Expediente Nº. LICT/99/138/2023/0274

Pliego de Prescripciones Técnicas para la Contratación del servicio de auditoría interna del Sistema de Gestión de Seguridad de la Información de FREMAP, Mutua Colaboradora con la Seguridad Social Nº61.

ÍNDICE

1. INTRODUCCIÓN

1.1 Objeto

El objeto del presente documento es establecer los requisitos técnicos que regirán la contratación del servicio de auditorías internas del Sistema de Gestión de Seguridad de la Información (SGSI) para FREMAP.

Los servicios profesionales objeto de contratación incluyen las actividades de auditoría interna para asegurar que los procedimientos y procesos de la seguridad de la información de FREMAP cumplen con la norma UNE-EN ISO/IEC 27001:2023 y el Esquema Nacional de Seguridad en su nivel alto.

Estos servicios, imprescindibles para el mantenimiento de las certificaciones vigentes, serán coordinados con los responsables de FREMAP a efectos de lograr su correcta ejecución, debiendo tener en cuenta la disponibilidad de centros y personal para no perjudicar la actividad ordinaria de la entidad.

1.2 Contexto

FREMAP dispone de un marco normativo recogido en sus estatutos y en la Ley General de la Seguridad Social en lo que se refiere al Reglamento de Colaboración de las Mutuas de Accidentes de Trabajo y Enfermedades Profesionales de la Seguridad Social.

De acuerdo a lo previsto en el artículo 80.2 del Texto Refundido de la Ley General de la Seguridad Social, FREMAP tiene por objeto el desarrollo de las siguientes actividades de la Seguridad Social:

- Gestión de las prestaciones económicas y de la asistencia sanitaria, incluida la rehabilitación, comprendidas en la protección de las contingencias de accidentes de trabajo y enfermedades profesionales de la Seguridad Social, así como de las actividades de prevención de las mismas contingencias que dispensa la acción protectora.
- Gestión de la prestación económica por incapacidad temporal derivada de contingencias comunes.
- Gestión de las prestaciones por riesgo durante el embarazo y riesgo durante la lactancia natural.
- Gestión de las prestaciones económicas por cese en la actividad de los trabajadores por cuenta propia, en los términos establecidos en el Título V de esta misma Ley.
- Gestión de la prestación por cuidado de menores afectados por cáncer u otra enfermedad grave.
- Actividades de la Seguridad Social que le sean atribuidas legalmente.

FREMAP tiene el firme propósito de contribuir a la eficiencia y sostenibilidad del sistema de la Seguridad Social gestionando de una forma diferencial las distintas prestaciones a través del mutualismo empresarial:

- Gestionamos prestaciones sanitarias, económicas y actividades de prevención de riesgos laborales, contribuyendo a mejorar la salud de las personas trabajadoras y su reinserción laboral, favoreciendo así la productividad de nuestras empresas mutualistas y la sostenibilidad del Sistema.
- Pretendemos ser una institución de referencia por la excelencia en el servicio y en la gestión, desde nuestros valores, la mejora continua, el talento de nuestros profesionales y el compromiso con la sociedad.
- Nuestros principios están centrados en desarrollar una actividad óptima y prestar un servicio excelente.
- La calidad es uno de los factores a los que FREMAP presta más atención, desde su creación, como se muestra mediante la permanente adopción de medidas dirigidas a mejorar su servicio y la calidad en la gestión.

Además, FREMAP tiene el compromiso inequívoco, de acuerdo con su misión y sus valores, de mantener y mejorar los servicios en alcance para lograr los siguientes objetivos recogidos en el Plan Estratégico vigente:

- Progresar en el compromiso con nuestros principales grupos de interés, con el objetivo de consolidar nuestra referencia y liderazgo por la prestación de un servicio excelente y contar con los medios e infraestructuras adecuados para mejorar la calidad de los servicios.
- Realizar una mejora continua de resultados a través de la eficiencia en la gestión y desarrollar la cartera tecnológica para mejorar la agilidad de procesos, proyectos y organización.
- Avanzar para reafirmar el compromiso de los empleados, núcleo de una prestación de servicio y gestión excelentes, con el Propósito, Misión, Visión y objetivos de FREMAP, así como mejorar la eficacia de los procesos de desarrollo y gestión del talento, aplicando políticas que garanticen la equidad e igualdad de oportunidades.

La Política de Seguridad de la Información de FREMAP está orientada a garantizar la protección de todos los activos de información y la tecnología utilizada para su tratamiento, de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar su integridad, disponibilidad y confidencialidad, favoreciendo el eficiente cumplimiento de los objetivos estratégicos de la entidad.

Para apoyar la política, FREMAP dispone de un Sistema de Gestión de Seguridad de la Información (SGSI) impulsado por la Dirección, que aporta un enfoque sistemático para la gestión de riesgos. Como referencia para establecer, implantar, mantener y mejorar dicho SGSI, se sigue el estándar internacional para la gestión de la seguridad de la información UNE-EN ISO/IEC 27001:2023, y el Esquema Nacional de Seguridad (ENS), desarrollado en el Real Decreto 311/2022, de 3 de mayo, cuya declaración de conformidad en nivel alto se estima que se obtendrá antes de finalizar 2024.

La Política de Seguridad de la Información es aplicable a todo el ámbito de la Mutua, a sus recursos y a la totalidad de los procesos internos, así como a todos los empleados de FREMAP y a colaboradores externos vinculados a la entidad a través de los contratos de prestación de servicios o convenios con terceros.

El Área de Seguridad de la Información de FREMAP tiene por objeto velar por el cumplimiento y evolución del Sistema de Gestión de Seguridad de la Información (SGSI), así como la consecución de la disponibilidad, integridad, confidencialidad y continuidad de la información.

Esta contratación se encuentra completamente alineada con los principios referidos y es vehículo para la consecución de los objetivos de FREMAP en materia de cumplimiento normativo de Seguridad de la Información en lo que se refiere al cumplimiento de la norma UNE-EN ISO/IEC 27001:2023 y el Esquema Nacional de Seguridad (ENS) en su nivel alto, persiguiendo la excelencia en todas las líneas de acción.

1.3 Alcance

FREMAP necesita un servicio integral de auditorías internas que permita asegurar el cumplimiento normativo y la mejora continua en materia de Seguridad de la Información. El alcance de la contratación incluye las siguientes actividades:

- Auditorías internas anuales de cumplimiento del Sistema de Gestión de Seguridad de la Información según la norma UNE-EN ISO/IEC 27001:2023 y los controles UNE-EN ISO/IEC 27002:2023 o versiones vigentes.
- Auditorías internas cada 2 años de cumplimiento del Esquema Nacional de Seguridad (ENS) en su nivel alto.
- Asesoramiento experto bajo demanda para orientar los planes de acción necesarios para resolver las incidencias y/o hallazgos que se detecten.

Además, la prestación incluirá, sin coste adicional, los siguientes aspectos:

- Todas las actuaciones, medios personales y medios materiales recogidos en este pliego.
- Planificación anual durante toda la vida del contrato.
- Reuniones iniciales previas a cada auditoría.
- Revisión de la documentación recibida y preparación de las visitas.
- Visitas presenciales y/o telemáticas.
- Actas de las visitas.
- Horas de realización de las auditorías estimadas.
- Informes de auditoría en fase de borrador.
- Informes de auditoría previos a los definitivos.
- Informes de auditoría definitivos.
- Todos los gastos inherentes a la prestación del servicio tales como desplazamientos, alojamiento, aparcamiento, manutención, papelería, etc.
- Asesoramiento experto que, bajo demanda, permita a FREMAP orientar los planes de acción necesarios para resolver las incidencias y/o hallazgos que se detecten.

Si bien uno de los objetivos de FREMAP es la renovación de las certificaciones vigentes, el proceso de certificación no está en alcance de esta contratación.

1.4 Normativa de carácter técnico

Será de aplicación toda la normativa legal establecida en la legislación española, así como de la Unión Europea que pudiese resultar de aplicación al objeto de esta contratación, destacando las siguientes:

- Normativas y disposiciones aplicables en materia de protección de datos, en concreto el Reglamento UE 2016/679, Reglamento General de Protección de Datos (RGPD), así como la Ley Orgánica de Protección de Datos de carácter personal nacional y demás legislación aplicable.
- Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.
- Norma UNE-EN ISO/IEC 27001:2023 o versión vigente. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información.
- Norma UNE-EN ISO/IEC 27002:2023 o versión vigente. Tecnología de la Información. Técnicas de seguridad. Código de prácticas para los controles de seguridad de la información.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Cualquier otra disposición en el ámbito del objeto de la licitación.

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

2. DESCRIPCIÓN DE SITUACIÓN ACTUAL

2.1 Sistema de Gestión de Seguridad de la Información

FREMAP dispone de un Sistema de Gestión de Seguridad de la Información (SGSI) impulsado por la Dirección, que aporta un enfoque sistemático para la gestión de los riesgos y la Política de Seguridad de la Información. Además, FREMAP dispone de un cuerpo normativo que incluye la organización documental de Sistema de Gestión de seguridad de la Información (SGSI), su taxonomía, la estructura de los documentos y su contenido.

Como referencia normativa para establecer, implantar, mantener y mejorar dicho SGSI, FREMAP dispone de las siguientes certificaciones:

- Certificación UNE-EN ISO/IEC 27001:2023 desde 2018, renovado en el año 2024.
- Certificación Esquema Nacional de Seguridad (ENS) en nivel ALTO (estimado antes de finalizar 2024).

2.2 Política de Seguridad de la Información

La Política de Seguridad de la Información de FREMAP está orientada a garantizar la protección de todos los activos de información y la tecnología utilizada para su tratamiento, de las amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar su integridad, disponibilidad y confidencialidad, favoreciendo el eficiente cumplimiento de los objetivos estratégicos de la entidad.

La Política de Seguridad de la Información es aplicable a todo el ámbito de la Mutua, a sus recursos y a la totalidad de los procesos internos, así como a todos los empleados de FREMAP y a colaboradores externos vinculados a través de los contratos de prestación de servicios o convenios con terceros.

2.3 Área de Seguridad de la Información

El Área de Seguridad de la Información de FREMAP tiene por objeto velar por el cumplimiento y la evolución del Sistema de Gestión de Seguridad de la Información (SGSI), así como la consecución de la disponibilidad, integridad, confidencialidad y continuidad de la información.

3. DESCRIPCIÓN DE LA PRESTACIÓN DE SERVICIOS

FREMAP necesita auditorías internas para conocer con profundidad el estado de cumplimiento de su Sistema de Gestión de Seguridad de la Información (SGSI) en relación con la norma UNE-EN ISO/IEC 27001:2023, el control ISO/IEC 27002 y el Esquema Nacional de Seguridad en su nivel alto, con el fin último de actuar y remediar cualquier hallazgo.

[REQ-1]: El adjudicatario prestará servicios de auditoría interna en relación al cumplimiento de las normas referidas adecuando su actividad a la planificación que se acuerde previamente y sin perjudicar la actividad ordinaria de FREMAP.

3.1 Volumetría estimada de auditorías

[REQ-2]: A efectos de la elaboración de la oferta técnica y económica, el licitador deberá tener en cuenta la siguiente planificación estimativa:

Año 1 Año 2025	Año 2 Año 2026	Año 3 Año 2027	Año 4 Año 2028	Año 5 Año 2029
Auditoría de UNE-EN ISO/IEC 27001:2023	Auditoría conjunta: Auditoría de UNE-EN ISO/IEC 27001:2023 y Esquema Nacional de Seguridad (ENS) en nivel alto	Auditoría de UNE-EN ISO/IEC 27001:2023	Auditoría conjunta: Auditoría de UNE-EN ISO/IEC 27001:2023 y Esquema Nacional de Seguridad (ENS) en nivel alto	Auditoría de UNE-EN ISO/IEC 27001:2023

Estimado: 48 horas	Estimado: 88 horas	Estimado: 48 horas	Estimado: 88 horas	Estimado: 48 horas

3.1 Volumetría estimada de auditorías

[REQ-3]: A efectos de la elaboración de la oferta técnica y económica, el licitador deberá estimar una actividad media de 48 horas para cada auditoría UNE-EN ISO/IEC 27001:2023 y 88 horas para cada auditoría conjunta (UNE-EN ISO/IEC 27001:2023 y ENS). En caso de que alguna auditoría requiera más horas de las estimadas, el adjudicatario informará detalladamente a FREMAP de la necesidad para permitir su valoración, aceptación, facturación y pago.

[REQ-4]: En caso de que no se prestara alguno de los servicios con la calidad esperada, FREMAP podrá resolver total o parcialmente dicho servicio, pudiendo resolver el contrato en caso de producirse una prestación defectuosa.

IMPORTANTE: FREMAP no se compromete al consumo de las auditorías estimadas, pudiendo indicar al adjudicatario, al comienzo de cada anualidad, las auditorías que se estimen necesarias de acuerdo al plan de certificación o necesidades de negocio que apliquen en cada momento de la vida del contrato.

3.2 Auditorías internas

3.2.1 Auditoría de UNE-EN ISO/IEC 27001:2023

[REQ-5]: El adjudicatario realizará de forma estimada y durante toda la vida del contrato, una auditoría anual de cumplimiento del Sistema de Gestión de Seguridad de la Información según la norma UNE-EN ISO/IEC 27001:2023 o versión vigente, identificando y detallando los hallazgos para permitir las acciones que se deriven.

[REQ-6]: El adjudicatario realizará, al comienzo de cada anualidad aplicable, una propuesta de contenidos necesarios para la ejecución exitosa de la auditoría, anticipando cualquier necesidad.

[REQ-7]: El adjudicatario incluirá un equipo auditor con las siguientes características:

- El ***Auditor/a Jefe/a***, también llamado Líder del equipo auditor, realizará la mayor parte del proceso de auditoría, supervisando además cualquier actividad realizada por su equipo y velando por la exactitud de los hallazgos y recomendaciones mencionados en los informes. El Auditor Jefe deberá reunir al menos los siguientes requisitos:
  - Acreditación de formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable y evidenciada de al menos 4 años, en auditoría de sistemas de gestión de seguridad de la información (UNE-EN ISO/IEC 27001:2023 y/o ENS).
  - Certificación "Auditor Líder ISO 27001" en versión vigente, emitida por una entidad certificadora reconocida por ENAC o equivalente, debiendo actualizarse durante toda la vida del contrato.
  - Conocimientos de seguridad y gestión de riesgos de seguridad (certificación y experiencia probada de al menos 4 años en estos elementos).
  - Conocimientos de otra legislación aplicable durante la vigencia del contrato.
- El Auditor Jefe, opcionalmente, podrá apoyarse en un equipo auditor que deberá reunir experiencia previa en seguridad y en auditoría de los sistemas de información, en consonancia con las responsabilidades asignadas.

- El Auditor Jefe deberá permanecer al servicio de FREMAP durante la vigencia del contrato. En caso de baja médica, ausencia, vacaciones, etc estos puedan ser sustituidos inmediatamente, por profesionales que cumplan los requisitos especificados en este pliego y lo establecido en las ofertas incluidas en los criterios de valoración.

[REQ-8]: Todos los integrantes del equipo auditor, especialmente los externos y los expertos técnicos, deberán firmar, antes de comenzar la auditoría, un acuerdo de confidencialidad.

[REQ-9]: Ningún integrante del equipo auditor podrá haber participado o tener responsabilidades previas (dos últimos años) en el sistema de información auditado, o bien haber sido consultor para ese sistema.

3.2.2 Auditoría de Esquema Nacional de Seguridad (ENS) - Nivel alto

[REQ-10]: El adjudicatario realizará, de forma estimada y durante toda la vida del contrato, 1 auditoría cada 2 años de cumplimiento del Esquema Nacional de Seguridad (ENS) según su norma de nivel alto, identificando y detallando los hallazgos para permitir las acciones que se deriven.

[REQ-11]: El adjudicatario realizará, al comienzo de cada anualidad aplicable, una propuesta de contenidos necesarios para la ejecución exitosa de la auditoría, anticipando cualquier necesidad.

[REQ-12]: Como parte de esta auditoría, el adjudicatario deberá tener en cuenta al menos lo dispuesto en el Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad, verificando el cumplimiento de los siguientes principios básicos:

1. Seguridad integral.
2. Gestión de riesgos.
3. Prevención, reacción y recuperación.
4. Líneas de defensa.
5. Reevaluación periódica.
6. Función diferenciada.

[REQ-13]: Como parte de esta auditoría, el adjudicatario deberá contemplar, total o parcialmente y detallándolo en su caso, los siguientes aspectos recogidos en la "Guía de Seguridad de las TIC CCN-STIC 802" en lo que respecta a la Guía de Auditoría del Esquema Nacional de Seguridad:

1. La Gestión del Riesgo.
2. El marco organizativo y la segregación de funciones.
3. El marco operacional (Planificación, Control de Accesos, Explotación, Servicios Externos, Continuidad del Servicio, y Monitorización del Sistema).
4. Las medidas de protección (Protección de las instalaciones e infraestructuras, Gestión del personal, Protección de equipos, de las comunicaciones, de los soportes de información, de las aplicaciones informáticas, de la información, y de los servicios).
5. La Declaración de Aplicabilidad que recoge las medidas de seguridad del Anexo II que son relevantes para el sistema de información sujeto a la auditoría.
6. Los procesos de mejora continua de la seguridad.
7. La aplicación de los modelos de cláusula administrativa particular a incluir en las prescripciones administrativas de los contratos correspondientes (según una muestra seleccionada de estos).

[REQ-14]: Como parte de esta auditoría, el adjudicatario deberá contemplar todas las medidas de seguridad de la "Guía de Seguridad de las TIC CCN-STIC 808" correspondientes al Esquema Nacional de Seguridad en su nivel alto:

- Marco organizativo
    - Política de seguridad.

  - Normativa de seguridad.
  - Procedimientos de seguridad.
  - Proceso de autorización.
- Marco operacional
  - Planificación.
  - Control de acceso.
  - Explotación.
  - Recursos externos.
  - Servicios en la nube.
  - Continuidad del servicio.
  - Monitorización del sistema.
- Medidas de protección
  - Protección de las instalaciones e infraestructuras.
  - Gestión del personal.
  - Protección de los equipos.
  - Protección de las comunicaciones.
  - Protección de los soportes de información.
  - Protección de las aplicaciones informáticas.
  - Protección de la información.
  - Protección de los servicios.

[REQ-15]: El licitador deberá tener en cuenta, a efectos de la elaboración técnica y económica de su oferta, que cada auditoría conjunta (UNE-EN ISO/IEC 27001:2023 y ENS) se estima en 88 horas de trabajo.

[REQ-16]: El adjudicatario incluirá un equipo auditor con las características que se recogen en la "Guía de Seguridad de las TIC CCN-STIC 802":

- El ***Auditor/a Jefe/a***, también llamado Líder del equipo auditor, realizará la mayor parte del proceso de auditoría, supervisando además cualquier actividad realizada por su equipo y velando por la exactitud de los hallazgos y recomendaciones mencionados en los informes. El Auditor Jefe deberá reunir al menos los siguientes requisitos:
  - Acreditación de formación y experiencia en auditoría de sistemas de información, a través de certificaciones reconocidas a nivel nacional e internacional, o bien a través de experiencia verificable y evidenciada de al menos 4 años, en auditoría de sistemas de gestión de seguridad de la información (UNE-EN ISO/IEC 27001:2023 y/o ENS).
  - Conocimientos de seguridad y gestión de riesgos de seguridad (certificación y experiencia probada de al menos 4 años en estos elementos).
  - Conocimientos sólidos de lo dispuesto en el Real Decreto 311/2022 por el que se regula el Esquema Nacional de Seguridad.
  - Conocimientos de otra legislación aplicable durante la vigencia del contrato.

- El Auditor Jefe, opcionalmente, podrá apoyarse en un equipo auditor que deberá reunir experiencia previa en seguridad y en auditoría de los sistemas de información, en consonancia con las responsabilidades asignadas.

- El Auditor Jefe deberá permanecer al servicio de FREMAP durante la vigencia del contrato. En caso de baja médica, ausencia, vacaciones, etc estos puedan ser sustituidos inmediatamente, por profesionales que cumplan los requisitos especificados en este pliego y lo establecido en las ofertas incluidas en los criterios de valoración.

[REQ-17]: Todos los integrantes del equipo auditor, especialmente los externos y los expertos técnicos, deberán firmar, antes de comenzar la auditoría, un acuerdo de confidencialidad.

[REQ-18]: Ningún integrante del equipo auditor podrá haber participado o tener responsabilidades previas (dos últimos años) en el sistema de información auditado, o bien haber sido consultor para ese sistema.

3.3 Ciclo de vida

3.3.1 Gestión

[REQ-19]: El adjudicatario gestionará de forma única e integral todos los servicios prestados, incluyendo en su propuesta un/a **Gestor/a del contrato** que, teniendo una dedicación parcial, llevará a cabo las siguientes funciones:

- Ejercer la interlocución con FREMAP a nivel de gestión contractual.
- Asegurar un adecuado control, seguimiento y cumplimiento de los servicios prestados.
- Gestionar toda la actividad laboral y supervisar el desempeño de los profesionales adscritos.
- Atender y dar respuesta a consultas y/o peticiones en relación al objeto de contratación.
- Realizar reuniones periódicas de seguimiento del contrato, inicialmente de forma anual.

[REQ-20]: El adjudicatario proporcionará toda la documentación requerida en fase de adscripción de medios, actualizada de acuerdo a los profesionales que finalmente sean presentados para la prestación del servicio. El adjudicatario confirmará a FREMAP los profesionales que se dispondrán en el equipo auditor para el primer año, cuya cualificación y experiencia deberá corresponderse al menos con el equipo presentado y valorado en fase de oferta.

3.3.1 Ciclo de vida de la gestión de auditorías internas

3.3.2 Planificación

[REQ-21]: A efectos de acordar la planificación y al comienzo de cada anualidad del contrato, FREMAP podrá requerir una reunión telemática o presencial en la Sede Social de FREMAP sita en Carretera de Pozuelo, 61 de Majadahonda.

[REQ-22]: FREMAP solicitará las auditorías en los periodos más adecuados para negocio, en términos de menor impacto y mejor eficiencia respecto al proceso de certificación posterior. El adjudicatario podrá consensuar con FREMAP las fechas de cada auditoría de acuerdo a estos requisitos.

[REQ-23]: El adjudicatario acordará con FREMAP el plan de auditorías anual, que incluirá al menos los siguientes datos:

- Objetivo de cada auditoría.
- Desglose de actividades.

- Calendario detallado.
- Visitas presenciales y/o telemáticas.
- Equipo auditor del adjudicatario, incluyendo los CVs y acreditaciones de los mismos.
- Personal necesario por parte de FREMAP.

[REQ-24]: La planificación del adjudicatario deberá incluir al menos las siguientes visitas en cada proceso de auditoría:

- De forma general, todos los procesos de auditoría requieren visitas presenciales en la Sede Social de FREMAP y en el Hospital de Majadahonda, situados en el mismo campus de Carretera de Pozuelo 61 de Majadahonda (Madrid).
- De forma adicional y a efectos de muestreo de cumplimiento normativo, podrá ser necesaria 1 visita telemática por cada auditoría en alguno de los centros de la Organización Territorial:
  - Hospital FREMAP de Sevilla, Av. de Jerez, s/n, 41012 Sevilla.
  - Hospital FREMAP de Barcelona, Carrer dels Madrazo, 8-10, 08006 Barcelona.
  - Hospital FREMAP de Vigo, Rúa de Feliciano Rolán, 12, 36203 Vigo, Pontevedra.
  - Sede de FREMAP de C/Joan Maragall en Madrid.
  - Otros centros de la Organización Territorial de FREMAP (todo el territorio nacional).

3.3.3 Ejecución

[REQ-25]: Antes de cada proceso de auditoría se detallará toda la actuación y se formalizará en una reunión inicial, consensuando el calendario de acuerdo a causar el menor impacto en la actividad de negocio de FREMAP.

[REQ-26]: En la reunión inicial, el equipo auditor del adjudicatario concretará las jornadas, horas, ubicaciones y personas necesarias para todo el proceso de auditoría, debiendo haber aprobación por parte de la persona asignada por FREMAP.

[REQ-27]: De forma general, esta reunión inicial tendrá lugar de forma presencial en la Sede Social de FREMAP, dentro del campus de Carretera de Pozuelo 61 de Majadahonda.

[REQ-28]: El equipo auditor del adjudicatario realizará las visitas presenciales y/o telemáticas que se hayan acordado, completando el programa planificado de acuerdo al cumplimiento normativo objetivo.

[REQ-29]: Una vez finalizada cada visita, ya sea presencial o telemática, se elaborará un **Acta de visita** que se incorporará al Informe de auditoría y que incluirá al menos la siguiente información:

- Objetivo.
- Ubicación.
- Modalidad (presencial/telemática).
- Fecha.
- Duración.
- Cuadro de horas dedicadas.
- Equipo auditor a cargo.
- Personal de FREMAP entrevistado.
- Hallazgos de auditoría.
- Campo de observaciones (para el personal de FREMAP).
- Check-list de cumplimiento que se ha documentado durante la visita.
- Firma del auditor/es y el responsable asignado por FREMAP.
- Conclusiones preliminares de la visita.

3.3.4 Entrega

[REQ-30]: Tras cada auditoría, el adjudicatario entregará a FREMAP un **Informe de auditoría** que incluirá información de alto y bajo nivel y clasificará y detallará los hallazgos encontrados. Dicho informe tendrá el formato establecido por la normativa de aplicación y será consistente con las actas de visita realizadas previamente. Este informe se elaborará de acuerdo al siguiente versionado:

- **Informe de auditoría (VB - Versión borrador).** Este informe deberá ser entregado a FREMAP el último día de la auditoría, formalizando la entrega en una reunión de cierre que incluirá al menos:
    - Puntuaciones
    - Puntos fuertes
    - Oportunidades de mejora
    - No conformidades
    - Observaciones
    - Comentarios

  Tras dar la conformidad al informe de auditoría en su versión borrador, se abrirá un proceso de alegaciones por parte de FREMAP en un plazo máximo de 5 días hábiles.

- **Informe de auditoría (VD - Versión definitiva).** Tras las alegaciones, el adjudicatario entregará a FREMAP el informe definitivo que será firmado por el auditor y el responsable que designe FREMAP en un plazo máximo de 5 días hábiles. Este informe se firmará digitalmente, mediante firma electrónica y en formato PDF.

[REQ-31]: El gestor del contrato del adjudicatario realizará una consulta de calidad del servicio que se evaluará sobre 10 puntos e incluirá al menos las siguientes informaciones:

- Trato, comportamiento y puntualidad del auditor.
- Cualificación y capacidades del auditor.
- Exactitud y utilidad del informe de auditoría.
- Comunicación y explicación del informe de auditoría.
- Cumplimiento de plazos y planificación prevista.
- Observaciones de responsables de FREMAP.

[REQ-32]: El adjudicatario procederá a emitir la factura de la auditoría realizada una vez que FREMAP acepte la entrega y la calidad del servicio ofrecido.

3.4 Acuerdo de nivel de servicio

[REQ-33]: El gestor del contrato y los profesionales del equipo auditor velarán por el cumplimiento de los plazos descritos en este pliego, asegurando la entrega de los informes de auditoría definitivos con la calidad esperada.

[REQ-34]: Los plazos descritos serán de obligado cumplimiento salvo en aquellos casos y circunstancias en los que una fuerza mayor o una dependencia con un tercero, escalada adecuadamente a FREMAP, hagan imposible su cumplimiento.

4. SEGURIDAD DE LA INFORMACIÓN

[REQ-35]: La empresa adjudicataria estará obligada a cumplir con todos los requisitos de Seguridad de la Información y continuidad derivados de la Política de Seguridad de FREMAP que se encuentre vigente a lo largo de toda la vida del contrato.

[REQ-36]: El licitador debe tener en cuenta que la Política de Seguridad de FREMAP está modelada actualmente en base al estándar UNE-EN ISO/IEC 27001:2023 y el Esquema Nacional de Seguridad (ENS) y que cualquier actividad en el ámbito de la entidad debe estar sujeta a dichos estándares.

[REQ-37]: Adicionalmente, FREMAP dispone de un cuerpo normativo en materia de seguridad de la información que incluye las normas que debe conocer y seguir todo usuario, incluyendo al personal externo. La empresa adjudicataria estará obligada a cumplir con todas las normas vigentes, entre las cuales destacan las siguientes:

- Norma de clasificación de la información.
- Norma del usuario en el uso seguro de herramientas.
- Norma de puestos de trabajo, dispositivos portátiles y teletrabajo.

[REQ-38]: El adjudicatario y el personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, evitará realizar cualquier tipo de acción que comprometa los procesos de negocio, sistemas de información e infraestructuras de TI de FREMAP. En cualquier caso, el adjudicatario comunicará de forma inmediata cualquier incidencia en materia de seguridad que pueda tener impacto en los activos de FREMAP, sin perjuicio de su resolución.

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

4.1 Confidencialidad de datos y propiedad intelectual

[REQ-39]: Todos los profesionales adscritos al contrato, incluyendo los que se incorporen al comienzo y todos los que se puedan incorporar durante toda la vida del mismo, deberán adquirir un inequívoco compromiso de confidencialidad mediante la firma del anexo que, en cumplimiento de la normativa de aplicación vigente, garantiza la confidencialidad de los datos y describe las medidas técnicas y organizativas que deben seguirse durante toda la prestación a este respecto.

[REQ-40]: La propiedad intelectual de todos los productos y/o entregables generados a partir del desarrollo de los servicios profesionales prestados durante la vida del contrato, corresponde a FREMAP.

[REQ-41]: La empresa adjudicataria deberá asegurar que toda la información, productos y/o entregables se entregan a FREMAP a la finalización del contrato, no pudiendo almacenarse ni utilizarse para fines diferentes al objeto del mismo, salvo autorización expresa.

4.2 Tratamiento de incidentes de seguridad

[REQ-42]: En relación a la integridad de la información, cualquier violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos transmitidos, conservados o tratados de otra forma, deberá ser comunicada a FREMAP de forma inmediata para que pueda ser notificada a la autoridad de control sin dilación.

[REQ-43]: En relación a la confidencialidad de la información, cualquier violación de la seguridad, sustracción o la comunicación o acceso no autorizados a dichos datos, deberá ser comunicada a FREMAP de forma inmediata para que pueda ser notificada a la autoridad de control sin dilación.

[REQ-44]: En relación a la disponibilidad de la información, cualquier incidente que impacte y/o afecte al servicio de forma grave, deberá ser comunicado a FREMAP de forma inmediata.

4.3 Acceso remoto

[REQ-45]: Para todos aquellos accesos remotos a recursos desplegados en FREMAP, se establecen las siguientes limitaciones y responsabilidades específicas que tanto el adjudicatario como quien actúe en su nombre, si fuera el caso, deberá cumplir:

- Condiciones técnicas:
  - Los accesos remotos se producirán desde equipos con plataforma corporativa FREMAP, haciendo uso de los sistemas de conexión segura VPN que se indiquen en cada momento de la vida del contrato, salvo autorización expresa.
- Recursos de FREMAP accesibles:
  - Solamente se proporcionará acceso remoto a los elementos e información estrictamente necesarios para el cumplimiento del objeto contractual.
  - La conexión se realizará única y exclusivamente por protocolos previamente consensuados con FREMAP.
- Potestad de control:
  - El personal autorizado de FREMAP, teniendo como finalidad la protección, optimización y mejora de los servicios, monitorizará el tráfico cursado en este tipo de conexiones para la detección de actuaciones anómalas.
- Deberes y obligaciones para la empresa adjudicataria:
  - Solamente deberá tener acceso a los recursos desplegados en FREMAP el personal adscrito y estrictamente necesario de la empresa adjudicataria y únicamente para los fines previamente autorizados por FREMAP.
  - Los usuarios del acceso remoto deberán hacer un uso adecuado de la conexión, utilizándola eficientemente con el fin de evitar en la medida de lo posible la congestión de la misma, la interrupción de los servicios de red o del equipamiento de la infraestructura conectada.
  - Se deberá acceder desde redes privadas protegidas que garanticen unas condiciones de seguridad adecuadas.
  - En el caso de sedes remotas de trabajo, todos los equipos de red del adjudicatario dispondrán de medidas para reducir los riesgos derivados del acceso no autorizado y para protegerlos contra pérdidas o daños y falta de disponibilidad. Se protegerá el acceso a la consola de todos los equipos y se realizarán backups de sus ficheros de manera que se puedan recuperar tras un desastre o ante un fallo de los soportes que albergan dichos ficheros.
  - Se deberá hacer un uso adecuado de las conexiones y cumplir la normativa y política vigente en FREMAP.

4.4 Ligada al personal

[REQ-46]: El personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, firmará un acuerdo de confidencialidad antes de su interacción con recursos e infraestructuras de FREMAP y antes de su acceso a aquellas infraestructuras del adjudicatario que soporten los servicios a entregar a FREMAP dentro del alcance de la presente licitación.

[REQ-47]: El personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, será informado de las políticas y procedimientos, incluyendo requisitos de seguridad y uso correcto de los recursos, antes de interactuar con recursos e infraestructuras de FREMAP y antes del acceso a aquellas infraestructuras del adjudicatario que soporten los servicios a entregar a FREMAP dentro del alcance de la presente licitación. El citado personal recibirá actualizaciones regulares sobre estas políticas y procedimientos.

[REQ-48]: FREMAP podrá evaluar periódicamente los conocimientos del personal adscrito en materia de seguridad de la información, incluyendo contenidos específicos con relación a las políticas que se definan

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

4.5 Física y del entorno

[REQ-49]: El personal que actúe bajo la responsabilidad del adjudicatario, de manera directa o indirecta, accederá a zonas "seguras" o "sensibles" como los CPDs durante el tiempo mínimo imprescindible para la realización de los trabajos que sean necesarios siempre con autorización previa y con control del acceso por parte de FREMAP. Dicho personal portará su identificación de manera visible.

[REQ-50]: En el caso de sedes remotas de trabajo, la empresa adjudicataria deberá contar con las medidas de seguridad adecuadas para proteger los activos de información de FREMAP que se encuentren en dichas ubicaciones.

4.6 Continuidad

[REQ-51]: En el caso de sedes remotas de trabajo, la empresa adjudicataria dispondrá de sistemas y/o redes de comunicaciones con mecanismos de alta disponibilidad para garantizar el servicio prestado.

[REQ-52]: FREMAP dispone de un plan de continuidad de negocio que se prueba de manera periódica. El adjudicatario colaborará en la ejecución de las comprobaciones de los planes de contingencia y de continuidad de FREMAP, en lo referido a los servicios dentro del alcance de la presente licitación.

4.7 Conformidad

[REQ-53]: El adjudicatario se compromete, en caso de ser requerido por FREMAP, a presentar declaraciones responsables de compromiso de cumplimiento de las medidas de seguridad contenidas en las políticas y normativas de aplicación, tanto a nivel de empresa como del personal adscrito al contrato.

4.8 Auditoría

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

[REQ-54]: FREMAP quedará capacitada para la realización de auditorías de seguridad de la información, a fin de velar por las políticas establecidas y las normativas de aplicación, en su caso. El plan de auditoría será acordado entre FREMAP y el adjudicatario.

[REQ-55]: FREMAP quedará capacitada para recabar cualquier información relacionada con la seguridad de los sistemas donde resida en reposo o en movimiento información de FREMAP, teniendo el adjudicatario que suministrar esta información de forma concisa y veraz. Esto se aplica tanto al adjudicatario como a cualquier subcontratación de sistemas que por parte de este se realice.

5. PREVENCIÓN DE RIESGOS LABORALES

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

- ✓**Declaración de modalidad PRL (*)**

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