

Expediente Nº. LICIT/99/139/2025/0207

Pliego de Prescripciones Técnicas para la Contratación del suministro de licencia a una plataforma web de neurorrehabilitación para los Hospitales de FREMAP, Mutua Colaboradora con la Seguridad Social nº 61

ÍNDICE

1. OBJETO	3
2. NORMATIVA DE CARÁCTER TÉCNICO	3
3. ALCANCE DEL SUMINISTRO	3
4. EJECUCIÓN DEL SUMINISTRO	3
4.1 Implantación	6
4.2 Formación	6
4.3 Soporte técnico	7
5. RESPONSABLE DEL CONTRATO	7
5.1 Medios humanos	7
5.2 Gestion de incidencias	7
6. MANTENIMIENTO	8
6.1 Mantenimiento rectificativo	8
6.2 Mantenimiento evolutivo	8
7. PREVENCIÓN DE RIESGOS LABORALES	8
8. SEGURIDAD DE LA INFORMACIÓN	8
9. NORMATIVA INTERNA EN MATERIA DE INTELIGENCIA ARTIFICIAL PARA PROVEEDORES	19

1. OBJETO

El objeto del presente contrato es la adquisición e implementación de un programa integral de suministro de una licencia de neurorrehabilitación basada en una plataforma tecnológica, diseñada para dar soporte a los profesionales con material de tratamiento y entrenamiento de funciones cognitivas y mejorar, con ello, la calidad de vida de las personas con discapacidad intelectual, permitiendo:

- Estimulación cognitiva a través de intervenciones personalizadas.
- Gestión automatizada de métricas y evolución.
- Adaptación a perfiles clínicos personalizados mediante algoritmos inteligentes.

2. NORMATIVA DE CARÁCTER TÉCNICO

El licitador queda obligado al cumplimiento de lo dispuesto en la Ley 9/2014, de 9 de mayo, General de Telecomunicaciones, en la Ley Orgánica 3/2018 de 5 de Diciembre, de Protección de Datos Personales y garantía de los derechos digitales, necesarias para garantizar la seguridad y confidencialidad de los datos.

Esta clasificación normativa no tiene carácter restrictivo, debiendo observarse en la ejecución de los trabajos cualquier otro tipo de reglamento, norma o instrucción oficial (de carácter estatal, autonómico o municipal) que, aunque no se mencione explícitamente en este documento, pueda afectar al objeto del contrato, así como las posibles modificaciones legales que puedan afectar a las normas de aplicación.

3. ALCANCE DEL SUMINISTRO

La aplicación de neurorrehabilitación debe aportar multitud de ejercicios debidamente mediante ordenador para facilitar el trabajo de nuestros profesionales. En cuanto al acceso y uso de la aplicación, deberá estar disponible en modo web, teniendo la aplicación la capacidad para autorizar a los usuarios y tener control del acceso.

La aplicación incluye tres licencias, una para cada uno de los Hospitales de FREMAP (Hospital de Majadahonda, Hospital de Barcelona y Hospital de Sevilla) con acceso para 4 profesionales por Hospital de FREMAP, con acceso de pacientes ilimitados, con acceso a todas las funcionalidades de la aplicación incluido la posibilidad de realizar informes

4. EJECUCIÓN DEL SUMINISTRO

Debe dar soporte a los siguientes bloques:

- Funciones Cognitivas

La plataforma deberá proporcionar soporte especializado en la intervención y estimulación de las funciones cognitivas, fundamentales para el desempeñodiario y la autonomía personal. Entre las funciones cognitivas que abordará se deberán incluir: atención, orientación (personal, temporal y espacial), memoria (episódica, semántica y procedimental), gnosias (reconocimiento sensorial), funciones

ejecutivas (planificación, razonamiento, flexibilidad, inhibición, toma de decisiones, etc.), praxias (habilidades motoras), lenguaje (expresión comprensión, vocabulario, etc.), cognición social y habilidades visoespaciales.

Permitirá trabajar de forma personalizada y estructurada sobre cada una de estas áreas, facilitando actividades y ejercicios adaptados a las necesidades del usuario. Además, la plataforma posibilitará el registro y seguimiento del progreso, así como la intervención, garantizando una mejora continua y pautada en las capacidades cognitivas de los usuarios.

Se requiere un enfoque estructurado y personalizado, basado en evidencia científica y herramientas especializadas que, incorpore los siguientes componentes clave:

➤ Evaluación neuropsicológica inicial:

- ➔ Identificación de déficits: Mediante pruebas estandarizadas, se determinan las funciones cognitivas afectadas (atención, memoria, funciones ejecutivas, lenguaje, etc.) y su impacto en la vida diaria.
- ➔ Análisis emocional y conductual: Se evalúan respuestas como frustración o ansiedad durante las pruebas, cruciales para adaptar la intervención.

➤ Diseño del programa basado en modelos teóricos:

- ➔ Restauración: Ejercicios específicos para recuperar funciones dañadas, como actividades de memoria episódica o atención sostenida, apoyadas en la neuroplasticidad.
- ➔ Compensación: Estrategias alternativas cuando la restauración no es viable (ej.: uso de agendas para suplir fallos de memoria).
- ➔ Optimización: Potenciación de habilidades preservadas.

➤ Herramientas tecnológicas y metodológicas:

- ➔ Plataformas digitales: ofrecer ejercicios personalizables para funciones como praxias o cognición social, con seguimiento automatizado de métricas.
- ➔ Telerrehabilitación: Permite continuar el tratamiento a distancia, garantizando consistencia del tratamiento en casos de períodos de estancia en casa, hospitalizaciones,...

➤ Intervención en áreas críticas:

- ➔ Funciones ejecutivas: Programas de planificación y toma de decisiones.
- ➔ Memoria y lenguaje: Actividades de reconocimiento y expresión oral que facilitan la interacción social.
- ➔ Habilidades visoespaciales: Ejercicios de orientación visoespacial para conocer la orientación o la ubicación de los objetos, para planificar cualquier acción sobre ellos y/o para imitar gestos,...

➤ Enfoque integral y multidisciplinar:

- ➔ Vinculación con salud mental: el mantenimiento y mejora de capacidades cognitivas permite la conexión con el medio y reducción de ansiedad, depresión, problemas de conducta, integrando técnicas de gestión emocional.
- ➔ Participación del entorno: Incluir a familiares en el proceso para reforzar estrategias compensatorias en el hogar.

➤ Monitoreo y ajuste continuo:

- ➔ Informes automatizados: generar datos objetivos sobre progresos, permitiendo modificar la intensidad o enfoque de las actividades.
- ➔ Reevaluaciones periódicas: Para cuantificar avances y redefinir objetivos, esencial en la rehabilitación de funciones cognitivas.

● Actividades de la vida diaria:

El programa ofrecerá soporte integral para la intervención y rehabilitación de funciones cognitivas implicadas en la planificación y ejecución eficaz de actividades de la vida diaria, facilitando el entrenamiento y la mejora en usuarios con necesidades de neurorrehabilitación.

Deberá abarcar tanto actividades básicas (como higiene, vestido, alimentación, movilidad, cuidado personal y descanso) como actividades instrumentales (gestión del hogar, manejo del dinero, uso de transporte, compras, preparación de comidas, cuidado de la salud, etc.), así como actividades relacionadas con el aprendizaje, el ocio, el juego y la participación social.

Proporcionará multitud de ejercicios y simuladores interactivos que permiten trabajar estas áreas de forma personalizada, graduados en dificultad y adaptados a las capacidades y objetivos de cada usuario.

La plataforma integrará la rehabilitación de funciones cognitivas implicadas en las actividades de la vida diaria, como la memoria, la atención, la planificación y la secuenciación, asegurando un enfoque global y operativo que facilita la transferencia de los aprendizajes al entorno real del usuario.

Será una herramienta versátil y basada en la evidencia para el soporte profesional en la rehabilitación neuropsicológica y de la autonomía funcional, garantizando seguimiento, personalización y eficacia en la intervención sobre las actividades de la vida diaria.

● Habilidades Sociales:

La plataforma debe ofrecer herramientas para la intervención en habilidades sociales, cruciales para la interacción efectiva y satisfactoria con los demás.

Abarcará áreas como empatía, inteligencia emocional, asertividad, capacidad de escucha, comunicación de sentimientos, resolución de problemas, negociación, modulación emocional.

Proporcionará ejercicios y actividades personalizables para mejorar estas habilidades en diversos entornos (Residencial, familiar, social), permitiendo a los usuarios expresarse, comprender a los demás, considerar diferentes perspectivas, resolver problemas. Facilitará el trabajo en cognición social (interpretar emociones e intenciones ajenas), teoría de la mente y reconocimiento emocional. La plataforma permitirá monitorizar el progreso y adaptar las intervenciones según la evolución del usuario.

En resumen, debe ofrecer un soporte integral y basado en evidencia para el desarrollo de habilidades sociales, promoviendo relaciones interpersonales saludables y una mejor adaptación al entorno social.

Seguridad:

Deberá garantizar el control de acceso lógico a la herramienta mediante mecanismos de identificación, autenticación, autorización y trazabilidad, garantizando la protección de datos altamente sensibles:

- Identificación:

Cada profesional dispone de un identificador de usuario personalizado y exclusivo que, junto a su contraseña, deberá ser incorporado.

- Autenticación: La aplicación debe permitir una medida adicional de seguridad en el control de acceso de los usuarios, incorporando mecanismos robustos de doble factor de autenticación (2FA), incrementando así el nivel de seguridad de un sistema basado únicamente en usuario/contraseña.

El Requisito de uso del 2FA deberá ofrecer flexibilidad, teniendo en cuenta las siguientes posibilidades:

- El administrador de la aplicación podrá forzar el uso de 2FA para cada cuenta de usuario
- Autorización: Se valorará la gestión de grupos de trabajo según distintos roles y definición de acceso a los distintos módulos y/o funcionalidades por usuarios para poder ver, añadir, modificar, imprimir y/o eliminar datos asegurando, en cualquier caso, que cada usuario tiene los permisos estrictamente necesarios para el desempeño de una tarea o actividad.
- Trazabilidad: Se llevará un registro de los accesos de cada uno de los usuarios, indicando la fecha, hora y acción realizada. Se podrá consultar la actividad en la aplicación por usuario, ficheros accedidos y por información modificada, borrada o consultada. Integridad, confidencialidad y seguridad de los datos:

Se dispondrá de todas las medidas técnicas y organizativas necesarias para garantizar la confidencialidad, integridad, disponibilidad y seguridad de los datos de la aplicación.

- Seguridad en las comunicaciones: Toda la transferencia de datos entre los puestos de trabajo se realizará mediante comunicaciones cifradas y con protocolos seguros y actualizados.

4.1 Implantación

La puesta en marcha se realizará en un periodo de tres meses contados a partir de la firma del contrato, quedarán incluidos los servicios de:

- Formación en el uso de la herramienta con la instalación, configuración, parametrización y prueba.

4.2 Formación

Durante el periodo de implantación, se procederá en paralelo a la formación necesaria para los profesionales que la utilicen. Es imprescindible desarrollar un proceso formativo inicial dirigido al conjunto de profesionales que van a utilizar esta herramienta informática

La formación se llevará a cabo según horario acordado con el licitador. Será necesario que se disponga de videotutoriales para la formación de los profesionales que se vayan incorporando con posterioridad en cada una de las áreas de actuación.

4.3 Soporte técnico

El adjudicatario dispondrá en todo momento de los recursos humanos necesarios para prestar apoyo, soporte técnico y garantizar el correcto funcionamiento del servicio durante la fase de operación.

5. RESPONSABLE DEL CONTRATO

5.1 Medios humanos

La empresa adjudicataria deberá poner al servicio de FREMAP, una persona que actúe como interlocutor o responsable único del proyecto, estando encargada de mantener en todo momento las relaciones con FREMAP para la buena marcha del mismo.

Será responsable, asimismo, de asegurar el acceso completo a la plataforma virtual y velará para que la plataforma esté operativa y accesible durante toda la vigencia del contrato.

Finalmente será responsable de resolver cualquier eventualidad que pueda producirse poniendo a disposición de FREMAP, en todo momento, la información y documentación sobre el estado del proyecto que le sea requerida vía correo electrónico.

5.2 Gestion de incidencias

El adjudicatario deberá prestar en su oferta un servicio de soporte para la apertura, seguimiento, escalado y cierre de incidencias. El servicio de asistencia técnica y mantenimiento deberá estar disponible 8 horas y 5 días a la semana.

- El horario mínimo será de 09:00 a 17:00 horas, de lunes a viernes.

La comunicación con el operador se establecerá a través de dos canales:

- Interlocutor o centro de atención. La comunicación podrá realizarse por teléfono, correo electrónico, mensajería instantánea, etc.
- Herramienta web que permita la apertura, notificación, seguimiento, aporte de documentación y cierre de incidencias.

El plazo entre la comunicación del aviso y la actuación correspondiente no debe ser superior a 24 horas, así como, la resolución de la incidencia no debe superar las 48 horas.

6. MANTENIMIENTO

6.1 Mantenimiento rectificativo

Creación de soluciones rectificativas del producto para solucionar cualquier incidencia o error en la aplicación.

6.2 Mantenimiento evolutivo

Acceso a nuevas versiones o actualizaciones del producto que aporten nuevas funcionalidades.

El adjudicatario deberá informar de los mantenimientos programados que afecten a los servicios contratados, al menos 7 días laborables de antelación.

Los trabajos de mantenimiento serán por cuenta del adjudicatario y se realizarán en una ventana de tiempo pactada previamente con FREMAP y ocupará horarios de baja actividad.

7. PREVENCIÓN DE RIESGOS LABORALES

En cumplimiento de lo establecido en el artículo 24 de la Ley de Prevención de Riesgos Laborales y R. D. 171/2004 sobre coordinación de la actividad preventiva, la empresa contratada debe entregar para la firma del contrato la siguiente documentación:

- Declaración de modalidad PRL (*)

(*) Documentación disponible en el perfil de contratante de la Mutua (<https://contrataciondelestado.es/wps/portal/perfilContratante>): Nombre O. Contratación: FREMAP – BUSCAR - Director Gerente de FREMAP – Documentos - Otros documentos.

8. SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información de FREMAP está basado en marcos normativos de referencia reconocidos tanto a nivel nacional como internacional. En particular, está alineado con la norma ISO/IEC 27001, en la que FREMAP mantiene la certificación desde 2018, y con el Esquema Nacional de Seguridad (ENS), con certificación en categoría ALTA desde 2025.

[REQ-1]: El adjudicatario estará obligado a cumplir con los requisitos de seguridad de la información y continuidad derivados de la Política de Seguridad de FREMAP, basada en las siguientes normas y directrices:

- “Norma UNE-ISO/IEC 27001” y su anexo A desarrollado en la norma UNE-ISO/IEC 27002.

- “Esquema Nacional de Seguridad (ENS)” regulado por el Real Decreto 311/2022 o normativa vigente, en su categoría ALTA.
- “Network and Information Security (NIS 2)”, regulada por la directiva 2022/2555 del Parlamento Europeo y del Consejo de 2022 relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, y la normativa que se genere de ésta.

[REQ-2]: En el caso de que el adjudicatario proporcione o tenga acceso a información, sistemas o servicios de FREMAP, éste se compromete a implementar cuantas medidas sean necesarias para cumplir con las normas y directrices indicadas, así como con la Política de Seguridad de FREMAP. En los siguientes apartados y sin perjuicio de otros requisitos detallados en el pliego, se describen algunas de las medidas de aplicación extraídas de la política vigente.

[REQ-3]: El adjudicatario se compromete, en caso de ser requerido, a proporcionar información de alto nivel sobre la Arquitectura de Seguridad de los sistemas, permitiendo a FREMAP valorar la protección y seguridad de la información de los activos y/o servicios subcontratados.

[REQ-4]: El adjudicatario se compromete a seguir un proceso formal para planificar y adquirir nuevos componentes de forma coherente con la seguridad y el análisis de riesgos, asegurando que las adquisiciones cumplan con las necesidades técnicas manteniendo la integridad y continuidad de los servicios. Igualmente realizará un estudio de las capacidades antes de prestar servicios a FREMAP, incluyendo requisitos técnicos, materiales, personal e instalaciones. Estas capacidades deben mantenerse durante su ciclo de vida.

[REQ-5]: El adjudicatario deberá proporcionar, si FREMAP lo solicita, un listado de productos y servicios utilizados, verificando que estén certificados según los estándares de seguridad aplicables, así como implementar medidas rigurosas para asegurar la identificación y el acceso seguro a la información, a los sistemas y a los servicios de FREMAP.

A continuación, se relacionan algunas de las medidas y controles extraídos de la Política de Seguridad de FREMAP, siendo de cumplimiento obligatorio y objeto de seguimiento periódico.

Confidencialidad de datos y propiedad intelectual

[REQ-6]: Todos los profesionales adscritos al contrato, incluyendo los que se incorporen al comienzo y todos los que se puedan incorporar durante toda la vida del mismo, deberán adquirir un inequívoco compromiso de confidencialidad mediante la firma del anexo que, en cumplimiento de la normativa de aplicación vigente, garantiza la confidencialidad de los datos y describe las medidas técnicas y organizativas que deben seguirse durante toda la prestación a este respecto.

[REQ-7]: La propiedad intelectual de todos los productos y/o entregables generados a partir del desarrollo de los servicios profesionales prestados durante la vida del contrato, corresponde a FREMAP.

[REQ-8]: La empresa adjudicataria deberá asegurar que toda la información, productos y/o entregables se entregan a FREMAP a la finalización del contrato, no pudiendo almacenarse ni utilizarse para fines diferentes al objeto del mismo, salvo autorización expresa.

Incidentes de seguridad

[REQ-9]: El adjudicatario se compromete a establecer un proceso integral, documentado y detallado para la gestión de incidentes de seguridad que abarque desde la detección del incidente hasta su resolución, notificando a FREMAP de inmediato ante cualquier brecha de seguridad. Igualmente, el adjudicatario

mantendrá un registro de los incidentes clasificados según su criticidad y establecerá tiempos de resolución según esta clasificación.

[REQ-10]: El adjudicatario deberá tomar medidas urgentes ante incidentes de alta severidad, incluyendo la asignación de recursos para investigación y resolución, obligación de informar a los responsables de FREMAP y tomar medidas preventivas para evitar la repetición de incidentes.

[REQ-11]: El adjudicatario deberá disponer de mecanismos de reconfiguración dinámica para detener, desviar o limitar ataques y acotar los daños. Además, el adjudicatario deberá ajustar estos procedimientos en función de los anuncios recibidos del CCN-CERT sobre ciber-amenazas sofisticadas y campañas de ataques.

[REQ-12]: El adjudicatario deberá disponer de herramientas automáticas para analizar la actividad del sistema y la información de auditoría, detectando posibles compromisos de seguridad. Además, establecerá un sistema automático de recolección de registros, correlación de eventos y respuesta automática ante incidentes, en línea con las necesidades de FREMAP.

[REQ-13]: En relación a la integridad de la información, cualquier violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos transmitidos, conservados o tratados de otra forma, deberá ser comunicada a FREMAP de forma inmediata para que pueda ser notificada a la autoridad de control sin dilación.

[REQ-14]: En relación a la confidencialidad de la información, cualquier violación de la seguridad, sustracción o la comunicación o acceso no autorizados a dichos datos, deberá ser comunicada a FREMAP de forma inmediata para que pueda ser notificada a la autoridad de control sin dilación.

[REQ-15]: En relación a la disponibilidad de la información, cualquier incidente que impacte y/o afecte al servicio de forma grave, deberá ser comunicado a FREMAP de forma inmediata.

[REQ-16]: No se permitirá la extracción de ninguna información, vía telemática o vía soporte extraíble, sin el correspondiente conocimiento y autorización por parte de FREMAP. Así mismo, se prohíbe expresamente la utilización de cualquier utilidad/herramienta sin el correspondiente conocimiento y autorización por parte de FREMAP.

Ligada al personal

[REQ-17]: El personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, firmará un acuerdo de confidencialidad antes de su interacción con recursos e infraestructuras de FREMAP y antes de su acceso a aquellas infraestructuras del adjudicatario que soporten los servicios a entregar a FREMAP dentro del alcance de la presente licitación.

[REQ-18]: El personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, será informado de las políticas y procedimientos, incluyendo requisitos de seguridad y uso correcto de los recursos, antes de interactuar con recursos e infraestructuras de FREMAP y antes del acceso a aquellas infraestructuras del adjudicatario que soporten los servicios a entregar a FREMAP dentro del alcance de la presente licitación. El citado personal recibirá actualizaciones regulares sobre estas políticas y procedimientos.

[REQ-19]: FREMAP podrá evaluar periódicamente los conocimientos del personal adscrito en materia de seguridad de la información, incluyendo contenidos específicos con relación a las políticas que se definan

desde FREMAP en cada momento. El adjudicatario deberá realizar formación continua de su personal a efectos de que se superen dichas evaluaciones.

[REQ-20]: Queda expresamente prohibido al personal del adjudicatario: (i) instalar software no autorizado (incluido libre o de desarrollo propio); (ii) modificar sin autorización configuraciones físicas o lógicas de hardware/software; (iii) acceder a áreas o datos no autorizados; (iv) elevar privilegios sin autorización; (v) alterar, borrar o distorsionar registros, archivos o correos; (vi) introducir código malicioso (virus, macros, applets, etc.); (vii) usar los recursos para fines ajenos al contrato; (viii) enviar correo masivo, cadenas o comunicaciones comerciales sin autorización expresa.

[REQ-21]: Todo el personal del adjudicatario firmará un documento individual de aceptación de obligaciones de seguridad y confidencialidad de tratamiento de datos de FREMAP. El adjudicatario custodiará dichas firmas y las pondrá a disposición de FREMAP cuando se requiera.

Control de accesos

[REQ-22]: El adjudicatario se compromete a implementar mecanismos de control de acceso para proteger los recursos del sistema y la información, permitiendo el acceso solo a usuarios identificados y autorizados.

[REQ-23]: El sistema de control de acceso estará organizado para requerir la concurrencia de dos o más personas en tareas críticas. Asimismo, deberá garantizar que las funciones de desarrollo y operación, autorización y control del uso, configuración y mantenimiento del sistema, auditoría o supervisión, no recaigan en la misma persona.

[REQ-24]: El adjudicatario se compromete a implementar políticas y mecanismos que garanticen la adecuada gestión de los derechos de acceso de manera que los accesos estén deshabilitados por defecto y los usuarios para el acceso sean creados por perfiles específicos y con competencia para ello. Estos perfiles se les aplicará el principio de mínimo privilegio y serán revisados periódicamente.

[REQ-25]: El adjudicatario deberá restringir y controlar el uso y asignación de privilegios para el acceso y ejecución de actividades de gestión en los equipos del adjudicatario relacionados con los servicios que entregue a FREMAP. La asignación de privilegios se controlará mediante un proceso formal siguiendo el principio de "necesidad de uso". Para ello, el adjudicatario utilizará un sistema AAA (Authentication, Authorization and Accounting). El acceso remoto a consolas y terminales de los equipos del adjudicatario se realizará utilizando protocolos que aseguren la confidencialidad de las comunicaciones como ssh o similar y se utilizará el sistema AAA referido para asegurar el cumplimiento de los privilegios asignados a cada administrador o grupo de administradores antes, durante y después de la ejecución de actividades de gestión en los equipos relacionados con los servicios que se entreguen a FREMAP. Cada administrador deberá disponer de un identificador único y contraseña. Las consolas y terminales de gestión deberán mostrar un mensaje que adviertan de la restricción de acceso, no ofrecer mensajes de ayuda y limitar el número de fallos de conexión. El acceso a consolas y terminales de gestión se deberá desactivar tras un periodo de inactividad de 5 minutos, cancelándose cualquier conexión que estuviera activa.

[REQ-26]: De cara a garantizar la exactitud de los registros de auditoría, todos los equipos con servicios que se entreguen a FREMAP deberán tener sincronizados sus relojes haciendo uso de un servicio tipo NTP o similar.

Los administradores de equipos relacionados con servicios que se entreguen a FREMAP deberán seguir buenas prácticas de seguridad para la selección y uso de contraseñas, manteniendo la confidencialidad de las mismas y cumpliendo características mínimas para su composición. Las contraseñas tendrán un plazo

de validez que obligue a su cambio periódico. A su vez, los administradores no deberán guardarlas en lugares inseguros (papel, escritorio, etc.), divulgarlas, compartirlas y en ningún caso se incluirán en ningún procedimiento o proceso automático que por ejemplo las almacene en una macro o fichero legible.

[REQ-27]: El adjudicatario deberá comunicar a FREMAP las necesidades de acceso a puertos de diagnóstico, puertos de gestión fuera de banda, puertos de gestión en banda o cualquier otro puerto de gestión sobre equipos del adjudicatario desplegados en FREMAP con objeto de inventarlos y protegerlos adecuadamente, evitando así los accesos no autorizados que pudieran producirse desde los mismos a otros elementos de la infraestructura TI o a sistemas de información de FREMAP. No estará permitido el acceso local o remoto por parte del adjudicatario a ningún sistema de información o elemento de la infraestructura de TI propiedad de FREMAP, salvo autorización expresa (como, por ejemplo, para el acceso de personal del adjudicatario al sistema de gestión de incidencias de FREMAP).

[REQ-28]: Todos los equipos que se desplieguen en dependencias de FREMAP soportarán la división de las redes en dominios lógicos, o redes virtuales, con objeto de poder fortalecer la seguridad ante riesgos de accesos no autorizados a los sistemas de información, especialmente a aquellos que albergan información crítica o sensible.

[REQ-29]: El personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, accederá a zonas “seguras” o “sensibles” como los CPDs durante el tiempo mínimo imprescindible para la realización de los trabajos que sean necesarios siempre con autorización previa y con control del acceso por parte de FREMAP. Dicho personal portará su identificación de manera visible.

[REQ-30]: En el caso de sedes remotas de trabajo, la empresa adjudicataria deberá contar con las medidas de seguridad adecuadas para proteger los activos de información de FREMAP que se encuentren en dichas ubicaciones.

[REQ-31]: FREMAP podrá revisar el uso de los sistemas de información, analizar registros y contenidos para verificar el cumplimiento contractual, e imponer medidas como la restricción o revocación inmediata de accesos del personal afectado cuando se detecten incumplimientos o riesgos de seguridad.

Acceso remoto

[REQ-32]: El adjudicatario utilizará sistemas de identificación que cumplan con las normativas aplicables, como sistemas de clave concertada, asignando identificadores únicos a cada usuario, asegurando que sus privilegios y permisos estén claramente definidos. Igualmente, debe gestionar adecuadamente las cuentas de usuario, incluyendo la desactivación de cuentas cuando un usuario deja de cumplir funciones y se evitará el uso de cuentas genéricas.

[REQ-33]: El adjudicatario se compromete a implementar los siguientes requisitos para la autenticación de usuarios externos previamente aprobados por FREMAP:

Los usuarios deberán identificarse de manera fidedigna antes de proporcionársele las credenciales de autenticación y deberán conocer y aceptar las obligaciones relacionadas con el manejo de estas. Las credenciales serán activadas cuando estén bajo control efectivo del usuario y serán inhabilitadas en caso de pérdida, compromiso o pérdida de relación con los sistemas de FREMAP, quién deberá ser notificado.

La información presentada para la autenticación debe ser mínima, evitando revelar detalles sobre el sistema. No se informará del motivo del rechazo si la autenticación falla y el número de intentos estará limitado según las directrices de FREMAP. El acceso será bloqueado tras superar este límite. El adjudicatario registrará los accesos exitosos y fallidos, informando al usuario del último acceso efectuado

con su identidad. El sistema deberá informar al usuario de sus derechos y obligaciones inmediatamente después de obtener el acceso.

[REQ-34]: El adjudicatario se compromete a implementar sistemas de autenticación para garantizar la identificación adecuada y segura de los usuarios propios o contratados que puedan tener acceso a la información de FREMAP cumpliendo con sus directrices, el ENS y las guías CCN-STIC.

[REQ-35]: El adjudicatario se compromete a mantener una gestión rigurosa y segura de todos los activos utilizados en la prestación de servicios a FREMAP, a través de un registro detallado de todos los activos que deben ser actualizados regularmente. Igualmente, deberá implementar un procedimiento para clasificar y categorizar los activos según los riesgos, que debe ser revisado y actualizado periódicamente.

[REQ-36]: El adjudicatario se compromete a garantizar la seguridad de los equipos utilizados en los servicios a FREMAP mediante la configuración segura de los equipos, asegurando la seguridad por defecto y la mínima funcionalidad, además de la instalación y configuración de elementos de protección contra virus y ataques de terceros. Esta configuración debe ser gestionada y actualizada regularmente por personal autorizado, actualizando los sistemas siguiendo las recomendaciones de los fabricantes y verificando regularmente la integridad del firmware. Igualmente, se gestionarán copias de seguridad de estas configuraciones.

[REQ-37]: El adjudicatario coordinará con FREMAP los cambios que afecten a los activos del servicio prestado, siguiendo un procedimiento para la planificación e implementación de estos cambios.

[REQ-38]: Para todos aquellos accesos remotos a recursos desplegados en FREMAP, se establecen las siguientes limitaciones y responsabilidades específicas que tanto el adjudicatario como quien actúe en su nombre, si fuera el caso, deberá cumplir:

Condiciones técnicas:

Los accesos remotos se producirán desde equipos con plataforma corporativa FREMAP, haciendo uso de los sistemas de conexión segura VPN que se indiquen en cada momento de la vida del contrato, salvo autorización expresa.

Recursos de FREMAP accesibles:

Solamente se proporcionará acceso remoto a los elementos e información estrictamente necesarios para el cumplimiento del objeto contractual.

La conexión se realizará única y exclusivamente por protocolos previamente consensuados con FREMAP.

Potestad de control:

El personal autorizado de FREMAP, teniendo como finalidad la protección, optimización y mejora de los servicios, monitorizará el tráfico cursado en este tipo de conexiones para la detección de actuaciones anómalas.

Deberes y obligaciones para la empresa adjudicataria:

Solamente deberá tener acceso a los recursos desplegados en FREMAP el personal adscrito y estrictamente necesario de la empresa adjudicataria y únicamente para los fines previamente autorizados por FREMAP.

Los usuarios del acceso remoto deberán hacer un uso adecuado de la conexión, utilizándola eficientemente con el fin de evitar en la medida de lo posible la congestión de la misma, la interrupción de los servicios de red o del equipamiento de la infraestructura conectada.

Se deberá acceder desde redes privadas protegidas que garanticen unas condiciones de seguridad adecuadas.

En el caso de sedes remotas de trabajo, todos los equipos de red del adjudicatario dispondrán de medidas para reducir los riesgos derivados del acceso no autorizado y para protegerlos contra pérdidas o daños y falta de disponibilidad. Se protegerá el acceso a la consola de todos los equipos y se realizarán backups de sus ficheros de manera que se puedan recuperar tras un desastre o ante un fallo de los soportes que albergan dichos ficheros.

Se deberá hacer un uso adecuado de las conexiones y cumplir la normativa y política vigente en FREMAP.

Registro de entrada y salida de equipamiento

[REQ-39]: El adjudicatario llevará un registro de entrada y salida de todos los activos de Información de FREMAP bajo su custodia debiendo estar físicamente resguardados en zonas de acceso controlado. Cualquier traslado o eliminación de sistemas o Activos de Información requerirá la previa autorización por escrito de FREMAP.

[REQ-40]: El adjudicatario se compromete a implementar medidas para acondicionar sus centros y entornos físicos, abordando incidentes naturales y humanos, tanto intencionados como fortuitos. Esto incluirá asegurar condiciones ambientales óptimas como temperatura y humedad para equipos críticos, protección del cableado, y tomas de energía eléctrica para garantizar el suministro y correcto funcionamiento de las luces de emergencia. Se establecerán protocolos específicos contra incendios según la normativa industrial aplicable, incluyendo sistemas de detección, alerta y extinción manual o automática de incendios.

[REQ-41]: El adjudicatario dispondrá de medidas y protocolos específicos de protección contra inundaciones como sistemas de detección de humedad y líquidos, preferiblemente instalados en las salas técnicas y en caso de ser necesario, se deben tener instalados sistemas de recogida de aguas con sus respectivos mantenimientos. Así como, deberá establecer un suministro eléctrico de emergencia para las infraestructuras críticas del servicio prestado.

[REQ-42]: El adjudicatario se asegurará de que sus empleados cumplan los requisitos profesionales y tengan la documentación necesaria para el desempeño de sus funciones, garantizando que están en concordancia con la gestión de riesgos asociados al servicio proporcionado a FREMAP.

[REQ-43]: El adjudicatario implementará medidas para gestionar adecuadamente los recursos humanos implicados en el servicio a FREMAP. Esto incluye establecer un código de conducta que detalle las responsabilidades y obligaciones del personal en materia de seguridad de la información, con medidas disciplinarias claras para incumplimientos. Se exigirá estricta confidencialidad sobre la información de FREMAP, incluso en caso de subcontratación, asegurando el cumplimiento de los estándares de seguridad y normativas. Además, deberá implementar planes de concienciación y formación periódicos sobre seguridad y protección de datos conforme a las directrices del ENS, documentando todas las acciones realizadas.

El adjudicatario deberá establecer medidas y políticas para la protección de la información, tales como:

Política de puesto de trabajo despejado que recoja las instrucciones necesarias para mantener los puestos de trabajo libres de información de FREMAP que no sea necesaria para el desempeño del servicio. Los lugares y soportes designados para el almacenamiento de la información deberán disponer de medidas de seguridad adecuadas al nivel de clasificación que tenga la información contenida. Al menos debe ser almacenada en lugares cerrados como archivadores o cuartos trancados bajo llave.

Protección de dispositivos portátiles con directrices específicas para el uso seguro de dispositivos informáticos, canal de comunicación de incidentes, conexión segura a través de VPN y procedimientos de borrado seguro antes de la eliminación de dispositivos. Los discos duros de los dispositivos deben estar sometidos a un proceso de cifrados.

[REQ-44]: Los equipos portátiles deben disponer de un sistema de detección de alteración que permita conocer si un equipo ha sido manipulado física o lógicamente. Para ello se instalarán medios físicos como tornillos de seguridad, pegatinas de manipulación, etc. y se usarán herramientas automatizadas que permitan detectar cuando algún componente ha sido extraído o se han realizado modificaciones de software.

En caso de ser necesario en función del riesgo y bajo indicación de FREMAP los dispositivos portátiles solo podrán ser usados en entornos protegidos y bajo control de acceso. Adicionalmente se instalará en los dispositivos portátiles un sistema de borrado remoto que podrá ser activado en caso de pérdida o robo.

Operación y registro de actividad

[REQ-45]: El adjudicatario deberá documentar y mantener actualizados los procedimientos de operación relacionados con los servicios que entreguen a FREMAP. Igualmente, el adjudicatario fijará responsabilidades y procedimientos de gestión para asegurar un control satisfactorio de todos los cambios en los equipos relacionados con los servicios que entreguen a FREMAP, conservando un registro de auditoría.

[REQ-46]: El personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, mantendrá un diario de sus actividades en el que se incluirán los errores de los equipos o infraestructuras que gestionen o administren y las acciones adoptadas para su corrección. Los diarios de operaciones podrán ser comprobados regularmente por FREMAP.

[REQ-47]: La documentación sobre las infraestructuras de TI de FREMAP de la que el adjudicatario tenga conocimiento, así como la generada por el propio adjudicatario sobre las infraestructuras que soportan los servicios a entregar a FREMAP, deberán ser protegidos y almacenados con seguridad y control de acceso.

[REQ-48]: Los equipos y herramientas informáticas de las que haga uso el personal del adjudicatario, o del personal que intervenga bajo su responsabilidad, estarán debidamente securizados de manera que la utilización de dichos equipos o herramientas en las instalaciones de FREMAP, o sobre los equipos relacionados con los servicios se entregan a FREMAP, no supongan un riesgo de seguridad para FREMAP. Estos equipos y herramientas informáticas dispondrán de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante de las mismas. Se considera código dañino: los virus, los gusanos, los troyanos, los programas espías, conocidos en terminología inglesa como spyware, y en general, todo lo conocido como malware.

[REQ-49]: El adjudicatario se compromete a tener un registro de actividad para asegurar la trazabilidad y seguridad de las operaciones, en colaboración con FREMAP y conforme al Esquema Nacional de Seguridad (ENS). Este registro de auditoría deberá incluir el identificador del usuario o entidad, fecha y hora del

evento, detalles de la acción realizada y su resultado. Estos registros deberán activarse en todos los servidores utilizados por el adjudicatario.

[REQ-50]: En términos de refuerzo y colaboración estrecha con FREMAP, el adjudicatario deberá:

Realizar una revisión periódica de los registros de actividad para identificar patrones anormales que puedan indicar posibles amenazas.

Garantizar que el sistema tenga una referencia de tiempo para facilitar las funciones de registro de eventos y auditoría, manteniendo la sincronización con otros dispositivos.

Documentar los eventos de seguridad que serán auditados y el tiempo de retención de los registros antes de su eliminación, conforme a las políticas de FREMAP.

Garantizar que el acceso y eliminación de registros de actividad, así como las copias de seguridad, solo podrán ser realizados por personal autorizado para reforzar la confidencialidad e integridad de la información registrada.

[REQ-51]: El adjudicatario garantizará la seguridad de las claves criptográficas en todas las fases de su ciclo de vida, desde su generación hasta su destrucción. Para ello las claves se protegerán rigurosamente siguiendo las políticas del Esquema Nacional de Seguridad (ENS). Igualmente, se mantendrá un estricto aislamiento entre los medios de generación y los de explotación, y las claves retiradas se almacenarán separadamente de las operativas.

[REQ-52]: Con el fin de garantizar el cumplimiento de las medidas y garantizar la seguridad de las operaciones, el adjudicatario deberá asegurar la utilización exclusiva de algoritmos y parámetros autorizados por el CCN.

[REQ-53]: El adjudicatario se compromete a cumplir con los Acuerdos a Nivel de Servicio (SLAs) y servicios mínimos contratados con FREMAP, entendiendo su responsabilidad en caso de incumplimiento. Implementará un sistema rutinario para medir el cumplimiento de las obligaciones del contrato y coordinar la gestión de incidencias, proporcionando un punto de contacto para la comunicación con FREMAP. Además, establecerá mecanismos para neutralizar desviaciones del margen acordado, integrando procedimientos de coordinación para el mantenimiento de sistemas y la gestión de incidentes, con entrega periódica de informes de seguimiento del servicio a FREMAP.

[REQ-54]: El adjudicatario deberá implementar medidas para fortalecer la seguridad de la cadena de suministro de aquellos proveedores que le presten servicios. Esto incluye la realización de un análisis exhaustivo del impacto potencial de incidentes en la cadena de suministros, considerando tanto los efectos internos para el adjudicatario como los que supondría para FREMAP. En base a este análisis de riesgos, deberán adoptarse medidas para garantizar la seguridad y confiabilidad de la interconexión de sistemas, ajustándose a las políticas de FREMAP. Esta interconexión siempre deberá realizarse con la autorización previa de FREMAP, quedando prohibido cualquier flujo de información no autorizado. Deberán establecerse enlaces y documentación detallada de las interconexiones, especificando requisitos de seguridad, protección de datos y naturaleza de la información intercambiada.

[REQ-55]: El adjudicatario deberá coordinar actividades al interconectar sistemas en diferentes dominios de seguridad, garantizando una adecuada identificación, autenticación y autorización. Debiendo establecerse mecanismos para asegurar una asignación efectiva de responsabilidades en cada sistema, complementando las medidas de seguridad locales.

[REQ-56]: En el caso de que se utilicen servicios en la nube, los sistemas deben cumplir con el Esquema Nacional de Seguridad (ENS) o con los requisitos de las guías CCN-STIC correspondientes a soluciones Cloud específicas. Además, el adjudicatario deberá garantizar que el servicio cloud esté certificado bajo una metodología de certificación reconocida por el Centro Criptológico Nacional.

[REQ-57]: Se prohíbe el uso de dispositivos no autorizados por FREMAP para acceder a información o servicios objeto del contrato.

[REQ-58]: El adjudicatario mantendrá la correcta actualización de parches, versiones y configuraciones de seguridad en sus equipos y aplicaciones.

Seguridad de los componentes

[REQ-59]: Todos los componentes que formen parte de la solución deberán cumplir con los requisitos establecidos por el Esquema Nacional de Seguridad (ENS) para sistemas de categoría ALTA, conforme al Real Decreto vigente.

[REQ-60]: Todos los componentes que cuenten con capacidades de almacenamiento de información de FREMAP, ya sea temporal o permanente, deberán cumplir con al menos uno de los siguientes criterios:

- Estar incluidos en el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación (CCN-STIC 105).
- Estar clasificados conforme a la Guía de Taxonomía de referencia para productos de seguridad (CCN-STIC 140).
- Acreditar el cumplimiento de la norma ISO/IEC 15408 (Common Criteria), la Directiva NIS2, o normativa equivalente reconocida.
- Cumplir un requerimiento expreso detallado en el pliego o un valor diferencial para cubrir necesidades técnicas específicas, debiendo en este caso:
- Incluir junto a su oferta económica una justificación técnica detallada.
- Proponer medidas de seguridad compensatorias que garanticen un nivel de protección equivalente, conforme a los requisitos del Esquema Nacional de Seguridad (ENS) en su nivel ALTO.

[REQ-61]: El adjudicatario se compromete a mantener la vigencia de las certificaciones y/o medidas compensatorias durante toda la duración del contrato, así como a proporcionar a FREMAP información actualizada y una declaración responsable periódica que acredite el cumplimiento de este requisito.

[REQ-62]: En caso de no disponer de certificación, el licitador deberá justificar documentalmente la idoneidad del componente para el uso previsto, incluyendo una evaluación de riesgos y medidas compensatorias que garanticen un nivel de seguridad equivalente.

Borrado seguro

[REQ-63]: El licitador deberá incluir en su oferta el compromiso de realizar el borrado seguro de los datos almacenados en cualquier equipo que sea retirado o sustituido durante la ejecución del contrato, en cumplimiento con los requisitos del ENS en su nivel ALTO.

[REQ-64]: El adjudicatario realizará el borrado seguro con al menos uno de los siguientes métodos:

- Utilizando una herramienta incluida en el Catálogo de Productos y Servicios de Seguridad TIC (CCN-STIC 105) de forma que se acredite el borrado seguro.

- Utilizando una herramienta incluida en la Guía de Taxonomía de Productos de Seguridad TIC (CCN-STIC 140) de forma que se acredite el borrado seguro.
- Acreditando el uso de un método de borrado seguro equivalente que garantice la sobreescritura a bajo nivel de los datos o su encriptación, impidiendo su recuperación por cualquier medio, en cumplimiento con los requisitos del ENS en su nivel ALTO.

[REQ-65]: El adjudicatario deberá mantener el cumplimiento normativo de borrado seguro durante toda la vida del contrato, proporcionando registros y certificados de los borrados realizados.

Continuidad

[REQ-66]: El adjudicatario deberá disponer de un plan en el que se identifiquen los requisitos de disponibilidad y estrategia para gestionar interrupciones, incluyendo el RTO (Tiempo de Recuperación Objetivo) y RPO (Punto de Recuperación Objetivo) de cada servicio junto con procedimientos de recuperación y estructura organizativa adecuada. Además, se garantizará la evaluación continua del plan para mantener su efectividad.

[REQ-67]: El adjudicatario, en situaciones de emergencia, activará un plan de contingencia que incluirá comprobaciones integrales del sistema operativo, firmware y ficheros de configuración para garantizar la integridad del sistema.

[REQ-68]: El adjudicatario proporcionará a FREMAP la información necesaria para establecer el plan conforme a los requisitos del ENS y considerando funciones, responsabilidades, actividades, medios alternativos y formación específica para el personal involucrado.

[REQ-69]: En el caso de sedes remotas de trabajo, la empresa adjudicataria dispondrá de sistemas y/o redes de comunicaciones con mecanismos de alta disponibilidad para garantizar el servicio prestado.

[REQ-70]: FREMAP dispone de un plan de continuidad de negocio que se prueba de manera periódica. El adjudicatario colaborará en la ejecución de las comprobaciones de los planes de contingencia y de continuidad de FREMAP, en lo referido a los servicios dentro del alcance de la presente licitación.

[REQ-71]: Para asegurar la continua disponibilidad e integridad de los equipos, se aplicarán las recomendaciones que publiquen los distintos fabricantes. Se realizará mantenimiento preventivo y correctivo sobre los equipos especialmente en el caso de la aparición de alguna vulnerabilidad en los mismos.

[REQ-72]: En casos que requieran medios alternativos para garantizar la continuidad del servicio, el adjudicatario podrá recurrir a servicios contratados a terceros, instalaciones alternativas, personal sustituto, equipamiento de respaldo o medios de comunicación alternativos, que estarán sujetos a las mismas garantías de seguridad que los originales.

Conformidad

[REQ-73]: El adjudicatario se compromete, en caso de ser requerido por FREMAP, a presentar declaraciones responsables de compromiso de cumplimiento de las medidas de seguridad contenidas en las políticas y normativas de aplicación, tanto a nivel de empresa como del personal adscrito al contrato.

[REQ-74]: El adjudicatario asumirá daños, gastos, costes y perjuicios de cualquier naturaleza derivados del incumplimiento por parte de éste o de su personal respecto de las obligaciones de este contrato, incluyendo las exigibles por vulneraciones de seguridad o uso indebido de los sistemas o aplicaciones.

Auditoría

FREMAP realiza procesos de auditoría periódicos a efectos de comprobación de cumplimiento de las medidas de seguridad contenidas en las políticas y normativas de aplicación.

[REQ-75]: FREMAP quedará capacitada para la realización de auditorías de seguridad de la información, a fin de velar por las políticas establecidas y las normativas de aplicación, en su caso. El plan de auditoría será acordado entre FREMAP y el adjudicatario.

[REQ-76]: FREMAP quedará capacitada para recabar cualquier información relacionada con la seguridad de los sistemas donde resida en reposo o en movimiento información de FREMAP, teniendo el adjudicatario que suministrar esta información de forma concisa y veraz. Esto se aplica tanto al adjudicatario como a cualquier subcontratación de sistemas que por parte de este se realice.

9. NORMATIVA INTERNA EN MATERIA DE INTELIGENCIA ARTIFICIAL PARA PROVEEDORES

El Proveedor se compromete a notificar a FREMAP, con carácter previo, cualquier uso, puntual o continuado, de herramientas, sistemas, modelos y/o soluciones de Inteligencia Artificial (en lo sucesivo, conjuntamente, las “tecnologías de IA”) que se lleve a cabo con motivo de la prestación de los servicios objeto del presente Contrato. En dicha notificación el Proveedor deberá facilitar a FREMAP:

- I. La identificación de la tecnología de IA que se pretende utilizar.
- II. La identificación del proveedor de dicha tecnología, en caso de que el Proveedor de servicios no sea quien ha desarrollado o para quien se ha desarrollado, específicamente, dicha tecnología de IA.
- III. La documentación técnica de la cual se disponga y que esté asociada a la tecnología de IA.
- IV. La finalidad prevista con el despliegue de la tecnología de IA.
- V. El nivel de riesgo que tiene dicha tecnología de IA conforme a la normativa aplicable en materia de inteligencia artificial.
- VI. De forma general, información clara y comprensible acerca del funcionamiento de la correspondiente tecnología de IA que pretenda utilizar con motivo de la prestación de los servicios, incluyendo los criterios y algoritmos utilizados.
- VII. Cualquier otra información solicitada por FREMAP, incluidas cuantas explicaciones resulten adecuadas para una correcta valoración y análisis de la tecnología de IA en caso de que dichas tecnologías de IA tomen decisiones basadas exclusivamente en capacidades de Inteligencia Artificial.

Una vez efectuada la notificación referida en el párrafo anterior, FREMAP dispondrá de un plazo de treinta (30) días laborables para oponerse al uso de las tecnologías de IA por el Proveedor. No obstante, lo anterior, el plazo referido no resultará de aplicación en caso de que concurran circunstancias de extraordinaria y urgente necesidad (por ejemplo, en caso de que se pueda ver comprometida de manera significativa la continuidad en la prestación de los servicios); circunstancias que deberán estar, siempre y en todo caso, debidamente justificadas. En estos supuestos, el uso de tecnologías de IA se limitará al tiempo mínimo e imprescindible que resulte necesario y con observancia de los requisitos establecidos en la presente Cláusula, así como en cualquier normativa que resulte de aplicación a tal efecto.

Transcurrido el plazo de treinta (30) días laborables anteriormente referido sin que FREMAP hubiese manifestado al Proveedor su oposición, se entenderá que autoriza el uso de tecnologías de IA.

El Proveedor garantiza a FREMAP que ha obtenido u obtendrá de los legítimos titulares de las tecnologías de IA cuantas autorizaciones, permisos y licencias que resulten necesarios, sea cual sea su índole y alcance, para el uso pacífico de las mismas.

Sin perjuicio de lo anterior, las Partes acuerdan que, en todo caso, el uso de tecnologías de IA se regirá por el régimen establecido a continuación:

- I. En ningún caso estará permitido el uso de tecnologías de IA públicas, ya sean de propósito general o especializado que, de cualquier forma, traten y/o almacenen información de FREMAP.
- II. El Proveedor se obliga a garantizar que ni este ni ningún tercero involucrado en la cadena de suministro empleen, en ninguna etapa relacionada con la provisión de los productos o la prestación de los servicios contratados por FREMAP, sistemas de inteligencia artificial catalogados como prohibidos por la legislación que resulte aplicable en cada caso, particularmente por el Reglamento (UE) 2024/1689 de Inteligencia Artificial (en adelante, el “Reglamento de IA”).
- III. La utilización de una tecnología de IA calificable como de alto riesgo conforme al Reglamento de IA será específicamente identificada e informada como tal a FREMAP. Dicha obligación también se aplicará cuando la tecnología de IA en cuestión haya sido considerada, dado su carácter accesorio, como excepcionada de la condición de alto riesgo.
- IV. Las tecnologías de IA se utilizarán exclusivamente con el propósito específico de mejorar la eficiencia, precisión o calidad de los servicios prestados, sin que dicho uso pueda afectar de manera significativa a los derechos o intereses de las Partes y/o cualesquiera otros terceros. En este sentido, se prohíbe el uso de información de FREMAP clasificada como interna, restringida y/o confidencial para, de cualquier forma, enriquecer las tecnologías de IA.
- V. El Proveedor deberá disponer de un sistema de gestión de calidad documentado de las tecnologías de IA de alto riesgo que utilice con motivo de la prestación de los servicios a favor de FREMAP, a partir del 02/08/2026, de conformidad con la normativa de aplicación y en los términos previstos en la misma. En caso de uso de tecnologías de IA de alto riesgo, el Proveedor deberá establecer, implementar y documentar un sistema de gestión de riesgos específicos asociado al uso de las mismas.
- VI. El uso de tecnologías de IA deberá estar controlado, directa o indirectamente, por el Proveedor, de manera que siempre haya una supervisión humana adecuada a fin de garantizar el cumplimiento de los estándares de calidad y medidas de seguridad establecidas durante todo el periodo en que las mismas estén en uso.
- VII. El Proveedor se compromete a comunicar a FREMAP, a la mayor brevedad posible y en todo caso antes de su implementación, cualquier cambio significativo que impacte en el uso de las tecnologías de IA utilizadas con motivo de la prestación de los servicios. Con carácter enunciativo, pero no limitativo, se entenderá por “cambio significativo”: cambios en los parámetros, reglas y criterios de funcionamiento del algoritmo o modelo subyacente al sistema de IA; cualquier modificación sustancial que se produzca en el sistema de IA; cualquier modificación o actualización de los modelos subyacentes al sistema de IA en cuestión; o el desarrollo de nuevas finalidades, como parte del servicio prestado, a partir de la tecnología de IA que hubiese sido autorizada.
- VIII. Cuando el Proveedor trate cualquier información de FREMAP que contenga datos de carácter personal a través de tecnologías de IA, deberá cumplir con las siguientes disposiciones:
 - a. El tratamiento deberá realizarse siempre y en todo caso, con estricto cumplimiento de la normativa de protección de datos que resulte de aplicación en cada momento. Para ello, el Proveedor tomará cuantas medidas resulten adecuadas para garantizar la confidencialidad y

seguridad de los datos personales objeto de tratamiento, ya sea un tratamiento en condición de responsable o encargado del tratamiento.

- b. Deberá abstenerse de tratar los datos personales, por medio del uso de tecnologías de IA, de forma incompatible con la finalidad para la que se le facilitan los datos personales.
- c. Deberá abstenerse de generar nuevos datos personales relativos a las categorías de interesados cuyos datos se tratan por cuenta de FREMAP. En caso de que la generación de nuevos datos y atributos personales sea parte esencial del servicio prestado, dicha cuestión deberá ser expresamente identificada e informada a FREMAP para su valoración y análisis.
- d. Deberá colaborar con FREMAP en el cumplimiento de cualesquiera obligaciones que le resulten de aplicación en materia de inteligencia artificial y que guarden relación con el tratamiento de datos personales.
- e. Deberá de comunicar a FREMAP, de forma previa a la implementación de cualesquiera otras tecnologías de IA adicionales a las autorizadas por FREMAP con las que se vayan a procesar datos personales facilitados por FREMAP, su intención de desplegar otras tecnologías de IA en el marco de prestación de sus servicios, especificando y aportando los siguientes detalles.
- f. El Proveedor no podrá utilizar, ni tampoco permitir que se utilicen por terceros, los datos personales que se faciliten por FREMAP con fines de entrenamiento, desarrollo ni/o mejora de modelos de IA de uso general, sistemas de IA o cualesquiera otras tecnologías de IA, ya sean propios o de terceros, salvo que exista autorización previa y expresa por parte de FREMAP cuando dicho entrenamiento, desarrollo o mejora de modelos y sistemas sea necesario para cumplir con instrucciones expresas de FREMAP.

Las anteriores condiciones resultarán de aplicación en el marco de toda la cadena de suministro del Proveedor, siendo de aplicación a cualesquiera proveedores con que cuente el Proveedor a la hora de prestar sus servicios en favor de FREMAP, ya sean dichos terceros proveedores considerados a los efectos de la normativa de protección de datos sub-encargados del tratamiento o responsables del tratamiento independientes.

Las anteriores condiciones son de aplicación sin perjuicio del resto de acuerdos y disposiciones suscritas entre las Partes en materia de protección de datos (por ejemplo: acuerdos de encargo de tratamiento o de corresponsabilidad), las cuales se complementan con las condiciones aquí expuestas. En caso de contradicción entre estas condiciones y cualesquiera otros acuerdos específicos, se estará al acuerdo específico alcanzado en materia de protección de datos entre las Partes.

- IX. Sin perjuicio del cumplimiento de lo establecido en el párrafo anterior, en ningún caso se podrán conectar algoritmos de tecnologías de IA con los sistemas de FREMAP si no se ha realizado una previa evaluación técnica por esta última.
- X. El Proveedor se compromete a notificar a FREMAP, a la mayor brevedad posible, cualquier incidente, real o potencial, o fallo de funcionamiento de las tecnologías de IA cuando suponga un incumplimiento de las obligaciones establecidas en la presente Cláusula.
- XI. El Proveedor no podrá comunicar o ceder a ningún tercero o utilizar para fines propios la información resultante que se obtenga tras la aplicación de tecnologías de IA con motivo de la prestación de los servicios, salvo que medie la autorización previa y por escrito de FREMAP.
- XII. El Proveedor deberá asegurarse de conservar e informar la siguiente documentación: (a) la tecnología de IA utilizada, (b) el alcance del uso de dicha tecnología para proporcionar el producto o servicio, (c) los datos e información recopilada, procesada y almacenada por la tecnología de IA, (d) cualquier otra tecnología de IA con la que interactúe la utilizada principalmente para la prestación

del producto o servicio. El Proveedor deberá facilitar a FREMAP dicha documentación si así los solicita.

- XIII. El Proveedor deberá informar a FREMAP en caso de (i) recibir requerimiento de información de una autoridad de control o (ii) gestionar y notificar a dichas autoridades de control un incidente de IA, cuando para dar curso a ambas acciones sea preciso facilitar información propiedad de FREMAP.
- XIV. El Proveedor mantendrá indemne a FREMAP por cualesquiera errores, defectos, fallos, incidentes graves o consecuencias derivadas del uso de tecnologías de IA durante la prestación de los servicios objeto del presente Contrato.

