitadas durante su ejecución, y, en su caso, de la resolución de los conflictos derivados de su aplicación.

e) Reporte trimestral y rendición de cuentas general a la comisión ejecutiva del Protocolo General de Actuación al que está adscrito el presente Convenio.

f) Adoptar las medidas oportunas, en caso de una resolución anticipada del Convenio, para garantizar la finalización de las actividades programadas.

g) Informar en materia de la actividad de comunicación y difusión de la iniciativa.

h) Cuantas otras se deriven del presente convenio y se consideren necesarias para su buena ejecución.

OCTAVA. VIGENCIA.

El presente Convenio de Colaboración surtirá efecto desde el día de su firma y tendrá una vigencia de dos años partir de la fecha de su firma, a no ser que una de las partes notifique a la otra el deseo de darlo por concluido con una antelación mínima de treinta (30) días, donde se expongan los motivos para ello. Las partes podrán igualmente prorrogar de manera expresa el presente Convenio de Colaboración por el plazo que las mismas consideren, lo que supondrá implícitamente prorrogado el Protocolo General de Actuación al que dicho Convenio específico está vinculado.

NOVENA. CAUSAS DE RESOLUCIÓN

El presente Convenio se extinguirá por las siguientes causas, la primera que tenga lugar en el tiempo:

(i) Por expiración del término contractual pactado sin haberse acordado la prórroga del mismo, según plazo estipulado en la cláusula séptima anterior.
(ii) La comunicación de una de las partes a la otra de considerar resuelto el presente documento, en los términos de la citada cláusula séptima.
(iii) El incumplimiento por cualquiera de las partes de las obligaciones asumidas con la suscripción del Convenio.
(iv) La resolución expresa y por escrito de mutuo acuerdo.
(v) Por decisión judicial declaratoria de la nulidad de la Adenda.

En el supuesto de extinción de este Convenio por causas distintas a la expiración de su plazo de vigencia, se procederá a la liquidación de las obligaciones contraídas por cada una de LAS PARTES, en caso de que se hubieran adquirido, sin perjuicio de la finalización de las actividades que estuvieran en curso.

DÉCIMA. - CONFIDENCIALIDAD

A los efectos del Convenio, tiene la consideración de “Información Confidencial" la información relativa al know-how, patentes, marcas y cualquier otro derecho de propiedad industrial o intelectual que sea propiedad de las partes.

Las partes quedan expresamente obligadas mutua y recíprocamente durante y con posterioridad a la vigencia de este convenio a mantener absoluta confidencialidad y reserva sobre los datos con los que se trabajen con ocasión del desarrollo del presente convenio, especialmente los de carácter personal, que no podrá copiar o utilizar con fin distinto al que figure en los respectivos documentos que suscriban, ni tampoco ceder a otros, ni siquiera a efectos de conservación, sin el previo consentimiento por escrito de la otra parte.

Las partes acuerdan no divulgar y mantener bajo estricta confidencialidad y secreto la Información Confidencial relativa a la otra parte u obtenida de la otra parte con motivo del Convenio. Cada una de las partes acuerda no publicar, comunicar, divulgar, revelar, o utilizar la Información Confidencial obtenida en virtud del Convenio, sin el consentimiento previo y por escrito de la otra parte, salvo que se prevea expresamente lo contrario en el 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.

El incumplimiento por cualquiera de las partes de esta cláusula de confidencialidad facultará a las otras partes para resolver el presente Convenio y además exigir los daños y perjuicios que se le hubiesen ocasionado.

Las restricciones de esta cláusula no serán aplicables en cuanto a:

a) La información que, en el momento de suscripción del Convenio ya se encuentre legítimamente en posesión de la parte receptora, sin que se haya impuesto ninguna obligación de confidencialidad a la parte que divulgue esta información.
b) La información que, en el momento de divulgarse, ya sea de dominio público o que, tras su divulgación, ya se haya publicado o pase a ser de dominio público, salvo que ello ocurra como consecuencia de la violación del Convenio por la parte que reciba la información.
c) La información que haya dejado de ser confidencial por acuerdo escrito entre las partes.
d) La información cuya publicación se exija de conformidad con la ley o por mandato de las autoridades judiciales o administrativas.

Con independencia de la finalización del Convenio, el citado compromiso de confidencialidad permanecerá por tiempo ilimitado tanto para los responsables y encargados del tratamiento de datos, como para todas las personas que intervengan en cualquier fase de éste.

UNDÉCIMA. DATOS DE CARÁCTER PERSONAL

Las partes se comprometen a cumplir, en los términos que le sean de aplicación, 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).

Si, por razón del presente convenio, cualquiera de las partes tuviera acceso a datos de carácter personal de cuyo tratamiento es responsable otra parte, aquella tendrá la consideración de encargado del 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.

En las actuaciones en las cuales dos o más partes sean corresponsables del tratamiento de datos personales en los términos del artículo 26 del RGPD, conjuntamente determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD según lo dispuesto en el citado artículo.

En el supuesto de que pueda producirse un potencial acceso por parte de cualesquiera de las partes a datos de carácter personal responsabilidad de la otra parte en su condición de responsable una y de encargada otra, las partes se comprometen a suscribir como parte del convenio específico, el acto jurídico que vincule a la entidad que actúa como encargada, y en el que deberá recogerse el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. En este supuesto, el acceso a esos datos por parte de que la que actúa como encargada de tratamiento no se considerará comunicación de datos. En dicho acto jurídico, la entidad que actúe como encargada de tratamiento ofrecerá a quien actúe como responsable garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD y garantice la protección de los derechos de los interesados (art. 28.1 del RGPD). En este supuesto y de conformidad con lo previsto en el artículo 28 del RGPD, la entidad que actúe como encargada garantizará el cumplimiento de las siguientes obligaciones mínimas de aplicación:

1. El uso de los datos personales objeto de tratamiento sólo para la finalidad objeto del encargo. En ningún caso podrá utilizar los datos para otros fines distintos o fines propios.
2. Tratar los datos de acuerdo con las instrucciones documentadas del responsable del tratamiento. Si la entidad que actúa como encargada considera que alguna de las instrucciones recibidas infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o Estados miembros, informará inmediatamente al responsable.
3. Llevar, por escrito, un registro de todas las operaciones relativas al tratamiento efectuadas por cuenta del organismo responsable, que contenga lo especificado en el artículo 30.2 del RGPD. Asimismo, La entidad que actúa como encargada colaborará con el responsable del tratamiento, en la identificación de la información que debe incluirse en su Registro de Actividades de Tratamiento.
4. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento en los supuestos legalmente admisibles.
5. La entidad que actúa como encargada se compromete a tratar los datos personales dentro del Espacio Económico Europeo, no tratándolos fuera de este espacio ni

directamente ni a través de cualesquiera subencargados autorizados, salvo que esté obligado a ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

6. Si la entidad que actúa como encargada debe transferir datos personales a un tercer país o a una organización internacional en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al responsable de esa exigencia legal de manera previa.
7. En todo caso, las transferencias internacionales de datos solo podrán llevarse a cabo si se cumplen las condiciones establecidas en el capítulo V del RGPD.
8. La entidad que actúa como encargada no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, la entidad que actúa como encargada, informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.
9. Mantener el deber de secreto respecto a los datos de carácter personal a los que tenga acceso en virtud del encargo, incluso después de que finalice su objeto.
10. Garantizar que sus empleados, así como las personas autorizadas para tratar datos personales, se comprometen de forma expresa y por escrito a respetar la confidencialidad a la que se refiere el artículo 5.1. de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Asimismo, dichas obligaciones se mantendrán aun cuando hubiese finalizado la relación del obligado, entidad que actúa como encargada, con el responsable del tratamiento. También deberán comprometerse a cumplir las medidas de seguridad correspondientes, de las que debe informárseles convenientemente.
11. Mantener a disposición del organismo responsable del tratamiento la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.
12. Garantizar la formación necesaria en materia de protección de datos personales de sus empleados y/o de las personas autorizadas para tratar datos personales.
13. Asistir al organismo responsable del tratamiento en los términos que este determine en la respuesta al ejercicio de los derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles).
14. La entidad que actúa como encargada, en el momento de la recogida de los datos y si es el caso, debe facilitar la información relativa al tratamiento de datos que se va a realizar.
15. La entidad que actúa como encargada notificará al organismo responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, a través del correo electrónico del responsable del organismo las violaciones

de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia.

16. Si se dispone de ella se facilitará, como mínimo, la información siguiente:
    - Descripción de la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados.
    - El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto.
17. La entidad que actúa como encargada ayudará en todo caso al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición.
18. La entidad que actúa como encargada suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.
19. La entidad que actúa como encargada pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el artículo 28, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.

En su condición de encargado de tratamiento, la aplicación del contenido de estas cláusulas, en todo caso mínimas junto con otras que el organismo que actúe como responsable estime oportuno concretar o añadir, deberán ser establecidas de mutuo acuerdo por las partes en la firma de los específicos acuerdos o convenios que se realicen en desarrollo de este Convenio, en los cuales se determinarán adicionalmente la naturaleza de cada actuación de colaboración, proyecto y circunstancias concurrentes en cada caso. Asimismo, deberá completarse el detalle del tratamiento de datos personales a efectuar por la entidad que actúa en su condición de encargado, los colectivos interesados, las operaciones del tratamiento que realiza sobre los mismos y los datos personales a los que la entidad que actúa como encargada podrá acceder, la disposición de los datos al terminar el encargo y las medidas de seguridad específicas que deba aplicar.

En cumplimiento con lo previsto 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 las partes informan a los firmantes que actúan en nombre y representación de cada una de las partes en el presente Convenio, y que los datos de carácter personal que faciliten en virtud del mismo, serán incorporados a los tratamientos de cada una de las partes cuya finalidad es el mantenimiento, cumplimiento, desarrollo, control y ejecución de los dispuesto en el presente Convenio.

Concretamente, en relación con los acuerdos o convenios que se celebren entre las entidades públicas y FUJITSU en cumplimiento y desarrollo de este Convenio:

1.- En las actuaciones en las cuales FUJITSU disponga productos o servicios en los que sea responsable del tratamiento de datos personales de sus usuarios, FUJITSU se compromete al cumplimiento como responsable de lo establecido 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 (Reglamento general de protección de datos, en adelante RGPD). Para ello FUJITSU pondrá a disposición de la Administración de la Junta de Andalucía cuantas evidencias estime oportunas para la verificación de dicho cumplimiento en relación con los productos o servicios implicados.

2.- En las actuaciones en las cuales FUJITSU sea corresponsable del tratamiento de datos personales conjuntamente con un órgano de la Administración de la Junta de Andalucía, en los términos del artículo 26 del RGPD, los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el RGPD, según lo dispuesto en el citado artículo.

3.- En el caso probable de actuaciones en las cuales FUJITSU actúe como encargado del tratamiento de datos personales cuyo responsable sea un órgano de la Administración de la Junta de Andalucía, dicho tratamiento deberá recogerse en un acto jurídico con arreglo al Derecho de la Unión que vincule a FUJITSU respecto del organismo responsable, en el que, deberá recogerse, según establece el artículo 28 del RGPD, el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. En este supuesto, el acceso a esos datos no se considerará comunicación de datos.

En este acto jurídico, como encargado del tratamiento, FUJITSU ofrecerá garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para que el tratamiento sea conforme al RGPD y garantice la protección de los derechos de los interesados (art. 28.1 del RGPD).

Los datos personales de las partes que figuran en el Convenio se integrarán en los respectivos tratamientos de datos de su titularidad para la gestión y ejecución de las actuaciones derivadas de la suscripción y ejecución de protocolos y convenios de colaboración. Los datos se conservarán durante el plazo previsto por la normativa vigente (especialmente, de tipo fiscal y contable) y no se comunicarán a terceros excepto que haya una obligación legal que requiera la comunicación a otras Administraciones Públicas.

Para obtener más información en relación con el tratamiento de datos personales pueden contactar a los respectivos delegados de protección de datos a:

Correo electrónico: [redacted]

Correo electrónico: [redacted]

DUODÉCIMA. COMUNICACIONES Y NOTIFICACIONES

Las comunicaciones dirigidas a las partes deberán hacerse llegar, por correo electrónico principalmente, a los siguientes datos de contacto:

AGENCIA DIGITAL DE ANDALUCÍA

- Cargo: Director Gerente
- Dirección: Gonzalo Jiménez Quesada, 2. Edif. Torre Sevilla, 3ª planta. 41092, Sevilla.
- Correo electrónico: [redacted]

FUJITSU

- Cargo: Director de Sector Público de Fujitsu en Andalucía
- Dirección: Edificio Catalana Occidente. Avenida San Francisco Javier, 20 41018 Sevilla
- Correo electrónico: [redacted]

En el supuesto de que sea necesario sustituir a la persona que actúa de interlocutor, cada parte notificará con una antelación mínima de 10 días a la otra los datos de la nueva persona de contacto.

DÉCIMO TERCERA. DERECHOS DE PROPIEDAD INDUSTRIAL E INTELECTUAL

Las partes reconocen que la ejecución del presente convenio no conferirá, en ningún caso, derechos de Propiedad Industrial o Intelectual, ni de naturaleza análoga, sobre los activos, contenidos, know-how, herramientas o cualquier otro recurso preexistente de la otra parte.

Asimismo, los derechos sobre los conocimientos, tecnologías y activos preexistentes aportados al convenio seguirán siendo de la parte que los aportó, siendo su uso limitado a la ejecución del convenio.

A los efectos del presente convenio, se entenderán por Derechos de Propiedad Industrial e Intelectual aquellos relacionados con invenciones (incluyendo patentes y modelos de utilidad), marcas, diseños, información confidencial (como secretos empresariales y know-how), bases de datos, programas de ordenador, algoritmos y cualquier otra creación protegida por legislación nacional o internacional.

Si para la ejecución del convenio es necesario el acceso o uso de herramientas, software o activos específicos de cualquiera de las partes, dicho acceso se otorgará bajo un derecho de uso limitado, no exclusivo, revocable, no sublicenciable y no transferible, exclusivamente para la ejecución de las tareas contempladas en el convenio. Cualquier otro uso requerirá autorización previa y por escrito, constituyendo su incumplimiento una infracción contractual y legal.

Si como consecuencia de la colaboración se obtuvieran Resultados susceptibles de protección por derechos de Propiedad Industrial e Intelectual, las partes acordarán su titularidad en función de su contribución al desarrollo. La viabilidad de los Resultados será evaluada conjuntamente, y ambas partes se comprometen a informarse mutuamente de los progresos.

La parte o partes que obtengan derechos sobre los Resultados otorgarán a la otra parte una licencia de explotación gratuita, irrevocable, no exclusiva, sublicenciable, sobre dichos Resultados para todo el territorio y con duración indefinida. Las partes se comprometen a negociar y acordar de buena fe los términos y condiciones de la titularidad de resultados, así como la protección, mantenimiento y defensa de los derechos de propiedad intelectual sobre los resultados. Igualmente, las partes se comprometen a negociar y acordar las condiciones de uso de los resultados obtenidos. Cada parte podrá utilizar los Resultados para actividades de investigación, desarrollo e innovación dentro del ecosistema de ciberseguridad sociosanitaria, respetando la confidencialidad y los derechos de terceros. La Agencia Digital

de Andalucía tendrá derecho de uso preferente para fines vinculados al Plan de Recuperación, Transformación y Resiliencia.

La parte titular gestionará el registro y protección de los Resultados, asumiendo los costes, salvo acuerdo en contrario. Cualquier explotación comercial requerirá un acuerdo específico entre las partes. Se garantizará el reconocimiento de la financiación de la Unión Europea según la normativa aplicable.

Cada parte garantiza que los elementos que aporte para la ejecución del convenio no infringen derechos de terceros y se compromete a respetar los derechos de Propiedad Intelectual e Industrial tanto de la otra parte como de terceros, así como la confidencialidad de los Resultados hasta su publicación o registro. Cualquier infracción será responsabilidad exclusiva de la parte que la haya causado.

DÉCIMO CUARTA. MODIFICACIONES

Toda modificación al presente Convenio únicamente tendrá validez si está explícitamente suscrita por las partes, debiéndose incorporar como adenda. En este caso, aparte de las estipulaciones explícitamente modificadas, las restantes conservarán su validez y por lo tanto serán de plena aplicación.

DÉCIMO QUINTA. CESIÓN

Las partes no podrán ceder su posición en el Convenio, ni tampoco los derechos y obligaciones que se deriven a favor o a su cargo sin el consentimiento previo y por escrito de las demás partes.

Y para que así conste, en prueba de conformidad, se firma el presente documento en el lugar y fecha indicados en el encabezamiento.

AGENCIA DIGITAL DE ANDALUCÍA

JIMENEZ JIMENEZ RAUL - [redacted]

Firmado digitalmente por JIMENEZ JIMENEZ RAUL [redacted]
Fecha: 2025.04.16 11:12:42 +02'00'

Fdo.: Raúl Jiménez Jiménez

Director Gerente

FUJITSU TECHNOLOGY SOLUTIONS, S.A.

URBEZ SANZ EVA PATRICIA - [redacted]

Digitally signed by URBEZ SANZ EVA PATRICIA - [redacted]
Date: 2025.04.14 14:24:57 +02'00'

Fdo.: Patricia Urbez Sanz

Directora General del Sector Público