Tecnicas para el control del tratamiento masivo de datos personales en el sector publico sanitario

Magdalena Jareño Butron
Técnica Superior Infomática

José Antonio Arratibel Arrondo
Interventor en el Servicio Vaco de Salud-Osakidetza. Gobierno Vasco-Eusko Jaurlaritza

Revista Auditoría Pública nº 81
Enero - junio 2023. Páginas: 180-195

Resumen: En este trabajo pretendemos hacer una reflexión partiendo del marco jurídico relativo a los derechos de los pacientes a la protección de sus datos de salud y las medidas que pueden implementarse para garantizar la seguridad en el tratamiento masivo de estos datos de especial protección jurídica. En este sentido, la seudonimización se ha convertido en una técnica común en el ámbito europeo de seguridad clave para facilitar el procesamiento de datos personales de salud, al tiempo que ofrece garantías sólidas para la protección de datos personales y, por lo tanto, protege los derechos y libertades de las personas. En definitiva, un trabajo necesariamente interdisciplinar que requiere el conocimiento de los límites jurídicos del derecho a la especial protección de los datos personales de salud y, el técnico de la ingeniería informática actual, para garantizar la ciberseguridad de los derechos que se pretenden proteger.

Palabras Clave: RGPD, Protección de datos personales salud, Privacidad, Big Data, Seudonimización, Ciberseguridad, ENISA.

Abstract: In this work we intend to make a reflection based on the legal framework related to the rights of patients to the protection of their health data and the measures that can be implemented to guarantee security in the massive treatment of this data of special legal protection. In this sense, pseudonymization has become a common technique in the European field of key security to facilitate the processing of personal health data, while offering strong guarantees for the protection of personal data and, therefore, protecting the rights and freedoms of people. In short, a necessarily interdisciplinary job that requires knowledge of the legal limits of the right to special protection of personal health data and, the current computer engineering technician, to guarantee the cybersecurity of the rights that are intended to be protected.

Keywords: GDPR, Protection of personal data, health, Privacy, Big Data, Pseudonymization, Cybersecurity, ENISA.

SUMARIO

I. Introducción

Todo usuario del sistema sanitario tiene derecho a la constancia, por escrito o en el soporte técnico más adecuado, de la información obtenida en todos sus procesos asistenciales, realizados por el servicio de salud, sobre sus datos médicos personales. Esto supone, per se, un tratamiento masivo de datos sensibles de salud de los ciudadanos por la Administración Sanitaria y sus entes gestores.

La protección de Datos personales es un derecho fundamental recogido en el artículo 18.4 de la Constitución Española y regulado por el Reglamento Europeo de Protección de Datos (RGPD), y la Ley de protección de datos_(LOPDGDD). En este caso en particular, la normativa en protección de datos se complementa con la Ley de Autonomía del Paciente 41/2002, de 14 de noviembre. La ley de protección de datos médicos se encarga de regular los derechos y las obligaciones en materia de información y documentación clínica en la que se regula su historial. Esta normativa afecta al personal que operan en el sector sanitario, a las clínicas, a los hospitales, a los centros médicos y a las instituciones sanitarias.

La LOPDGDD y el RGPD contemplan la posibilidad de que la introducción de tecnologías inadecuadas, innovadoras o no suficientemente maduras en las actividades de tratamiento sean un factor que incremente el riesgo para los derechos y libertades de los interesados.

Esta cada vez mayor protección jurídica de los datos relativos a la salud de las personas choca con una asistencia sanitaria cada vez más conectada a distintos dispositivos tecnológicos. Esto supone la introducción de problemas relacionados con la seguridad cibernética. Estos problemas van desde malware que compromete la integridad de los sistemas y la privacidad de los pacientes hasta ataques de denegación de servicio distribuido (DDoS) que interrumpen la capacidad de las instalaciones para brindar atención al paciente. Los ataques cibernéticos pueden, además de consecuencias financieras una violación de la privacidad datos, constitucionalmente protegidos, relativos a la salud de los pacientes.

En este sentido, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) señala que la seudonimización se está convirtiendo cada vez más en una técnica de seguridad clave para proporcionar un medio que puede facilitar el procesamiento de datos personales, al tiempo que ofrece garantías sólidas para la protección de datos personales de salud y, por lo tanto, protege los derechos y libertades de las personas en relación a la Administración Sanitaria.

II. El tratamiento masivo de datos personales en el Sector Público

La LOPDGDD y el RGPD contemplan la posibilidad de que la introducción de tecnologías inadecuadas, en las actividades de tratamiento sean un factor que incremente el riesgo para los derechos y libertades de los interesados. Este riesgo debe ser evaluado por las AAPP[1].

La evaluación, gestión y minimización del riesgo para los derechos y libertades es una obligación del responsable del tratamiento (artículos 23.2.g, 24.1, 25, 32, 33, 34, 35 y 36 entre otros); no obstante, la norma no determina cómo realizar la gestión del riesgo de cada tratamiento de forma específica. Cualquier tratamiento en el seno de las AA.PP. conlleva una serie de riesgos que se han de gestionar como en cualquier otro proceso que se desarrolle dentro de una organización. Pero los riesgos no se analizan por separado, sino que se han de analizar de forma integral para alcanzar una decisión en el marco de un planteamiento global que tome en consideración todo el contexto del tratamiento[2]. En concreto, ese análisis integral es fundamental en la gestión de los riesgos para los derechos y libertades de las personas. Pero a diferencia de otros sectores, en el sector sanitario y de la salud, la evaluación requiere un plus. Es decir, que la evaluación no está solo en relación con el riesgo de cumplimiento de los principios de tratamiento, derechos y obligaciones establecidos en el RGPD, sino que incluso cumpliendo formalmente con lo establecido en la normativa de protección de datos, el contexto y el alcance en el que se realiza el tratamiento pueda introducir cierto grado de incertidumbre sobre su necesidad y proporcionalidad, así como de la eficacia y efectividad de las garantías jurídicas y técnicas informáticas aplicadas.

Hay que tener en cuenta que el tratamiento de datos personales en la Administración Pública, en general, y en la Sanitaria, en particular, implican riesgos distintos frente a los riesgos de un tratamiento que pueda realizar cualquier otro sector y que se derivan, al menos, de su especial protección jurídica. En consecuencia, las AA.PP., en tanto que son responsables del tratamiento de los datos de los ciudadanos, antes de poner en marcha nuevas actividades de tratamiento o modificar servicios ya prestados que hagan uso de nuevas tecnologías, deberán identificar aquellos riesgos a los que pueda estar expuesto el tratamiento. También deberán adoptar las medidas técnicas y organizativas necesarias que permitan eliminar, los daños que, para los derechos y libertades de las personas, pudieran derivarse del tratamiento. Ha de tenerse en cuenta que los ciudadanos que se podrían encontrar en una situación de riesgo no son solo los administrados, sino también los propios empleados públicos en el ejercicio de sus funciones.

Una de las tecnologías más extensamente utilizadas o que tienen más potencial de implantación en la actualidad en las AAPP es el tratamiento masivo de datos (BIG DATA). Nos referimos a grandes conjuntos de datos, caracterizados por su volumen, variedad, velocidad y/o variabilidad, que requieren de una tecnología escalable para un almacenamiento, manipulación, gestión y análisis eficiente[3]. Las tecnologías de tratamiento masivo se han desarrollado de forma espectacular en los últimos años abriendo un amplio abanico de tratamientos. Internet ha puesto a disposición de toda una gran cantidad de datos que pueden ser utilizados. Las propias AA.PP. promocionan la apertura y reutilización de la información pública y el desarrollo de servicios avanzados basados en datos[4].

1. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
2. Norma ISO 31000:2018: Marco de trabajo para la gestión del riesgo.
3. ISO/IEC 20546:2019 Tecnología de la información – Big Data – Resumen y vocabulario.
4. La Iniciativa Aporta se desarrolla en el contexto del marco legislativo vigente y se articula la plataforma datos.gob.es como punto de encuentro entre las Administraciones, las empresas y los ciudadanos que forman parte del ecosistema de los datos abiertos en España.

El análisis masivo de datos ha permitido obtener informaciones en tiempo real, o casi real, a partir de fuentes de información y conjuntos de datos repartidos por todo el mundo. Existen plataformas software específicas para extraer, cargar y transformar (se emplean las siglas ELT o *Extract, Load and Transform* frente al acrónimo ETL de los cuadros de mando) de distintos orígenes y explotar esa información.

Todo ello choca con la protección jurídica de los datos personales de los ciudadanos[5]. Por tanto, en el diseño de los tratamientos de *Big Data* hay que tener en cuenta de forma objetiva qué cantidad de datos es necesaria y suficiente con relación al objetivo del tratamiento, ajustarse al principio de minimización de datos y no adoptar estrategias maximalistas en las que, sin haber establecido criterios de selección previos, se recurre a recoger la máxima cantidad posible de datos[6]. Este problema se puede ver acentuado en el caso de recopilación masiva de datos soportada por sensores en contextos de tratamiento como los realizados en las *Smart Cities*. Esta tecnología permite el perfilado o el enriquecimiento de perfiles de personas, tratamiento que precisa de una legitimación y debe cumplir unos requisitos y condiciones[7], entre ellas las relativas a las decisiones individuales automatizadas, y en su caso, la realización de una evaluación de impacto para la protección de datos y si procede, la consulta previa a la Autoridad de Control[8].

II.1 Limites y control del tratamiento masivo de datos personales

Las AAPP liberan muchos datos en formatos sencillos dentro de las iniciativas de datos abiertos[9]. Estas iniciativas consideran la apertura de datos como una forma de transparencia y pretenden hacer accesibles y reutilizables los datos referentes a población, transporte, entorno, salud, energía, territorio, educación, etc., que las AA.PP. tienen almacenados en sus sistemas. El propósito es facilitar información a los ciudadanos en un ejercicio de transparencia que ayude a generar mayor confianza en el organismo, y también al sector empresarial para que integre estos datos en sus sistemas y los aproveche en sus propios procesos, contribuyendo así al fomento de la economía y la innovación[10].

En este sentido, las Administraciones con capacidad para analizar esos grandes conjuntos de datos han desarrollado equipos y están cruzando diferentes fuentes de información para extraer conocimiento y aplicar el análisis masivo de datos en diferentes sectores y escenarios como el sanitario, el turístico, la investigación, el desarrollo sostenible, la seguridad o la lucha contra el fraude. Sin embargo, no debe perderse de vista que este análisis masivo puede tener consecuencias negativas desde el punto de vista ético, de la privacidad y, en particular jurídico, en la protección de datos, si se hace un mal uso de la información obtenida.

Ya hemos avanzado que en todo tratamiento, se ha de cumplir el principio de licitud, lealtad y limitación del tratamiento[11]. En el caso de los tratamientos basados en *Big Data*, por su propia naturaleza, parece fácil que se den situaciones en las que la finalidad inicial del tratamiento se vea desvirtuada cuando el dato es explotado con finalidades secundarias. La normativa de protección de datos no impide que los datos personales puedan reutilizarse para finalidades diferentes para las que fueron recogidos, si no que éstas no deben ser incompatibles con las iniciales. Por lo tanto, para su reutilización en nuevos proyectos, resulta clave realizar un análisis de los límites y control de compatibilidad. A tal fin, se debe tenerse en cuenta las siguientes consideraciones recogidas en el artículo 6.4 y el Considerando 50 del RGPD:

- Relación entre la finalidad inicial del tratamiento y otras finalidades posteriores.
- Los tratamientos posteriores se encuentren dentro de las expectativas razonables de los interesados.

5. Artículo 6 del RGPD – Licitud del tratamiento y Artículo 9 del RGPD – Tratamiento de categorías especiales de datos personales. En este sentido, hay que asegurarse que existe una legitimación y, en el caso de que se incluyan categorías especiales de datos, es necesario levantar previamente la prohibición para su tratamiento.

6. Artículo 5.1.c) del RGPD – Principios relativos al tratamiento. Principio de minimización.

7. Artículo 22 del RGPD - Decisiones individuales automatizadas, incluida la elaboración de perfiles.

8. Artículo 35 del RGPD – Evaluación de impacto relativa a la protección de datos y Artículo 36 del RGPD – Consulta previa.

9. Iniciativa de Datos Abiertos del Gobierno de España https://datos.gob.es/

10. En Europa partimos de la Directiva 2003/98/CE, de 17 de noviembre de 2003, actualizada por la Directiva 2013/37/UE del Parlamento Europeo y del Consejo, de 26 de junio. En España han dado lugar a la Ley 37/2007, de 16 de noviembre, de reutilización de la información del sector público, actualizada por la Ley 18/2015, de 9 de julio.

11. Artículo 5.1.a) del RGPD - Principios relativos al tratamiento. Principio de licitud, lealtad y transparencia y Artículo 5.1.b) del RGPD - Principios relativos al tratamiento. Principio de limitación de la finalidad.

- La naturaleza y sensibilidad de los datos objeto de tratamiento.
- El impacto que el tratamiento posterior puede tener sobre los interesados.
- Que se hayan adoptado medidas de protección, técnicas y organizativas adecuadas.

Es importante tener en cuenta que no todas las bases legitimadoras se pueden invocar para el caso de tratamientos realizados por las AA.PP., en particular, las limitaciones establecidas para invocar el interés legítimo.

A) La protección de los derechos y libertades asociados al Big Data

El RGPD requiere que se adopten precauciones especiales ya que, desde el punto de vista de la protección de datos personales, el procesamiento de grandes volúmenes de información puede encerrar riesgos que es necesario gestionar. El tratamiento masivo de datos de carácter personal es uno de los supuestos para los que los art. 35 y 36 del RGPD exige una evaluación del riesgo más sistemática, requiriendo la realización de una evaluación de impacto relativa a la protección de datos y, en su caso, en función del resultado obtenido de una consulta previa a la Autoridad de Control.

Toda Administración al abordar el desarrollo de una solución basada en Big Data debe realizar una evaluación previa de impacto o EIPD. Debería tener en cuenta una serie de consideraciones para minimizar los riesgos que el tratamiento puede suponer para los derechos y libertades de las personas, adoptando una serie de cautelas y garantías en el diseño de las diferentes operaciones que forman parte del tratamiento[12]:

- Fase de adquisición de datos: selección previa de los datos que se requiere recoger y minimizar el grado de detalle con que se tratan recurriendo a la anonimización o seudonimización de las fuentes de origen, el enmascaramiento de los datos o el cifrado de la información.
- Fase de análisis y validación: debe minimizarse, en la medida de lo posible, el detalle de los datos mediante técnicas de anonimización y cifrado.

12. Tecnologías y protección de datos en las APP. AGEPD, 2020.

- Fase de disociación, anonimización o seudonimización de la información: preferiblemente las personas que lleven a cabo esta actividad no deberán ser las mismas que participen en la fase de explotación de la información Esta recomendación se convierte en obligación del responsable cuando se trate de datos de salud como se señala en la disposición adicional decimoséptima de la LOPDGDD, sin perjuicio del resto de obligaciones que se indican en dicha disposición adicional y en particular a la garantía de la trazabilidad de la información en el marco de las garantías prevista en el RGPD. Es preciso señalar que el propio proceso de disociación, anonimización o seudonimización es en sí mismo un tratamiento de datos personales y, por tanto, le es de aplicación las garantías previstas en la normativa de aplicación de datos personales.
- Fase de almacenamiento: debe garantizarse la confidencialidad de los datos y que estos no son accedidos por terceros no autorizados, recurriendo para ello a técnicas de cifrado y mecanismos autenticación y de control de acceso. También es importante, a fin de evitar posibles inferencias derivadas de un cruce no autorizado de distintas fuentes de información, recurrir a estrategias de distribución de datos que dificulten realizar vinculaciones entre los datos.
- Fase de explotación: cuando se vaya a hacer uso de los datos debe garantizarse su anonimización, recurriendo a las diferentes técnicas y, en su caso, a garantías jurídicas dirigidas a evitar la reidentificación, si es que no se ha hecho un uso previo de estas y los datos en esta fase aún siguen permitiendo la identificación de los interesados.

El proceso de agregación para obtener conocimiento implica combinar datos, muchas veces de diferentes fuentes de información, con los riesgos para la privacidad de los interesados que ello representa:

- Reidentificación de los individuos o singularización, aumentando la probabilidad de que esta se produzca cuanto mayor sea el volumen de datos procesados, incluso en aquellos conjuntos de datos que aparente-mente pueden no contener identificadores primarios o explícitos[13].
- Vinculabilidad de diferentes registros de un mismo interesado o grupo de interesados, ya sea en el mismo conjunto de datos o a través de la conexión de fuentes de datos heterogéneas e independientes, mediante análisis de correlación.
- Inferencia, a partir de datos personales calificados como cuasi-identificadores, de información personal mucho más crítica y que no estaba previsto ser procesada[14].

Si se trata de datos de categorías especiales, como los datos médicos de salud, nos encontramos ante una situación de mayor riesgo por el mayor impacto que representa sobre los derechos y libertades de las personas, por lo que las garantías a adoptar han de ser superiores. Estos riesgos para la privacidad deben de ser evaluados desde la misma concepción del tratamiento que haga uso de técnicas Big Data y de sus herramientas analíticas de explotación de información, incorporando, desde el diseño, las estrategias necesarias para mitigarlos y que habrán sido identificadas como resultado de la evaluación de impacto para la protección de datos llevada a cabo.

B) La protección de la cesión de datos anonimizados

El análisis de riesgo es importante en el uso interno de los datos por parte de las propias AA.PP. De igual manera lo es el que se ha de realizar antes de la cesión de datos anonimizados por parte de las AA.PP. a terceros. En caso del que el riesgo de reidentificación sea elevado, dicho tratamiento quedaría sujeto a la normativa de protección de datos y tendría que estar legitimado. Para el caso de los riesgos relacionados con la reidentificación de los interesados y la inferencia de información resultan útiles las siguientes aproximaciones[16]:

- Minimización de datos: el procesamiento de los datos se debe limitar al máximo posible y a lo necesario para alcanzar la finalidad del tratamiento, tanto desde el punto de vista del volumen de población (número de registros) como de datos analizados (atributos procesados).
- Maximización del nivel de agregación: se debe evitar en la medida de lo posible reidentificar a los individuos o inferir información sobre ellos dentro del dataset o conjunto de datos, para lo cual se precisa minimizar el detalle de la información tratada.

13. Los identificadores primarios o explícitos son aquellos que identifican unívocamente a un individuo, como su número de identificación fiscal, su número de la seguridad social o su número de teléfono móvil.

14. Los cuasi-identificadores son atributos que no identifican directamente a una persona (fecha de nacimiento, código postal, género, profesión, ...) pero que pueden permitir su reidentificación se si combinan o cruzan con otros conjuntos de datos que compartan esos mismos cuasi-identificadores.

15. Tecnologías y protección de datos en las APP. AGEPD, 2020.

- Abstracción de la información: se deben proteger los datos personales y ocultar sus relaciones.
- Distribución de los datos: deben distribuirse los datos. y procesarse en entornos separados, con el objetivo de dificultar la inferencia de información por el cruce de datos.

Para poner en marcha estas estrategias puede recurrirse a diferentes técnicas entre las que destacan las técnicas de anonimización en el caso de las estrategias de minimización y agregación, y el cifrado de la información para las estrategias de abstracción y distribución de datos. Estas estrategias deben complementarse con otras medidas dirigidas a garantizar la transparencia, el control de los usuarios sobre sus datos a través de los mecanismos adecuados para ejercer sus derechos y la aplicación del principio de responsabilidad proactiva por parte del responsable mediante la monitorización, la auditoría y la trazabilidad de las decisiones tomadas y las acciones realizadas.

III. Marco jurídico del tratamiento masivo de los datos de salud

Es preciso dejar claro que entendemos por datos de salud al objeto de este trabajo. Es el conjunto de documentos que contienen los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo de su proceso asistencial. La nueva normativa europea de protección de datos (RGPD), considera la información sanitaria de las personas como especialmente protegida[16]. De este modo, los usuarios tienen nuevos derechos cuando acuden a centros médicos u hospitales. Nos vamos a centra en esta norma para obtener los principios básicos relativos a la protección de datos de salud.

En primer lugar, el RGPD los define de la siguiente manera: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud. Por lo tanto cualquier información relativa, a título de ejemplo: a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el **historial médico del paciente**, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo, un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro.

Por lo trascendental que puede tener este tipo de datos para la privacidad del interesado, el RGPD, da a este tipo de datos el adjetivo de **Especialmente Protegidos**, lo cual hace que se deban cumplir una serie de condiciones adicionales para su tratamiento conforme a la normativa.

En segundo lugar, estos principios fundamentales para la protección de datos médicos son los siguientes:

a) Confidencialidad de los datos médicos: el secreto profesional es de obligatorio cumplimiento por el personal que tenga acceso a los datos del paciente. Incluso cuando la relación que vincule a las partes haya finalizado. La **ley de confidencialidad del paciente** obliga a los centros médicos a adoptar las medidas necesarias para garantizar la **confidencialidad de los datos relativos a la salud** y el procedimiento legal de acceso.

b) Calidad de los datos: se permite recoger **datos personales de un paciente**, siempre que sean adecuados, veraces y pertinentes. La información sanitaria no puede recopilarse de forma desleal, fraudulenta o ilícita. La recogida y el tratamiento de datos de salud persiguen una finalidad principal muy clara plasmada en la propia finalidad de la historia clínica: garantizar una asistencia adecuada al paciente.

   La información trascendental para la asistencia sanitaria ha de contar, como mínimo, con los siguientes datos:

   - Documentación referida a la hoja clínico-estadística.
   - Autorización de ingreso.
   - Informe de urgencia.
   - Exploración física.
   - Evolución.
   - Órdenes médicas.
   - Hoja de interconsulta.
   - Informes de exploración complementaria.
   - Consentimiento informado.
   - Informe de anestesia.
   - Informe de quirófano o de registro del parto.

16. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Día General. (2016).

- Dosier de anatomía patológica.
- Evolución y planificación de cuidados de enfermería.
- Aplicación terapéutica de enfermería.

c) Consentimiento por parte del paciente

La principal base legal para el tratamiento de los **datos médicos de una persona** la encontramos en el artículo 9 del RGPD y es el **consentimiento**. Según la nueva normativa europea, este deberá ser: explícito y recogido por escrito. Por tanto, está totalmente prohibido el **uso de datos personales sin consentimiento.**

d). Dar cumplida información al paciente sobre el tratamiento de su información sanitaria

La **ley de protección de datos en el ámbito sanitario** contempla el **deber de información** a los pacientes: Existencia de estos ficheros, Finalidad del mismo, Posibles destinatarios de la información, Identidad y dirección del responsable del mantenimiento del mismo y Posibilidad del ejercicio de sus derechos

Es **obligatorio** en cada centro sanitario la existencia de una **hoja de información al paciente** en la que le solicita su autorización **para el tratamiento de sus datos.** En ella se recoge, entre otros datos:

- Nombre del profesional y del centro donde ha sido atendido el paciente.
- Propósitos de la petición.
- Expresa conformidad de publicación del caso clínico en publicaciones científicas dirigidas a profesionales de la salud.
- Nombre del paciente.
- Documento de identidad o pasaporte y su firma autorizando expresamente que se utilicen los datos de su historia clínica en las condiciones que se describen en el informe.

III.1 Nuevas medidas de seguridad en relación al ámbito sanitario

Las nuevas medidas del RGPD en relación al ámbito sanitario en relación a la seguridad y garantía de los datos protegidos de salud las podemos agrupar en las siguientes:

a) Medidas organizativas y de seguridad: la nueva normativa ya no establece las medidas de seguridad por niveles, sino que prevé que se apliquen medidas en función del riesgo que puedan ocurrir en el tratamiento de los datos. En el caso del tratamiento de datos de salud el nivel del riesgo es enorme, por lo que habrá que diseñar unas medidas organizativas y de seguridad conforme a dicho riesgo.

b) Evaluación de Impacto: La **evaluación de impacto** es un análisis del riesgo cuyo objetivo es permitir a los responsables del tratamiento tomar medidas adecuadas para reducir dichos riesgos (minimizar la probabilidad de su materialización y las consecuencias negativas para los interesados).

c) Registro de las actividades de tratamiento: Los responsables y los encargados están obligados siempre en los casos de tratamientos de datos de salud, genéticos o biométricos con independencia de emplear o no a más o menos de 250 personas, a mantener un registro de las actividades de tratamiento que realicen. Este registro debe de contener al menos los siguientes datos: identificación y datos de contacto de responsable, corresponsable, representante y delegado de protección de datos, fines del tratamiento; descripción de categorías de interesados y datos; categorías de destinatarios existentes o previstos (inclusive en terceros países u organizaciones internacionales); transferencias internacionales de datos y documentación de garantías para transferencias de datos internacionales exceptuadas sobre base de intereses legítimos imperiosos.

d) Nombrar un Delegado de Protección de Datos: Se debe contar con un Delegado de protección de Datos, ya que así lo exige la nueva normativa comunitaria. Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes tendrán que tener nombrado un **Delegado de Protección de datos** y comunicar dicho nombramiento a la AEPD.

e) Comunicación de los datos. Es habitual que los datos se comuniquen entre entidades para el mejor tratamiento del paciente. En estos casos, el interesado debe tener constancia de ello, ya que será él quien permita esta transmisión. El responsable del fichero deberá cumplir determinados requisitos: definir en un contrato escrito la regulación del tratamiento de datos por cuenta de un tercero; establecer que ese tercero (únicamente tratará los datos conforme a sus instrucciones; comprobar que los datos no serán utilizados con fines distintos a los determinados en el contrato, ni serán comunicados a otras personas; el tercero deberá cumplir con las mismas medidas de seguridad que las que cumpla el responsable del fichero (la única excepción a este consentimiento se establece en el caso de que la comunicación de los datos tenga por objeto la prevención, el diagnóstico y la asistencia sanitaria de los afectados a los que se refieren); Mutuas y compañías de seguro (excepcionalmente los datos médicos pueden comunicarse de acuerdo al principio de calidad y únicamente para llevar a cabo la elaboración de la factura del gasto sanitario).

f) Facilitar los derechos ARCO: Los pacientes podrán ejercer libremente sus derechos ARCO de acceso, rectificación, cancelación y oposición de su historia clínica. Para ello, el responsable deberá colaborar con ellos, facilitarles un informe o, en su defecto, una copia del mismo.

Como conclusión señalamos que las **regulaciones actuales como el Reglamento General de Protección de Datos (RGPD)** han supuesto un antes y un después en los mecanismos para la seguridad y denuncia de los delitos cibernéticos. La RGPD es fundamental en la protección de datos. Como otras normativas HIPPA en Estados Unidos han ayudado a elevar el nivel de seguridad de los datos médicos.

III.2 La ciberseguridad para proteger los datos de salud hospitalarios

La seguridad a la hora de compartir los datos de salud, en los que se facilita información privada de los pacientes ha de contar con las **garantías tecnológicas apara eradas a los derechos reconocidos a los pacientes y usuarios del sistema nacional de salud.**

Recordamos que la obligación legal del RGPD afecta a las instituciones sanitarias pública y privadas en el tratamiento de los datos personales. Además, los datos relativos a la salud son considerados como datos sensibles especialmente protegidos, y como una categoría especial de datos personales. Por tanto, el **sector sanitario tiene el enorme reto de protegerse ante los ciberataques a nivel mundial.**

La asistencia sanitaria está cada vez más conectada. La proliferación de soluciones de tecnología médica ha cambiado por completo el panorama de las TIC en las organizaciones sanitarias de todo el mundo. La creciente interconexión de dispositivos médicos y el uso de conexiones remotas para su mantenimiento; la necesidad de monitorear continuamente a los pacientes, incluso los que están fuera del hospital; el uso de teléfonos inteligentes para acceder a información de salud por parte de pacientes y médicos; y la falta de presupuesto para servicios y soluciones de ciberseguridad hace que el sector sanitario sea especialmente vulnerable.

La protección de los datos de salud está plagada de una gran cantidad de problemas relacionados con la seguridad cibernética. Estos problemas van desde malware que compromete la integridad de los sistemas y la privacidad de los pacientes hasta ataques de denegación de servicio distribuido (DDoS) que interrumpen la capacidad de las instalaciones para brindar atención al paciente. Es muy importante que en tu hospital o centro médico analices todas las vulnerabilidades existentes para evitar ser víctima de un ciberataque que cause importantes daños al servicio.

La doctrina ha señalado como principales vulnerabilidades a las que se enfrenta el sector sanitario las siguientes:

a) Dispositivos heredados o anticuados que ejecutan software o sistemas operativos obsoletos. Las preocupaciones sobre el presupuesto, los recursos y las operaciones a menudo pueden impedir la práctica de reemplazar software y dispositivos antes de que lleguen al final de su vida útil, dejándolos más susceptibles a un ataque.

b) Las vías más fáciles para los atacantes se encuentran en la gestión integrada del edificio, la seguridad física y los dispositivos clínicos. Estos dispositivos a menudo están fuera del control de TI, o se pasan por alto, y pueden permanecer sin parches durante años, proporcionando un punto de entrada potencial para actores hostiles.

c) Las redes de atención médica a menudo están diseñadas para minimizar los costes y maximizar la eficiencia, creando redes planas que son objetivos fáciles para los atacantes. Todo lo demás queda en segundo plano, a menudo incluyendo la ciberseguridad.

d) Las organizaciones sanitarias están centradas en su misión principal: salvar vidas y ayudar a los pacientes, y los riesgos de ciberseguridad no están siempre contemplados. Todo lo demás queda en segundo plano. Hay muy poca tolerancia para la instalación de parches que pueden causar conflictos con el software patentado de dispositivos médicos.

e) Algunas organizaciones sanitarias aprovechan proveedores externos para administrar y ejecutar sus sistemas, lo que puede introducir una cantidad significativa de riesgo. En lugar de atacar directamente a organizaciones grandes y bien financiadas con capacidades cibernéticas avanzadas, los actores hostiles a menudo intentan comprometer a un proveedor externo más pequeño que tiene acceso a la organización objetivo, evitando de manera efectiva todos los controles de seguridad de la entidad más grande y proporcionando acceso directo a sus redes.

f) La excesiva descentralización de algunos centros sanitarios puede hacer que sea mucho más difícil priorizar las inversiones en seguridad cibernética,

A. Protección hardware

En primer lugar, hay que tener en cuenta que los dispositivos móviles (portátiles, tabletas, teléfonos inteligentes, medios de almacenamiento portátiles) pueden presentan amenazas a la privacidad y seguridad de la información por: movilidad (estos dispositivos son fáciles de perder y vulnerables al robo), falta de control (no todos los dispositivos móviles están equipados con fuertes controles de autenticación y acceso) y a menudo se utilizan para transmitir y recibir datos de forma inalámbrica. Estas comunicaciones inalámbricas deben estar protegidas contra escuchas e intercepción.

En segundo lugar, para minimizar el riesgo para la información electrónica de salud al configurar de manera efectiva los dispositivos, son importantes los controles de acceso. La contraseña, sin embargo, es solo la mitad de lo que constituye las credenciales de un usuario de ordenador. La otra mitad es la identidad del usuario o nombre de usuario. Estas credenciales (nombre de usuario y contraseña) se utilizan como parte de un sistema de control de acceso en el que los usuarios tienen determinados derechos para acceder a los datos dentro. De ahí que la configuración de los dispositivos para conceder acceso electrónico a la información de salud solo se a las personas autorizadas.

En tercer lugar, debido a la sensibilidad de la información de atención médica y al hecho de que debe estar especialmente protegida, se deben utilizar herramientas que permitan a personas externas obtener acceso a la red de consultorios de atención médica con extrema precaución. La información de salud electrónica que fluye por la red inalámbrica debe estar protegida, es crucial asegurar la señal inalámbrica para que solo aquellos a quienes se les permite acceder a la información pueden captar la señal. Los enrutadores inalámbricos deben ser configurados para operar solo en modo encriptado. Y también es importante usar una VPN para proteger la conexión.

B. Protección del software

La mayoría del software requiere actualizaciones periódicas para mantenerlo seguro y agregar funciones. Mantener el software actualizado es fundamental para mantener un sistema seguro, ya que muchas de estas actualizaciones corrigen vulnerabilidades encontradas en el producto. A modo de ejemplo: se debe tener en cuenta que las cuentas de usuario de los ex empleados están deshabilitadas de manera adecuada y oportuna; que los ordenadores y cualquier otro dispositivo, como discos duros, que tengan datos almacenados en ellos deben «limpiarse» antes de tirarlos; los archivos de datos antiguos se archivan para almacenamiento si es necesario, o se limpian del sistema si no son necesarios. El software que ya no se necesita debe desinstalarse completamente.

Algunas medidas tradicionales de protección eficaces contra los ataques son: instalar un firewall y antivirus para proteger contra intrusiones y amenazas de fuentes externas. Mientras el antivirus ayudará a encontrar y destruir el software malicioso

que ya ha entrado, el trabajo de un firewall es evitar que los intrusos entren. En resumen, el antivirus puede considerarse como un control de infecciones mientras que el firewall tiene el papel de prevención de enfermedades.

Un firewall puede tomar la forma de un producto de software o un dispositivo de hardware. En cualquier caso, su trabajo es inspeccionar todos los mensajes que ingresan al sistema desde el exterior y decidir, de acuerdo con criterios predeterminados, si el mensaje debe ser permitido o no.

III.3 Protección de datos de salud

La protección de la información debe ser una prioridad para cualquier persona que trabaje en la atención médica. Las organizaciones sanitarias que tienen las medidas de seguridad adecuadas en torno a la información personal limitarán el riesgo de sufrir una violación. Si ocurriera una violación, estará mejor preparada para responder a la misma. La protección de los datos es una parte esencial para prevenir o mitigar una violación de la atención médica. Para ello, es necesario es saber dónde se almacenan los datos confidenciales, cómo se transmiten y cómo se usan. La identificación de estos testamentos le permite a una organización determinar qué protecciones deben implementarse para cada dispositivo, lo que permite implementar medidas de seguridad más exhaustivas.

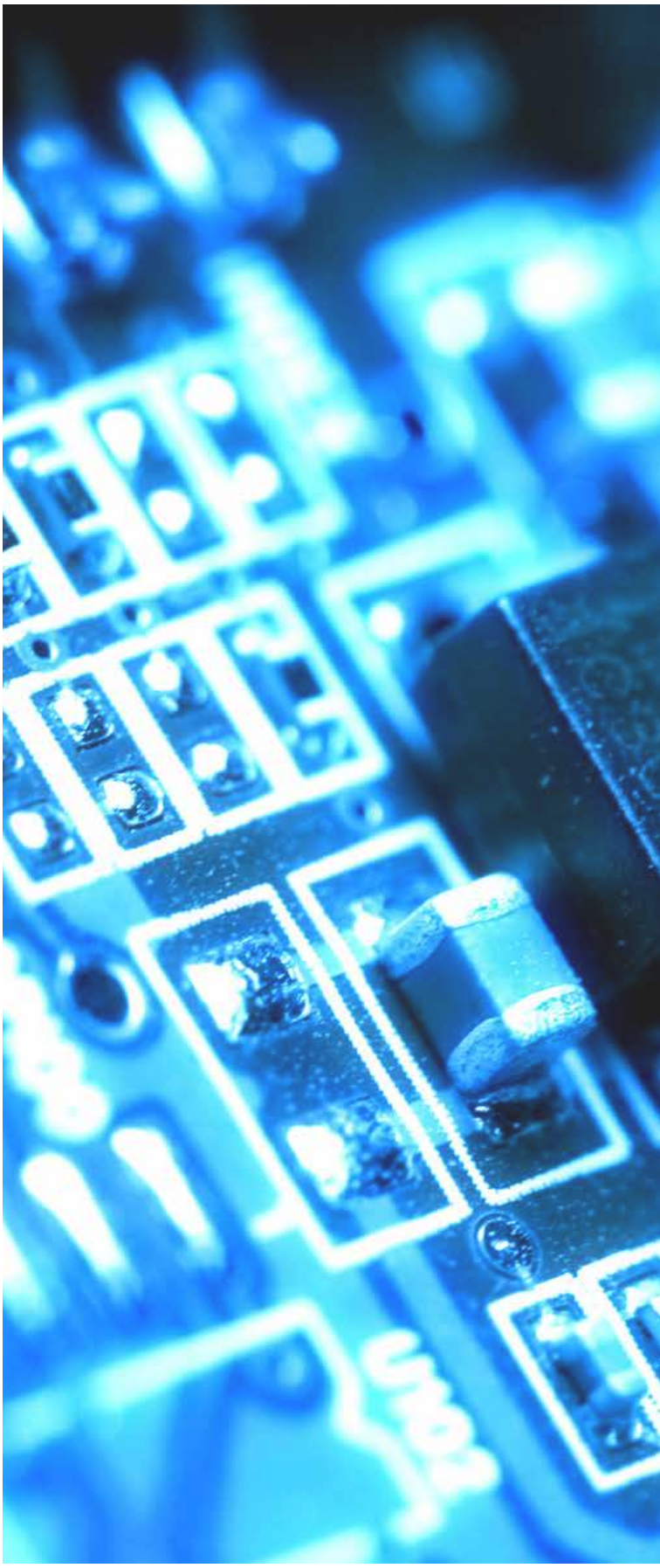
Además, los centros sanitarios deben tener en cuenta algunas actuaciones como las siguientes actuaciones.

a) Evaluación de riesgos en seguridad. Nos referimos a la evaluación de Impacto que recoge el **RGPD**: La **evaluación de impacto** es un análisis del riesgo cuyo objetivo es permitir a los responsables del tratamiento tomar medidas adecuadas para reducir dichos riesgos (minimizar la probabilidad de su materialización y las consecuencias negativas para los interesados).

b) Cifrado. Cifrar los datos sirve también para reducir el riesgo de violaciones de datos en la atención médica. Los datos cifrados no se pueden ver sin una clave de descifrado, por lo que es lo más efectivo para su protección.

c) Formación. capacitar a los empleados en las políticas y procedimientos de la organización, así como en los requisitos de seguridad. La mayoría de las infracciones de salud ocurren como resultado de un error humano. Los empleados deben estar capacitados sobre lo que constituye la información personal y cómo manejarla adecuadamente.

d) Evaluar a proveedores.



Las entidades sanitarias tienen que asegurar la obligación de garantizar que los proveedores con los que están trabajando tengan las medidas adecuadas para la protección de la información personal. Si el vendedor carece de medidas de seguridad, debe implementar salvaguardas adecuadas antes de que se les permita recibir esos datos personales.

También deben firmarse acuerdos de socios comerciales con todos los proveedores antes de compartir información personal. Estos acuerdos limitan la responsabilidad de ambas partes en caso de incumplimiento, ya que afirman que cada parte ha aceptado cumplir con sus obligaciones para proteger esa información y que son responsables de su propio cumplimiento.

En definitiva, las instituciones sanitarias son las que han de diseñar las plataformas para garantizar la protección de los datos personales de los pacientes estableciendo sus **planes de ciberseguridad** en los que aplican tecnologías para tener sistemas menos vulnerables. Ello va a suponer la correcta actualización del software y hardware y se realizar acciones de concienciación sobre el uso responsable de los sistemas. En este sentido, las aplicaciones y plataformas pasan por **técnicas de anonimización** o **seudonimización** para evitar la identificación de los pacientes que las organizaciones sanitarias utilizan en sus proyectos de BIG data e inteligencia artificial para investigación.

IV. Técnicas de protección de datos de salud y seguridad cibernética

Los datos de salud siempre han sido una valiosa fuente de conocimiento en el cuidado de la salud. el cuidado de la salud históricamente ha generado grandes cantidades de datos, tanto para el tratamiento de pacientes como para para la investigación y el análisis posterior. Se ha producido una abundancia de nuevas fuentes de datos de salud como resultado del uso generalizado de registros de salud electrónicos, aplicaciones de salud y dispositivos portátiles. Además, los avances en el poder informático han permitido el desarrollo de nuevos datos técnicas de análisis y aprendizaje automático que mejoran el diagnóstico, el tratamiento y administración en salud. El resultado es un cambio en los supuestos que está alejando cada vez más al paciente de hospitalización hacia un sistema de salud distribuido proporcionado por una combinación de servicios públicos y privados. La integración de nuevas tecnologías en salud abre nuevos problemas con respecto a los datos protección y la seguridad cibernética.

Sin embargo, el aumento del procesamiento de datos médicos digitalizados también ha aumentado los riesgos, en términos de la ciberseguridad, la protección de datos y la probabilidad de violaciones de datos. Instrumentos legales pertinentes de la UE, como la Directiva NIS, el Reglamento General de Protección de Datos, el Reglamento de Dispositivos Médicos, la Directiva sobre la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza, etc. impuso obligaciones a proveedores de atención médica y fabricantes de dispositivos médicos para garantizar una adecuada y uniforme nivel de protección de los datos médicos y los productos y servicios que los utilizan. Además, el RGPD distingue, en el art. 9, datos relativos a la salud como categoría especial de datos (sensibles) y conjuntos establecer requisitos adicionales y obligaciones más estrictas para el procesamiento y protección de dichos datos, en para salvaguardar los derechos y libertades de las personas (interesados).

IV.1 La seudonimización en el sector sanitario

La seudonimización se está convirtiendo cada vez más en una técnica clave de seguridad de protección de datos y, además, garantiza el resguardo de dichos datos personales, salvaguardando de esa manera los derechos y libertades de las personas relativas a los datos de salud. El RGPD define la seudonimización en el art. 4 como el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

En este sentido se manifiesta la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) en uno de sus últimos documentos publicados[17]. Este hecho es cada vez más frecuente sobre todo en el sector sanitario, ya que "este intenta aprovechar al máximo la evolución de la tecnología y adecuar la prestación de sus servicios para atender de manera oportuna las crecientes necesidades de los pacientes". Por ello, en el sector sanitario, "entran en juego los desafíos de ciberseguridad y la protección de los datos personales».

Así, la Agencia ha detallado en el documento citado tres nuevas técnicas sustanciales para mejorar la protección de dichos datos personales en el ámbito sanitario y son las siguientes:

a) Seudonimización determinista: usar siempre el mismo seudónimo para el mismo dato.

b) Documento de seudonimización aleatoria: utilizando el mismo seudónimo para el mismo dato solo dentro de un alcance consistente.

c) Seudonimización completamente aleatoria: siempre usando un seudónimo diferente para el mismo dato.

Estas nuevas técnicas son sustanciales en cuanto a su implementación, ya que también es de suma importancia elegir la política con la que se aplicarán dichas técnicas, según el documento. En cuanto a las consideraciones de seudonimización, ENISA asegura que los controladores y procesadores de datos en el ámbito sanitario pueden hacer uso de dichas técnicas ya sea de forma conjunta, usando siempre los mismos criterios, o inconexamente.

Las principales diferencias entre estas técnicas se basan en cómo se genera el seudónimo. Para los más comunes, la Tabla 1 a continuación proporciona un resumen:

IV.2. La seudonimización en el ámbito hospitalario

En términos generales, la seudonimización tiene como objetivo proteger los datos personales ocultando la identidad de individuos (sujetos de datos) en un conjunto de datos, p. reemplazando uno o más identificadores de datos personales con los llamados seudónimos y protegiendo adecuadamente el vínculo entre los seudónimos y las identificadoras iniciales. La seudonimización es una de varias técnicas de "desidentificación" (como la agregación, ofuscación, enmascaramiento, etc.) destinados a eliminar la asociación entre un conjunto de datos de identificación y el principal de datos.

Por tanto, la principal ventaja de la seudonimización, es ocultar la identidad de un individuo en el contexto de un conjunto de datos específico, por lo que no es posible conectar los datos con el individuo especifico. Por lo tanto, también puede reducir el riesgo de la vinculación de datos personales para un individuo específico a través de diferentes dominios de procesamiento de datos.

Tabla 1. Descripción general de las técnicas básicas de seudonimización

Técnica	Generador de seudónimos
Contador	Contador monotónico que comienza en un cierto valor y se incrementa cada vez que se necesita un nuevo seudónimo.
Número aleatorio	Valor aleatorio extraído entre un límite mínimo y máximo cada vez que es necesario un nuevo seudónimo.
Función hash	Función criptográfica unidireccional (no reversible) que transforma los datos personales de entrada en valores de longitud fija.
Código de autenticación de mensajes basado en hash (HMAC)	Función criptográfica unidireccional (no reversible) que agrega una clave que la hace menos predecible que una función hash.
Cifrado	Función criptográfica bidireccional (reversible) que transforma un dato personal de entrada en valores que se pueden volver a transformar en su formato original utilizando una clave.

17. DEPLOYING PSEUDONYMISATION TECHNIQUES The case of the Health Sector. The European Union Agency for Cybersecurity, ENISA MARCH 2022. ISBN 978-92-9204-576-0, DOI 10.2824/092874.

En un intento de demostrar el valor añadido de la seudonimización en el ámbito hospitalario, ENISA presenta tres casos de uso en los que los datos médicos personales que se procesan son un seudónimo. En este sentido, el documento detalla que «si bien no se analizan en profundidad las técnicas específicas de seudonimización, los diferentes casos de uso intentan proporcionar una visión general de las posibilidades y de los aspectos clave de su aplicación". Todo ello con un único objetivo: " Aumentar el nivel de protección de los datos personales mediante la eliminación de identificadores personales directos". Estos tres casos son los siguientes:

- En primer lugar, intercambio de datos de salud del paciente: en la práctica médica actual, el intercambio de datos entre organizaciones es una táctica común y se utiliza principalmente con fines diagnósticos y terapéuticos. Esto incluye los casos de intercambio entre diferentes departamentos dentro de la misma entidad, como un hospital, y entre individuos, como los profesionales médicos o laboratorios.

- En segundo lugar, ensayos clínicos: los ensayos clínicos estudian nuevas intervenciones y tratamientos médicos y evalúan sus efectos directos y los posibles efectos secundarios. Se considera un requisito previo para adquirir la aprobación necesaria de las autoridades pertinentes. Por ello, y en general, no los realiza el fabricante, sino organizaciones independientes denominadas Organizaciones de Investigación Clínica (CROs, por sus siglas en inglés).

- En tercer lugar, monitoreo de datos de salud orientados al paciente: actualmente, los dispositivos portátiles inteligentes pueden controlar los signos vitales, como la frecuencia cardíaca, el nivel de oxígeno o de presión arterial, entre otros. El control regular de dichos signos es una intervención común en el cuidado del paciente que tiene como objetivo facilitar el reconcomiendo temprano de las alteraciones fisiológicas. Sin embargo, solo el propio paciente debería ser quien pueda visualizar las mediaciones y ponerse en contacto con su médico cuando se observe un valor anormal.

Por último, cabe señalar que estos casos de uso sirven para demostrar la aplicación de seudonimización y no intentar cubrir los casos de uso operativos en toda su extensión, es decir, que los procesadores de datos deberían de tener en cuenta todas las operaciones de tratamiento de datos pertinentes. Los diferentes avances en la tecnología y en los tipos de servicios relacionados con la salud pueden afectar en la eficacia y aplicabilidad de la seudonimización que a día de hoy ya se está implantando. Esto, según ENISA, "no solo es relevante para la elección de las técnicas utilizadas, sino también para el diseño general de proceso de seudonimización incluyendo la protección de la información adicional, como es la información que permite asociar los seudónimos con las identificadoras iniciales". ENISA también alerta de los desafíos o limitaciones de implementación que pueden surgir con respecto a cada una de las nuevas técnicas presentadas. Por ello, el organismo europeo anima a que "la comunidad investigadora sigua trabajando en la protección y seguridad de los datos, incluidas las técnicas de seudonimización de última generación y sus posibles implementaciones, con el apoyo de las instituciones de la Unión Europea en términos de orientación política y fondos de investigación".

VI. Consideraciones finales

A medida que el sector de la salud intenta aprovechar al máximo el panorama técnico en evolución y adaptar la prestación de servicios para satisfacer, de manera oportuna, las crecientes necesidades de los pacientes de todas las edades y culturas en todo el mundo, surgen desafíos adicionales en materia de ciberseguridad y protección jurídica de datos de salud.

La seudonimización se está convirtiendo cada vez más en una técnica de seguridad clave al proporcionar un medio que puede facilitar el procesamiento de datos personales masivos, al tiempo que ofrece garantías sólidas para la protección de datos personales y, por lo tanto, salvaguarda de los derechos y libertades de las personas.

ENISA pretende implementar la seudonimización en la práctica para promover aún más la protección de los intercambios de datos de salud coordinados y seguros en la Unión Europea en el contexto jurídicos europeo de la RGPD.

No existe una solución única sobre cómo y cuándo aplicar la seudonimización; de hecho, diferentes soluciones pueden proporcionar resultados igualmente buenos en escenarios específicos, dependiendo de los requisitos en términos de protección, utilidad, escalabilidad, etc.

La seudonimización puede ser una opción "sencilla" de adoptar, pero también puede comprender un proceso muy complejo tanto a nivel técnico como organizativo. Por ello, es muy importante definir los fines y objetivos de la seudonimización en cada caso concreto y cada tratamiento. Con este fin, las buenas prácticas relevantes y los ejemplos de seudonimización en el contexto del RGPD pueden ser de gran valor para los proveedores de atención médica y los desarrolladores de aplicaciones de atención médica.

Los desarrolladores y reguladores a nivel nacional y europeo deben promover el intercambio de buenas prácticas y proporcionar orientación práctica sobre la implementación de la seudonimización en la práctica.

Los avances en tecnología y en los tipos de servicios relacionados con la salud que se ofrecen pueden afectar la eficacia y la aplicabilidad de una solución de seudonimización que ya se está implementando. Esto no solo es relevante para la elección de la técnica en sí, sino también para el diseño general del proceso de seudonimización, incluida, especialmente, la protección de la información adicional (es decir, la información que permite la asociación entre seudónimos e identificadoras iniciales).

Las soluciones de seudonimización presentadas dependen en gran medida del estado de la técnica informática y pueden surgir desafíos o limitaciones de implementación con respecto a cada técnica con el tiempo. No obstante, la comunidad investigadora debe seguir trabajando en la protección de datos y la ingeniería de seguridad, incluidas las técnicas de seudonimización de última generación y sus posibles implementaciones, con el apoyo de las instituciones de la UE en términos de orientación política y financiación de la investigación.

Bibliografía

- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, sobre medidas para un alto nivel común de seguridad de las redes y los sistemas de información en toda la Unión. (2016)
- ENISA: Procurement Guidelines for Cybersecurity in Hospitals (2020). ENISA: Pseudonymisation techniques and best practices. (2019).
- ENISA: Procurement Guidelines for Cybersecurity in Hospitals. (2020).
- ENISA: Cloud Security for Healthcare Services (2021).
- ENISA: Data Pseudonymisation: Advanced Techniques and Use Cases (2021). ENISA: Deploying Pseudony-misation Techniques: the case of the Health Sector. The European Union Agency for Cybersecurity, ENISA March 2022.
- Iniciativa de Datos Abiertos del Gobierno de España https://datos.gob.es/
- ISO/IEC 20546:2019 Tecnología de la información – Big Data – Resumen y vocabulario.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- Norma ISO 31000:2018: Marco de trabajo para la gestión del riesgo.
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Día General. (2016).
- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Día General. (2016).
- Reglamento (UE) 2017/745 del Parlamento Europeo y del Consejo, de 5 de abril de 2017, sobre productos sanitarios, por el que se modifican la Directiva 2001/83/CE, el Reglamento (CE) nº 178/2002 y el Reglamento (CE) nº 1223/2009 y se deroga Directivas del Consejo 90/385/EEC y 93/42/EE. (2017) 9. Directiva 2011/24/UE del Parlamento Europeo y del Consejo, de 9 de marzo de 2011, relativa a la aplicación de los derechos de los pacientes en la asistencia sanitaria transfronteriza. (2011).
- Tecnologías y protección de datos en las APP. AGEPD, 2020.