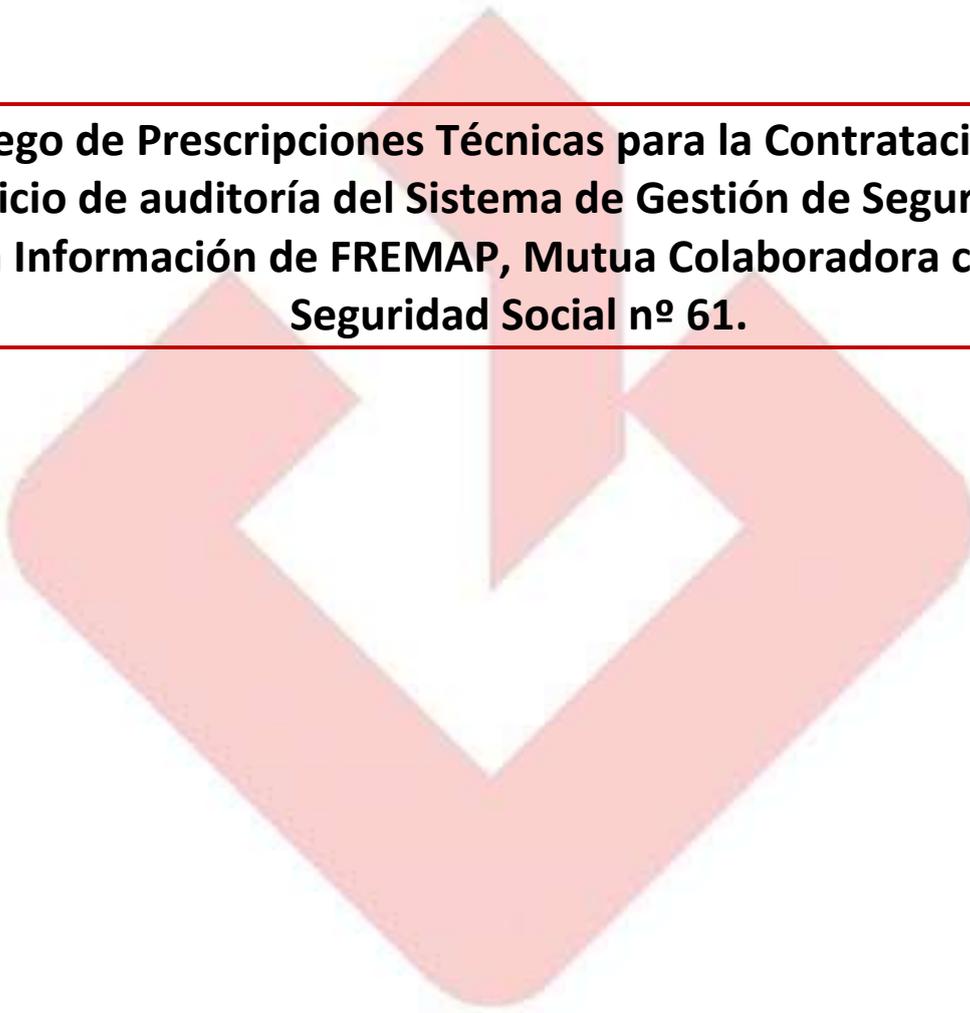


**Expediente N°. LICIT/99/138/2020/0203**

**Pliego de Prescripciones Técnicas para la Contratación del servicio de auditoría del Sistema de Gestión de Seguridad de la Información de FREMAP, Mutua Colaboradora con la Seguridad Social nº 61.**



## ÍNDICE

<b>1. OBJETO .....</b>	<b>3</b>
<b>2. NORMATIVA DE CARÁCTER TÉCNICO .....</b>	<b>3</b>
<b>3. ALCANCE DEL SERVICIO .....</b>	<b>3</b>
<b>4. ORGANIZACIÓN DEL SERVICIO .....</b>	<b>4</b>
<b>5. EJECUCIÓN DE LOS SERVICIOS .....</b>	<b>5</b>
<b>5.1 PLAN DE AUDITORÍA.....</b>	<b>5</b>
<b>5.2 HORAS ESTIMADAS PARA LA REALIZACIÓN DE LA AUDITORÍA.....</b>	<b>6</b>
<b>5.3 ACTUACIONES .....</b>	<b>6</b>
<b>5.4 SISTEMA DE VALORACIÓN .....</b>	<b>9</b>
<b>5.5 CONDICIONES DE LA PRESTACIÓN DEL SERVICIO .....</b>	<b>10</b>
<b>6. CONTROL Y SEGUIMIENTO DEL CONTRATO.....</b>	<b>10</b>
<b>6.1 Control de Calidad .....</b>	<b>10</b>



## 1. OBJETO

---

El objeto del presente Pliego de Prescripciones Técnicas es definir el alcance y condiciones técnicas que regirán la **Contratación del servicio de auditoría del Sistema de Gestión de Seguridad de la Información de FREMAP, Mutua Colaboradora con la Seguridad Social nº 61.**

Dado que FREMAP ha implantado los procedimientos de gestión de la seguridad recogidos en la UNE-ISO/IEC 27001:2014, al haber obtenido dicha Certificación, entre los mismos se encuentra la necesaria realización de una Auditoría Interna periódica.

Los servicios se prestarán en las instalaciones de FREMAP de tal forma que no se vea perjudicada la actividad ordinaria de la entidad, debiendo tener en cuenta la disponibilidad de centros y el personal de los mismos.

## 2. NORMATIVA DE CARÁCTER TÉCNICO

---

Será obligación del adjudicatario el cumplimiento del presente Pliego y del Pliego de Cláusulas Administrativas, así como la legislación vigente que afecte al objeto de la licitación, adoptando a su vez, las medidas necesarias para respetar la legalidad en el caso de promulgarse nueva normativa.

Además, será de aplicación la siguiente normativa específica:

- Norma UNE-ISO/IEC 27001:2014. Tecnología de la información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información.
- Norma UNE-EN ISO/IEC 27002:2017. 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.
- 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 esos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

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

## 3. ALCANCE DEL SERVICIO

---

Realización de las siguientes tareas:

- Auditoría del Sistema de Gestión de Seguridad de la Información según la norma UNE-ISO/IEC 27001:2014, en concreto, el equipo de seguridad de FREMAP.
- Auditoría de los Sistemas de Información de las Áreas de Gestión según la norma Norma UNE-EN ISO/IEC 27002:2017.

- Subdirección General de RRHH.
- Secretaría general, Auditoría Interna Área de Protección de datos.
- Subdirección General de Gestión.
- Subdirección General Médica: Hospitales de FREMAP.

El primer año se auditará el Hospital de Majadahonda y si se ejecutaran las prórrogas del contrato, anualmente se realizaría la auditoría de distintos Hospitales de FREMAP de entre los siguientes en el siguiente orden: Barcelona, Vigo y Sevilla.

La dirección de los Hospitales de FREMAP se indica a continuación:

HOSPITAL	DIRECCIÓN
SEVILLA	Av. de Jerez, s/n, 41012 Sevilla
MAJADAHONDA	Carr. de Pozuelo, 61, 28222 Majadahonda, Madrid
VIGO	Rúa de Feliciano Rolán, 12, 36203 Vigo, Pontevedra
BARCELONA	Carrer dels Madrazo, 8-10, 08006 Barcelona

- Subdirección General de Medios: El entorno administrativo y la Dirección de Procesos y Operaciones.

## 4. ORGANIZACIÓN DEL SERVICIO

---

### A. AUDITORÍA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El servicio se prestará sin perjudicar la actividad ordinaria de la entidad.

### B. RESPONSABLE DEL CONTRATO

La empresa adjudicataria deberá nombrar un responsable del contrato que será la persona de contacto en lo relativo a la correcta ejecución del contrato, es decir, cuestiones tales como la facturación, las incidencias del contrato, la organización del servicio, etc.

El responsable será el coordinador que la empresa adjudicataria debe poner a disposición de FREMAP.

Además de las funciones relativas a la organización y al correcto funcionamiento del servicio prestado, el responsable que se asigne deberá estar disponible para las comunicaciones que se le hagan por teléfono o correo electrónico en horario de 08:00h a 16:00h, dando respuesta con la mayor premura posible.

Cualquier cambio relativo al nombramiento del responsable del contrato deberá ser comunicado a FREMAP de forma inmediata mediante correo electrónico.

Asimismo, FREMAP designará un responsable del contrato que mantendrá con el adjudicatario los contactos oportunos y convocará las reuniones que resulten necesarias a efectos de garantizar la correcta ejecución del servicio.

### C. PROTOCOLO DE FUNCIONAMIENTO DEL SERVICIO

Para el correcto funcionamiento del servicio, será necesario además de la asignación de un responsable, una correcta organización del mismo desde el inicio del contrato.

Una vez formalizado el contrato se mantendrá una primera reunión en los términos que se disponen en el apartado 5.3 Actuaciones.

Es estrictamente necesario que se preste el servicio según lo dispuesto en el punto 5. Ejecución de los servicios. Además, deberán prestarse los servicios en las fechas exactas que se fijen para la realización de la Auditoría.

## 5. EJECUCIÓN DE LOS SERVICIOS

---

Se realizarán anualmente las tareas descritas en el apartado 5.1 Plan de Auditoría y el grado de madurez de implantación en el conjunto de FREMAP se valorará según lo dispuesto en el apartado 5.4 Sistema de valoración, debiendo cumplirse con lo dispuesto en el apartado 3. Alcance del servicio, siendo el objetivo el siguiente:

- Análisis del grado de implantación y madurez de la UNE-EN ISO/IEC 27001:2014.
- Revisión de la implantación, madurez y cumplimiento de los 114 controles de la UNE-EN ISO/IEC 27002:2017.

### 5.1 PLAN DE AUDITORÍA

---

Todos los años de duración del contrato se realizarán las siguientes tareas:

- Se revisará en la Sede Social de FREMAP el Sistema de Seguridad de la Información y un hospital, y en concreto, se realizará la revisión completa de los controles del 4 al 10 de la norma UNE-EN ISO/IEC 27001:2014, siendo estos los siguientes:

**4-Contexto de la organización**

**5-Liderazgo**

**6-Planificación**

**7-Soporte**

**8-Operación**

**9-Evaluación del desempeño**

**10-Mejora**

- Se realizará la revisión de controles UNE-EN ISO/IEC 27002:2017, en las siguientes Áreas Administrativas de Gestión:
  - **Subdirección General de RRHH.**
  - **Secretaría General, Auditoría Interna y Área de Protección de datos.**
  - **Subdirección General de Gestión.**

- **Subdirección General Médica: Debe tenerse en cuenta lo reflejado en el apartado 3. Alcance del servicio, respecto a la realización de la auditoría de los distintos Hospitales de FREMAP.**
- **Subdirección General de Medios: Entorno administrativo y Dirección de Procesos y Operaciones.**

Se revisarán y puntuarán los controles conforme al sistema de valoración establecido en el apartado 5.4 del presente pliego.

En el apartado 5.2 Horas estimadas para la realización de la Auditoría aparecen reflejadas las horas de auditoría previstas.

Deberán incorporarse a los objetivos de control de la UNE-EN ISO/IEC 27001 y de su Anexo A) UNE-EN ISO/IEC 27002, mapeo RGPD, verificando la atención y cumplimiento de los principios relativos al tratamiento, el cumplimiento con las bases de legitimación, la obligación de transparencia e información, el ejercicio de los derechos ARSOPL, realización de análisis de riesgos y evaluaciones de impacto, procedimiento de brechas de seguridad, notificaciones a la autoridad de control, designación del Delegado de Protección de Datos, registro de actividades de tratamiento, encargos de tratamiento y exigencias de responsabilidad proactiva.

## 5.2 HORAS ESTIMADAS PARA LA REALIZACIÓN DE LA AUDITORÍA

Las áreas a auditar y las horas estimadas anuales para su realización son las siguientes, teniendo en cuenta las tareas a realizar y que se identifican a continuación:

AUDITORÍA		TIEMPO ANUAL ESTIMADO
Sistema de Gestión de Seguridad de la Información		4 horas
Áreas Administrativas de Gestión	Subdirección General de RRHH (2h)	10 horas
	Secretaría General y Auditoría Interna (1h)	
	Subdirección General de Gestión (1h)	
	Subdirección General Médica-Hospital (5 h)	
	Subdirección General de Medios: Infraestructuras y Compras y Contratación (1h)	
	Subdirección General de Medios: Dirección de Procesos y Operaciones	12 horas
	Protección de datos	4 horas
TIEMPO ESTIMADO TOTAL		30 horas

Se trata de una estimación por lo que en caso de ser necesario podría haber variación sobre la misma, requiriéndose una inversión mayor de tiempo o menor.

## 5.3 ACTUACIONES

Deberán realizarse las siguientes actuaciones en el primer año de duración del contrato y anualmente en caso de ejecutarse la prórroga:

**-Planificación:** Se fijará un calendario con al menos un mes de antelación a la auditoría.

**-Reunión inicial.**

En la reunión inicial que se mantendrá con el adjudicatario, se concretarán las horas y jornadas que se dedicarán, debiendo haber aprobación por parte de la persona asignada por FREMAP.

La reunión tendrá lugar en la Sede Social de FREMAP cuya dirección es la siguiente:

**Sede Social de FREMAP,**  
**Mutua Colaboradora con la Seguridad Social nº61.**  
**Carretera de Pozuelo, 61.**  
**Majadahonda**  
**CP: 28222**

**-Entrega de documentación y preparación de las visitas.**

FREMAP entregará de forma anterior a realización de la jornada de auditoría, la documentación que el responsable designado considere necesaria para realizar la auditoría y que deberá revisarse por el auditor de forma anterior a la visita.

Asimismo, se facilitará la Normativa Interna de FREMAP si fuera necesario.

**-Visitas in situ o auditoría a distancia si FREMAP lo considerara oportuno**

FREMAP comunicará al adjudicatario la forma de realización de la auditoría. En el supuesto de que sea “in situ”, las visitas tendrán lugar en la Sede Social de FREMAP y en el Hospital objeto de auditoría en el ejercicio en curso, según se especifica en el apartado 3. Alcance del servicio, siendo la finalidad de las mismas comprobar la adecuación de las distintas actividades a la normativa aplicable, teniendo como resultado la preparación de un Informe sobre el cumplimiento de la entidad vinculado a los estándares recogidos en la normativa aplicable.

**-Horas de prestación del servicio.**

Las horas de prestación del servicio por centro y materia indicadas en el apartado 5.2 horas estimadas para la realización de la auditoría, comprenderán la realización de todas las actuaciones reflejadas en el presente apartado

**-Actas de la visita.**

Una vez finalizada la visita in situ se entregará a la persona asignada por FREMAP el acta de la visita en la que deberá aparecer la siguiente información:

- La fecha de la visita.
- La duración de la visita.
  - Se deberá entregar un cuadro horario, reflejando en cada caso las horas de auditoría dedicadas, el auditor/es encargado/s de realizarla/s y el objeto de auditoría.
- El auditor que realiza la visita.
- El personal entrevistado.
- El campo de observaciones que será únicamente para el personal de FREMAP.
- El check list que se ha rellenado durante la visita adjunto.
- La firma del auditor/es y el responsable asignado por FREMAP.

- Conclusiones preliminares de la visita. Lo que posteriormente se refleje en el informe previo al definitivo no podrá contradecir lo dispuesto en este punto.

Este documento se lo quedará FREMAP y servirá como justificación de las actuaciones realizadas.

#### **-Informe de auditoría en fase de borrador.**

En el plazo máximo de 5 días hábiles desde la realización de la visita y la auditoría in situ, el adjudicatario entregará el informe de auditoría.

El informe tendrá el formato establecido por la normativa de aplicación y se ajustará al check list utilizado en la visita, recogiendo en cada caso:

- Puntuaciones
- Puntos fuertes
- Oportunidades de mejora
- No conformidades
- Observaciones
- Comentarios

#### **-Informe previo al definitivo.**

Tras dar la conformidad al informe de auditoría en fase de borrador, se emitirá el informe previo al definitivo. En este momento se abre el proceso de las alegaciones en un plazo máximo de 10 días hábiles por parte de FREMAP.

#### **-Informe definitivo.**

Tras las alegaciones se 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.** Será en ese momento cuando se pueda presentar la factura a FREMAP, según lo que se especifica en el Pliego de Cláusulas Administrativas.

El informe deberá estar firmados y entregarse de la siguiente forma:

- Digital, mediante firma electrónica y en formato PDF.

## 5.4 SISTEMA DE VALORACIÓN

Valoración 27001			Valoración 27002		
Peso	Situación	Descripción	Peso	Situación	Descripción
0	Inexistente	Total falta de cualquier proceso reconocible. La Organización ni siquiera ha reconocido que hay un problema a tratar. No se aplican controles.	0	Inexistente	No hay en absoluto ningún proceso reconocible asociado al asunto.
1	Inicial	Hay una evidencia de que la Organización ha reconocido que existe un problema y que hay que tratarlo. No hay procesos estandarizados. La implementación de un control depende de cada individuo y es principalmente reactiva.	1	Inicial	Se dispone de planteamientos ad hoc que se aplican individualmente o en cada caso concreto. El asunto no se aborda de manera uniforme.
2	Repetible	Los procesos y los controles siguen un patrón regular. Los procesos se han desarrollado hasta el punto en que diferentes procedimientos son seguidos por diferentes personas. No hay formación ni comunicación formal sobre los procedimientos y estándares. Hay un alto grado de confianza en los conocimientos de cada persona, por eso hay probabilidad de errores.	2	Repetible	Se establecen formalmente procesos asociados respecto al asunto, que cuentan con una participación y supervisión activas por parte de la dirección, pero no se adoptan en toda la organización. No hay formación y la comunicación sobre normas y responsabilidades se efectúa individualmente.
3	Definido	Los procesos y los controles se documentan y se comunican. Es poco probable la detección de desviaciones.	3	Definido	Los procedimientos se han normalizado, documentado y aplicado ampliamente en la organización. La dirección ha dado a conocer procedimientos normalizados y se ha establecido una formación informal. Los procedimientos, sin ser complejos, pueden evaluarse y son el resultado de oficializar las prácticas habituales.
4	Gestionado	Los controles se monitorean y se miden. Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas de acción donde los procesos no estén funcionando eficientemente.	4	Gestionado	Se tiene un conocimiento claro de quien es el cliente y las responsabilidades están definidas. Los procesos están bien definidos e integrados en toda la organización y se utilizan adecuadamente en toda ella. Está determinada la titularidad de los procesos y se respalda mediante formación formal. Todas las partes que intervienen en los procesos asociados son conscientes de los riesgos y de las oportunidades.
5	Optimizado	Las buenas prácticas se siguen y automatizan. Los procesos han sido redefinidos hasta el nivel de mejores prácticas, basándose en los resultados de una mejora continua.	5	Optimizado	Los procesos asociados se han refinado hasta el nivel de las mejores prácticas externas, basándose en los resultados de una mejora continua y en los modelos de madurez establecidos con otras organizaciones. Los riesgos y consecuencias de los procesos asociados se definen, equilibran y comunican en la organización. La formación y comunicación están actualizadas. La aplicación de la política se traduce en una organización, un personal y unos procesos que se adaptan rápidamente y que respaldan plenamente las modificaciones de la estructura de riesgos.

## 5.5 CONDICIONES DE LA PRESTACIÓN DEL SERVICIO

---

En el precio deberán estar incluidos:

- Todas las actuaciones recogidas en el apartado 5.3 Actuaciones del presente Pliego y los medios reflejados en el Pliego de Cláusulas Administrativas:
  - Reunión anual inicial.
  - Revisión de la documentación recibida y preparación de las visitas.
  - Las visitas in situ.
  - Las actas de las visitas.
  - Horas de realización de la auditoría anuales estimadas.
  - Los informes de auditoría en fase de borrador.
  - Los informes anuales previos al definitivo.
  - Los informes anuales definitivos.
  - Los medios personales y materiales indicados en el Pliego de Cláusulas Administrativas.
- Todos los gastos inherentes a la prestación del servicio tales como desplazamientos, alojamiento, y manutención, papelería.

## 6. CONTROL Y SEGUIMIENTO DEL CONTRATO

---

FREMAP se reserva el derecho a realizar en cualquier momento una verificación de los servicios objeto del presente pliego para garantizar el pleno cumplimiento de las condiciones establecidas en el mismo, así como de solicitar a la empresa adjudicataria la documentación acreditativa de estar en pleno cumplimiento de todas las condiciones estipuladas en el presente Pliego.

### 6.1 Control de Calidad

---

Tras la finalización de todas las actuaciones reflejadas en el punto 5.3 Actuaciones en cada centro, FREMAP realizará una encuesta de calidad del servicio, valorando la calidad percibida.

Se evaluará sobre 10 puntos, siendo 1 la mínima puntuación y 10 la máxima. Se evaluará:

- Trato y comportamiento del auditor.
- Exactitud del informe.
- Cumplimiento de expectativas.
- Comunicación de resultados.
- Plazo de recepción del informe definitivo.
- Desarrollo de la auditoría.
- Cualificación del auditor.
- Utilidad del informe de auditoría.
- Puntualidad.
- Inversión del tiempo en cada materia según lo previsto en el apartado 5.2 Horas estimadas para la duración de la auditoría.
- Acta y entrega del cuadro horario.
- Sugerencias por parte del Director.

La puntuación obtenida en cada apartado de la encuesta deberá ser superior a 7, de no ser así, FREMAP aplicará a la empresa adjudicataria las penalidades que se describen en el Pliego de Cláusulas Administrativas.

