



ANÁLISIS DE RIESGOS DE CENTRO NUESTRA SEÑORA LOURDES

*El contenido de este documento es propiedad de **CENTRO NUESTRA SEÑORA LOURDES**, y ha sido elaborado por **PRODAT**, no pudiendo ser reproducido, ni comunicado total o parcialmente a otras personas distintas de las incluidas en esta lista de distribución adjunta a este documento, sin la autorización expresa de **CENTRO NUESTRA SEÑORA LOURDES** y **PRODAT**, quien ostenta los derechos de propiedad intelectual.*

ÍNDICE

1. IDENTIFICACIÓN DEL RESPONSABLE	3
2. VERSIÓN DEL DOCUMENTO	3
3. OBJETO DEL ANÁLISIS.....	4
3.1. Conceptos y Definiciones	5
4. DESCRIPCIÓN DE LAS OPERACIONES DE ACTIVIDADES DE TRATAMIENTO	7
6. ANÁLISIS DE LA NECESIDAD DE REALIZAR UNA EVALUACIÓN DE IMPACTO SOBRE LA PROTECCIÓN DE LOS DATOS	32
7. GESTIÓN DE RIESGOS POR DEFECTO	37
8. VALORES DEL RIESGO POR TRATAMIENTO	48
9. GRÁFICOS.....	50
10. RESUMEN EJECUTIVO.	52
11. CONCLUSIONES.....	56

1. IDENTIFICACIÓN DEL RESPONSABLE

CENTRO NUESTRA SEÑORA LOURDES (en adelante, C. NSTR. SÑRA. LOURDES) considerado como RESPONSABLE DEL TRATAMIENTO en base a lo establecido en el artículo 30.1 del 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.

C. NSTR. SÑRA. LOURDES	
CIF	R0900098E
Domicilio fiscal	Calle San Julián, 10 09002 Burgos
Domicilio social	Calle San Julián, 10 09002 Burgos

2. VERSIÓN DEL DOCUMENTO

Código	N.º de Edición/Fecha	Edición vigente	Autor/a modificación y actuación
RGPD-AR-01	PRIMERA	4 de enero de 2023	PRODA CYL

Clasificación	Ámbito de Difusión	Tipo de documento	Estado
Público	Equipo directivo	Documento técnico	Borrador
Interno X		Presentación	En revisión
Uso exclusivo		Análisis/Informe X	Actualizable
Confidencial		Otros:	Informe final X

A continuación, se enumeran las personas involucradas en el análisis de riesgos, que han permitido tanto la identificación de información como su clasificación.

NOMBRE	ÁREA /DEPARTAMENTO
Ana María del Val	Dirección

3. OBJETO DEL ANÁLISIS

El 25 de mayo de 2018, se cumplieron dos años desde la entrada en vigor del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en cuanto al tratamiento y la libre circulación de datos personales, (en adelante, RGPD). Desde ese momento, es aplicable el RGPD y obligatorio el cumplimiento de los requerimientos y obligaciones para el responsable y el encargado de tratamiento que este incluye, entre las que destaca, la necesidad de llevar a cabo un análisis de riesgos con el fin de establecer medidas de seguridad y control para garantizar los derechos y libertades de las personas.

Asimismo, el 6 de diciembre de 2018 se publicó la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

Esta norma nacional, tiene como objeto Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones, así como garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.

La LOPDGDD no realiza ninguna mención específica respecto del Análisis de riesgos y tampoco en relación con la Evaluación de Impacto, sino que únicamente se remite al articulado del RGPD. Es por ello por lo que este análisis centra su mención a los artículos previstos en el RGPD. El diseño adecuado de las actividades de tratamiento es un aspecto clave para poder garantizar los derechos y libertades de los interesados. La fase de diseño de un tratamiento define el flujo de los datos personales, así como todos los elementos que intervendrán a lo largo del mismo.

De igual modo, es el momento idóneo para definir las medidas de control y seguridad para garantizar los derechos y libertades de los interesados con el objetivo de que un tratamiento nazca respetando los requerimientos de privacidad asociados al nivel de riesgo al que está expuesto.

Dos elementos de carácter general constituyen la mayor innovación del RGPD para los responsables y se proyectan sobre todas las obligaciones de las organizaciones:

❖ EL PRINCIPIO DE RESPONSABILIDAD PROACTIVA

El RGPD describe este principio como la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita como aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión. En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

❖ EL ENFOQUE DE RIESGO

El RGPD señala que las medidas dirigidas a garantizar su cumplimiento deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas. De acuerdo con este enfoque, algunas de las medidas que el RGPD establece se aplicarán sólo cuando exista un alto riesgo para los derechos y libertades, mientras que otras deberán modularse en función del nivel y tipo de riesgo que los tratamientos presenten. La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado, no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

Todos los responsables deberán realizar una valoración del riesgo de los tratamientos que realicen, a fin de poder establecer qué medidas deben aplicar y cómo deben hacerlo. El tipo de análisis variará en función de:

- los tipos de tratamiento,
- la naturaleza de los datos,
- el número de interesados afectados,
- la cantidad y variedad de tratamientos que una misma organización lleve a cabo.

Organizaciones de menor tamaño y con tratamientos de poca complejidad: el análisis será el resultado de una reflexión, mínimamente documentada, sobre las implicaciones de los tratamientos en los derechos y libertades de los interesados. La reflexión deberá dar respuesta a cuestiones como las que se exponen en el apartado 4 relativo a la descripción de las actividades de tratamiento. Cuanto mayor sea el número de respuestas afirmativas mayor sería el riesgo que podría derivarse del tratamiento. Si la respuesta a estas preguntas y otras del mismo tipo fuera negativa, es razonable concluir que la organización no realiza tratamientos que generen un elevado nivel de riesgo.

3.1. Conceptos y Definiciones

A efectos del presente Análisis, se entenderá por:

I. Gestión de Riesgos.

Es el conjunto de actividades y tareas que permiten controlar la incertidumbre relativa a una amenaza mediante una secuencia de actividades que incluyen la identificación y evaluación del riesgo, así como las medidas para su reducción o mitigación. La gestión de riesgos se puede dividir en tres etapas diferenciadas: La identificación, la evaluación y el tratamiento de los riesgos.

II. Identificar amenazas y riesgos

El riesgo se deriva de la exposición a amenazas, por tanto, desde la perspectiva de la privacidad, es fundamental entender qué es una amenaza y cómo se pueden identificar escenarios de riesgo para los datos personales a partir de la misma.

Una amenaza es cualquier factor de riesgo con potencial para provocar un daño o perjuicio a los interesados sobre cuyos datos de carácter personal se realiza un tratamiento. Si ponemos el foco en la protección de los datos, las amenazas se pueden categorizar principalmente en tres tipos:

Acceso ilegítimo a los datos: ¿qué daño causaría que lo conociera quien no debe?

➡ Confidencialidad

Modificación no autorizada de los datos: ¿qué perjuicio causaría que estuviera dañado o corrupto? ➡ Integridad

Eliminación de los datos: ¿qué perjuicio causaría no tener un dato o no poder utilizarlo?
➡ Disponibilidad.

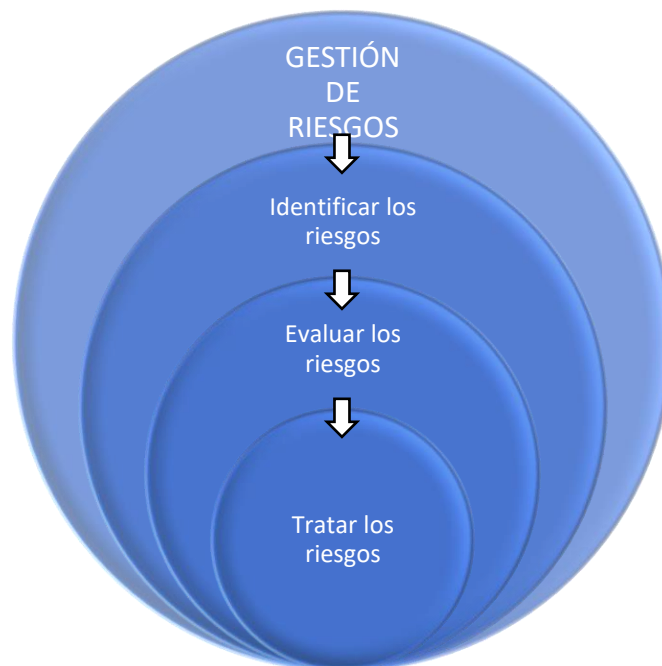
Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo. Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, identificar los riesgos siempre implica considerar la amenaza que los puede originar.

III. Evaluación del Riesgo.

Evaluar un riesgo implica considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice. El impacto, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se materializa, por ejemplo, un impacto sería despreciable si no tuviera consecuencias sobre el interesado o, por el contrario, un impacto sería significativo si el daño ocasionado sobre los derechos y libertades del interesado fuese crítico. Según la probabilidad y el impacto, asociados a las amenazas, es posible determinar el nivel de riesgo inherente.

IV. Tratar los riesgos

La última fase del proceso de gestión de riesgos es tratar los mismos. El objetivo de tratar los riesgos es disminuir su nivel de exposición con medidas de control que permitan reducir la probabilidad y/o impacto de que estos se materialicen. El riesgo inherente se puede tratar con el objetivo de reducir o mitigar el mismo, en función de la medida que se adopte, hasta situar el riesgo residual en un nivel que se considere razonable.



4. DESCRIPCIÓN DE LAS OPERACIONES DE ACTIVIDADES DE TRATAMIENTO

La descripción de los tratamientos sujetos al análisis de riesgos, permite obtener un conocimiento de las actividades realizadas y de cualquier elemento que interviene en las mismas.

Apartado 1 del artículo 30 del RGPD

“Cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad”. Adicionalmente indica que “cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable”.

En la práctica, puede identificarse un tratamiento como el conjunto de operaciones dirigidas a conseguir una determinada finalidad que se legitima en una misma base jurídica. Cada tratamiento incluirá una serie de operaciones como, por ejemplo, la recogida, registro, organización, estructuración, consulta o utilización de los datos.

La identificación y descripción de las actividades del tratamiento, no solo es una obligación, sino una necesidad en las fases iniciales para facilitar el análisis de riesgos.

A continuación, vamos a evaluar las características de los distintos tratamientos realizados por **CENTRO NUESTRA SEÑORA DE LOURDES**, (verificando los aspectos previstos en el **artículo 35.1 RGPD**: naturaleza, alcance, contexto y finalidades), identificando para cada tratamiento la tipología de datos, finalidades, colectivos afectados, los sistemas que intervienen en cada uno de los tratamientos, cesión de datos y transferencias internacionales, terceros intervinientes y plazos de conservación.

Estas preguntas, y el análisis de las respuestas, nos permiten detectar cuestiones que, si bien de forma aislada tal vez no tendrían una incidencia directa en la decisión de hacer la EIPD, su valoración conjunta quizás sí que nos lleva a considerar que estamos ante un tratamiento que supone un alto riesgo.

TRATAMIENTOS	FINALIDADES	CÓDIGO
GESTIÓN DE COLABORACIONES VOLUNTARIAS	– Gestión de las colaboraciones del programa de voluntariado del centro educativo	T01
CONSEJO ESCOLAR	– Gestión y mantenimiento de la relación existente entre el centro y los miembros del consejo escolar.	T02
GESTIÓN DE CONTACTOS PROFESIONALES, RRSS Y PÁGINA WEB	– Gestionar de la relación profesional existente entre las partes. – Contestar a consultas, solicitudes o peticiones. – Gestionar el servicio solicitado, contestar a la solicitud, o tramitar una petición. – Establecer una relación usuario-responsable, y crear una comunidad de seguidores.	T03
GESTIÓN ESCOLAR	– Gestionar la relación del alumno/a y sus familiares con el Centro. – Realización de todos los procedimientos necesarios para el mantenimiento, control y gestión de la relación académica con el centro.	T04
SERVICIOS COMPLEMENTARIOS	– Gestionar la relación del alumno/a con el Centro. – Gestionar los servicios solicitados. – Realizar todos aquellos trámites administrativos, fiscales y contables necesarios para cumplir con nuestros compromisos contractuales y obligaciones fiscales y contables.	T05

	<ul style="list-style-type: none"> – Gestionar los cobros correspondientes mediante recibo domiciliado u otras formas de pago permitidas a través de entidad financiera. 	
ACTIVIDADES EXTRAESCOLARES	<ul style="list-style-type: none"> – Gestionar la solicitud de inscripción en la actividad extraescolar ofertada por el centro. – Realizar todos aquellos trámites administrativos, fiscales y contables necesarios para cumplir con nuestros compromisos contractuales y obligaciones fiscales y contables. – Gestionar el cobro de la actividad extraescolar mediante entidad financiera. 	T06
PROGRAMA DE INTERCAMBIOS	<ul style="list-style-type: none"> – Gestionar la participación del alumno en el programa de intercambios en el extranjero organizado por el Centro. 	T07
DEPARTAMENTO DE ORIENTACIÓN	<ul style="list-style-type: none"> – Realización de aquellas las pruebas de evaluación psicopedagógicas y pruebas de aptitud que se estimen convenientes en el Departamento de Orientación del centro con el fin de poder orientar y elaborar un informe diagnóstico acorde a cada alumno/a. 	T08
GESTIÓN DE EMPLEADOS, EVALUACIÓN Y PROMOCIÓN	<ul style="list-style-type: none"> – Gestión de la relación laboral existente entre el centro y el empleado. 	T09
GESTIÓN DE SELECCIÓN DE PERSONAL	<ul style="list-style-type: none"> – Gestionar los procesos de selección de personal que realicemos. 	T10
GESTIÓN DE PRÁCTICAS PROFESIONALES	<ul style="list-style-type: none"> – Gestionar la realización de las prácticas profesionales del colaborador. 	T11

T01 GESTIÓN COLABORACIÓN VOLUNTARIADO

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.		X	
Características personales		X	
Circunstancias sociales			X
Datos académicos y profesionales		X	
Detalles del empleo			X
Información comercial			X
Datos económicos, financieros y de seguro			X
Transacciones de bienes y servicios			X
COLECTIVOS AFECTADOS		SÍ	NO
Miembros del programa de voluntariado del centro educativo		X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO		SÍ	NO
Office 365		X	
Correo electrónico		X	
Equipos informáticos		X	
Formularios de inscripción en papel		X	
FINALIDADES DE TRATAMIENTO		DETALLE	
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales?			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. <input type="checkbox"/> Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.		X

¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?		X
¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
– Las distintas áreas del centro.		
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?, en caso afirmativo, indicar su denominación social:		X
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
– Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.	X	
– Las imágenes publicadas en las redes sociales y página web del centro se conservarán salvo que el colaborador solicite la supresión de las mismas.	X	

T02 CONSEJO ESCOLAR

TIPOLOGÍA DE DATOS	SÍ	NO
Datos de carácter identificativo.	X	
Categorías especiales de datos.		X
Características personales		X
Circunstancias sociales		X
Datos académicos y profesionales		X
Detalles del empleo		X
Información comercial		X

Datos económicos, financieros y de seguro		X
Transacciones de bienes y servicios		X
COLECTIVOS AFECTADOS	SÍ	NO
Miembros del Consejo Escolar	X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
Office 365	X	
Correo electrónico	X	
Equipos informáticos	X	
Libros de actas en formato papel	X	
FINALIDADES DE TRATAMIENTO	DETALLE	SÍ NO
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000	
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.	
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.	
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales?		X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. <input type="checkbox"/> Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.	X
¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?		X
¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en		X

particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
– Las distintas áreas del centro.		
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?, en caso afirmativo, indicar su denominación social:		X
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
– Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.	X	
– Las imágenes publicadas en las redes sociales y página web del centro se conservarán salvo que el colaborador solicite la supresión de las mismas.	X	

T03 GESTIÓN DE CONTACTOS PROFESIONALES, RRSS Y PÁGINA WEB

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.			X
Características personales			X
Circunstancias sociales			X
Datos académicos y profesionales			X
Detalles del empleo			X
Información comercial			X
Datos económicos, financieros y de seguro			X
Transacciones de bienes y servicios			X
COLECTIVOS AFECTADOS		SÍ	NO
Contactos profesionales		X	
Contactos en RRSS		X	
Contactos web		X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO		SÍ	NO
Office 365		X	
Correo electrónico		X	
Equipos informáticos		X	
FINALIDADES DE TRATAMIENTO		DETALLE	
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	<input type="checkbox"/> Regional. X Nacional. <input type="checkbox"/> Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. <input type="checkbox"/> Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.		X
¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?			X

¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?		X
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
– Las distintas áreas del centro		
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles).	X	
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?, en caso afirmativo, indicar su denominación social.		X
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
– Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron.	X	

T04 GESTIÓN ESCOLAR

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.		X	
Características personales		X	
Circunstancias sociales		X	
Datos académicos y profesionales		X	
Detalles del empleo			X
Información comercial			X
Datos económicos, financieros y de seguro		X	
Transacciones de bienes y servicios			X
COLECTIVOS AFECTADOS		SÍ	NO
Alumnos/as		X	
Familiares		X	
Personas de contacto		X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO		SÍ	NO
Office 365		X	
Correo electrónico		X	
Plataforma de gestión educativa-Educamos		X	
Expedientes académicos en formato papel		X	
Actas en papel		X	
FINALIDADES DE TRATAMIENTO		SÍ	NO
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. X Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.		

¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?		X
¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
<ul style="list-style-type: none"> - Ministerio de Educación y Consejería de Educación de acuerdo a la legislación vigente. - A entidades bancarias, los datos relacionados con el cobro de la matrícula para gestionar los recibos domiciliados. - Cuando sea requerido por la Agencia Estatal de la Administración Tributaria, aquellos datos relacionados con el cobro de la matrícula. - Agencias de viaje para la organización de viajes y compañías aseguradoras para la contratación de seguros (accidentes, viajes), a entidades públicas y/o privadas para el control de asistencia de los alumno/as en excursiones y actividades análogas. - Entidades visitadas o encargadas de la organización cuando el alumno/a participe en salidas, excursiones y visitas a terceras entidades públicas o privadas. - Al AMPA del Centro para la realización de las gestiones propias de esta asociación. - A Escuelas Católicas nos lo solicite para posibles publicaciones tanto en su página web como en la revista de Escuelas Católicas. 	X	
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?	X	
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
<ul style="list-style-type: none"> - Mientras dure la escolarización del alumno/a y las prestaciones de los servicios solicitados en su caso. 	X	

ANÁLISIS DE RIESGOS - CENTRO NUESTRA SEÑORA LOURDES

– Finalizada la escolarización, el expediente académico del alumno/a se conservará durante el plazo necesario establecido en la legislación vigente.	X	
– En los supuestos de traslado a otro Centro, el expediente del alumno/a se remitirá al centro escolar de acogida indicado.	X	
– Las imágenes publicadas en las redes sociales y página web del Centro se conservarán hasta que solicite la supresión de las mismas.	X	

T05 SERVICIOS COMPLEMENTARIOS

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.		X	
Características personales		X	
Circunstancias sociales			X
Datos académicos y profesionales			X
Detalles del empleo			X
Información comercial			X
Datos económicos, financieros y de seguro		X	
Transacciones de bienes y servicios			X
COLECTIVOS AFECTADOS		SÍ	NO
Alumnos/as		X	
Familiares		X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO (Automatizados/No automatizados)		SÍ	NO
Office 365		X	
Correo electrónico		X	
Educamos		X	
Fichas de inscripción en formato papel		X	
FINALIDADES DE TRATAMIENTO		DETALLE	
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. <input type="checkbox"/> Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.		X
¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?			X

¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo?	X	
– Los distintos departamentos del centro.		
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?	X	
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
– Los datos personales serán conservados mientras dure la prestación del servicio.	X	
– Finalizada la misma, los datos se conservarán durante el tiempo necesario para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.	X	
– Los datos económicos se conservarán conforme a lo dispuesto en la Ley 58/2003, de 17 de diciembre, General Tributaria.	X	

T06 ACTIVIDADES EXTRAESCOLARES

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.		X	
Características personales			X
Circunstancias sociales			X
Datos académicos y profesionales			X
Detalles del empleo			X
Información comercial			X
Datos económicos, financieros y de seguro		X	
Transacciones de bienes y servicios			X
COLECTIVOS AFECTADOS		SÍ	NO
Familiares		X	
Alumnos/as		X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO (Automatizados/No automatizados)		SÍ	NO
Office 365		X	
Correo electrónico		X	
Equipos informáticos		X	
Recibos en formato papel		X	
FINALIDADES DE TRATAMIENTO		DETALLE	
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. X Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.	X	
¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?			X

¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles).	X	
<ul style="list-style-type: none"> - Entidades financieras. - Agencias Estatal de Administración Tributaria 	X	
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?	X	
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos?	X	
<ul style="list-style-type: none"> - Los datos personales serán conservados mientras dure la actividad. - Finalizado el mismo, los datos se conservarán durante el tiempo necesario para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. - Los datos económicos se conservarán conforme a lo dispuesto en la Ley 58/2003, de 17 de diciembre, General Tributaria. - Las imágenes publicadas en las redes sociales y página web del Centro se conservarán hasta que solicite la supresión de las mismas. 		

T07 PROGRAMA DE INTERCAMBIOS

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.		X	
Características personales		X	
Circunstancias sociales			X
Datos académicos y profesionales		X	
Detalles del empleo			X
Información comercial			X
Datos económicos, financieros y de seguro		X	
Transacciones de bienes y servicios			
COLECTIVOS AFECTADOS		SÍ	NO
Alumnos/as		X	
Familiares		X	
Personas de contacto		X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO		SÍ	NO
Office 365		X	
Correo electrónico		X	
PSP		X	
Inscripciones en formato papel		X	
Convenios de terceras entidades		X	
FINALIDADES DE TRATAMIENTO	DETALLE	SÍ	NO
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	<input type="checkbox"/> Regional. <input type="checkbox"/> Nacional. X Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. X Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.		

¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?		X
¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
Para la correcta prestación del servicio, los datos son cedidos a las entidades de destino.	X	
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)	X	
Cuando los programas de intercambio se realicen en países diferentes a los pertenecientes al Espacio Económico Europeo, se podrán realizar transferencias internacionales a los centros internacionales de acogida. Para ello se cumplirá en todo momento lo establecido en el RGPD.	X	
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?	X	
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
<ul style="list-style-type: none"> – Los datos necesarios para poder participar en estos programas serán conservados mientras dure la prestación del servicio solicitado. Finalizado el mismo, los datos se conservarán durante el tiempo necesario para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. 	X	

T08 DEPARTAMENTO DE ORIENTACIÓN

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.		X	
Características personales		X	
Circunstancias sociales		X	
Datos académicos y profesionales		X	
Detalles del empleo			X
Información comercial			X
Datos económicos, financieros y de seguro			X
Transacciones de bienes y servicios			X
COLECTIVOS AFECTADOS		SÍ	NO
Familiares		X	
Alumnos/as		X	
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO (Automatizados/No automatizados)		SÍ	NO
Office 365		X	
Correo electrónico		X	
Equipos informáticos		X	
Expedientes psicoterapéuticos		X	
FINALIDADES DE TRATAMIENTO	DETALLE	SÍ	NO
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. X Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.	X	
¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?			X

¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?	X	
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo?		X
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?	X	
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos?	X	
– Mientras dure la escolarización del alumno/a y las prestaciones de los servicios solicitados en su caso.	X	
– Finalizada la escolarización, el expediente académico del alumno/a se conservará durante el plazo necesario establecido en la legislación vigente.	X	
– En los supuestos de traslado a otro Centro, el expediente del alumno/a se remitirá al centro escolar de acogida indicado.	X	

T09 GESTIÓN DE EMPLEADOS, EVALUACIÓN Y PROMOCIÓN DE TRATAMIENTO

TIPOLOGÍA DE DATOS		SÍ	NO		
Datos de carácter identificativo.		X			
Categorías especiales de datos.		X			
Características personales		X			
Circunstancias sociales		X			
Datos académicos y profesionales		X			
Detalles del empleo		X			
Información comercial			X		
Datos económicos, financieros y de seguro		X			
Transacciones de bienes y servicios			X		
COLECTIVOS AFECTADOS		SÍ	NO		
Empleados		X			
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO (Automatizados/No automatizados)		SÍ	NO		
Office 365		X			
Correo electrónico		X			
Expedientes.		X			
Certificados negativos de delitos de naturaleza sexual.		X			
Contratos.		X			
Currículum.		X			
Nóminas.		X			
FINALIDADES DE TRATAMIENTO		DETALLE		SÍ	NO
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000				
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.				
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.				
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).					X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. X Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.			X	

¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?		X
¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?		X
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
<ul style="list-style-type: none"> – Entidades financieras. – Agencia Estatal de Administración Tributaria. – Entidades sanitarias. – Entidades aseguradoras. – Administración Pública con competencia en la materia. – Tesorería General de la Seguridad Social. – Organizaciones sindicales. – En el supuesto de que el empleado haya otorgado su consentimiento para el tratamiento de su nombre e imágenes y otras informaciones, relacionadas con la actividad del centro, se divulgarán en las diferentes redes sociales y página web del centro. 	X	
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?	X	
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
<ul style="list-style-type: none"> – Se conservarán durante el tiempo necesario para cumplir con la finalidad para la que se recabaron y para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos. 	X	
<ul style="list-style-type: none"> – La entidad conservará bloqueados durante el plazo legal de 4 años la documentación necesaria para acreditar el cumplimiento de las obligaciones en materia de afiliación, altas, bajas, documentos de cotización y los recibos justificativos del pago de salarios y del pago delegado de prestaciones. 	X	
<ul style="list-style-type: none"> – Toda aquella documentación fiscal obligatoria según la normativa tributaria que proceda será conservada durante un plazo de 4 años, de conformidad con la Ley General Tributaria. 	X	
<ul style="list-style-type: none"> – Las imágenes del trabajador publicadas en las redes sociales y página web del centro se conservarán salvo que solicite la supresión de las mismas. 	X	

T10 GESTIÓN DE SELECCIÓN DE PERSONAL

TIPOLOGÍA DE DATOS		SÍ	NO
Datos de carácter identificativo.		X	
Categorías especiales de datos.			X
Características personales		X	
Circunstancias sociales			X
Datos académicos y profesionales		X	
Detalles del empleo		X	
Información comercial			X
Datos económicos, financieros y de seguro			X
Transacciones de bienes y servicios			X
COLECTIVOS AFECTADOS		SÍ	NO
Candidatos		X	
Empleados			X
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO (Automatizados/No automatizados)		SÍ	NO
Office 365		X	
Correo electrónico		X	
Equipos informáticos			
Curriculum Vitae en formato papel		X	
FINALIDADES DE TRATAMIENTO		DETALLE	
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000		
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.		
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.		
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).			X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. <input type="checkbox"/> Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.		X
¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?			X

¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?		X
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
– Las distintas áreas del centro.		
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		X
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?		X
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos? (en caso afirmativo detallar cuáles)	X	
– En virtud de la política de conservación del centro, los datos de carácter personal serán conservados durante el plazo máximo de un año desde la recepción de los currículums vitae.	X	

T11 GESTIÓN DE PRÁCTICAS PROFESIONALES

TIPOLOGÍA DE DATOS		SÍ	NO		
Datos de carácter identificativo.		X			
Categorías especiales de datos.			X		
Características personales		X			
Circunstancias sociales			X		
Datos académicos y profesionales		X			
Detalles del empleo			X		
Información comercial			X		
Datos económicos, financieros y de seguro			X		
Transacciones de bienes y servicios			X		
COLECTIVOS AFECTADOS		SÍ	NO		
Miembros del Consejo Escolar			X		
Empleados			X		
Usuarios			X		
Alumnos/as			X		
Personas en prácticas.		X			
SISTEMAS QUE INTERVIENEN EN EL TRATAMIENTO (Automatizados/No automatizados)		SÍ	NO		
Office 365		X			
Correo electrónico		X			
Equipos informáticos		X			
Expedientes en formato papel		X			
FINALIDADES DE TRATAMIENTO		DETALLE		SÍ	NO
¿La recogida de los datos tiene como finalidad el tratamiento a gran escala? El número de sujetos afectados (es decir, cuantos interesados van a ser objeto de este tratamiento).	X de 0 a 10.000 <input type="checkbox"/> de 10.000 a 100.000 <input type="checkbox"/> + de 100.000				
La duración del tratamiento	X Temporal. X Plazo determinado. <input type="checkbox"/> Indefinido.				
La extensión geográfica del tratamiento (Tratamiento a nivel regional (R), nacional (N) o internacional (I))	X Regional. <input type="checkbox"/> Nacional. <input type="checkbox"/> Internacional.				
¿La recogida de los datos tiene como finalidad la monitorización o evaluación sistemática y exhaustiva de aspectos personales? (tratamiento para monitorizar, observar y/o controlar a los interesados, a través del cual, se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas identificadas o identificables).					X
¿La recogida de los datos tiene como finalidad el tratamiento de categorías especiales de datos?	<input type="checkbox"/> Ideología u opiniones políticas. <input type="checkbox"/> Afiliación sindical. <input type="checkbox"/> Convicciones religiosas o filosóficas <input type="checkbox"/> Origen étnico o racial. <input type="checkbox"/> Datos relativos a salud. <input type="checkbox"/> Vida sexual u orientación sexual. <input type="checkbox"/> Datos biométricos. <input type="checkbox"/> Datos genéticos.				X

¿El tratamiento implica un contacto con los interesados de manera que, dicho contacto, pueda resultar intrusivo o se prevé el uso de tecnologías que se pueden percibir como especialmente intrusivas en la privacidad?		X
¿Se van a usar específicamente datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad (p.e.: menores de 14 años, ancianos, personas con riesgo de exclusión social)?		X
¿Se van a tratar datos personales para elaborar perfiles, categorizar/segmentar, hacer ratings/scoring o para la toma de decisiones?		X
¿El tratamiento de los datos implica una toma de decisiones automatizada sin que haya ninguna persona que intervenga en la decisión o valore los resultados?		X
¿Se enriquece la información de los interesados mediante la recogida de nuevas categorías de datos o se usan las existentes con nuevas finalidades que antes no se contemplaban, en particular, si estas finalidades son más intrusivas o inesperadas para los afectados, o incluso pueda llegar a bloquear el disfrute de algún servicio?		X
¿El tratamiento implica que un elevado número de personas tenga acceso a los datos personales tratados?		X
¿Se van a tratar datos relativos a la observación de zonas de acceso público?		X
¿Se utilizan datos de carácter personal no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica?		X
CESIONES DE DATOS Y TRANSFERENCIAS INTERNACIONALES	SÍ	NO
¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuáles)	X	
– Las distintas áreas del centro.		
¿Se realizan transferencias internacionales de datos a países fuera de la Unión Europea y que no cuenten con medidas de protección de datos de carácter personal similares a las establecidas por la Autoridad de Control? (en caso afirmativo detallar cuáles)		
TERCEROS QUE INTERVIENEN EN EL TRATAMIENTO	SÍ	NO
¿Interviene algún proveedor en el proceso?	X	
PLAZOS DE CONSERVACIÓN	SÍ	NO
¿Están definidos plazos de conservación para cada uno de los tratamientos?	X	
– Se conservarán durante el tiempo necesario para cumplir con la finalidad de gestionar las prácticas profesionales del colaborador, así como para determinar las posibles responsabilidades que se pudieran derivar de dicha finalidad y del tratamiento de los datos.	X	

6. ANÁLISIS DE LA NECESIDAD DE REALIZAR UNA EVALUACIÓN DE IMPACTO SOBRE LA PROTECCIÓN DE LOS DATOS

¿Cuándo se debe realizar una EIPD?

Una EIPD no se requiere siempre, sino que, en cada actividad de tratamiento, se debe valorar la necesidad de llevar a cabo la misma. Es fundamental realizar un análisis previo para determinar de forma preliminar el nivel de riesgo al que puede estar expuesto el tratamiento y tomar la decisión adecuada en base a ello.

¿Qué criterios se deben seguir para analizar la necesidad de llevar a cabo o no una EIPD?

Para determinar si es necesario llevar a cabo la EIPD o no, se puede seguir una breve metodología de análisis atendiendo a las listas de tratamientos previstas en los arts. 35.3, 35.4 y 35.5.

Análisis de las listas de tratamientos previstos en la regulación (arts. 35.3, 35.4 y 35.5)

La regulación establece supuestos en los cuales **es obligatorio realizar la EIPD sin necesidad de realizar un análisis de riesgos**, por tanto, la comprobación de las listas y supuestos incluidos en la regulación, debe ser el **primer paso** para determinar la necesidad de llevar a cabo una EIPD.

Para facilitar a los responsables de los tratamientos la identificación de aquellos tratamientos que requieren una EIPD, el RGPD dispone que las autoridades de control deberán publicar una lista con los tratamientos que requieran de una EIPD. Dicha lista deberá ser comunicada al Comité Europeo de Protección de Datos (CEPD).

En el momento de analizar **tratamientos de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la lista expuesta** a continuación, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en **artículo 35.5 del RGPD**. **Cuantos más criterios reúna el tratamiento en cuestión, mayor será el riesgo que entrañe dicho tratamiento y mayor será la certeza de la necesidad de realizar una EIPD.**

Esta lista se basa en los criterios establecidas por el antiguo Grupo de Trabajo del Artículo 29 (actual CEPD) en la guía WP248 “Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD”, los complementa y debe entenderse como **una lista no exhaustiva**.

LISTAS DE TIPOS DE TRATAMIENTOS DE DATOS QUE REQUIEREN EVALUACIÓN DE IMPACTO RELATIVA A PROTECCIÓN DE DATOS (art 35.4)	SI/NO	Código Tratamiento
1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.	NO	
2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.	NO	
3. Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.	NO	
4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.	SÍ	T04 y T08
5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.	NO	
6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.		
7. Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 “Directrices sobre los delegados de protección de datos (DPD)” del Grupo de Trabajo del Artículo 29.	NO	
8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.	NO	
9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.	SÍ	T04, T08
10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.	NO	
11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.	NO	

Por otro lado, el artículo 35.3 recoge tres casos en qué es obligatorio hacer la EIPD:

1. Cuando la finalidad es la **evaluación "sistemática y exhaustiva", de carácter automatizado, de varios aspectos de la persona**, en general cuando se elaboran perfiles y su alcance implica efectos de tipo jurídico, o que pueden afectar significativamente a las personas como consecuencia de la toma de decisiones basadas en la información que se trata.
2. El segundo caso se refiere a la **naturaleza del tratamiento**, si se pretenden tratar a **gran escala categorías especiales de datos** o datos personales relativos a condenas e infracciones penales (más adelante se dan algunas orientaciones respecto del concepto "a gran escala").
3. Para el tercer caso también es de aplicación la idea del **tratamiento a gran escala**, pero vinculado a **"la observación" sistemática de zonas de acceso público**. Tenemos que interpretar el concepto "observación" de manera amplia, como equivalente de "seguimiento"; por lo tanto, no tiene por qué limitarse a los sistemas de videovigilancia, sino que su alcance incluye cualquier tratamiento que implique la monitorización de personas.

CONCLUSIÓN:

Del resultado del análisis a las preguntas anteriormente expuestas atendiendo a la naturaleza, alcance, contexto y fines de cada uno de los tratamientos (art. 35.1) y de su encaje o no en las listas de tratamientos de los artículos 35.3 y 35.4, debe tomarse la decisión sobre la necesidad de realizar una EIPD.

La AEPD considera que **cuando se den dos o más de los criterios** mencionados en las listas expuestas, en un tratamiento u operaciones concretas dentro de un mismo tratamiento, **más probable es que suponga un alto riesgo para los derechos y las libertades de los interesados**.

Sin embargo, el responsable del tratamiento puede considerar que, por la naturaleza, contexto y fines del tratamiento, aunque los tratamientos cumplen varios de los criterios mencionados, realmente no hay un probable alto riesgo. En este caso, hay que documentar y argumentar de forma clara las razones por las que no se lleva a cabo la EIPD.

X NO ES NECESARIO REALIZAR EIPD:

Código	Tratamiento
T01	GESTIÓN COLABORACIÓN VOLUNTARIADO
T02	CONSEJO ESCOLAR
T03	GESTIÓN DE CONTACTOS PROFESIONALES, RRSS Y PÁGINA WEB
T05	SERVICIOS COMPLEMENTARIOS
T06	ACTIVIDADES EXTRAESCOLARES
T07	PROGRAMAS DE INTERCAMBIO
T09	GESTIÓN DE EMPLEADOS, EVALUACIÓN Y PROMOCIÓN
T10	GESTIÓN DE SELECCIÓN DE PERSONAL
T11	GESTIÓN DE PRÁCTICAS PROFESIONALES

El/los tratamientos de **C. NSTR. SÑRA. LOURDES** no encajan en ninguno de los supuestos de la listas expuestas ni puede derivarse de las respuestas a la preguntas formuladas que hay factores suficientes para determinar que, en base al nivel de riesgo derivado de la naturaleza, alcance, contexto y fines de las operaciones de tratamiento de datos personales planteadas por

C. NSTR. SÑRA. LOURDES estén expuestas a riesgos relevantes para los derechos y deberes fundamentales de las personas físicas que motiven la necesidad de realizar una EIPD en profundidad.

X SI ES NECESARIO REALIZAR EIPD:

Código	Tratamiento
T04	GESTIÓN ESCOLAR
T08	DEPARTAMENTO DE ORIENTACIÓN

El/los tratamientos de C. NSTR. SÑRA. LOURDES se incluye en alguna de las listas de los artículos 35.4 y 35.5 y/o de los casos descritos en el 35.3 del RGPD, o bien se deriva de las respuestas a las preguntas formuladas, que hay factores suficientes para determinar que, en base al nivel de riesgo derivado de la naturaleza, alcance, contexto y fines de las operaciones de tratamiento de datos personales planteadas por C. NSTR. SÑRA. LOURDES, estas deben ser objeto de una evaluación de impacto, a fin de valorar la gravedad y probabilidad del alto riesgo que suponen, con el objeto de seleccionar las medidas, garantías y mecanismos más adecuados para mitigar ese riesgo, garantizando la protección de los datos personales.

Por tanto, se recomienda llevar a cabo una evaluación de impacto, en los términos previstos en el RGPD, para las operaciones de tratamiento de C. NSTR. SÑRA. LOURDES.

No obstante, la AEPD ha establecido determinados supuestos en los que no resulta necesario realizar una EIPD, aunque se den al menos dos de los supuestos de estos listados:

- 1. Tratamientos que se realizan estrictamente bajo las directrices establecidas o autorizadas con anterioridad mediante circulares o decisiones emitidas por las Autoridades de Control, en particular la AEPD, siempre y cuando el tratamiento no se haya modificado desde que fue autorizado.*
- 2. Tratamientos que se realizan estrictamente bajo las directrices de códigos de conducta aprobados por la Comisión Europea o las Autoridades de Control, en particular la AEPD, siempre y cuando una EIPD completa haya sido realizada para la validación del código de conducta y el tratamiento se implementa incluyendo las medidas y salvaguardas definidas en la EIPD.*
- 3. Tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.*
- 4. Tratamientos realizados en el ejercicio de su labor profesional por trabajadores autónomos que ejerzan de forma individual, en particular médicos, profesionales de la salud o abogados, sin perjuicio de que pueda requerirse cuando el tratamiento que lleven a cabo cumpla, de forma significativa, con dos o más criterios establecidos en la lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicada por la AEPD.*
- 5. Tratamientos obligatorios por ley y realizados con relación a la gestión interna del personal de las PYMES con finalidad de contabilidad, gestión de recursos humanos y nóminas, seguridad social y salud laboral, pero nunca relativos a los datos de los clientes.*

6. *Tratamientos realizados por comunidades y subcomunidades de propietarios tal como se definen en el artículo 2 (a, b y d) de la Ley 49/1960 de Propiedad Horizontal.*
7. *Tratamientos realizados por colegios profesionales y asociaciones sin ánimo de lucro para la gestión de los datos personales de sus propios asociados y donantes, y en el ejercicio de su labor, siempre que no incluyan en el tratamiento de datos sensibles tales como los que se establecen en el artículo 9.1 del RGPD y no sea de aplicación el artículo 9.2(d) de dicho Reglamento.*

De entre todos los supuestos de excepción planteados, los tratamientos (T03 y T06) se encuadran dentro del **supuesto de excepción número 3**. Por todo lo expuesto se considera que **C. NSTRA. SÑRA. LOURDES** no tiene la necesidad de realizar una EIPD en profundidad.

7. GESTIÓN DE RIESGOS POR DEFECTO

Considerando 74

“...el responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el presente Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.”

Considerando 76

“La probabilidad y la gravedad del riesgo para los derechos y libertades del interesado debe determinarse con referencia a la naturaleza, el alcance, el contexto y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.”.

Considerando 75

Enumera una serie de factores o supuestos asociados a riesgos para los derechos y libertades de los interesados.

Bajo el supuesto de que las actividades de tratamiento no requieren una EIPD, el análisis de riesgos para determinar las medidas técnicas y organizativas que garanticen los derechos y libertades de los interesados se puede simplificar con un enfoque de mínimos considerando que el nivel de riesgo al que están expuestas las actividades de tratamiento no es elevado.

Los principales riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, se pueden diferenciar en 2 dimensiones:

- **Riesgos asociados a la protección de la información** con foco en la integridad, disponibilidad y confidencialidad de los datos.
- **Riesgos asociados al cumplimiento** de los requisitos regulatorios relacionados con los derechos y libertades de los interesados.

En las metodologías de riesgos tradicionales, el proceso de gestión de riesgos se estructura en tres fases diferenciadas:

- Identificación
- Evaluación
- Tratamiento

A partir de la identificación de un riesgo inherente a la actividad de tratamiento de partida, se aplican una serie de medidas de seguridad y se obtiene un riesgo residual.

Sin embargo, el método simplificado propuesto, en base a las dos dimensiones descritas anteriormente, se deben identificar cuáles son los principales riesgos a los que están expuestas las actividades de tratamiento, sin llegar a valorar los riesgos, considerando siempre que el nivel inherente de los mismos será medio o bajo.

RIESGO = PROBABILIDAD × IMPACTO

La probabilidad se determina en base a las posibilidades que existen de que la amenaza se materialice.

Escala de posibles valores para el cálculo de la probabilidad:

Probabilidad despreciable	La posibilidad de ocurrencia es muy baja (por ejemplo, un evento que puede pasar de forma fortuita).
Probabilidad limitada	La posibilidad de ocurrencia es baja (por ejemplo, un evento que puede pasar de forma ocasional).
Probabilidad significativa	La posibilidad de ocurrencia es alta (por ejemplo, un evento que puede pasar con bastante frecuencia).
Probabilidad máxima	La posibilidad de ocurrencia es muy elevada (por ejemplo, un evento cuya ocurrencia se produce con mucha frecuencia).

El impacto se determina en base a los posibles daños que se pueden producir si la amenaza se materializa. De igual modo, el impacto también se evaluará con la misma escala de cuatro valores posibles:

Impacto despreciable	El impacto es muy bajo (por ejemplo, un evento cuyas consecuencias son prácticamente despreciables sin impacto sobre el interesado).
Impacto limitado	El impacto es bajo (por ejemplo, un evento cuyas consecuencias implican un daño menor sin impacto relevante sobre el interesado).
Impacto significativo	El impacto es alto (por ejemplo, un evento cuyas consecuencias implican un daño elevado con impacto sobre el interesado).
Impacto máximo	El impacto es bajo (por ejemplo, un evento cuyas consecuencias implican un daño muy elevado con un impacto crítico sobre el interesado).

Tomando como base las escalas de probabilidad e impacto, para poder determinar el riesgo inherente, es necesario **asignar valores a cada uno de los niveles** de las escalas de probabilidad e impacto. La escala de valores comprende desde el valor 1, en el caso de que la magnitud sea despreciable, hasta el valor 4 en el caso donde la magnitud es máxima:

1. **Despreciable**
2. **Limitado**
3. **Significativo**
4. **Máximo**

Si se establece un valor numérico a la probabilidad y otro valor al impacto, según la escala de valores definida, se obtiene una posición en la matriz de riesgos que se corresponde con el **riesgo inherente**, resultado de aplicar la fórmula de estimación del riesgo. El resultado del riesgo inherente se puede considerar en los siguientes niveles en función del valor obtenido:

Bajo	Si el valor resultante se sitúa entre los valores 1 y 2
Medio	Si el valor resultante es mayor de 2 y menor o igual que 6.
Alto	Si el valor resultante es mayor que 6 y menor o igual que 9.
Muy Alto:	Si el valor resultante es mayor que 9.

Considerando los criterios establecidos, si se deseara valorar un riesgo, por ejemplo, al añadir valores numéricos a la probabilidad y al impacto, ante un riesgo con **probabilidad limitada (2)** e **impacto significativo (3)**, el nivel de riesgo inherente será **medio** ($2 \times 3 = 6$).

PROBABILIDAD	Máxima 4	4	8	12	16
	Significativa 3	3	6	9	12
	Limitada 2	2	4	6	8
	Despreciable 1	1	2	3	

	Despreciable 1	Limitada 2	Significativa 3	Máxima 4
IMPACTO				

■ Bajo ■ Medio ■ Alto ■ Muy Alto

¿Cómo identificar y gestionar los riesgos potenciales asociados a una actividad de tratamiento?

Los riesgos son variables y dependen de las amenazas a las que está expuesta la actividad de tratamiento, por ello, es fundamental disponer de una descripción detallada del tratamiento, de su contexto y de los elementos más relevantes que intervienen en la misma.

El método descrito a continuación, es un método simple que tiene como objetivo facilitar significativamente el proceso de gestión de riesgos para aquellas actividades de tratamiento que están expuestas a un nivel de riesgo medio o bajo y en consecuencia el nivel de riesgo se moverá siempre por debajo del umbral de riesgo elevado y, por tanto, la valoración exacta del nivel de riesgo carece de relevancia.

En cada actividad de tratamiento, se debe analizar y determinar cuáles de los riesgos situados dentro de las **dimensiones de protección de los datos personales y derechos y libertades de los interesados** son de aplicación.

Los **riesgos identificados y las medidas de control definidas deben documentarse**, con el objetivo de evidenciar la evaluación de riesgos realizada y tener una base de trabajo ante futuras revisiones del análisis derivadas de cambios en las actividades de tratamiento.

Atendiendo a la metodología expuesta, a continuación, se indican los criterios de aceptación de riesgos:

- 1) Durante la etapa de evaluación de riesgos se aceptan aquellos riesgos de nivel “Bajo” y “Medio”,
- 2) No se aceptan los riesgos de nivel “Alto” y “Muy Alto” que deberán ser tratados con el fin de mitigarlos, transferirlos o evitarlos.

Monitorización continua

Los riesgos son variables y pueden cambiar ante variaciones en las actividades de tratamiento. Garantizar una adecuada gestión de riesgos requiere la monitorización continua de los riesgos y la evaluación periódica de la efectividad de las medidas de control definidas para mantenernos en un nivel de exposición de riesgo bajo/medio. Se recomienda **revisar el análisis de riesgos** realizado ante cualquier cambio significativo en las actividades de tratamiento que pueda derivar en la aparición de nuevos riesgos.

A continuación, partiendo de los tratamientos llevados a cabo por **C. NSTR. SÑRA. LOURDES** en los que del resultado del análisis de riesgos nos da como resultado que **no es necesario realizar una EIPD**, pasaremos a describir el catálogo de amenazas a las que pueden estar expuestos dichos tratamientos teniendo en cuenta las medidas de seguridad existentes y poder valorar en términos de probabilidad e impacto si es necesario o no llevar a cabo mejoras en las medidas de seguridad actualmente implantadas.

GESTIÓN DE RIESGOS POR DEFECTO	
CÓDIGO	TRATAMIENTOS
T01	GESTIÓN DE COLABORACIÓN VOLUNTARIADO
T02	CONSEJO ESCOLAR
T03	GESTIÓN DE CONTACTOS PROFESIONALES, RRSS Y PÁGINA WEB
T04	GESTIÓN ESCOLAR
T05	SERVICIOS COMPLEMENTARIOS

T06	ACTIVIDADES EXTRAESCOLARES
T07	PROGRAMA INTERCAMBIO
T08	DEPARTAMENTO DE ORIENTACIÓN
T09	GESTIÓN DE EMPLEADOS, EVALUACIÓN Y PROMOCIÓN
T10	GESTIÓN DE SELECCIÓN DE PERSONAL
T11	GESTIÓN DE PRÁCTICAS PROFESIONALES

RIESGOS ASOCIADOS A LA PROTECCIÓN DE LA INFORMACIÓN						
Ref. amenaza	AMENAZAS	MEDIDAS DE SEGURIDAD	CÓDIGO TRATAMIENTO	PA	IM	VALOR DEL RIESGO
1.	Imposibilidad de atribuir a usuarios identificados todas las acciones que se lleven a cabo en un sistema de información.	Existe una relación de usuarios autorizados y perfiles de usuarios en los Anexos I y II del procedimiento interno POL-CONT, en los que se detallan los accesos autorizados para cada usuario. Sin embargo, no se cumple en la actualidad con la Política de contraseñas establecida en el procedimiento, y ello conlleva la posibilidad de que se produzcan accesos sin poder atribuirlos a usuarios identificados.	TODOS	2	3	6
			TODOS	2	3	6
			TODOS	2	3	6
2.	Software malicioso (virus, troyanos, secuestradores de la información).	Todos los usuarios con acceso a datos reciben un Anexo de medidas de seguridad y prohibiciones en el que se le informa, entre otras cuestiones, de que, en el supuesto de detectar una incidencia durante el uso del correo electrónico, el usuario ha de ponerlo en conocimiento del administrador del sistema.	TODOS	1	2	2
3.	Robo o extravío de equipos, soportes o dispositivos con datos personales.	En centro, el acceso a las instalaciones se encuentra protegido mediante llave, tanto en la puerta de entrada principal como en los despachos en los que se encuentran ubicados los sistemas de información. <u>Copias de respaldo</u> Se realizan copias de seguridad de la información en la plataforma de gestión escolar Educamos, por lo que se garantiza la disponibilidad de la información, aunque esta sufra alteraciones. Sin embargo, no se realizan copias de seguridad de la información almacenada en local por parte del centro educativo. <u>Identificación y autenticación</u> Los soportes informáticos del centro no disponen de mecanismos que requieren la identificación del usuario mediante la introducción de una contraseña, impidiendo así el acceso a la información almacenada en los mismos por parte de terceros no autorizados	TODOS	1	2	2
			TODOS	2	3	6
			TODOS	2	3	6
			TODOS	2	3	6
4.	Errores humanos en tareas de mantenimiento.	Se gestiona de manera externa la actualización y mantenimiento de los programas utilizados en los sistemas de información del centro, para que cuenten con las últimas actualizaciones de seguridad, incluyendo mejoras de funcionalidad.	TODOS	1	2	2
5.		<u>Acuerdos de confidencialidad o no divulgación.</u>	TODOS	1	2	2

ANÁLISIS DE RIESGOS - CENTRO NUESTRA SEÑORA LOURDES

	Fuga de empleados: fraude, robos, revelación de información.	Existen documentos que informan a los usuarios del centro acerca de las medidas de seguridad y prohibiciones que les aplican por motivo de las funciones que desempeñan en este.	TODOS	1	2	2
			TODOS	1	2	2
6.	Divulgación no intencionada de información	En dichos compromisos se establece: <i>“Utilizar la información a que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en el centro y no disponer de ella de ninguna otra forma o con otra finalidad. No utilizar en forma alguna cualquier otra información que hubiese podido obtener prevaliéndose de su condición de empleado del centro, y que no sea necesaria para el desempeño de sus funciones en el centro.”</i>	TODOS	1	2	2
			TODOS	1	2	2
			TODOS	1	2	2
			TODOS	2	3	6
			TODOS	2	3	6
7.	Usos de credenciales ajenas	Adicionalmente, se está reforzando la concienciación de los empleados, mediante charlas formativas en materia de protección de datos se produce el uso de credenciales de otros compañeros para acceder a los sistemas de información cuando se requiere por cuestiones de trabajo.	TODOS	2	3	6
8.	Medidas de control de acceso físico (tornos de acceso, rayos x, tarjetas de acceso, etc.) insuficientes o inexistentes.	Los locales del centro disponen de mecanismos que impiden la entrada a personal no autorizado. A mayor abundamiento, la naturaleza del local en el que se ubica la información impide el acceso de personas no autorizadas sin el consentimiento del personal del centro.	TODOS	1	2	2
9.	Catástrofes naturales que afectan a las infraestructuras (inundaciones, huracanes, terremotos, etc.).	<u>Acceso físico</u> Los locales del centro disponen de mecanismos que impiden la entrada a personal no autorizado. A mayor abundamiento, la naturaleza del local en el que se ubican, impide el acceso de personas no autorizadas sin el consentimiento del personal del centro. <u>Copias de seguridad</u> Se realizan copias de seguridad de la información de manera diaria en la plataforma de gestión escolar, por lo que se garantiza la disponibilidad de la información, aunque esta sufra alteraciones. Sin embargo, no se realiza una copia de seguridad de la información almacenada en local.	TODOS	2	2	4
10.	Deficiencias en los protocolos de almacenamiento de datos personales en formato físico.	<u>Seguridad física.</u> La documentación almacenada en formato papel se encuentra ubicada en salas que disponen de mecanismos que obstaculizan su apertura, de igual que se protegen los armarios o archivadores en los que se almacenan. Adicionalmente, y en base a la configuración del centro, no sería posible el acceso a la documentación por personal no autorizado sin ser visto por el personal de administración del centro.	TODOS	1	3	3

| ANÁLISIS DE RIESGOS - CENTRO NUESTRA SEÑORA LOURDES

11.	Destrucción de la información y soportes	La destrucción de cualquier documento o soporte que contiene datos de carácter personal se realiza mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.				
12.	Errores de mantenimiento / actualización de programas (software)	El centro cuenta con los servicios de una empresa externa que actualiza y mantiene los programas utilizados en los sistemas de información para que cuenten con las últimas actualizaciones de seguridad, incluyendo mejoras de funcionalidad.	TODOS	1	2	2

RIESGOS ASOCIADOS AL CUMPLIMIENTO NORMATIVO						
Ref. amenaza	AMENAZAS	MEDIDAS DE SEGURIDAD	CÓDIGO TRATAMIENTO	PA	IM	VALOR DEL RIESGO
LEGITIMACIÓN DE LOS TRATAMIENTOS Y CESIONES DE DATOS PERSONALES						
1.	Tratar datos personales cuando no es necesario para la finalidad perseguida	<p>Los datos que se recaban en el centro son necesarios para las finalidades perseguidas en cada uno de los tratamientos.</p> <p>No obstante, existe la posibilidad de que, por parte del personal del centro, se recabe determinada información que puede llegar a ser excesiva, o incluso ya estar en disposición del centro.</p> <p>Por ello, se refuerza la concienciación por parte del centro, para que cualquier nuevo proyecto con impacto en materia de protección de datos, se ponga en conocimiento de los responsables LOPD.</p>	TODOS	1	3	3
2.	Carecer de una legitimación clara y suficiente para el tratamiento o la cesión de datos personales.	<p>Todos los tratamientos de datos personales se llevan a cabo conforme a alguno de los supuestos del artículo 6 RGPD.</p> <p>Ante nuevos tratamientos, se ha informado al personal de la necesidad de realizar la consulta correspondiente a los responsables LOPD del centro, o en su caso, al Delegado de Protección de Datos.</p>	TODOS	1	2	2
3.	Obtener un consentimiento dudoso, viciado o inválido para el tratamiento o cesión de datos personales.	Cuando la legitimación para el tratamiento de los datos personales es el consentimiento, este se recaba conforme a los criterios del RGPD.	TODOS	1	2	2
			TODOS	1	2	2
			TODOS	1	2	2
4.	Dificultar la revocación del consentimiento o la manifestación de la oposición a un tratamiento o cesión.	Se facilita al interesado la revocación del consentimiento otorgado, por el mismo medio en el que lo otorgó, y se pone a disposición de los interesados en cualquier recogida de información, el contacto para poder ejercitar cualquiera de sus derechos reconocidos en la materia.	TODOS	1	2	2
TRANSFERENCIAS INTERNACIONALES						
5.	Carencia de mecanismos de control de cumplimiento de las garantías establecidas para la transferencia.	<p>No se producen, por parte del centro, transferencias internacionales de datos a países ubicados, en consecuencia, fuera del Espacio Económico Europeo.</p> <p>En caso de realizarlas, sólo se realizarán a entidades que hayan demostrado que cumplen con el nivel de protección y garantías de acuerdo con los parámetros y exigencias previstas en la normativa vigente en materia de protección de datos, como el Reglamento Europeo, o cuando exista una habilitación legal para realizar la transferencia internacional.</p>	TODOS	1	2	2
NOTIFICACIÓN Y REGISTRO DE ACTIVIDADES DE TRATAMIENTO						

ANÁLISIS DE RIESGOS - CENTRO NUESTRA SEÑORA LOURDES

6.	Carecer de los mecanismos y procedimientos necesarios para detectar cuándo debe registrarse la creación, modificación o cancelación de actividades de tratamiento.	Se ha elaborado un Registro de Actividades de Tratamiento, que se actualiza en atención a los cambios que se producen en los tratamientos de datos ya detectados, o ante nuevos tratamientos. En el mismo, se incluye la referencia a una serie de procedimientos internos que se encuentran implementados en el centro.	TODOS	1	1	1
TRANSPARENCIA E INFORMACIÓN						
7.	Recoger datos personales sin proporcionar la debida información o de manera fraudulenta o no autorizada.	La información proporcionada en materia de protección de datos se encuentra redactada de una manera clara, sencilla y transparente, conforme a las exigencias de la normativa. Adicionalmente, y de manera anual, se revisan todas las cláusulas y documentos elaborados en materia de protección de datos del centro en aras de determinar su idoneidad conforme a las exigencias de la normativa vigente en materia de protección de datos.	TODOS	1	1	1
8.	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 hagan muy difícil su acceso conjunto y detallado.	La política de privacidad web se encuentra en un entorno visible y accesible para cualquier usuario que quiera proceder a su revisión.	TODOS	2	2	4
9.	Redactar la información en materia de protección de datos en un lenguaje oscuro e impreciso	La información proporcionada en materia de protección de datos se encuentra redactada de una manera clara, sencilla y transparente, conforme a las exigencias de la normativa.	TODOS	1	1	1
CALIDAD DE LOS DATOS						
10.	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.	El centro cuenta con un procedimiento interno (CON-DAT-01) que recoge: - El deber de custodia de la documentación mientras la misma se está trabajando por parte del centro. - Los plazos de custodia y conservación de la documentación que genera el centro y que contienen datos de carácter personal. No obstante, este procedimiento se encuentra en un estado actualizable.	TODOS	2	1	2
CATEGORÍAS ESPECIALES DE DATOS						
11.	Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando éste sea la causa que legitima su tratamiento o cesión.	El centro tiene establecidos procedimientos que garantizan la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él. El centro ha nombrado a PRODACYL SLU como Delegado de Protección de datos, conforme a lo establecido en el artículo 34 de la Ley Orgánica Española en materia de protección de datos y garantía de los derechos digitales.	TODOS	1	2	2
12.	Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de categorías especiales.		TODOS	1	1	1

ANÁLISIS DE RIESGOS - CENTRO NUESTRA SEÑORA LOURDES

		Esta figura se encarga de revisar que las habilitaciones legales sean las adecuadas e idóneas para cada uno de los tratamientos efectuados por el centro, incluidos los que conlleva el tratamiento de datos especialmente protegidos.				
DEBER DE SECRETO						
13.	Accesos no autorizados a datos personales.	Se entrega a los empleados y colaboradores que comienzan a desempeñar sus funciones en el centro, un compromiso de confidencialidad que contempla entre otras cuestiones, el deber de secreto al que están sujetos todos aquellos que, en el desempeño de sus funciones, accedan a datos responsabilidad del centro, indicando, asimismo, las consecuencias que el incumplimiento de este deber podría acarrear. Así, es un paso imprescindible, toda vez que entra un nuevo empleado o colaborador del centro, la firma del compromiso que corresponda a su categoría profesional.	TODOS	2	2	4
14.	Violaciones de la confidencialidad de los datos personales por parte de los empleados de la organización.	Adicionalmente se está trabajando en la concienciación de los empleados con formaciones en materia de protección de datos. Entre otras cuestiones, se informa a los trabajadores de los procedimientos internos que rigen en esta materia, mediante su explicación en claustro, estando siempre a su disposición para su consulta en un área interna.	TODOS	1	2	2
TRATAMIENTOS POR ENCARGO						
15.	Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.	El centro tiene establecido un procedimiento (SEL-ET) que garantiza que siempre que se recurre a un encargado de tratamiento se firma el correspondiente contrato en los términos establecidos por la legislación de protección de datos. El centro selecciona encargados de tratamiento que proporcionen garantías suficientes de cumplimiento de los contratos y de la adopción de las medidas de seguridad estipuladas a través, por ejemplo, de su adhesión a posibles códigos de conducta o a esquemas de certificación homologados y de acreditada solvencia. Existen contratos de encargo de tratamiento con los proveedores del centro. Dichos contratos incluyen: - Las pautas que deben regir el servicio y que garantice el correcto cumplimiento de las instrucciones del responsable y la adopción de las medidas de seguridad adecuadas. - La obligación de comunicar al responsable las peticiones de ejercicio de los derechos de los interesados a través de los datos de contacto que el centro ha dispuesto al efecto.	TODOS	2	2	4
16.	Falta de diligencia (o dificultad para demostrarla) en la elección de encargado de tratamiento.		TODOS	1	2	2

| ANÁLISIS DE RIESGOS - CENTRO NUESTRA SEÑORA LOURDES

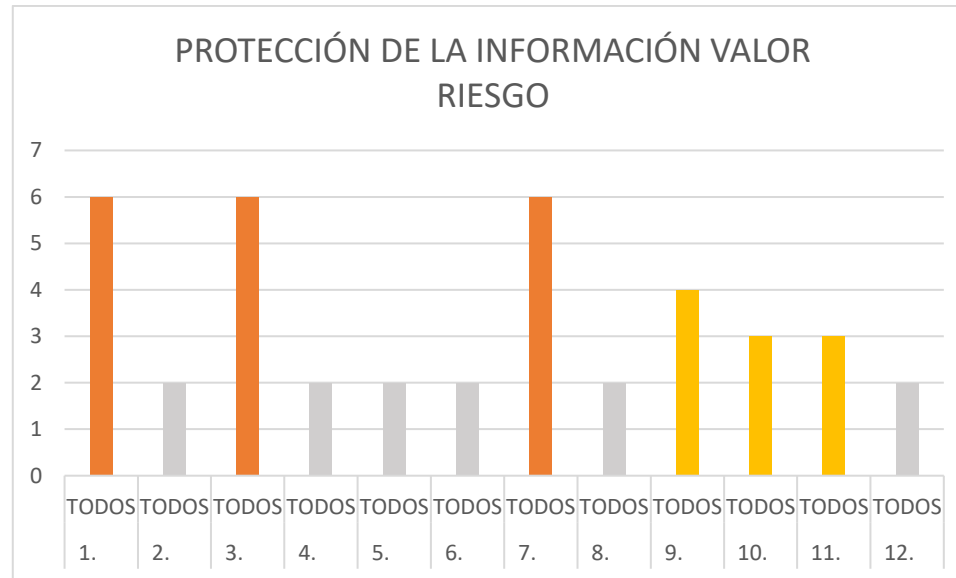
DERECHOS DE LOS INTERESADOS						
17.	Dificultar o imposibilitar el ejercicio de los derechos de los interesados.	Existe un procedimiento interno de actuación ante las solicitudes de ejercicio de derechos (ARSO-POL), que tiene por objeto facilitar a los interesados el ejercicio de sus derechos, poniendo para ello a su disposición los modelos de ejercicio de derechos de acceso, rectificación, supresión (derecho al olvido), limitación del tratamiento, portabilidad y oposición.	TODOS	1	2	2

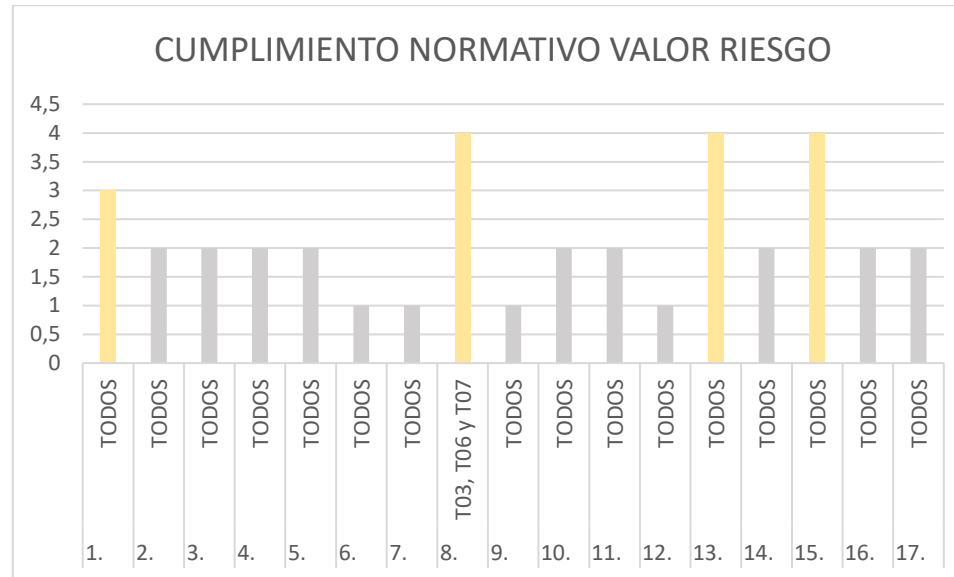
8. VALORES DEL RIESGO POR TRATAMIENTO

PROTECCIÓN DE LA INFORMACIÓN		
Ref. amenaza	OPERACIÓN DE TRATAMIENTO	VALOR RIESGO
1.	TODOS	6
2.	TODOS	2
3.	TODOS	6
4.	TODOS	2
5.	TODOS	2
6.	TODOS	2
7.	TODOS	6
8.	TODOS	2
9.	TODOS	4
10.	TODOS	3
11.	TODOS	3
12.	TODOS	2

CUMPLIMIENTO NORMATIVO		
Ref. amenaza	OPERACIÓN DE TRATAMIENTO	VALOR RIESGO
1.	TODOS	3
2.	TODOS	2
3.	TODOS	2
4.	TODOS	2
5.	TODOS	2
6.	TODOS	1
7.	TODOS	1
8.	T03, T06 y T07	4
9.	TODOS	1
10.	TODOS	2
11.	TODOS	2
12.	TODOS	1
13.	TODOS	4
14.	TODOS	2
15.	TODOS	4
16.	TODOS	2
17.	TODOS	2

9. GRÁFICOS





10. RESUMEN EJECUTIVO.

Realizada la evaluación de riesgos, y tras haber detectado determinados riesgos que, aun siendo aceptables, conviene tratar para reducir el nivel obtenido a uno más bajo, se recoge a continuación el conjunto de salvaguardas adicionales que el centro puede implementar.

Las salvaguardas se establecen principalmente por cuatro posibles causas:

1. Necesidad de reducir el riesgo residual asociado a alguna de las amenazas identificadas a niveles aceptables, por ser considerados actualmente “Altos” o “Muy altos”.
2. A criterio del responsable del tratamiento, como parte de los procesos de mejora
3. continua, o por considerarlo oportuno.
4. Necesidad de adoptar medidas mitigantes adicionales como fruto de cambios previstos en el ciclo de vida del tratamiento.
5. Aplicación de medidas adicionales como buenas prácticas que contribuyan a mejorar el nivel de protección general de los datos de carácter personal.

Amenaza	Tratamiento afectado	Salvaguarda	Fecha prevista
Imposibilidad de atribuir a usuarios identificados todas las acciones que se lleven a cabo en un sistema de información.	TODOS	<p>Debe existir una relación de usuarios autorizados y perfiles de usuarios en los Anexos I y II del procedimiento interno POL-CONT, en los que se detallan los accesos autorizados para cada usuario.</p> <p>SE HA CREADO UN PERFIL: ALUMNO, PADRE, ADMIN. Y SUPERVISOR.</p>	En los próximos 3 meses

<p>Robo o extravío de equipos, soportes o dispositivos con datos personales.</p>	<p>TODOS</p>	<p><u>Copias de respaldo</u> Se realizan copias de seguridad de la información en la plataforma de gestión escolar Educamos, por lo que se garantiza la disponibilidad de la información, aunque esta sufra alteraciones. Sin embargo, se recomienda realizar una copia de seguridad alternativa en local y/o en la nube de manera independiente por parte del centro educativo.</p> <p><u>Identificación y autenticación</u> Los soportes informáticos del centro deben disponer de un sistema de requerimiento de identificación del usuario mediante la introducción de una contraseña, impidiendo así el acceso a la información almacenada en los mismos por parte de terceros no autorizados y la correspondiente diferenciación de las sesiones por perfiles y usuarios.</p>	<p>En los próximos 3 meses</p>
<p>Uso de credenciales ajenas.</p>	<p>TODOS</p>	<p><u>Acuerdos de confidencialidad o no divulgación.</u> Existen documentos que informan a los usuarios del centro acerca de las medidas de seguridad y prohibiciones que les aplican por motivo de las funciones que desempeñan en este. En dichos compromisos se establece: <i>“Utilizar la información a que alude el apartado anterior únicamente en la forma que exija el desempeño de sus funciones en el centro y no disponer de ella de ninguna otra forma o con otra finalidad. No utilizar en forma alguna cualquier otra información que hubiese podido obtener prevaliéndose de su condición de empleado del centro, y que no sea necesaria para el desempeño de sus funciones en el centro.”</i> Adicionalmente, se debe reforzar la concienciación de los empleados, mediante charlas formativas en materia de protección de datos se produce el uso de credenciales de otros compañeros para acceder a los sistemas de información cuando se requiere por cuestiones de trabajo. Se debe establecer una limitación del acceso por usuarios no autorizados a través del uso de credenciales ajenas,</p>	<p>En los próximos 3 meses</p>

		con el objetivo de que cada usuario acceda con sus propias claves de acceso, exclusivamente, a los datos personales estrictamente necesarios para el desempeño de su función profesional.	
Seguridad física de la información que incluye datos personales.	TODOS	Reforzar las medidas de seguridad relativas al archivo de la documentación, tanto del departamento de administración, profesorado y orientación psicopedagógica para que solo el personal autorizado acceda a la documentación que necesita para el desempeño de su labor profesional.	En los próximos 3 meses
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 hagan muy difícil su acceso conjunto y detallado.	T 03, T06 y T07	Actualizar el contenido de la página web con la información normativa reportada por el departamento de consultoría (certificado SSL, cuadro informativo de cookies RGPD y política de privacidad).	30-45 días

Inexistencia de contrato o elaboración de un contrato incorrecto que no refleje todos los apartados necesarios y las garantías adecuadas.	T03, T05, T06, T07 y T11	Firmar el contrato de protección de datos con los proveedores que tengan acceso a datos personales titularidad del centro.	30-45 días
---	--------------------------	--	------------

11. CONCLUSIONES

En el presente Análisis de Riesgos, se ha explicado la metodología aplicada para analizar y determinar el riesgo en términos de probabilidad y de gravedad al que se expone las operaciones de tratamiento llevadas a cabo por **C. NSTRA. SÑRA. LOURDES**.

En una primera fase de análisis sobre la necesidad de realizar una Evaluación de Impacto sobre protección de datos, se ha detectado que algunos de los tratamientos en los que se realice el tratamiento de categorías especiales de datos de colectivos vulnerables, como es el caso de los menores de 14 años, al incluirse en las listas de los **artículos 35.4 y 35.5** y derivarse de las respuestas a las preguntas formuladas, que hay factores suficientes para determinar que, en base al nivel de riesgo derivado de la naturaleza, alcance, contexto y fines de esta operación de tratamiento de datos personales, debe ser objeto de una evaluación de impacto, a fin de valorar la gravedad y probabilidad del alto riesgo que supone, con el objeto de seleccionar las medidas, garantías y mecanismos más adecuados para mitigar ese riesgo, garantizando la protección de los datos personales.

No obstante, se determinó que dichos tratamientos se encontraban dentro de los supuestos de exclusión que, la propia AEPD, publicó. Todo ello por tratarse de tratamientos que sean necesarios para el cumplimiento de una obligación legal, cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, siempre que en el mismo mandato legal no se obligue a realizar una EIPD, y siempre y cuando ya se haya realizado una EIPD completa.

En la segunda fase de este análisis, en la que se realiza una gestión de riesgos por defecto, para cada una de las amenazas expuestas, se han tenido en cuenta las medidas de seguridad ya implementadas por el **C. NSTRA. SÑRA. LOURDES**, para cada uno de los tratamientos.

Atendiendo a los resultados obtenidos podemos concluir que el nivel del riesgo para las operaciones de tratamiento del **C. NSTRA. SÑRA. LOURDES** se sitúan dentro de un rango **ACEPTABLE** para los derechos y libertades de los interesados, puesto que los datos se están tratando en unas condiciones de riesgos razonablemente controlados. Sin embargo, debemos estar atentos a posibles variaciones de este riesgo y revisar la eficacia de las medidas implantadas, principalmente en los supuestos en los que el nivel de riesgo alcanza un valor medio

En cualquier caso, se recomienda aplicar las salvaguardas reflejadas en el Plan de acción que se incluye en este Análisis, con el fin de minimizar algunos riesgos que, aun siendo aceptables, se encuentra en un nivel medio.

En Burgos, a 28 de noviembre de 2022.

Dar de alta en el portal y subir toda la doc. Actualizada. Confirmar contratos con proveedores y actualizar página web.