ANEXO III

FICHA DE TRATAMIENTO DE DATOS

Condiciones especiales en el marco del Acuerdo General de Encargo del Tratamiento de Datos Personales

Artículo 28 del Reglamento (UE) 2016/679 («**RGPD**»)

Entre

El **Responsable del Tratamiento**, según se identifica en el Acuerdo, representado por su representante legal investido de los poderes necesarios,

y

El **Encargado del Tratamiento**, según se identifica en el Acuerdo, representado por su representante legal investido de los poderes necesarios,

Asimismo, el Responsable y el Encargado podrán denominarse conjuntamente «**Partes**» e individualmente «**Parte**».

CONSIDERANDO QUE

I. Las Partes han suscrito el Acuerdo Principal de Encargo del Tratamiento de Datos Personales («Acuerdo»), que regula los términos y modalidades del tratamiento de datos personales realizado por el Encargado en el marco de la prestación de los Servicios objeto del Contrato;
II. De conformidad con el citado Acuerdo, el tratamiento de datos personales relacionado con la prestación de Servicios concretos se regula mediante Fichas de Tratamiento de Datos que definen las características operativas, las categorías de datos tratados, las finalidades, las medidas de seguridad aplicadas y, en su caso, la intervención de subencargados del tratamiento;
III. La presente Ficha de Tratamiento de Datos especifica los detalles del Servicio de conformidad con el Acuerdo. Integra y completa las disposiciones generales del Acuerdo, constituyendo parte integrante y vinculante entre las Partes;
IV. En caso de conflicto entre las disposiciones de la presente Ficha de Tratamiento de Datos y las del Acuerdo, prevalecerán las disposiciones del Acuerdo, salvo que la Ficha de Tratamiento de Datos prevea expresamente excepciones acordadas entre las Partes;
V. Para los aspectos no previstos expresamente en el presente documento, se aplicarán las disposiciones y definiciones establecidas en el Acuerdo y en el Contrato, que quedan aquí íntegramente incorporadas por referencia.

Expuesto todo lo anterior, las Partes presentan, en la siguiente tabla, las especificaciones del tratamiento de Datos Personales relacionado con el Servicio, incluyendo información sobre las finalidades, las categorías de datos tratados, las medidas de seguridad aplicadas y cualquier otro detalle relevante a los efectos del Acuerdo.

	DESCRIPCIÓN
SERVICIO	*Servicio de Entrega Electrónica Certificada (SERC) y Servicio de Entrega Electrónica Certificada Cualificado (SERCQ)*
ENTIDAD PRESTADORA	**Uanataca SAU** Cuando la Entidad Prestadora no coincida con el Proveedor identificado en la Propuesta Comercial, esta actuará como subencargado del tratamiento intragrupo por cuenta del Proveedor, operando en virtud de acuerdos intragrupo preexistentes entre las empresas del Grupo Namirial, conformes con el artículo 28 del RGPD.
NATURALEZA DEL TRATAMIENTO	El Encargado podrá tratar los Datos Personales del Cliente en el marco de la prestación del servicio, dentro de los límites estrictamente necesarios para la ejecución de los servicios previstos en el Contrato, en términos de:

	recogida, registro, organización o estructuración, consulta, tratamiento, selección, extracción, cotejo, uso, comunicación, supresión o destrucción.
FINALIDAD DEL TRATAMIENTO	Celebración del Contrato y ejecución de los servicios objeto del Contrato.
MODALIDAD DE PRESTACIÓN	*SaaS (Compartido/Privado)*
CATEGORÍAS DE INTERESADOS	• Clientes finales; • Usuarios del servicio.
CATEGORÍAS DE DATOS PERSONALES TRATADOS	Los Datos Personales tratados por el Encargado por cuenta del Responsable pertenecen a las siguientes categorías: **DATOS COMUNES:** • **Datos personales** (nombre, apellidos, correo electrónico, fecha de nacimiento, lugar de nacimiento, nacionalidad, sexo, código fiscal, dirección de residencia/domicilio); • **Datos de contacto** (correo electrónico, número de teléfono); • **Datos de navegación** (dirección IP); • **Otros datos posibles**: datos presentes en las comunicaciones**certificadas**. **CATEGORÍAS ESPECIALES DE DATOS PERSONALES:** • **Otros datos posibles**: datos especiales presentes en las comunicaciones certificadas.
UBICACIÓN DE ALMACENAMIENTO DE LOS DATOS	Los datos se almacenan en servidores del Encargado y/o de los subencargados del tratamiento ubicados dentro de la Unión Europea/EEE.
DURACIÓN DEL TRATAMIENTO DE DATOS PERSONALES	El tratamiento de los Datos Personales para la prestación de los Servicios tendrá la siguiente duración: toda la duración del Contrato con el Responsable; toda la duración del Acuerdo con el Responsable si, por cualquier motivo, fuera superior a la duración del Contrato. Una vez transcurridos los plazos mencionados, se permite al Encargado conservar ulteriormente los Datos Personales en la medida en que ello constituya el cumplimiento de obligaciones legales específicas o de órdenes de las Autoridades competentes. La conservación de los Datos Personales se permite también, exclusivamente, en la medida en que dichos Datos Personales sean necesarios para que el Encargado pueda demostrar, ejercer o defender su propio derecho, por un plazo máximo de 10 años.
MEDIDAS DE SEGURIDAD	Ref. **Anexo III A - MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD**
SUBENCARGADOS DEL TRATAMIENTO	La Entidad Prestadora del Servicio (identificada en la fila anterior) recurre, para la prestación del Servicio, a otras empresas del Grupo Namirial y a terceros seleccionados que ofrecen garantías de confidencialidad de los datos. La lista actualizada se recoge en el Anexo III B, dividida en

	la **Tabla A** (empresas del Grupo Namirial que intervienen en la prestación del servicio, que operan en virtud de acuerdos intragrupo preexistentes conformes con el artículo 28 del RGPD y distintos del presente Acuerdo) y la **Tabla B** (subencargados del tratamiento terceros). Algunos de estos terceros pueden operar también fuera del Espacio Económico Europeo (EEE), incluidos los Estados Unidos. Para garantizar el cumplimiento del RGPD (artículos 44 a 49) y de la normativa de protección de datos personales, el Proveedor podrá utilizar mecanismos adecuados para la transferencia de datos. Estas entidades se seleccionan de conformidad con lo previsto en el Acuerdo, reciben instrucciones precisas sobre el tratamiento de datos y realizan únicamente las actividades necesarias, de conformidad con las directrices proporcionadas. La lista actualizada de dichas entidades se recoge en el Anexo III B del presente documento.

ANEXO III - A

MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

Las medidas de seguridad descritas en el presente Anexo se aplican de manera adicional a las previstas en el Acuerdo y constituyen un nivel de protección adicional para el tratamiento regulado por la Ficha de Tratamiento a la que se adjuntan. Se aplican a la Entidad Prestadora del Servicio a que se refiere el Contrato, que puede o no coincidir con el Encargado.

1. MEDIDAS TÉCNICAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Medidas para garantizar de forma permanente la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas y servicios de tratamiento	El proceso de verificación de la integridad de los paquetes de información y documentos dentro del servicio incluye: • Auditorías internas periódicas para comprobar y verificar que el estado del Sistema de Gestión de la Seguridad de la Información es adecuado y conforme a la ley; • Los empleados están formados para comprender los flujos de comunicación y, sin autenticación previa, no tendrán acceso a los datos tratados; • Los flujos de comunicación están protegidos mediante el uso de redes privadas virtuales (VPN). De este modo, las conexiones establecidas con las VPN protegerán la información intercambiada, ya que dicha información se cifrará entre ambos extremos del túnel; • Para cada servicio ofrecido, se elaboran procedimientos para determinar el alcance y la frecuencia de las copias de seguridad cifradas (AES256) de los datos tratados, especificando el plazo de conservación. En estos casos, se establecerá el número de copias necesarias y el plazo de conservación.
Medidas para garantizar la capacidad de restablecer, de forma oportuna, la disponibilidad y el acceso a los datos personales en caso de incidente físico o técnico	En caso de violación de la seguridad de los datos, Uanataca dispone de un proceso de gestión de incidentes informáticos que funciona como sigue: • Un equipo responsable, sobre la base de un análisis exhaustivo de incidentes informáticos anteriores, desarrollará un plan de acción compuesto por medidas preventivas para limitar la repetición de tales episodios; • Al detectar un incidente físico o técnico, este se clasificará y dividirá en las categorías apropiadas necesarias para determinar la gravedad y la prioridad del tratamiento que deba aplicarse; • Posteriormente, a través del proceso de notificación de incidentes, se destacarán las acciones inmediatas que deban adoptarse para garantizar la capacidad de restablecer con prontitud la disponibilidad y el acceso a los datos personales afectados; • Uanataca también prevé la elaboración de un registro de incidentes informáticos, en el que es necesario disponer de la mayor cantidad de información posible sobre el incidente, en concreto: • Fecha y hora del incidente; • Tipo y gravedad del incidente; Recursos afectados; Posibles orígenes; Estado del incidente; Acciones adoptadas para resolver el problema;

	Quién realizó las acciones anteriores; Fecha y hora de resolución y cierre del incidente. Por último, para la resolución del incidente informático, se elabora un documento explicativo del procedimiento que debe aplicarse en caso de violación de la seguridad de los datos, teniendo en cuenta los distintos escenarios posibles.
Medidas de protección de los datos durante el almacenamiento	Uanataca supervisará la evolución de las herramientas y mecanismos existentes para el control de malware (antimalware, antiphishing, antispam, análisis web y de correo electrónico) con el fin de mejorar la protección de los activos de información. **La supervisión podrá:** • Realizar análisis automáticos y periódicos para detectar cualquier tipo de malware; • Realizar comprobaciones automáticas de los archivos adjuntos de correo electrónico y de las descargas de la web, ya que pueden contener códigos maliciosos; • Bloquear el acceso a determinadas aplicaciones o sitios web en función de la política de privacidad, creando así «listas negras» de prevención; • Permitir el acceso a determinadas aplicaciones o sitios web en función de la política de privacidad, creando así «listas blancas»; • Analizar y detectar posibles páginas web que puedan contener amenazas que pongan en riesgo los datos tratados.
Medidas para garantizar el registro de eventos	Para los empleados y colaboradores de Uanataca se prevé una fase de registro en la que se crearán cuentas específicas con el dominio uanataca.com. • Estas medidas de registro se aplican también a las cuentas con acceso directo a las VPN de Uanataca para el trabajo remoto. • Uanataca se ha dotado de software (Kibana + ElasticSearch) para la gestión de eventos relacionados con la seguridad y la supervisión de usuarios. Este software está configurado en modo On-premise, directamente en los servidores de Uanataca. • Este sistema de gestión establece que los sujetos considerados pueden acceder a sus cuentas introduciendo una contraseña, que debe cumplir determinados requisitos para ser suficientemente difícil de adivinar o descifrar. • Uanataca también prevé el desarrollo de procedimientos para garantizar la custodia de los archivos centralizados, permitiendo el acceso a ellos únicamente mediante autenticación de dos factores, consistente en la introducción de una contraseña y un PIN. Además, teniendo en cuenta que los dispositivos de acceso pueden pertenecer a Uanataca o al empleado o colaborador, se distinguen varios tipos de acceso: Acceso simple de trabajador, que tendrá acceso a la información contenida en los archivos, correos electrónicos y wikis, para llevar a cabo su actividad laboral, incluso de forma remota; Acceso de administración, mediante VPN, con autenticación de dos factores (contraseña más clave privada RSA), para quienes

	ocupen funciones administrativas de mayor nivel; Por último, el acceso especial. Este tipo de acceso, que debe autorizarse previamente, se concederá para la realización de actividades específicas y de duración limitada.
Medidas para garantizar la configuración de los sistemas, incluida la configuración por defecto	Los proyectos de desarrollo se gestionarán a través de REDMINE, una herramienta integrada de gestión de tickets, código fuente y documentación (wiki). Se trata de un software de gestión de proyectos y seguimiento de errores de código abierto y basado en web, descargado y configurado directamente en los servidores internos de Uanataca. El código fuente de las aplicaciones se mantendrá actualizado mediante repositorios de gestión de datos (GIT). La autenticación para acceder a los repositorios se realizará mediante la introducción de nombre de usuario y contraseña (en posesión de cada usuario que trata los datos) a través de canales de comunicación cifrados. Cada proyecto, tanto en REDMINE como en GIT, contará con distintos roles de acceso, tales como: Administrador, Product Owner, desarrollador. Los cambios e iteraciones del código se realizarán en ramas independientes dentro del mismo gestor de código fuente.
Medidas internas de gestión y gobernanza de TI y ciberseguridad	Uanataca cuenta con un Comité Técnico de Seguridad que desempeñará las siguientes funciones: Elaboración de normas de seguridad, de conformidad con las directrices establecidas; Elaboración de procedimientos de seguridad, para la implementación de controles derivados de las normas anteriores y de conformidad con el Comité de Seguridad; Desarrollo y elaboración de procedimientos derivados de los planes operativos de continuidad de negocio. El sistema cumple con la certificación ISO/IEC 27001.
Medidas para garantizar una conservación limitada de los datos	La custodia de la información y los datos se clasifica en términos de conservación y supresión de la información en posesión de Uanataca. Para cumplir con este requisito, se elaborarán documentos para cada país, teniendo en cuenta los distintos regímenes legales que deban respetarse, con el fin de determinar los siguientes plazos: Plazo de conservación: se refiere al período mínimo durante el cual Uanataca debe conservar la información facilitada por los usuarios; Plazo máximo de supresión: se refiere al período máximo transcurrido el cual Uanataca debe suprimir la información mencionada. Este plazo comienza a contar desde el momento en que finaliza el plazo de conservación.
Medidas para garantizar la responsabilidad proactiva (accountability)	Para garantizar la seguridad de los datos tratados, Uanataca designará a un Responsable de Seguridad encargado de las siguientes funciones: 1. Elaboración del análisis de riesgos. 2. Centralizar todas las acciones del Sistema de Gestión de la Seguridad de la Información (SGSI) de Uanataca. 3. Comunicar la Política de Seguridad a todo el personal y

	a las partes interesadas. 4. Impartir formación en el SGSI y clasificar la información conforme a los criterios de clasificación definidos en la normativa correspondiente. 5. Coordinar y supervisar las acciones llevadas a cabo por los Responsables de Riesgos. 6. Notificar a todo el personal que se incorpore a Uanataca sus obligaciones en materia de cumplimiento de la Política de Seguridad y su marco normativo. 7. Verificar el cumplimiento de la Política de Seguridad en la gestión de todos los contratos con terceros que se encuadren en el ámbito del SGSI. 8. Organizar, planificar y realizar auditorías periódicas del SGSI. Uanataca también designará a Responsables de Riesgos, que tendrán las siguientes funciones: 1. Serán responsables de dirigir y controlar las acciones de mejora para minimizar los riesgos; 2. Controlarán las acciones de minimización de riesgos de forma que exista siempre su trazabilidad; 3. Se coordinarán con el responsable de seguridad para informar sobre su progreso hacia el SGSI.
Medidas para posibilitar la portabilidad de los datos y garantizar su supresión	Uanataca garantiza la supresión de los datos tratados cuando dejen de cumplirse los requisitos legales y contractuales. A continuación se indican algunas de las causas que permitirán la supresión de la información: 1. Finalización de la condición legítima del tratamiento, asociada a la finalización de la relación contractual que permite la conservación de dicha información. 2. Vencimiento del plazo legal para la conservación de la información y los datos tratados. Ejercicios de derechos por parte de los interesados. Los interesados podrán solicitar legítimamente la supresión de su información personal en posesión de Uanataca. Para esta actividad, se tendrá en cuenta la legislación del país de origen del interesado. Para atender estas hipótesis, Uanataca ha desarrollado un procedimiento capaz de garantizar la supresión de los datos mediante dos métodos distintos: 1. La información puede ser destruida completamente, si está en formato papel, mediante el uso de trituradoras o utilizando servicios específicos de destrucción de información en papel. 2. La información digital se eliminará de los archivos informáticos. Cualquier copia de seguridad que contenga copias de dicha información también se eliminará, de modo que no puedan reutilizarse.

2. MEDIDAS ORGANIZATIVAS DE SEGURIDAD

TIPO DE MEDIDA	DESCRIPCIÓN
Procedimientos para probar, verificar y evaluar	Uanataca garantiza la autenticidad e integridad de los contenidos cumpliendo la normativa aplicable en materia de

regularmente la eficacia de las medidas técnicas y organizativas destinadas a garantizar la seguridad del tratamiento	firma electrónica y ateniéndose a las normas internacionales. • Uanataca utiliza cifrado TLS para el protocolo HTTPS en sus sistemas de comunicación, aplicando conjuntos de cifrado limitados en los que solo se permiten protocolos considerados suficientemente seguros para el acceso AES256 (TLS 1.2 o superior). • Todos los algoritmos utilizados por Uanataca para la creación y validación de firmas digitales y electrónicas cumplen con la «suite criptográfica» ETSI TS 119 312. • Las actividades se llevan a cabo dentro de los controles de la certificación ISO/IEC 27001.

ANEXO III - B

SUBENCARGADOS DEL TRATAMIENTO

El presente Anexo enumera los Subencargados del Tratamiento aprobados en la fecha de firma de la Ficha de Tratamiento de Datos correspondiente, de conformidad con el Acuerdo.

Las entidades enumeradas han sido seleccionadas con arreglo a criterios de experiencia, fiabilidad y garantías de cumplimiento de la normativa aplicable, en particular de lo dispuesto en el artículo 28 del Reglamento (UE) 2016/679.

Operan bajo la autoridad del Encargado, ateniéndose a las instrucciones recibidas y adoptando medidas de seguridad adecuadas para la protección de los Datos Personales tratados.

La lista de Subencargados del Tratamiento podrá actualizarse a lo largo del tiempo de conformidad con lo previsto en el Acuerdo.

TABLA A

EMPRESAS DEL GRUPO NAMIRIAL QUE INTERVIENEN EN LA PRESTACIÓN DEL SERVICIO

NOMBRE DE LA EMPRESA	DIRECCIÓN	LUGAR DE TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Uanataca S.A.U.	Avenida Meridiana 350, piso 3 08027 Barcelona (España)	EEE/EE. UU.	Prestación del Servicio SERQC y SERC. La lista de encargados de tratamiento adicionales puede consultarse en la siguiente dirección: https://www.evicertia.com/es/rgpd
Namirial Spa	Via Caduti sul Lavoro, 4 Senigallia (AN) 60019 - Italia	EEE	Servicios operativos de grupo: operaciones técnicas locales, desarrollo, soporte, entornos de pruebas, copias de seguridad, así como servicios de apoyo administrativo, financiero, contable y corporativo.

TABLA B

SUBENCARGADOS DEL TRATAMIENTO TERCEROS

NOMBRE DE LA EMPRESA	DIRECCIÓN	LUGAR DE TRATAMIENTO	ÁMBITO DE ACTIVIDAD
Atlassian Corporation	Amsterdam, Singel 236 1016 AB Ámsterdam, Países Bajos	EEE/EE. UU.	Gestión de tickets de soporte
Zendesk Inc.	989 Market St, San Francisco, CA 94103	EEE	Gestión de tickets de soporte
Exalate NV	Roderveldlaan 2 bus 3, 2600 Berchem, Bélgica	EEE	Sincronización de tickets de soporte
Var Group S.p.A. (Yarix)	Via della Piovola, 138 - 50053	EEE	SOC (Security Operation Center) y MOC (Monitoring Operation Center)

	Empoli FI		