Expediente Nº. LICT/99/159/2024/0275

Pliego de Prescripciones Técnicas para la Contratación del servicio y mantenimiento del sistema de reconocimiento de voz de radiólogos de FREMAP, Mutua colaboradora con la Seguridad Social Nº61.

ÍNDICE

1. OBJETO

El objeto del presente Pliego de Prescripciones Técnicas es definir el alcance y condiciones técnicas que regirán la contratación del servicio y mantenimiento del sistema de reconocimiento de voz de radiólogos de FREMAP.

Este servicio se prestará en los Centros Hospitalarios de Majadahonda, Sevilla y Barcelona, así como en el Centro Asistencial de Madrid, sito en la calle del Poeta Joan Maragall, 39.

El contrato comprenderá, **como mínimo**, las siguientes prestaciones:

- Conexión, pruebas de funcionamiento y puesta en marcha del servicio mediante el suministro del equipamiento software y hardare según especificaciones.
- Formación de uso y manejo dirigida al personal sanitario o técnico de FREMAP.
- Servicio de asistencia técnica y mantenimiento durante la ejecución del contrato, en los términos establecidos en el presente Pliego.

Todos los puntos anteriores, así como el resto de aspectos técnicos, condiciones de ejecución y responsabilidades del adjudicatario se regirán por lo dispuesto en este Pliego de Prescripciones Técnicas y en el Pliego de Cláusulas Administrativas que rige esta licitación.

2. NORMATIVA DE CARÁCTER TÉCNICO

Será obligación del adjudicatario el cumplimiento del presente Pliego de Prescripciones Técnicas, del Pliego de Cláusulas Administrativas, así como de toda la legislación y normativa técnica vigente, tanto de carácter estatal, autonómico o municipal, que resulte de aplicación al objeto del contrato, incluyendo Directivas, Leyes, Reales Decretos, Reglamentos, Normas UNE, Instrucciones, Protocolos, o cualquier otra disposición normativa que pueda afectar al servicio objeto de la licitación.

Igualmente, el adjudicatario estará obligado a cumplir las posibles modificaciones o nuevas disposiciones legales que pudieran aprobarse durante la vigencia del contrato, debiendo adoptar de forma inmediata las medidas necesarias para respetar la legalidad vigente en todo momento.

Esta relación de normativa tiene carácter meramente orientativo y no restrictivo. Será responsabilidad del adjudicatario observar cualquier otra normativa, reglamento o instrucción oficial aplicable, aunque no esté citada expresamente en el presente Pliego.

Asimismo, el adjudicatario deberá cumplir durante toda la vigencia del contrato con lo establecido en los siguientes anexos del Pliego de Prescripciones Técnicas:

- **Anexo I: Seguridad de la información.**
- **Anexo II: Protección de datos.**
- **Anexo III: Normativa interna en materia de inteligencia artificial para proveedores.**

3. ALCANCE DEL SERVICIO

Las características técnicas para el servicio y mantenimiento del sistema de reconocimiento de voz que son objeto de la licitación se detallan en el punto 3.1 Descripción del servicio del presente pliego.

El servicio incluirá todos los accesorios necesarios aunque no esté especificados en las características, siempre y cuando fueran necesarios para el correcto funcionamiento del mismo. Se considera que forma parte del sistema y, por tanto, se considera incluido en la oferta:

- El software, licencias de uso y actualizaciones para su puesta en funcionamiento así como que en ningún momento el sistema esté inoperativo.
- Mano de obra y adaptación de los elementos existentes para garantizar el correcto funcionamiento del sistema.

Asimismo, el sistema dispondrá de:

- Manual de uso, el cual debe presentarse en castellano, incluyendo las características del sistema, así como una explicación detallada de su funcionamiento.

3.1 Descripción del servicio

Se requiere un sistema de dictado con reconocimiento de voz que permita en tiempo real y a una velocidad de conversación hablada transcribir en texto directamente sobre la historia clínica corporativa, este sistema incluirá licencias de software, hardware y dispositivos de entrada de voz (micrófonos).

El servicio incluiría a los Centros Hospitalarios de Majadahonda, Sevilla y Barcelona y al centro de Madrid (sito en la calle del Poeta Joan Maragall, 39) pudiendose ampliar, en caso necesario, a otros centros de FREMAP.

Las necesidades estimadas, al inicio del contrato, son:

Hospital / Centro	Licencias	Micrófonos
Barcelona	3	3
Majadahonda	7	4
Sevilla	4	3
Centro Asistencial Madrid	1	1
TOTAL	**15**	**11**

Estas necesidades podrán variar en función de las necesiadades del servicio, así como inclusión de nuevos centros hospitalarios y/o asistenciales.

3.2 Condiciones del servicio

En cuanto a los requisitos funcionales del sistema:

- Reconocimiento de voz en tiempo real con una precisión mínima del 95% en terminología médica.
- Transcripción directa sobre la historia clínica electrónica (HCE), RIS o PACS.
- Adaptación al vocabulario clínico específico de radiología y otras especialidades.
- Capacidad de aprendizaje automático (IA/Deep Learning) para mejorar la precisión con el uso.
- Navegación y corrección por voz, sin necesidad de teclado o ratón.
- Multidispositivo: compatible con ordenadores, tablets y móviles.
- SO: Windows 11 o superior.
- Idiomas soportados: español, además de la posibilidad de incluir idiomas soportados adicionales como: catalán, euskera, gallego y/o portugués.
- Generación automática de informes estructurados y plantillas personalizadas.
- Registro de actividad y generación de informes de uso e incidencias mensuales.
- No almacenamiento local de audios ni datos sensibles.
- Auditorías periódicas y plan de continuidad.

Respecto a los requisitos técnicos del software, deben cumplir como minino:

- Licencias nominales o concurrentes, con actualizaciones incluidas.
- Motor de reconocimiento de voz propio, entrenado en lenguaje médico.
- Integración con sistemas corporativos (HCE, PACS, RIS) mediante HL7, FHIR o API.
- Posibilidad de SDK disponible para integración personalizada.
- Despliegue flexible: en servidor local, nube privada o infraestructura del proveedor.
- Interfaz intuitiva, personalizable por especialidad y perfil clínico.
- MSI personalizable para despliegue centralizado o distribuido.

Requisitos técnicos del hardware (Micrófonos profesionales), con las siguientes características mínimas de calidad de captación de voz, ergonomía, conectividad y compatibilidad:

- Tipo de micrófono: Electret de condensador o equivalente de calidad profesional.
- Direccionalidad: Unidireccional con cancelación activa de ruido.
- Frecuencia de respuesta: Mínimo 200 Hz – 10.000 Hz.

o Relación señal/ruido: ≥ 70 dBA.

- Sensibilidad: Alta, optimizada para dictado en entornos clínicos.
- Uso con una sola mano: Botonera accesible y ergonómica.
- Material: Plástico ABS o similar, con superficie antimicrobiana.

o Peso: ≤ 200 g.

- Dimensiones: Adaptadas para uso prolongado sin fatiga.

- Interfaz: USB 2.0 o superior, Plug & Play, con una longitud mínima del cable de 2,5 metros. Opcional: Bluetooth con dongle seguro (en modelos inalámbricos).
- Compatibilidad: Con software ofertado.
- Drivers: No requiere instalación adicional en sistemas Windows 11 o superior.
- Botones programables: Para funciones como grabar, pausar, guardar, enviar.
- Altavoz integrado: Para reproducción de audio (opcional).
- Sensor táctil o trackball: Para navegación sin ratón (en modelos avanzados).
- Indicadores LED: Estado de grabación, conexión, batería (si aplica).
- Superficie antimicrobiana: Certificada para uso sanitario.
- Protección de datos: No almacenamiento local de audio.
- Certificaciones: CE, RoHS, ISO 9001, ISO 13485 (preferente).
- Sistemas operativos: Windows 11 o superior.

Las referencias se indican como orientativas de las características de calidad mínimas que deben tener los artículos ofertados por los distintos licitadores.

En la definición del servicio, puede haberse incluido de forma excepcional la referencia a una marca o producto concreto con el único propósito de identificar una parte del objeto del contrato, cuando no ha sido posible una descripción genérica por parte del personal técnico usuario del equipamiento. En estos casos, se deja constancia expresa de que dicha mención tiene carácter meramente orientativo y no limita la presentación de ofertas con soluciones técnicas equivalentes o superiores. De este modo, la existencia de mecanismos equivalentes o superiores garantizan la libre concurrencia y el acceso a la licitación por parte de cualquier licitador interesado impide que la inclusión de dicha referencia pueda considerarse causa suficiente para justificar la anulación del Pliego de Prescripciones Técnicas.

En caso de que, durante el proceso de valoración de las características técnicas del sistema ofertado, se constate que alguna de ellas pudiera tener carácter exclusivo, se podrán admitir soluciones técnicas alternativas que garanticen prestaciones equivalentes y sin que esas alteren el funcionamiento de la necesidad que recogen estos pliegos.

3.3 Operativa de la instalación del servicio

- La instalación y puesta en marcha será realizada por el servicio de asistencia técnica oficial del fabricante o autorizado, debidamente acreditado.

- La coordinación previa de las fechas y horarios de instalación será acordada con FREMAP para evitar interferencias en la actividad asistencial.

- El adjudicatario será responsable de la instalación del servicio, incluyendo la provisión de medios auxiliares si fueran necesarios.

La empresa adjudictaria deberá encargarse de la configuración del servicio para su correcta integración con los sistemas de FREMAP para lo cual en coordinación con la Mutua habrá de realizar

una planificación conjunta y detallada de todas las actividades para su consecución. Todo ello a cargo del licitador.

El adjudicatario será responsable de cualquier daño y/o desperfecto ocasionado durante todas las fases de instalación, directa o indirectamente, ya sea a personas, bienes o instalaciones de FREMAP.

Todos los costes derivados de la instalación y puesta en marcha, incluyendo medios auxiliares, y permisos estarán incluidos en la oferta económica.

3.4 Plazo de entrega del servicio

El plazo máximo de entrega efectiva del sistema de renconocimiento de voz requerido así como de los materiales y medios auxiliares será desde el inicio del contrato.

En caso de causa de fuerza mayor debidamente acreditada, podrá concederse una prórroga adicional de 30 días naturales, previa solicitud formal antes del vencimiento del plazo inicial, y validado, por escrito, por parte de FREMAP.

A efectos del cómputo del plazo se entiende que el servicio ha sido instalado de manera efectiva cuando el adjudicatario ha realizado sus pruebas de funcionamiento y puesta en marcha del servicio, así como el personal del Centro ha recibido la formación inicial establecida, de tal forma que sea posible, desde ese momento, su uso por FREMAP.

4. EJECUCIÓN DEL SERVICIO

- El adjudicatario realizará la renovación de las licencias identificadas en el apartado “Alcance del servicio” de este documento. Para ello FREMAP delegará en el adjudicatario los números de suscripción y/o números de serie que actualmente tiene en activo para que éste pueda realizar la renovación de las mismas. Esta información no puede ser comunicada a terceros sin el consentimiento expreso de FREMAP.

- El adjudicatario facilitará a FREMAP cualquier información o claves que su proveedor le proporcione de cara a contactar o a acceder a la zona privada de las web de los fabricantes.

- A la finalización del contrato el adjudicario se compromete a eliminar de sus sistemas la información relativa a los números de serie de las licencias de FREMAP que estuviera gestionando, así como los usuarios y contraseñas de acceso para FREMAP a las web de los fabricantes.

- El modelo de facturación debe ajustarse a un pago semestral.

- Todas la licencias objeto del contrato deberán figurar a nombre de FREMAP. En el supuesto de ser necesario el nombre de una persona de contacto de FREMAP el adjudicatario deberá contactar con el responsable del contrato para que éste le comunique quien o quienes serán. Asimismo, el adjudicario deberá designar un gestor de cuenta para la interlocución con FREMAP.

- La entrega de las licencias objeto del contrato se realizarán en formato digital al responsable del contrato.

Servicio de mantenimiento

En la duración del contrato, se incluirá el servicio de mantenimiento, tanto preventivo como correctivo, del sistema de reconocimiento de voz, así como cualquier sistuitución necesaria para el perfecto funcionamiento del sistema requerido, sin que ello, suponga un coste adicional para FREMAP.

Asimismo, deberá garantizarse la continuidad del servicio, actualización del software y disponibilidad de licencias.

5. GESTIÓN DE INCIDENCIAS

Cuando FREMAP detecte alguna incidencia en la ejecución del contrato, la pondrá en conocimiento del responsable designado por el adjudicatario, con el fin de que se adopten las medidas necesarias para su urgente y total subsanación. Las incidencias se comunicarán mediante correo electrónico -en caso de modificación de la dirección de email deberá comunicarselo a FREMAP con una semana de antelación- o por otro medio electrónico que el adjudicatario proporcione para ello.

El adjudicatario dará respuesta en un plazo máximo de:

- **1 hora** para respuesta de manera telemática
- **1 día hábil** para solución que requiera asistencia in situ.
- El tiempo de respuesta para el servicio no podrá ser superior en ningún caso a **1 día hábil** a contar desde la hora de envío de las consultas y considerando el horario de referencia indicado al final del punto 6 del Pliego de Prescripciones Técnicas.

Estos plazos comienzan a contar desde la hora de envío de la comunicación, aportando información sobre las causas de la incidencia y las actuaciones previstas para su urgente resolución.

El plazo de solución podrá ampliarse en supuestos excepcionales, a petición por escrito del adjudicatario, previa autorización de FREMAP que le será también trasladada por escrito , en el supuesto de que se encuentre debidamente justificada la causa.

6. INTERLOCUCIÓN Y ATENCIÓN AL CLIENTE

La empresa adjudicataria designará a una persona que actuará como interlocutor único con FREMAP, con conocimientos y capacidad suficiente para atender las necesidades diarias y que dispondrá de un teléfono y una dirección de correo electrónico de contacto. Esta persona será la responsable de atender en primera instancia las incidencias, peticiones y consultas que le traslade el responsable del contrato por parte de FREMAP en relación con el mismo.

El tiempo de respuesta para el servicio no podrá ser superior en ningún caso a **1 día hábil** a contar desde la hora de envío de las consultas y considerando el horario de referencia indicado al final del presente punto.

En caso de ausencia, el adjudicatario comunicará a FREMAP, con una semana de antelación, los datos de contacto de la persona que vaya a sustituirle.

Siempre que FREMAP lo requiera, el adjudicatario prestará asesoramiento técnico respecto a las distintas prestaciones objeto del contrato. Dicho asesoramiento se prestará preferentemente por vía telefónica o

correo electrónico, pudiendo ser presencial cuando FREMAP lo precise; en este último caso, los costes de traslado del personal de la empresa adjudicataria correrán exclusivamente por su cuenta. Esta obligación incluirá la elaboración de los presupuestos que la Mutua pudiera solicitar a efectos de las posibles modificaciones contempladas en el contrato, en un plazo nunca superior a **3 días hábiles** a contar desde el día siguiente a la comunicación de la petición.

Asimismo, el adjudicatario mantendrá informado a FREMAP sobre la entrada en el mercado de servicios que atañen al objeto del contrato que, como consecuencia del desarrollo tecnológico u otras innovaciones, mejoren las prestaciones y características de los habitualmente utilizados.

El adjudicatario contará además con un servicio de atención telefónica al cliente, en horario de 8:00 a 18:00 horas de lunes a viernes, para atender cualquier consulta relacionada con el objeto de contrato que sea comunicada por los centros de FREMAP. El número de teléfono de este servicio para los centros de FREMAP no podrá ser de tarificación especial.

7. CONTROL Y SUPERVISIÓN DE LA EJECUCIÓN DEL CONTRATO

Antes del inicio del contrato, se celebrará una reunión entre FREMAP y la empresa adjudicataria con objeto de presentar a los responsables e interlocutores por ambas partes y de concretar todos los aspectos necesarios para asegurar una óptima puesta en marcha del servicio.

La persona designada como responsable del contrato por parte del adjudicatario supervisará su normal desarrollo, manteniendo las relaciones necesarias con los responsables de FREMAP para garantizar su correcta y eficaz ejecución. De igual forma, FREMAP, a través de responsables designados en cada uno de sus centros, realizará el oportuno seguimiento del contrato a fin de que su ejecución se efectúe conforme a las condiciones estipuladas.

El adjudicatario facilitará al responsable del contrato por parte de FREMAP toda la información y documentación que éste solicite para disponer de un pleno conocimiento técnico del desarrollo del contrato, además de la relativa a los eventuales problemas técnicos o actualizaciones que puedan plantearse y de las tecnologías, métodos y herramientas utilizadas para resolverlos.

FREMAP podrá requerir al adjudicatario cuando lo estime oportuno, cualquier información o documentación relacionada con el contrato, así como la celebración de reuniones de seguimiento en el lugar que señale FREMAP y en la fecha que se consensúe entre ambas partes.

Si se detectaran deficiencias graves o sistemáticas en la ejecución del contrato, éstas se notificarán por correo electrónico al adjudicatario, que tendrá la obligación de remitir a FREMAP, en un plazo máximo de 3 días hábiles, un informe pormenorizado de las causas que han motivado dichas deficiencias y que recoja las medidas a adoptar y el plazo previsto de resolución, que en ningún caso superará los 5 días hábiles a contar desde la fecha de respuesta.

8. PREVENCIÓN DE RIESGOS LABORALES

En cumplimiento de lo establecido en el artículo 24 de la Ley de Prevención de Riesgos Laborales y del R. D. 171/2004 sobre coordinación de la actividad preventiva, el adjudicatario deberá entregar para la firma del contrato una declaración responsable acreditativa del cumplimiento de la normativa en materia de prevención de riesgos laborales, con arreglo al modelo disponible en el perfil de contratante de la Mutua

(Criterio de búsqueda: campo "Nombre O. Contratación" = "Director Gerente de FREMAP" ® Pestaña "Documentos" ® Sección "Otros documentos").

9. ANEXO I - SEGURIDAD DE LA INFORMACIÓN

El sistema de gestión de seguridad de la información de FREMAP se basa en marcos de trabajo reconocidos nacional e internacionalmente, en concreto la norma ISO 27001, en la que FREMAP está certificada desde 2018, y el Esquema Nacional de Seguridad en el que FREMAP está certificada en su categoría ALTA desde 2025.
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.
- "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.

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.

Estos requisitos son de obligado cumplimiento y serán evaluados de forma continua a lo largo de la vida del contrato, pudiendo solicitarse las evidencias oportunas. Cualquier deficiencia o incumplimiento se considerará una prestación defectuosa del objeto del contrato, pudiendo aplicarse las penalidades que correspondan o la resolución del contrato según se indique en el Pliego de Cláusulas Administrativas.
El adjudicatario se compromete a realizar de Evaluaciones de Riesgos utilizando para ello una metodología reconocida internacionalmente que garantice la seguridad de los servicios prestados. FREMAP podrá requerir la documentación del último Análisis de Riesgo realizado.

El adjudicatario igualmente se compromete a realizar revisiones periódicas y actualizar el análisis de riesgos ante cambios tecnológicos significativos en los servicios a FREMAP y a mantener un plan para gestionar los riesgos que puedan afectar los servicios prestados a FREMAP.

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

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.

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.

El adjudicatario se compromete a implementar medidas rigurosas para asegurar la identificación y el acceso seguro a la información, a los sistemas y a los servicios de FREMAP.

Identificación de Usuarios
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.

Control de Acceso
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.

Segregación de Funciones y Tareas
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.

Gestión de Derechos de Acceso
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.

Mecanismos de autenticación
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 registrar 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.

Mecanismos de Autenticación (Usuarios de la Organización)
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.

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.

El adjudicatario se compromete a identificar y gestionar los medios de almacenamiento a través de un sistema de etiquetado comprensible. Igualmente establecerá procedimientos para todos los medios de información que garanticen la seguridad de estos en los procesos tanto de administración, acceso, custodia, manejo, eliminación, etc.

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.

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.

Gestión de incidentes

El adjudicatario se compromete a establecer un proceso integral, documentado y detallado para la gestión de incidentes 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.

El adjudicatario deberá implementar soluciones de ventanilla única para la notificación de incidentes al CCN-CERT. El proceso integral de gestión de incidentes debe incluir la implantación de medidas urgentes según el tipo de incidente, 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.

El adjudicatario deberá implementar 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 ciberamenazas sofisticadas y campañas de ataques.
Implementar 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.

Registro de actividad

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

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.

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 de FREMAP y el 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.

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.

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.

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.

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.

El adjudicatario de servicios en la nube (Cloud) se compromete a cumplir con medidas de seguridad específicas para cada modelo de servicio ofrecido (SaaS, PaaS, IaaS) según las guías CCN-STIC aplicables. Si se utilizan servicios en la nube de terceros, 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.

Finalmente, debe garantizarse que la configuración de seguridad de los sistemas que proporcionan estos servicios cloud se realiza según la correspondiente guía CCN-STIC de Configuración de Seguridad Específica.

El Adjudicatario deberá llevar a cabo un análisis de impacto en estrecha colaboración con FREMAP, adaptándose a sus políticas y requerimientos específicos. Este análisis se centrará en determinar los

requisitos de disponibilidad para cada servicio, evaluando el impacto potencial de una interrupción durante un periodo de tiempo determinado.
Este proceso de análisis de impacto no solo se llevará a cabo internamente, sino que también deberá integrar las perspectivas y consideraciones proporcionadas por FREMAP.

El adjudicatario deberá implementar un plan de continuidad sólido y eficaz que aborde todas las fases de interrupción desde su inicio hasta su conclusión de modo que se garantice la continuidad de los servicios de FREMAP.

Plan de continuidad
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.

En situaciones de emergencia, se activará un plan de contingencia que incluirá comprobaciones integrales del sistema operativo, firmware y ficheros de configuración para garantizar la integridad del sistema.

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.

Pruebas Periódicas
El adjudicatario deberá realizar pruebas periódicas para localizar y corregir errores o deficiencias del plan siguiendo un procedimiento establecido que incluirá la corrección de problemas identificados y la realización de los informes de prueba.

Medios Alternativos
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.

El adjudicatario se compromete a disponer de herramientas especializadas que permitan la detección, prevención de intrusiones y monitorización de eventos de seguridad. Los registros generados, de los eventos de seguridad y la actividad de los usuarios, deben de estar protegidos contra manipulaciones indebidas y no autorizadas.

Asimismo, el adjudicatario deberá implementar:

- Sistema de reglas predefinidas que permitan generar alertas en los casos de detección de intrusiones.
- Sistema que permita la correlación de los eventos de seguridad.
- Soluciones de vigilancia que permitan determinar la superficie de exposición con relación a vulnerabilidades y deficiencias de configuración y sistemas para detección de amenazas avanzadas.
- Sistemas de detección de amenazas avanzadas y comportamientos anómalos, así como, sistemas para la detección de amenazas persistentes avanzadas (Advanced Persistent Threat, APT), mediante la identificación de anomalías significativas en el tráfico de la red.
- Observatorios digitales con fines de cibervigilancia dedicados a la detección y seguimiento de anomalías.

- Medidas para prevenir, detectar y reaccionar frente a intentos de minería de datos como limitación de consultas, monitorizando su volumen y frecuencia; y alerta a los administradores de seguridad ante comportamientos sospechosos en tiempo real.
- Inspecciones de seguridad periódica o tras incidentes que hayan revelado vulnerabilidades del sistema, incluyendo verificación de configuración, análisis de vulnerabilidades y pruebas de penetración.
- Procedimientos de respuesta a las alertas generadas por el sistema, de manera que en función de estas se ejecuten unas acciones u otras.

FREMAP podrá solicitar datos precisos que posibiliten evaluar el comportamiento del sistema de gestión de incidentes de acuerdo con la Instrucción Técnica de Seguridad de Notificación de Incidentes de Seguridad y con la correspondiente guía CCN-STIC 817, más concretamente, podrá solicitar información sobre los indicadores previstos en el apartado "5.2 Métricas de resolución de incidentes" de dicha guía.

El adjudicatario implementará medidas estrictas para controlar el acceso a áreas críticas, como los Centros de Proceso de Datos (CPD), asegurando que los accesos a las instalaciones estén cerrados para evitar accesos no autorizados. Se utilizarán sistemas de acceso y métodos de identificación para regular la entrada a oficinas y CPD, restringiendo el ingreso solo a personal autorizado y empleando videovigilancia para monitorizar las actividades.

Los activos de información de FREMAP estarán físicamente resguardados en áreas de acceso controlado o contenedores seguros. Igualmente, todas las entradas y salidas serán registradas y supervisadas, comunicando a FREMAP cualquier intento de acceso indebido. En todo caso, FREMAP podrá solicitar registros detallados de estas operaciones.

Registro de entrada y salida de equipamiento

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.

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.

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.

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.

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.

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.

Equipos conectados a la red

En los casos en los que el adjudicatario disponga de equipos o dispositivos que estén conectados a la red pudiendo tener o permitir el acceso a la información responsabilidad de FREMAP, estos deberán tener una configuración de seguridad que garantice el control del flujo de entrada y salida de la información. Si estos dispositivos disponen de almacenamiento temporal o permanente de información, se configurarán para poder eliminar esta información. De acuerdo a lo anterior:

- El licitador incluirá equipamientos y soluciones relacionados en el "*Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y la Comunicación - TIC CCN-STIC 105*", la "*Guía de Taxonomía de referencia para productos de seguridad - TIC CCN-STIC 140*" o bien acreditar el cumplimiento de la norma "*ISO/IEC 15408 (Common Criteria)", Directiva NIS2* o equivalente. En el caso de que los elementos hayan sido expresamente requeridos o bien existan componentes que aporten un valor diferencial para cubrir necesidades técnicas específicas sin estar relacionados en las guías indicadas, el licitador deberá incluir en su oferta las medidas de seguridad compensatorias que serán ejecutadas a efectos de valorar el cumplimiento de lo establecido en el Esquema Nacional de Seguridad en su nivel ALTO. En el caso de que los componentes estén en proceso de certificación, hará constar en su oferta la fecha estimada de certificación y declaración responsable al efecto. Además de lo anterior, el adjudicatario mantendrá la vigencia del cumplimiento y/o medidas compensatorias durante toda la vida del contrato, proporcionando información actualizada a FREMAP y declaración responsable al efecto.
- El licitador incluirá en su oferta el borrado seguro de los datos cada vez que un equipo sea retirado o sustituido, utilizando una herramienta de borrado relacionada en el "*Catálogo de Productos y*

Servicios de Seguridad de las Tecnologías de la Información y la Comunicación - TIC CCN-STIC 105" o la "*Guía de Taxonomía de referencia para productos de seguridad - TIC CCN-STIC 140*" o bien acreditar el método de borrado seguro que se va a llevar a cabo, asegurando en cualquier caso que incluye un borrado con sobreescritura a bajo nivel de forma que los datos no sean recuperables en ningún caso, en cumplimiento de lo establecido en el Esquema Nacional de Seguridad en su nivel ALTO. Además de lo anterior, el adjudicatario mantendrá la vigencia del cumplimiento y/o medidas compensatorias durante toda la vida del contrato, proporcionando registro de borrado, certificados de borrado a FREMAP y declaración responsable al efecto.

Bloqueo del puesto de trabajo

El adjudicatario deberá tener configurado, en los terminales usados para la prestación del servicio, un sistema de bloqueo automático tras un periodo de inactividad. Este periodo no podrá ser superior a 5 minutos y no podrá ser modificado por los empleados. Este sistema de bloqueo requerirá el uso de clave cada vez que se reanude la actividad.

La sesión del usuario será cancelada y deberá ser introducida una contraseña cada vez que el equipo tenga un periodo largo de inactividad.

Seguridad de Red

El adjudicatario se compromete a implementar medidas de seguridad específicas para proteger la información de FREMAP. Esto incluye establecer un sistema de seguridad perimetral con firewall para filtrar y controlar el tráfico entre redes internas y externas. Se debe garantizar la confidencialidad, integridad y autenticidad de la información en reposo y en tránsito, utilizando conexiones VPN seguras para comunicaciones fuera del dominio del adjudicatario, según las directrices del CCN-STIC 836. Además, se implementarán protocolos de autenticación como TLS/SSL y se utilizarán herramientas como IDS/IPS para detectar y responder a violaciones en el sistema.

El adjudicatario deberá disponer de un sistema de segmentación de redes realizado a través de un método reconocido (LAN físicos, VLAN, Virtualización de redes, etc.) que permita diferenciar entre segmentos externos y segmentos internos, incluyendo en los casos necesarios la segmentación de una red para invitados. Esta segmentación debe de quedar reflejada en la documentación de arquitectura de sistema del adjudicatario.

La segmentación debe procurar al menos:

- La segregación de segmentos entre equipos y por roles.
- Control de entrada de los usuarios que pueden trabajar en cada segmento.
- Control de salida de la información disponible en cada segmento.
- Control de entrada de las aplicaciones utilizables en cada segmento.
- Control del flujo de tráfico entre segmentos.

La información responsabilidad de FREMAP deberá estar alojada en segmentos que sean de acceso exclusivos a los usuarios autorizados para cumplir con la prestación del servicio. En los casos en los que se trate información altamente sensible se deberá tener una capa de protección firewall.

El adjudicatario debe garantizar la inexistencia de protocolos directos entre los segmentos internos y externos y la implementación de puntos de interconexión internos como método de defensa ante intrusiones. Estos puntos de interconexión deben estar correctamente asegurados y monitorizados.

El adjudicatario deberá disponer de un sistema de marcado de soportes (físicos y lógicos) que permita establecer marcas o metadatos en aquellos soportes que contengan información responsabilidad de FREMAP.

El etiquetado de los soportes se realizará identificando los mismos con el nivel más alto de la calificación de la información que contienen, sin revelar su contenido, e indicando el nivel de seguridad que requiere la información contenida o a través de un sistema de códigos o referencias interno que indique igualmente las normativas y procedimientos que deben aplicarse a los mismos.

Toda la información propiedad de FREMAP debe tener, al menos, la consideración equivalente a información de uso interno y/o restringida. No tendrá carácter público salvo que se disponga expresamente de lo contrario por FREMAP.

Cualquier información clasificada como confidencial o altamente sensible propiedad de FREMAP y, en particular, la información sobre las infraestructuras de TI de FREMAP de la que el adjudicatario tenga conocimiento, así como la generada por el propio adjudicatario en base al servicio prestado a FREMAP, debe ser protegida, procesada y almacenada de manera segura mediante métodos de criptografía. Esto incluye tanto los dispositivos (tanto fijos como portátiles), como las bases de datos y repositorios que contengan datos de los que FREMAP sea responsable del tratamiento.

Los algoritmos de cifrado deben cumplir con los protocolos (TLS, SSL, etc.) y mecanismos criptográficos autorizados (Cifrado simétrico, acuerdo de claves, etc.). Así como, deben establecerse con longitudes de clave conformes a las prácticas y normas internacionalmente reconocidas.

El Adjudicatario tiene la obligación de salvaguardar las claves de cifrado mediante la implementación de mecanismos adecuados de seguridad a lo largo de todo su ciclo de vida.

El Adjudicatario deberá tener actualizada la documentación pertinente relacionada con la administración de claves de cifrado en el caso de que sea requerida por FREMAP.

El Adjudicatario igualmente cifrará las copias de seguridad con los mismos algoritmos y parámetros que para el resto de información.

El adjudicatario deberá emplear productos certificados en base a la Guía para la realización del proceso de cifrado.

El adjudicatario, para asegurar la custodia adecuada de la información de FREMAP y los dispositivos y/o soportes (incluidos los soportes en papel) que la contienen, se compromete a garantizar su mantenimiento siguiendo las recomendaciones del fabricante y aplicará un procedimiento de control de acceso a los mismos. Además, debe garantizar el transporte seguro de estos dispositivos y/o soportes mediante registros precisos y protección criptográfica. Al finalizar el contrato o si los dispositivos son reutilizados, debe implementar métodos seguros para el borrado de información o destrucción de los dispositivos, asegurando que la información eliminada no sea recuperable. Igualmente, debe proporcionar a FREMAP un registro detallado de los dispositivos y/o soportes borrados o destruidos y así como compartir los contratos y medidas de seguridad si externaliza estos servicios.

El adjudicatario que disponga de aplicaciones de desarrollo “in-house” usadas para la prestación del servicio deberá disponer de una política y procedimiento de desarrollo seguro que podrán ser requeridas por parte de FREMAP.

En estas políticas deben identificar al menos los siguientes extremos:

1. Principios de seguridad y recomendaciones de seguridad que garanticen un desarrollo seguro.
2. Existencia de entornos separados, estando separados los entornos de desarrollo, producción y preproducción.
3. Aplicación de una metodología de desarrollo que sea un estándar reconocido que incluya la seguridad como parte integral (ej.: DevSecOps, Métrica, Owasp, etc.) que, al menos:
    a) Tenga en consideración los aspectos de seguridad a lo largo de todo el ciclo de vida desde el inicio, no concibiendo el desarrollo únicamente en el apartado funcional.
    b) Garantice que durante las pruebas de desarrollo y de aceptación se utilizarán datos específicos que no sean reales, y en caso de serlo serán modificados y se asegurará el nivel de seguridad correspondiente.
    c) Permita la inspección del código fuente tanto durante el desarrollo como durante la vida útil del software, pudiendo analizar incidentes y permitiendo la realización de pruebas de pentesting.
4. Identificación de los siguientes elementos como parte integral del diseño del sistema:
    a) Los mecanismos de identificación y autenticación necesarios para garantizar la seguridad de acceso.
    b) Los mecanismos de protección de la información tratada a través de técnicas de validación, criptografía, gestión segura de archivos, seguridad en las transacciones y comunicaciones, etc.
    c) Un sistema de gestión de errores y registro seguro.

Como recomendación general, FREMAP recomienda seguir el informe de buenas prácticas sobre desarrollo seguro del CCN-CERT.

FREMAP podrá solicitar evidencias de seguridad del software del adjudicatario para su integración. Esto incluye pruebas de funcionamiento y configuración segura, revisión de componentes incluyendo capacidades de interacción con otros softwares y/o usuarios, y vulnerabilidades, verificación de librerías seguras, y pruebas de pentesting. Además, se deben seguir las guías de instalación segura, uso y relación cliente-adjudicatario para aplicaciones on-premise.

El adjudicatario deberá facilitar a FREMAP evidencias de que se han realizado las pruebas en un entorno separado seguro y que no han afectado al entorno de producción, ni alterado los datos, asegurando de esta forma el nivel de seguridad adecuado a los datos utilizados en caso de que no pueda garantizarse el uso de datos ficticios.

El adjudicatario dispondrá de un sistema de calificación de la información que permitirá establecer la escala de criticidad de la información manejada por la empresa y su ámbito de difusión según su clasificación.

Este sistema de calificación debe tener en cuenta al menos los siguientes criterios:

- Procedencia: La información procedente de la posición jerárquica de FREMAP más elevada deberá tener la categoría más alta.
- Contenido: La información de FREMAP estará clasificada en base a criterios establecidos por FREMAP, debiendo el adjudicatario mantener esta clasificación.
- Confidencialidad: El acceso a la información usada en la prestación de servicio a FREMAP debe estar restringida a las personas indicadas para cada tipo de información.

Toda la información propiedad de FREMAP debe tener, al menos, la consideración equivalente a información de uso interno y/o restringida. No tendrá carácter público salvo que FREMAP disponga expresamente lo contrario.

La calificación de la información deberá llevar incorporado un sistema de etiquetado correspondiente a los niveles clasificatorios establecidos, independientemente del soporte donde se encuentre almacenada esta información.

El adjudicatario se compromete a implementar un procedimiento de limpieza que incluya la eliminación de metadatos y datos ocultos en los documentos, asegurando de que solo contengan la información necesaria para el servicio. Además, informará a FREMAP sobre las herramientas específicas utilizadas para ello.
El adjudicatario deberá implementar una normativa de copias de seguridad y recuperación acorde a la guía CCN-STIC-822 Anexo III, asegurando la capacidad de restaurar la información del servicio prestado a FREMAP en caso de pérdida o destrucción. En caso de externalización del servicio, el adjudicatario proporcionará a FREMAP las evidencias y los informes detallados correspondientes.

El adjudicatario debe establecer protocolos formales de copias de seguridad y restauración. Estos protocolos deben:

- Ser probados de forma regular, estableciendo periodos de pruebas adaptados a la criticidad de la información.
- Establecer la frecuencia de las copias de seguridad.
- Establecer copias de respaldo semanales o mensuales adicionales a las copias de seguridad diarias.
- Establecer medidas de seguridad para el almacenamiento en las instalaciones y controles para el acceso autorizado a las copias de respaldo.
- Establecer medidas de seguridad para el almacenamiento en lugares fuera de las instalaciones en aras de evitar incidentes que puedan afectar tanto al repositorio original como a la copia.

El adjudicatario se compromete a implementar medidas para el uso seguro del correo electrónico y los navegadores web, como la autenticación de dos factores para el acceso, configuración de filtros SPAM para protección contra virus, actualización regular de navegadores con plugins permitidos, y uso de tecnologías como DNSSEC y HTTPS para asegurar las comunicaciones. Igualmente, se establecerán normas de uso que limiten el correo electrónico a fines laborales y regulen el uso seguro de navegadores web. Se proporcionarán evidencias de la configuración segura del servidor de correo electrónico cuando sea aplicable, y se realizarán formaciones enfocadas en concienciar sobre riesgos como el phishing.

El adjudicatario deberá cumplir con las medidas y configuraciones de seguridad recomendadas por el CCN en su guía CCN-STIC-812, entre ellas:

- Configuración segura del control de acceso a la información garantizando que el servidor ofrezca acceso a la información por vías alternativas al protocolo determinado, así como, que tenga medidas para evitar la manipulación de URL, prevenir manipulación de las cookies, ataques de inyección de código y ataques de “cross site scripting”.
- Presentar evidencias, a petición de FREMAP, de la realización de auditorías de seguridad de “caja negra” (pruebas de intrusión y Web Application Security Scanners - WASS) durante la fase de desarrollo y producción.
- Presentar evidencias, a petición de FREMAP, de la realización de auditorías de seguridad de “caja blanca” (revisión de código manual y automático) durante la fase de desarrollo.
- Implementación de medidas para evitar ataques “proxies” y de “cache”.

El adjudicatario deberá establecer las medidas preventivas y reactivas necesarias frente a ataques de denegación de servicio (DOs Denial of Service) y denegación de servicio distribuido (DDoS) que puedan afectar a la información y/o al servicio prestado. Para ello:

- El adjudicatario deberá realizar un análisis de sus servicios para determinar la capacidad que será suficiente para atender la carga prevista de forma estable.

- El adjudicatario, a petición de FREMAP, deberá aportar la planificación y la dotación que está prevista para el sistema en base al análisis anterior.
- El adjudicatario deberá implementar las medidas técnicas de prevención necesarias. Algunas de estas medidas pueden ser las siguientes:
    - Instalación del enrutador configurado con una lista de control de acceso (ACL)
    - En los casos necesarios, cuando la carga prevista sea elevada, se instalará un proxy inverso para una gestión correcta de la carga del servicio entre varios servidores.
    - Configuración correcta de puertos de acceso.
    - Configuración de parámetros de registros como SynAttackProtect o TcpMaxPortsExhausted para el control de las conexiones TCP/IP.
    - Se establecerá un sistema de detección de ataques y bloqueo como puede ser un “Web Application Firewalls”
- En los casos de uso de aplicaciones web para el desarrollo del servicio que incluyan la recogida de datos personales será obligatorio el uso de protocolo TLS actualizado a la última versión.
- Se establecerán procedimientos de reacción a los ataques, incluyendo la comunicación con el adjudicatario de las comunicaciones.

10. ANEXO II – PROTECCIÓN DE DATOS

En el caso de que para la prestación del servicio de mantenimiento, el adjudicatario no necesite acceder para su tratamiento a datos personales de la responsabilidad de FREMAP, se le considerará como prestador de servicios sin acceso a datos y se regularán sus obligaciones de protección de datos de conformidad con los puntos siguientes:

- Se atendrá a las instrucciones de FREMAP comprometiéndose a informar a sus trabajadores de la prohibición de acceder a datos de carácter personal o a los recursos del sistema de información durante la realización de las tareas que les sean encomendadas por FREMAP, sin su previa autorización.

- Si los servicios objeto de contrato se van a desarrollar en los locales de FREMAP, deberá informar a los trabajadores sobre la prohibición de acceso a cualquier área, zona o espacio físico dentro de las instalaciones de FREMAP, así como del acceso y/o sustracción de cualquier información técnica u otras, sin previa autorización.

- En caso de que, por cualquier motivo, se produzca algún acceso a datos de FREMAP, voluntario o accidental, no previsto en este contrato, el prestador del servicio y sus trabajadores se comprometen a ponerlo en conocimiento de FREMAP a la mayor brevedad posible, quedando obligados en todo caso al secreto profesional sobre las informaciones de las que hayan podido tener conocimiento. No obstante, el prestador del servicio se reserva el derecho de requerir a sus empleados la firma de cláusulas de confidencialidad y deber de secreto.

11. ANEXO III – 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.

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.