

**CONTRATO DE SUMINISTROS**

**OBJETO:** Cesión de uso de licencias de doble factor de autenticación de empleados de la Gerencia Regional de Salud de Castilla y León

**IMPORTE TOTAL DEL CONTRATO:**

<u>Importe sin IVA(€)</u>	<u>Cuantía del IVA(€)</u>	<u>Importe total(€)</u>
62.240,00 €	13.070,40€	75.310,40€

**APLICACIÓN PRESUPUESTARIA:** 05.22.491A01.20600.0

**PROCEDIMIENTO DE ADJUDICACIÓN:** Abierto (artículos 131 y 136 y siguientes de la LCSP).

**ADJUDICATARIO:** SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U

**N.I.F.:** A82733262. **LOCALIDAD:**ALCOBENDAS (MADRID)

**DURACIÓN INICIAL DEL CONTRATO:** 12 meses desde el 25 de enero de 2025.

**SE REUNEN:**

DE UNA PARTE, D.Israel Diego Aragón, como Director Económico, Presupuestario y Financiero de la Gerencia Regional de Salud de Castilla y León, en la representación que ostenta, en virtud de las competencias que le confiere el Decreto 19/2018 de 21 de junio, de desconcentración de competencias del en materia de contratación y gestión económica en el ámbito de la Gerencia Regional de Salud.

DE OTRA PARTE Dña., Ana Isasi Gómez con DNI número \*\*\*4561\*\* y D Joaquín Ciruelo Meléndez, con D.N.I. número\*\*\*1918\*\* como representantes de la empresa SISTEMAS INFORMÁTICOS ABIERTOS, SAU, y con domicilio social en Alcobendas (Madrid), C/ Avenida Bruselas, 35 (C.P. 28108), según se acredita mediante certificado del ROLECE donde se recoge el apoderamiento.

Ambas partes se reconocen competencia y capacidad, respectivamente, para formalizar el presente contrato administrativo.

### **ANTECEDENTES:**

**PRIMERO.-** El expediente de suministro fue promovido por la Dirección General de Salud Digital.

**SEGUNDO.-** La retención de crédito fue efectuada por la Intervención Delegada de esta Gerencia con fecha 21 de mayo de 2024 con cargo a la aplicación presupuestaria 05.22.491A01.20600.0 con un presupuesto total de 103.818,00€,realizándose la intervención previa del expediente de contratación el día 3 junio de 2024.

**TERCERO.-** La aprobación del gasto fue realizada por el Director Económico, Presupuestario y Financiero con fecha de 5 de junio de 2024, por importe de 103.818,00€

**CUARTO.-** La adjudicación fue acordada por Resolución del Director Económico, Presupuestario y Financiero de la Gerencia Regional de Salud de Castilla y León, el día 9 agosto de 2024.

### **CLÁUSULAS:**

#### **PRIMERA.- OBJETO.**

El presente contrato tiene por objeto la Cesión de uso de licencias de doble factor de autenticación de empleados de la Gerencia Regional de Salud: 5.000 licencias del producto **IntelliTrust Authentication Service Enterprise** incluidas las licencias necesarias de Mobile Soft Token.

Las prestaciones del suministro de referencia se realizarán con estricta sujeción al pliego de cláusulas administrativas particulares y al pliego de prescripciones técnicas que rigen esta contratación.

#### **SEGUNDA.- RÉGIMEN JURÍDICO.**

El presente contrato tiene naturaleza administrativa, y se registrá, para todo lo no previsto en él, por 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, de 26 de febrero de 2014 (en adelante LCSP), y por el Real Decreto 1098/2001, de 12 de octubre, por el que se aprueba el Reglamento General de la Ley de Contratos de las Administraciones Públicas, así como lo dispuesto en el pliego de cláusulas administrativas particulares y en el de prescripciones técnicas correspondientes al expediente de contratación.

La empresa acepta de forma expresa su sumisión a la legislación de contratos del Sector Público reseñada en el párrafo anterior, así como al pliego de cláusulas administrativas particulares y al pliego de prescripciones técnicas correspondientes.

Será competencia de la Jurisdicción Contencioso-Administrativa el conocimiento, de cualquier cuestión litigiosa que pudiera surgir respecto de su cumplimiento, interpretación, efectos y resolución.

#### **TERCERA.- DOCUMENTOS QUE INTEGRAN EL CONTRATO.**

Este contrato esta integrado por los siguientes documentos y con el siguiente orden de prioridad:

1. Pliego de Cláusulas Administrativas Particulares.
2. Pliego de Prescripciones Técnicas.
3. La oferta del contratista.
4. El presente contrato

#### **CUARTA.- CONFORMIDAD DEL CONTRATISTA.**

El adjudicatario presta su conformidad al pliego de cláusulas administrativas particulares y al pliego de prescripciones técnicas que rigen esta contratación, quedando unidos al presente contrato.

El adjudicatario manifiesta que las circunstancias reflejadas en el certificado del Registro Oficial de Licitadores y Empresas Clasificadas, presentado para la licitación de este contrato, no han experimentado variación.

#### **QUINTA.- PRECIO.**

La cuantía total del presente contrato asciende a 75.310,40€, tal como se detalla a continuación:

DENOMINACIÓN	AÑO	PRECIO (Sin IVA)	IMPORTE IVA	PRECIO TOTAL (Incluido IVA 21%)	APLICACIÓN PRESUPUESTARIA
Cesión de uso de 5.000 licencias del producto <b>IntelliTrust Authentication Service Enterprise</b> incluidas las licencias necesarias de <b>Mobile Soft Token</b> .	2025	42.664,52 €	8.959,55 €	51.624,07 €	05.22.491A01.20600.0
	2026	19.575,48 €	4.110,85 €	23.686,33 €	05.22.491A01.20600.0
total		62.240,00 €	13.070,40 €	75.310,40 €	

#### **SEXTA.- REVISIÓN DE PRECIOS.**

El precio de este contrato no podrá ser objeto de revisión, de acuerdo con la cláusula 6ª del pliego de cláusulas administrativas particulares y el apartado 12.5 del cuadro de características del citado pliego.

#### **SEPTIMA.- DURACIÓN DEL CONTRATO.**

La duración inicial del presente contrato es de 12 meses desde el 25 de enero de 2025.

El contrato podrá prorrogarse, antes de finalizar aquel y de forma expresa, por un periodo máximo de 12 meses, tal como se establece en el pliego de cláusulas administrativas particulares, permaneciendo las características de este inalterables durante el periodo de ejecución de ésta. La prórroga se realizará en la forma y condiciones indicadas en el citado pliego.

La prórroga se acordará por el órgano de contratación y será obligatoria para el empresario, siempre que su preaviso se produzca al menos con dos meses de antelación a la finalización del plazo de duración del contrato.

#### **OCTAVA.- ENTREGA DE LOS BIENES.**

Durante el plazo de ejecución del contrato, el contratista se compromete a suministrar los bienes objeto de este a los precios y en las condiciones y plazos máximos ofertados por el adjudicatario.

#### **NOVENA.- RÉGIMEN DE PAGOS.**

El pago se tramitará una vez recibido de conformidad el suministro realizado y previa la presentación de la correspondiente factura electrónica.

El pago se realizará de conformidad con lo establecido en la cláusula 6.1 y en el apartado correspondiente al "Régimen de pago" del cuadro de características del pliego de cláusulas administrativas particulares, es decir por trimestres naturales vencidos, previa entrega de la factura correspondiente, y a la emisión de un informe favorable de la Dirección Técnica de Tecnologías de la Información y Comunicación o del Servicio de Comunicaciones

#### **DÉCIMA.- PLAZO DE GARANTÍA.**

El plazo de garantía será de 1 mes contado a partir de la fecha del acto formal y positivo de recepción o de conformidad de la prestación del objeto contractual, y en los términos indicados en el pliego de cláusulas administrativas particulares.

#### **UNDÉCIMA.- GARANTÍA DEFINITIVA.**

Para responder del cumplimiento de las obligaciones contraídas con la firma de este contrato, el adjudicatario ha constituido a favor de la Gerencia Regional de Salud una garantía por importe de 3.112,00 €, según se acredita mediante la presentación del correspondiente resguardo.

#### **DUODÉCIMA.- PRERROGATIVAS**

El órgano de contratación, dentro de los límites y con sujeción a los requisitos y efectos señalados en el artículo 190 LCSP, ostenta la prerrogativa de interpretar los contratos administrativos, resolver las dudas que ofrezca su cumplimiento, modificarlos por razones de interés público, declarar la responsabilidad imputable al contratista a raíz de la ejecución del contrato, suspender la ejecución del mismo, acordar su resolución, determinar los efectos de esta y la inspección de las actividades del contratista, limitando su ejercicio a los aspectos que tengan relación con la ejecución del contrato

#### **DÉCIMOTERCERA.- MODIFICACIÓN DEL CONTRATO.**

De acuerdo con lo establecido en el cuadro de características del pliego de cláusulas administrativas particulares este contrato no puede ser objeto de modificación.

No obstante, lo indicado en el párrafo anterior, en todo caso, el contrato podrá ser objeto de modificación cuando se cumplan los requisitos establecidos en el artículo 205 de la LCSP.

#### **DÉCIMOCUARTA.- RÉGIMEN DE PENALIDADES.**

**1.- PENALIDADES POR DEMORA.** El contratista estará obligado a cumplir el plazo fijado para la ejecución del contrato. Si el contratista, por causas imputables al mismo, hubiera incurrido en demora respecto del plazo establecido, la Administración procederá a la imposición de las penalidades establecidas en el artículo 193 de la LCSP.

**2.- OTRAS PENALIDADES.** El órgano de contratación aplicará en la ejecución del contrato las penalidades por incumplimiento de los compromisos o de las condiciones especiales de ejecución que, en su caso, estén establecidas en el apartado 23.4 del cuadro de características del pliego de cláusulas administrativas que rige este contrato.

### **3.- EJECUCIÓN DE LAS PENALIDADES.**

Las penalidades se ejecutarán de acuerdo con el procedimiento establecido en el apartado 23.4 del cuadro de características del pliego de cláusulas administrativas que rige este contrato.

El importe de las penalidades no incluye la indemnización de daños y perjuicios a que pueda tener derecho la Administración, originados por el contratista.

El importe de las penalidades se hará efectivo mediante deducción del mismo en las facturas que deban abonarse al contratista. En todo caso, la garantía responderá de la efectividad de ellas, de acuerdo con lo establecido en el artículo 110. b) de la LCSP.

### **DÉCIMOQUINTA.- OBLIGACIÓN DEL CONTRATISTA DE CUMPLIMIENTO DE CONVENIO COLECTIVO.**

El adjudicatario tiene obligación de cumplir durante todo el periodo de ejecución de contrato las normas y condiciones salariales que respecto de sus trabajadores estén fijadas en el convenio colectivo de aplicación.

### **DÉCIMOSEXTA.- INFORMACIÓN A PROPORCIONAR POR EL CONTRATISTA.**

El adjudicatario está obligado a proporcionar toda la información que le sea requerida por el órgano de contratación relacionada con este contrato, de conformidad con lo establecido en la D. A. Tercera de la Ley 3/2015, de 4 de marzo, de Transparencia y Participación Ciudadana de Castilla y León.

### **DÉCIMOSEPTIMA.- RESOLUCIÓN DEL CONTRATO**

El órgano de contratación acordará la resolución del contrato, y determinará los efectos de ésta en los supuestos señalados en la LCSP y, en su caso, en el pliego de cláusulas administrativas particulares. La resolución del contrato se realizará dentro de los límites y con sujeción a los requisitos y efectos establecidos en la LCSP.

### **DÉCIMOCTAVA.- CONDICION ESPECIAL DE EJECUCIÓN**

1.-El adjudicatario deberá entregar la documentación asociado al contrato exclusivamente en formato electrónico, con el objetivo de favorecer la reducción de las emisiones de gases de efecto invernadero.

Penalidad: el incumplimiento de esta condición especial de ejecución conlleva una penalización del 1% del importe de adjudicación del contrato, IVA excluido. Se descontará de cada factura que se emita a lo largo del incumplimiento, hasta alcanzar la penalización máxima permitida legalmente.

Forma de verificación del cumplimiento de esta condición especial de ejecución: El designado como responsable del contrato, por parte de la Administración, verificará la entrega de la documentación en formato electrónico dejando constancia del justificante del correo recibido antes del pago de la factura

2.- El contratista tiene la obligación de someterse a la normativa nacional y de la Unión Europea en materia de protección de datos.

Esta obligación tiene el carácter de contractual esencial de conformidad con lo dispuesto en la letra f) del apartado 1 del artículo 211 de la Ley de Contratos del Sector Público. siendo causa de resolución del contrato en caso de incumplimiento.

Forma de verificación del cumplimiento de esta condición especial de ejecución: se realizará mediante declaración del contratista del sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos, que se presentará durante el plazo de ejecución del contrato

## **DÉCIMONOVENA.- PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL**

### **1.-Objeto del encargo del tratamiento**

Mediante las presentes cláusulas se habilita a la empresa SISTEMAS INFORMÁTICOS ABIERTOS, SAU, encargada del tratamiento, para tratar por cuenta de la Gerencia Regional de Salud, responsable del tratamiento, los datos personales necesarios para prestar los servicios de doble autenticación y dar mayor seguridad en el acceso de los usuarios a los servicios y sistemas de información de la GRS.

El tratamiento consistirá en las tareas a desarrollar definidas pormenorizadamente en el Pliego de Prescripciones Técnicas del contrato.

#### **Concreción de los tratamientos a realizar:**

<input type="checkbox"/> Recogida (captura de datos)	<input checked="" type="checkbox"/> Registro (grabación)	<input type="checkbox"/> Estructuración	<input type="checkbox"/> Modificación
<input type="checkbox"/> Conservación (almacenamiento)	<input type="checkbox"/> Extracción	<input checked="" type="checkbox"/> Consulta	<input type="checkbox"/> Comunicación por transmisión
<input type="checkbox"/> Difusión	<input type="checkbox"/> Interconexión	<input type="checkbox"/> Cotejo	<input type="checkbox"/> Limitación
<input type="checkbox"/> Supresión	<input type="checkbox"/> Destrucción (incluidas copias temporales)	<input type="checkbox"/> Conservación (en sus sistemas de información)	<input type="checkbox"/> Recuperación
<input type="checkbox"/> Duplicado	<input type="checkbox"/> Copia (copias temporales)	<input type="checkbox"/> Copia de Seguridad	<input type="checkbox"/> Comunicación
<input type="checkbox"/> Seudonimización	<input type="checkbox"/> Anonimización	<input type="checkbox"/> Sincronización de resultados con la nube	<input type="checkbox"/> Otros: _____

### **2.-Identificación de la información afectada**

Para la ejecución de las prestaciones derivadas del cumplimiento del objeto de este encargo, de la Gerencia Regional de Salud responsable del tratamiento, pone a disposición de la empresa SISTEMAS INFORMÁTICOS ABIERTOS, S.A.U, encargada del tratamiento, la información que se describe a continuación:

#### **Colectivos de personas interesadas:**

<input checked="" type="checkbox"/> EMPLEADOS	<input type="checkbox"/> COLABORADORES EXTERNOS	<input type="checkbox"/> PACIENTES	<input type="checkbox"/> PADRES, TUTORES Y/O REPRESENTANTES LEGALES
<input type="checkbox"/> ASOCIADOS O MIEMBROS	<input type="checkbox"/> ESTUDIANTES	<input type="checkbox"/> INVESTIGADORES	<input type="checkbox"/> PERSONAS DE CONTACTO
<input type="checkbox"/> VOLUNTARIOS	<input type="checkbox"/> SOLICITANTES	<input type="checkbox"/> DONANTES	<input type="checkbox"/> RECEPTORES
<input type="checkbox"/> BENEFICIARIOS	<input type="checkbox"/> PARTICIPANTES	<input type="checkbox"/> PROVEEDORES	<input type="checkbox"/> Otros: _____

**Tipología de datos por colectivo identificado:**

- **Identificativos:** Nombre y apellidos; DNI / CIF / documento identificativo; Correo electrónico

**3.- Duración**

El presente contrato tiene una duración coincidente con el plazo de ejecución del contrato mencionado, sin perjuicio de las responsabilidades dimanantes del mismo (por vulneración de las previsiones del RGPD por el encargado del tratamiento) y la confidencialidad a la que el encargado del tratamiento y sus trabajadores se encuentran sujetos.

Una vez finalice el presente contrato, el encargado del tratamiento deberá suprimir o devolver al responsable del tratamiento, a su elección, todos los datos personales a los que haya tenido acceso para prestar el servicio. Asimismo, el encargado del tratamiento se obliga a suprimir las copias existentes, a menos que exista una norma jurídica que exija la conservación de los datos personales. Una vez destruidos de forma segura, el encargado debe certificar su destrucción por escrito y debe entregar dicho certificado al responsable. No obstante, el encargado del tratamiento podrá conservar los datos, debidamente bloqueados, en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

**4.- Obligaciones del encargado del tratamiento**

El encargado del tratamiento y todo su personal se obliga a:

- Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, solo para la finalidad objeto de este encargo. En ningún caso podrá utilizar los datos para fines propios.
- Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento.  
Si el encargado del tratamiento considera que alguna de las instrucciones infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, el encargado informará inmediatamente al responsable.
- Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, que contenga:

1. El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado y, en su caso, del representante del responsable o del encargado y del delegado de protección de datos.
  2. Las categorías de tratamientos efectuados por cuenta de cada responsable.
  3. En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 apartado 1, párrafo segundo del RGPD, la documentación de garantías adecuadas.
  4. Una descripción general de las medidas técnicas y organizativas de seguridad relativas a:
    - a) La seudonimización y el cifrado de datos personales.
    - b) La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
    - c) La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
    - d) El proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- d) No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles.

El encargado puede comunicar los datos a otros encargados del tratamiento del mismo responsable, de acuerdo con las instrucciones del responsable. En este caso, el responsable identificará, de forma previa y por escrito, la entidad a la que se deben comunicar los datos, los datos a comunicar y las medidas de seguridad a aplicar para proceder a la comunicación.

Si el encargado 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, salvo que tal Derecho lo prohíba por razones importantes de interés público, según la letra g) de este punto 4.

- e) El encargado del tratamiento aportará la documentación que detalle si la información se va a tratar en sistemas e instalaciones propias o de la entidad pública contratante.

Cuando el personal del Encargado desempeñe sus funciones en las instalaciones del responsable del tratamiento, deberá conocer y cumplir las medidas de seguridad establecidas para el acceso a las instalaciones. Es responsabilidad del Encargado la distribución de dichas medidas a su personal, cuando sea necesario.

- f) En todo caso, y previo a la formalización del contrato de prestación de servicios, el encargado del tratamiento, mediante una declaración, informará al responsable del tratamiento de la ubicación de sus servidores y desde dónde se van a prestar los servicios asociados a los mismos. Asimismo, el encargado informará al responsable de cualquier cambio que se produzca, a lo largo de la vida del contrato, en relación a la ubicación de los servidores, de conformidad con el artículo 122.2 de la Ley 9/2017, de 8 de noviembre de Contratos del Sector Público.

- g) No están permitidas las transferencias internacionales de datos. Los tratamientos de datos se realizarán dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente. Por tanto, los datos no podrán ser tratados fuera de este espacio, ni directamente, ni a través de cualquier subcontratista autorizado, conforme a lo establecido en el pliego o contrato y demás documentos contractuales, salvo que esté obligado a



ello en virtud del Derecho de la Unión o del Estado miembro que le resulte de aplicación.

En el caso de que el Derecho nacional o de la Unión Europea obliguen al encargado del tratamiento a llevar a cabo transferencias internacionales de datos, el encargado informará por escrito al responsable del tratamiento de esa exigencia legal, con antelación suficiente antes de llevar a cabo el tratamiento y garantizando el cumplimiento de los requisitos legales aplicables al responsable, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.

No obstante, el responsable del tratamiento podrá autorizar expresamente y por escrito la transferencia internacional de datos cuando el encargado del tratamiento justifique el mecanismo jurídico en que se basa la transferencia y garantías suficientes para la protección de los derechos y libertades de las personas interesadas. El encargado, antes de realizar la transferencia, deberá notificar al responsable los detalles de esta con una antelación mínima de un (1) mes, que, a falta de respuesta del responsable, se entenderá como no autorizada.

#### h) Subcontratación

No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten el tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.

Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito al responsable, con una antelación de 15 días laborables, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratista y sus datos de contacto. La subcontratación podrá llevarse previo consentimiento expreso por escrito del responsable del tratamiento.

El subcontratista, que también tendrá la condición de encargado del tratamiento, está obligado igualmente a cumplir las obligaciones establecidas en este documento para el encargado del tratamiento y las instrucciones que dicte el responsable. Corresponde al encargado inicial regular la nueva relación de forma que el nuevo encargado quede sujeto a las mismas condiciones (instrucciones, obligaciones, medidas de seguridad...) y con los mismos requisitos formales que él, en lo referente al adecuado tratamiento de los datos personales y a la garantía de los derechos de las personas afectadas. En el caso de incumplimiento por parte del subencargado, el encargado inicial seguirá siendo plenamente responsable ante el responsable en lo referente al cumplimiento de las obligaciones.

Asimismo, si el establecimiento o el mantenimiento de los servidores fueran objeto de subcontratación, el encargado deberá comunicarlo al responsable en los mismos términos.

El responsable del tratamiento autoriza expresamente las subcontratas que a continuación se detallan.

#### Subencargados contratados por el encargado del tratamiento y servicio prestado:

- 1.
- 2.

i) Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del presente encargo, incluso después de que finalice su objeto.

j) Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y deber de secreto y a cumplir las medidas de

seguridad correspondientes, de las que hay que informarles convenientemente. La obligación de confidencialidad y deber de secreto tiene carácter indefinido, y se mantendrá incluso finalizada la prestación del servicio y la relación de la persona autorizada con el encargado del tratamiento.

El encargado del tratamiento debe garantizar la misma obligación de confidencialidad y deber de secreto respecto de aquellas personas, que sin estar autorizadas a tratar los datos personales objeto de este encargo, puedan tener acceso a ellos de forma accesorio, circunstancial o fortuita.

k) Mantener a disposición del responsable la documentación acreditativa del cumplimiento de la obligación establecida en el apartado anterior.

l) Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.

m) Asistir al responsable del tratamiento para que este pueda cumplir con la obligación de dar respuesta a las solicitudes de ejercicio de los derechos de:

- 1) Acceso, rectificación, supresión y oposición
- 2) Limitación del tratamiento
- ...3) Portabilidad de datos
- ...4) A no ser objeto de decisiones individualizadas automatizadas (incluida la elaboración de perfiles)

Cuando las personas interesadas ejerzan los derechos de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, ante el encargado del tratamiento, este debe comunicarlo por correo electrónico a la dirección [dpd@saludcastillayleon.es](mailto:dpd@saludcastillayleon.es). La comunicación debe hacerse de forma inmediata y en ningún caso más allá de los cinco días laborables siguientes al de la recepción de la solicitud, juntamente, en su caso, con otras informaciones que puedan ser relevantes para resolver la solicitud.

n) Derecho de información: corresponde al responsable facilitar el derecho de información en el momento de la recogida de los datos.

o) Notificación de violaciones de la seguridad de los datos.

El encargado del tratamiento notificará al responsable del tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 24 horas, y a través de correo electrónico a la dirección [dpd@saludcastillayleon.es](mailto:dpd@saludcastillayleon.es), 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.

No será necesaria la notificación cuando sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas.

Si se dispone de ella se facilitará, como mínimo, la información siguiente:

- 1) 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 personas afectadas, y las categorías y el número aproximado de registros de datos personales afectados.

- 2) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información.
- 3) Descripción de las posibles consecuencias de la violación de la seguridad de los datos personales.
- 4) Descripción de las medidas adoptadas o propuestas para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Si no es posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

El encargado del tratamiento prestará su apoyo al responsable en la notificación a la Agencia Española de Protección de Datos u otra Autoridad de Control competente, y en su caso, a los interesados de las violaciones de seguridad que se produzcan

- p) Dar apoyo al responsable del tratamiento en la realización de las evaluaciones de impacto relativas a la protección de datos, cuando proceda.
- q) Dar apoyo al responsable del tratamiento en la realización de las consultas previas a la autoridad de control, cuando proceda.
- r) Poner a disposición del responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para la realización de las auditorías o las inspecciones que realicen el responsable u otro auditor autorizado por él.
- s) Implantar las medidas técnicas y organizativas de seguridad de la información, señaladas en el Anexo Medidas de Seguridad, parte de este contrato.

En todo caso, deberá implantar mecanismos para:

- a) Garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
  - b) Restaurar la disponibilidad y el acceso a los datos personales de forma rápida, en caso de incidente físico o técnico.
  - c) Verificar, evaluar y valorar, de forma regular, la eficacia de las medidas técnicas y organizativas implantadas para garantizar la seguridad del tratamiento.
  - d) Seudonimizar y cifrar los datos personales, en su caso.
- t) Designar un delegado de protección de datos y comunicar su identidad y datos de contacto al responsable.

Miguel Angel Canora: [dpo@indra.es](mailto:dpo@indra.es).

u) Destino de los datos: suprimir o devolver al responsable del tratamiento, a su elección, todos los datos personales a los que haya tenido acceso para prestar el servicio. Asimismo, el encargado del tratamiento se obliga a suprimir las copias existentes, a menos que exista una norma jurídica que exija la conservación de los datos personales. No obstante, el encargado del tratamiento

podrá conservar los datos, debidamente bloqueados, en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento. En el plazo de 15 días hábiles, el Encargado aportará un certificado acreditativo de la destrucción de forma segura de la información.

En el caso de que fuera necesaria su conservación en los términos señalados en el párrafo anterior, adicionalmente el Encargado acreditará en el mismo certificado el bloqueo de los datos en el soporte original o la conservación en una copia bloqueada de acuerdo a lo previsto en el artículo 32 de la Ley Orgánica 3/2018, de 5 de diciembre de Protección de Datos Personales y garantía de los derechos digitales.

#### **5.-Obligaciones del responsable del tratamiento**

Corresponde al responsable del tratamiento:

- a) Entregar al encargado los datos a los que se refiere la cláusula 2 de este documento.
- b) Realizar, si procede, una evaluación del impacto en la protección de datos personales de las operaciones de tratamiento a realizar por el encargado.
- c) Realizar las consultas previas que corresponda.
- d) Velar, de forma previa y durante todo el tratamiento, por el cumplimiento del RGPD por parte del encargado.
- e) Supervisar el tratamiento, incluida la realización de inspecciones y auditorías.

#### **6) Legislación aplicable y jurisdicción**

La presente cláusula se regirá por lo dispuesto en el RGPD y LOPDGDD, y demás normativa nacional y europea aplicable en materia de protección de datos personales. Asimismo, las partes acuerdan que la AEPD será competente para actuar como autoridad de control en los tratamientos de datos transfronterizos.

En el caso de controversia derivada de la aplicación del presente contrato, las partes acuerdan la renuncia expresa a su fuero propio y se someten a la jurisdicción de los Juzgados y Tribunales de Valladolid.

## ANEXO MEDIDAS DE SEGURIDAD

### RESTRICCIONES GENERALES

En el marco de la ejecución del contrato, y respecto a los sistemas de información que le dan soporte, las siguientes actividades están específicamente prohibidas:

- La utilización de los sistemas de información para la realización de actividades ilícitas o no autorizadas, como la comunicación (cesión) o distribución de medios, datos u otros contenidos a los que se tenga acceso en virtud de la ejecución de los trabajos y, especialmente, los que estén protegidos por disposiciones de carácter legislativo o normativo.
- La instalación no autorizada de software, modificación de la configuración o conexión a redes.
- La modificación no autorizada del sistema de información o del software instalado, el uso del sistema distinto al de su propósito.
- La sobrecarga, prueba, o desactivación de los mecanismos de seguridad y las redes, así como la monitorización no autorizada de redes o teclados.
- La reubicación física y los cambios de configuración de los sistemas de información o de sus redes de comunicación.
- La instalación de dispositivos o sistemas ajenos al desarrollo del contrato sin autorización previa, tales como dispositivos USB, soportes externos, ordenadores portátiles, puntos de acceso inalámbricos, tabletas o PDA's.
- La posesión, distribución, comunicación, revelación o alteración de cualquier información sin el consentimiento expreso del propietario o responsable de la misma.
- Compartir cuentas e identificadores personales (incluyendo contraseñas y PIN) o permitir el uso de mecanismos de acceso, sean locales o remoto, a personas no autorizadas.
- Inutilizar o suprimir de forma no autorizada cualquier elemento de seguridad o protección o la información que generen.

### MEDIDAS DE SEGURIDAD

Los datos deberán protegerse mediante medidas de seguridad que salvaguarden la confidencialidad, integridad y disponibilidad. Se deben implantar, al menos las siguientes medidas de seguridad:

1.- El encargado deberá concienciar y formar a su personal en materia de seguridad de la información y de protección de datos, y en particular sobre aquellos aspectos de la Política de Seguridad de la Información y de Protección de Datos vigente en la Gerencia Regional de Salud de Castilla y León y su marco normativo de seguridad, que sean de aplicación en base a la naturaleza de los servicios prestados.

Los trabajadores del encargado por su parte deben tener siempre presentes durante el desempeño de sus funciones los principios de la ética, la profesionalidad, la confidencialidad y deber de secreto, y la responsabilidad.

De forma general, todo el personal del encargado del tratamiento que acceda a la información del responsable del tratamiento deberá cumplir con las siguientes normas:

- Acceder exclusivamente a los sistemas de información mediante el acceso y los medios autorizados.
- Proteger la confidencialidad de la información de toda revelación no autorizada.
- Proteger la integridad de la información del responsable del tratamiento a la que tenga acceso en el ámbito de la prestación de los servicios.

Todos los empleados del encargado del tratamiento deben hacerse responsables de la custodia personal de las credenciales que tienen asignadas para el acceso a los recursos de los sistemas de información y/o a la información del responsable del tratamiento. Estas credenciales nunca podrán ser facilitadas a terceras personas, sean o no empleados del encargado del tratamiento, y los propietarios de las mismas deberán ser únicos responsables del uso que se haga de ellas.

Además, el encargado deberá poner en marcha medidas de control para garantizar la supervisión de las actuaciones para sus trabajadores.

2.- El encargado del tratamiento deberá aplicar medidas técnicas y organizativas apropiadas a un nivel de seguridad adecuado al riesgo, que en su caso incluyan, entre otras:

- La seudonimización y el cifrado de datos personales.
- La interconexión de sistemas.
- Las validaciones oportunas para proteger la cadena de suministro.
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.
- Cifrado de datos personales, mediante algoritmos aprobados por el CCN, Guía CCN-STIC-807.
- Cifrado de la información en tránsito HTTPS (TLS1.2 o superior) e indicación de la existencia de dispositivos de seguridad para el análisis de este tipo de tráfico.
- Garantías de borrado seguro y destrucción de la información en todos los medios de almacenamiento, incluidos los de las plataformas de proveedores y subcontratistas del encargado del tratamiento.
- La capacidad de garantizar que el suministro del servicio en la nube cumple con el conjunto de medidas de seguridad en función del modelo de servicio que se preste.

3.- El encargado del tratamiento no podrá transmitir, enviar, compartir o poner a disposición de otras entidades información propiedad del responsable del tratamiento, a no ser que de manera previa haya sido expresamente autorizado para hacerlo, independientemente del medio o formato de la información y de su contenido. En el caso de existir dicha autorización se deberá velar por el cumplimiento de las siguientes normas:

- Deberán extenderse al receptor de la información todas las obligaciones del encargado en

materia de seguridad de la información y protección de datos impuestas por el responsable del tratamiento.

- El encargado del tratamiento será responsable del uso y la protección de la información del responsable del tratamiento que le haya sido proporcionada, así como de los perjuicios ocasionados al responsable del tratamiento en los casos en los que la seguridad de la información o de los datos personales hubieran sido comprometidas.
- Se podrá transmitir única y exclusivamente la información estrictamente necesaria para que el subencargado autorizado pueda llevar a cabo su cometido.
- La información solo podrá ser transmitida a los destinatarios autorizados, que han de estar unívocamente identificados, y por medios que garanticen la identidad de dicho destinatario.
- En la transmisión de la información se deberán aplicar mecanismos que imposibiliten el acceso a ella por parte de otras entidades no autorizadas. Igualmente, en el almacenamiento de la información en dispositivos portátiles o extraíbles se deberán aplicar mecanismos que imposibiliten dichos accesos.

4.- En todo aquel equipamiento informático propiedad del encargado del tratamiento en el cual se almacene, procese o desde el que se acceda a información del responsable del tratamiento, el encargado del tratamiento deberá aplicar las medidas de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de dicha información. Al menos, el encargado debe aplicar las siguientes medidas de seguridad:

- Protección contra código malicioso: todos los equipos deberán contar con programas antivirus y de protección ante software malicioso (malware) actualizados de forma automática y permanente.
- Control de acceso: todos los equipos deberán disponer de medidas que aseguren el acceso sólo por parte del personal autorizado.
- Bloqueo de terminales: no se deberán dejar los terminales desatendidos sin antes haber bloqueado la sesión de usuario con el fin de evitar accesos no autorizados. El bloqueo automático tras un periodo de inactividad también debe estar activado.
- Actualización de sistemas: todo el equipamiento informático deberá estar al día con las últimas actualizaciones y parches de seguridad disponibles.
- Salvaguarda de la información: se han de implementar mecanismos de copia de seguridad y recuperación en aquella información de la Gerencia Regional de Salud de Castilla y León.
- Privilegios: los usuarios no deben poder deshabilitar o desinstalar las protecciones de seguridad implantadas en los equipos.

El responsable del tratamiento se reserva el derecho de exigir la implantación de las medidas de seguridad adicionales que considere oportunas, en el equipamiento informático del encargado.

5.- Cuando el encargado del tratamiento deba acceder de forma remota a los sistemas de información del responsable del tratamiento, los equipos desde los que efectúe dicho acceso deberán contar con las medidas de seguridad indicadas en el punto precedente (punto 4).

Además, el acceso se debe efectuar siempre a través de conexiones seguras cifradas y con credenciales individuales.

En cualquier caso, el encargado del tratamiento deberá asegurar la imposibilidad de acceso no autorizado a los equipos informáticos desde los que se inicie el canal de comunicaciones con los sistemas de información del responsable del tratamiento.

6.- El acceso físico a las dependencias del responsable del tratamiento únicamente podrá llevarse a cabo cuando el personal del encargado del tratamiento disponga de autorización previa para ello.

7.- En aquellas instalaciones, donde se almacene o procese información del responsable del tratamiento, el encargado deberá implementar medidas de seguridad física, ambiental y de control de acceso, y todo su personal deberá participar activamente en la implantación y cumplimiento de estas medidas.

8.- El encargado del tratamiento deberá definir e implementar medidas y estrategias que garanticen la continuidad de los servicios prestados al responsable del tratamiento en caso de contingencia, tal y como se indica en el punto 3.18 del pliego.

El encargado no podrá dejar de implementar estas medidas, tampoco suprimirlas basándose en un análisis de riesgo o evaluación de impacto salvo aprobación expresa y por escrito del responsable del tratamiento.

Las personas que trabajen para el encargado del tratamiento deben seguir las medidas de seguridad e instrucciones especificadas por el responsable, no pudiendo realizar tratamientos diferentes a los definidos por el responsable.

El encargado del tratamiento, en el caso de que el tratamiento de los datos se lleve a cabo en sus instalaciones, deberá especificar adicionalmente las medidas de seguridad física adoptadas en este apartado "Medidas de seguridad" de este Anexo.

Y para que conste, y en prueba de conformidad por ambas partes, se firma electrónicamente este contrato y se considera formalizado en la fecha de la última de sus firmas

EL DIRECTOR ECONÓMICO,  
PRESUPUESTARIO Y FINANCIERO  
Israel Diego Aragón

EL ADJUDICATARIO  
Ana Isasi Gómez  
D Joaquín Ciruelo Meléndez