ANEXO II — CONTRATO DE ENCARGADO DEL TRATAMIENTO DE DATOS PERSONALES Y SEGURIDAD DE LA INFORMACIÓN (ATD)

El presente Anexo forma parte integrante del Contrato de Servicios de Gestión Documental (pack suministrador) y tiene por objeto regular el tratamiento de datos personales que Nalanda realiza por cuenta del Cliente en el marco del Contrato.

A estos efectos, Nalanda tratará los datos personales únicamente en la medida necesaria para la prestación del Servicio y conforme a las instrucciones documentadas del Cliente, de acuerdo con lo establecido en la normativa aplicable en materia de protección de datos personales y en las cláusulas que se desarrollan a continuación.

La formalización del Contrato de Servicios de Gestión Documental implicará la aceptación expresa y la adhesión del Cliente al presente Acuerdo de Tratamiento de Datos Personales, formando ambos documentos un conjunto contractual único y vinculante.

Cláusulas

1. Objeto.- Con el fin de dar cumplimiento a la normativa de Protección de Datos Personales, principalmente, al 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 ("**RGPD**"), ambas partes acuerdan que el presente Anexo II "*Contrato de Encargado del Tratamiento de Datos Personales y Seguridad de la Información*", incorporado al Acuerdo de Suscripción entre el CLIENTE y NALANDA (el "**Contrato**") y del que forma parte integrante, que regirá el tratamiento de los datos personales a los que NALANDA tenga acceso para la prestación de los servicios contratados por el CLIENTE de conformidad con el Contrato.

   A estos efectos, el CLIENTE tendrá la consideración de responsable del tratamiento ("**Responsable del Tratamiento**") y NALANDA la de encargado del tratamiento ("**Encargado de Tratamiento**").

2. Categorías de interesados y tipologías de datos objeto de tratamiento por NALANDA por cuenta del CLIENTE para la prestación de los servicios contratados

   a. *Categorías de interesados*: Empleados del Cliente y/o de sus subcontratistas, sus representantes legales, socios o accionistas y usuarios web.

   b. *Tipologías de datos*. La tipología de datos que tratará el Encargado del Tratamiento y/o los subencargados (si es el caso) por cuenta del Responsable del Tratamiento para prestar los servicios contratados son las siguientes: datos de carácter identificativo (como el nombre y apellidos, DNI o documento de identificación equivalente, número de seguridad social, firma), datos de contacto (como el domicilio, correo electrónico, teléfono, etc.), datos profesionales o de empleo (como los datos curriculares, vida laboral), datos económicos y/o financieros (como la nómina, cuenta bancaria, solvencia patrimonial) y, en su caso, datos biométricos.

c. *Tratamientos*. Los tratamientos que se harán por el Encargado o subencagados variará en función de la categoría de interesados a que se refiera, siendo los mismos: la estructuración, conservación, consulta, comparación, interconexión, comunicación y, en su caso, destrucción.

En cualquier caso, NALANDA no podrá tratar los datos para finalidades diferentes de la prestación de los servicios contratados y el cumplimiento de sus obligaciones legales y contractuales.

3. Obligaciones de NALANDA como Encargado del tratamiento

NALANDA asume las siguientes obligaciones:

- Acceder a los datos personales responsabilidad del Responsable del Tratamiento cuando sea necesario para la prestación de los servicios para los que ha sido contratado.

- Tratar los datos conforme a las instrucciones que reciba del Responsable del Tratamiento.

- Llevar un registro de las categorías de actividades de tratamiento efectuadas por cuenta del responsable.

- En el caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del Responsable del Tratamiento, NALANDA deberá seguir los procedimientos e instrucciones que reciba de aquél, especialmente en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados.

- Si NALANDA considera que alguna de las instrucciones del Responsable del Tratamiento infringe el RGPD o cualquier otra disposición en materia de protección de datos de la Unión o de los Estados miembros, le informará inmediatamente de ello.

- No revelar, transferir, ceder o de otra forma comunicar los datos personales responsabilidad del Responsable del Tratamiento a ningún tercero, salvo que exista autorización o instrucción del Responsable del Tratamiento.

- Garantizar que las personas autorizadas para tratar datos personales se comprometan, de forma expresa y por escrito, a respetar la confidencialidad y a cumplir las medidas de seguridad correspondientes, de las que hay que informarles convenientemente.

- Poner a disposición del Responsable del Tratamiento la información necesaria para demostrar el cumplimiento de sus obligaciones, así como para permitir y/o contribuir a la realización de auditorías en caso de violación de los datos personales por incumplimiento de las obligaciones del Encargado de Tratamiento.

- Adoptar y aplicar las medidas de seguridad estipuladas en el Apéndice A del presente Anexo conforme a lo previsto en el artículo 32 del RGPD, dirigidas a garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que estén expuestos, ya provengan de la acción humana o del medio físico o natural.

- En caso de que NALANDA deba transferir o permitir acceso a datos personales responsabilidad del Responsable del Tratamiento a un tercero en virtud del Derecho de la Unión o de los Estados miembros que le sea aplicable, informará al Responsable del Tratamiento de esa exigencia legal de manera previa, salvo que estuviese prohibido por razones de interés público.

4. Obligaciones del Responsable del Tratamiento

El Cliente y/o su subcontratista en su condición de Responsable del Tratamiento manifiesta y hace constar a los efectos legales oportunos que:

- En caso de que el tratamiento incluya la recogida de datos personales en nombre y por cuenta del Responsable del Tratamiento, establecerá los procedimientos correspondientes a la recogida de los datos, especialmente en lo relativo al deber de información y, en su caso, la obtención del consentimiento de los afectados, garantizando que estas instrucciones cumplen con todas las prescripciones legales y reglamentarias que exige la normativa vigente en materia de protección de datos.

- En caso de que el tratamiento no incluya la recogida de datos personales en nombre y por cuenta del Responsable del Tratamiento, los datos personales a los que accederá NALANDA en virtud del Contrato, han sido obtenidos y tratados cumpliendo con todas las prescripciones legales y reglamentarias que exige la normativa vigente en materia de protección de datos.

- Cumple con todas sus obligaciones en materia de protección de datos como responsable del tratamiento y es consciente de que los términos del presente Anexo en nada alteran ni sustituyen las obligaciones y responsabilidades que le sean atribuibles como responsable del tratamiento.

- La información que sube a la Plataforma es verdadera y no contine errores. En caso de existencia de errores en la información subida a la Plataforma, o de otro modo facilitada al Encargado del Tratamiento, se compromete a subsanarlos de inmediato.

- Si fuera aplicable, recabará los consentimientos explícitos y específicos de los interesados para el tratamiento de sus datos personales con fines de marketing, conforme a lo establecido en el RGPD y la LOPDGDD, y lleva un registro actualizado de los consentimientos obtenidos para aquellos fines.

- Indemnizará y mantener indemne al Encargado del Tratamiento frente a cualquier reclamación, sanción, multa, perdida o daño que pueda sufrir como consecuencia de una acción u omisión del Responsable del Tratamiento.

5. Medidas de seguridad y violación de la seguridad

Teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, NALANDA aplicará medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- la seudonimización y el cifrado de datos personales;
- la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento, así como la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico.
- un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Al evaluar la adecuación del nivel de seguridad, NALANDA tendrá en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Se adjuntan como **Apéndice A** las *medidas técnicas y organizativas de seguridad de la información adoptadas por NALANDA* conforme a lo dispuesto anteriormente y como **Apéndice B** el *acuerdo de interconexión de sistemas de seguridad de la información*, según lo previsto en el Real Decreto 311/2022, por el que regula el Esquema Nacional de Seguridad.

En caso de violación de la seguridad de los datos personales en los sistemas de información utilizados por NALANDA para la prestación de los servicios objeto del Contrato, NALANDA deberá notificar al Responsable del Tratamiento, sin dilación indebida, y en cualquier caso antes del plazo máximo de 72 horas, las violaciones de la seguridad de los datos personales a su cargo de las que tenga conocimiento, juntamente con toda la información relevante para la documentación y comunicación de la incidencia conforme a lo dispuesto en el artículo 33.3 del RGPD.

En tal caso, corresponderá al Responsable del Tratamiento comunicar las violaciones de seguridad de los datos a la Autoridad de Protección de Datos y/o a los interesados conforme a lo establecido en la normativa vigente.

6. Destino de los datos al finalizar el Contrato.

Una vez cumplida o resuelta la relación contractual entre el CLIENTE y NALANDA, aquél tendrá la facultad de extraer de la Plataforma los datos personales sobre los que ostente la condición de responsable del tratamiento. También podrá solicitar a NALANDA como

alternativa su destrucción, salvo que exista previsión legal que exija la conservación de los datos.

No obstante, NALANDA podrá conservar, debidamente bloqueados, los datos de carácter personal responsabilidad del Responsable del Tratamiento, en tanto pudieran derivarse responsabilidades de su relación con él.

7. Ejercicio de derechos ante NALANDA

NALANDA deberá dar traslado al Responsable del Tratamiento de cualquier solicitud de ejercicio del derecho de acceso, rectificación, supresión y oposición, limitación del tratamiento, portabilidad de los datos y a no ser objeto de decisiones individualizadas automatizadas, efectuada por un afectado cuyos datos hayan sido tratados por NALANDA en cumplimiento del Contrato, a fin de que se atienda por el Responsable del Tratamiento en los plazos establecidos por la normativa vigente.

El traslado de la solicitud al Responsable del Tratamiento deberá hacerse con la mayor celeridad posible y en ningún caso más allá del día laborable siguiente al de la recepción de la solicitud, juntamente, en su caso, con aquella otra información que pueda ser relevante para resolver la solicitud.

8. Subcontratación.

NALANDA está autorizada a subcontratar todo o parte de los servicios contratados por el CLIENTE en que se efectúe tratamiento de datos personales, siempre que informe de ello con una antelación de 15 días, a través de la actualización del listado de subencargados que se adjunta a este anexo como **Apéndice C** ("*Lista de Subencargados*"), indicando los tratamientos que se pretenden subcontratar e identificando de forma clara e inequívoca la empresa subcontratista, su localización y sus datos de contacto. La subcontratación podrá llevarse a cabo si el Responsable del Tratamiento no manifiesta su oposición en el plazo establecido de 15 días.

Transferencias internacionales y subencargados fuera del Espacio Económico Europeo (Reino Unido y países terceros)

Sin perjuicio de lo previsto en el presente Anexo, cuando para la prestación de los Servicios resulte necesario transferir o permitir el acceso a datos personales a entidades ubicadas fuera del Espacio Económico Europeo:

(a) **Reino Unido (servicio Precalificación y/o de Marketplace – Artio).**
El Cliente autoriza expresamente el acceso y tratamiento de datos personales en el Reino Unido por parte de la entidad del Grupo Once For all Limited, LTD que opera técnicamente la plataforma Artio, en su condición de subencargado del tratamiento. A la fecha de firma, las transferencias al Reino Unido se amparan en la Decisión de Adecuación de la Comisión Europea de 28/06/2021, por lo que no requieren garantías adicionales mientras dicha decisión permanezca vigente. Nalanda mantendrá un registro actualizado de dicho subencargado en el Apéndice C y comunicará cualquier cambio conforme al procedimiento de notificación de subencargados.

(b) Terceros países sin decisión de adecuación

Cuando el subencargado se ubique en un tercer país sin decisión de adecuación, Nalanda suscribirá con el importador de los datos las Cláusulas Contractuales Tipo (SCC) 2021/914/UE en el módulo aplicable y aplicará, cuando proceda, medidas suplementarias técnicas y organizativas, de conformidad con la evaluación de impacto de transferencias (TIA), manteniendo dicha documentación a disposición del Responsable.

(c) Principios comunes.
En todos los supuestos, Nalanda: (i) limitará el acceso a los datos a lo estrictamente necesario para la prestación del servicio; (ii) exigirá al subencargado obligaciones equivalentes a las de este ATD; (iii) verificará que el subencargado aplica medidas técnicas y organizativas adecuadas; y (iv) informará al Responsable de cualquier cambio en la Lista de Subencargados (Apéndice C) con al menos 15 días de antelación para que pueda oponerse en los términos establecidos

9. Responsabilidad.

NALANDA, en relación con el presente encargo de tratamiento, se compromete a cumplir con las obligaciones establecidas en este Anexo y en la normativa vigente.

Las Partes responderán de las infracciones cometidas por cada una de ellas. No obstante, se obligan a mantenerse indemnes por aquellos daños y/o perjuicios que sufran como consecuencia de un incumplimiento por la otra parte de sus obligaciones como encargado o responsable del tratamiento, según el caso. A tal efecto, la parte incumplidora acepta indemnizar a la otra en la cantidad en que sea condenada en concepto de sanción, multa, principal e intereses, así como cualquier otro daño o perjuicio directo. Nalanda no responderá en ningún caso, de forma acumulada, por una cuantía mayor a los importes efectivamente cobrados al Cliente en el periodo de los últimos 12 meses.

APÉNDICE A

Medidas técnicas y organizativas de seguridad de la información

I. MEDIDAS TÉCNICAS Y ORGANIZATIVAS DE SEGURIDAD DE LA INFORMACIÓN

El Grupo NALANDA (integrado por Nalanda Global, CTGA, Construred, Areaseys y Dokify) es un grupo líder en software colaborativo para gestión de riesgos de la cadena de suministro y subcontratación, y cumplimiento normativo en materia de seguridad, salud en el trabajo y sostenibilidad empresarial. NALANDA es consciente de que la información es un activo fundamental así como la dependencia de sus servicios de los sistemas y tecnologías de información y comunicaciones para alcanzar los objetivos del negocio.

Por todo ello, el Grupo Nalanda establece a través de su Dirección y de su Comité de Gobierno de Seguridad un Sistema de Gestión de Seguridad de la Información conforme a la norma **ISO/IEC 27001:2022**, aplicando las mejores prácticas internacionales, además de la regulación normativa y legislativa vigente en materia de Seguridad de la Información.

Asimismo, la entidad da pleno cumplimiento a la normativa vigente en materia de seguridad, específicamente, el Real Decreto 311/2022, de 3 de mayo, por el que se regula el **Esquema Nacional de Seguridad.**

El Grupo Nalanda se ha adaptado también a la **NIS2 - Directiva (UE) 2022/2555** del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión.

La Política y Normas de Seguridad de la Información son observadas por el personal del Grupo Nalanda en España y sus filiales internacionales, así como transmitidas a sus colaboradores y proveedores, estando a disposición de cualquier persona que muestre interés por ella. El marco normativo de seguridad está a disposición de todos los implicados en su cumplimiento.

II. MEDIDAS DE SEUDONIMIZACIÓN Y CIFRADO DE LOS DATOS PERSONALES

Las comunicaciones con la plataforma puesta a disposición por el Grupo Nalanda, así como los dispositivos utilizados en las instalaciones de la entidad y el almacenamiento de los datos de la plataforma se encuentran cifrados. Se detallan a continuación algunas de las medidas:

- Almacenamiento de datos en reposo con cifrado en BBDD, discos e Infraestructura.
- Sistema de encriptación y segmentación del dato en reposo y en tránsito.
- Uso de VPN de ultima generación basada en Zero Trust Security para las comunicaciones remotas.
- Equipos personales con cifrado de disco y Hardening de Seguridad en el plataformado.

- Política de Criptología alineada con Normativas de seguridad nacionales, Europeas e internacionales.

III. MEDIDAS PARA GARANTIZAR LA CONFIDENCIALIDAD, INTEGRIDAD, DISPONIBILIDAD Y RESILIENCIA PERMANENTE EN LOS SISTEMAS.

La organización dispone de procedimientos de copias de seguridad y un Plan de Continuidad de negocio que incluye:

- Realización de copias de seguridad estableciendo una redundancia para toda la información contenida de respaldo, con la periodicidad y retención oportunas que garantizan la disponibilidad de la información.
- Plan de Continuidad de negocio documentado con todos los procesos considerados críticos, un análisis de riesgos y un BIA. Estos planes contienen la comunicación entre las partes participantes e interno a sus empleados, la referencia a los procedimientos de actuación, etc.
- Se realizan pruebas de Continuidad de negocio una vez al año para comprobar el estado de madurez de los escenarios del BIA.

IV. MEDIDAS PARA RESTAURAR LA DISPONIBILIDAD Y EL ACCESO A LOS DATOS PERSONALES DE FORMA RÁPIDA EN CASO DE INCIDENTE DE SEGURIDAD.

- Los eventos de seguridad de la información y ciberseguridad son monitorizados 24x7 mediante los servicios de vigilancia y monitorización de un CSOC.
- Se dispone de un Plan de Ciberresiliencia que contempla un DFIR, un Plan de Comunicación y protocolos de respuesta específicos antes incidentes complejos.
- El Grupo Nalanda dispone de un Comité de Crisis de incidentes de Ciberseguridad.
- Tanto el CISO como la Oficina de Seguridad de la Información y Ciberseguridad dispone de contacto directo con los organismos oficiales del Estado en la comunicación de un incidente.
- El Grupo Nalanda se compromete a notificar a los clientes cualquier incidente de Seguridad relacionada con la perdida de datos personales del CLIENTE en un plazo de 48 a 72 horas. En el caso de que exista interconexión de algún sistema del Grupo Nalanda y el cliente , el cliente se compromete a notificar al Grupo Nalanda cualquier incidente de Seguridad que pueda afectar a la integridad, disponibilidad y confidencialidad de la información del Grupo Nalanda en un plazo de 24 a 48 horas.

V. PROCESOS DE VERIFICACIÓN, EVALUACIÓN Y VALORACIÓN REGULAR DE LA EFICACIA DE LAS MEDIDAS TÉCNICAS Y ORGANIZATIVAS PARA GARANTIZAR LA SEGURIDAD DEL TRATAMIENTO

- Se realiza auditorias técnicas anuales de pentesting y/o hacking Ético en las plataformas web y en la infraestructura mediante un proveedor externo e independiente. El Grupo Nalanda pone a disposición de los clientes sus certificados de conformidad de la auditoria técnica externa. Este certificado conforma que las plataformas web no tienen vulnerabilidades criticas o altas.
- El Grupo Nalanda se compromete a solucionar las vulnerabilidades lo antes posible.
- Se realizan 6 auditorías anuales internas y externas de Seguridad de la información según la norma ISO9001, ISO27001:2022, Esquema Nacional de Seguridad (ENS) y el PCE NIS2 mediante un proveedor externo e independiente.
- El Grupo Nalanda pone a disposición de sus clientes sus certificados de conformidad de las normativas y leyes vigentes en Seguridad de la Información y Ciberseguridad.

VI. MEDIDAS PARA LA IDENTIFICACIÓN Y AUTORIZACIÓN DEL USUARIO

- Los usuarios del Grupo Nalanda son únicos e intransferibles, todos los usuarios están creados bajo el principio del mínimo privilegio y con una fuerte Política de gestión de contraseñas que regula la complejidad y el formato de los usuarios y sus contraseñas.
- Todos los usuarios están identificados y controlados mediante la aplicación de Políticas basadas en 30-60-90 que regula la inhabilitación de los usuarios por inactividad y regula el cambio periódico de contraseñas impidiendo la repetición.
- La segregación del sistema de control de acceso se organiza de forma que se exige la concurrencia de dos o más personas para realizar tareas críticas, anulando la posibilidad de que un solo individuo autorizado, pueda abusar de sus derechos de administración para cometer alguna acción ilícita.
- Los accesos de los usuarios están restringidos mediante un sistema de gestión de identidades, con Security group, políticas de autenticación y autorización y accesos con Doble factor de autenticación.
- Se generan trazas de todos los eventos y todos los usuarios están monitorizados y vigilados mediante el servicio 24x7 que nos otorga el CSOC.

VII. MEDIDAS PARA LA PROTECCIÓN DE LA INFRAESTRUCTURA Y ENTORNO DE USUARIO.

- El Grupo Nalanda cuenta con medidas de seguridad tecnológicas en su Perímetro Cloud, mediante sistemas WAF, Firewall, IDS/IPS, medidas Anti DDoS y sistemas avanzados de XDR con detección de Zero Days vulnerability.

- Se dispone de medidas de seguridad tecnológicas en el entorno de oficina mediante Firewall dedicado en la protección de la infraestructura de oficina y protección del usuario.

- Se dispone de medidas tecnológicas en el entorno de usuario desplegadas en los dispositivos personales de los empleados, con fuertes políticas de autorización basada en el mínimo privilegio y mediante sistemas tecnológicos con capacidades de Detección, monitorización, Bloqueo y respuesta al malware o a cualquier acción no permitida según las Políticas y Normas de Seguridad de la información del Grupo Nalanda.

- Todos los eventos y elementos de infraestructura, tecnología de seguridad, entorno de oficina y entorno de usuario se encuentra vigilado y monitorizado mediante el servicio 24x7 que nos otorga el CSOC.

VIII. MEDIDAS PARA GARANTIZAR LA SEGURIDAD FÍSICA

- El Grupo Nalanda cuenta con una Política y Normas de seguridad física en sus instalaciones cumpliendo con todos los controles marcados en la norma ISO27001:2022, el Esquema Nacional de Seguridad (ENS) y la Directiva NIS2 Europea.

IX. MEDIDAS DE GOBERNANZA Y GESTIÓN DE LA INFORMÁCIÓN Y LA SEGURIDAD

- El Grupo Nalanda cuenta con la figura de un CISO cuya finalidad es velar por el cumplimento normativo de seguridad de la Información y Ciberseguridad y velar por la protección de la compañía.

- Se dispone de una Oficina de Seguridad de la Información y Ciberseguridad con un equipo dedicado.

- Se dispone de un Comité de Gobierno de Seguridad con periodicidad mensual.

- El Grupo Nalanda dispone de un completo marco normativo interno y un sistema de gestión de Seguridad de la Información que da soporte a toda la actividad de negocio cumpliendo así con las normativas Nacionales, Europeas e internacionales.

X. MEDIDAS PARA GARANTIZAR LA TRANSFERENCIA EN LA INTERCONEXION.

- El Grupo Nalanda dentro de su **Anexo 1,** en la interconexión de sistemas vía API

describe las medidas necesarias y requisitos de interconexión dando así cumplimiento al **Real Decreto 311/2022** que regula el Esquema Nacional de Seguridad (ENS) y a la Directiva NIS2 Europea.

XI. MEDIDAS PARA GARANTIZAR EL DESARROLLO SEGURO

- Se dispone de una Política y Normas de desarrollo seguro contemplando la seguridad en todas las fases del desarrollo tanto en su planteamiento y definición hasta la puesta en producción de los servicios.
- Se disponen de herramientas de análisis de seguridad de código estático y dinámico.
- Existe segregación de los entornos de desarrollo, preproducción y producción.

XII. MEDIDAS PARA GARANTIZAR LA FORMACIÓN Y LA CONCIENCIACIÓN

- El Grupo Nalanda con su fuerte compromiso por la Seguridad de la Información dispone de un Plan de Formación y capacitación para todos los empleados, este plan se contempla desde el proceso de Onboarding de todos los empleados que trabajan en el Grupo.

XIII. MEDIDAS PARA PERMITIR LA PORTABILIDAD DE LOS DATOS Y GARANTIZAR LA SUPRESIÓN

- El Grupo Nalanda cuenta con un procedimiento de portabilidad de los datos que permite a un cliente que finaliza su servicio, disponer de toda su información.
- Se dispone de procedimientos específicos en la destrucción y borrado seguro de la información, así como de los dispositivos. Se emiten certificados de borrado seguro y destrucción.

APÉNDICE B
Medidas técnicas de Ciberseguridad en la interconexión de sistemas

I. Grupo Nalanda da cumplimento a los requerimientos del acuerdo de interconexión de sistemas de seguridad de la información establecido por el Real Decreto 311/2022, que regula el Esquema Nacional de Seguridad ("ENS"),

II. El ENS establece principios mínimos a los que Grupo Nalanda da cumplimiento, a saber: mínimo privilegio, nodo auto protegido, despliegue mínimo, definiciones y aplicabilidad, API, endpoint y token de autenticación.

III. Responsabilidad de las partes:

- Con el fin de poder prestar los servicios contratados de manera segura y acorde con la normativa de seguridad aplicable, incluido el ENS, en función de las especificaciones del Contrato y posibilidades técnicas del Cliente, NALANDA proveerá acceso a su plataforma mediante su interfaz Web y su API. Asimismo, mantendrá la documentación actualizada de su API y asegurará el tiempo de actividad y la disponibilidad de la API.

- En el caso de que el CLIENTE haya solicitado en el Contrato el uso de los servicios de API para el acceso a la plataforma de Nalanda, el CLIENTE se compromete a hacer un uso adecuado y responsable de mismos, con sujeción a lo establecido en el Contrato. El CLIENTE también se compromete a mantener la seguridad y confidencialidad de las claves de acceso proporcionadas, a mantener y llevar a cabo las oportunas evaluaciones de riesgo y de seguridad periódicas para identificar y corregir vulnerabilidades en los sistemas interconectados.

- El CLIENTE se obliga a mantener indemne a NALANDA frente a cualquier reclamación, multa, sanción, daño o perjuicio que sufra y tenga su causa en el incumplimiento por parte del CLIENTE de lo dispuesto en este Anexo (y sus apéndices) y/o en la normativa aplicable.

IV. Las *especificaciones técnicas* con las que NALANDA cuenta son las siguientes:

- La interconexión se realizará en formato Web o mediante la API REST publicada destinada a proporcionar una interfaz programable con la plataforma.

- La arquitectura de protección de perímetro será acorde a los requerimientos del Centro Criptológico Nacional en su guía sobre las interconexiones CCN-STIC 811.

- La comunicación se realizará siempre de manera segura, para ello se utilizará el protocolo de seguridad TLS, aportando autenticación, encriptación e integridad en los datos transferidos. La versión de TLS y la suite criptográfica a utilizar serán las autorizadas y consideradas robustas por el Centro Criptológico Nacional español en su guía CCN-STIC-807.

- Se dispondrá de una documentación web en la que se encontrarán descritos los endpoints, el método utilizado (GET, POST, PUT o DELETE), el formato de datos (JSON), así como sus parámetros y tipos de respuesta.

V. *Procedimientos operativos de seguridad*: NALANDA se reserva el derecho de implementar y ajustar medidas de limitación de ejecuciones ("*rate limits*") a su discreción, con el fin de proteger la estabilidad y el rendimiento del servicio. Estas limitaciones podrán ser aplicadas de manera automática o manual, sin previo aviso.

NALANDA se reserva el derecho de cortar el servicio si el CLIENTE no cumple con las especificaciones establecidas en el Contrato, sus anexos y/o apéndices.

APENDICE C
Lista de subencargados del tratamiento

A continuación, se relaciona la lista de los principales proveedores en quienes concurre la condición de subencargados del tratamiento, en relación con los datos personales tratados por Nalanda por cuenta del Cliente:

Subencargado	Servicio	Ubicación
Amazon Web Services EMEA SARL (AWS)	Hosting e infraestructura cloud de la Plataforma	**UE (principal)**
DoIT International	Optimización/gestión multi-cloud	**UE / España**
Once For all Limited, LTD[1]	Operación técnica del servicio Precalificación y validación documental asociado – Plataforma Artio	**Reino Unido**
Once For all Limited, LTD[2]	Operación técnica del servicio Marketplace – Plataforma Artio	**Reino Unido**

[1] La operación técnica de Precalificación se realiza en el Reino Unido por la entidad del Grupo identificada como Once For all Limited, LTD, actuando como subencargado para el tratamiento exclusivo de datos vinculados al módulo Précalificación. La prestación contractual frente al Cliente corresponde a Nalanda Global, S.A., que asume la coordinación, facturación y soporte de primer/segundo nivel. (Véase también el clausulado principal del Acuerdo de Suscripción y el Anexo de Servicios).

[2] La operación técnica de Marketplace se realiza en el Reino Unido por la entidad del Grupo identificada como Once For all Limited, LTD, actuando como subencargado para el tratamiento exclusivo de datos vinculados al módulo Marketplace. La prestación contractual frente al Cliente corresponde a Nalanda Global, S.A., que asume la coordinación, facturación y soporte de primer/segundo nivel. (Véase también el clausulado principal del Acuerdo de Suscripción y el Anexo de Servicios).