

En Sarriguren, a 29 de agosto de 2024

REUNIDOS

DE UN PARTE: D. Daniel Goñi Merino (mayor de edad, con domicilio profesional en Sarriguren-Valle de Egüés, Navarra, calle Cabárceno, nº6 y con NIF nº 33.435.846-X), en calidad de apoderado de **“TRACASA INSTRUMENTAL, S.L.”** y en su representación, en virtud de las facultades que le confiere el poder otorgado ante el Notario de Pamplona, D. Rafael Unceta Morales con fecha 23 de julio de 2.020, numero 765 de protocolo e inscrito en el Registro Mercantil de Navarra al tomo 1806, folio 32, hoja NA-35819, inscripción 19.

“TRACASA INSTRUMENTAL S.L.” está domiciliada en Sarriguren-Valle de Egüés (Navarra), calle Cabárceno, nº6. Se constituyó por tiempo indefinido en escritura autorizada el 18 de marzo de 2016 por el Notario de Pamplona D. Rafael Unceta Morales, nº412 de protocolo que se inscribió en el Registro Mercantil de Navarra al tomo 1806, folio 23, hoja NA-35819, inscripción 1.

C.I.F. B-71280689

Correo electrónico a efectos de comunicaciones: cvasquez@itracasa.es

En adelante se la denominará **“ITRACASA”**.

Y, DE OTRA PARTE: D. Carlos Moles Abelló (mayor de edad, con domicilio profesional en Reus, y con NIF nº 38534466-J), en calidad de Representante de **“SUMMAR SOFTWARE Y SERVICIOS INFORMÁTICOS, S.A.”** y en su representación, en virtud de las facultades contenidas en la escritura formalizada el 01 de Abril de 1985, ante el Notario de Reus, D. Agustín Maria Altés Salafranca con nº677 de su protocolo, e inscrita en el Registro Mercantil de Tarragona al tomo 1892, folio 220, hoja T-2582, inscripción 31ª.

“SUMMAR SOFTWARE Y SERVICIOS INFORMÁTICOS, S.A.” está domiciliada en Reus (Tarragona), calle Vilafortuny, número 3, bajos. Se constituyó por tiempo indefinido en escritura autorizada el 1 de abril de 1985 por el Notario de Reus, D. Agustín Maria Altés Salafranca. Está inscrita en el Registro Mercantil de Tarragona al tomo 1892, folio 220, hoja T-2582, inscripción 31ª

C.I.F. A-43064781.

Correo electrónico a efectos de comunicaciones: administracion@summar.es

En adelante se la denominará **“SUMMAR”**.

Ambas partes se reconocen competencia y capacidad, respectivamente, para formalizar el presente contrato conforme a los antecedentes y cláusulas siguientes:

ANTECEDENTES

PRIMERO. – **ITRACASA** es el ente instrumental de referencia para el Gobierno de Navarra en servicios y conocimientos de transformación digital, gestión tributaria, gestión del territorio y atención a la ciudadanía. **ITRACASA** está conformada por un equipo de más de 500 personas, con un alto porcentaje de titulados superiores. **ITRACASA** tiene el compromiso de cumplir con los servicios encomendados y de dotar personal a los mismos para poder ejecutarlos.

SEGUNDO. – De cara a la administración de su personal, **ITRACASA** necesita disponer de un Software para el Área de Personas y Talento que le permita gestionar todo lo relacionado con las nóminas, la selección de personal, formaciones, desarrollo, prevención de riesgos laborales, etc. El Software ofrecido por **SUMMAR** cumple con todos los requerimientos de **ITRACASA**.

SUMMAR ostenta la propiedad intelectual del mencionado Software, que incluye las herramientas “Labor” para la gestión de nóminas y “Mentor” para la selección, formación y evaluación de personal, así como para la gestión de PRL, junto con Portales para Empleados, Managers y Candidatos.

TERCERO. – Dada su condición de sociedad pública, **ITRACASA** debe formalizar el correspondiente procedimiento de licitación para el suministro del mantenimiento anual de las herramientas Labor y Mentor.

Por la condición de **SUMMAR** de proveedor único por motivos de propiedad intelectual, único proveedor habilitado para el suministro de licencias y soporte oficial, con fecha 20 de agosto de 2023 **ITRACASA** formaliza un informe jurídico en el cual, amparándose en el artículo 75.1c) de la Ley Foral 2/2018, de 13 de Abril, de Contratos Públicos autoriza la contratación directa con **SUMMAR**. Con fecha 17 de agosto de 2023 se formalizó contrato entre ambas partes.

CUARTO. – Con fecha 28 de agosto de 2024, el Departamento Jurídico de **ITRACASA** analiza la situación y considera que la necesidad de contratar los servicios con **SUMMAR** como suministrador único persiste, por lo que procede a la redacción de un nuevo informe jurídico en el cual, amparándose en la misma legislación, autoriza la contratación por un máximo de cuatro años si así lo estimasen las partes.

QUINTO. – **SUMMAR** dispone de la solvencia técnica necesaria para llevar a cabo el trabajo que **ITRACASA** necesita, por lo que, ambos se han puesto de acuerdo para contratar la prestación de los servicios requeridos y el precio de los mismos.

SEXTO. – Ambas partes otorgan el presente contrato con las siguientes

CLÁUSULAS

PRIMERA. OBJETO. El objeto del presente contrato son los trabajos relativos al “**Suministro del mantenimiento anual de las herramientas Labor y Mentor**”, con arreglo a lo establecido en las siguientes condiciones en esta contratación.

SEGUNDA. PRECIO Y ABONO. El precio, excluido el IVA., por la realización del trabajo contratado conforme a las condiciones esenciales, asciende a **DIEZ MIL NOVECIENTOS SETENTA Y SEIS euros (10.976,00€, IVA excluido)**. Este precio podrá ser modificado cuando por necesidades de **ITRACASA** sea necesaria una ampliación de la funcionalidad y/o del número de usuarios.

No obstante, lo indicado en el primer párrafo, las obligaciones económicas de **ITRACASA** se limitarán exclusivamente de las que resulten de los servicios efectivamente ejecutados por **SUMMAR** conforme a las necesidades de **ITRACASA**, resultando que solo podrán facturarse los servicios realmente realizados y aceptados por **ITRACASA**, sin que haya posibilidad de exigir el pago de la totalidad del importe si al acabar la duración del contrato quedan importes sin consumir.

SUMMAR facturará los trabajos al inicio de los mismos previa aceptación por **ITRACASA**. **ITRACASA** realizará el pago, previa presentación de factura, mediante transferencia a los 30 días de su aprobación y teniendo en cuenta las fechas de pago que son los días 10 y 25 de cada mes.

TERCERA. REVISIÓN DE PRECIOS. No se aplicará.

CUARTA. PLAZO. El plazo de ejecución de los trabajos se extenderá desde el 1 de septiembre de 2024 hasta el 31 de agosto de 2025, con posibilidad de renovación por períodos anuales con un máximo de 3 prórrogas.

Esta renovación será expresa debiendo mediar acuerdo previo de las partes.

QUINTA. RESOLUCIÓN DEL CONTRATO. El contrato podrá ser objeto de resolución cuando concurra alguna de las siguientes causas:

- El incumplimiento de las cláusulas y/o condiciones contenidas en el contrato.
- La muerte o incapacidad sobrevenida de la persona adjudicataria o la extinción de su personalidad jurídica, salvo que se acuerde la continuación del contrato con sus personas herederas o entidades/empresas sucesoras. En los casos de fusión, escisión, aportación o transmisión de empresas o ramas de la empresa se entenderá subrogada en los derechos y deberes de la persona adjudicataria la entidad resultante o beneficiaria siempre que conserve la solvencia requerida para la formalización del contrato.
- La declaración de insolvencia en cualquier procedimiento y, en caso de concurso, la apertura de la fase de liquidación, salvo que, en este último caso, la persona adjudicataria preste las garantías suficientes a juicio de **ITRACASA** para la ejecución del mismo.
- La falta de acatamiento de las instrucciones en todo lo referente a este servicio.
- El incumplimiento de las condiciones especiales de ejecución del contrato.

- El incumplimiento de la persona adjudicataria en sus obligaciones laborales en materia de salarios, seguridad social, accidentes de trabajo, mutualismo laboral, formación, seguridad e higiene, etc.; estando **ITRACASA** exonerada de toda responsabilidad en esta materia.
- El mutuo acuerdo entre las partes.
- Cualquier otra determinada por la legislación vigente.

Además de las causas resolutorias del contrato reguladas en el derecho positivo y de las especificadas en el presente apartado, el contrato podrá resolverse por **ITRACASA** por el defectuoso cumplimiento técnico.

Bastará para la resolución del contrato con la notificación de la decisión y la causa al contratista por parte de **ITRACASA**, con una antelación de 60 días.

SEXTA. CONFIDENCIALIDAD. La empresa adjudicataria en general y, en particular, el personal de ésta que, de manera directa o indirecta, participe en la ejecución del presente contrato (a los presentes efectos quedan recogidos todos bajo el término “adjudicatario”) deberá mantener reserva total, respecto de la información técnica, económica, comercial, metodológica, jurídica u organizativa, o cualquier otra información confidencial que conciernan al negocio de **ITRACASA**, durante el tiempo de vigencia del presente contrato y, tras la finalización del mismo, durante tres años. El adjudicatario se compromete, asimismo, a no utilizar nada de ello, ni en su propio provecho, ni en el de terceros y tampoco revelarlo a ninguna persona física o jurídica.

El adjudicatario se compromete a no sacar ni favorecer la salida de información relativa a **ITRACASA**, a sus productos o clientes, por ninguna vía (escrita, impresa, digital, etc.), salvo que sea necesario para el correcto desempeño de sus funciones o regulado por normativas de obligado cumplimiento.

El adjudicatario no podrá reproducir por ningún medio parte o la totalidad de la información confidencial de **ITRACASA** sin su autorización previa. El adjudicatario se compromete a utilizar la información confidencial con la única finalidad de desarrollar la actividad objeto de las presentes condiciones esenciales.

Al término del presente contrato, cualquiera que fuese su causa, el adjudicatario deberá entregar a **ITRACASA** todos los documentos, materiales y demás bienes correspondientes a la actividad de la misma que en su momento pudieran estar en su control o bajo su potestad, no pudiendo conservar ningún documento físico o informático utilizado durante la vigencia de su relación laboral con **ITRACASA**.

Igualmente se compromete a respetar las normas específicas establecidas para garantizar la seguridad de la información relativa a los servicios en los que participe, tiene el derecho de conocer los condicionantes especiales relativos a la seguridad de la información antes de aceptar el proyecto y la responsabilidad de cumplir con ellos una vez aceptado.

El adjudicatario reconoce la extrema importancia que supone para **ITRACASA** la información confidencial y los gravísimos perjuicios que le puede ocasionar el incumplimiento de las obligaciones de confidencialidad establecidas en la presente cláusula.

SÉPTIMA. PROTECCION DE DATOS.

1.- Normativa

De conformidad con la Ley Foral 2/2018 de 13 de abril de Contratos Públicos, por la que se transponen al ordenamiento jurídico Navarro las Directivas del Parlamento Europeo y del Consejo 2014/23/UE y 2014/24/UE, de 26 de febrero de 2014, los contratos que impliquen el tratamiento de datos de carácter personal deberán respetar en su integridad 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 (RGPD), y la normativa complementaria.

Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquél tendrá la consideración de encargado del tratamiento. En este supuesto, el acceso a esos datos no se considerará comunicación de datos, cuando se cumpla lo previsto en el artículo 28 del RGPD. En todo caso, las previsiones de este deberán de constar por escrito.

2.- Información sobre los tratamientos de datos de los adjudicatarios

En relación con el tratamiento de los datos de carácter personal que pudieran darse como consecuencia de la adjudicación, de conformidad con lo indicado en el art. 13 del Reglamento (UE) 2016/679 (RGPD) se informa a los adjudicatarios de los siguientes extremos:

- Datos del Responsable: TRACASA INSTRUMENTAL, S.L., (en adelante el Responsable) sita en C/ Cabárceno, número 6, Sarriguren (Navarra), con número de teléfono 948 19 48 88 y dirección de correo electrónico sarteta@itracasa.es).

- Finalidad y legitimación de los tratamientos:

- a) Este de datos de los adjudicatarios queda legitimado por el consentimiento válidamente prestado por éstos en el momento de la presentación de su candidatura.
- b) Se emplearán los datos del adjudicatario para el control y ejecución de la relación jurídica que surja entre las partes. La recogida y tratamiento de los datos tiene su fundamento en el cumplimiento de una obligación legal aplicable al responsable del tratamiento (Ley Foral 2/2018 de 13 de abril de Contratos Públicos) y el desarrollo del contrato (Art. 6.1. b) del RGPD) para los tratamientos de datos correspondientes al adjudicatario.
- c) Publicación de los datos de los adjudicatarios a través de los medios que el Responsable considere oportunos.

- Plazos de conservación: Durante la vigencia de la relación y hasta la finalización de cualesquiera plazos derivados del cumplimiento de obligaciones legales inclusive de cualesquiera plazos de prescripción de la responsabilidad que pudiera afectar al Responsable.

- Comunicaciones y/o transferencias: Las cesiones de datos previstas son las que vienen determinadas por la Ley Foral 5/2018 de 17 de mayo de Transparencia, Acceso a la Información Pública y Buen Gobierno y Ley Foral 2/2018 de 13 de abril de Contratos Públicos.

- Derechos del titular de los datos: Respecto a los datos de carácter personal recogidos para su tratamiento tiene la posibilidad de ejercitar los derechos de acceso, rectificación, supresión y portabilidad. Asimismo, en determinadas circunstancias tendrá derecho a solicitar la limitación u oposición del tratamiento de sus datos en cuyo caso el Responsable cesará en su tratamiento y únicamente conservará los mismos en el caso de que exista alguna obligación normativa que así se lo imponga o hasta la prescripción de las acciones que pudieran concurrir. Todo ello podrá hacerlo dirigiéndose al Responsable, en donde les serán facilitados los modelos para el ejercicio y a través de la dirección del delegado de protección de datos dpd@itracasa.es. Del mismo modo puede dirigirse también ante la autoridad de control que considere oportuno para interponer su reclamación (por ejemplo, en el país donde tenga su residencia habitual, lugar de trabajo o en el

que considere que se ha producido la supuesta infracción). Asimismo, en cualquier momento las reclamaciones podrán dirigirse indistintamente al Responsable o la Agencia Española de Protección de datos a través de los formularios que ésta entidad tiene habilitados al efecto y que son accesibles a través de su página web, <https://sedeagpd.gob.es>.

3.- Acceso a datos personales por parte del adjudicatario.

Los tratamientos de datos que llevará a cabo el adjudicatario serán los necesarios para el cumplimiento del servicio: recepción de los datos personales, registro en los sistemas de información propios del adjudicatario, alojamiento, copias, y comunicación en casos necesarios. Podrán llevarse a cabo otros tratamientos no descritos anteriormente siempre que fueran necesarios para la consecución del servicio.

El tipo de datos que se tratarán de los interesados son: Datos identificativos y datos de características personales. En caso de que como consecuencia de la ejecución del contrato resultara necesario en algún momento el tratamiento de nuevos datos personales u operaciones de tratamiento, el adjudicatario lo requerirá razonadamente y señalará los cambios que solicita al Responsable, quien podrá decidir si lo admite o no y en qué condiciones deba llevarse a la práctica.

4.- Estipulaciones como encargado del tratamiento

De conformidad con lo previsto en el artículo 28 del RGPD, el adjudicatario se obliga y garantiza el cumplimiento de las siguientes obligaciones en su condición de Encargado de Tratamiento:

- I. Tratar los Datos Personales conforme a las instrucciones documentadas en el presente Contrato o demás documentos contractuales aplicables a la ejecución del contrato y aquellas que, en su caso, reciba del Responsable por escrito en cada momento.
- II. Utilizar los datos personales objeto de tratamiento, o los que recoja para su inclusión, sólo para la finalidad objeto del encargo. En ningún caso podrá utilizar los datos para fines propios.
- III. Tratar los datos de acuerdo con las instrucciones del responsable del tratamiento. Si la persona encargada 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, la persona encargada del tratamiento informará inmediatamente a la persona responsable del contrato.
- IV. Mantener el deber de secreto respecto a los datos de carácter personal a los que haya tenido acceso en virtud del encargo, incluso después de que finalice su objeto.
- V. Llevar un listado de personas autorizadas para tratar los Datos Personales objeto de este contrato y garantizar que las mismas se comprometen, de forma expresa y por escrito, a respetar la confidencialidad, y a cumplir con las medidas de seguridad correspondientes, de las que les debe informar convenientemente. Y mantener a disposición del Responsable dicha documentación acreditativa.
- VI. Llevar, por escrito, un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable.
- VII. Mantener la más absoluta confidencialidad sobre los Datos Personales a los que tenga acceso para la ejecución del contrato, así como sobre los que resulten de su tratamiento, cualquiera que sea el soporte en el que se hubieren obtenido. Esta obligación se extiende a toda persona que pudiera intervenir en cualquier fase del tratamiento por cuenta del adjudicatario, siendo deber del adjudicatario instruir a las personas que de él dependan, de este deber de secreto, y del mantenimiento de dicho deber aún después de la terminación de la prestación del Servicio o de su desvinculación.
- VIII. No comunicar los datos a terceras personas, salvo que cuente con la autorización expresa del responsable del tratamiento, en los supuestos legalmente admisibles. En este caso, el responsable identificara, 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.

- IX. Salvo que se indique otra cosa por escrito por el Responsable, a tratar los Datos Personales dentro del Espacio Económico Europeo u otro espacio considerado por la normativa aplicable como de seguridad equivalente, no tratándolos fuera de este espacio ni directamente ni a través de cualesquiera subcontratistas autorizados conforme a lo establecido en este Contrato o 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 por causa de Derecho nacional o de la Unión Europea el adjudicatario se vea obligado a llevar a cabo alguna transferencia internacional de datos, el adjudicatario informará por escrito al Responsable de esa exigencia legal, con antelación suficiente a efectuar el tratamiento, y garantizará el cumplimiento de cualesquiera requisitos legales que sean aplicables al Responsable, salvo que el Derecho aplicable lo prohíba por razones importantes de interés público.
- X. No subcontratar ninguna de las prestaciones que formen parte del objeto de este contrato que comporten tratamiento de datos personales, salvo los servicios auxiliares necesarios para el normal funcionamiento de los servicios del encargado.
- XI. Si fuera necesario subcontratar algún tratamiento, este hecho se deberá comunicar previamente y por escrito a la persona responsable del contrato, indicando los tratamientos que se pretende subcontratar e identificando de forma clara e inequívoca la empresa subcontratada y sus datos de contacto. La subcontratación podrá llevarse a cabo si el responsable no manifiesta su oposición en el plazo de un mes.
- XII. La empresa subcontratada, que también tendrá la condición de encargado del tratamiento, está obligada igualmente a cumplir las obligaciones establecidas en este contrato para el encargado del tratamiento y las instrucciones que dicte la persona responsable del contrato.
- XIII. Garantizar la formación necesaria en materia de protección de datos personales de las personas autorizadas para tratar datos personales.
- XIV. Asistir a la persona encargada del tratamiento en la respuesta al ejercicio de los derechos de las personas interesadas.
- XV. Tratar los Datos Personales de conformidad con los criterios de seguridad y el contenido previsto en el artículo 32 del RGPD, así como observar y adoptar las medidas técnicas y organizativas de seguridad necesarias o convenientes para asegurar la confidencialidad, secreto e integridad de los Datos Personales a los que tenga acceso.
- XVI. Colaborar con el Responsable en el cumplimiento de sus obligaciones en materia de (i) medidas de seguridad, (ii) comunicación y/o notificación de brechas (logradas e intentadas) de medidas de seguridad a las autoridades competentes o los interesados, y (iii) colaborar en la realización de evaluaciones de impacto relativas a la protección de datos personales y consultas previas al respecto a las autoridades competentes; teniendo en cuenta la naturaleza del tratamiento y la información de la que disponga. Asimismo, pondrá a disposición del Responsable, a requerimiento de éste, toda la información necesaria para demostrar el cumplimiento de las obligaciones previstas en este Contrato y demás documentos contractuales y colaborará en la realización de auditorías e inspecciones llevadas a cabo, en su caso, por el Responsable
- XVII. Dar apoyo a la persona responsable del tratamiento en la realización de las consultas previstas a la autoridad de control, cuando proceda.
- XVIII. Disponer de evidencias que demuestren su cumplimiento de la normativa de protección de Datos Personales y del deber de responsabilidad activa, como, a título de ejemplo, certificados previos sobre el grado de cumplimiento o resultados de auditorías, que habrá de poner a disposición del Responsable a requerimiento de éste. Asimismo, durante la vigencia del contrato, pondrá a disposición del Responsable toda información, certificaciones y auditorías realizadas en cada momento.
- XIX. Nombrar Delegado de Protección de Datos, en caso de que sea necesario según el RGPD, y comunicarlo al Responsable, también cuando la designación sea voluntaria, así como la identidad y datos de contacto de la(s) persona(s) física(s) designada(s) por

el adjudicatario como sus representante(s) a efectos de protección de los Datos Personales (representantes del Encargado de Tratamiento), responsable(s) del cumplimiento de la regulación del tratamiento de Datos Personales, en las vertientes legales/formales y en las de seguridad.

- XX. Garantizar que la persona con el cargo de Delegado de Protección de Datos o en su defecto de Responsable de Privacidad participe de forma adecuada en el tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
- XXI. Cuando una persona ejerza un derecho (de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de datos y a no ser objeto de decisiones individualizadas automatizadas, u otros reconocidos por la normativa aplicable (conjuntamente, los "Derechos"), ante el Encargado del Tratamiento, éste debe comunicarlo al Responsable con la mayor prontitud. La comunicación debe hacerse de forma inmediata y en ningún caso más allá del tercer día laborable siguiente al de la recepción del ejercicio de derecho, juntamente, en su caso, con la documentación y otras informaciones que puedan ser relevantes para resolver la solicitud que obre en su poder, e incluyendo la identificación fehaciente de quien ejerce el derecho. Asistirá al Responsable, siempre que sea posible, para que ésta pueda cumplir y dar respuesta a los ejercicios de Derechos.
- XXII. De conformidad con el artículo 33 RGPD, comunicar al Responsable, de forma inmediata y a más tardar en el plazo de 72 horas, cualquier violación de la seguridad de los datos personales a su cargo de la que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia o cualquier fallo en su sistema de tratamiento y gestión de la información que haya tenido o pueda tener que ponga en peligro la seguridad de los Datos Personales, su integridad o su disponibilidad, así como cualquier posible vulneración de la confidencialidad como consecuencia de la puesta en conocimiento de terceros de los datos e informaciones obtenidos durante la ejecución del contrato. Comunicará con diligencia información detallada al respecto, incluso concretando qué interesados sufrieron una pérdida de confidencialidad.
- XXIII. Una vez finalizada la prestación contractual objeto del presente Contrato, debe devolver a la persona responsable o devolver a otra persona encargada que aquella designe, los datos personales objeto del tratamiento, sin conservar copia alguna; salvo que se permita o requiera por ley o por norma de derecho comunitario su conservación, en cuyo caso no procederá la destrucción. El Encargado del Tratamiento podrá, no obstante, conservar los datos durante el tiempo que puedan derivar responsabilidades de su relación con el Responsable del Tratamiento. En este último caso, los Datos Personales se conservarán bloqueados y por el tiempo mínimo, destruyéndose de forma segura y definitiva al final de dicho plazo.

La presente cláusula y las obligaciones en ella establecidas, constituyen el contrato de encargo de tratamiento entre el Responsable y el adjudicatario a que hace referencia el artículo 28.3 RGPD. Las obligaciones y prestaciones que aquí se contienen no son retribuibiles de forma distinta de lo previsto en el presente contrato y demás documentos contractuales y tendrán la misma duración que la prestación de Servicio objeto de este contrato y su contrato, prorrogándose en su caso por períodos iguales a éste. No obstante, a la finalización del contrato, el deber de secreto continuará vigente, sin límite de tiempo, para todas las personas involucradas en la ejecución del contrato.

Para el cumplimiento del objeto de este contrato no se requiere que el adjudicatario acceda a ningún otro Dato Personal responsabilidad del Responsable, y por tanto no está autorizado en caso alguno al acceso o tratamiento de otro dato, que no sean los necesarios para la prestación del servicio. Si se produjera una incidencia durante la ejecución del contrato que conllevará un acceso accidental o incidental a Datos Personales responsabilidad del Responsable el adjudicatario deberá ponerlo en su conocimiento, en concreto de su Delegado de Protección de Datos, con la mayor diligencia y a más tardar en el plazo de 72 horas.

OCTAVA. REQUERIMIENTOS DE CARÁCTER SOCIAL, MEDIO AMBIENTAL, IGUALDAD DE GÉNERO

El contrato se halla sujeto al cumplimiento de las disposiciones legales, reglamentarias y convencionales vigentes en materia de fiscalidad, de Seguridad Social, protección del medio ambiente, protección del empleo, igualdad de género, de acoso por razón de sexo o acoso sexual, condiciones de trabajo, prevención de riesgos laborales y demás disposiciones en materia laboral. **ITRACASA** podrá solicitar al contratista, en cualquier momento, la entrega de informes, documentos, ficheros o cualquier otro ítem que permita verificar el cumplimiento de esta normativa.

NOVENA. SEGURIDAD DE LA INFORMACIÓN

Normativa de seguridad de la información

El adjudicatario está obligado al cumplimiento de la normativa de seguridad de la información a la que **ITRACASA** pueda estar obligada a dar cumplimiento, así como a su propia normativa interna de seguridad de la información. En consecuencia, el adjudicatario se compromete y obliga a dar cumplimiento a la política de seguridad de **ITRACASA**, así como la distinta normativa de seguridad desarrollada a instancias de dicha política.

El adjudicatario deberá concienciar, formar y entrenar regularmente a su personal acerca de su papel y responsabilidad para que la seguridad del sistema y de los servicios prestados alcance los niveles exigidos, enfocando la labor hacia las materias que requieran para el desempeño de sus funciones referidas al servicio prestado, y especialmente en las normas de seguridad de la información antes referidas.

Conformidad con el Esquema Nacional de Seguridad (ENS)

De conformidad con lo señalado en el artículo 2 del vigente Real Decreto 311/2022, de 3 de mayo, y en la Resolución de 13 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Instrucción Técnica de Seguridad de conformidad con el Esquema Nacional de Seguridad, de desarrollo del Real Decreto 311/2022 (ENS), cuando los operadores del sector privado presten servicios o provean soluciones a las entidades públicas, a los que resulte exigible el cumplimiento del Esquema Nacional de Seguridad, deberán estar en condiciones de exhibir la correspondiente Declaración de la Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categoría BÁSICA, o la Certificación de Conformidad con el Esquema Nacional de Seguridad, cuando se trate de sistemas de categorías MEDIA o ALTA, y opcionalmente los de BÁSICA, utilizando los mismos procedimientos que los exigidos en dicha Instrucción Técnica de Seguridad para las entidades públicas. La declaración o certificado de conformidad de la empresa adjudicataria debe incluir en su alcance actividad o actividades relacionadas con el objeto del contrato.

Tracasa Instrumental podrá solicitar a la entidad adjudicataria, al inicio de la prestación de los servicios, una Declaración Responsable del cumplimiento de las medidas de seguridad recogidas en la presente contratación y referidas al servicio o producto objeto del contrato.

En el supuesto de que el adjudicatario no pudiera mantener la conformidad con el ENS durante la vigencia del contrato -por pérdida, retirada, suspensión de la Certificación de Conformidad o imposibilidad de mantener la Declaración de Conformidad o por carecer de la misma-, deberá comunicar esta circunstancia, de forma inmediata y sin dilación indebida, a **ITRACASA**, quien considerará el impacto de dicha circunstancia en la prestación objeto del contrato.

En caso de carecer de la Certificación, **ITRACASA** podrá solicitar a la empresa adjudicataria el cumplimiento de lo establecido en el capítulo segundo y tercero del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad, referido a sus principios básicos y política de seguridad y requisitos mínimos de seguridad.

Por último, y como así se refleja en la Instrucción Técnica de Seguridad de Conformidad con el Esquema Nacional de Seguridad, el Informe de Autoevaluación o de Auditoría y sus resultados deben estar en cualquier momento a disposición de los responsables de ITRACASA con competencias en seguridad, al objeto de verificar la adecuación o idoneidad del cumplimiento del ENS, así como cualquier otra información relativa al cumplimiento de los requisitos en materia de seguridad de la información.

Auditoría de la seguridad y trazabilidad de los servicios

El adjudicatario adquirirá el compromiso de ser auditado por personal autorizado por **ITRACASA**, o por aquellos técnicos en los que **ITRACASA** delegue, en cualquier momento en el desarrollo de los trabajos y en el periodo de garantía, con el fin de verificar la seguridad implementada, comprobando que se cumplen las recomendaciones de protección y las medidas de seguridad de la distinta normativa, en función de las condiciones de aplicación en cada caso.

Asimismo, y en el marco de la ejecución de los trabajos, y con el fin de garantizar la seguridad de la información manejada, **ITRACASA** se reserva la capacidad de monitorizar la actividad de los sistemas, por lo que se informará a la empresa contratista de este aspecto. Será responsabilidad de la empresa contratista gestionar este requisito con sus usuarios.

Incidentes de seguridad

El adjudicatario se compromete a implantar un procedimiento de notificación y gestión de Incidentes de Seguridad que cumpla con lo requerido por el RGPD y el ENS a través de las instrucciones publicadas por el CCN, que divulgará entre su personal, y actuará con especial diligencia en aquellos casos en los que se vean involucrada la seguridad de la información y datos personales de **ITRACASA** o cuando se puedan ver afectadas la reputación o responsabilidad de **ITRACASA** o los intereses de las personas cuya información es tratada

DÉCIMA. PREVENCIÓN DE LA CORRUPCIÓN. El adjudicatario debe ser consciente, conocer y comprender los términos de las normas contra la corrupción, por lo que se abstendrá de cualquier actividad que constituya una violación de las disposiciones de dichas normas de lucha contra la corrupción.

El adjudicatario no realizará u ofrecerá, ya sea de forma directa o través de persona interpuesta, cualquier beneficio o ventaja no justificados de cualquier naturaleza, para sí o para un tercero,

como contraprestación para favorecer indebidamente a otro en la adquisición o venta de mercancías o en la contratación de relaciones mercantiles.

Igualmente, no realizará ofrecimiento, ventaja o promesa, ya sea directamente o a través de persona interpuesta, de ningún tipo, a miembros de la Administración Pública dentro del marco de la relación comercial del presente contrato.

En el supuesto de que, en cualquier momento de la relación de prestación de servicios, **ITRACASA** tuviera la sospecha de que el adjudicatario (o cualquiera de las personas relacionadas con él) ha vulnerado o se detecta el riesgo de incumplimiento de las obligaciones en materia de prevención de la corrupción, **ITRACASA** notificará por escrito al adjudicatario la suspensión de la relación de prestación de servicios por período de un mes, durante el cual el adjudicatario facilitará a **ITRACASA** toda aquella información y documentación que **ITRACASA** pudiera requerir a efectos de determinación y esclarecimiento de las circunstancias que han motivado la sospecha. **ITRACASA** podrá extender el período de suspensión durante un mes adicional si lo considerase necesario para evaluar adecuadamente la información y documentación entregada.

UNDÉCIMA. DOCUMENTACIÓN DEL CONTRATO. Son documentos que forman parte del contrato: la oferta presentada para esta contratación por **SUMMAR**, y la política de seguridad que se anexan al presente contrato, siempre que estos documentos no estén en contradicción con el presente contrato.

En caso de discrepancia entre el contenido de los documentos relacionados en el párrafo anterior, tendrá preferencia el presente contrato.

DUODÉCIMA. FUERO JUDICIAL. Las partes, con expresa renuncia al fuero judicial correspondiente, se someten a los juzgados y tribunales de Pamplona para el conocimiento y resolución de cuantas diferencias surjan en la ejecución del presente contrato.

Y en prueba de conformidad, para su constancia, cumplimiento y efectos, se firma el presente contrato a fecha de la última firma digital.

Por **ITRACASA**

D. Daniel Goñi Merino

Por **SUMMAR**

D. Carlos Moles Abelló

TRACASA INSTRUMENTAL, S.L.U**Att. Sra. Idoia Areopagita****Referencia: 0827 Propuesta Renovación del mantenimiento anual de Labor y Mentor**

27 de agosto de 2024

Distinguido Cliente,

Estando próximo el vencimiento del servicio de mantenimiento anual de Labor y Mentor, a continuación, le detallamos el importe de renovación:

Licencia: 5400494	Vencimiento: 01/09/2024	Importe, €
Renovación Mantenimiento Anual Labor y Mentor. Periodo del 1/9/24 al 31/8/25		10.976

El Mantenimiento anual como ya les hemos indicado con anterioridad es obligatorio, ya que al ser aplicaciones sometidas a cambios legales, si no se aplicaran las actualizaciones la funcionalidad quedaría obsoleta.

Condiciones

- ☐ El Mantenimiento anual, se facturará anticipadamente.
- ☐ La forma de pago es la acordada previamente.
- ☐ Todos los importes son en euros, IVA excluido.

Para proceder a la contratación de los conceptos ofertados, les rogamos nos remitan al email administracion@summar.es esta hoja debidamente cumplimentada.

Referencia: 0827 Oferta Renovación del mantenimiento anual de Labor y Mentor**Conforme, Cliente:**

33435846X
DANIEL GOÑI
(R: B71280689)

Firmado digitalmente
por 33435846X DANIEL
GOÑI (R: B71280689)
Fecha: 2024.08.27
14:06:25 +02'00'

Nombre: _____

Cargo: _____

Fecha: _____

Firma, sello y fecha

Fecha
05.06.2024

Política de Seguridad de la Información



Índice

1	Aprobación y entrada en vigor	2
2	Principios rectores	2
	2.1 Prevención	3
	2.2 Detección	3
	2.3 Respuesta	3
	2.4 Recuperación	3
3	Alcance	3
4	Misión de Tracasa Instrumental	4
5	Marco normativo	4
6	Procedimientos de Seguridad	5
	6.1 Alta Dirección	6
	6.2 Comité de Seguridad de la Información (CSI)	6
	6.3 Roles: funciones y responsabilidades	7
	6.4 Responsable de Seguridad	10
	6.5 Procedimiento de designación	11
	6.6 Resumen de funciones de cada rol	11
	6.7 Nombramientos y jerarquía	13
	6.8 Especificidades	13
	6.9 Resolución de conflictos	13
7	Profesionalidad	14
8	Autorización y control de accesos	14
9	Protección de las instalaciones	14
10	Adquisición de productos de seguridad y contratación de servicios de seguridad	14
11	Mínimo privilegio	15
12	Integridad y actualización del sistema	15
13	Protección de la información almacenada y en tránsito	15
14	Prevención ante otros sistemas de información interconectados	16
15	Registro de la actividad y detección de código dañino	16
16	Mejora continua del proceso de seguridad	16
17	Gestión de riesgos	17
18	Datos de carácter personal	17
19	Desarrollo de la política de seguridad de la información	17
	19.1 Ciclo de vida de la Política	18
20	Obligaciones del personal	18
21	Terceras partes	18

1 Aprobación y entrada en vigor

Texto aprobado el día 5 de junio de 2024 por la Dirección de la empresa.

Esta Política de Seguridad de la Información es efectiva desde dicha fecha y hasta que sea reemplazada por una nueva Política.

Este texto anula el anterior, que fue aprobado el día 9 de noviembre de 2023 por la Dirección de la empresa.

Par la elaboración de esta Política, así como las futuras modificaciones que pueda experimentar, se ha seguido la documentación relativa al ENS y en especial la [GUÍA DE SEGURIDAD \(CCN-STIC-805\) ESQUEMA NACIONAL DE SEGURIDAD: POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN](#).

2 Principios rectores

Tracasa Instrumental enfoca la seguridad de la información como un proceso integral constituido por todos los elementos humanos, materiales, técnicos, jurídicos y organizativos relacionados con el sistema de información. La aplicación de la seguridad está presidida por este principio, que excluye en consecuencia cualquier actuación puntual o tratamiento coyuntural.

Tracasa Instrumental dispone de un Sistema de Gestión de la Seguridad de la Información (SGSI) para alcanzar sus objetivos, certificado bajo el estándar internacional ISO 27000.

Este SGSI debe ser administrado con diligencia, tomando las medidas adecuadas para proteger a las empresas frente a daños accidentales o deliberados que puedan afectar a la disponibilidad, integridad o confidencialidad de la información tratada o los servicios prestados.

El objetivo de la seguridad de la información es garantizar la calidad de la información y la prestación continuada de los servicios actuando preventivamente, supervisando la actividad diaria y reaccionando con presteza a los incidentes.

Los sistemas TIC deben estar protegidos contra amenazas de rápida evolución con potencial para incidir en la confidencialidad, integridad, disponibilidad, uso previsto y valor de la información y los servicios. Para defenderse de estas amenazas, se requiere una estrategia que se adapte a los cambios en las condiciones del entorno para garantizar la prestación continua de los servicios. Esto implica que la empresa debe aplicar las medidas mínimas de seguridad exigidas por el Esquema Nacional de Seguridad y el estándar ISO 27000, así como realizar un seguimiento continuo de los niveles de prestación de servicios, seguir y analizar las vulnerabilidades reportadas, y preparar una respuesta efectiva a los incidentes para garantizar la continuidad de los servicios prestados.

La empresa debe cerciorarse de que la seguridad TIC es una parte integral de cada etapa del ciclo de vida del sistema, desde su concepción hasta su retirada de servicio, pasando por las decisiones de desarrollo o adquisición y las actividades de explotación. Los requisitos de seguridad y las necesidades de financiación deben ser identificados e incluidos en la planificación, en la solicitud de ofertas, y en pliegos de licitación para proyectos de TIC.

La empresa debe estar preparada para prevenir, detectar, reaccionar y recuperarse de incidentes, de acuerdo al Artículo 7 del ENS.

2.1 Prevención

Tracasa Instrumental debe evitar, o al menos prevenir en la medida de lo posible, que la información o los servicios se vean perjudicados por incidentes de seguridad. Para ello, la empresa implementará las medidas mínimas de seguridad determinadas por el ENS, así como cualquier control adicional identificado a través de una evaluación de amenazas y riesgos. Estos controles, y los roles y responsabilidades de seguridad de todo el personal, deben estar claramente definidos y documentados.

Para garantizar el cumplimiento de la política, la empresa debe:

- Autorizar los sistemas antes de entrar en operación.
- Evaluar regularmente la seguridad, incluyendo evaluaciones de los cambios de configuración realizados de forma rutinaria.
- Solicitar la revisión periódica por parte de terceros con el fin de obtener una evaluación independiente.

2.2 Detección

Dado que los servicios se pueden degradar rápidamente debido a incidentes, que van desde una simple desaceleración hasta su detención, los servicios deben monitorizar la operación de manera continua para detectar anomalías en los niveles de prestación de los servicios y actuar en consecuencia según lo establecido en el Artículo 9 del ENS.

La monitorización es especialmente relevante cuando se establecen líneas de defensa de acuerdo con el Artículo 8 del ENS. Se establecerán mecanismos de detección, análisis y reporte que lleguen a los responsables regularmente y cuando se produce una desviación significativa de los parámetros que se hayan preestablecido como normales.

2.3 Respuesta

Tracasa Instrumental se compromete a:

- Establecer mecanismos para responder eficazmente a los incidentes de seguridad.
- Designar punto de contacto para las comunicaciones con respecto a incidentes detectados en otros organismos con los que guarde relación.
- Establecer protocolos para el intercambio de información relacionada con el incidente. Esto incluye comunicaciones, en ambos sentidos, con los Equipos de Respuesta a Emergencias (CERT).

2.4 Recuperación

Para garantizar la disponibilidad de los servicios críticos, la empresa debe desarrollar y mantener planes de continuidad de los sistemas TIC como parte de su plan general de continuidad de negocio y actividades de recuperación.

3 Alcance

Esta política se aplica a Tracasa Instrumental y a todos los miembros de la organización, sin excepciones.

4 Misión de Tracasa Instrumental

Desarrollar conocimiento, personas y servicios innovadores, en colaboración con las administraciones públicas y con empresas privadas.

5 Marco normativo

El listado de las principales leyes, reglamentos y otra normativa a la que Tracasa Instrumental está sujeta es:

1. Empresa:

- Real Decreto Legislativo 1/2010, de 2 julio por el que se Aprueba el texto refundido de la ley de Sociedades de Capital.
- Ley Foral 13/2007, de 4 de Abril, de la Hacienda Pública de Navarra.
- Ley Foral 14/2007, de 4 de abril, del Patrimonio de Navarra
- Ley Foral 11/2019, de 11 de marzo, de la Administración de la Comunidad Foral de Navarra y del Sector Público institucional foral
- Ley Foral 2/2018 de Contratos Públicos de Navarra
- Ley 15/2007, de 3 de julio, de Defensa de la Competencia.
- Ley 38/2003, de 17 de noviembre, General de Subvenciones
- Ley Foral 11/2002 de 9 de Noviembre de Subvenciones
- Convenio Colectivo del Sector Oficinas y Despachos de Navarra
- Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores)

2. Seguridad de la Información:

- Artículo 18 de la Constitución Española
- Ley Foral 5/2018, de 17 de mayo, de Transparencia, acceso a la información pública y buen gobierno.
- Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno.
- 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)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando, aclarando y armonizando las disposiciones legales vigentes sobre la materia.
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico
- Ley 10/2021, de 9 de julio, de trabajo a distancia
- Ley 9/2014, de 9 de mayo, General de Telecomunicaciones.

- Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE
- Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.
- Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
- Instrucción 1/2021, de 2 de noviembre, de la Agencia Española de Protección de Datos, por la que se establecen directrices respecto de la función consultiva de la Agencia, de conformidad con 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 la libre circulación de esos datos, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y el Estatuto de la Agencia Española de Protección de Datos, aprobado por el Real Decreto 389/2021, de 1 de junio. Ley 1/2019, de 20 de febrero, de Secretos Empresariales.
- Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Ley 2/2023, de 20 de febrero, reguladora de la protección de las personas que informen sobre infracciones normativas y de lucha contra la corrupción.
- Instrucciones Técnicas de Seguridad (ITS) publicadas por el CCN.

3. Normativa por la ejecución de fondos MRR:

- Reglamento (UE) 2021/241 del Parlamento Europeo y del Consejo de 12 de febrero de 2021 por el que se establece el Mecanismo de Recuperación y Resiliencia.
- Orden HFP/1030/2021, de 29 de septiembre, por la que se configura el sistema de gestión del Plan de Recuperación, Transformación y Resiliencia
- Orden HFP/1031/2021, de 29 de septiembre, por la que se establece el procedimiento y formato de la información a proporcionar por las Entidades del Sector Público Estatal, Autonómico y Local para el seguimiento del cumplimiento de hitos y objetivos y de ejecución presupuestaria y contable de las medidas de los componentes del Plan de Recuperación, Transformación y Resiliencia.)
- Resolución 1/2022, de 12 de abril, de la Secretaría General de Fondos Europeos, por la que se establecen instrucciones a fin de clarificar la condición de entidad ejecutora, la designación de órganos responsables de medidas y órganos gestores de proyectos y subproyectos, en el marco del sistema de gestión del Plan de Recuperación, Transformación y Resiliencia.
- Orden HFP/55/2023, de 24 de enero, relativa al análisis sistemático del riesgo de conflicto de interés en los procedimientos que ejecutan el Plan de Recuperación, Transformación y Resiliencia.

6 Procedimientos de Seguridad

Dado que la Política de Seguridad está escrita a un nivel muy amplio, se requiere complementarla con documentos más precisos que ayuden a llevar a cabo lo propuesto y que forman parte del SGSI de Tracasa Instrumental, principalmente:

- normas de seguridad: uniformizan el uso de aspectos concretos del sistema. Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio.

- guías de seguridad: carácter formativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos donde no existen procedimientos precisos
- procedimientos de seguridad: afrontan tareas concretas, indicando lo que hay que hacer, paso a paso. Son útiles en tareas repetitivas.

6.1 Alta Dirección

- La Alta Dirección es responsable de que Tracasa Instrumental alcance sus objetivos a corto, medio y largo plazo.
- Debe respaldar explícita y notoriamente las actividades del SGSI en la organización.
- Expresa sus inquietudes al CSI a través del Responsable de Seguridad de Información (RSI).
- Aprueba la Política de Seguridad de Tracasa Instrumental.
- Decide sobre la aprobación de presupuestos presentados por el CSI.

6.2 Comité de Seguridad de la Información (CSI)

El CSI de Tracasa Instrumental tiene las siguientes funciones y responsabilidades:

- Coordinar todas las funciones de seguridad de la empresa
- Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial.
- Velar por el alineamiento de las actividades de seguridad y los objetivos de la Organización.
- Responsabilizarse de la elaboración de la Política de Seguridad de la Información, que será aprobada por la Alta Dirección.
- Aprobar las políticas de seguridad de las diferentes áreas.
- Coordinar y aprobar las propuestas recibidas de proyectos de los diferentes ámbitos de seguridad.
- Escuchar las inquietudes de la Alta Dirección y transmitirlos a los responsables de la empresa que tengan competencias en el ámbito de la seguridad. De estos últimos podrá recabar respuestas y soluciones que, una vez coordinadas, son notificadas a la Alta Dirección.
- Recabar del Responsable de Seguridad de la Información (CSO de acuerdo a la denominación del ENS) informes regulares del estado de seguridad de la organización y de los posibles incidentes.
- Coordinar y dar respuesta a las inquietudes transmitidas a través del CSO.
- Definir, dentro de la Política de Seguridad de la Información, la asignación de roles y los criterios para alcanzar las garantías que estime pertinentes en lo relativo a segregación de tareas.

El CSI de Tracasa Instrumental está formado por los siguientes roles:

- Gerencia
- Responsable de la Información / Responsable del Servicio
- Responsable de Seguridad de la Información
- Responsable de Sistemas
- Dirección de Servicios Corporativos
- Responsable de Jurídico, Protección de Datos, Compliance y Seguridad física
- Responsable de Personas y Talento

El Secretario del CSI será el Responsable de Seguridad de la Información y tendrá las siguientes funciones en el ámbito del CSI:

- Convocar al CSI, recopilando la información pertinente.
- Recabar las inquietudes de la Dirección de la entidad y de las distintas áreas, incorporándolas al Orden del Día del CSI, para su examen y acciones pertinentes.
- Estar al tanto de cambios regulatorios o normativos (leyes, reglamentos o prácticas sectoriales) que afecten a la entidad, debiendo informarse de las consecuencias para las actividades de la organización, alertando al CSI y proponiendo las medidas oportunas de adecuación al nuevo marco.
- Responsable de la toma de decisiones cotidianas entre dos reuniones del CSI. Estas decisiones darán respuesta a propuestas de las áreas, velando por la unidad de acción y la coordinación de actuaciones, especialmente en caso de incidencias que tengan repercusión fuera de la organización y en caso de desastres.

6.3 Roles: funciones y responsabilidades

Se concretan en este apartado las funciones y responsabilidades de los siguientes roles, tal y como establece el Esquema Nacional de Seguridad y habiéndose aplicado [guía CCN-STIC 801](#) como modelo:

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
Responsable de la Información	ENS, art. 10	Determina los requisitos (de seguridad) de la información tratada, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de la información constituye asimismo una actividad indelegable. El ENS define “sistema de información” como: “Conjunto organizado de recursos para que la información se pueda recoger, almacenar, procesar o tratar, mantener, usar, compartir, distribuir, poner a disposición, presentar o transmitir”. (Anexo IV. Glosario).
Responsable del servicio	ENS, art. 10	Determina los requisitos (de seguridad) de los servicios prestados, según los parámetros del Anexo I del ENS. Puede tratarse de una persona física singular o un órgano colegiado, formando parte de lo que se suele denominar Comité de Seguridad de la Información. Como la seguridad constituye un principio de actuación propio de las entidades públicas, la aprobación de los niveles de seguridad de los servicios constituye asimismo una actividad indelegable.
	ENS, art. 39	Debe incluir las especificaciones de seguridad en el ciclo de vida de los servicios y sistemas, acompañadas de los correspondientes procedimientos de control.
	ENS, art. 43	Valorará las consecuencias de un impacto negativo sobre la seguridad de los servicios se efectuará atendiendo a su repercusión en la capacidad de la organización para el logro de sus objetivos, la protección de sus activos, el cumplimiento de sus obligaciones de servicio, el respeto de la legalidad y los derechos de los ciudadanos.

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
Responsable de la Seguridad	ENS, art. 10	Determina las decisiones de seguridad pertinentes para satisfacer los requisitos establecidos por los responsables de la información y de los servicios. Deberá ser una persona física, jerárquicamente independiente del Responsable del Sistema. Nota: En caso de servicios externalizados, la responsabilidad última la tiene siempre la entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio).
	ENS, art. 15.3	Las Administraciones públicas exigirán, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.
	ENS, art. 18	En la adquisición de productos de seguridad de las tecnologías de la información y comunicaciones se utilizarán, de forma proporcionada a la categoría del sistema y nivel de seguridad determinados, aquellos que tengan certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, salvo en aquellos casos en que las exigencias de proporcionalidad en cuanto a los riesgos asumidos no lo justifiquen a juicio del Responsable de la Seguridad.
	ENS, arts. 27.3, 27.4 y 27.5	Las medidas del Anexo II del ENS, así como aquellas otras necesarias para garantizar el adecuado tratamiento de datos personales podrán ser ampliadas por causa de la concurrencia indicada o del prudente arbitrio del Responsable de la Seguridad del sistema, habida cuenta del estado de la tecnología, la naturaleza de los servicios prestados y la información manejada, y los riesgos a que están expuestos. La relación de medidas seleccionadas del Anexo II se formalizará en un documento denominado Declaración de Aplicabilidad, firmado por el Responsable de la Seguridad. Las medidas de seguridad referenciadas en el Anexo II podrán ser reemplazadas por otras compensatorias siempre y cuando se justifique documentalmente que protegen igual o mejor el riesgo sobre los activos (Anexo I) y se satisfacen los principios básicos y los requisitos mínimos previstos en los capítulos II y III del real decreto. Como parte integral de la Declaración de Aplicabilidad se indicará de forma detallada la correspondencia entre las medidas compensatorias implantadas y las medidas del Anexo II que compensan y el conjunto será objeto de la aprobación formal por parte del responsable de la seguridad.

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
	ENS, art. 28	La utilización de infraestructuras y servicios comunes reconocidos en las Administraciones Públicas facilitará el cumplimiento de los principios básicos y los requisitos mínimos exigidos en el ENS en condiciones de mejor eficiencia. Los supuestos concretos de utilización de estas infraestructuras y servicios comunes serán determinados por cada Administración.
	ENS, art. 34.6 y Anexo III	Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas.
Responsable del Sistema	ENS	Se encarga de la operación del sistema de información, atendiendo a las medidas de seguridad determinadas por el Responsable de la Seguridad.
	La derivada de la aplicación de la Ley 40/2015	Su responsabilidad puede estar situada dentro de la organización (utilización de sistemas propios) o estar compartimentada entre una responsabilidad mediata (de la propia organización) y una responsabilidad inmediata (de terceros, públicos o privados), cuando los sistemas de información se encuentran externalizados.
	ENS, art. 34.6 y 34.7	Los informes de autoevaluación y/o los informes de auditoría serán analizados por el Responsable de la Seguridad competente, que elevará las conclusiones al Responsable del Sistema para que adopte las medidas correctoras adecuadas. En el caso de los sistemas de categoría ALTA, visto el dictamen de auditoría, el responsable del sistema podrá acordar la retirada de operación de alguna información, de algún servicio o del sistema en su totalidad, durante el tiempo que estime prudente y hasta la satisfacción de las modificaciones prescritas.
Administrador de la Seguridad del Sistema (ASS)	N/A	La persona designada figurará en la documentación de seguridad del Sistema de información, y sus funciones son las siguientes: La implementación, gestión y mantenimiento de las medidas de seguridad aplicables al Sistema de Información. La gestión, configuración y actualización, en su caso, del hardware y software en los que se basan los mecanismos y servicios de seguridad del Sistema de Información. La gestión de las autorizaciones concedidas a los usuarios del sistema, en particular los privilegios concedidos, incluyendo la monitorización de que la

ROL	IDENTIFICACIÓN LEGAL	DESCRIPCIÓN
		actividad desarrollada en el sistema se ajusta a lo autorizado. La aplicación de los Procedimientos Operativos de Seguridad. Aprobar los cambios en la configuración vigente del Sistema de Información. Asegurar que los controles de seguridad establecidos son cumplidos estrictamente. Asegurar que son aplicados los procedimientos aprobados para manejar el sistema de información. Supervisar las instalaciones de hardware y software, sus modificaciones y mejoras para asegurar que la seguridad no está comprometida y que en todo momento se ajustan a las autorizaciones pertinentes. Monitorizar el estado de seguridad del sistema proporcionado por las herramientas de gestión de eventos de seguridad y mecanismos de auditoría técnica implementados en el sistema. Informar a los Responsables de la Seguridad y del Sistema de cualquier anomalía, compromiso o vulnerabilidad relacionada con la seguridad. Colaborar en la investigación y resolución de incidentes de seguridad, desde su detección hasta su resolución. <pre> graph TD subgraph "supervisión" RS[responsable de la seguridad] end subgraph "operación" RDS[responsable del sistema] end subgraph "ejecución" AS[administrador de seguridad] end RDS --> AS </pre> Ilustración 2 - El ASS depende del Responsable del Sistema

6.4 Responsable de Seguridad

El Responsable de la Seguridad (de la información) es la persona designada por la Dirección de la entidad, según el procedimiento descrito en su Política de Seguridad de la Información.

El ENS señala que el Responsable de la Seguridad determina las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios.

Además de ello, en caso de servicios externalizados, la responsabilidad última la tiene siempre la Entidad del Sector Público destinataria de los servicios, aun cuando la responsabilidad inmediata pueda corresponder (vía contrato, convenio, encomienda, etc.) a la organización prestataria del servicio (lo que sucede, por ejemplo, en la utilización de servicios en la nube).

Las dos funciones esenciales del Responsable de la Seguridad son:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo a lo establecido en la Política de Seguridad de la Información de la organización.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad.

Además de ello, cuando la figura del Responsable de la Seguridad del ENS coincide con la Entidad Responsable de Seguridad de la Información derivada de la Directiva NIS15, como es el caso de Tracasa Instrumental, podrá desplegar las siguientes funciones:

- Elaborar y proponer para aprobación por la organización las políticas de seguridad, que incluirán las medidas técnicas y organizativas, adecuadas y proporcionadas, para gestionar los riesgos que se planteen para la seguridad de las redes y sistemas de información utilizados y para prevenir y reducir al mínimo los efectos de los ciberincidentes que afecten a la organización y los servicios.
- Desarrollar las políticas de seguridad, normativas y procedimientos derivados de la organización, supervisar su efectividad y llevar a cabo auditorías periódicas de seguridad.
- Elaborar el documento de Declaración de Aplicabilidad.
- Actuar como capacitador de buenas prácticas en seguridad de las redes y sistemas de información, tanto en aspectos físicos como lógicos.
- Constituirse como punto de contacto con la autoridad competente en materia de seguridad de las redes y sistemas de información y responsable ante aquella del cumplimiento de las obligaciones que se derivan del RD-I 12/2018 y de su Reglamento de Desarrollo.
- Constituir el punto de contacto especializado para la coordinación con el CSIRT de referencia.
- Notificar a la autoridad competente, a través del CSIRT de referencia y sin dilación indebida, los incidentes que tengan efectos perturbadores en la prestación de los servicios.
- Recibir, interpretar y aplicar las instrucciones y guías emanadas de la Autoridad Competente, tanto para la operativa habitual como para la subsanación de las deficiencias observadas.
- Recopilar, preparar y suministrar información o documentación a la autoridad competente o el CSIRT de referencia, a su solicitud o por propia iniciativa.

6.5 Procedimiento de designación

El Responsable de Seguridad de la Información será nombrado por Gerencia a propuesta del Comité de Seguridad. El nombramiento se revisará cada 2 años o cuando el puesto quede vacante.

6.6 Resumen de funciones de cada rol

En la tabla se usan las siguientes abreviaturas:

CSI – Comité de Seguridad de la Información
 RINFO – Responsable de la Información
 RSERV – Responsable del Servicio
 RSEG – Responsable de la Seguridad
 RSIS – Responsable del Sistema
 ASS– Administrador de la Seguridad del Sistema

tarea	responsable
Determinación de los niveles de seguridad requeridos en cada dimensión	RINFO + RSERV o CSI
Determinación de la categoría del sistema	RSEG
Análisis de riesgos	RSEG
Declaración de aplicabilidad	RSEG
Medidas de seguridad adicionales	RSEG
Configuración de seguridad	elabora: RSEG aplica: ASS
Implantación de las medidas de seguridad	ASS
Aceptación del riesgo residual	RINFO + RSERV
Documentación de seguridad del sistema	RSEG
Política de seguridad	elabora: CSI aprueba : Dirección
Normativa de seguridad	elabora: RSEG aprueba: CSI
Procedimientos operativos de seguridad	elabora: RSIS aprueba: RSEG aplica: ASS
Estado de la seguridad del sistema	monitoriza: ASS reporta: RSEG

Planes de mejora de la seguridad	elaboran: RSIS + RSEG aprueba: CSI
Planes de concienciación y formación	elabora: RSEG aprueba: CSI
Planes de continuidad	elabora: RSIS valida: RSEG coordina y aprueba: CSI ejercicios: RSIS
Suspensión temporal del servicio	RSIS
Ciclo de vida: especificación, arquitectura, desarrollo, operación, cambios	elabora: RSIS aprueba: RSEG

6.7 Nombramientos y jerarquía

La Dirección de Tracasa Instrumental, en cumplimiento de la [guía CCN-STIC 801 en su apartado 10](#), nombra:

- al Responsable de la Información
- al Responsable del Servicio, si fuera distinto al Responsable de la Información
- al Responsable de la Seguridad, que debe reportar directamente a la Dirección y al Comité de Seguridad de la Información.
- al Responsable del Sistema, que, en materia de seguridad, debe reportar al Responsable de la Seguridad

6.8 Especificidades

1. Independencia entre el Responsable de Seguridad y el Responsable del Sistema

El Responsable de la Seguridad será distinto del Responsable del Sistema, no debiendo existir dependencia jerárquica entre ambos y tal y como establece el artículo 13 del ENS.

2. Responsabilidades unificadas entre el Responsable de la Información y el Responsable del Servicio

La diferenciación entre ambos roles tiene sentido:

- Cuando el servicio maneja información de diferentes procedencias, no necesariamente de la misma unidad departamental que la que presta el servicio.
- Cuando la prestación del servicio no depende de la unidad que es Responsable de la Información.

En el caso de Tracasa Instrumental ambos roles están unificados en la figura del Director de Operaciones.

6.9 Resolución de conflictos

De conformidad con lo dispuesto en el artículo 3 de la Ley 40/2015, que señala que las Administraciones Públicas, sirviendo los intereses generales, desarrollarán su actividad con plena observancia de los principios de eficacia, jerarquía, descentralización, desconcentración y coordinación, los conflictos entre distintos elementos de la organización serán resueltos por el superior jerárquico.

7 Profesionalidad

La seguridad de los sistemas de información estará atendida y será revisada y auditada por personal cualificado, dedicado e instruido en todas las fases de su ciclo de vida: planificación, diseño, adquisición, construcción, despliegue, explotación, mantenimiento, gestión de incidencias y desmantelamiento.

Tracasa Instrumental exigirá, de manera objetiva y no discriminatoria, que las organizaciones que les presten servicios de seguridad cuenten con profesionales cualificados y con unos niveles idóneos de gestión y madurez en los servicios prestados.

Tracasa Instrumental determinará los requisitos de formación y experiencia necesaria del personal para el desarrollo de su puesto de trabajo.

8 Autorización y control de accesos

El acceso controlado a los sistemas de información comprendidos en el ámbito de aplicación deberá estar limitado a los usuarios, procesos, dispositivos u otros sistemas de información, debidamente autorizados, y exclusivamente a las funciones permitidas.

9 Protección de las instalaciones

Los sistemas de información y su infraestructura de comunicaciones asociada deberán permanecer en áreas controladas y disponer de los mecanismos de acceso adecuados y proporcionales en función del análisis de riesgos, sin perjuicio de lo establecido en la normativa aplicable relativa a la protección de las infraestructuras críticas.

10 Adquisición de productos de seguridad y contratación de servicios de seguridad

En la adquisición de productos de seguridad o contratación de servicios de seguridad de las tecnologías de la información y la comunicación que vayan a ser empleados en los sistemas de información se utilizarán, de forma proporcionada a la categoría del sistema y el nivel de seguridad determinados, aquellos que tengan

certificada la funcionalidad de seguridad relacionada con el objeto de su adquisición, a través del Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de Seguridad de las Tecnologías de la Información del CCN considerando, excepcionalmente, el criterio a seguir en los casos en que no existan productos o servicios certificados.

11 Mínimo privilegio

Los sistemas de información deben diseñarse y configurarse otorgando los mínimos privilegios necesarios para su correcto desempeño.

12 Integridad y actualización del sistema

La inclusión de cualquier elemento físico o lógico en el catálogo actualizado de activos del sistema, o su modificación, requerirá autorización formal previa.

La evaluación y monitorización permanentes permitirán adecuar el estado de seguridad de los sistemas atendiendo a las deficiencias de configuración, las vulnerabilidades identificadas y las actualizaciones que les afecten, así como la detección temprana de cualquier incidente que tenga lugar sobre los mismos.

13 Protección de la información almacenada y en tránsito

En la organización e implantación de la seguridad se prestará especial atención a la información almacenada o en tránsito a través de los equipos o dispositivos portátiles o móviles, los dispositivos periféricos, los soportes de información y las comunicaciones sobre redes abiertas, que deberán analizarse especialmente para lograr una adecuada protección.

Se aplicarán procedimientos que garanticen la recuperación y conservación a largo plazo de los documentos electrónicos producidos por los sistemas de información comprendidos en el ámbito de aplicación de este real decreto, cuando ello sea exigible.

Toda información en soporte no electrónico que haya sido causa o consecuencia directa de la información electrónica a la que se refiere este real decreto, deberá estar protegida con el mismo grado de seguridad que ésta. Para ello, se aplicarán las medidas que correspondan a la naturaleza del soporte, de conformidad con las normas que resulten de aplicación.

14 Prevención ante otros sistemas de información interconectados

Se protegerá el perímetro del sistema de información, especialmente, si se conecta a redes públicas, reforzándose las tareas de prevención, detección y respuesta a incidentes de seguridad.

En todo caso, se analizarán los riesgos derivados de la interconexión del sistema con otros sistemas y se controlará su punto de unión. Para la adecuada interconexión entre sistemas se estará a lo dispuesto en la Instrucción Técnica de Seguridad del ENS correspondiente.

15 Registro de la actividad y detección de código dañino

Tracasa Instrumental registrará las actividades de los usuarios, reteniendo la información estrictamente necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

Tracasa Instrumental podrá, en la medida estrictamente necesaria y proporcionada, analizar las comunicaciones entrantes o salientes, y únicamente para los fines de seguridad de la información, de forma que sea posible impedir el acceso no autorizado a las redes y sistemas de información, detener los ataques de denegación de servicio, evitar la distribución malintencionada de código dañino así como otros daños a las antedichas redes y sistemas de información.

Para corregir o, en su caso, exigir responsabilidades, cada usuario que acceda al sistema de información deberá estar identificado de forma única, de modo que se sepa, en todo momento, quién recibe derechos de acceso, de qué tipo son éstos, y quién ha realizado una determinada actividad.

16 Mejora continua del proceso de seguridad

El proceso integral de seguridad implantado deberá ser actualizado y mejorado de forma continua. Para ello, se aplicarán los criterios y métodos reconocidos en la práctica nacional e internacional relativos a la gestión de la seguridad de las tecnologías de la información.

17 Gestión de riesgos

Todos los sistemas sujetos a esta Política deberán realizar un análisis de riesgos, evaluando las amenazas y los riesgos a los que están expuestos. Este análisis se repetirá:

- regularmente, al menos una vez al año
- cuando cambie la información manejada
- cuando cambien los servicios prestados
- cuando ocurra un incidente grave de seguridad
- cuando se reporten vulnerabilidades graves

Para la armonización de los análisis de riesgos, el SGSI establecerá una valoración de referencia para los diferentes tipos de información manejados y los diferentes servicios prestados. El CSI dinamizará la disponibilidad de recursos para atender a las necesidades de seguridad de los diferentes sistemas, promoviendo inversiones de carácter horizontal.

18 Datos de carácter personal

Tracasa Instrumental trata datos de carácter personal. Todos los sistemas de información de Tracasa Instrumental se ajustarán a los niveles de seguridad requeridos por la normativa para la naturaleza y finalidad de los datos de carácter personal.

19 Desarrollo de la política de seguridad de la información

Esta Política de Seguridad de la Información complementa las políticas de seguridad de Tracasa Instrumental recogidas en su SGSI.

Esta Política se desarrollará por medio de normativa de seguridad que afronte aspectos específicos. La normativa de seguridad estará a disposición de todos los miembros de la organización que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones.

La normativa de seguridad estará disponible en la intranet: : [Intranet de Tracasa Instrumental \(tracasa.es\)](http://tracasa.es) e impresa y custodiada en las oficinas de la empresa pública NASERTIC sitas en Calle Orcoyen, s/n, 31011 Pamplona, Navarra.

19.1 Ciclo de vida de la Política

Será misión del CSI la revisión anual de esta Política de Seguridad de la Información y la propuesta de revisión o mantenimiento de la misma. La Política será aprobada por el Comité de Seguridad y difundida para que la conozcan todas las partes afectadas.

20 Obligaciones del personal

Todos los miembros de Tracasa Instrumental tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad, siendo responsabilidad del CSI disponer los medios necesarios para que la información llegue a los afectados.

Se establecerá un programa de concienciación continua para atender a todos los miembros de Tracasa Instrumental, en particular a los de nueva incorporación.

Las personas con responsabilidad en el uso, operación o administración de sistemas TIC recibirán formación para el manejo seguro de los sistemas en la medida en que la necesiten para realizar su trabajo. La formación será obligatoria antes de asumir una responsabilidad, tanto si es su primera asignación o si se trata de un cambio de puesto de trabajo o de responsabilidades en el mismo.

21 Terceras partes

Cuando Tracasa Instrumental preste servicios a otros organismos o maneje información de otros organismos, se les hará partícipes de esta Política de Seguridad de la Información, se establecerán canales para reporte y coordinación de los respectivos Comités de Seguridad TIC y se establecerán procedimientos de actuación para la reacción ante incidentes de seguridad.

Cuando Tracasa Instrumental utilice servicios de terceros o ceda información a terceros, se les hará partícipes de esta Política de Seguridad y de la Normativa de Seguridad que atañe a dichos servicios o información. Dicha tercera parte quedará sujeta a las obligaciones establecidas en dicha normativa, pudiendo desarrollar sus propios procedimientos operativos para satisfacerla. Se establecerán procedimientos específicos de reporte y resolución de incidencias.

Cuando algún aspecto de la Política no pueda ser satisfecho por una tercera parte según se requiere en los párrafos anteriores, se requerirá un informe del Responsable de Seguridad que precise los riesgos en que se incurre y la forma de tratarlos. Se requerirá la aprobación de este informe por los responsables de la información y los servicios afectados antes de seguir adelante.

Firmado digitalmente por:
44624007M MARGARITA
GONZALEZ (R: B71280689)
Fecha y hora: 03.07.2024
09:06:56

Mar González Paredes
Directora General de Tracasa Instrumental

