**GESTIÓN DE RIESGOS**

Actividad de tratamiento: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Operación de tratamiento (opcional): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Fecha de inicio: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

Fecha de conclusión: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.

**1.- Identificación de amenazas**

|  |
| --- |
| **Identificación de amenazas** |
| **Actividad de tratamiento fuente del riesgo** | **Operación de tratamiento** | **Referencia de amenaza** | **Amenazas** | **Descripción de la amenaza** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

**2.- Valoración del riesgo inherente**

**A. Instrucciones para valorar el riesgo inherente y el riesgo residual**

|  |
| --- |
| **Tabla de probabilidad del riesgo**  |
|  | **Valor** | **Probabilidad de ocurrencia del riesgo** |
| **Máxima** | 4 | La posibilidad de ocurrencia es muy elevada |
| **Significativa** | 3 | La posibilidad de ocurrencia es alta |
| **Limitada** | 2 | La posibilidad de ocurrencia es baja |
| **Despreciable** | 1 | La posibilidad de ocurrencia es muy baja |

|  |
| --- |
| **Tabla de probabilidad del riesgo y de valor del impacto** |
| **Gravedad** | **Valor** | **Valor del Impacto sobre el interesado** | **Posibles daños sobre el interesado** |
| **Máxima** | 4 | El impacto es muy alto* Consecuencias significativas
* Consecuencias irreversibles
* Consecuencias insuperables
 | * Agresiones físicas con consecuencias irreparables.
* Asunción de una deuda inafrontable, imposibilidad de volver a trabajar o incumplimiento de obligaciones materiales con perjuicios económicos irreparables.
* Se agrede significativamente contra los derechos y libertades de los interesados, por ejemplo, padecimiento psicológico con consecuencias a largo plazo o irreparables por la divulgación de datos sensibles.
 |
| **Significativa** | 3 | El impacto es alto* Consecuencias significativas
* Consecuencias superables
 | * Empeoramiento del estado de salud o agresiones físicas.
* Apropiación indebida de fondos, pérdida del empleo o incumplimiento de obligaciones materiales con perjuicios económicos relevantes.
* Se agrede contra los derechos y libertades de los interesados, por ejemplo, una citación judicial, entrar en una lista de morosidad o divulgación de datos personales con impacto significativo en la reputación del interesado.
 |
| **Limitada** | 2 | El impacto es bajo* Encontrarán inconveniencias no significativas
 | * Estrés o padecimientos físicos menores.
* Costes extra, denegación de acceso a algunos servicios o incumplimiento de obligaciones materiales con perjuicios económicos.
* Se priva de los derechos y libertades de los interesados, por ejemplo, por difamación de un interesado por divulgación de datos personales.
 |
| **Despreciable**  | 1 | El impacto es muy bajo* No se verán prácticamente afectados
* Encontrarán solo pequeñas inconveniencias
 | * Molestias o irritación
* Se incumplen obligaciones materiales sin perjuicios relevantes
* No se priva de los derechos y libertades
 |

|  |
| --- |
| **Cuadro de riesgo [Riesgo = Probabilidad x Impacto]** |
| **Probabilidad** | **Máxima – 4** | **4** | **8** | **12** | **16** |
| **Significativa – 3** | **3** | **6** | **9** | **12** |
| **Limitada – 2** | **2** | **4** | **6** | **8** |
| **Despreciable – 1**  | **1** | **2** | **3** | **4** |
| **Bajo – Alto .** **Medio – Muy Alto** |  | **Despreciable – 1** | **Limitada – 2** | **Significativa – 3** | **Máxima – 4**  |
| **Impacto** |

**B.- Valoración del riesgo inherente**

Deben agregarse a continuación las amenazas que se identifiquen, así como suprimir aquellas ya incluidas que no correspondan con la realidad.

|  |
| --- |
| **Amenazas generales – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto****(1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Pérdidas económicas y daños reputacionales derivados del incumplimiento de la legislación sobre protección de datos personales. |  |  |  |  |  |
| Pérdidas económicas y daños reputacionales derivados del incumplimiento de legislaciones sectoriales con incidencia en la protección de datos personales a las que pueda estar sujeto el responsable del tratamiento. |  |  |  |  |  |
| Pérdidas económicas, pérdida de clientes y daños reputacionales derivados de la carencia de medidas de seguridad adecuadas o de la ineficacia de las mismas, en particular, cuando se producen pérdidas de datos personales. |  |  |  |  |  |
| Pérdida de competitividad del producto o servicio derivada de los daños reputacionales causados por una deficiente gestión de la privacidad. |  |  |  |  |  |
| Falta de conocimiento experto sobre protección de datos y de canales de comunicación con los afectados. |  |  |  |  |  |
| Incorporación tardía de los expertos en protección de datos (en particular, del delegado de protección de datos o DPO) al proyecto o definición deficiente de sus funciones y competencias. |  |  |  |  |  |

|  |
| --- |
| **Legitimación de los tratamientos y cesiones de datos personales – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Tratar o ceder datos personales cuando no es necesario para la finalidad perseguida. |  |  |  |  |  |
| Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales. |  |  |  |  |  |
| Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales. |  |  |  |  |  |
| Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión. |  |  |  |  |  |
| Dificultades para garantizar la legitimidad de la recogida y la cesión de datos personales provenientes de terceros. |  |  |  |  |  |
| Solicitar y tratar datos especialmente protegidos sin necesidad o sin adoptar las salvaguardias necesarias. |  |  |  |  |  |
| Enriquecer los datos personales de forma no prevista en las finalidades iniciales y sin la información adecuada a los afectados al realizar una interconexión con otras bases de datos de la organización o de terceros, en particular, la re-identificación de información disociada. |  |  |  |  |  |
| Impedir la utilización anónima de un determinado producto o servicio cuando la identificación del usuario no resulta indispensable. |  |  |  |  |  |

|  |
| --- |
| **Transferencias internacionales – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Acceso secreto a los datos personales por parte de autoridades de terceros países. |  |  |  |  |  |
| Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia. |  |  |  |  |  |
| Impedimentos por parte del importador para el ejercicio de los procedimientos de supervisión y control pactados. |  |  |  |  |  |
| Incapacidad de ayudar a los ciudadanos en el ejercicio de sus derechos ante el importador. |  |  |  |  |  |
| No obtención de las autorizaciones legales necesarias. |  |  |  |  |  |

|  |
| --- |
| **Notificación y registro de las actividades de tratamiento – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe registrarse la creación, modificación o cancelación de actividades de tratamiento. |  |  |  |  |  |
| Carecer de los mecanismos y procedimientos necesarios para detectar cuando debe realizarse análisis de impacto en protección de datos y su consulta a la autoridad de control. |  |  |  |  |  |

|  |
| --- |
| **Transparencia de los tratamientos – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada (ubicación geográfica, comportamiento, hábitos de navegación, etc.). |  |  |  |  |  |
| En el entorno web, ubicar la información en materia de protección de datos (políticas de privacidad, cláusulas informativas) en lugares de difícil localización o diseminada en diversas secciones y apartados que dificulten su acceso conjunto y detallado. |  |  |  |  |  |
| Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso que impida que los afectados se hagan una idea clara y ajustada de los elementos esenciales que deben conocer para que exista un tratamiento leal de sus datos personales. |  |  |  |  |  |

|  |
| --- |
| **Calidad de los datos – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Solicitar datos o categorías de datos innecesarios para las finalidades del nuevo sistema, producto o servicio. |  |  |  |  |  |
| Existencia de errores técnicos u organizativos que propicien la falta de integridad de la información, permitiendo la existencia de registros duplicados con informaciones diferentes o contradictorias, lo que puede derivar en la toma de decisiones erróneas. |  |  |  |  |  |
| Garantías insuficientes para el uso de datos personales con fines históricos, científicos o estadísticos. |  |  |  |  |  |
| Utilizar los datos personales para finalidades no especificadas o incompatibles con las declaradas.* Datos transaccionales, de navegación o de geolocalización para la monitorización del comportamiento, la realización de perfiles y la toma de decisiones sobre las personas.
* Toma de decisiones económicas, sociales, laborales, etc. relevantes sobre las personas (en particular las que pertenecen a colectivos vulnerables), especialmente si pueden ser adversas o discriminatorias, incluyendo diferencias en los precios y costes de servicios y productos o trabas para el paso de fronteras.
* Toma de decisiones automatizadas con posibles consecuencias relevantes para las personas.
* Utilización de los metadatos para finalidades no declaradas o incompatibles con las declaradas.
 |  |  |  |  |  |
| Realizar inferencias o deducciones erróneas (y, en su caso, perjudiciales) sobre personas específicas mediante la utilización de técnicas de inteligencia artificial (en particular, minería de datos), reconocimiento facial o análisis biométricos de cualquier tipo. |  |  |  |  |  |
| Carecer de procedimientos claros y de herramientas adecuadas para garantizar la cancelación de oficio de los datos personales una vez que han dejado de ser necesarios para la finalidad o finalidades para las que se recogieron. |  |  |  |  |  |

|  |
| --- |
| **Categorías especiales de datos – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando este sea la causa que legitima su tratamiento o cesión. |  |  |  |  |  |
| Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de categorías especiales. |  |  |  |  |  |
| Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos. |  |  |  |  |  |

|  |
| --- |
| **Deber de secreto – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Accesos no autorizados a datos personales. |  |  |  |  |  |
| Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización. |  |  |  |  |  |

|  |
| --- |
| **Tratamientos por encargo – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas. |  |  |  |  |  |
| Falta de diligencia (o dificultad para demostrarla) en la elección del encargado de tratamiento. |  |  |  |  |  |
| Gestión deficiente de las subcontrataciones e insuficiente control sobre encargados y subcontratistas y, en particular, dificultades para comprobar o supervisar que el encargado y los subcontratistas cumplen las instrucciones y, especialmente, las medidas de seguridad. |  |  |  |  |  |
| No definición o deficiencias en los procedimientos para comunicar al responsable el ejercicio de los derechos de los interesados realizados ante los encargados de tratamiento. |  |  |  |  |  |
| Dificultades para conseguir la portabilidad de los datos personales a otros entornos una vez finalizado el contrato. |  |  |  |  |  |

|  |
| --- |
| **Derechos de los interesados – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Dificultar o imposibilitar el ejercicio de los derechos de los interesados. |  |  |  |  |  |
| Carencia de procedimientos y herramientas para la gestión de los derechos de los interesados. |  |  |  |  |  |
| Carencia de procedimientos y herramientas para la comunicación de rectificaciones, cancelaciones u oposiciones a los cesionarios de los datos personales. |  |  |  |  |  |

|  |
| --- |
| **Seguridad – Valoración del riesgo inherente** |
| **Amenaza** | **Riesgo y probabilidad** | **Impacto (1-4)** | **Riesgo inherente****= proba. X impacto** | **Valoración del riesgo inherente** |
| **Descripción** | **(1-4)** |
| Inexistencia de responsable de seguridad o deficiente definición de sus funciones y competencias. |  |  |  |  |  |
| Inexistencia de política de seguridad. |  |  |  |  |  |
| Deficiencias organizativas en la gestión del control de accesos. |  |  |  |  |  |
| Deficiencias técnicas en el control de accesos que permitan que personas no autorizadas accedan y sustraigan datos personales. |  |  |  |  |  |
| Imposibilidad de atribuir a usuarios identificados todas las acciones que se llevan a cabo en un sistema de información. |  |  |  |  |  |
| Uso de identificadores que revelan información del afectado. |  |  |  |  |  |
| Deficiencias en la protección de la confidencialidad de la información. |  |  |  |  |  |
| Falta de formación del personal sobre las medidas de seguridad que están obligados a adoptar y sobre las consecuencias que se pueden derivar de no hacerlo. |  |  |  |  |  |
| Existencia de incentivos para obtener la información ilícitamente por su valor (económico, político, social, laboral, etc.) para terceros no autorizados. |  |  |  |  |  |

**3.- Identificación de medidas de control**

Clasificación de medidas:

* Reducción del riesgo: reducen la probabilidad o el valor de impacto.
* Retención del riesgo: [riesgo inherente < riesgo aceptable = no es necesario adoptar medidas adicionales].
* Transferencia del riesgo: Un tercero asume las consecuencias. Por ejemplo, una aseguradora.
* Anulación del riesgo: [riesgo residual > riesgo aceptable] Se abandona el tratamiento.

Tipos de medidas:

* Tipología A: Organizativas, legales o técnicas
* Tipología B: Físicas, lógicas, organizativas, legales y formativas

|  |
| --- |
| **Identificación de medidas de control (para la eliminación, la mitigación o la minimización del riesgo hasta un nivel aceptable)** |
| **Amenaza** | **Riesgo** | **Medida de control** | **Descripción de la medida de control** | **Probabilidad(1-4)** | **Impacto(1-4)** | **Riesgo residual****= proba. X impacto** | **Valoración del riesgo residual** |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**4.- Identificación de tareas para la implantación de medidas**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Prioridad (1-4)** | **Medida** | **Concepto** | **Detalle** | **¿Completado?****Sí / No** |
|  |  | **Fecha prevista** |  |  |
| **Responsable** |  |  |
| **Ejecutor** |  |  |
| **Consultor** |  |  |
| **Persona a informar** |  |  |
| **Problemas detectados** |  |
|  |
|  |  | **Fecha prevista** |  |  |
| **Responsable** |  |  |
| **Ejecutor** |  |  |
| **Consultor** |  |  |
| **Persona a informar** |  |  |
| **Problemas detectados** |  |

**5.- Información adicional**

|  |
| --- |
|  |

**Firma:**

Use firma electrónica con marca visible o firme todas las páginas con firma ológrafa.