



DOCUMENTACIÓN CONTRACTUAL

Acuerdo de Encargo del Tratamiento

Artículo 28 del Reglamento (UE) 2016/679 (RGPD). Forma parte del Contrato de Servicios Gestionados de Ciberseguridad por referencia (Condición Novena de las Condiciones Generales).

Artículo 28 del Reglamento (UE) 2016/679, de 27 de abril, General de Protección de Datos

Referencia: Artículo 28 RGPD — Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD)

En [Ciudad del cliente], a ____ de _____ de 20____

REUNIDOS

De una parte, [NOMBRE COMPLETO DEL CLIENTE], con CIF [CIF], domicilio social en [DIRECCIÓN COMPLETA], inscrita en el Registro Mercantil de [CIUDAD], representada por D./Dña. [NOMBRE REPRESENTANTE], en calidad de [CARGO], con facultades suficientes para este otorgamiento (en adelante, **el Responsable del Tratamiento o [NOMBRE ABREVIADO CLIENTE]**).

Y de otra, ELANTIA CANARIAS S.L.U., con CIF B22913412 y domicilio en C. Alfonso Trujillo, 9, Puerta 7, 38300 La Orotava, Santa Cruz de Tenerife, titular de la marca comercial Ciberia28, representada por D. Carlos Castillo Úbeda, en su condición de Administrador Único, con facultades suficientes para este acto (en adelante, **el Encargado del Tratamiento o el Encargado**).

Ambas partes, reconociéndose mutuamente capacidad jurídica y de obrar suficiente para obligarse mediante el presente contrato,

MANIFIESTAN

- I. Que [NOMBRE ABREVIADO CLIENTE] desarrolla su actividad empresarial tratando datos personales de clientes, empleados, proveedores, colaboradores y demás personas físicas relacionadas con su actividad, ostentando la condición de Responsable del Tratamiento conforme al Reglamento (UE) 2016/679, de 27 de abril, General de Protección de Datos (RGPD), y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).
- II. Que ELANTIA CANARIAS S.L.U. (Ciberia28) presta servicios profesionales especializados en ciberseguridad, protección de infraestructuras tecnológicas, monitorización de eventos de seguridad, respuesta ante incidentes, gestión de vulnerabilidades, administración de soluciones de seguridad, soporte técnico y demás servicios relacionados con la protección de los sistemas de información.
- III. Que ambas entidades han suscrito un Contrato de Prestación de Servicios de Ciberseguridad, cuya ejecución puede requerir que ELANTIA CANARIAS S.L.U. acceda o pueda tener acceso a datos personales responsabilidad de [NOMBRE ABREVIADO CLIENTE], exclusivamente para la correcta prestación de los servicios contratados y sin determinar, en ningún caso, los fines ni los medios esenciales del tratamiento.
- IV. Que, de conformidad con el artículo 28 del Reglamento (UE) 2016/679, el tratamiento de datos personales por cuenta del Responsable debe regularse mediante un contrato que establezca las obligaciones y garantías aplicables al Encargado del Tratamiento, asegurando el cumplimiento de la normativa de protección de datos y la adecuada protección de los derechos y libertades de las personas afectadas.
- V. Que ELANTIA CANARIAS S.L.U. declara disponer de la capacidad técnica, organizativa y profesional necesaria para prestar los servicios contratados con las garantías exigidas por la normativa vigente, comprometiéndose a aplicar las medidas técnicas y organizativas apropiadas para garantizar la seguridad de los datos personales tratados por cuenta del Responsable.

ACUERDAN

Suscribir el presente Contrato de Encargo del Tratamiento de Datos Personales, que complementa el contrato principal de prestación de servicios y regula las condiciones en las que el Encargado podrá tratar datos personales por cuenta del Responsable, con arreglo a las siguientes

ESTIPULACIONES

PRIMERA. OBJETO

1.1. El presente Contrato de Encargo del Tratamiento tiene por objeto regular las condiciones en las que ELANTIA CANARIAS S.L.U. (Ciberia28) tratará datos personales por cuenta de [NOMBRE ABREVIADO CLIENTE], exclusivamente para la correcta ejecución del contrato de prestación de servicios de ciberseguridad suscrito entre ambas partes.

1.2. El Encargado actuará únicamente siguiendo las instrucciones documentadas del Responsable del Tratamiento y no podrá utilizar los datos personales para fines propios, distintos de los previstos en este contrato o incompatibles con la finalidad del tratamiento, salvo obligación legal.

1.3. El presente contrato complementa el contrato principal de prestación de servicios y se limita a regular el acceso y tratamiento de datos personales que resulte necesario para su ejecución, sin modificar las restantes obligaciones asumidas por las partes.

SEGUNDA. DURACIÓN

2.1. El presente contrato permanecerá vigente durante toda la duración del contrato principal de prestación de servicios.

2.2. La extinción del contrato principal determinará la finalización automática del presente contrato, sin perjuicio de las obligaciones que, por su naturaleza, deban mantenerse con posterioridad, especialmente las relativas a confidencialidad, seguridad de la información, cooperación, responsabilidad y destino de los datos personales.

2.3. Cualquier modificación del alcance de los servicios que implique cambios en el tratamiento de datos personales deberá documentarse por escrito y, cuando proceda, reflejarse mediante la actualización de los anexos del presente contrato.

TERCERA. NATURALEZA Y FINALIDAD DEL TRATAMIENTO

3.1. El Encargado realizará únicamente las operaciones de tratamiento imprescindibles para la prestación de los servicios contratados por el Responsable.

3.2. La finalidad del tratamiento será exclusivamente la prestación de servicios de ciberseguridad, incluyendo, cuando resulte necesario: monitorización de sistemas, protección avanzada de equipos, gestión de vulnerabilidades, administración de soluciones de seguridad, soporte técnico, respuesta ante incidentes, gestión de copias de seguridad y demás actuaciones previstas en el contrato principal.

3.3. El acceso a datos personales tendrá carácter meramente instrumental respecto de los servicios contratados. El Encargado no determinará los fines ni los medios esenciales del tratamiento y limitará el acceso a la información estrictamente necesaria para la ejecución de cada actuación.

3.4. Las categorías de interesados, categorías de datos personales y operaciones autorizadas se describen en el **Anexo I**, que forma parte integrante del presente contrato.

CUARTA. CATEGORÍAS DE DATOS PERSONALES

4.1. El Encargado podrá acceder únicamente a los datos personales necesarios para la prestación de los servicios contratados.

4.2. Los tratamientos podrán afectar, entre otros, a datos correspondientes a empleados, clientes, proveedores, colaboradores y usuarios de los sistemas de información gestionados por el Responsable.

4.3. El acceso podrá comprender:

- Datos identificativos (nombre, apellidos, DNI/NIE, cargo)
- Datos de contacto (email, teléfono, dirección)
- Credenciales de acceso a sistemas
- Direcciones IP e identificadores de dispositivos
- Registros de actividad (logs)
- Información contenida en equipos, servidores o copias de seguridad
- Cualquier otro dato cuyo tratamiento resulte imprescindible para la correcta prestación del servicio

4.4. El acceso a categorías especiales de datos únicamente podrá producirse de forma incidental cuando resulte inevitable para la resolución de una incidencia, quedando sujeto a las mismas garantías de seguridad y confidencialidad previstas en el presente contrato.

QUINTA. OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO

5.1. El Encargado tratará los datos personales únicamente conforme a las instrucciones documentadas del Responsable y exclusivamente para la ejecución del contrato principal.

- 5.2.** El Encargado garantizará que el acceso a los datos quede limitado al personal autorizado que necesite conocerlos para la prestación del servicio, aplicando el principio de mínimo privilegio.
- 5.3.** El Encargado garantizará que las personas autorizadas para tratar datos personales hayan asumido un compromiso de confidencialidad y reciban formación adecuada en protección de datos y seguridad de la información.
- 5.4.** El Encargado adoptará las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo, de conformidad con el artículo 32 del RGPD y con las medidas descritas en el **Anexo II**.
- 5.5.** El Encargado asistirá al Responsable, cuando resulte necesario, para el cumplimiento de las obligaciones derivadas de la normativa de protección de datos, incluyendo la atención del ejercicio de derechos, la gestión de brechas de seguridad, la realización de análisis de riesgos y evaluaciones de impacto.
- 5.6.** El Encargado informará sin demora al Responsable cuando considere que una instrucción recibida pudiera infringir la normativa de protección de datos.
- 5.7.** El Encargado mantendrá la documentación necesaria para acreditar el cumplimiento de las obligaciones asumidas en el presente contrato y colaborará en las actuaciones de verificación y auditoría previstas.
-

SEXTA. DEBER DE CONFIDENCIALIDAD

- 6.1.** El Encargado garantizará que todas las personas autorizadas para acceder a los datos personales o a los sistemas de información del Responsable estén sujetas al deber de confidencialidad, ya sea por obligación contractual o legal, manteniéndose dicha obligación incluso después de finalizar la relación contractual.
- 6.2.** El acceso a la información quedará limitado al personal estrictamente necesario para la prestación de los servicios contratados, conforme al principio de necesidad de conocer y mínimo privilegio.
- 6.3.** Salvo obligación legal o autorización previa y escrita del Responsable, el Encargado no comunicará ni pondrá los datos personales a disposición de terceros.
- 6.4.** El régimen aplicable al personal autorizado y a los compromisos de confidencialidad se desarrolla en el **Anexo IV** del presente contrato.
-

SÉPTIMA. MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

- 7.1.** El Encargado implantará y mantendrá las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, conforme al artículo 32 del Reglamento (UE) 2016/679.
- 7.2.** Dichas medidas estarán orientadas a preservar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas de información utilizados para la prestación de los servicios contratados.
- 7.3.** El Encargado aplicará, entre otras, medidas relativas a:
- Control de accesos y autenticación multifactor (AMF)
 - Protección de puestos de trabajo y servidores mediante soluciones de detección y respuesta (EDR)
 - Monitorización de eventos de seguridad (Centro de Operaciones de Seguridad)
 - Gestión de vulnerabilidades y aplicación de parches
 - Copias de seguridad cifradas y verificadas
 - Acceso remoto seguro mediante canales cifrados
 - Registro de actividades (logs) con retención mínima de 2 años
 - Gestión documentada de incidentes de seguridad
- 7.4.** El detalle de las medidas de seguridad aplicables figura en el **Anexo II**, que forma parte integrante del presente contrato.
-

OCTAVA. SUBENCARGADOS DEL TRATAMIENTO

- 8.1.** El Encargado no podrá recurrir a otro encargado para realizar tratamientos por cuenta del Responsable sin la autorización previa de éste, en los términos previstos en el artículo 28 del Reglamento (UE) 2016/679.
- 8.2.** Cuando exista autorización general, el Encargado informará previamente al Responsable de cualquier incorporación o sustitución de subencargados, permitiéndole formular oposición motivada cuando existan razones relacionadas con la protección de los datos personales.

8.3. Todo subencargado quedará vinculado mediante contrato escrito que imponga obligaciones equivalentes a las asumidas por el Encargado, especialmente en materia de confidencialidad, seguridad, asistencia al Responsable y destino de los datos al finalizar la prestación del servicio.

8.4. El Encargado responderá frente al Responsable del cumplimiento de las obligaciones asumidas por los subencargados que autorice.

8.5. El Responsable otorga autorización general al Encargado para recurrir a los subencargados relacionados en el **Anexo III**. La relación vigente se publica de forma permanente en ciberia28.ai/subencargados y en el Portal del Cliente, y se incorpora al presente contrato por referencia. El Encargado informará al Responsable con treinta (30) días naturales de antelación de toda incorporación, sustitución o cambio de ubicación de los datos, mediante comunicación individual al email designado y aviso en el Portal del Cliente. El Responsable podrá formular oposición motivada en razones de protección de datos dentro de dicho plazo; en tal caso el Encargado propondrá una alternativa razonable. La oposición no faculta a la resolución anticipada del contrato de servicios durante su periodo de permanencia.

NOVENA. ASISTENCIA AL RESPONSABLE DEL TRATAMIENTO

9.1. El Encargado prestará al Responsable la asistencia necesaria para el cumplimiento de las obligaciones derivadas de la normativa de protección de datos, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga.

9.2. Cuando el Encargado reciba directamente una solicitud de ejercicio de derechos presentada por un interesado, la remitirá al Responsable sin dilación indebida y, siempre que sea posible, dentro del plazo máximo de dos (2) días hábiles, absteniéndose de responder salvo autorización expresa o imposición legal.

9.3. El Encargado colaborará con el Responsable en la localización, rectificación, supresión, limitación, portabilidad o cualquier otra actuación técnica necesaria para atender dichas solicitudes.

9.4. Asimismo, prestará la asistencia razonablemente necesaria en materia de análisis de riesgos, evaluaciones de impacto, consultas previas ante la Agencia Española de Protección de Datos y demás obligaciones derivadas del Reglamento (UE) 2016/679.

DÉCIMA. BRECHAS DE SEGURIDAD DE LOS DATOS PERSONALES

10.1. El Encargado dispondrá de procedimientos documentados para la detección, análisis, contención, gestión y resolución de incidentes de seguridad que puedan afectar a los datos personales tratados por cuenta del Responsable.

10.2. Cuando tenga conocimiento de una brecha de seguridad, adoptará inmediatamente las medidas necesarias para limitar sus efectos, preservar las evidencias y reducir los riesgos para los derechos y libertades de las personas afectadas.

10.3. El Encargado notificará al Responsable cualquier brecha de seguridad sin dilación indebida y, en todo caso, dentro del plazo máximo de **veinticuatro (24) horas** desde que tenga conocimiento razonable del incidente, aportando la información disponible y completándola progresivamente.

10.4. La notificación incluirá, siempre que sea posible:

- Descripción del incidente y fecha de detección
- Sistemas afectados
- Categorías de datos e interesados afectados
- Medidas adoptadas de forma inmediata
- Valoración inicial del riesgo
- Persona de contacto designada para la gestión del incidente

10.5. El Encargado colaborará con el Responsable en la evaluación del incidente y en la preparación de la información necesaria para el cumplimiento de los artículos 33 y 34 del Reglamento (UE) 2016/679.

10.6. Salvo obligación legal o autorización expresa del Responsable, el Encargado no notificará directamente la brecha de seguridad a la Agencia Española de Protección de Datos ni a los interesados.

10.7. Una vez resuelto el incidente, el Encargado elaborará un informe de cierre con la cronología de los hechos, análisis de causa raíz, medidas correctoras adoptadas y recomendaciones para evitar incidentes similares.

UNDÉCIMA. COLABORACIÓN CON LA AUTORIDAD DE CONTROL

11.1. El Encargado colaborará con el Responsable para facilitar el cumplimiento de las obligaciones derivadas del RGPD y la LOPDGDD cuando intervenga la Agencia Española de Protección de Datos u otra autoridad de control competente.

11.2. Si el Encargado recibiera directamente cualquier requerimiento, solicitud de información o actuación inspectora relacionada con los tratamientos objeto del presente contrato, lo notificará al Responsable sin dilación indebida y, siempre que sea posible, dentro de las veinticuatro (24) horas siguientes a su recepción, salvo prohibición legal.

11.3. El Encargado facilitará la información y asistencia técnica razonablemente necesarias para atender los requerimientos de la autoridad de control.

DUODÉCIMA. AUDITORÍAS Y VERIFICACIÓN DEL CUMPLIMIENTO

12.1. El Encargado pondrá a disposición del Responsable la información necesaria para acreditar el cumplimiento de las obligaciones derivadas del presente contrato y de la normativa de protección de datos.

12.2. El Responsable podrá realizar, directamente o mediante un tercero independiente sujeto a deber de confidencialidad, auditorías o revisiones documentales proporcionadas al riesgo y a la naturaleza de los tratamientos realizados.

12.3. El Encargado facilitará la documentación y evidencias relacionadas con el tratamiento efectuado por cuenta del Responsable, sin que ello implique revelar información que afecte a otros clientes o constituya secreto empresarial ajeno al objeto de la verificación.

12.4. Cuando las actuaciones de verificación detecten incumplimientos relevantes, el Encargado adoptará las medidas correctoras necesarias e informará al Responsable de su implantación en un plazo razonable.

DECIMOTERCERA. FINALIZACIÓN DEL CONTRATO Y DESTINO DE LOS DATOS

13.1. Finalizado el contrato principal, el Encargado cesará en el tratamiento de los datos personales y procederá, conforme a las instrucciones del Responsable, a devolver o suprimir los datos personales y los soportes que los contengan, salvo obligación legal de conservación.

13.2. Cuando proceda la supresión, ésta se realizará mediante procedimientos que impidan la recuperación posterior de la información. Si el Responsable lo solicita, el Encargado emitirá certificación de destrucción o supresión.

13.3. En caso de existir obligación legal de conservación, el Encargado mantendrá exclusivamente los datos imprescindibles, debidamente bloqueados y protegidos, limitando su tratamiento al cumplimiento de dicha obligación.

13.4. La finalización del contrato no extinguirá las obligaciones de confidencialidad ni las responsabilidades derivadas de los tratamientos efectuados durante su vigencia.

DECIMOCUARTA. RESPONSABILIDAD

14.1. Cada parte responderá del cumplimiento de las obligaciones que le correspondan conforme al Reglamento (UE) 2016/679, la Ley Orgánica 3/2018 y el presente contrato, atendiendo a su condición de Responsable o Encargado del Tratamiento.

14.2. El Encargado responderá de los daños y perjuicios que resulten de los tratamientos realizados incumpliendo las instrucciones del Responsable, las obligaciones asumidas en este contrato o la normativa de protección de datos.

14.3. El Responsable responderá de la licitud del tratamiento, de la determinación de sus fines y de las instrucciones facilitadas al Encargado, así como de las obligaciones que la normativa atribuya exclusivamente al Responsable.

14.4. La responsabilidad del Encargado quedará limitada a los daños directos causados por incumplimiento imputable al mismo, con un máximo equivalente al importe total facturado en los doce (12) meses anteriores al incidente, salvo dolo o culpa grave.

DECIMOQUINTA. LEY APLICABLE Y JURISDICCIÓN

15.1. El presente contrato se rige por el Reglamento (UE) 2016/679 (RGPD), la Ley Orgánica 3/2018 (LOPDGDD) y la legislación española complementaria vigente en cada momento.

15.2. Para la resolución de cualquier controversia derivada del presente contrato, las partes se someten a los juzgados y tribunales de Las Palmas de Gran Canaria, con renuncia expresa a cualquier otro fuero que pudiera corresponderles.

DECIMOSEXTA. MODIFICACIONES Y DISPOSICIONES GENERALES

- 16.1.** Cualquier modificación del presente contrato requerirá acuerdo escrito firmado por ambas partes.
- 16.2.** Si alguna estipulación del presente contrato fuera declarada nula o ineficaz, las demás permanecerán plenamente válidas y eficaces.
- 16.3.** Todas las notificaciones previstas en el presente contrato se realizarán por escrito, a las personas de contacto designadas por cada parte en el **Anexo V**.
- 16.4.** El presente contrato, integrado por dieciséis (16) estipulaciones y cinco (5) anexos, constituye un único documento contractual que complementa el contrato principal de prestación de servicios.

FIRMAS

Las partes manifiestan haber leído íntegramente el presente contrato, comprender su contenido y aceptar expresamente todas y cada una de sus estipulaciones y anexos.

EL RESPONSABLE DEL TRATAMIENTO

[NOMBRE COMPLETO DEL CLIENTE]

Representante: D./Dña. [NOMBRE REPRESENTANTE] Cargo: [CARGO]

Firma: _____

Fecha: ____ / ____ / 20____

EL ENCARGADO DEL TRATAMIENTO

ELANTIA CANARIAS S.L.U. (Ciberia28)

Representante: D. Carlos Castillo Úbeda Cargo: Administrador Único

Firma: _____

Fecha: ____ / ____ / 20____

ANEXO I — CATEGORÍAS DE DATOS, INTERESADOS Y OPERACIONES AUTORIZADAS

1. Interesados cuyos datos pueden ser tratados

- ☐ Empleados y colaboradores del Responsable ☐ Clientes del Responsable ☐ Clientes potenciales ☐ Proveedores y suministradores
- ☐ Usuarios de sistemas de información ☐ Otros: _____

2. Categorías de datos personales

- ☐ Datos identificativos (nombre, apellidos, DNI/NIE) ☐ Datos de contacto (email, teléfono, dirección) ☐ Credenciales de usuario (usuarios, contraseñas cifradas) ☐ Direcciones IP e identificadores de dispositivos ☐ Registros de actividad (logs de sistemas) ☐ Datos contenidos en servidores y equipos ☐ Copias de seguridad ☐ Otros: _____

3. Categorías especiales de datos

- ☐ No previstas en el alcance del servicio ☐ Acceso únicamente de forma incidental e inevitable ☐ Tratamiento expresamente autorizado (especificar): _____

4. Operaciones de tratamiento autorizadas

- ☐ Acceso y consulta ☐ Monitorización y análisis técnico ☐ Diagnóstico y soporte remoto ☐ Mantenimiento y administración ☐ Copia de seguridad ☐ Restauración ☐ Supresión ☐ Otras: _____

ANEXO II — MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD

Medidas técnicas aplicadas por ELANTIA CANARIAS S.L.U.

Medida	Descripción
Cifrado en tránsito	TLS 1.3 en todas las comunicaciones
Cifrado en reposo	AES-256 en almacenamiento de datos
Autenticación multifactor	Obligatoria para acceso a sistemas de clientes
Principio de mínimo privilegio	Accesos limitados a lo estrictamente necesario
Protección de endpoints	Soluciones EDR en equipos del Encargado
Monitorización	Centro de Operaciones de Seguridad activo
Gestión de vulnerabilidades	Análisis periódico y aplicación de parches
Copias de seguridad	Cifradas, verificadas y con retención mínima 90 días
Acceso remoto	Exclusivamente mediante canales cifrados y autenticados
Registro de actividad	Logs conservados mínimo 2 años con control de integridad

Medidas organizativas aplicadas por ELANTIA CANARIAS S.L.U.

- Política de seguridad de la información documentada y actualizada
- Compromisos de confidencialidad suscritos por todo el personal
- Formación anual obligatoria en protección de datos y ciberseguridad
- Procedimiento documentado de gestión de incidentes y brechas de seguridad
- Control de accesos con revisión periódica y revocación inmediata al cese
- Acuerdos de encargo del tratamiento suscritos con todos los subencargados

ANEXO III — SUBENCARGADOS DEL TRATAMIENTO

El Responsable otorga autorización general para el uso de los siguientes subencargados. La relación vigente, con el detalle de país, ubicación de los datos, finalidad y garantías, se publica en ciberia28.ai/subencargados y en el Portal del Cliente, y prevalece sobre la presente tabla en caso de discrepancia por actualización posterior comunicada conforme a la Estipulación 8.5.

Subencargado	País	Ubicación de los datos	Servicio	Finalidad	Garantías
NinjaOne, LLC	EE. UU.	Unión Europea — AWS eu-central-1 (Frankfurt, Alemania)	CiberRecovery; gestión y monitorización de dispositivos	Copias de seguridad de servidores, equipos y Microsoft 365 / Google Workspace; inventario, parcheado y monitorización de dispositivos	Acuerdo de encargo con Cláusulas Contractuales Tipo (Decisión 2021/914, módulos 2 y 3) suscrito el 08/06/2026; EU-U.S. Data Privacy Framework; ISO 27001; SOC 2 Tipo 2. Sub-subencargados: ninjaone.com/approved-subprocessors
Bitdefender S.R.L.	Rumanía (UE)	Unión Europea	Protección de endpoints (EDR/XDR)	Detección y respuesta frente a amenazas en dispositivos; telemetría de seguridad	Entidad establecida en la UE; acuerdo de encargo del fabricante

Subencargado	País	Ubicación de los datos	Servicio	Finalidad	Garantías
CYREBRO (CyberHat Ltd.)	Israel	Israel / Unión Europea, conforme a su acuerdo de encargo	SOC 24/7	Correlación y análisis de registros de seguridad; gestión de alertas e incidentes	Decisión de adecuación de la Comisión Europea (Decisión 2011/61/UE); acuerdo de encargo enlazado en la Condición 6bis.1 de las Condiciones Generales
ORIZON CYBER SECURITY S.L.	España (UE)	Unión Europea	SOC 24/7	Analistas de seguridad; operación del servicio SOC	Entidad establecida en la UE; contrato de encargo
Cloudflare, Inc.	EE. UU.	Red global de Cloudflare; datos del Portal del Cliente e informes en Cloudflare D1/R2/KV	Portal del Cliente	Alojamiento, almacenamiento de informes y contratos, seguridad perimetral	Acuerdo de encargo de Cloudflare con Cláusulas Contractuales Tipo; EU-U.S. Data Privacy Framework
Google Cloud EMEA Limited	Irlanda (UE)	Unión Europea / Estados Unidos (infraestructura global de Google Workspace)	Comunicaciones	Correo y ofimática corporativa del Encargado (Google Workspace) por los que transitan comunicaciones e informes	Google Cloud Data Processing Addendum con Cláusulas Contractuales Tipo; EU-U.S. Data Privacy Framework
Resend, Inc.	EE. UU.	EE. UU. / Unión Europea según región del servicio	Portal del Cliente	Envío de correos transaccionales del Portal (avisos, informes)	Acuerdo de encargo con Cláusulas Contractuales Tipo

Los dispositivos NAS, tenants de Microsoft 365 / Google Workspace y demás infraestructura de titularidad del Responsable integrados en los servicios no constituyen subencargados del Encargado.

Cualquier incorporación, sustitución o cambio de ubicación será comunicado al Responsable con un mínimo de **treinta (30) días** de antelación conforme a la Estipulación 8.5.

ANEXO IV — PERSONAL AUTORIZADO Y CONTROL DE ACCESOS

1. Principios generales

El Encargado garantizará que el personal con acceso a datos del Responsable:

- Haya firmado un compromiso de confidencialidad
- Haya recibido formación adecuada en protección de datos
- Disponga únicamente de los permisos estrictamente necesarios
- Tenga revocado el acceso de forma inmediata al cesar su relación con el Encargado

2. Control de accesos

- Los accesos se gestionarán mediante un sistema de control con registro de altas, modificaciones y bajas
- Se aplicará autenticación multifactor para cualquier acceso a sistemas o datos del Responsable
- Los accesos remotos se realizarán exclusivamente mediante mecanismos seguros y registrados
- Se conservarán registros de acceso durante un mínimo de dos (2) años

3. Dispositivos y medios

- El personal autorizado utilizará exclusivamente dispositivos, herramientas y credenciales autorizados por el Encargado
- Queda prohibido el uso de dispositivos personales no autorizados para acceder a datos del Responsable
- Los dispositivos estarán protegidos con cifrado y soluciones de protección de endpoints

ANEXO V — FICHA DE CONTROL DEL ENCARGO DEL TRATAMIENTO

(Documento de control contractual y operativo)

1. Identificación del encargo

Concepto	Información
Responsable del Tratamiento	[NOMBRE COMPLETO DEL CLIENTE]
Encargado del Tratamiento	ELANTIA CANARIAS S.L.U., CIF B22913412 (marca comercial Ciberia28)
Contrato principal	Contrato de Prestación de Servicios de Ciberseguridad
Fecha de inicio	_____
Fecha de finalización	_____
Responsable interno (cliente)	_____
Responsable técnico (ELANTIA CANARIAS S.L.U.)	_____
Email de contacto (cliente)	_____
Email de contacto (ELANTIA CANARIAS S.L.U.)	privacidad@ciberia28.ai

La **Ficha de encargo del tratamiento** de cada Responsable (servicios contratados, subencargados aplicables, ubicación de las copias, retención y versión vigente de este Anexo) se genera y descarga desde el Portal del Cliente, y constituye el documento acreditativo previsto en el artículo 28.3.h) del RGPD.

2. Servicios contratados

(Marcar los servicios efectivamente contratados)

Servicio	Sí	No
Monitorización de seguridad (Centro de Operaciones de Seguridad)	☐	☐
Protección avanzada de equipos (EDR)	☐	☐
Gestión de vulnerabilidades	☐	☐
Administración de soluciones de seguridad	☐	☐
Soporte técnico remoto	☐	☐
Soporte presencial	☐	☐
Gestión de copias de seguridad	☐	☐
Recuperación de sistemas	☐	☐
Respuesta ante incidentes	☐	☐
Otros (especificar)	☐	☐

3. Gestión de brechas de seguridad

Concepto	Valor
Plazo máximo de notificación al Responsable	24 horas desde conocimiento del incidente
Canal de comunicación	privacidad@ciberia28.ai / +34 922 27 80 11 (horario laboral)

Concepto	Valor
Persona de contacto en ELANTIA CANARIAS S.L.U.	D. Carlos Castillo Úbeda

4. Destino de los datos al finalizar el contrato

☐ Devolución al Responsable ☐ Supresión segura con certificación ☐ Conservación por obligación legal (especificar plazo y base legal)

Según instrucciones del Responsable y conforme a la Estipulación Decimotercera.

5. Revisiones del contrato

Fecha	Motivo	Responsable

El presente contrato, integrado por dieciséis (16) estipulaciones y cinco (5) anexos, es obligatorio conforme al artículo 28 del Reglamento (UE) 2016/679 y debe ser firmado antes del inicio de cualquier tratamiento de datos personales por parte del Encargado.

Versión: 2.0 — Agosto 2026