

**Procedimiento N°: E/05443/2018**

## **RESOLUCIÓN DE ARCHIVO DE ACTUACIONES**

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante Don **A.A.A.** S.L., (en lo sucesivo A.A.A.), y la SUBCOMUNIDAD DE PROPIETARIOS CLÍNICA ASTARTÉ, en virtud de reclamación presentada por SATINEL SYSTEM S.L., (en lo sucesivo la reclamante), y teniendo como base los siguientes:

### **HECHOS**

**PRIMERO:** Con fecha 2/08/2018 se recibe la notificación de un incidente que puede afectar a la seguridad de información de datos personales, manifestando el reclamante:

- 1) SATINEL tiene como objeto social el análisis, diseño, programación de sistemas informáticos, montajes y diseño de redes, mantenimiento de sistemas informáticos y presta a la SUBCOMUNIDAD DE PROPIETARIOS CLÍNICAS ASTARTÉ (SUBCOMUNIDAD en lo sucesivo) asistencia técnica para los sistemas de datos y voz, contando con la instalación de elementos necesarios de hardware y software en las propias instalaciones de dicha clínica ASTARTÉ.

*“Es encargado del tratamiento de CLÍNICA ASTARTÉ, centro sanitario de naturaleza privada con hasta 31 especialidades médicas, y que “gira en el tráfico jurídico como SUBCOMUNIDAD al amparo de la Ley 49/1960 de Propiedad horizontal, aunque se trate de una sociedad civil.”*

Aporta como soporte de sus afirmaciones, copia de contrato, de fecha 28/09/2009, de SATINEL con SUBCOMUNIDAD, entidad *“encargada de la prestación de servicios médicos varios”*. El contrato tiene como objeto la contratación de asistencia técnica para los sistemas de datos y voz. Entre algunos de los servicios que presta, figuran:

- i. Monitorización del tráfico interno de la red.
- ii. Todas las licencias necesarias para el sistema operativo.
- iii. Adaptación y auditorías necesarias para el cumplimiento LOPD.
- iv. Control y monitorización de las entradas de usuarios externos.
- v. Instalación y configuración del hardware.
- vi. Gestión y realización de copias de seguridad. Instalación y configuración de firewall.

- 2) La SUBCOMUNIDAD *“tiene una base de datos conjunta”*, gestionada a través del software *“SALUS”* que ofrece distintos tipos de utilidades a cada una de las especialidades, señalando *“ocho”*, *“correspondiéndose con entidades que gestionan datos”*, indicando algunas de ellas (especialidad de estética, área quirúrgica, urología), siendo unas sociedades limitadas, o limitadas profesionales SLP, figurando entre ellas la de Don **A.A.A.** SLP, indicando que *“estas entidades son responsables del tratamiento contando también la SUBCOMUNIDAD.”* Además, A.A.A., integrante de la

SUBCOMUNIDAD, como subcomunero tiene instalaciones médicas en la primera planta del edificio ASTARTÉ, ajenas a la clínica que giran bajo la marca GRUPO MÉDICO **A.A.A.**, y otra actividad que es una consulta médica en dicho edificio, considerando que por esta consulta, es *“co-responsable del tratamiento”*,

- 3) A.A.A. a principios de febrero 2018, decidió rescindir unilateralmente el contrato de mantenimiento informático *“que tenía suscrito y vigente con SATINEL”*, contratando los servicios con TÉCNICA 24 SOFTWARE Y SERVICIOS SL.; y a primeros de junio 2018, A.A.A. les manifestó su intención de *“independizar su instalación telefónica de la común de la SUBCOMUNIDAD”*. A.A.A. *“ha organizado su propia red llevando a cabo una labor de exfiltración de la base de datos de la SUBCOMUNIDAD que incluye la de sus pacientes y la de pacientes de otros facultativos”*, efectuada a través del prestador de servicios TÉCNICA 24.
- 4) Aporta como documento 4 un correo electrónico que GRUPO MÉDICO **A.A.A.** remite, el 11/06/2018, al Administrador de la SUBCOMUNIDAD y que se entrega también a SATINEL. En él se indica que han decidido prescindir de los servicios de SATINEL como proveedor de mantenimiento informático de GRUPO MÉDICO **A.A.A.**, porque han cambiado el sistema de telecomunicaciones y del software de la clínica a partir de 11/06/2018. Indica que *“No obstante, seguiremos abonando nuestra parte proporcional como copropietarios de la CLÍNICA ASTARTÉ que asciende según el contrato de mantenimiento firmado con SATINEL y la propia clínica a 679,8 euros mensuales.”* Manifiesta SATINEL que la referencia *“a este contrato es al mencionado de 28/09/2009.”*
- 5) El día 9/06/2018, personal de SATINEL, al acudir a efectuar tareas de mantenimiento en el habitáculo en el que se encuentran los elementos de hardware y software de la SUBCOMUNIDAD, *“comprobó como uno de los técnicos contratados por A.A.A. había accedido al citado habitáculo levantando las placas de escayola del techo de la clínica, hasta llegar a dicho espacio.”*
- 6) Aporta SATINEL una copia de informe pericial, de 5/07/2018, por las *“sospechas de incidencia en los sistemas de información a los que accedió GRUPO MÉDICO **A.A.A.**- GMLC- con la cooperación de la empresa TÉCNICA 24”*. Manifiesta que *“esta información se encontraba almacenada en los servidores informáticos de SATINEL SYSTEM que tiene a disposición de CLÍNICA ASTARTÉ”*.
- 7) El informe pericial consiste en la personación con un notario a instancia del administrador de SATINEL en el edificio de CLÍNICA ASTARTÉ en Cádiz, acompañados de un perito informático que efectúa un informe en nombre de SATINEL.

Comienza indicando que se le proporciona por SATINEL una serie de números de identificaciones de historias clínicas más las iniciales de pacientes a los que corresponden y de los departamentos especialistas a los que pertenece el dato, obtenida de la fuente originaria, aplicación SALUS. Se trata de verificar la existencia de una aplicación de gestión clínica del GMLC y de comprobar si existen réplicas de los datos a buscar.

Los identificados acuden a la recepción de la clínica, y allí contactan con D<sup>a</sup> **B.B.B.**, (\*\*PUESTO.1). Esta empleada contacta con el Administrador de SUBCOMUNIDAD

CLÍNICA ASTARTÉ, se le pone en antecedentes, y entabla una conversación con el Administrador de SATINEL, que *“concede autorización para proceder a practicar las pruebas necesarias”*.

En los datos personales que se obtiene en este informe han pixelado los mismos, de modo que no se ven. Indica el informe que *“El objetivo de nuestra actuación será la reproducción ante notario de una sesión de trabajo para comprobar los permisos de acceso a la información que posee el personal de la recepción general, registrando la información a la que se tiene acceso con las credenciales habitualmente utilizadas por este personal, tanto las propias del sistema operativo como las de las aplicaciones que utilizan”*. *“Nos interesa comprobar la existencia de una nueva aplicación de gestión clínica para GMLC y en caso afirmativo, si a través de ella se tiene acceso a los datos reservados de carácter personal de pacientes de otros especialistas”*.

*“La primera de las preguntas que teníamos que responder era si se podía comprobar la existencia de un nuevo software de gestión clínica usado por GMLC de forma independiente, exclusiva y ajeno al software de gestión clínica de CLÍNICA ASTARTÉ denominado “SALUS”. La respuesta la obtenemos por un lado mediante la confirmación por parte de la \*\*\*PUESTO.1 de la existencia de esta nueva aplicación, y, por otro lado, mediante la inspección directa como se puede ver en la siguiente fotografía”* Se aporta una fotografía del ordenador en la que en la pantalla se ve algo, pero no se distingue lo que es, manifestándose que es *“la nueva aplicación de GMLC en ejecución”*. *“La información se obtiene desde el puesto de trabajo del personal de recepción general”*.

*“Procedemos a realizar unas búsquedas en la aplicación de gestión clínica de GMLC. Utilizaremos para ello datos proporcionados por el administrador de SATINEL procedentes de la fuente de información original”*.

Se buscan los números de historia clínica previamente extraídos, *“confirmando por un lado su existencia y por otro, su coincidencia con las iniciales del nombre del paciente, advirtiendo que esta información, perteneciente a distintas especialidades médicas, nunca debería existir en una específica para el GMLC”*.

Manifiestan que efectúan capturas de pantallas de estos hallazgos, si bien en la copia que aportan no figura, por protección de datos, según indica, *“existiendo una copia con los datos reales en poder del notario y el Administrador de SATINEL”*.

Se indica que, consultado un historial clínico, se puede acceder a todos sus datos personales, y al *“registro de visitas”* así como a una serie de documentos sensibles: autorización de ingreso, hoja de evolución, hoja quirúrgica. *“En la dirección en la que figuran los documentos y las carpetas aparece el termino SALUS, indicativo indiciario del origen de los datos.”* Aportan captura de pantallas en la que manifiestan que se puede ver el histórico de visitas de los pacientes, aunque como se ha indicado en el informe ahora aportado no se ve dato alguno.

Manifiesta el informe que en las consultas de citas se hacen referencias a especialistas ajenos al GMLC, como ejemplo Urología, Otorrino, Traumatología, y se puede acceder a *“información sensible, Anamnesis”*, *“a la que no se debería poder acceder por el tipo de usuario con el que estamos realizando la prueba-nivel de \*\*\*PUESTO.1- cuyo único acceso debería ser el específico y necesario para \*\*\*TAREA.1”*.

Se llega a la conclusión que de ocho historias clínicas a consultar, todas existían en la nueva aplicación, *“coinciden las iniciales de nombre y apellidos y DNI con los datos completos a lo que tiene acceso el administrador de SATINEL en base a los datos completos a los que tienen acceso de la aplicación oficial de gestión clínica de CLÍNICA ASTARTÉ”, “Salus”.*

8) SATINEL aporta documento, de fecha 6/07/2018, denominado *“incidente de seguridad brecha de confidencialidad Clínica Astarté 2/2018”* en el que se dirige a la CLÍNICA ASTARTÉ-SUBCOMUNIDAD DE PROPIETARIOS. En el escrito se manifiesta:

*“Como encargado del mantenimiento informático de esa CLÍNICA, y por ende del tratamiento de datos de los que ustedes son responsables, poniendo en su conocimiento un incidente de seguridad en los datos de salud de sus pacientes. “Desde hace poco tiempo por parte del Subcomunero A.A.A. se había dado instrucciones a recepción general de la CLÍNICA ASTARTÉ para que todo lo concerniente a la gestión de sus pacientes se efectuará en la aplicación web <https://www.Técnica24.es/A.A.A.> para lo que se proporcionaron las distintas claves de usuario y contraseña” “Por distintas informaciones y consultas recibidas de los usuarios y pacientes albergamos la sospecha de que en dicha aplicación no solo se encontraban los datos de los pacientes de dicho subcomunero sino de pacientes de otras especialidades de la Clínica y que no lo son ni lo han sido de A.A.A.”. “El pasado 13/06 A.A.A., GMLC comunicó a esta empresa su decisión unilateral de prescindir de los servicios de mantenimiento informático del proveedor del resto de la CLÍNICA por haberse procurado un nuevo proveedor a dichos fines”.*

También informa que los mencionados habrían obtenido y exportado una copia de los datos de todos los pacientes de CLÍNICA ASTARTÉ tanto de los que sería responsable como de otros de los que son responsables los distintos especialistas. Propone en el mismo comunicado algunas medidas de contención como bloquear el acceso de todos los equipos de la clínica ASTARTÉ a la web <https://www.Técnica24.es/A.A.A.>, o propone a la SUBCOMUNIDAD la instalación de un software auditor para controlar el flujo de información entre los distintos usuarios.

Declara SATINEL que la SUBCOMUNIDAD ha negado el incidente y no ha notificado a los afectados extremo alguno, y que encargó por su parte un informe a la entidad denominada DIRECCION DE CUMPLIMIENTO NORMATIVO SL.

8) SATINEL aporta escrito de TÉCNICA 24, fechado el 9/07/2018, en el que le comunica que *“habiendo suscrito con A.A.A., el 5/02/2018, contrato de tratamiento de datos, certifica que A.A.A.” “nos realiza encargo para resolver problemática generada en el cumplimiento de la LOPD por el acceso a una base de datos única y compartida por todas las empresas pertenecientes a la Comunidad de Propietarios de la CLÍNICA ASTARTÉ. Hecho que se comprueba ante la empresa encargada de la protección de datos del cliente, MENTORA y ante Notario, levantándose acta correspondiente”. “El proceso de exportación de la antigua base de datos única del sistema SALUS contenía datos globales de toda la CLÍNICA ASTARTÉ. El proceso de importación de datos a la nueva base de datos ORACLE incluyó todos los datos provenientes del anterior sistema SALUS. Se ha realizado un proceso de*

*depuración de información para dejar exclusivamente los datos pertenecientes a historia clínicas tratadas por facultativos que han trabajado o trabajan actualmente en A.A.A. “*

9) Aporta SATINEL copia de un escrito de 18/07/2018 de la entidad COMPLIANCE CORPORATE en el que indica que como consultores externos de la SUBCOMUNIDAD “entendemos que no ha existido violación de seguridad en el copiado de BBDD de la SUBCOMUNIDAD por parte de A.A.A. ya que los privilegios de acceso antes y después de la copia de la BDD eran similares”.

10) Los hechos están denunciados el 12/06/2018 en el Juzgado de Instrucción 4 que instruye diligencias previas **XXX/2018**, originariamente por el acceso al elemento físico donde se encontraban ubicados los servidores informáticos de la clínica que ha sido ampliada por el Administrador de SATINEL el 25/07/2018. En la copia que aportan figura que es el encargado del sistema informático de la clínica ASTARTÉ y que la ampliación se produce tras la realización del informe pericial de SATINEL llevado a cabo en los sistemas de A.A.A. el 5/07/2018.

SEGUNDO: Con fecha 4/09/2018, la directora de la AEPD acuerda iniciar actuaciones previas de investigación.

A) Con fecha 26/10/2018 se obtiene del acceso a la web CLÍNICA ASTARTÉ, la impresión de la “política de privacidad”, informándose por la SUBCOMUNIDAD DE PROPIETARIOS CLÍNICA ASTARTÉ (CIF...) de la existencia de un fichero automatizado denominado *Clientes* creado con la finalidad de realizar la gestión contable, fiscal y administrativa de los usuarios, y que “el envío de los datos de carácter personal es obligatorio para contactar y recibir información sobre los productos y servicios de CLÍNICA ASTARTÉ” y que el fichero es titularidad de CLÍNICA ASTARTÉ (no señala el CIF), si una dirección. Se informa que las finalidades son las de “desarrollo de actividades y prestación de información sobre productos de CLÍNICA ASTARTÉ”.

B) Con fecha 6/11/2018, se remite escrito a la SUBCOMUNIDAD en relación con los hechos denunciados, solicitándole:

1) *Informe detallado de las causas y circunstancias acontecidas en junio de 2018, por parte de (A.A.A.) se realizó una copia de la base de datos de pacientes de la Clínica ASTARTÉ, indicando la tipología de los datos que contiene dicha base de datos.*

2) *Especificación y acreditación de que (A.A.A.) disponía de autorización por parte de la SUBCOMUNIDAD para realizar la extracción de los datos, no solo de sus pacientes, si no de los pacientes de todas las empresas que pertenecen a esa Comunidad y para desplegar su propia red de telecomunicaciones paralela.*

3) *Especificación de las medidas organizativas y técnicas que se han adoptado por parte de la SUBCOMUNIDAD de propietarios como consecuencia de los hechos descritos.*

4) *Copia de toda la documentación de que dispongan en relación con los citados hechos.*

5) Descripción detallada, en su caso, de las acciones correctivas tomadas indicando fecha y hora de las medidas adoptadas.

6) Información, en su caso, respecto de las notificaciones realizadas a los afectados. Aportar copia, en su caso, de la notificación remitida.

Con fecha 27/11/2018 se recibe respuesta en la que indica:

a) La SUBCOMUNIDAD, o CLÍNICA ASTARTÉ no proporciona servicios médicos de ningún tipo, solo aglutina en un nombre común y en un lugar concreto a distintos profesionales de la medicina, es una mera forma jurídica que se adopta por acuerdo de todos los profesionales que la componen, si bien cada comunero es responsable del tratamiento de sus propios datos, entre ellos los de los pacientes. Los fines de la SUBCOMUNIDAD son dotar a los comuneros de unas herramientas que faciliten el desarrollo de sus actividades, no tratando dato médico alguno, ni propios ni por cuenta de terceros.

*“Debería ser cada comunero o cada profesional que compone esa Comunidad el que debe responder de los datos que tratan.”*

b) Manifiesta que colaborando con la petición, hace constar que el 26/06/2006 fecha de constitución de la SUBCOMUNIDAD, se firmó un compromiso por parte de los comuneros para compartir los datos de pacientes de cada una de las clínicas en una única base de datos con el objetivo de ofrecer a los pacientes una asistencia sanitaria lo más completa y ajustada posible a cada caso. Adjuntan ANEXO I en el que en un escrito de 26/06/2006, ante notario, distintas personas físicas entre las que se incluye A.A.A., cada uno en nombre de una entidad mercantil, invariablemente del sector clínico o relacionado con la salud con forma societaria, suscriben un contrato de compromiso. En el mismo se indica que han adquirido al Consorcio de la Zona Franca de Cádiz, un local comercial en planta baja del edificio ASTARTÉ y que según el proyecto en su día presentado se dedicaría a clínica de asistencia sanitaria especializada. *“Han procedido a dividir el local en diferentes módulos los cuales se han adjudicado a las diferentes personas físicas y jurídicas aquí actuantes”* *“Con ocasión de dicha división y extinción de condominio, se ha constituido una subcomunidad entre todos los módulos resultantes por división del local a que se refiere el expositivo 1”,* y *“Que, de acuerdo con el destino de CLINICA DE ASISTENCIA SANITARIA ESPECIALIZADA, los intervinientes procederán al ejercicio de la medicina en los módulos o departamentos independientes a cada uno de ellos adjudicado por virtud de la antes citada extinción de comunidad, y que actualmente comprenden las siguientes especialidades...”*

En la primera estipulación se indica: *“Los Señores comparecientes, según intervienen, se comprometen entre ellos a mantener estrechas relaciones profesionales de colaboración para potenciar la interrelación en su caso de las diferentes especialidades médicas, con el fin de cumplir la finalidad primordial de funcionamiento como UNA CLINICA DE ASISTENCIA SANITARIA ESPECIALIZADA.”*

En las estipulaciones no se hace referencia alguna a los historiales, datos médicos o base de datos, si se mencionan servicios comunitarios y de zonas comunes

c) La SUBCOMUNIDAD, en Junta celebrada el 20/09/2018 procedió a solicitar ofertas a distintas empresas de prestación de servicios informáticos con la finalidad de encontrar un proveedor de servicios que garantice los mínimos de seguridad.

Aportan ANEXO 2 en el que en el orden del día figura *“información sobre supuesta vulneración de seguridad informática”* y en el tercero, el cambio de proveedor informático. Como asistentes figuran varias Sociedades. En relación con la vulneración de seguridad informática, el representante de SATINEL explica los hechos, existiendo algunas entidades encargadas de la protección de datos de las sociedades que acuden o de la misma SUBCOMUNIDAD. Indica un enlace en *drive.google* para descargar las distintas opiniones manifestadas. Indica como conclusión, excepto SATINEL, que consideran que no ha habido vulneración de seguridad informática. Se pregunta al representante de SATINEL, si en su opinión, el acceso directo a la página web de A.A.A. existente en la parte local de los puestos de recepción general de la Comunidad, para atender la agenda de A.A.A. es un riesgo de fuga de datos, responde afirmativamente, *“luego hace la misma pregunta a los técnicos informáticos y de protección de datos presentes, respondiendo que dicho acceso no provoca ninguna fuga de datos”*

En el punto de suministro y mantenimiento de la informática de la comunidad así como el telefónico, se pide que se envíen las ofertas que se harán llegar a los distintos propietarios.

C) Con fecha 6/11/2018 se remite escrito a A.A.A. en relación con los hechos denunciados, solicitándole:

*“1. Especificación y acreditación de que esa entidad, disponía de autorización por parte de la SUBCOMUNIDAD para realizar la extracción de los datos, no solo de sus pacientes, sino de los pacientes de todas las empresas que pertenecen a la citada Comunidad y para desplegar su propia red de telecomunicaciones paralela.”*

*2. Especificación del procedimiento por el que, con posterioridad, se procedió al borrado de los datos de los pacientes de las otras sociedades.*

*3. Copia de toda la documentación de que dispongan en relación con los citados hechos.*

*4. Copia del contrato de prestación de servicios suscrito CON TÉCNICA 24 SOFTWARE Y SERVICIOS S.L., indicando la participación de esta sociedad en la copia de la citada base de datos y en la instalación de una red de telecomunicaciones paralela.”*

Con fecha 27/11/2018 se recibe respuesta en la que indica:

a) En la antes citada escritura de compromiso se firmaba por las entidades que tienen como objeto social directa o indirectamente la prestación de servicios médicos, un acuerdo en el que en una de las cláusulas se comprende: mantener estrechas relaciones profesionales de colaboración para interrelacionar en su caso las distintas especialidades médicas con el fin de cumplir la finalidad primordial de funcionamiento como una clínica de asistencia sanitaria especializada, y por tanto se comprometen a utilizar de forma coordinada los servicios comunitarios y complementarios del local con el fin de potenciarlos y seguir los criterios de funcionamiento para lograr la mejor coordinación entre los diferentes módulos especialidades que la componen y la mejor coordinación en la utilización de las instalaciones y equipos o instrumentos comunes.

b) Indica que el 30/08/2007 se suscribe entre la SUBCOMUNIDAD de propietarios CLÍNICA ASTARTÉ y la empresa SATINEL, *“dedicada a servicios informáticos, integrante como comunero de la misma, un acuerdo mercantil para la prestación de asistencia técnica para los sistemas de datos voz bajo una solución única sobre convergencia IP”* recogiendo los diversos servicios incluidos entre otros, voz, datos, puestos telefónicos, equipos, copias de seguridad, firewall e incluso un software de gestión llamado SALUS para gestión de agendas, citas e historia clínica de pacientes. A pesar de contratarse de común el servicio, los honorarios se abonaban de forma individualizada según los servicios acordados a prestar a cada copropietario.

c) Manifiesta que *“desde el principio ha sido general y normalizado en el día a día, para favorecer el tratamiento integral, completo y responsable hacia los pacientes, el uso compartido de la base de datos del sistema SALUS depositado en los servidores instalados en la zona común de la clínica ASTARTÉ de modo que todos y cada uno de los copropietarios venían volcando la información relativa a todos sus pacientes-clientes en dicho sistema, en la creencia y buena fe de las partes que lo entendían como un sistema idóneo, en el que todos accedían a todo, sin problema, autorizándose mutuamente contando con el permiso y total libertad de movimiento de modo habitual y sistemático, y que “En dicho sistema nunca se colocaron por SATINEL cortapisas ni limitaciones de acceso ni de usos para los copropietarios”*

d) Aporta un relato cronológico del tenor:

*“En mayo de 2018, A.A.A. realiza en sus instalaciones un seguimiento y control sobre el grado de cumplimiento en materia de protección de datos- por parte de la empresa externa MENTORA GROWTH. Tras comprobaciones se aprecian indicios de que en el programa SALUS:*

*d.1) La información propia se podría estar confundiendo con la información de otras empresas en una única base de datos indisociable.*

*d.2) Es posible realizar copia de información en soporte electrónico por parte de cualquiera de los usuarios con acceso a la misma, Independientemente de su nivel de atribuciones o responsabilidad en la empresa o de otras empresas que comparten el programa de gestión.*

*d.3) Por ello, y cara a la entrada en vigor del RGPD se recomienda adaptar el sistema y adoptar medidas que:*

*-Garanticen la confidencialidad y disponibilidad de la información.*

*-Impidan el acceso a la misma por parte de quien no esté autorizado.*

*-Garanticen la integridad de la información.*

*-Determinen la segregación de la información perteneciente exclusivamente a la organización y el poder disociarla de la común de otras entidades que comparten el servidor.*

*-Implanten medidas que impidan la captación y copia de bases de datos por parte de cualquiera con acceso a la información”.*

e) Indica que el 24/05/2018, encarga a TÉCNICA 24 SOFTWARE Y SERVICIOS SL la comprobación técnica del sistema y estabilización y aseguramiento de la información propia de A.A.A.. *“Se verifica que en la aplicación de gestión SALUS implantada por SATINEL, la seguridad de la base de datos no es suficiente, por cuanto es accesible por cualquier usuario con un doble clic para realizar copia sin precisar contraseña no existiendo diferencias significativas entre roles con idénticos permisos y absoluta disponibilidad de la información a todos los efectos, no solo de inclusión o integración, manipulación o tratamiento sino copia y borrado de la información.”*

f) El 4/06/2018 se solicitó la presencia del notario para levantar acta, efectuando una comprobación en un puesto de trabajo aleatorio, con la posibilidad de exportar datos y su extracción del servidor de la SUBCOMUNIDAD en cualquier dispositivo móvil, sin precisar ningún protocolo especial, siendo el resultado de esta comprobación positivo, adjuntan copia de documento 6.

g) Con fecha 8/06/2018 se envió burofax a SATINEL, para dar conocimiento de los hechos, adjunta documento 7, para trasladarle la inquietud de que no existe contrato de prestación de servicios firmado entre ambas partes, y que todos los servicios recibidos, básicos o complementarios devenían del contrato entre la SUBCOMUNIDAD y SATINEL.

*“Ante la inseguridad en el archivo y custodia de la información, como medida preventiva por si SATINEL al recibir la comunicación referida adoptara represalias que impidieran la continuidad de la prestación del servicio médico por A.A.A., o se produjera algún borrado o alteración accidental por algún usuario de la base, mientras se comienza a desarrollar el nuevo sistema de gestión, de manera urgente y como medida necesaria, A.A.A. decide realizar la copia de seguridad de la base de datos para salvaguarda de la información de los pacientes”* *“TÉCNICA 24 según instrucciones de A.A.A. comienza a trabajar en ello, accediendo a la información de modo anonimizado para intentar seleccionar aquella exclusivamente identificada a priori, como información subida a la aplicación SALUS por A.A.A.”* *“finalmente se comprueba que el proceso conllevaría una dificultad extraordinaria e insuperable que hace inviable extraer exclusivamente la información subida por A.A.A. a la aplicación SALUS por ser técnicamente indisociable la información restante, con una inversión viable de tiempo y recursos.”* Se aporta certificado de TÉCNICA 24 en el que con fecha 9/07/2018 se informa sobre todo el proceso. Aporta documento 8.

*“Dado que la información era compartida y de uso común desde siempre, y no iba a producir ningún tipo de daño, indisponibilidad o falta de integridad de la misma, ni cambio alguno a Subcomunidad, clientes, terceros ni a A.A.A., se entendió en todo momento y siempre en la confianza de la buena fe que venía presidiendo todo el movimiento diario de información dentro de la Clínica, que no había problemática alguna en adoptar dicho procedimiento”.*

*“Posteriormente, si se pudo realizar con menor grado de dificultad un proceso de depuración de información para dejar activos exclusivamente los datos pertenecientes a pacientes tratados por médicos y especialistas de A.A.A.. Respecto al proceso de borrado de la restante información el proceso fue:*

- Se obtuvo una lista de facultativos que habían trabajado alguna vez para A.A.A..
- Se cruzó esta información con los facultativos existentes en alta en A.A.A..
- Se borraron todos los datos de pacientes vinculados a facultativos no A.A.A..

En el funcionamiento de modo independiente, solo existe información de A.A.A..

h) Aporta copia de informe elaborado por orden de la SUBCOMUNIDAD, por la empresa denominada “COMPLIANCE CORPORATE” en documento 11, señalando que en uno de sus puntos se indica *“niega accesos ilegítimos por cuanto los accesos y usos de la base de datos volcada en el programa de Gestión SALUS estaban consentidos desde el primer momento y de forma unánime para y entre todos los copropietarios “los privilegios antes y después del copiado de la base de datos son exactamente los mismos”*

Aporta copia de escritura en la que se mencionan diversas clínicas y que son dueños entre todos del pleno dominio en la proporción y por el título que se dice más adelante, correspondiente al local de planta baja de Edificio ASTARTÉ. La propiedad se divide en módulos, atribuyendo los diferentes módulos a distintas especialidades por coeficientes entre las obligaciones de los propietarios.

i) Se aporta copia de contrato de prestación de servicios de 30/08/2007 entre SATINEL y la SUBCOMUNIDAD. Se indica que la SUBCOMUNIDAD es una *“sociedad dedicada a la prestación de servicios médicos varios”*, y para llevar a cabo su actividad necesita la instalación y administración de diferentes elementos de software y hardware. Se contrata la asistencia técnica para los sistemas de datos y voz bajo una solución única sobre convergencia IP, solo se hace referencia en alguna cuestión supuestamente relacionada con lo que podrá ser protección de datos a la prestación de *“gestión y realización de las copias de seguridad que se realizarán de manera diaria a soporte físico y anualmente a soporte de cinta quedando en posesión del cliente”* y *“adaptación y auditorías necesarias para el cumplimiento LOPD en los terminales comunes”*.

j) Aporta copia de informe de 24/05/2018 de *“proyecto de servicio IT”* elaborado por TÉCNICA 24 por encargo de A.A.A. en que destaca:

*-Objeto del proyecto: fase 1, comprobación y análisis técnico del sistema informático del cliente, fase 2 salvaguarda y aseguramiento de la información del cliente, sin que se aporte copia del resultado.*

k) Aporta copia de escrito dirigido por A.A.A., Grupo Médico **A.A.A.** dirigido al administrador de SATINEL indicando que *“dispone de elementos probatorios que acreditan graves incumplimientos respecto de la prestación del servicio con carácter general por parte de SATINEL como en particular respecto al nivel de cumplimiento de dichos servicios para GRUPO MÉDICO LC de la LOPD en relación con los estándares exigidos por el nuevo RGPD, principalmente en lo que respecta a la base de datos común de la clínica*

*ASTARTÉ -datos de pacientes, historias clínicas, etc.- y en sus sistemas de acceso y nulo sistema de seguridad de la misma”, y le informa que ha a cambiar sus sistemas informáticos propios, bases de datos, software de gestión etc.*

l) Aporta copia de acta notarial de 1/06/2018 en la que comparece un representante de A.A.A. y formando parte como comunero de CLÍNICA ASTARTÉ. En el acta de requerimiento en la clínica, para verificar la base de datos general de la clínica ASTARTÉ, el contenido de los datos que se ofrezcan en pantalla y si para el acceso a dicha base de datos existe algún tipo de restricción previa o limitación. Se indica que se accede al PC del despacho de **C.C.C.** con usuario y contraseña, y desde el mismo se accede al servidor de la clínica, igualmente con usuario y contraseña. Manifiesta que desde dicho servidor, a través de la aplicación SALUS se puede acceder libremente a los ficheros comprensivos del historial clínico de los “*pacientes de la clínica*”, no solo de los del grupo representado por el requirente, sino también de los pacientes de otros grupos de especialistas. Igualmente comprueba la posibilidad de exportar estos datos y su extracción del servidor en cualquier dispositivo móvil. *“Estas mismas comprobaciones las hacemos en el ordenador de una de las administrativas del centro elegida por mí al azar, con iguales consecuencias “según manifiesta el requirente, cualquier operario con clave de acceso puede de esta forma acceder sin filtro al contenido del servidor, y por ende a la totalidad de los datos contenidos en el mismo.”*

m) Copia de certificado de 9/06/2018 emitido por TÉCNICA 24 que indica que suscribió con A.A.A. el 5/02/2018 contrato de tratamiento de datos, y que A.A.A. *“nos realiza el encargo para resolver problemática generada en cumplimiento de la LOPD por el acceso a una base de datos única y compartida por todas las empresas pertenecientes a la comunidad de propietarios de la clínica Astarté. Hecho que se comprueba ante la empresa encargada de la protección de datos del cliente MENTORA y ante Notario, levantándose acta”. “El proceso de exportación de la antigua base de datos única del sistema SALUS contenía datos globales de toda la clínica ASTARTÉ. El proceso de importación de datos a la nueva base de datos ORACLE incluyó todos los datos provenientes del anterior sistema SALUS.”*

## FUNDAMENTOS DE DERECHO

### I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

### II

La Ley 41/2002 básica reguladora de la autonomía del paciente define en su artículo 3:

*“Centro sanitario: el conjunto organizado de profesionales, instalaciones y medios técnicos que realiza actividades y presta servicios para cuidar la salud de los pacientes y usuarios.”*

*“Servicio sanitario: la unidad asistencial con organización propia, dotada de los recursos técnicos y del personal cualificado para llevar a cabo actividades sanitarias.”*

*“Historia clínica: el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y la evolución clínica de un paciente a lo largo del proceso asistencial”.*

En el artículo 16, se establecen los usos de la historia clínica:

*“1. La historia clínica es un instrumento destinado fundamentalmente a garantizar una asistencia adecuada al paciente. Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.*

*2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.*

*3. El acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación o de docencia, se rige por lo dispuesto en la legislación vigente en materia de protección de datos personales, y en la Ley 14/1986, de 25 de abril, General de Sanidad, y demás normas de aplicación en cada caso. El acceso a la historia clínica con estos fines obliga a preservar los datos de identificación personal del paciente, separados de los de carácter clínicoasistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.*

*Se exceptúan los supuestos de investigación previstos en el apartado 2 de la Disposición adicional decimoséptima de la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales.*

*Asimismo, se exceptúan los supuestos de investigación de la autoridad judicial en los que se considere imprescindible la unificación de los datos identificativos con los clínicoasistenciales, en los cuales se estará a lo que dispongan los jueces y tribunales en el proceso correspondiente. El acceso a los datos y documentos de la historia clínica queda limitado estrictamente a los fines específicos de cada caso.*

*Cuando ello sea necesario para la prevención de un riesgo o peligro grave para la salud de la población, las Administraciones sanitarias a las que se refiere la Ley 33/2011, de 4 de octubre, General de Salud Pública, podrán acceder a los datos identificativos de los pacientes por razones epidemiológicas o de protección de la salud pública. El acceso habrá de realizarse, en todo caso, por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto, previa motivación por parte de la Administración que solicitase el acceso a los datos.*

*4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.*

*5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes*

*y usuarios o la propia Administración sanitaria.*

*6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.*

*7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso.*

En el presente supuesto se ha indicado por los reclamantes y reclamados que la Subcomunidad constituye lo que se define como centro sanitario dedicado a prestar asistencia sanitaria integral en unas determinadas especialidades médicas y que ha establecido los medios que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

### III

En cuanto a los datos de salud, el artículo 9 del RGPD señala:

*1. Quedan prohibidos el tratamiento de datos personales... relativos a la salud...*

*2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:*

*a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;*

*h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3.*

SATINEL denuncia el acceso de un médico que forma parte de la SUBCOMUNIDAD a las historias clínicas de la misma. El médico denunciado contrató la prestación de servicios informáticos y de adecuación a la nueva normativa de protección de datos con otra entidad; y para continuar la gestión de la asistencia sanitaria, copió las historias clínicas a las que legítimamente tenía acceso.

Por último, SATINEL denuncia que se ha producido una quiebra de seguridad en la información de los pacientes. El RGPD define, en su artículo 4.12 «violación de la seguridad de los datos personales»: como *“toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos”*. Como se ha indicado de forma exhaustiva en la recogida de los hechos denunciados y de las investigaciones realizadas, no se ha producido ningún acceso indebido a los datos de los pacientes de los profesionales que forman parte de la SUBCOMUNIDAD.

En consecuencia, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la directora de la Agencia Española de Protección de Datos,

**SE ACUERDA**

1. **PROCEDER AL ARCHIVO** de las presentes actuaciones.
2. **NOTIFICAR** la presente resolución a Don **A.A.A.**, a la SUBCOMUNIDAD DE PROPIETARIOS CLÍNICA ASTARTÉ, y a SATINEL SYSTEM S.L.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPCAP), y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13/07, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Mar España Martí  
Directora de la Agencia Española de Protección de Datos