**EVALUACIÓN DE IMPACTO Y ANÁLISIS DE RIESGOS DE TRATAMIENTO DE DATOS PERSONALES**

**CON FINES DE INVESTIGACIÓN BIOMÉDICA**

|  |  |
| --- | --- |
| **PROYECTO/ESTUDIO (TRATAMIENTO):** | Haga clic o pulse aquí para escribir texto. |
| **VERSIÓN DEL PROTOCOLO:** | Haga clic o pulse aquí para escribir texto. |
| **INVESTIGADOR PRINCIPAL O PRINCIPALES**  **(RESPONSABLE O CORRESPONSABLES):** | Haga clic o pulse aquí para escribir texto. |
| **FECHA:** | Haga clic o pulse aquí para escribir texto. |
| **CORREO ELECTRÓNICO DE CONTACTO:** | Haga clic o pulse aquí para escribir texto. |

**COMO EVIDENCIA DE LA PROTECCIÓN DE DATOS PERSONALES DESDE EL DISEÑO DEL PROYECTO/ESTUDIO, SE INTEGRARÁN A LA DOCUMENTACIÓN DEL MISMO, AL MENOS LOS SIGUIENTES ELEMENTOS:**

1. **REGISTRO DE ACTIVIDAD DE TRATAMIENTO (RAT)**
2. **EVALUACIÓN DE IMPACTO Y ANÁLISIS DE RIESGOS**

**ANTECEDENTES Y BASE LEGAL**

El RGPD[[1]](#footnote-1) establece la obligación que tienen los responsables de los tratamientos de datos de realizar una Evaluación de Impacto en la Protección de Datos con carácter previo a la puesta en funcionamiento de tales tratamientos cuando sea probable que éstos entrañen un alto riesgo para los derechos y libertades de las personas físicas. En el caso específico de los tratamientos de *datos de salud,* se aplica lo indicado en la disposición adicional decimoséptima de la LODPyGDD[[2]](#footnote-2). La cual, en su apartado f) 1º, indica que todo tratamiento con fines de *investigación* en salud pública, y en particular, biomédica, se procederá a realizar una evaluación de impacto, la cual, es el objeto de este documento[[3]](#footnote-3).

El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible, es considerada una infracción grave por el artículo 73 de la LOPDyGDD.

La evaluación de impacto en la privacidad (EIPD) amplía la visión del análisis de riesgos sobre la “seguridad del tratamiento de datos” añadiendo un punto de vista sobre los derechos y libertades de las personas y el punto de vista del cumplimiento. Se encuentra ligada a los principios de protección de datos desde el diseño y la protección de datos por defecto y una de sus conclusiones podría ser la necesidad de una consulta previa a la autoridad de control.

Está regulada en el artículo 35 del RGPD y resulta obligatoria si el tratamiento (naturaleza, alcance, contexto o fines) entraña alto riesgo para derechos y libertades de las personas físicas, antes de proceder al mismo o siempre que se introduzcan cambios significativos en el caso de tratamientos de riesgo existentes.

Una vez llevada a cabo la evaluación inicial, el responsable la someterá a la consideración del DPD.

Los datos personales *relativos a la salud* son definidos por el artículo 9 del RGPD como de “categoría especial”, por lo que su tratamiento solo se puede realizar bajo circunstancias y condiciones específicas. En el caso de su uso con fines de *investigación* científica deben tener observar las garantías y excepciones indicadas en el artículo 89 del RGP.

**GLOSARIO DE TÉRMINOS**

**TRATAMIENTO:** Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción. En este caso, el Proyecto/estudio.

**INTERESADO:** Persona de la que se utilizan datos para la investigación. Sujeto de estudio.

**RESPONSABLE (DEL TRATAMIENTO):** la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento. Es decir, quien define los objetivos y metodología de la investigación[[4]](#footnote-4). La organización o el Investigador Principal, según el caso.

**ENCARGADO (DEL TRATAMIENTO):** la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. Es decir, proveedores que realicen operaciones con o sobre los datos personales, para los fines de la investigación.

**INFORMACIÓN SOBRE LAS ACTIVIDADES RELATIVAS AL TRATAMIENTO**

La información registrada es este documento debe ser totalmente compatible con la incluida en el protocolo del proyecto/estudio de investigación.

|  |  |
| --- | --- |
| **INFORMACIÓN INICIAL SOBRE EL TRATAMIENTO Y SOBRE LA SEGURIDAD DE LOS DATOS** | |
| ¿Dónde está previsto almacenar y procesar los datos personales de investigación?  Seleccione tantas casillas como sea pertinente | En el servidor del centro sanitario. Cumpliendo con el estándar del ENS[[5]](#footnote-5).  En un servidor o CPD (centro de procesamiento de datos) de la entidad de gestión del proyecto/estudio  En un ordenador de sobremesa bajo control y custodia del Investigador Principal. Describa su ubicación.Haga clic o pulse aquí para escribir texto.  En un ordenador portátil bajo control y custodia del Investigador Principal. Describa su ubicación y al responsable del uso del equipo. Haga clic o pulse aquí para escribir texto.  En una unidad de red con acceso exclusivo al equipo investigador. Describa la ubicación de la red y quién la administra.Haga clic o pulse aquí para escribir texto.  En un dispositivo extraíble bajo control y custodia del Investigador Principal. Describa.Haga clic o pulse aquí para escribir texto.  Otra. Definir Haga clic o pulse aquí para escribir texto. |
| Indique las características que se corresponden con el equipo informático en el que se almacenarán y procesarán los datos.  Marque tantas casillas como corresponda. | Cuenta con controles de identificación y autenticación de usuarios  Su acceso es exclusivo al equipo investigador y a su administrador  Se utiliza exclusivamente a actividades de investigación  Se ubica en una zona de acceso restringido en exclusiva al personal investigador  El dispositivo cuenta con un método de cifrado de datos  Dispone de un procedimiento documentado de respaldo de la información  Otro. En su caso, describir |
| En caso de que los datos vayan a ser transmitidos por redes públicas o redes inalámbricas de comunicaciones electrónicas, indique el tipo de cifrado o de mecanismo que garantice que la información no será inteligible ni manipulada por terceros. | Haga clic o pulse aquí para escribir texto. |
| Indique la ubicación y características de seguridad donde se guardará la información de carácter personal **en soporte físico**, en caso de que existiese para el proyecto/estudio (por ejemplo, los consentimientos informados firmados). | Haga clic o pulse aquí para escribir texto. |
| Indique la manera en que los datos de carácter personal se usarán por el equipo investigador | Los datos se utilizarán seudonimizados  Los datos se utilizarán codificados  Los datos se utilizarán codificados, teniendo el equipo investigador acceso a la identidad de los participantes. |
| En su caso, describa la manera en que se realizará la seudonimización de los datos[[6]](#footnote-6) | Haga clic o pulse aquí para escribir texto. |
| ¿Quién está previsto que tenga acceso a los datos personales en el marco del proyecto/estudio? | Miembros del equipo investigador vinculados al centro  Miembros del equipo investigador de otro centro. Especifique: Haga clic o pulse aquí para escribir texto.  Personal externo al equipo investigador. Especifique: Haga clic o pulse aquí para escribir texto. |
| **Observaciones:**  Haga clic o pulse aquí para escribir texto. | |

|  |  |
| --- | --- |
| **DESCRIPCIÓN DEL TRATAMIENTO DE DATOS**  Describir la naturaleza del tratamiento teniendo en cuenta todos los posibles aspectos del mismo (datos en papel, tratamiento automatizado, procedencia, uso, comunicaciones, publicaciones, etc). | |
| **Características del tratamiento** | |
| Tipo de tratamiento | Unicentrico  Multicéntrico  Big Data[[7]](#footnote-7)  Registro de pacientes  Otro (en su caso, detallarlo en el apartado de observaciones) |
| El objetivo y metodología de la investigación ¿han sido definidos por? | El IP del proyecto  Los IPs del proyecto  Una persona u organización externa  Otro (en su caso, detallarlo en el apartado de observaciones) |
| Licitud del tratamiento[[8]](#footnote-8) | Los interesados darán su consentimiento  Necesario para cumplir con una obligación legal  Interés público o ejercicio de intereses púbicos  Interés legítimo del responsable |
| **Observaciones:**  Haga clic o pulse aquí para escribir texto. | |
| **Naturaleza del tratamiento** | |
| ¿Cómo se recogen los datos? | Los proporciona al equipo investigador el hospital o la GVA  Los proporciona directamente el interesado  Se extraen de la historia clínica y/o de otros registros preexistentes  Se extraen de muestras biológicas |
| Los datos recogidos, ¿Se cruzarán con datos de otras fuentes o bases de datos? | Sí  No |
| ¿Quién va a tener acceso a los datos? | Los miembros del equipo investigador  Investigadores de otros centros  Prestadores de servicios (estadísticos, alojamiento de bases de datos, etc.)  Otro. Describir: Haga clic o pulse aquí para escribir texto. |
| Cómo parte del proyecto/estudio ¿Se enviarán los datos personales? ¿A qué destinatarios? | No  Sí. Describir los destinatarios: Haga clic o pulse aquí para escribir texto. |
| ¿Un tercero realizará alguna operación de tratamiento de los datos[[9]](#footnote-9)? | No  Sí. Describir el tratamiento que previsiblemente realizará: Haga clic o pulse aquí para escribir texto. |
| **Observaciones:**  Haga clic o pulse aquí para escribir texto. | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Alcance del tratamiento** | | | |
| ¿Qué datos se recogen? | Haga clic o pulse aquí para escribir texto. | | |
| ¿Incluyen categorías especiales de datos? ¿Cuáles? | De salud  Genéticos | Biométricos  Vida sexual | Orientación sexual |
| ¿De cuántas personas se espera tratar datos en la investigación? | Haga clic o pulse aquí para escribir texto. | | |
| ¿Cuántas personas se encuentra previstas que participen en el equipo investigador y tengan acceso a datos personales? | Haga clic o pulse aquí para escribir texto. | | |
| ¿Con qué frecuencia se recogerán datos y durante cuánto tiempo? | Haga clic o pulse aquí para escribir texto. | | |
| ¿A qué área geográfica pertenecen las personas que se incluirán en el tratamiento? | Haga clic o pulse aquí para escribir texto. | | |
| ¿cuál es el tiempo previsto para la realización de la investigación? | Haga clic o pulse aquí para escribir texto. | | |
| Una vez finalice el proyecto/estudio ¿Durante cuánto tiempo se prevé conservar los datos? | Haga clic o pulse aquí para escribir texto. | | |
| **Observaciones:**  Haga clic o pulse aquí para escribir texto. | | | |

|  |  |
| --- | --- |
| **Contexto del tratamiento** | |
| ¿Qué relación hay entre el responsable y los afectados? | Son pacientes, directos o indirectos, de la consulta o servicio médico  Ninguna, son totalmente desconocidos para el equipo investigador  Otra. Definir en la sección de observaciones. |
| ¿Qué control tienen los interesados sobre sus datos? | Los interesados pueden retirar su consentimiento en cualquier momento y se dejarán de recoger datos, pero no se eliminarán los ya recogidos.  Al utilizar datos seudonimizados no es posible identificar interesados, ni realizar ninguna acción por solicitud de ellos  Otra. Defina: Haga clic o pulse aquí para escribir texto. |
| ¿Esperarían los afectados que sus datos se trataran de este modo? | Haga clic o pulse aquí para escribir texto. |
| ¿Incluye tratamiento de datos de menores o de personas en situación de vulnerabilidad? | Sí  No |
| ¿Es un tratamiento de datos novedoso en algún aspecto? | Sí. Defina: Haga clic o pulse aquí para escribir texto.  No, se utilizarán sobre los datos técnicas y tecnologías de uso común. |
| ¿Cuál es el estado de la tecnología que se va a utilizar en el tratamiento de datos?[[10]](#footnote-10), [[11]](#footnote-11) | Tecnología de uso general. Ampliamente probada.  Tecnología diseñada específicamente para el tratamiento.  Otra. Definir Haga clic o pulse aquí para escribir texto. |
| ¿Existe alguna preocupación “a priori” sobre este tratamiento o sobre la seguridad de los medios que se empleen? | Haga clic o pulse aquí para escribir texto. |
| **Observaciones:**  Haga clic o pulse aquí para escribir texto. | |

|  |  |
| --- | --- |
| **Propósito del tratamiento** | |
| ¿Qué se pretende conseguir con el tratamiento? | Haga clic o pulse aquí para escribir texto. |
| ¿Qué beneficios se pretende obtener para los afectados? | Haga clic o pulse aquí para escribir texto. |
| ¿Qué beneficios se pretende obtener para el responsable? | Haga clic o pulse aquí para escribir texto. |
| ¿Qué efectos se prevén sobre los afectados? | Haga clic o pulse aquí para escribir texto. |
| **Observaciones:**  Haga clic o pulse aquí para escribir texto. | |

|  |
| --- |
| **Diagrama de flujo de datos, desde su obtención, hasta la publicación de resultados y su disposición final** |
|  |

|  |  |
| --- | --- |
| **CONSULTAS** | |
| ¿Se prevé consultar a los afectados por el tratamiento? Indicar en qué sentido o, en caso de respuesta negativa, justificarlo. | No  Sí  Indicar: Pulse aquí para escribir texto. |
| ¿Se prevé involucrar a otros órganos o departamentos de la administración? | No  Sí  Indicar: Pulse aquí para escribir texto. |
| ¿Se va a solicitar asistencia por parte de terceros encargados del tratamiento? | No  Sí  Indicar: Pulse aquí para escribir texto. |
| ¿Se prevé consultar a expertos en seguridad de la información? | No  Sí  Indicar: Pulse aquí para escribir texto. |
| ¿Se prevé consultar a otros expertos? | No  Sí  Indicar: Pulse aquí para escribir texto. |
| **Observaciones:**  Pulse aquí para escribir texto. | |

|  |  |
| --- | --- |
| **EVALUACIÓN DE LA NECESIDAD Y LA PROPORCIONALIDAD** | |
| ¿Habría otros modos de conseguir los fines que persigue el tratamiento? | Sí. Defina: Haga clic o pulse aquí para escribir texto.  No |
| ¿Qué mecanismos va a aplicar para asegurar la calidad de los datos? | Monitorización o seudomonitorización  Otro. Defina: Haga clic o pulse aquí para escribir texto.  Ninguno |
| ¿El protocolo identifica claramente las variables a obtener y su pertinencia con los objetivos del proyecto, para asegurar la minimización de los datos? | Sí  No |
| ¿Qué información se va a proporcionar a los afectados? | Se les ha proporcionado información de la forma de ejercer sus derechos previamente a obtener su consentimiento  Se les ha notificado del tratamiento y se ha dispuesto la información en la página web del centro  Los datos se reciben seudonimizados por lo que no es posible proporcionar información a los interesados. Hay información del tratamiento en la página web del centro  Otra. Defina: Haga clic o pulse aquí para escribir texto. |
| ¿Cómo se va a garantizar el ejercicio de los derechos de los afectados?[[12]](#footnote-12) | Las solicitudes se atenderán íntegramente por el IP  Las solicitudes se atenderán por el IP en coordinación con el personal del HCUV  Las solicitudes se atenderán por el IP en coordinación con el personal del centro donde se realiza el proyecto/ensayo  Otro. Defina: Haga clic o pulse aquí para escribir texto. |
| ¿Qué medidas se tomarán para asegurar el cumplimiento por parte de los encargados de tratamiento o de otros proveedores de servicios | Se elaborará y firmará un contrato de tratamiento de datos  Se firmará contrato de adhesión a un servicio comercial  Otro. Defina: Haga clic o pulse aquí para escribir texto.  Ninguno  No aplica |
| ¿se enviarán datos a personas u organizaciones ubicadas fuera de la UE? | Sí  No |
| ¿En qué se basarán las transferencias internacionales de datos, si las hubiera?  Mayor información en este [ENLACE](https://www.aepd.es/reglamento/cumplimiento/transferencias-internacionales.html) | Existe autorización de la Agencia Española de Protección de Datos - AEPD  El país de destino garantiza un nivel de protección adecuado, de acuerdo a la Comisión  El país de destino no se considera con un nivel adecuado de protección, pero se establecen las garantías adecuadas y se asegura que los interesados cuentan con los derechos exigibles y acciones legales efectivas, a través de:  documentos legales entre las organizaciones  normas corporativas vinculantes  cláusulas tipo de protección de datos  código de conducta  mecanismos de certificación  Documentos legales entre las organizaciones  Documentos legales entre las organizaciones  No aplica |
| **Observaciones:**  Haga clic o pulse aquí para escribir texto. | |

|  |
| --- |
| **ANÁLISIS DE RIESGOS** |

El valor del riesgo se calcula a partir de la estimación de la probabilidad de que se concrete una determinada amenaza y de la cuantificación del impacto que pueda tener en los derechos y libertades o en la esfera íntima de los individuos afectados.

El nivel de cada riesgo se determina a partir de un factor que considera la probabilidad de su ocurrencia y el impacto, que podría generar en el individuo afectado, en su caso.

**Criterios para la estimación de la PROBABILIDAD:**

La probabilidad de la materialización de una amenaza, que pueden afectar a los tratamientos de datos personales es una estimación que debe tomar en consideración al menos los factores siguientes:

* Si la amenaza se ha materializado en el pasado próximo, y con qué frecuencia,
* las medidas de seguridad existentes que pueden evitar la materialización de la amenaza,
* la posibilidad y oportunidad de que la amenaza sea ejecutada por el agente
* el origen y la fuente de la amenaza.

Se seleccionará una de las siguientes opciones, para cada amenaza.

|  |  |
| --- | --- |
| **Valoración de la PROBABILIDAD:** | **Ejemplos o directrices** |
| **Es muy poco probable que ocurriera** | Amenazas que **no se han concretado nunca** (incendio, inundación…) y que la previsión de que pasen es remota. |
| **Es difícil que ocurra** | Se tiene constancia que la amenaza se concreta, pero sucede **esporádicamente** (ataques, robo de datos…) |
| **Podría ocurrir** | Se tiene constancia que la amenaza se concreta **con alguna frecuencia** en el entorno, en el sector o en tratamientos equivalentes (filtraciones de datos, pérdidas de soportes, acceso indebido por personal interno...) |
| **Es muy probable que ocurra** | Amenazas que se concretan con mayor periodicidad o frecuencia en el entorno, en el sector o en tratamientos equivalentes (pérdida de disponibilidad por fallos en sistemas o redes...) |

**Criterios para la estimación del IMPACTO[[13]](#footnote-13):** Impacto que la materialización de la amenaza podría tener para la persona propietaria de los datos implicados.

|  |  |
| --- | --- |
| **Valoración del IMPACTO** | **Ejemplos o directrices** |
| BAJO | En caso de ocurrencia, le genera al afectado una **situación molesta** pero que no implica un potencial riesgo para sus derechos o libertades |
| MEDIO | En caso de ocurrencia, le genera al afectado **una situación que debe gestionar** y que puede derivar en un menoscabo de su patrimonio, salud, imagen pública, intimidad o seguridad. |
| ALTO | En caso de ocurrencia, el afectado **podría correr un riesgo que pusiera en peligro algún aspecto** de su patrimonio, salud, imagen pública, intimidad o seguridad del que no pudiera recuperarse en su totalidad en un periodo corto de tiempo. |

Elnivel de riesgo se calculará a partir de la siguiente tabla:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **RIESGO** | | **Impacto** | | |
| **BAJO** | **MEDIO** | **ALTO** |
| **Probabilidad** | **MUY BAJA** | INSIGNIFICANTE | BAJO | MEDIO |
| **BAJA** | BAJO | MEDIO | MEDIO |
| **MEDIA** | MEDIO | MEDIO | ALTO |
| **ALTA** | MEDIO | ALTO | MÁXIMO |

La tabla siguiente incluye un listado de amenazas que pueden afectar a los tratamientos de datos de carácter personal. La mayor parte de ella se centran en riesgos a los que pueden estar sometidos los datos en sí mismos, pero se incluyen también para su valoración amenazas sobre algunos procesos críticos relacionados con los tratamientos. En el anexo I se incluyen orientaciones para la estimación de la probabilidad de las amenazas y del impacto. Cuando haya dudas sobre la estimación o se asuman determinados condicionantes, se deberán indicar en el campo de observaciones estas circunstancias. Las amenazas que no sean de aplicación en el caso concreto que se está analizando se dejarán en blanco dado que no habrá un riesgo asociado a la misma.

Al valorar la amenaza y el impacto sobre los datos (y lo que estos representan en la esfera privada de los afectados) deben tomarse en consideración las medidas de seguridad conocidas que se estén aplicando en los sistemas sobre los que se va a llevar a cabo el tratamiento.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **ANÁLISIS DE RIESGOS PARTE I** | | | | |
| ID | AMENAZA | PROBAB. | IMPACTO | RIESGO |
| DT 1 | Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos al **rendimiento en el trabajo** del afectado. | Seleccione | Seleccione | Seleccione |
| DT 2 | Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a la **situación económica** del afectado. | Seleccione | Seleccione | Seleccione |
| DT 3 | Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a **preferencias o intereses personales** del afectado. | Seleccione | Seleccione | Seleccione |
| DT 4 | Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a **la fiabilidad, comportamiento o solvencia financiera** del interesado. | Seleccione | Seleccione | Seleccione |
| DT 5 | Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a la **localización o los movimientos** del interesado. | Seleccione | Seleccione | Seleccione |
| DT 6 | Uso desleal de datos de grupos de afectados en situación de especial vulnerabilidad. | Seleccione | Seleccione | Seleccione |
| DT 7 | Uso desleal de datos de menores de edad. | Seleccione | Seleccione | Seleccione |
| DT 8 | Uso desleal de datos de personas con discapacidad. | Seleccione | Seleccione | Seleccione |
| PR 9 | Imposibilidad de cumplir con el deber de información.[[14]](#footnote-14) | Seleccione | Seleccione | Seleccione |
| PR 10 | Imposibilidad de que el afectado ejerza los derechos que la ley le reserva. | Seleccione | Seleccione | Seleccione |

|  |
| --- |
| **ANÁLISIS DE RIESGOS PARTE II** |

La siguiente tabla determina la valoración del impacto que pudiese causar en los interesados, un tratamiento incorrecto de sus datos personales.

|  |  |
| --- | --- |
| DAÑOS Y PERJUICIOS | IMPACTO |
| 1. **Discriminación** como consecuencia del conocimiento o revelación de los datos tratados a terceros no autorizados o de su incorrecto tratamiento. | Seleccione el valor adecuado. |
| 1. **Usurpación de identidad** como consecuencia del conocimiento o revelación de los datos tratados a terceros no autorizados o de su incorrecto tratamiento. | Seleccione el valor adecuado. |
| 1. **Fraude** como consecuencia del conocimiento o revelación de los datos tratados a terceros no autorizados o de su incorrecto tratamiento. | Seleccione el valor adecuado. |
| 1. **Pérdidas financieras** de los interesados como consecuencia del conocimiento o revelación de los datos tratados a terceros no autorizados o de su incorrecto tratamiento. | Seleccione el valor adecuado. |
| 1. **Daño para la reputación** de los interesados como consecuencia del conocimiento o revelación de los datos tratados a terceros no autorizados o de su incorrecto tratamiento. | Seleccione el valor adecuado. |
| 1. Perjuicio económico, moral o social significativo para los afectados, no contemplado en las opciones anteriores. | Seleccione el valor adecuado. |

**El valor máximo de los obtenidos en la tabla anterior, se colocará en la columna de “impacto” de las amenazas que aplicasen, incluidas en la siguiente tabla.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ID | AMENAZA | PROBAB. | IMPACTO | RIESGO |
| DT 11 | **Pérdida de confidencialidad** de datos. Sujetos al secreto profesional y que incluyen datos de categoría especial. | Seleccione | Seleccione | Seleccione |
| DT 12 | **Reversión no autorizada** de datos seudonimizados. | Seleccione | Seleccione | Seleccione |
| DT 13 | Uso de datos relacionados con las características personales, el estado físico y la salud, actual o futura del afectado **con cualquier fin distinto a alcanzar el objetivo del proyecto/estudio que se analiza en este formulario** (Uso desleal[[15]](#footnote-15)). | Seleccione | Seleccione | Seleccione |
| DT 14 | Pérdida de confidencialidad o integridad de datos que implique a **un gran número de afectados**. | Seleccione | Seleccione | Seleccione |
| DT 15 | Pérdida de confidencialidad o integridad de **gran cantidad de datos personales** de un solo individuo.[[16]](#footnote-16) | Seleccione | Seleccione | Seleccione |
| PR 16 | Transferencia a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección. | Seleccione | Seleccione | Seleccione |
| SEG 17 | Acceso **de personas no autorizadas** al equipo o instalación donde se almacenan los datos | Seleccione | Seleccione | Seleccione |
| SEG 18 | **Comunicación no intencionada** de datos a terceros, por parte de miembros del equipo investigador | Seleccione | Seleccione | Seleccione |
| SEG 19 | **Intrusión fraudulenta** al equipo informático donde se almacenan y tratan los datos por parte de terceros (ataque informático)[[17]](#footnote-17) | Seleccione | Seleccione | Seleccione |
| SEG 20 | Robo o pérdida **del equipo informático o soporte** dónde se ubican los datos personales | Seleccione | Seleccione | Seleccione |
| SEG 21 | Intercepción de los datos al ser **enviados sin un método de cifrado** o transmitidos por canales no seguros | Seleccione | Seleccione | Seleccione |
| SEG 22 | Intrusión o acceso no autorizado, involuntario o no, a datos alojados en **servicios “cloud”[[18]](#footnote-18)** | Seleccione | Seleccione | Seleccione |
| SEG 23 | Uso desleal de datos o brecha de seguridad por parte de un **encargado de su tratamiento**.[[19]](#footnote-19) | Seleccione | Seleccione | Seleccione |
| SEG 24 | Inadecuada disposición de los dato personales **una vez alcanzados los objetivos** del proyecto/estudio | Seleccione | Seleccione | Seleccione |
|  | **Observaciones:**  Haga clic o pulse aquí para escribir texto. | | | |

**MEDIDAS DE MINIMIZACIÓN DE RIESGOS**

Cuando un determinado riesgo se cuantifique como MÁXIMO o ALTO deberán considerarse medidas que lo mitiguen. En el caso de riesgos de nivel MEDIO quedará a criterio del responsable considerarlas o no.

En el Anexo I se incluye un listado de medidas asociadas a cada amenaza que pueden completarse con otras que, a juicio del responsable, sean adecuadas para minimizar el riesgo.

No deben incluirse medidas compensatorias de las cuales se tenga constancia que ya se aplican sistemáticamente a todos los tratamientos en aplicación de políticas o criterios de seguridad generales.

|  |  |
| --- | --- |
| MEDIDA | ID DE RIESGOS QUE MITIGA LA MEDIDA |
| Haga clic o pulse aquí para escribir texto. | Haga clic o pulse aquí para escribir texto. |
| Haga clic o pulse aquí para escribir texto. | Haga clic o pulse aquí para escribir texto. |
| Haga clic o pulse aquí para escribir texto. | Haga clic o pulse aquí para escribir texto. |
| Haga clic o pulse aquí para escribir texto. | Haga clic o pulse aquí para escribir texto. |
| Haga clic o pulse aquí para escribir texto. | Haga clic o pulse aquí para escribir texto. |
| Haga clic o pulse aquí para escribir texto. | Haga clic o pulse aquí para escribir texto. |
| **Conclusiones:**  Haga clic o pulse aquí para escribir texto. | |

|  |  |  |
| --- | --- | --- |
| **ACEPTACIÓN DE RIESGOS RESIDUALES**  Si el riesgo residual es MEDIO, el mismo debe ser formalmente aceptado por el Investigador Principal (Responsable de tratamiento) con su firma en el siguiente apartado.  Si, aun aplicando las medidas de minimización de riesgos, el riesgo residual es ALTO, no es suficiente la aceptación del responsable, se debe consultar a la autoridad de control[[20]](#footnote-20). | | |
| ID. RIESGO | VALOR DE RIESGO RESIDUAL | ACEPTACIÓN DEL IP |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |
| Id. | Elija un elemento. |  |

|  |  |
| --- | --- |
| **Aprobación del riesgo residual por el responsable** | |
| Haga clic o pulse aquí para escribir texto. | |
| **Fecha:** | **Firma:** |

|  |  |  |
| --- | --- | --- |
| **Revisión por el Responsable de Protección de Datos del Centro** | | |
| Texto. | | |
| **Fecha:**  Fecha | **El tratamiento requiere de la revisión del DPD de la GVA[[21]](#footnote-21):**  Sí  No | **Firma:** |

|  |  |
| --- | --- |
| **Revisión por el Delegado de Protección de Datos de la GVA** | |
| Texto. | |
| **Fecha:**  Fecha | **Firma:** |

**ANEXO I: MEDIDAS ASOCIADAS A LOS RIESGOS**

El riesgo generado por cada una de las amenazas puede ser mitigado mediante la adopción de algunas medidas. Una **relación no exhaustiva de medidas que se podrían aplicar** en el caso de que los riesgos obtenidos no fueran asumibles se puede ver en la tabla siguiente:

|  |  |
| --- | --- |
| RIESGO (AMENAZA): | MEDIDAS PROPUESTAS |
| 1. Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos al rendimiento en el trabajo del afectado. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales |
| 2. Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a la situación económica del afectado. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales |
| 3. Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a preferencias o intereses personales del afectado. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales |
| 4. Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a la fiabilidad, comportamiento o solvencia financiera del interesado. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales |
| 5. Uso desleal de datos relacionados con el análisis o la predicción de aspectos referidos a la localización o los movimientos del interesado. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales * Valorar la seudonimización de los datos |
| 6. Uso desleal de datos de grupos de afectados en situación de especial vulnerabilidad. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales * Valorar el enmascaramiento de los datos |
| 7. Uso desleal de datos de menores de edad. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles incidencias |
| 8. Uso desleal de datos de personas con discapacidad. | * Aplicar medidas técnicas de seguridad en el grado superior al que corresponda según la catalogación de activos del ENS * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales |
| 9. Imposibilidad de cumplir con el deber de información. | * Reforzar los mecanismos de información sobre los tratamientos ofreciendo fuentes redundantes * Introducir recordatorios periódicos sobre el tratamiento a los afectados. |
| 10. Imposibilidad de que el afectado ejerza los derechos que la ley le reserva. | * Establecer medidas organizativas (formularios en papel, procedimientos alternativos, etc.) que refuercen el procedimiento de ejercicio de derechos |
| 11. Pérdida de confidencialidad de datos sujetos al secreto profesional. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Reforzar la seguridad de los sistemas de almacenamiento * Realización de auditorías periódicas sobre los accesos para detectar posibles incidencias |
| 12. Reversión no autorizada de datos seudonimizados. | * Adoptar medidas organizativas que mejoren el proceso de seudonimización. * Reforzar controles de acceso a los datos identificados * Realización de pruebas controladas de reidentificación a partir de los datos seudonimizados |
| 13. Uso de datos relacionados con las características personales, el estado físico y la salud, actual o futura del afectado con cualquier fin distinto a alcanzar el objetivo del proyecto/estudio que se analiza en este formulario | * Aplicar medidas técnicas de seguridad en el grado superior al que corresponda según la catalogación de activos del ENS * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales |
| 14. Pérdida de confidencialidad o integridad de datos que implique a un gran número de afectados. | * Aplicar medidas técnicas de seguridad en el grado superior al que corresponda según la catalogación de activos del ENS * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales * Establecer protocolos de información a los afectados |
| 15. Pérdida de confidencialidad o integridad de gran cantidad de datos personales de un solo individuo. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles usos desleales * Establecer protocolos de información al afectado |
| 16. Transferencia a terceros Estados u organizaciones internacionales respecto de los que no se hubiese declarado un nivel adecuado de protección. | * Fijar claramente las condiciones en las que se lleva a cabo la transferencia (reglas corporativas vinculantes, cláusulas contractuales tipo, autorización de la AEPD). |
| 17. Acceso de personas no autorizadas al equipo o instalación donde se almacenan los datos | * Establecer controles de acceso al equipo o instalación * Buscar una nueva ubicación de los datos que asegure el control del acceso |
| 18. Comunicación no intencionada de datos a terceros, por parte de miembros del equipo investigador | * Eliminación del posible canal de comunicación en el equipo * Establecer medidas que disminuyan las posibilidades de error que pudieran generar las comunicaciones no intencionadas * Establecer medidas para que, en caso de una comunicación no intencionada, los datos no pudieran ser accesibles o interpretados con facilidad. Por ejemplo, encriptación. |
| 19. Intrusión fraudulenta al equipo informático donde se almacenan y tratan los datos por parte de terceros (ataque informático)[[22]](#footnote-22) | * Establecer medidas de seguridad adicionales que disminuyeran la probabilidad de éxito de un ataque informático * Limitar el acceso a la red del equipo en el que se almacenan los datos * Establecer medidas para que, en caso de extracción de los datos, estos no pudieran ser accesibles o interpretados con facilidad. Por ejemplo, encriptación. |
| 20. Robo o pérdida del equipo informático o soporte dónde se ubican los datos personales | * Modificar la ubicación de los datos a equipos o soportes con menor probabilidad de robo o pérdida * Establecer medidas para que, en caso de robo o pérdida del equipo, los datos no pudieran ser accesibles o interpretados con facilidad. Por ejemplo, encriptación. |
| 21. Intercepción de los datos al ser enviados sin un método de cifrado o transmitidos por canales no seguros | * Valorar la posibilidad de eliminar la comunicación de datos a través de redes informáticas * Uso de redes seguras y métodos de cifrado de datos en la comunicación |
| 22. Intrusión o acceso no autorizado, involuntario o no, a datos alojados en servicios “cloud”[[23]](#footnote-23) | * Valorar la posibilidad de almacenar los datos en un entorno local en lugar del “cloud” * Selección de un proveedor del servicio que ofrezca mayor seguridad y garantías |
| 23. Uso desleal de datos o brecha de seguridad por parte de un encargado de su tratamiento.[[24]](#footnote-24) | * Selección de un encargado del tratamiento que ofrezca mayor seguridad y garantías * Solicitar al encargado del tratamiento los registros del análisis de riesgo y verificar que se encuentran en valores adecuados |
| 24. No eliminación de los dato personales una vez alcanzados los objetivos del proyecto/estudio | * Asignar un responsable para su disposición final y establecerlo en el protocolo del proyecto/estudio * Identificar en el protocolo el método de disposición final de los datos adecuado al proyecto/estudio y a la legislación |

Medidas que se podrían considerar en caso de que el tratamiento tuviera un alto impacto en alguno de los ámbitos de riesgo para los interesados.

|  |  |
| --- | --- |
| a). Discriminación como consecuencia de la revelación de los datos tratados. | * Reforzar controles de acceso a los datos * Limitar el período de conservación de los datos * Reforzar el sistema de trazabilidad de los accesos * Permitir la trazabilidad de los accesos por parte del afectado |
| b). Usurpación de identidad como consecuencia del conocimiento de los datos tratados. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles incidencias * Contratación de seguros |
| c). Fraude como consecuencia del conocimiento de los datos tratados. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Realización de auditorías periódicas sobre los accesos para detectar posibles incidencias * Contratación de seguros |
| d). Pérdidas financieras de los interesados como consecuencia de la revelación o alteración de los datos. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Contratación de seguros |
| e). Daño para la reputación de los interesados como consecuencia de la revelación de los datos. | * Reforzar controles de acceso a los datos * Limitar el período de conservación de los datos * Reforzar el sistema de trazabilidad de los accesos * Permitir la trazabilidad de los accesos por parte del afectado |
| f). Perjuicio económico, moral o social significativo para los afectados no contemplado anteriormente. | * Reforzar controles de acceso a los datos * Reforzar el sistema de trazabilidad de los accesos * Contratación de seguros |

1. 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. [↑](#footnote-ref-1)
2. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. [↑](#footnote-ref-2)
3. La evaluación de impacto puede ser realizada siguiendo cualquier otra metodología, siempre que cumpla con lo dispuesto en el artículo 35.7 del RGPD. [↑](#footnote-ref-3)
4. Si desea mayor información sobre las implicaciones del ser Responsable de tratamiento, puede consultar la Guía disponible en este [ENLACE](https://www.aepd.es/media/guias/guia-rgpd-para-responsables-de-tratamiento.pdf) [↑](#footnote-ref-4)
5. Esquema Nacional de Seguridad. De aplicación obligatoria para la administración pública y sus proveedores tecnológicos. [↑](#footnote-ref-5)
6. La disposición adicional decimoséptima de la LOPDyDGG, en su apartado 2,d) indica que, con fines de investigación en salud pública y biomédica, salvo excepciones, solo se pueden utilizar datos seudonimizados, e indica las dos condiciones que debe cumplir la seudonimización: separación técnica y funcional entre el equipo investigador y quienes realizan la seudonimización y que SOLO sean accesibles al equipo investigador cuando existen compromisos de confidencialidad y de no reidentificación de los datos, así como cuando se ha implantado medidas de seguridad para evitar acceso de terceros no autorizados a los datos. [↑](#footnote-ref-6)
7. Si su proyecto es de “Big Data”, se le recomienda observar el código de buenas prácticas disponible en este [ENLACE](https://www.aepd.es/media/guias/guia-codigo-de-buenas-practicas-proyectos-de-big-data.pdf) [↑](#footnote-ref-7)
8. Marcar la misma base jurídica que se especificó en el RAT. [↑](#footnote-ref-8)
9. En caso de que se considere la contratación de servicios de “cloud computing”, se recomienda observar la guía disponible en este [ENLACE](https://www.aepd.es/media/guias/guia-cloud-clientes.pdf) [↑](#footnote-ref-9)
10. Si como parte del proyecto/estudio, está previsto el desarrollo de herramientas para plataforma ANDROID, se recomienda consultar la guía disponible en este [ENLACE](https://www.aepd.es/media/estudios/estudio-flujos-informacion-android.pdf) [↑](#footnote-ref-10)
11. Si como parte del proyecto/estudio, está previsto utilizar dispositivos de identificación por huella digital, se recomienda consultar la guía disponible en este [ENLACE](https://www.aepd.es/media/estudios/estudio-fingerprinting-huella-digital.pdf) [↑](#footnote-ref-11)
12. En caso de que el “afectado” (solicitante) no quedase satisfecho con la respuesta recibida sobre su solicitud de ejercicio de derechos, podrá presentar una reclamación al Delegado de Protección de Datos de la GVA o a la Agencia Española de Protección de Datos, si así lo considerase oportuno. [↑](#footnote-ref-12)
13. El proyecto/estudio de investigación no realizará tratamiento sobre los datos destinados al servicio que se le presta al interesado, por lo que su destrucción, pérdida o alteración, podría poner en riesgo el proyecto y sus objetivos, más no los derechos y libertades del interesado. Por lo anterior, la valoración del impacto y por tanto, de los riesgos, se realiza sobre una potencial comunicación o acceso indebido a los datos objeto de investigación, exclusivamente. [↑](#footnote-ref-13)
14. Por ejemplo, en la Hoja de Información al Paciente, se le proporciona información sobre el tratamiento de datos que se realizará. La información proporcionada debe cumplir con lo especificado en el artículo 13 o 14 del RGPD. [↑](#footnote-ref-14)
15. Por “Uso desleal” debe entenderse cualquier uso de los datos, incluida la posesión, con un objeto distinto de alcanzar los objetivos del proyecto/estudio sujeto de este análisis. Dicho en otras palabras, cualquier operación sobre los datos no descritos en el protocolo o en el registro de actividad de tratamiento, sería uso desleal. [↑](#footnote-ref-15)
16. Algunos ficheros de información genética podrían considerarse “gran cantidad de datos”. Por ejemplo, si se han secuenciado genes o cromosomas completos. [↑](#footnote-ref-16)
17. Menor probabilidad de ocurrencia si es un equipo gestionado por los servicios informáticos del centro y si solo se conecta a redes protegidas con cortafuegos u otras medidas de protección. [↑](#footnote-ref-17)
18. El riesgo está en función de las características del servicio en el que se alojan, del número de usuarios con los que se comparten y el número de dispositivos desde los que se acceden. [↑](#footnote-ref-18)
19. El riesgo variará en función de la infraestructura y profesionalidad del encargado de tratamiento elegido por el IP. [↑](#footnote-ref-19)
20. según establece el artículo 36 del RGPD [↑](#footnote-ref-20)
21. Por ejemplo, por ser un tratamiento que implique un alto volumen de datos, exista un riesgo de especial atención o que tenga una extensión que requiriese especial atención. [↑](#footnote-ref-21)
22. Menor probabilidad de ocurrencia si es un equipo gestionado por los servicios informáticos del centro y si solo se conecta a redes protegidas con cortafuegos u otras medidas de protección. [↑](#footnote-ref-22)
23. El riesgo está en función de las características del servicio en el que se alojan, del número de usuarios con los que se comparten y el número de dispositivos desde los que se acceden. [↑](#footnote-ref-23)
24. El riesgo variará en función de la infraestructura y profesionalidad del encargado de tratamiento elegido por el IP. [↑](#footnote-ref-24)