Expediente N.º. LICT/99/145/2024/0252

Pliego de Prescripciones Técnicas para la Contratación de los servicios de consultoría para el cumplimiento de la normativa en materia de Inteligencia Artificial en FREMAP, Mutua Colaboradora con la Seguridad Social nº61.

ÍNDICE

1. OBJETO

El objeto de la presente licitación es la contratación, por parte de FREMAP, de los servicios de consultoría para la adecuación y cumplimiento de la normativa de Inteligencia Artificial en la entidad y, en particular, al Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial.

Este servicio de consultoría comprenderá el asesoramiento, formación y soporte continuo en materia de Inteligencia Artificial, la implantación de un modelo de gobernanza de la IA, la redacción e implementación de aquellos documentos, procedimientos y/o políticas que resulten necesarios para tal fin, así como los sistemas de revisión, actualización, verificación y validación continua del cumplimiento de las obligaciones que en esta materia pudieran ser exigibles a esta Mutua de acuerdo con la normativa y criterios vigentes en cada momento:

2. NORMATIVA DE CARÁCTER TÉCNICO

- Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial y por el que se modifican los Reglamentos (CE) N.º 300/2008, (UE) N.º 167/2013, (UE) N.º 168/2013, (UE) 2018/858, (UE) 2018/1139 y (UE) 2019/2144 y las Directivas 2014/90/UE, (UE) 2016/797 y (UE) 2020/1828 (Reglamento de Inteligencia Artificial).

- Reglamento (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos).

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Esta clasificación normativa no tiene carácter restrictivo, debiendo observarse en la ejecución de los trabajos cualquier otro tipo de reglamento, norma, criterio o instrucción oficial (de carácter europeo, estatal o autonómico) 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. CONSIDERACIONES PREVIAS

3.1 Naturaleza de FREMAP.

FREMAP es una Entidad Colaboradora con la Seguridad Social, sin ánimo de lucro, autorizada por el Ministerio de Inclusión, Seguridad Social y Migraciones, que tiene por objeto colaborar en la gestión de las prestaciones económicas y de la asistencia sanitaria, incluida la rehabilitación, comprendidas en la protección de las contingencias profesionales, así como la prestación económica de las contingencias comunes, de los trabajadores de sus empresas asociadas y trabajadores autónomos adheridos mediante los documentos de asociación, en los términos legalmente previstos en el artículo 80 y siguientes del Real Decreto Legislativo 8/2015, de 30 octubre, por el que se aprueba el Texto Refundido de la Ley General de la Seguridad Social.

A tal efecto, FREMAP forma parte del sector público estatal de carácter administrativo, de conformidad con la naturaleza pública de sus funciones y de los recursos económicos que gestiona, sin perjuicio de la naturaleza privada de la entidad, como asociación privada de empresarios.

Es de advertir que, el objeto de negocio de **FREMAP** no es, en ningún caso, el desarrollo ni la distribución de sistemas de inteligencia artificial, por lo que **actuará, principalmente, como responsable del despliegue de sistemas de IA de terceros.**

3.2 Causa del contrato.

El Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial, establece una serie de obligaciones y prácticas prohibidas en la puesta en servicio y la utilización de sistemas de Inteligencia artificial, tanto a proveedores y distribuidores como a responsables del despliegue de estos sistemas, para garantizar un elevado nivel de protección de la salud, la seguridad y los derechos fundamentales, incluidos la democracia, el Estado de Derecho y la protección del medio ambiente.

A mayor abundamiento, dichos sistemas de IA están sujetos a un mayor control cuando se encuentran destinados a la utilización de la gestión de trabajadores, acceso a servicios esenciales y prestaciones, tanto públicos como privados y, en particular, cuando evalúen la admisibilidad de las personas para ser beneficiarios de servicios y prestaciones esenciales de asistencia pública, incluidos los servicios de asistencia sanitaria, así como para conceder, reducir o retirar dichos servicios y prestaciones o reclamar su devolución.

A tal efecto, FREMAP ha constituido una comisión de adaptación a la normativa en materia de IA, integrada por las diferentes subdirecciones y áreas implicadas, entre las que se encuentra RR.HH., Protección de Datos, Seguridad en la Información, DTI y Asesoría Jurídica, desde la cual se ha elaborado una política de uso de IA, que resultará de aplicación a todos sus empleados, a los miembros de los órganos de gobierno y participación de la entidad, así como a los profesionales y proveedores externos vinculados a la Mutua. Asimismo, se ha elaborado un análisis GAP efectuado por un consultor externo que evalúa la situación de la entidad en relación con su adaptación al RIA y establece las próximas actuaciones a llevar a cabo para la adaptación al citado reglamento.

Así pues, con el fin de garantizar el cumplimiento de todas las obligaciones que pudieran imponerse a esta Mutua, resulta necesaria la contratación de los servicios de consultoría que asegure la correcta adecuación y adaptación de los sistemas de gestión de FREMAP en materia de inteligencia artificial a la normativa vigente.

3.3 Condiciones de realización del servicio.

La empresa adjudicataria se compromete a prestar el servicio de acuerdo con lo establecido en los pliegos, utilizando para ello los medios personales, mecánicos, informáticos o de cualquier otra naturaleza que considere mejor para garantizar la finalidad perseguida y para la resolución de incidencias que surjan durante la ejecución del contrato. Los medios utilizados para la prestación del servicio serán por cuenta de la adjudicataria.

La empresa adjudicataria ofrecerá un servicio personalizado con la designación de un **responsable** con preparación y experiencia mínima de 4 años en la materia del objeto de la licitación, que actuará de interlocutor con la Mutua, y será la persona a la que se le remitirán todas las comunicaciones.

FREMAP se reserva el derecho de solicitar otro interlocutor responsable. Cualquier cambio en la persona designada será inmediatamente comunicado a FREMAP informando de los datos del nuevo responsable asignado.

La empresa adjudicataria del contrato pondrá a disposición de FREMAP una línea telefónica y una dirección de correo electrónico las 24 horas del día durante los 365 días del año, con objeto de atender los requerimientos derivados de este contrato.

La prestación del servicio de consultoría deberá adaptarse al organigrama, estructura, documentación interna y procesos establecidos por FREMAP.

3.4 Carácter confidencial de los datos aportados

Toda la información que reciba la empresa adjudicataria con motivo de la celebración de la presente licitación y posterior contrato será considerado estrictamente confidencial y sólo será utilizada en el marco de la presente contratación.

En consecuencia, no se podrá utilizar ni proporcionar a terceros datos o información de carácter personal para finalidades distintas a aquellas para las que los datos hubieran sido recogidos, estando por tanto obligadas a poner todos los medios a su alcance para garantizar el carácter confidencial de esta información, así como los resultados obtenidos.

Cualquier infracción en este sentido será calificada como grave y será causa de resolución del contrato, sin perjuicio de las responsabilidades penales o de cualquier otro tipo en que pudieran incurrir.

4. CONSIDERACIONES PREVIAS

Se detallan a continuación los servicios objeto de contratación recogidos en el presente Pliego:

4.1 Asesoramiento en la gestión de riesgos y apoyo continuado en materia de IA.

La empresa que resulte adjudicataria de la presente licitación deberá diseñar/revisar e implementar un procedimiento de inventariado y categorización de sistemas de IA, así como un procedimiento de gestión de riesgos en sistemas de IA.

Una vez implantados los procedimientos anteriores, la adjudicataria proporcionará a la entidad el asesoramiento necesario en la gestión de riesgos y apoyo continuado en materia de IA para cumplir con las obligaciones que la normativa de aplicación pueda imponer a FREMAP.

Dicho asesoramiento comprenderá la resolución de cuestiones, mediante notas o informes, que pudieran plantearse en los procesos de análisis de riesgos y evaluaciones de impacto del sistema de IA, incluida la identificación de posibles riesgos para la salud, seguridad y derechos fundamentales, así como la implementación de medidas preventivas y correctivas para la minimización de dichos riesgos.

Asimismo, la empresa adjudicataria prestará su apoyo en los procesos de documentación, triaje, categorización y registro de los sistemas de IA, en relación con los diferentes niveles de riesgo, (mínimo, limitado, alto e inadmisible), que prevé la norma.

4.2 Formación y concienciación en materia de IA.

El adjudicatario deberá proporcionar formación continua al personal de FREMAP sobre el uso y gestión de los sistemas de IA. Esta información incluirá aspectos técnicos, éticos y legales, asegurando que el personal esté capacitado para manejar los sistemas de IA de manera responsable y conforme a la normativa vigente, en cumplimiento de las obligaciones de alfabetización de la entidad.

A estos efectos, el adjudicatario diseñará y entregará a FREMAP, para la divulgación a sus empleados, 3 píldoras que deberán incluir locuciones profesionales y subtituladas. La duración de estas no será inferior a 3 minutos y se realizarán en un formato compatible con los sistemas de la Mutua.

Asimismo, el adjudicatario diseñará y entregará a FREMAP un curso inicial en formato online destinado a todos los empleados, sobre el uso adecuado de las herramientas de IA y las obligaciones legales en esta materia. Dicho curso se entregará durante los dos primeros meses de vigencia del contrato, debiendo realizarse en un formato compatible con los sistemas de la Mutua y tendrá una duración aproximada de 60 minutos.

En este sentido, el contenido online del curso deberá estar producido en formato SCORM 1.2 o SCORM 2004, visible en cualquier dispositivo móvil, para su completa integración en la plataforma de aprendizaje LMS de FREMAP.

Este paquete SCORM será propiedad de FREMAP y dispondrá de control de visionado, seguimiento y evaluación a través de actividades de pregunta/respuesta, así como una evaluación final mediante cuestionario que deberá configurarse para que el usuario alcance un 70% de aciertos. El SCORM deberá estar configurado con un "completed", si el usuario supera el curso, y un "failed" si no lo supera.

El diseño y el contenido de las acciones formativas deberá ser de calidad gráfica y técnica alta, deberá incluir locuciones profesionales y subtitulados cuando corresponda, con recursos creativos e interactivos que incentiven el interés del alumnado, y emplearán el "Look and Feel" de FREMAP, (se facilitará libro de estilos), respetando un equilibrio entre imágenes y texto, uniformidad de colores y tiempo de carga inferior a 5 segundos. En todo caso, dichas acciones formativas tendrán que ser previamente aprobadas por FREMAP.

La metodología del curso estará basada en la adquisición y asimilación de ideas a través de contenidos claros y coherentes, bien estructurados y con un diseño atractivo en pantalla.

Sin perjuicio de la formación que se imparta con carácter general a todos los empleados, se podrán establecer formaciones especificas por áreas técnicas, en función de las necesidades y la finalidad de los sistemas de IA de la entidad. Esta formación será valorada conforme al criterio de formación específica en distintas áreas.

De igual modo, el adjudicatario deberá implementar medidas de concienciación y uso responsable de los sistemas de manera periódica.

4.3 Implantación de un modelo de gobernanza de la IA en la entidad.

El adjudicatario dará el soporte necesario para definir un sistema interno de gobernanza de la IA que permita establecer los roles y responsabilidades de cada uno de los departamentos o áreas respecto de los sistemas de gestión de la IA que deberá ser aprobado por los órganos de gobierno de la entidad En cumplimiento de esta obligación del adjudicatario se debe redactar y entregar la documentación necesaria a la Mutua.
De igual modo, se deberán identificar a las personas encargadas de supervisar y vigilar el funcionamiento de los sistemas de IA.

4.4 Implementación de procedimientos, políticas y documentación relacionadas con la IA.

El adjudicatario deberá definir, redactar y, en su caso, revisar los procesos, políticas y documentos necesarios para el uso responsable de los sistemas de IA que hasta la fecha no hayan sido definidos por FREMAP y resulten necesarios para el cumplimiento de los principios y obligaciones previstos en la norma.

Asimismo, deberán establecerse y redactarse los procesos y documentación necesaria para garantizar que el uso de servicios, productos o materiales proporcionados por proveedores se alinee con las políticas de uso responsable de los sistemas de IA y la normativa vigente.

4.5 Soporte ante requerimientos efectuados por una autoridad competente en la materia y comunicación de incidentes.

La empresa adjudicataria deberá diseñar un procedimiento de gestión y notificación de incidentes graves de IA y proporcionará soporte integral ante cualquier requerimiento efectuado por una autoridad competente en materia de IA, así como ante cualquier incidente que haya que comunicar a los proveedores y/o a la autoridad competente.

Este soporte incluye la elaboración de informes detallados que respondan a las solicitudes de información de las autoridades competentes, asistencia en la recopilación y análisis de datos, así como la defensa en procedimientos administrativos y judiciales relacionados con el cumplimiento de la normativa de IA.

4.6 Revisión, verificación y validación del sistema de gestión de las herramientas de IA.

Deberá establecerse un sistema de verificación, auditoria y validación para los sistemas de IA y los procedimientos de gestión establecidos que garantice la actualización continua del sistema de gestión de la IA y posibilite, en un futuro, la consecución de los correspondientes certificados de calidad del sistema.

El adjudicatario deberá realizar una auditoria completa antes de la finalización del contrato.

4.7 Otros servicios.

El adjudicatario llevará a cabo la ejecución del plan de acción para la adaptación de la entidad al Reglamento en materia de IA que se detalla en el Anexo I que se localiza en la carpeta comprimida "Anexos", así como cualquier servicio adicional de asesoramiento, redacción de documentación necesaria o revisión de aquella que ya tenga la entidad y que venga exigido por la aplicación de la normativa vigente en materia de IA.

4.8 Lugar de realización de los trabajos.

Los trabajos de asesoramiento, apoyo y formación en materia de IA, así como la recopilación de información, reuniones y entrevistas con el personal de FREMAP, se llevarán a cabo, preferiblemente, en las instalaciones de FREMAP, sin perjuicio de que se pueda pactar su realización de forma telemática o en las dependencias del adjudicatario.

4.9 Duración.

La duración del contrato para la prestación de los servicios de consultaría en materia de adecuación y cumplimiento de la normativa de IA será de 12 meses.

Durante este periodo, la empresa adjudicataria deberá cumplir con todas las obligaciones y servicios especificados en los pliegos que prevalecerán sobre el contrato.

5. PREVENCIÓN EN MATERIA 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 (*)
- Declaración PRL-trabajadores (*)
- CAE Ficha Coordinación (*): Informe, firmado por técnico competente, que contenga exclusivamente los riesgos específicos que su actividad pueda generar en nuestras instalaciones, tanto a sus trabajadores como a los de FREMAP, así como las medidas preventivas y de protección que establecerán para su control. El contenido debe ser el incluido en el documento Ficha CAE, pudiéndose utilizar este u otro similar.
- Recibí de las Normas de prevención para empresas externas que realizan trabajos en instalaciones de FREMAP. (*)

(*) 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

Antes del comienzo de la actividad, la empresa adjudicataria debe haber impartido la formación/información específica del puesto de trabajo en prevención de riesgos laborales a todos sus trabajadores según los artículos 18 y 19 de la Ley 31/1995, así como cualquier formación específica que requieran en función de las tareas que vayan a realizar. Así mismo debe asegurarse que todos son aptos para la realización de su trabajo según los protocolos médicos indicados por su servicio de Vigilancia de la Salud, debiendo indicar a FREMAP si alguno de ellos presenta alguna limitación y si en su caso necesita una adaptación de puesto.

Antes del comienzo de la actividad, la empresa adjudicataria facilitará a sus trabajadores la totalidad de EPIs derivada de su evaluación de riesgos, estando los mismos obligados a su uso correcto en todas aquellas operaciones donde exista riesgos de accidentes que puedan prevenir con su utilización. El encargado será el responsable de vigilar por la utilización de los mismos de manera correcta.

La empresa adjudicataria debe trasmitir a todos los trabajadores que realicen trabajos en nuestras instalaciones el contenido del documento Normas de prevención para empresas externas que realizan trabajos en instalaciones de FREMAP, documento que será de obligado cumplimiento durante toda la vigencia del contrato, así como cualquier actualización que pueda producirse de la misma.

Cualquier equipo de trabajo que la empresa adjudicataria necesite utilizar en las instalaciones de FREMAP dispondrá de la declaración de conformidad y marcado CE o se ajustará a los requisitos del Anexo 1 del RD 1215/1997, de 18 de julio, sobre condiciones mínimas de seguridad y salud para la utilización por los trabajadores de los equipos de trabajo, siendo obligación de la adjudicataria revisarlos periódicamente de manera que durante la vigencia del contrato los mismos cumplan con la legislación vigente.

Cualquier producto químico que se utilice en las instalaciones de FREMAP deben cumplir la correspondiente normativa y se proporcionará copia de las FDS para su revisión por parte del Servicio de Prevención y Promoción de la Salud de FREMAP cuando se solicite.

La empresa adjudicataria determinará los medios de coordinación que sean necesarios en función de las características del trabajo a realizar, ya sean designando recursos preventivos o personas encargadas de la coordinación de actividades empresariales.

La empresa adjudicataria está obligada a comunicar a FREMAP cualquier accidente o incidente sufrido por alguno de sus trabajadores en las instalaciones de FREMAP, así como de los posibles daños a la propiedad causados. Esta comunicación deberá efectuarse en un plazo máximo de 48 horas, excepto en los casos de especial gravedad que se hará de inmediato. Si FREMAP lo considera oportuno efectuará un informe complementario.

Si la empresa adjudicataria subcontrata alguna de las actividades contenidas en este contrato le será de aplicación todo lo dicho anteriormente y deberá incluir la correspondiente información, tanto de la empresa subcontratada como de sus trabajadores en los cuatro documentos entregados para la firma de contrato.

FREMAP podrá requerir en cualquier momento la documentación que estime oportuna para comprobación de contenido de la documentación entregada para la firma del contrato, así como cualquier documentación adicional que el Servicio De Prevención Y Promoción de la Salud de FREMAP considere necesaria para la seguridad tanto de los trabajadores de la contrata como de los trabajadores de FREMAP.

La empresa adjudicataria está obligada a comunicar cualquier cambio que se produzca en las condiciones de trabajo con tiempo suficiente y siempre antes de la realización de los mismos.

6. ANEXOS

Anexo I: Seguridad de la Información

CATEGORÍA	TIPOLOGÍA	DESCRIPCIÓN
SERVICIOS DE AUDITORÍA	Distintas tipologías de auditorías	Contratación de auditorías externas para la comprobación de

CLASIFICACIÓN DE CLAUSULADO DE SEGURIDAD DE LA INFORMACIÓN	
CRITICIDAD	MEDIO
TIPO DE SERVICIO	Servicios Totalmente Externos
NIVEL DE CONFIDENCIALIDAD	Confidencial

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.

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 CNN-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.
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.

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 hora 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 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 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.
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.

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.

Otros equipos conectados a la red

En los casos en los que el adjudicatario disponga de otros dispositivos (de multifunción, multimedia, dispositivos relacionados con el Internet de las Cosas (IoT), sistemas cloud, etc.) 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.
Solamente podrán utilizarse los dispositivos que estén establecidos en la guía de componentes certificados del CCN.

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.
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.

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 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, 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 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.

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 plugin 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.