UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Escuela Técnica Superior de Ingeniería Informática

Guia para el responsable del tratamiento de datos en colegios

Trabajo Fin de Grado

Grado en Ingeniería Informática

AUTOR/A: Perez Galiana, Josep

Tutor/a: Oltra Gutiérrez, Juan Vicente

CURSO ACADÉMICO: 2022/2023

Escola Tècnica Superior d'Enginyeria Informàtica
Universitat Politècnica de València

Guía para el responsable de tratamiento de datos en colegios

Trabajo Fin de Grado

Grado en Ingeniería Informática

Autor: Josep Pérez Galiana

Tutor: Juan Vicente Oltra

4º Curso

Resumen

Este manual proporciona una orientación integral para los responsables del tratamiento de datos en instituciones educativas, abarcando todo, desde ideas básicas de protección de datos hasta sofisticados procedimientos de seguridad y cumplimiento legal. Esta guía tiene como objetivo proporcionar a los profesionales el conocimiento y los recursos necesarios para gestionar los datos personales de manera responsable y garantizar la privacidad de los estudiantes, profesores y personal escolar a través de ejemplos del mundo real y directrices concisas

Palabras clave: Responsable de Datos, Protección de Datos, LOPD (Ley Orgánica de Protección de Datos), RGPD (Reglamento General de Protección de Datos), Colegios, Tratamiento de Datos, Privacidad, Consentimiento, Políticas de Protección de Datos, Derechos de Protección de Datos, Seguridad de Datos, Cumplimiento Legal, Datos Personales, Auditorías de Protección de Datos, Normativa

Abstract

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed nisi turpis, iaculis a pulvinar quis, luctus et lorem. Vestibulum ante ipsum primis in faucibus orci luctus et ultrices posuere cubilia Curae; Nullam vitae purus eros, id auctor dolor. Sed et nisl quis nibh fermentum cursus ut at elit. Etiam condimentum porta leo quis tempor. Quisque commodo lobortis aliquet. Etiam tincidunt, libero ut vehicula euismod, justo augue lobortis sem, et facilisis velit lacus tristique dolor.

Keywords : integer, blandit, pharetra, urna, id.

Tabla de contenidos

1. Introducción

En la era de la tecnología de la información la toma de decisiones junto con la recopilación, la gestión y el análisis de datos juegan un papel vital en varias industrias, incluida la educación. En el entorno escolar, el papel del responsable del tratamiento de datos se ha vuelto fundamental para garantizar que las instituciones educativas puedan hacer un uso completo de la información disponible para mejorar la eficacia de la enseñanza, el aprendizaje y la administración. Los profesionales de datos escolares son responsables de recopilar, organizar y analizar una variedad de datos relacionados con el rendimiento académico, la asistencia, el comportamiento de los estudiantes y otros aspectos relacionados. Estos datos no solo pueden ayudar a los educadores y administradores a comprender mejor el progreso de los estudiantes, sino que también pueden ayudar a identificar patrones y tendencias que se pueden usar para implementar estrategias educativas más efectivas y personalizadas.

Además de trabajar con datos de estudiantes, los responsables del tratamiento de datos pueden trabajar con profesores y equipos administrativos para analizar la efectividad de los cursos, evaluar la eficiencia de los recursos de enseñanza y medir el impacto de las iniciativas de enseñanza. A través de un enfoque basado en datos, busca mejorar continuamente el proceso educativo y brindar a los estudiantes un entorno de aprendizaje más rico.

La ética y la privacidad son partes importantes del trabajo de los profesionales de datos en entornos escolares. Es imperativo garantizar que los datos se recopilen y almacenen de manera segura y que se respeten las leyes y reglamentos relacionados con la privacidad de los estudiantes y educadores. Además, los profesionales de datos deben poder comunicar de manera clara y efectiva los hallazgos y las recomendaciones a los educadores y administradores para impulsar mejoras tangibles en el sistema educativo.

En conclusión, el papel de los responsables del tratamiento de datos en los entornos escolares es fundamental para llevar la educación al siguiente nivel mediante el uso estratégico de los datos. Al aprovechar la información disponible, estos profesionales contribuyen a desarrollar estrategias educativas más efectivas, personalizar el aprendizaje y mejorar continuamente la calidad de la educación en las escuelas.

2. Análisis Del Problema

La protección de datos y la privacidad son ahora cruciales en un mundo que se está volviendo cada vez más digital y donde los datos de carácter personal se han convertido en un activo invaluable. En esta situación, es crucial que las instituciones educativas, como las escuelas, garanticen que la información personal de los estudiantes, profesorado, padres y miembros del personal se maneje de manera ética, segura y de acuerdo con todas las leyes de protección de datos que se aplican.

Un colegio necesita urgentemente crear un guía para responsable el del tratamiento de datos. La guía sienta una base sólida para el futuro y al mismo tiempo intenta abordar los problemas actuales de gestión de datos. La guía se convierte en una herramienta esencial para garantizar la confianza y la integridad en el manejo de datos en un entorno educativo al abordar cuestiones como la falta de conciencia, los riesgos de seguridad y el incumplimiento legal.

Imaginemos un entorno en el que todos los miembros de la comunidad educativa, desde los estudiantes más jóvenes hasta los padres y el personal, sean plenamente conscientes de cómo se recopilan, almacenan y utilizan sus datos personales. Imagine un entorno en el que las políticas y procedimientos internos sean transparentes y coherentes en todos los departamentos, lo que se traducirá en un manejo de datos coherente y responsable. Al hacer esto, reduce el riesgo de infringir la ley y pagar una multa y, al mismo tiempo, establece una buena reputación en materia de protección de la privacidad.

Además de discutir temas legales y de seguridad, la guía informa a la comunidad académica sobre el valor de la privacidad de los datos y sus propios derechos con respecto a sus propios datos personales. Esta apertura y transparencia fomentan una cultura de responsabilidad compartida y confianza mutua.

Una inversión en el desarrollo de una guía del responsable del tratamiento de datos es una inversión en la excelencia académica y el bienestar de todas las partes. Una comunidad educativa exitosa se basa en la confianza, razón por la cual protegemos no solo los datos sino también los valores, la ética y otros principios importantes. La escuela expresa su dedicación a defender la seguridad y privacidad de todos mediante la implementación de estrictas prácticas de protección de datos. El manual sirve como catalizador para un futuro de gestión de datos en la educación que sea más seguro y confiable.

3. Objetivo De La Guía

Con el fin de garantizar el estricto cumplimiento de las leyes de protección de datos y promover una gestión responsable y segura de la información personal en el entorno educativo, este proyecto pretende proporcionar una guía exhaustiva y útil para los responsables del tratamiento de datos en las escuelas. Con el objetivo de facilitar la comprensión y aplicación de buenas prácticas en el tratamiento de datos personales en las escuelas, esta guía cubre desde ideas fundamentales hasta medidas específicas de cumplimiento legal, seguridad de datos y protección de la privacidad.

Esta guía tiene como objetivo capacitar a los responsables del tratamiento de datos para que adopten un enfoque proactivo y moral en la gestión de datos, fortaleciendo la confianza en la comunidad educativa y ayudando a cumplir con las leyes de protección de datos y la privacidad de los estudiantes, profesores y personal escolar. Lo logra mediante el uso de ejemplos del mundo real, sugerencias útiles y pautas claras.

Esta guía tiene varios propósitos fundamentales:

- Cumplimiento Legal: Las leyes y regulaciones de protección de datos, como el RGPD y la LOPD, establecen obligaciones legales que los colegios deben seguir al tratar datos personales. La guía tiene como objetivo asegurarse de que la persona responsable comprenda y cumpla con estas leyes para evitar posibles sanciones y consecuencias legales.

- Protección de la Privacidad: La guía ayuda a garantizar que los datos personales de estudiantes, profesores, personal administrativo y otros miembros de la comunidad escolar se traten de manera respetuosa y se proteja su privacidad. Esto es fundamental para construir y mantener la confianza de los interesados.

- Gestión Eficiente de Datos: Proporciona directrices sobre cómo recopilar, almacenar, procesar y utilizar los datos de manera eficiente y segura. Esto puede incluir mejores prácticas para la gestión de registros, la implementación de medidas de seguridad y la reducción de riesgos de violaciones de seguridad.

- Transparencia y Comunicación: La guía promueve la transparencia al establecer procedimientos claros para informar a los interesados sobre cómo se utilizan sus datos, qué derechos tienen y cómo pueden ejercer esos derechos. Esto es esencial para construir una relación de confianza con la comunidad escolar.

- Responsabilidad y Coherencia: La guía establece roles y responsabilidades claros en relación con el tratamiento de datos. Esto ayuda a asegurarse de que todas las personas involucradas entiendan sus funciones y se tomen decisiones coherentes en toda la institución.

- Prevención de Riesgos: Proporciona pautas para identificar y abordar posibles riesgos y problemas relacionados con el tratamiento de datos, como la seguridad de la información y la prevención de incidentes de seguridad.

- Adaptación a Cambios Legales: Las regulaciones de protección de datos pueden cambiar con el tiempo. La guía puede ayudar a mantenerse actualizado con los cambios y adaptar las prácticas de tratamiento de datos en consecuencia.

- Fomento de la Cultura de Protección de Datos: La guía contribuye a fomentar una cultura de protección de datos en el colegio, donde todos los miembros de la comunidad escolar entiendan la importancia de la privacidad y la seguridad de los datos.

Muchos de estos conceptos los veremos repetidos a través de la guía para enfatizar que se visualicen correctamente y se entienden. Lo primero que comprobaremos y conoceremos son los aspectos básicos sobre el tratamiento de datos y luego desarrollaremos una guía completa sobre los usos y las pautas que debe usar un responsable de tratamiento de datos para el correcto cumplimiento de las normativas.

4. Ley de Datos

4.1. ¿Las leyes intervienen en el tratamiento de estos datos?

Sí, tanto la LOPD (Ley Orgánica de Protección de Datos) como el RGPD (Reglamento General de Protección de Datos) son normas relacionadas con la recogida y gestión de datos en las instituciones educativas y otros ámbitos. Estas regulaciones establecen pautas y requisitos para garantizar la privacidad y protección de los datos personales de las personas, incluidos estudiantes, maestros y administradores escolares.

LOPD (Ley Orgánica de Protección de Datos): La LOPD es un estatuto español que establece normas para la protección de datos personales y garantías del derecho a la intimidad de las personas. La ley tiene implicaciones directas para la recopilación, el almacenamiento y el procesamiento de datos por parte de entidades educativas como las escuelas. Los centros educativos deben adherirse a los principios de la LOPD para garantizar que los datos personales se traten de forma adecuada y respetuosa de los derechos de las personas.[1]

RGPD (Reglamento general de protección de datos): RGPD es un reglamento de la UE que se aplica en toda la Unión Europea y establece estándares más estrictos para proteger los datos personales. Si bien es más amplio que la LOPD, también es relevante para la gestión de datos en las escuelas y otras instituciones educativas. Si las escuelas procesan datos de personas en la UE (como estudiantes de intercambio), deben cumplir con el RGPD independientemente de su ubicación geográfica.

LOE (Ley Orgánica de Educación): La Ley Orgánica de Educación (LOE), promulgada en 2006 en España, no trata específicamente sobre el tratamiento de datos en los colegios. La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) de 1999, entonces vigente, trataba fundamentalmente de las normas que regulaban la protección de datos personales. Pero es fundamental tener en cuenta que la LOE crea un marco regulatorio para el sistema educativo. La LOPD y su normativa de desarrollo establecen requisitos legales en materia de protección de datos y, en consecuencia, el tratamiento de datos en los centros educativos debe ajustarse a dichas normas.

El Reglamento General de Protección de Datos (RGPD), que sustituyó a la LOPD en España y en todos los demás Estados miembros de la UE, entró en vigor por la UE en 2018. El RGPD establece un marco más amplio y estricto para la protección de datos personales y es aplicable a todas las organizaciones, incluidas las instituciones educativas, que manejan datos personales de ciudadanos de la UE.

Como resultado, aunque la LOE no aborda específicamente cómo se procesan los datos en las escuelas, aún deben cumplir con las leyes de protección de datos del RGPD, cualquier ley nacional aplicable y cualquier otra ley local aplicable. En España es autonómico o regional. Esto sugiere que, de acuerdo con las normas actuales de protección de datos, las escuelas deben establecer procedimientos y políticas que garanticen la seguridad y privacidad de la información personal de los estudiantes, padres, profesores y miembros del personal.

En cuanto a las escuelas, tanto la LOPD como el RGPD exigen que las instituciones educativas tomen medidas para garantizar que los datos personales se recopilen y procesen de forma segura, informen a las personas sobre cómo se utilizarán sus datos y respeten sus derechos. Sus datos personales. Esto incluye obtener el consentimiento cuando sea necesario, implementar las medidas de seguridad adecuadas y tener procedimientos claros en caso de una violación de datos.

Para garantizar el correcto cumplimiento de la LOPD y el RGPD en todas las actividades relacionadas con la gestión de datos en la institución educativa, es fundamental que un profesional de datos que trabaje en una escuela conozca esta normativa y colabore con el personal jurídico y administrativo.

4.2. ¿Por qué se desarrollaron leyes para el trato y la protección de los datos de las personas?

La LOPD (Ley Orgánica de Protección de Datos) y el RGPD (Reglamento General de Protección de Datos) se desarrollaron para establecer un marco legal sólido y coherente que salvaguarde los derechos y la privacidad de las personas en relación con el tratamiento de sus datos personales en la era digital. Ambas leyes están destinadas a abordar las dificultades y los peligros que conlleva un mundo en el que la recopilación, el procesamiento y el intercambio de datos son comunes.

Ley Orgánica de Protección de Datos (LOPD):

Con el fin de controlar y proteger los derechos fundamentales de las personas en relación con el tratamiento de sus datos personales, se establece la LOPD de España. Fue adoptado por primera vez en 1999 y posteriormente revisado en 2018 para cumplir con el RGPD de la UE. La LOPD establece los deberes y derechos de los responsables y encargados del tratamiento, así como las precauciones de seguridad que deben adoptarse para salvaguardar los datos de carácter personal y las sanciones en caso de incumplimiento.

Reglamento General de Protección de Datos (RGPD):

La Directiva de Protección de Datos de la Unión Europea fue reemplazada por el RGPD, que entró en vigor en mayo de 2018. Sus objetivos son crear un marco de protección de datos uniforme para toda la Unión Europea y brindar a los usuarios y ciudadanos un mayor control sobre sus datos personales. El RGPD establece estándares más estrictos para el consentimiento, la apertura y la responsabilidad de las empresas que manejan datos personales. Además, establece sanciones más estrictas para las infracciones y otorga a las personas un mayor control sobre sus datos.

Estas leyes se establecieron por las siguientes razones principales:

- Protección de la privacidad: a medida que aumenta la conectividad y la digitalización, los datos personales son más susceptibles de abuso y explotación. Las leyes de protección de datos tienen como objetivo salvaguardar el derecho de las personas a la privacidad y el control sobre sus datos personales.

- Globalización: las leyes de protección de datos son cruciales en un mundo interconectado para garantizar que los datos personales se manejen de manera consistente y segura en todas las jurisdicciones relevantes.

- Desarrollos tecnológicos: se recopilan y analizan más datos como resultado de los avances tecnológicos. Las leyes de protección de datos funcionan para garantizar que las tecnologías contemporáneas se utilicen moral y legalmente.

- Transparencia y confianza: las leyes de protección de datos fomentan la transparencia en la recopilación y el uso de datos personales, lo que refuerza la confianza de las personas en las empresas y en línea.

- Derechos de las personas: las leyes de protección de datos otorgan a las personas poder sobre sus datos personales al otorgarles derechos como el derecho de acceso, rectificación, eliminación y portabilidad.

5. Conceptos Básicos del Tratamiento y Protección de Datos

Para que el responsable de los datos del centro educativo conciba todo lo descrito en la guía debemos dar unos toques de conceptos básicos sobre el tratamiento y la protección de los datos, donde se legitiman, quien se responsabiliza de ellos y quien se encarga de tratarlos.

Primero de todo, se debe entender que el tratamiento de los datos es un proceso inherente con el sistema educativo, lo que implica: recopilar, almacenar, procesar, usar y divulgar datos personales y confidenciales sobre individuos. Se refiere a todas las operaciones que involucran el manejo y manipulación de información perteneciente a estudiantes, docentes, personal de apoyo, padres de familia y demás actores del sistema educativo.

La administración de la enseñanza y el aprendizaje, la interacción con los padres y tutores, la gestión de los recursos humanos, la planificación del plan de estudios y el control de la seguridad son solo algunos de los muchos propósitos para los que el sistema educativo recopila y utiliza datos. Se puede incluir información personal como nombres, direcciones, números de teléfono, correos electrónicos, fechas de nacimiento y datos académicos, médicos y de comportamiento.

Entre las formas en que se realiza el procesamiento de datos en el sistema educativo se encuentran:

- Mantener bajo estricta vigilancia y protección todo dato de carácter personal relacionado con las personas del centro educativo.

- Expediente académico: La recopilación y el mantenimiento de los expedientes de las calificaciones, la asistencia y el rendimiento académico de los estudiantes.

- Mantener a los padres informados sobre el progreso académico y los eventos escolares implica el uso de información de contacto.

- Para administrar la nómina y los recursos humanos, la administración de personal recopila información de los maestros y el personal de apoyo.

- La planificación del plan de estudios implica el uso de datos para crear planes de lecciones y programas educativos.

- Implementación de sistemas de video vigilancia para seguridad y administración del campus.

- Actividades extracurriculares: registro y planificación de actividades extracurriculares, incluidas excursiones y eventos patrocinados por la escuela.

- Gestión de eventos: La planificación de encuentros, reuniones y conferencias en el sector académico.

- Apoyo a la toma de decisiones: el uso de datos para detectar tendencias y patrones que pueden mejorar la eficiencia de la instrucción y la administración escolar.

Dado que el sistema educativo maneja una gran cantidad de datos delicados y privados, es esencial asegurarse de que el procesamiento de estos datos se realice de manera moral, legal y segura. La LOPD y el RGPD, entre otras leyes y normativas de protección de datos, tienen por objeto garantizar que los datos de las personas se utilicen de forma adecuada y que se respeten sus derechos y privacidad durante todo el proceso.

5.1. ¿Qué es un dato de carácter personal?

Un dato de carácter personal es lo que permite identificar de forma directa o indirecta a una persona física. Esto cubre una amplia gama de información sobre la identidad de una persona, rasgos personales, circunstancias familiares, sociales, profesionales y económicas. Nombres, direcciones, números de teléfono, direcciones de correo electrónico, grabaciones de voz, ubicaciones de GPS, números de identificación, fotos, grabaciones de voz, datos médicos, datos financieros, etc...

La capacidad que tienen estos datos para identificar a una persona es lo que las acentúa como datos personales. Aunque exista una parte de la información que no sea peculiarmente personal, puede ser decisiva para poder identificar a una persona especifica.

La LOPD y la RGPD están diseñadas para garantizar que los datos personales se manejen de forma correcta y que las personas físicas tengan control sobre cómo se van a usar sus datos personales.

Dentro de los datos de categoría personal existen datos que deben ser especialmente protegidos debido a que podrían llegar a ser más sensibles que el resto de la información personal y más íntima relacionada con las personas físicas. Aparte, se deben adoptar medidas organizativas y técnicas de forma que se pueda evitar que el tratamiento de estos datos pueda provocar fracturas en los derechos y libertades de las personas afectadas

- Datos que revelen ideologías, afiliaciones, religión o creencias.
- Datos que hagan alusión al origen de la persona, a su vida sexual y principalmente, a su salud.
- Datos que den firmeza sobre haber cometido infracciones: ya sean del tipo administrativo o penal.
- Datos genéticos y biométricos.

Es frecuente dentro del ámbito educativo, que los datos referentes a la salud, tanto físicos o mentales sean tratados junto con la prestación de servicios sanitarios que permitan revelar los datos sobre el estado de salud de los alumnos.

5.2. ¿A quiénes pertenecen estos datos de carácter personal?

Los datos de carácter personal pertenecen exclusivamente a la persona física a la que está relacionada la información. Esto quiere decir que la persona de la fueron recopilados los datos es la titular de los datos y tiene cierto control y derechos sobre cómo se usan y tratan.

Tanto la Ley Orgánica de Protección de Datos (LOPD) como el Reglamento General de Protección de Datos (RGPD) reconocen y garantizan los derechos de las personas sobre sus datos personales. Estos derechos incluyen:

- Derecho de Acceso: Las personas tienen el derecho de obtener información sobre si sus datos personales están siendo tratados y, en su caso, acceder a esos datos.

- Derecho de Rectificación: Las personas pueden solicitar la corrección de datos inexactos o incompletos.

- Derecho de Supresión (Derecho al Olvido): Las personas pueden solicitar la eliminación de sus datos personales en ciertas circunstancias, como cuando ya no son necesarios para los fines para los que fueron recopilados.

- Derecho a la Limitación del Tratamiento: Las personas pueden solicitar que se limite el procesamiento de sus datos en situaciones específicas, como durante la resolución de disputas sobre la exactitud de los datos.

- Derecho a la Portabilidad de Datos: Las personas pueden solicitar una copia de sus datos en un formato estructurado y de uso común para transferirlos a otro responsable del tratamiento.

- Derecho de Oposición: Las personas tienen el derecho de oponerse al procesamiento de sus datos en ciertas circunstancias, como el procesamiento con fines de marketing directo.

- Derecho a Retirar el Consentimiento: Si el tratamiento se basa en el consentimiento, las personas pueden retirar su consentimiento en cualquier momento.

- Derechos Relacionados con Decisiones Automatizadas: Las personas tienen el derecho de no estar sujetas a decisiones basadas únicamente en el procesamiento automatizado, incluida la elaboración de perfiles, que les afecten significativamente.

GOBIERNO DE ESPAÑA MINISTERIO DE CONSUMO

FORMULARIO DE SOLICITUD DE EJERCICIO DE DERECHOS
Reglamento General de Protección de Datos - RGPD

INTERESADO / REPRESENTANTE LEGAL (Campo obligatorio)	
N.I.F / N.I.E.	
APELLIDOS Y NOMBRE	

RESPONSABLE DEL TRATAMIENTO AL QUE DIRIGE LA SOLICITUD (Campo obligatorio)

Debe seleccionar un valor del desplegable. Puede consultar en la página web del Ministerio de Consumo con respecto al Tratamiento de Datos Personales y quien es el responsable del tratamiento que le afecta en:
https://consumo.gob.es/es/protecci-n-de-datos-personales

EJERCICIO DEL DERECHO (campo obligatorio. Seleccione al menos un derecho)

Por medio de la presente solicitud ejerce el derecho seleccionado, de conformidad con lo previsto en los artículos 15 a 22 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 sus datos personales y a la libre circulación de estos datos.

☐ **ACCESO**	El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que conciernen y, en tal caso, derecho de acceso a los datos personales y a la información establecida en el art. 15 del Reglamento (UE) 2016/679
☐ **RECTIFICACIÓN**	El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional, de acuerdo a lo establecido en el art. 16 del Reglamento (UE) 2016/679
☐ **SUPRESIÓN**	El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los da tos personales que le conciernan, el cual deberá estar obligado a suprimir los datos personales cuando concurra alguna de las circunstancia previstas en el art. 17 del Reglamento (UE) 2016/679
☐ **OPOSICIÓN**	En determinadas circunstancias, y por motivos relacionados con su situación particular, que deberá motivar junto a la presente solicitud, podrá oponerse a que los datos personales que le conciernan sean objeto de tratamiento en base a lo establecido en el art. 21 del Reglamento (UE) 2016/679
☐ **LIMITACIÓN DEL TRATAMIENTO**	El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones establecidas en el art. 18 del Reglamento (UE) 2016/679
☐ **PORTABILIDAD DE DATOS**	El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable de tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se les hubiera facilitado, cuando se cumplan algunos de los requisitos establecidos en el art. 20 del Reglamento (UE) 2016/679

Imagen 1: Formulario de solicitud de ejercicios de derechos – RGPD (1)

FORMULARIO DE SOLICITUD DE EJERCICIO DE DERECHOS
Reglamento General de Protección de Datos - RGPD

TEXTO DE LA SOLICITUD Y DOCUMENTACIÓN QUE ACOMPAÑA (Campo obligatorio)

MEDIO DE NOTIFICACIÓN		
☐ **ELECTRÓNICO**	**EMAIL**	
☐ **POSTAL**	(Cumplimente los datos de domicilio a efectos de notificaciones)	

DOMICILIO A EFECTO DE NOTIFICACIONES (Campo obligatorio en caso de notificación postal)							
N.I.F / N.I.E.							
APELLIDOS Y NOMBRE							
VÍA PÚBLICA							
NÚMERO		ESCALERA		PISO		PUERTA	
MUNICIPIO		PROVINCIA		C.POSTAL			

FIRMA (Campo obligatorio)					
EN		A		DE		DE	
Firma:							

Antes de firmar la solicitud debe leer la siguiente información sobre protección de datos personales:

INFORMACIÓN SOBRE PROTECCIÓN DE DATOS PERSONALES
De acuerdo con el Art.13 del **Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 (Reglamento General de Protección de Datos Personales)**, le informamos que los datos personales facilitados mediante el presente formulario, y demás que se adjuntan, serán tratados por la Subsecretaría del Ministerio de Consumo con la finalidad de recepción, registro y traslado al órgano competente para su tramitación. Adicionalmente, serán tratados por el responsable del tratamiento al que se dirige con la finalidad de tramitar su solicitud y dar respuesta al ejercicio de sus derechos. Sus datos personales no se comunicarán a terceros, ni está prevista transferencia a terceros países u organizaciones internacionales. Para más detalles del tratamiento específico de sus datos, así como información de cómo ejercitar sus derechos, consulte la información actualizada en la página web del Ministerio de Consumo, área de protección de datos en servicios al ciudadano, antes de firmar y presentar el presente formulario.

Imagen 2: Formulario de solicitud de ejercicios de derechos – RGPD (2)

GOBIERNO DE ESPAÑA MINISTERIO DE CONSUMO

FORMULARIO DE SOLICITUD DE EJERCICIO DE DERECHOS
Reglamento General de Protección de Datos - RGPD

ANEXO	
INFORMACIÓN ADICIONAL SOBRE PROTECCIÓN DE DATOS PERSONALES **EJERCICIO DE DERECHOS DE PROTECCIÓN DE DATOS**	
RESPONSABLE DEL TRATAMIENTO	Datos de contacto del Responsable: Consulte los datos del Responsable del tratamiento en el formulario en el que aportó sus datos personales o en la página Web del Ministerio, apartado Servicios al Ciudadano, Protección de Datos.
	Delegado de Protección de Datos: Calle Alcalá 27, 28014-MADRID. Email: dpd@consumo.gob.es
FINES DEL TRATAMIENTO	Descripción: Recepcionar, registrar y dar traslado de su solicitud de ejercicio de derechos al órgano competente, como responsable del tratamiento, a fin de que tramite la misma. Así como permitir, a través de los datos de registro, poder realizar las notificaciones y comunicaciones pertinentes, gestionar sus solicitudes, gestionar su cuenta de la Sede en el caso de usar el medio electrónico, etc".
	Plazo de conservación: Se conservarán durante el tiempo necesario para resolver las reclamaciones. Será de aplicación lo dispuesto en la normativa de archivos y documentación.
	Decisiones automatizadas: No existen decisiones automatizadas. Indicar en su caso.
LEGITIMACIÓN	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.(Reglamento General de Protección de Datos - RGPD). Art. 6.1.c) RGPD. Obligación legal del responsable. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y Real Decreto 495/2018, de 28 de abril, por el que se desarrolla la estructura orgánica básica del Ministerio de Consumo y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales
DESTINATARIOS	Categorías de destinatarios: Agencia Española de Protección de Datos, en caso de reclamación.
	Transferencias: No hay previstas transferencias de datos a terceros países.
DERECHOS	Cómo ejercer sus derechos: Puede ejercer los derechos de acceso, rectificación, supresión, limitación y oposición del tratamiento de los datos, cuando proceden, dirigiéndose al responsable del tratamiento de forma presencias en cualquiera de sus oficinas de la red de asistencia en materia de registros (https://administracion.gob.es/) o a través de la sede electrónica del Ministerio de Consumo (https://sede.mscbs.gob.es)
	Derecho a reclamar: Ante la Agencia Española de Protección de Datos. C/Jorge Juan, 6, 28001-Madrid. (https://sedeagpd.gob.es/)

Imagen 3: Formulario de solicitud de ejercicios de derechos – RGPD (3)

5.3. ¿Quién se hace responsable del tratamiento de los datos?

Llamamos responsable del tratamiento de datos a la persona física o jurídica, autoridad pública o privada, agencia u otro organismo que toma decisiones sobre cómo y porque los datos van a ser recopilados, almacenados, procesados para según que finalidad, uso o contenido, ya sea por decisión propia o ya sea por normativa legal. El responsable tiene la responsabilidad legal de garantizar que la forma de tratar los datos se realice dentro del marco legal, conforme a la ley. Todo esto implica que se obtenga el consentimiento adecuado, que se usen las medidas de seguridad pertinentes para la protección de los datos, que se respeten los derechos de los titulares y que se cumplan todas las formalidades con carácter obligatorio sobre todo lo relacionado con el tratamiento de los datos.

Para esta guía para el responsable de datos en los centros educativos, se determina que es el propio centro quien podría ser el responsable de los datos. Esto deriva en que el centro es el responsable de los datos de los estudiantes, profesores, personal administrativo, empleados, familiares de los estudiantes y otras personas involucradas con la institución educativa. Es también posible que la responsabilidad de los datos pertenezca a terceros contratados para procesos específicos, como la realización de nóminas o administración de sistemas informáticos, encargados del tratamiento de datos bajo supervisión y de la que existe una responsabilidad del responsable del tratamiento de datos.

En los centros educativos dependiendo del tipo que sean, el responsable puede ser diferente:

- En los centros educativos privados o concertados, la responsabilidad de los datos recae sobre el propio centro y, por ende, al propietario del centro educativo.

- En los centros públicos, la responsabilidad pertenece a la administración u organismo capacitada en materia de educación: la Administración Educativa (Consejería de Educación de la Comunidad Autónoma). Para poner un ejemplo; en las Islas Canarias el organismo que se responsabiliza del tratamiento de datos en colegios públicos es la Dirección General de Modernización y Calidad de los Servicios del Gobierno de Canarias.

5.4. ¿Quién se encarga del tratamiento de los datos?

Llamamos encargado del tratamiento de datos a la persona física o jurídica, autoridad o privada, agencia u otro organismo, que procesa los datos personales en nombre del responsable del tratamiento de datos. En otras palabras, es una existencia que realiza el trato de datos siguiendo las directrices de responsable del tratamiento y en nombre de este.

La entidad encargada del tratamiento de datos no decide el uso ni el propósito ni los medios a usar para el tratamiento de datos por decisión propia, si no que actúa como un proveedor para llevar a cabo actos de procesado de datos en nombre del responsable. Estos actos o actividades pueden ser almacenamiento de datos, análisis de datos, gestión de las nóminas y otras gestiones sobre el tratamiento de datos.

Es importante que el encargado actúe siguiendo las instrucciones del responsable de datos y que cumpla con todas las regulaciones sobre la protección de los datos que está tratando. Así como el encargado es responsable seguir lo que el responsable dicta, el responsable tiene una responsabilidad legal donde se debe garantizar que el encargado cumpla con las normativas y que proteja los datos según las leyes de protección y privacidad de los datos. Ambas partes: responsable y encargado, deben establecer un acuerdo donde se detallen las obligación o responsabilidades de cada parte con lo que respecta a la relación con el tratamiento de datos.

Para poner un ejemplo de encargado del tratamiento de datos para un centro educativo, podría tratarse de una empresa de software que proporciona un sistema que gestiona el aprendizaje en línea en nombre del centro educativo. La institución educativa seria la responsable del tratamiento de los datos y la empresa de software seria la encargada ya que procesaría los datos de las personas en nombre del centro.

5.5. ¿Qué pasaría si el responsable del tratamiento de datos no cumple con sus obligaciones?

Puede haber una serie de repercusiones legales, financieras y de reputación si el responsable del tratamiento de datos de la escuela incumple sus obligaciones de protección de datos. La privacidad y seguridad de los datos personales están protegidas por las leyes de protección de datos, por lo que violarlas puede tener graves repercusiones. Estos son algunos efectos potenciales.

- Sanciones financieras: cuando no se siguen las reglas, las autoridades de protección de datos tienen la autoridad de imponer multas y otras sanciones financieras. Dependiendo de la gravedad del delito y de la jurisdicción aplicable, las multas pueden ser muy elevadas y variar.

- Reclamaciones por daños y perjuicios: las personas cuya información personal se haya visto comprometida como resultado de la infracción pueden presentar una reclamación por daños y perjuicios. Puede surgir la necesidad de compensar a los afectados por esto.

- Investigaciones y Auditorias: Las autoridades de protección de datos pueden realizar auditorías e investigaciones para evaluar el cumplimiento de las regulaciones por parte de una escuela. Puede ser un proceso costoso e invasivo.

- Intervención de la Autoridad de Protección de Datos: En casos extremos de incumplimiento, las autoridades de protección de datos podrán imponer medidas adicionales, como ordenar la paralización del procesamiento de datos o la adopción de acciones correctivas.

- Daño a la reputación: una violación de la protección de datos podría dañar la reputación de la escuela. La confianza de los estudiantes, padres, personal y otras partes interesadas puede verse dañada por un manejo inadecuado de los datos.

- Prohibición de procesamiento de datos: las autoridades de protección de datos tienen la autoridad para restringir o prohibir rotundamente que la escuela procese cualquier dato personal en determinadas circunstancias.

- Acciones legales por parte de las autoridades: Para asegurarse de que la escuela cumpla con las reglas, las autoridades de protección de datos tienen derecho a presentar una demanda en su contra.

- Impacto en las relaciones comerciales: una violación de la protección de datos puede tener un efecto negativo en las relaciones con proveedores y socios comerciales que exigen el cumplimiento de las regulaciones como parte de sus acuerdos contractuales.

- Fuga de información: una infracción puede provocar la divulgación o divulgación no autorizada de información personal, lo que puede tener graves repercusiones para los afectados.

El responsable del tratamiento de datos en una escuela debe tomarse en serio sus funciones y cumplir estrictamente las leyes de protección de datos para evitar estos efectos desfavorables. Esto implica la adopción de pautas y procedimientos adecuados para garantizar consistentemente la seguridad y privacidad de la información personal.

En los establecimientos educativos es sancionable violar las leyes de protección de datos. Según las infracciones previstas en la LOPD y el RGPD se establece la cuantía de estas sanciones en función de la gravedad, resultando en:

- Las infracciones leves (art. 74 de la LOPDG) están sancionadas con hasta 40.000 euros.
- Las infracciones graves (art. 73 de la LOPD) están sancionadas desde 40.001 a 300.00 euros.
- Las infracciones muy graves (art. 72 de la LOPD) están sancionadas desde 300.001 a 20 millones de euros (o el 4% del volumen de facturación, la cuantía que resulte superior).

6. Legitimación y Principios de Protección para el Tratamiento de Datos

Las leyes que rigen el procesamiento de datos para instituciones educativas se basan en las leyes de protección de datos vigentes en cada nación y la Unión Europea en su conjunto. El Reglamento General de Protección de Datos (RGPD) establece las normas y directrices para el tratamiento de datos personales en todos los sectores de la Unión Europea, incluido el educativo. Sin embargo, cada país puede optar por implementar y adaptar sus leyes de manera diferente.

Las instituciones educadoras están certificadas por la Ley Orgánica de Educación del 2006 (LOE) para el uso del tratamiento de datos en base a la tarea formativa.

Los siguientes son algunos elementos importantes de la legislación sobre procesamiento de datos para instalaciones educativas:

- Datos de Menores: El RGPD establece que, salvo que un estado miembro establezca una edad inferior, que no puede ser inferior a 13 años, el tratamiento de datos de menores de 16 años debe estar sujeto al consentimiento de la persona que se encuentra en cargo de su cuidado o tutela legal. Esto indica que es crucial obtener el permiso de los padres o tutores antes de recopilar y procesar datos de jóvenes estudiantes en entornos educativos.

- Consentimiento informado: Antes de recopilar y procesar la información personal de un estudiante, las instituciones educativas deben obtener el consentimiento de los padres o tutores después de proporcionarles toda la información. El uso de los datos debe quedar claro en el consentimiento, el cual debe ser explícito, claro y voluntario.

- Transparencia: las escuelas deben dar a los padres y estudiantes explicaciones lúcidas y comprensibles, es decir, con un lenguaje claro y sencillo sobre cómo se procesarán los datos de los estudiantes, incluidas las categorías de datos que se procesarán, los propósitos del procesamiento, la duración del procesamiento y los derechos de los padres y los estudiantes. Para los Centro de la Comunidad Valenciana, estas

explicaciones o instrucción están recogidas en la Resolución del 28 de junio, donde se registra que se tienen que informar, aunque no haya un consentimiento en medio:

a. De la finalidad para la cual se van a recoger los datos
b. De la obligación o no de facilitar los datos y las consecuencias que podrían aparecer si se niegan dichos datos
c. De los derechos de las personas titulares de los datos y de donde se van a usar.

- Derechos de los interesados: según el RGPD, los miembros del personal, los padres y los estudiantes tienen derechos de acceso, derechos de rectificación, derechos de borrado y derechos de portabilidad para sus datos personales. Las escuelas deben facilitar a los estudiantes el ejercicio de estos derechos.

- Seguridad de los datos: las instituciones educativas deben implementar suficientes salvaguardas organizativas y técnicas para protegerse contra el acceso no autorizado, la divulgación, la pérdida y el robo de datos personales.

- Procesadores de datos: si las escuelas emplean a terceros para llevar a cabo tareas de procesamiento de datos, como software o proveedores de servicios en línea, deben establecer acuerdos específicos para garantizar que estos terceros cumplan con las leyes de protección de datos.

- Notificación de violación de seguridad: las escuelas deben notificar a las autoridades de protección de datos y, en algunos casos, a los titulares de datos sobre cualquier violación de seguridad que pueda afectar los derechos y libertades de los titulares de datos.

- Deber de secreto: las personas u organismos que tengan acceso a los datos personales están obligadas por ley a guardar secretos sobre los datos. Se trata de una practica vinculada a todas las personas de los centros o administraciones educativos que prestan sus servicios en estos. Este deber no finaliza incluso si la relación con el responsable del tratamiento de datos, del encargado o del propio centro haya terminado.

- Cancelación de los datos: Como parte de la normativa general, los datos de las personas físicas se conservan por un tiempo por un limitado para la finalidad para que se recogieron y para afrontar todos aquellos compromisos que se pueden regenerar al tratarlos. Cuando el tiempo de conservación de datos haya finalizado, damos paso a la cancelación de estos. La cancelación da paso al bloqueo de datos, pero no a su borrado material, con el fin de parar su proceso o su uso, a excepción de ponerlos a disposición de las Administración Publicas. Al final se procede a la destrucción, para el que se usaran medios o servicios que aseguraran que esos datos ya no puedan ser utilizados o ser accedidos por terceras personas.

7. Tratamiento de los Datos por las Instituciones Educativas

Los centros educativos recopilan datos académicos y personales para administrar la educación. Los datos deben estar relacionados con los propósitos educativos y se deben obtener los consentimientos necesarios.

7.1. ¿Cómo debería ser el tratamiento de datos en línea para los centros educativos?

Al tratamiento de datos de instituciones educativas en España se aplican las disposiciones del Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos (LOPD), que establecen las pautas para la recogida, tratamiento y uso de datos personales en línea. Las pautas que se debería seguir para el correcto trato de los datos serian la siguiente:

- Consentimiento Informado: Los padres o tutores legales de alumnos menores de edad deberán dar su consentimiento informado antes de que un centro educativo pueda recopilar información personal a través de su sitio web. El uso de los datos debe ser divulgado explícitamente y el consentimiento debe ser voluntario, específico y claro.

- Información trasparente: En el sitio web del centro educativo debe estar disponible información clara y comprensible sobre la recopilación, almacenamiento y uso de datos personales. En este documento se puede incluir una declaración de privacidad que describa los objetivos del procesamiento, las categorías de datos que maneja, sus políticas de retención y los derechos de los interesados.

- Seguridad de los datos: las instituciones educativas deben implementar salvaguardias organizativas y técnicas para protegerse contra pérdidas, robos y acceso no autorizado a la información de los estudiantes almacenada en línea. Esto podría implicar el uso de cifrado, protección con contraseña y actualizaciones frecuentes de software.

- Derechos de los interesados: según el RGPD, el personal, los padres y los estudiantes tienen derecho a acceder, corregir, eliminar y transferir sus datos personales. El centro educativo está obligado a facilitar a los estudiantes el ejercicio de sus derechos y a darles instrucciones sobre cómo hacerlo.

- Cookies y seguimiento en línea: si el sitio web de la escuela emplea cookies u otras tecnologías de seguimiento en línea, debe notificar a los usuarios sobre su uso y obtener su consentimiento antes de permitir que se guarden o accedan a ellas en sus dispositivos.

- Menores en línea: El RGPD establece protecciones específicas para los datos personales de los niños en línea. Al recopilar y utilizar datos de estudiantes en línea, obtener el permiso de los padres y mantener la seguridad de los datos, las escuelas deben tener especial precaución.

- Plataformas educativas en línea: Si un establecimiento educativo las utiliza para la enseñanza y el aprendizaje, debe asegurarse de que cumplan con las leyes de protección de datos y ofrezcan suficiente seguridad.

- Vulnerabilidades de Seguridad: Ante una vulnerabilidad de seguridad que pueda afectar a los derechos y libertades de los interesados, la institución educativa está obligada a notificarlo a la Agencia Española de Protección de Datos y, en algunas circunstancias, a los propios interesados.

- Procedimientos y políticas: Deben existir políticas y procedimientos claros en el centro educativo para el procesamiento de datos en línea. Todo el personal involucrado en la gestión de datos debe conocer y seguir estas políticas.

Se debe tener en cuenta que las regulaciones de datos para los centros u cualquier organismo puede ir actualizándose con el tiempo, por lo que el responsable del tratamiento de los datos debe estar siempre informado de los recientes cambios con respecto a las ultimas leyes más

recientes que implementen directrices sobre la protección de datos en internet para los centros educativos.

7.2. ¿Sobre qué, quién y cómo se pueden recopilar los datos para su tratamiento?

Dentro de los centros educativos, aparte del propio centro, existen personas físicas que forman parte del marco educativo como el profesorado, terceras personas contratadas por el centro o organismos y entidades compuestas por miembros que representan los intereses de los padre, madres o tutores legales conforme a sus hijos en los centros educativos: el AMPA.

Según la LOE, se legitima que, para los centros educativos, siempre que sirva para una función orientativa, se podrá recopilar y tratar datos tanto del alumnado, familiares: padre, madre o tutor legal, incluyendo datos especiales como la salud, orientación sexual, religión, etc. Y que, para este tipo de casos dictados por la LOE, no haría falta un consentimiento anticipado de las personas que van a ser afectadas

Cada uno de estos integrantes (centro, profesorado, AMPA, otras entidades), según el marco educativo, puede recopilar información dependiendo de a quien afecte y que tipos de datos puede recopilar. El responsable del tratamiento de datos debe tener en cuenta que no todos pueden recopilar todos los datos del alumnado u otras personas. Realicemos unas tablas de contenido para saber que puede o podría hacer cada integrante.

Estas tablas están recogidas dentro del *marco educativo para la Comunidad Valenciana*[4].

7.2.1. Para Centros educativos

¿Se puede recabar datos sobre la situación familiar de los padres y madres del alumnado?	SÍ
¿Se pueden recoger datos de salud?	SÍ, para el ejercicio de la función educativa.
¿Se pueden recoger datos biométricos?	Sólo huella dactilar codificada Sólo para acceso.
¿Se pueden recaudar imágenes del alumnado para el expediente académico?	SÍ
¿Se pueden recabar datos para finalidades diferentes de la función propiamente educativa?	Con consentimiento.

En los casos en los cuales es necesario el consentimiento del alumnado o de sus familias o tutores ¿cuándo y cómo es debido recabarlo?	Antes de la recogida de los datos o en el mismo impreso.
¿Puede un centro educativo acceder al contenido de dispositivos electrónicos del alumnado, como los sistemas de mensajería instantánea o redes sociales?	Con consentimiento. Solo si existe riesgo para la integridad del alumno podemos prescindir.
¿Puede un centro dar publicidad a los listados del alumnado admitido?	SÍ, sólo los resultados finales.
En caso de situaciones de violencia de género ¿se puede oponer el alumnado a la publicación de su admisión en los listados de un centro educativo?	SÍ, se puede oponer.
¿Pueden los centros hacer públicas las relaciones de los beneficiarios de becas, subvenciones y otras ayudas públicas?	SÍ (identificados con DNI o NIA)
¿Pueden los centros colocar en los tablones de anuncios o a las puertas de las aulas la relación del alumnado por clases y actividades? ¿y en Internet?	SÍ. En Internet con acceso de usuario y contraseña.
¿Se pueden publicar en el comedor del centro el menú del alumnado?	SÍ
¿Pueden los padres y madres pedir los exámenes de sus hijos e hijas par a llevarlos a casa?	No depende de la normativa de protección de datos. No es derecho de acceso a datos.
¿Pueden los padres y madres pedir acceso a la información sobre ausencias escolares de sus hijos e hijas?	Sí, incluso >18 si los mantienen.
¿Pueden los padres y madres solicitar información sobre datos de salud de sus hijos e hijas a los equipos de orientación?	SÍ
¿Se pueden facilitar la información escolar del alumnado a sus familiares?	Solo a padres, madres y tutores legales. Otros solo con autorización.
¿Cómo se da el acceso a la información académica por padres y madres separadas?	A ambos, aunque la custodia sea compartida. Salvo que alguno este privado de la patria potestad.
¿Qué competencias tiene el centro educativo en cuanto al tratamiento de las imágenes del alumnado?	Si es con fines educativos no requiere consentimiento. Para otros motivos o persona ajenas, con consentimiento.

Tabla 1: Tratamiento de datos para Centros Educativos

7.2.2. Para el Profesorado

¿Puede el profesorado recoger datos personales directamente del alumnado?	Solo para evaluar
¿Puede el profesorado solicitar datos de los familiares del alumnado?	Los recaba el centro, el profesorado puede tener acceso.
¿Puede el profesorado crear grupos con aplicaciones de mensajería instantánea con el alumnado?	NO. Solo medios y herramientas establecidos por la Conselleria o correo electrónico.
¿Puede el profesorado crear grupos con aplicaciones de mensajería instantánea donde sean miembros los padres y madres del alumnado de su clase?	NO. Solo medios y herramientas establecidos por la Conselleria
¿Puede el profesorado grabar imágenes del alumnado y difundirlas a través de aplicaciones de mensajería instantánea a sus familias?	NO. Solo si el interés superior del menor estuviera comprometido: accidentes en una excursión.
¿Se pueden hacer públicas las calificaciones escolares?	NO. Solo alumno y sus responsables legales pueden acceder.
¿Puede el profesorado facilitar las calificaciones oralmente en clase?	Puede, evitando comentarios adicionales.
¿Puede el profesorado acceder a los expedientes académicos del alumnado matriculado en el centro y a sus datos de salud?	Solamente a los alumnos a los que imparta docencia.
¿Puede el profesorado utilizar aplicaciones digitales en su dispositivo personal?	Se debe garantizar la seguridad y privacidad de los datos personales si no se utilizan las herramientas de Conselleria.
¿Se puede publicar información académica del alumnado en blogs del profesorado?	NO. En las instrucciones de inicio de curso se limita la posibilidad de utilizar plataformas externas a las oficiales.
¿Se pueden grabar imágenes en actividades escolares?	Sí, para los interesados. No se pueden publicar en Internet salvo consentimiento.

Tabla 2: Tratamiento de datos para el Profesorado

7.2.3. Para el AMPA

Para empezar a detallar que datos trata el AMPA, debemos saber de qué trata este organismo y cuál es su función.

La Asociación de Madres y Padres de Alumnos, o AMPA, tiene un impacto significativo en la comunidad educativa de un colegio en términos de gestión de datos y otras áreas. Aunque con frecuencia se centra en las asociaciones entre padres y escuelas para el bienestar de los estudiantes, ocasionalmente también se involucra en cuestiones de protección de datos. Las siguientes son algunas tareas relacionadas con la gestión de datos que AMPA podría agregar a su repertorio.

- Promover la transparencia y la comunicación: AMPA puede trabajar para garantizar que los padres y tutores estén al tanto de cómo se recopila, utiliza y protege la información personal sobre los estudiantes y las familias en la escuela. Para brindar a los padres el conocimiento que necesitan para tomar decisiones acertadas, se puede promover la transparencia en los procedimientos de gestión de datos.

- Defensa de la Privacidad y Derechos: Para garantizar que se respeten los derechos de privacidad de los estudiantes y sus familias, AMPA puede hablar como grupo en su nombre. La AMPA podría abogar por leyes y procedimientos que salvaguarden adecuadamente la privacidad de los datos si hay problemas con la forma en que se maneja la información personal.

- Participación en las Decisiones Relevantes: La AMPA puede participar en la planificación y toma de decisiones de proyectos o sistemas que involucren la gestión de datos. Podría entrar en esta categoría cualquier procedimiento que afecte la privacidad y seguridad de los datos, incluida la implementación de sistemas de información, plataformas de comunicación en línea u otros procesos.

- Educación y Concientización: AMPA puede organizar charlas, talleres o sesiones informativas para padres y tutores sobre temas relacionados con la protección de datos,

la privacidad en línea y las mejores prácticas para proteger la información personal de sus hijos.

- Colaboración con el colegio y las autoridades: trabajar con la administración del colegio y el personal docente para garantizar que las políticas y prácticas de protección de datos sean eficientes y estén en línea con los requisitos de la comunidad escolar. En cuestiones pertinentes, también podría trabajar con las autoridades educativas y de protección de datos.

- Revisión de políticas y documentación: la AMPA puede participar en la revisión de las políticas, prácticas y documentos relacionados con la protección de datos de la escuela. Como resultado, la toma de decisiones garantizará que se escuchen las opiniones de los padres.

- Resolución de conflictos: si hay un problema o desacuerdo con respecto a la gestión de datos y la privacidad, la AMPA podría ayudar a los padres y a la escuela a comunicarse para que el problema pueda resolverse de manera amistosa.

- Promoción de la seguridad en línea: dado que mucha información se maneja en línea, AMPA podría alentar a los padres y estudiantes a aprender sobre la seguridad de los datos y la seguridad en línea.

Es importante señalar que, dependiendo de la escuela y el área, los propósitos y alcance específicos de la AMPA pueden cambiar. Su trabajo, con carácter general, consiste en fomentar la comunicación y el bienestar general de la comunidad escolar, que en ocasiones puede incluir también la protección de datos y la privacidad.

Datos que puede tratar el AMPA:

¿Se necesita de un consentimiento para el tratamiento de datos de sus asociados y asociadas y alumnado?	Sólo si no son asociados.
¿Se pueden comunicar datos del alumnado y de sus familiares a las AMPA?	NO sin el previo consentimiento de los interesados.
Si fueran contratadas para dar un servicio sí que tendrían acceso, pero sólo como encargadas del tratamiento.	
¿Puede la AMPA publicar en su blog, web o redes sociales los datos del alumnado?	Con consentimiento.
¿Qué pasa con el alumnado que no es socio de la AMPA?	Solo se pueden facilitar sus datos con consentimiento.

Tabla 3: Tratamiento de datos para el AMPA

7.2.4. Para terceras personas contratadas u organismos públicos

Los centros educativos, aparte de solicitar y recoger ellos mismos los datos de las personas físicas asociadas al centro, existen otros centros, entidades e instituciones que pueden pedir la información del alumnado como pueden ser los Servicios Sociales, la Administración Sanitaria, e incluso las Fuerzas y Cuerpos de Seguridad del Estado).

Aunque se trate de administraciones públicas, la petición sobre los datos personales del alumnado debe requerir dentro de la legalidad el consentimiento de las personas afectadas, la de sus padres y madres o tutores legales si fuera el caso, aunque existan excepciones.

Datos que pueden tratar las terceras personas contratadas u organismos públicos:

Casos que no requieren consentimiento	Respuesta
Comunicación de datos del alumnado a otro centro educativo	En caso de traslado de expediente
Comunicación de datos a otros centros situados en otros países	En caso de intercambios o estancias en el extranjero, se entiende que hay una solicitud o autorización previa.
Comunicación de datos a la Administración educativa	Para ejercicio de sus competencias como, por ejemplo, la expedición de títulos.
Comunicación de datos a las Fuerzas y Cuerpos de Seguridad	Son obligatorias siempre que sean necesarias para la prevención de un peligro real para la seguridad pública o para la represión de infracciones penales. Es aconsejable que el centro documente la comunicación de los datos.
Comunicación de datos a Servicios Sociales	Siempre que sea para la determinación o tratamiento de situaciones de riesgo o desamparo que sean de su competencia.
Comunicación datos a centros sanitarios	Cuando el motivo sea la prevención o el diagnóstico médico, la prestación de asistencia sanitaria o de tratamientos médicos, o la gestión de servicios sanitarios.
Comunicación de datos a Servicios Sanitarios autonómicos o ayuntamientos para campañas de salud o vacunación	Para garantizar la salud pública o para llevar a cabo actuaciones sanitarias recomendadas.

Tabla 4: Tratamiento de datos para el 3ª personas (Sin consentimiento)

Casos que requieren consentimiento	Respuesta
Comunicación de datos a otras entidades externas para la gestión de actividades extraescolares	Sólo si van a ser utilizados para fines de control de entrada y aforo, se entiende que hay consentimiento para la actividad extraescolar
Grabación de imágenes de actividades desarrolladas fuera del centro escolar	Es imprescindible el consentimiento que se puede haber recaudado a través del centro.

Tabla 5: Tratamiento de datos para las 3ª personas (Con consentimiento)

7.2.5. Tratamiento de Datos por los Familiares del Alumnado

Cuando los padres, tutores u otros familiares de los estudiantes interactúan con la información personal de los estudiantes y otros miembros de la comunidad escolar, esto se conoce como procesamiento de datos por parte de familiares de los estudiantes en un centro educativo. Esta interacción puede tener lugar en una variedad de entornos y contextos, incluido hablar con la escuela, participar en actividades patrocinadas por la escuela y utilizar los recursos en línea de la escuela. Los puntos interesantes para recordar son los siguientes:

1. Comunicación con el centro educativo: Los familiares de los estudiantes podrán proporcionar información personal al centro educativo durante el proceso de inscripción, al actualizar la información de contacto o al participar en eventos escolares. Es fundamental que la escuela obtenga el consentimiento después de revelar completamente el uso previsto de los datos.

2. Acceso a Plataformas en Línea: En muchas instalaciones educativas, las Plataformas en Línea se utilizan para comunicarse con los padres y brindar información sobre el progreso académico de los estudiantes. Estas plataformas permiten a los miembros de la familia acceder a calificaciones, tareas y otros datos relacionados con la educación de sus hijos. Es fundamental que estas plataformas cumplan con las leyes de protección de datos e informen a los familiares de manera clara y comprensible sobre cómo se manejarán los datos en línea.

3. Consentimiento para la publicación de imágenes: Es una práctica común fotografiar o grabar a los estudiantes durante eventos y actividades relacionados con la escuela. Obtener la aprobación de los padres o tutores es crucial si tiene la intención de publicar estas fotografías en línea o en otros medios, especialmente si las fotografías muestran claramente qué estudiantes son.

4. Privacidad en la comunicación: Tanto las instituciones educativas como las familias deben ser conscientes de la privacidad en la comunicación. Los correos electrónicos, mensajes y otras formas de comunicación que contengan información personal o sensible deben tratarse con respeto y confidencialidad.

5. Uso Responsable de Datos: Los familiares deberán utilizar la información proporcionada por el centro educativo con sensatez y únicamente para los fines previstos. Participar en actividades escolares o hablar con otros padres puede entrar en esta categoría.

6. Respeto por la privacidad de los demás: se espera que las familias respeten la privacidad de otros estudiantes y sus familias. No se les permite divulgar información privada o delicada sobre otros estudiantes sin su permiso.

En conclusión, el tratamiento de datos por parte de los familiares de los estudiantes implica el manejo ético y responsable de la información personal en el ámbito educativo. La obligación de cumplir las leyes de protección de datos y respetar la privacidad de los estudiantes y otros miembros de la comunidad escolar recae tanto en los centros educativos como en las familias.

7.3. Tratamiento de datos: Certificados de Delincuentes Sexuales del Registro Central en Centros Educativos

Para garantizar la seguridad de los estudiantes y el personal en el ámbito educativo, el tratamiento de los certificados del Registro Central de Delincuentes Sexuales es un tema pertinente. Los certificados enumerados aquí son registros oficiales de las agencias correspondientes que revelan el historial de delitos sexuales de una persona.

Es requisito no haber sido condenado por ningún delito contra la libertad y la identidad sexual, incluidas las agresiones y abusos sexuales, el acoso sexual, el exhibicionismo y la provocación sexual, la prostitución y la explotación sexual y la corrupción de menores, así como la trata de personas, para poder Realizar actividades docentes que impliquen contacto con menores. No se exigiría un nuevo aporte ni renovación periódica, pero quien quiera acceder a las actividades antes mencionadas deberá acreditar este hecho aportando una certificación negativa del Registro Central de Delincuentes Sexuales. Aquí hay algunos puntos cruciales para recordar sobre este tema:

- Propósito y Justificación: El Registro Central de Delincuentes Sexuales puede emitir certificados a instituciones educativas como parte de sus protocolos de seguridad y protección. El objetivo principal es garantizar que las personas con antecedentes de delitos sexuales no puedan ser acusadas de delitos que impliquen contacto directo con estudiantes, como los cometidos por profesores, miembros del personal de apoyo o voluntarios.

- Consentimiento: Previamente a la solicitud y tramitación de las actas del Registro Central de Delincuentes Sexuales, los centros educativos están obligados a obtener el consentimiento expreso de las personas afectadas. Tanto los empleados actuales como los nuevos solicitantes que se consideran para puestos en la escuela deben ser conscientes de esto.

- Alcance limitado: Las solicitudes de estos certificados deben estar enfocadas y relacionadas específicamente con tareas que requieran interactuar con los estudiantes. Las únicas personas que deberían someterse a este procedimiento son aquellas cuyos trabajos requieren un contacto frecuente o cercano con los estudiantes.

- Tratamiento Confidencial: Los datos de las actas del Registro Central de Delincuentes Sexuales deben manejarse de forma confidencial y segura. El acceso a esta información solo debe permitirse al personal autorizado y se deben implementar medidas de seguridad para evitar la divulgación no autorizada.

- Transparencia y comunicación: Las instituciones educativas deben explicar el proceso de solicitud de certificado a los miembros del personal y a los solicitantes, así como cómo manejarán los datos que recopilen. Para generar confianza y comprensión con respecto a esta medida de seguridad, la transparencia es crucial.

- Respeto a los derechos: Se deben respetar los derechos de privacidad y confidencialidad de una persona que tiene antecedentes de delitos sexuales. Al decidir si contratarlos o

no, se deben tener en cuenta los antecedentes de una persona, las leyes aplicables y la seguridad de los estudiantes.

- Retención de datos: Es fundamental tener una política clara sobre la retención de estos datos una vez que se haya tomado una decisión utilizando los certificados del Registro Central de Delincuentes Sexuales. Cuando no sean necesarios, los datos deben almacenarse y eliminarse de forma segura.

En conclusión, tratar las actas del Registro Central de Delincuentes Sexuales es un paso crítico para garantizar la seguridad del personal y de los estudiantes en las instalaciones educativas. Pero debe hacerse abiertamente, defendiendo al mismo tiempo los derechos de las personas y respetando las leyes que rigen la seguridad y privacidad de los datos.

8. Videovigilancia

En España, el Reglamento General de Protección de Datos (RGPD) y la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), que desarrolla el RGPD a nivel nacional, son las principales fuentes de la ley que regula la videovigilancia en los centros educativos. Para realizar videovigilancia en un entorno destinado al aprendizaje, como una escuela, se deben cumplir ciertas pautas y requisitos.

8.1. Requisitos generales de la Videovigilancia

- El uso de la videovigilancia debe estar justificado y ser específico, como por ejemplo para control de acceso, prevención de incidentes o seguridad del edificio.
- La videovigilancia debe tener una justificación legal, como el consentimiento, el cumplimiento de un requisito legal o el interés legítimo del responsable del tratamiento.
- A través de una señalización adecuada e inequívoca, se debe informar a quienes puedan ser grabados de la existencia y finalidad de la videovigilancia.

Imagen 4: Cartel de zona vigilada

8.2. Aspectos que debe considerar el responsable del tratamiento de datos en los colegios

- Definir finalidad: La escuela debe definir claramente el propósito de la videovigilancia, ya sea garantizar la seguridad de los estudiantes y el personal, detener el vandalismo o restringir el acceso a áreas específicas.

- Justificación legal: Identifique la justificación legal para la videovigilancia, como el buen interés de la escuela en mantener la seguridad de sus instalaciones. También se debe tener en cuenta la Ley de Seguridad Privada si se trata de grabar espacios públicos.
- Denuncias y Consentimiento: Hacer señalización clara y visible que alerte a las personas sobre el uso de videovigilancia. Es recomendable obtener el consentimiento explícito de las personas antes de realizar fotografías en lugares de acceso restringido o privados.

- Minimización de datos: recopile y conserve únicamente la cantidad mínima de imágenes necesarias para lograr el objetivo previsto. Evite tomar fotografías inútiles de sujetos no relacionados.

- Acceso restringido: asegurarse de que solo el personal autorizado pueda acceder a las grabaciones y de que se mantenga un registro de quién accede al metraje y por qué.

- Las grabaciones deben almacenarse de forma segura y protegerse del acceso no autorizado. Establezca pautas de retención de datos para que las grabaciones puedan eliminarse cuando ya no sean necesarias.

- Respetar los derechos de los sujetos, como el derecho a acceder a su información personal y el derecho a solicitar la eliminación de grabaciones.

- Transparencia: asegúrese de que la política de privacidad de la escuela contenga información clara sobre la videovigilancia y esté preparado para responder a las consultas del personal, los estudiantes y los padres.

- Realizar una evaluación del impacto de la protección de datos para identificar y reducir cualquier riesgo potencial para los derechos y libertades de las personas en situaciones en las que la videovigilancia es más generalizada o extensa.

- Notificación a la Autoridad de Protección de Datos: En algunas circunstancias, podría ser necesario informar a la Agencia Española de Protección de Datos sobre la implantación de videovigilancia, especialmente si supone un riesgo significativo para los derechos y libertades de las personas.

Es fundamental que el responsable del tratamiento de datos de la escuela conozca estas reglas y se asegure de que la videovigilancia se realice de acuerdo con los principios de privacidad y protección de datos.

9. Procedimiento

Durante la guía solamente hemos estado leyendo y comprendiendo el tratamiento de datos a nivel teórico, sobre todo sobre cómo se tratarían los datos, que podemos o no podemos hacer, e incluso quien puede ver esos datos y tratarlos, pero como responsable del tratamiento de datos en un colegio, para que se trate de un proceso completo debemos dar métodos, herramientas y ejemplos de cómo volcar toda esta teórica a la práctica. Se ha de recalcar que es posible que las herramientas que vayamos a utilizar no sean las correctas que se puedan usar dentro de una institución educativa, ya que puede ser que sean de pago o que de deba disponer de X licencia para su uso. Por lo que usaremos herramientas parecidas para que se pueda dar a entender el uso que haremos de ellas y se puedan replicar.

9.1. Evaluación de Datos y Riesgos

9.1.1. Herramientas para Evaluación de Datos y Riesgos

9.1.1.1. Matriz de Riesgos

Usar una matriz de riesgos para identificar el tipo de datos que vamos a manejar en el colegio y que riesgos pueden ser asociados. Podemos categorizar estos riesgos mediante la probabilidad de que ocurra dicho riesgo y que impacto causaría. También podemos clasificar estas probabilidades e impactos considerando un Valor de Riesgo Ponderado y así podemos enfocar nuestras prioridades de forma más sesgada dándole valores números.

Tipo de Datos	Descripcion del Riesgo	Probabilidad	Impacto	Valor de Riesgo Ponderado
Datos del Estudiante	Acceso no autorizado a calificaciones y registros academicos	Medio	Alto	6
Datos de Profesores	Riesgo de fuga de informacion confidencial	Bajo	Medio	2
Datos de los Padres / tutores	Divulgación no autorizada de información de contacto	Medio	Bajo	2
Datos financieros	Posible exposición de información financiera de padres	Bajo	Alto	3
Datos Medicos	Filtración de información médica confidencial	Bajo	Medio	2
Datos de Asistencia	Acceso no autorizado a registros de asistencia	Bajo	Bajo	1
Datos de Conducta	Posible divulgación de incidentes de conducta	Medio	Medio	4
Datos de Discapacidades	Riesgo de filtración de información sobre discapacidades	Medio	Alto	6
Datos de Salidas y excuersiones	Exposición de información sobre salidas escolares	Bajo	Medio	2
Datos de Evaluacion Docente	Posible acceso no autorizado a evaluaciones de profesores	Bajo	Medio	2
Datos de Recursos Humanos	Riesgo de acceso no autorizado a información de empleados	Medio	Medio	4
Datos de Formacion Profesional	Posible filtración de información de cursos y formación	Bajo	Bajo	1
Datos de Menores de edad	Riesgo de divulgar datos personales de menores	Bajo	Medio	2
Datos de Comunicaciones	Fuga de información de comunicaciones internas	Bajo	Bajo	1
Datos de Investigaciones	Acceso no autorizado a investigaciones en curso	Medio	Medio	4

Valores	Probabilidad	Impacto
Bajo	1	1
Medio	2	2
Alto	3	3

Valor Riesgo Ponderado	Resultado
1	Bajo
2	Medio-Bajo
3	Medio
4	Medio-Alto
6	Alto

Imagen 5: Ejemplo de Matriz de Riesgo

9.1.1.2. Mapa de Datos

El mapa de datos nos permitirá identificar con un mapa visual todos los datos que se recopilan, donde van a almacenarse y como se distribuyen a través de los sistemas informáticos del colegio. En este caso, vamos primero a definir una serie de pasos para poder realizar el mapeo de los datos de forma exitosa. Posteriormente, crearemos un ejemplo de mapeo de datos para que se entienda.

Los pasos que seguir serían los siguientes:

- Paso 1: Identificación de datos.

Describe todo tipo de datos que se manejan en el colegio, incluyendo información sobre alumnos, profesores, personal de apoyo, padres, expedientes académicos, registros médicos, etc.

- Paso 2: Identificar los procedimientos

Enumere los procedimientos utilizados para recopilar, almacenar, procesar o compartir datos, incluido el registro de estudiantes, la planificación de lecciones, la evaluación de estudiantes, la comunicación con los padres, etc.

- Paso 3: Identificar los flujos de datos.

Realice un seguimiento de las transferencias de datos que se realizan entre varios sistemas y divisiones. Piense en cómo se ingresa la información de los estudiantes en el sistema de inscripción y luego se traslada al sistema de administración académica.

- Paso 4: Identificar el almacenamiento de datos.

Especifica la ubicación del almacenamiento de datos en cada etapa del proceso. Entre otros, esto puede implicar sistemas de comunicación con los padres, sistemas de gestión de estudiantes y bases de datos de profesores.

- Paso 5: Determinación de usuarios y acceso.

Haga un seguimiento de quién tiene acceso a qué bases de datos y sistemas. Esto puede aplicarse a directivos, educadores, ayudantes, padres y estudiantes.

- Paso 6: Evaluación de riesgos

Cada paso del proceso debe incluir una evaluación de los riesgos involucrados con el manejo de datos. identifica posibles puntos débiles y agujeros de seguridad que podrían poner en peligro la integridad o confidencialidad de los datos.

- Paso 7: Poner en práctica las medidas de seguridad.

Crear e implementar las medidas de seguridad adecuadas para proteger los datos en cada etapa. Algunos ejemplos de estos son los controles de acceso, el cifrado y la autenticación.

- Paso 8: La documentación

Asegúrese de registrar cada paso del proceso de mapeo de datos, incluidos los tipos de datos, sistemas, controles de acceso y diagramas de flujo.

- Paso 9: Mantenimiento y modificación.

Actualizar el mapeo de datos a medida que cambien los procedimientos, sistemas o leyes. Revíselo con frecuencia para asegurarse de que sea preciso.

- Paso 10: Formación y la comunicación.

A todo el personal implicado, explicar el mapa de datos y las medidas de seguridad. enseñar a los usuarios cómo manejar los datos de forma segura y de acuerdo con las políticas establecidas.

Ejemplo básico de mapeo de datos junto con el flujo de almacenamiento:

Vamos a considerar el proceso de matriculación de un alumno en el colegio. Lo primero que se presenta en el registro de la matricula: un formulario sencillo, ya sea a papel u online, donde se va metiendo la información personal del estudiante y sus datos de contacto. Estos datos recopilados son tratados como de carácter personal: nombre, fecha de nacimiento, dirección, número de teléfono, correo electrónico y datos de carácter mas sensible. Una vez se ha presentado la matricula, el personal de admisiones ingresa esos datos en nuestro sistema de gestión del colegio. Estos datos deberán ser validados por el sistema lo que asignaría un número de identificación único al estudiante (ID). Estos datos se almacenarán en una base de datos segura dentro del sistema de gestión y creara un registro único con los datos del estudiante

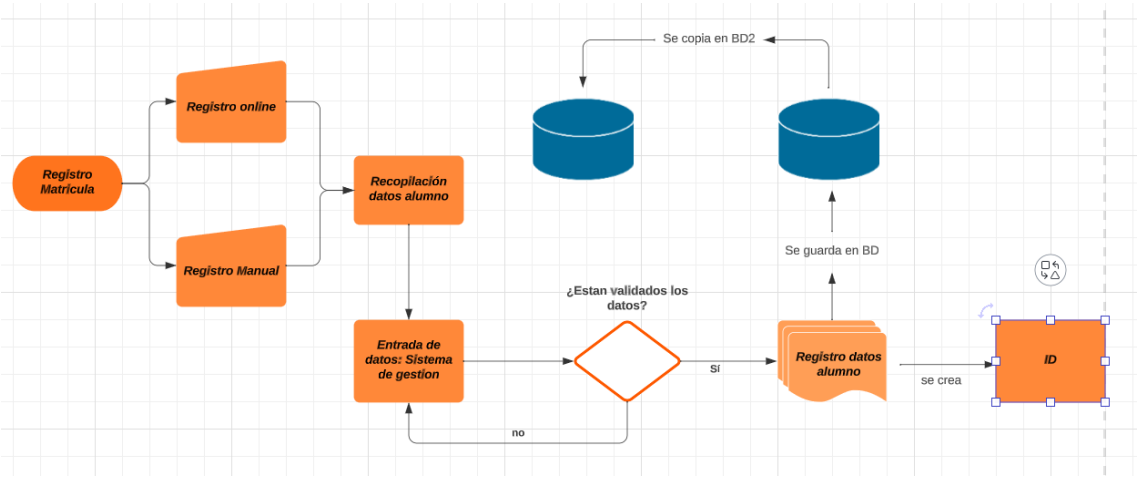

Imagen 6: Flujo básico de registro y almacenamiento

A medida que el estudiante progresa en sus estudios, se agregan registros académicos, como calificaciones y asistencia dentro su registro de perfil en el sistema de gestión de estudiantes. A parte de un sistema de gestión, el colegio también dispone de un sistema de comunicación con los padres o tutores legales para que puedan recibir información y notificaciones como pueden ser boletines, horarios de clase y anuncios. El colegio tendrá a su disposición la información de los familiares a través de este sistema de comunicación. Los padres también podrán cambiar su información personal o de contacto.

Una vez que el alumno se gradúa o abandona el colegio, esa información queda registrada dentro de sistema de gestión de estudiante y junto con toda su información personal y

académica, estas serán mantenidas dentro la base de datos a colmo de finalizar dentro de un archivo. Según las políticas de retención de datos, el colegio conservara dentro de un periodo de tiempo limitado toda esta información y luego serán eliminados de forma segura.

Llevado a la practica y siendo conscientes del mundo real, este ejemplo sería mucho más complejo ya que involucraría múltiples sistemas, departamentos, procesos y mucha más información. El objetivo es tener claro lo que se propone hacer y asegurarse que todos los datos que se manejan dentro del colegio sean seguros y adecuados a las políticas de privacidad y seguridad establecidas.

9.1.1.3. Software de Evaluación de Riesgos

Podemos usar herramientas como software y herramientas oficinales para la evaluación de riesgos y el cumplimiento normativo que podemos usar en una institución educacional que pueden ayudar en la identificación y la gestión de estos riesgos. Las herramientas o programas que podemos usar podrían ser estas:

- Microsoft Excel: Se pueden crear hojas de cálculo de evaluación de riesgos personalizadas utilizando Excel, una herramienta flexible. Para cuantificar y clasificar los riesgos, puede crear cuadros, gráficos y fórmulas.

- GRC Software: Existen soluciones de software de GRC (Governance, Risk, and Compliance) que permiten a las empresas gestionar el cumplimiento, el riesgo y la gobernanza de forma integral, incluida la evaluación de riesgos. Los ejemplos incluyen ServiceNow GRC, SAP GRC y RSA Archer.

- Software para evaluación de riesgos de ciberseguridad: El Marco de ciberseguridad (CSF) del NIST y la herramienta de autoevaluación de ciberseguridad de la FTC (para instituciones educativas en los Estados Unidos) son dos herramientas que pueden ser útiles para las escuelas que buscan evaluar riesgos específicos de ciberseguridad.

- Encuestas on-line: Para obtener información y comentarios de participantes importantes en la evaluación de riesgos, como el personal y los padres, puede utilizar herramientas de encuestas en línea como Google Forms.

- Software de gestión de proyectos: Las actividades de evaluación de riesgos se pueden planificar y monitorear con la ayuda de herramientas de gestión de proyectos como Asana o Trello.

9.1.2. Métodos para Evaluación de Datos y Riesgos

- Análisis de riesgos y amenazas: identifica los riesgos particulares que enfrenta la escuela en relación con la gestión de datos, como pérdida de dispositivos, acceso no autorizado o fuga de información.

- Realizar una evaluación de impacto de la protección de datos (EPID) si los derechos y libertades de las personas se ven significativamente amenazados por la videovigilancia u otras actividades de procesamiento de datos. Los riesgos potenciales serán más fáciles de detectar y reducir gracias a esta evaluación.

- Examina los sistemas y procedimientos que tratan datos personales para encontrar posibles debilidades de seguridad o acceso no autorizado.

9.1.3. Ejemplos para Evaluación de Datos y Riesgos

Disponemos que varios ejemplos simples para poder tener un inicio a la hora de que el responsable del tratamiento de datos pueda empezar a ejecutar tareas de evaluación. Algunos de los ejemplos que podríamos visualizar podrían ser los siguientes:

- Evaluación de Riesgos en Videovigilancia: Si la escuela utiliza videovigilancia, evalúe los riesgos asociados con ella, incluido el acceso no autorizado a las grabaciones, la propensión a conservar demasiados datos y la falta de alerta a quienes están siendo observados. A continuación, ordene estos riesgos según su gravedad.
- Evaluación de riesgos para los sistemas de gestión de estudiantes: si la escuela utiliza un sistema para administrar los datos de los estudiantes, evalúa los peligros de la seguridad de los datos, el acceso no autorizado y la información precisa.

- Evaluación de riesgos en los sistemas de comunicación: La escuela evalúa los riesgos de interceptación de mensajes y robo de información personal si utiliza sistemas de comunicación electrónica para interactuar con padres y estudiantes.
- Análisis de vulnerabilidades de la red Wi-Fi: examina la seguridad de las redes Wi-Fi utilizadas en la escuela para protegerlas contra posibles intrusiones y fugas de datos.
- Análisis de riesgos en el almacenamiento de datos: Es importante evaluar los riesgos de seguridad y el acceso no autorizado asociados con el almacenamiento de datos, ya sea en servidores internos o en la nube.

9.2. Establecimiento de Políticas y Procedimientos Internos

Para garantizar que los datos personales se manejen de manera consistente y segura en una escuela, es crucial establecer políticas y procedimientos internos sólidos. Puede completar esta tarea utilizando las siguientes herramientas, programas, técnicas y ejemplos.

9.2.1. Herramientas para Establecimiento de Políticas y Procedimientos Internos

- Plantillas para políticas y procedimientos: utilice plantillas prediseñadas para redactar políticas y procedimientos relacionados con la protección de datos. Hay plantillas en línea disponibles o puede utilizar las que ofrecen las organizaciones de protección de datos.

- Software de Gestión Documental: Cree, almacene y administre políticas y procedimientos de manera efectiva mediante el uso de software de gestión de documentos. Los ejemplos incluyen SharePoint, Google Workspace (anteriormente G Suite) y DocuWare.

- Herramientas de Colaboración: Las herramientas de colaboración en línea pueden ayudar con el desarrollo conjunto y la revisión de políticas y procedimientos. Trello, Slack y Microsoft Teams son algunos ejemplos.

9.2.2. Método y Ejemplos para Establecimientos de Políticas y Procedimientos Internos

En este apartado vamos a establecer varios métodos y ejemplos de forma conjunta para el establecimiento de políticas y procedimientos internos. Algunos métodos ya de por si son ejemplos del uso por lo que no hará falta extender el apartado.

Identificar Áreas Clave: Determina las áreas principales donde se manejan los datos personales, como matrícula de estudiantes, comunicaciones con padres, expedientes académicos, etc.

Definición de Roles y Responsabilidades: La definición de roles y responsabilidades identifica quién está a cargo de diversos aspectos de la protección de datos en la escuela, como el controlador de datos, el gerente de seguridad de datos, etc.

Desarrollo de políticas: Desarrollar regulaciones que cubran temas específicos, como consentimiento de procesamiento de datos, retención de datos, seguridad de datos, notificación de incidentes, etc. Podemos dar un ejemplo: políticas de consentimiento para el tratamiento de datos describiendo de cuándo, dónde y cómo se obtiene el consentimiento de las personas para el tratamiento de sus datos y creando pautas a seguir para obtener el consentimiento legítimo y cómo registrarlo.

Desarrollo de Procedimientos: Establecer procedimientos en detalle le ayudará a manejar datos en una variedad de circunstancias. Un buen ejemplo es el proceso de gestión de solicitudes de acceso a datos donde se describe cómo se deben tratar y abordar las solicitudes de acceso de las personas, contiene fechas de vencimiento de respuesta e instrucciones sobre cómo verificar la identidad del solicitante.

Implementación de Medidas de Seguridad: Especifica las medidas de seguridad organizativas y técnicas que se deben implementar para salvaguardar los datos. Para dar ejemplo podemos hablar de un procedimiento para la seguridad de datos: explicar cómo se protegerán los datos mediante el uso de contraseñas seguras, cifrado de datos, acceso basado en roles, etc.

Educación y capacitación: establece los medios por los cuales el personal recibirá educación sobre procedimientos y prácticas de protección de datos. Algún ejemplo de ello es el procedimiento de formación en materia de protección de datos donde explicamos cómo los miembros del personal recibirán formación periódica sobre directrices de protección de datos y manejo seguro de datos.

Revisión y actualización: describe el proceso para evaluar y revisar de forma rutinaria las políticas y procedimientos para garantizar que cumplan con los requisitos legales en evolución y las mejores prácticas de la industria. Ejemplo: El procedimiento de revisión y actualización de políticas y explicaremos cómo se revisarán las políticas y procedimientos anualmente y cómo se incorporarán las actualizaciones necesarias.

9.3. Obtención de Consentimiento y Comunicación

La obtención del consentimiento y la comunicación efectiva dentro de la gestión de los datos personales es un aspecto fundamental en las instituciones educacionales. Por lo que para la guía proporcionaremos herramientas, programas, métodos y ejemplos de cómo se debería implementar dentro de un colegio.

9.3.1. Herramientas para la Obtención de Consentimiento y Comunicación

Correo electrónico: Herramientas para la comunicación por correo electrónico para ponerse en contacto con padres, estudiantes y personal de la escuela, utilice servicios de correo electrónico como Microsoft Outlook o Gmail. Para recordar a las personas que den su consentimiento o envíen comunicaciones importantes, puede programar el envío de correos electrónicos.

Software de Automatización de Marketing: El software para la automatización del marketing se puede utilizar para crear campañas de correo electrónico automatizadas y segmentadas con comunicaciones personalizadas y solicitudes de consentimiento, como MailChimp o HubSpot.

Encuestas on-line: para crear encuestas y formularios en línea para obtener electrónicamente el consentimiento de los padres y estudiantes, utilice SurveyMonkey o Google Forms.

Plataformas de comunicación escolar: para comunicarse eficazmente con padres y estudiantes, muchas escuelas utilizan herramientas de comunicación escolar especializadas como ClassDojo o Remind.

Sistemas de gestión de datos estudiantiles (SDGE): algunos SDGE tienen funciones para obtener consentimiento y facilitar la comunicación. Verifique si estas funciones están disponibles en el SDGE de la escuela.

9.3.2. Métodos y ejemplos para la Obtención de Consentimiento y Comunicación

Formularios de consentimiento electrónico: Crear formularios de consentimiento electrónicos que los padres y estudiantes puedan completar en línea para dar su permiso para actividades particulares, como excursiones, compartir fotografías o participar en eventos. A modo de ejemplo, podemos considerar crear un formulario de consentimiento para la publicación de fotografías. Los padres pueden acceder al formulario en línea y dar su aprobación para que las fotografías de sus hijos se publiquen en el sitio web o en publicaciones escolares. Envíe correos electrónicos periódicos a padres y estudiantes para mantenerlos actualizados sobre eventos, políticas y solicitudes de consentimiento pendientes.

Comunicación por vía email: El correo electrónico que sirve como recordatorio para dar el consentimiento. Antes de una excursión escolar, deberíamos enviar un correo electrónico a los padres pidiéndoles que inscriban a sus hijos en la excursión en línea antes de la hora especificada.

Portal para padres en línea: Establezca un sitio web donde los padres puedan acceder a información pertinente, modificar sus preferencias de comunicación y dar permiso para una variedad de actividades relacionadas con la escuela. Un buen ejemplo sería un portal para padres en línea, a modo de ilustración. ¿Qué pasos deberían seguir? Iniciar sesión en el portal permite a los padres ver y actualizar su información de contacto, así como otorgar o revocar el consentimiento para determinadas actividades relacionadas con la escuela.

Lenguaje sencillo y comunicaciones claras: asegúrese de que todas las comunicaciones relacionadas con el consentimiento y la privacidad estén escritas en términos simples y comprensibles para que los padres y los estudiantes puedan tomar decisiones informadas.

Registro de Consentimiento: Mantenga un registro exhaustivo de todas las solicitudes y concesiones de consentimiento, incluida la ocasión y la empresa precisa para la cual se otorgó el consentimiento.

9.4. Seguridad de Datos

Para proteger la privacidad y cumplir con las leyes de protección de datos, una escuela debe garantizar la seguridad de los datos. Para esta guía generaremos algunos recursos que pueden ayudar al responsable del tratamiento de datos con esta tarea: herramientas, programas, técnicas y ejemplos.

9.4.1. Herramientas para la Seguridad de Datos

Software de Seguridad: Utilice software de seguridad de la información, como antivirus y antimalware, para proteger las computadoras y otro hardware de la escuela.

Firewalls: Se deben implementar cortafuegos de red y sistemas de seguridad perimetral para salvaguardar la infraestructura de red de la escuela de amenazas externas.

Cifrado de datos: Utilice software de cifrado de datos para proteger los datos confidenciales que se almacenan en los dispositivos y viajan a través de las redes.

Gestor de contraseñas: Utilice administradores de contraseñas para asegurarse de que las contraseñas utilizadas para acceder a los sistemas y aplicaciones sean seguras y se administren adecuadamente.

Software de monitoreo de seguridad: Implemente herramientas de monitoreo de seguridad para identificar actividades inusuales o intrusiones en tiempo real.

9.4.2. Métodos y ejemplos para la Seguridad de Datos

Políticas de contraseñas seguras: cree reglas que requieran contraseñas seguras, que deben incluir una combinación de letras, números y caracteres especiales, y fomente la rotación frecuente de contraseñas. Podemos considerar como ejemplo la política de contraseñas: Utilizando combinaciones de letras mayúsculas y minúsculas, números y caracteres especiales, las contraseñas deben tener al menos 8 caracteres. Al menos cada 90 días, poder establecer una nueva contraseña.

Controles de accedo con uso de Roles: Implementar un sistema de control de acceso que restrinja el acceso de los usuarios a los datos y recursos que necesitan para desempeñar sus funciones. Acceso a los datos de los estudiantes, a modo de ejemplo. El acceso a los expedientes académicos de los estudiantes está restringido al personal docente y administrativo autorizado.

Parches y actualizaciones de seguridad: para protegerse contra vulnerabilidades conocidas, mantenga todos los sistemas y software actualizados con las actualizaciones de seguridad más recientes. Los programas de actualización de software son un ejemplo de ello ya que las actualizaciones y parches de seguridad más recientes se aplican automáticamente a los sistemas y aplicaciones.

Copia de seguridad de los datos: Implemente un programa de respaldo regular para garantizar la accesibilidad de los datos en caso de pérdida o daño. El mejor ejemplo posible es un plan de respaldo de copias de seguridad. En servidores y sistemas importantes del centro escolar, se deben realizar copias de seguridad de los datos todos los días.

Conciencia de seguridad: educa al personal y a los estudiantes sobre las mejores prácticas de seguridad, incluida la detección de correos electrónicos de phishing y la prevención de la divulgación de datos privados. Formación en sensibilización en seguridad, por ejemplo. El personal y los estudiantes asisten a sesiones de capacitación anuales sobre mejores prácticas y seguridad cibernética.

Plan de respuesta a incidentes: cree una estrategia de respuesta a incidentes que describa cómo se manejarán y reportarán las violaciones de seguridad, si ocurren. A modo de ilustración lo correcto sería un plan de respuesta a incidentes. Por ejemplo, en el caso de una violación de la seguridad, un equipo de respuesta a incidentes designado actuará de inmediato y puede incluso alertar a las autoridades correspondientes.

9.5. Retención y eliminación de Datos

Para cumplir con las leyes de protección de datos y proteger la privacidad de las personas, es fundamental que los datos se almacenen y eliminen de manera adecuada. Los siguientes recursos pueden ayudar al responsable del tratamiento de datos con su tarea mediante el uso de herramientas, programas, técnicas y ejemplos.

9.5.1. Herramientas para la Retención y eliminación de datos

Software de Gestión Documental: Utilice software de gestión documental para organizar y gestionar documentos y registros que contengan datos personales. SharePoint, DocuWare y M-Files son algunos ejemplos.

Herramientas de programación: Utilice herramientas de programación, como cronjobs en sistemas Linux o tareas programadas en Windows, para planificar la eliminación automática de datos obsoletos.

Herramientas de copia de seguridad: asegúrese de tener herramientas de copia de seguridad confiables para poder realizar una copia de seguridad de los datos importantes antes de eliminarlos.

9.5.2. Métodos y ejemplos para la Retención y eliminación de datos

Política de retención de datos: establezca una política de retención de datos que describa la duración del tiempo que se conservarán los distintos tipos de datos y la fecha en la que se eliminarán. Un ejemplo podría ser el siguiente: Una vez que los estudiantes se gradúen, sus expedientes académicos se conservarán durante diez años antes de ser descartados de forma segura.

Proceso de eliminación Segura: Implemente un proceso de eliminación segura para asegurarse de que los datos se eliminen permanentemente. Esto podría implicar la destrucción física de sistemas o medios de almacenamiento. La trituración destruirá físicamente los discos duros de las computadoras viejas para garantizar que los datos no se puedan recuperar.

Registro de Retención y Eliminación: Mantenga un registro completo de cuándo se conservaron y eliminaron los datos, qué datos se eliminaron y quién estuvo a cargo de la eliminación.

Ejemplo:

"Fecha: 15 de julio de 20XX.

Datos eliminados: Los registros de estudiantes de la clase 20XX

Responsable: [Nombre del responsable].”

Notificar a los interesados: si es necesario, informar a las personas cuyos datos se eliminarán de acuerdo con la política de retención. Por ejemplo, enviar un aviso de eliminación de datos a las personas afectadas.

“Saludos, [Nombre del estudiante/padre].

De acuerdo con nuestra política de retención de datos, por la presente se le notifica que los datos relacionados con [detalle de datos] se eliminarán el [fecha de eliminación].

[Instrucciones adicionales].”

Copia de seguridad de datos importantes: asegúrese de hacer una copia de seguridad de todos los datos importantes que puedan ser necesarios por motivos legales o de auditoría antes de eliminar cualquier cosa. Ejemplo: copia de seguridad de datos críticos. Antes de borrar los registros financieros de los últimos siete años, se realizará una copia de seguridad de esta información en medios seguros y se almacenará de forma segura durante el tiempo necesario.

9.6. Capacitación y Sensibilización

9.6.1. Herramientas para Capacitación y Sensibilización

Plataformas de capacitación online: Utilice cursos interactivos de protección y privacidad de datos utilizando plataformas de capacitación en línea. Moodle, Canvas y Blackboard son algunos ejemplos.

Software de Gestión de Aprendizaje: La implementación de un sistema de gestión del aprendizaje (LMS) simplificará la gestión de los cursos y controlará el progreso del personal.

Herramientas de Comunicación Interna: Envíe actualizaciones y recordatorios sobre políticas de protección de datos utilizando herramientas de comunicación interna como correo electrónico y plataformas de colaboración.

9.6.2. Métodos y ejemplos para Capacitación y Sensibilización

Cursos de Capacitación Obligatorios: Diseña los programas de capacitación necesarios sobre seguridad y privacidad de los datos para todos los empleados, completos con exámenes de conocimientos. Ejemplo: Curso de formación en protección de datos. Los temas incluyen cosas como principios de privacidad, protección de datos privados y derechos individuales. Una hora de duración. Los empleados deben aprobar la prueba de conocimientos con una puntuación mínima del 80%.

Sesiones de concienciación: realice sesiones periódicas sobre temas de privacidad y protección de datos, donde se fomente el debate y se cubran ejemplos del mundo real. Por ejemplo: Tema: Protección de datos confidenciales e identificación de correos electrónicos de phishing. Duración: 30 minutos.

Material de Capacitación Interactivo: Crea materiales de capacitación interactivos para que los miembros del personal practiquen sus habilidades de seguridad, como simulaciones de ataques de phishing. Ejemplo: ataque de phishing simulado. Los empleados deben reconocer los correos electrónicos de phishing falsos y tomar las medidas necesarias después de recibirlos.

Boletines: distribuya boletines periódicos que incluyan consejos de seguridad, actualizaciones de políticas y estudios de casos pertinentes. Ejemplo para utilizar sería un Boletín Mensual de Seguridad. Donde destacamos casos de divulgación no autorizada, consejos de protección de información confidencial y pautas de seguridad en línea.

Programa de Certificación: Ofrece un programa de certificación de protección de datos para que los empleados puedan demostrar su conocimiento y compromiso con las prácticas seguras. Se otorga un certificado a los miembros del personal que finalizan con éxito el programa de formación y aprueban el examen.

Reconocimientos y recompensas: Reconoceremos y recompensaremos a los miembros del personal que demuestran un alto nivel de compromiso y conciencia sobre la seguridad de los datos. Los empleados que participan activamente en la capacitación y demuestran un alto nivel de concienciación sobre la seguridad pueden recibir reconocimiento y recompensas.

9.7. Respuesta a Incidentes y Notificaciones

9.7.1. Herramientas para Respuesta a Incidentes y Notificaciones

Herramientas de gestión de incidentes: Utilice software de gestión de incidentes que permita el registro y seguimiento del desarrollo de incidentes de seguridad de datos. Jira Service Management y ServiceNow son algunos ejemplos.

Plataformas de comunicación interna: Las plataformas de comunicación interna deben mantenerse actualizadas y eficientes para que el personal pueda informar incidentes de forma rápida y segura.

Software para notificación de incidentes: implementar software para notificación de incidentes que permita la notificación necesaria a las autoridades pertinentes y a las partes afectadas.

9.7.2. Métodos y ejemplos para Respuesta a Incidentes y Notificaciones

Procedimientos de respuesta a incidentes: Los procedimientos para responder a diversos tipos de incidentes relacionados con la seguridad de los datos deben desarrollarse con detalle claro y completo.

Ejemplo: Procedimiento de Respuesta a Incidentes

Paso 1: Identificación del incidente.

Paso 2: Evaluación del impacto y alcance.

Paso 3: Contención del incidente.

Paso 4: Notificación a las partes afectadas, si es necesario.

Paso 5: Investigación del incidente.

Paso 6: Mitigación y recuperación.

Paso 7: Documentación del incidente y lecciones aprendidas.

Equipo de respuesta: establezca un equipo de respuesta contra incidentes con funciones y responsabilidades muy definidas. A modo de ejemplo, el equipo estaría constituido por:

1. Coordinador de Incidentes.
2. Responsable de Notificación.
3. Responsable de Investigación.
4. Responsable de Comunicación

Simulacro de Incidentes: realiza simulacros de incidentes de rutina para instruir al personal sobre cómo reaccionar adecuadamente en situaciones de emergencia. Por ejemplo, simulación de un incidente:

"Escenario: Pérdida de datos de estudiantes.

Objetivo: Examinar la capacidad del equipo para controlar la situación y alertar a los afectados."

Notificación a las Autoridades: Establecer un procedimiento para alertar a las autoridades competentes, como la Agencia de Protección de Datos, en caso de incidentes graves de seguridad de los datos. Ejemplo: Notificación a las Autoridades

- Identificación del incidente.
- Evaluación del impacto.
- Notificación dentro de las 72 horas, si es necesario

Comunicación externa: En caso de incidencias significativas, preparar mensajes de comunicación con información clara sobre la incidencia y las actuaciones adoptadas para la prensa y los afectados. Consideremos un mensaje de comunicación externa:

- Descripción del incidente.
- Acciones tomadas para resolverlo.
- Medidas para prevenir futuros incidentes.

Documentación y reportes: Se deben producir informes y todos los incidentes y acciones deben documentarse para analizar las lecciones aprendidas. Usemos de partida crear un informe del incidente con el siguiente contenido:

- Fecha y hora del incidente.
- Impacto y alcance.
- Medidas tomadas.
- Recomendaciones para evitar incidentes futuros.

9.8. Auditoría y Mejora Continua

Para que las políticas y procedimientos de protección de datos sigan siendo efectivos y cumplan con las leyes y regulaciones en evolución, la auditoría y la mejora continua son cruciales. Estos procedimientos ayudan a identificar áreas que requieren mejoras y mantienen estándares estrictos para la seguridad y privacidad de los datos.

9.8.1. Herramientas para Auditorias y Mejora Continua

Software de auditoría: utilice software de auditoría para planificar, realizar y registrar auditorías internas y externas. Los ejemplos incluyen TeamMate y ACL Analytics.

Herramientas de análisis e informes: Utilice herramientas de informes y análisis para evaluar el éxito de las políticas y procedimientos de protección de datos. Los ejemplos populares incluyen Tableau y Microsoft Power BI.

9.8.2. Métodos y ejemplos para Auditorias y Mejora Continua

Plan de auditoria interna: Asegúrese de que su plan anual de auditoría interna incluya una revisión de las políticas, procedimientos y controles relacionados con la protección de datos. Ejemplos de auditoría interna:

- Auditoría de cumplimiento de políticas de protección de datos.
- Auditoría de registros de consentimiento.
- Auditoría de procedimientos de retención y eliminación.

Auditoria externa: Para evaluar el cumplimiento de las leyes y mejores prácticas de protección de datos, programe auditorías externas realizadas por expertos independientes.

- Contratar a una firma de auditoría externa para revisar los procedimientos de protección de datos y emitir un informe de cumplimiento.

Revisión de incidentes pasados: Para determinar las razones detrás de incidentes pasados y mejorar los procesos para evitar que se repitan, realice auditorías específicas.

Ejemplo: Auditoría de Incidente de Divulgación de Datos

- Identificación de las fallas que condujeron a la divulgación no autorizada.
- Implementación de controles adicionales para prevenir incidentes similares.

Medición de Indicadores Clave de Rendimiento (KPI): Definir los KPI relacionados con la protección de datos y realizar un seguimiento de su desempeño en el tiempo.

Ejemplo: KPI de Protección de Datos

- Porcentaje de empleados que han completado la capacitación en protección de datos.
- Tiempo promedio de respuesta a solicitudes de derechos de los individuos.

Entrevistas y Encuestas: Periódicamente realizar entrevistas a los miembros del personal y administrar encuestas para obtener sus opiniones y sugerencias sobre qué tan bien están funcionando las políticas y procedimientos para proteger los datos personales.

Unas preguntas de ejemplo para una encuesta sobre protección de datos podrían ser:

- ¿Crees que las políticas de protección de datos son precisas y acertadas?
- ¿Ha habido casos en los que tuvo dificultades para seguir las políticas de protección de datos?

Informe de auditoría y planes de acción: Crea informes de auditoría que sinteticen hallazgos y recomendaciones, y desarrolla planes de acción para encontrarse con las áreas de mejora identificadas.

Ejemplo: Informe de Auditoría junto con el plan de acción.

- Hallazgo: Falta de registros de consentimiento para ciertos datos.
- Recomendación: Implementar un proceso de registro de consentimiento.
- Plan de Acción: Desarrollar un formulario de consentimiento y establecer un proceso para su registro.

9.9. Documentación y Mantenimiento de Registros

Mantener registros precisos es necesario para respaldar la responsabilidad y la transparencia en la gestión de datos y la protección de la privacidad. Las técnicas y herramientas antes mencionadas garantizarán que los registros se mantengan de manera ordenada y cumplan con los requisitos legales y reglamentarios.

9.9.1. Herramientas para Documentación y Mantenimiento de Registros

Software de Gestión Documental: Organice, almacene y recupere documentos relacionados con la protección de datos utilizando software de gestión de documentos. SharePoint, Documentum y Alfresco son algunos ejemplos.

Sistemas de Administración de Registros (RMS): Implementar un sistema de gestión de registros para controlar todo el ciclo de vida de los registros, desde su creación hasta su eliminación. HP Records Manager y M-Files son dos ejemplos.

9.9.2. Métodos y ejemplos para Documentación y Mantenimiento de Registros

Políticas de Documentación: Establece políticas claras y concisas sobre qué documentos deben mantenerse y cuales no, cuánto tiempo y en qué formato. Definir quién es responsable de mantener los registros.

- Registros de consentimiento se mantendrán durante 5 años a partir de la fecha de obtención.
- El Departamento de Recursos Humanos es responsable de mantener los registros del personal.

Estructura de Carpetas y Etiquetado: Organiza los documentos en carpetas y utiliza un sistema de etiquetado para facilitar la búsqueda y recuperación.

- Carpeta: "Registros de Consentimiento"
- Etiqueta: "Consentimiento de Estudiantes 2023"

Control de Versiones: Implementa un sistema de control de versiones para rastrear cambios en los documentos y mantener un historial durante la documentación.

- Nombre del Documento: "Política de Privacidad"
- Versión 1.0 (Fecha: 01/01/2023)
- Versión 1.1 (Fecha: 15/03/2023, Cambio: Actualización de contacto de privacidad)

Fechas de Retención: Determinar fechas de retención sobre los registros y documentos para asegurarte de que se descarten de manera oportuna cuando ya no sean necesarios.

- Documento: "Registro de Consentimiento de Estudiantes"
- Fecha de Retención: 5 años desde la fecha de obtención.

Auditorías de Registros: Realiza auditorías periódicas de datos para garantizar que se mantengan apropiadamente y que se cumplan las políticas de documentación.

- Revisión de registros de consentimiento para verificar su retención adecuada.

Informes de Documentación: Crea informes de documentación que reduzcan la cantidad y el estado de los registros y documentos relacionados con la protección de datos.

- Total, de registros de consentimiento: 500.
- Total, de registros eliminados en el último trimestre: 25.

Capacitación en Documentación: Facilita capacitación al personal sobre cómo crear y mantener registros de manera efectiva y de acuerdo con las políticas de documentación.

- Tema: Buenas Prácticas en Documentación.
- Duración: 1 hora

10. Conclusiones

Conforme van pasando los años, la tecnología tal y como la conocemos hoy en día desaparecerá y se reinventarán nuevas, o bien se seguirán utilizando las mismas pero mejoradas y actualizadas a los tiempos que están por venir, pero la única cosa que no va a variar es la existencia de datos: datos personales, financieros, etc. Sera de vital importancia que el mismo responsable del tratamiento de datos no solamente acceda a esta guía y la entienda, sino que también la pueda modificar a posteriori entendiendo la evolución tecnología, las leyes que se van a aplicar a y sobre todo a como se van a tratar esos datos. Es por ello por lo que el comienzo de todo debe ser esta guía que no solo garantizara el cumplimiento legal, sino que a la vez se promuevan la protección de la privacidad de los datos y que se acreciente la confianza en la comunidad educativa. A través de este procedimiento se ampliará la conciencia sobre la importancia de los datos y su privacidad y la que se tiene que dar reconocimiento por la gran gestión y complejidad que conlleva gestión datos en una institución educativa.

La guía permitirá que se establezcan políticas claras para poder optimizar los procedimientos llevados por el responsable sobre el tratamiento de datos y poder garantizar una transparencia durante la gestión de datos. Al mismo tiempo, se remarca una responsabilidad ética y legal en el colegio sobre la protección de los datos personales y destaca, dicho en el anterior apartado, la necesaria necesidad de adaptarse a los cambios de normativa que siguen en constante evolución.

Para terminar, la guía será un elemento definitivo y dinámico que fomentará la mejora continua de las practicas y procesos de privacidad y seguridad de los datos, que a su vez también proteger a la reputación del colegio, lo que contribuirá a su éxito y a la confiabilidad dentro de la comunidad educativa

11. Objetivos de Desarrollo Sostenible

Grado de relación del trabajo con los Objetivos de Desarrollo Sostenible (ODS).

Objetivos de Desarrollo Sostenibles	**Alto**	**Medio**	**Bajo**	**No Procede**
ODS 1. **Fin de la pobreza.**				**X**
ODS 2. **Hambre cero.**				**X**
ODS 3. **Salud y bienestar.**				**X**
ODS 4. **Educación de calidad.**	**X**			
ODS 5. **Igualdad de género.**		**X**		
ODS 6. **Agua limpia y saneamiento.**				**X**
ODS 7. **Energía asequible y no contaminante.**				**X**
ODS 8. **Trabajo decente y crecimiento económico.**	**X**			
ODS 9. **Industria, innovación e infraestructuras.**				**X**
ODS 10. **Reducción de las desigualdades**.		**X**		
ODS 11. **Ciudades y comunidades sostenibles**.				**X**
ODS 12. **Producción y consumo responsables.**				**X**
ODS 13. **Acción por el clima.**				**X**
ODS 14. **Vida submarina.**				**X**
ODS 15. **Vida de ecosistemas terrestres.**				**X**
ODS 16. **Paz, justicia e instituciones sólidas.**	**X**			
ODS 17. **Alianzas para lograr objetivos.**	**X**			

Tabla 6: Grado de relación del trabajo con los ODS

Reflexión sobre la relación del TFG/TFM con los ODS y con el/los ODS más relacionados.

Una guía de trabajo para el responsable del tratamiento de datos en una escuela tiene un impacto significativo en múltiples ODS al fomentar prácticas responsables de gestión de datos, respetar los derechos individuales y promover la igualdad, la justicia y el desarrollo sostenible en el ámbito de la educación y más allá. La capacidad de crear un entorno de aprendizaje que respete la privacidad y fomente el acceso equitativo a una educación de alta calidad es lo que le da su importancia.

Al garantizar que la gestión de datos en las escuelas esté en consonancia con los principios de la educación de calidad, la guía puede promover significativamente el ODS 4 (Educación de calidad). La guía puede contribuir a elevar los estándares educativos y crear un entorno de aprendizaje más productivo al ayudar en el establecimiento de políticas y procedimientos eficientes para la gestión de datos en entornos educativos.

El manual puede ser una herramienta útil para promover la igualdad de género (ODS 5: Igualdad de género) en el sector educativo. Se pueden prevenir los prejuicios de género y se puede garantizar la igualdad de oportunidades para todos los estudiantes y empleados mediante prácticas justas y respetuosas de la privacidad.

Al fomentar un entorno de trabajo más seguro y moral en las escuelas, un enfoque adecuado en la gestión de datos puede apoyar el ODS 8(Trabajo decente y crecimiento económico). Como resultado, al preparar mejor a los estudiantes para el mercado laboral, esto puede mejorar la calidad de empleo en el sector educativo y contribuir al crecimiento económico a largo plazo.

Al promover prácticas justas y equitativas de gestión de datos, la guía puede abordar directamente el ODS 10 (Reducción de las desigualdades). Esto incluye salvaguardar el derecho de las personas a la privacidad y prevenir la discriminación o el acceso desigual a la educación y la información.

Una gestión adecuada de los datos en las instituciones educativas puede ayudar a alcanzar el ODS 16 ("Paz, justicia e instituciones sólidas"). Al crear una base de confianza, promover la transparencia, la rendición de cuentas y la gobernanza eficiente de los datos en entornos educativos promueve sociedades más pacíficas y justas.

12. Referencias

[1] BOE-A-2006-7899 Ley Orgánica 2/2006, de 3 de mayo, de Educación. (s. f.). Recuperado 6 de septiembre de 2023, de Boe.es website: https://www.boe.es/buscar/doc.php?id=BOE-A-2006-7899

[2] BOE-A-2018-10751 Real Decreto-ley 5/2018, de 27 de julio, de medidas urgentes para la adaptación del Derecho español a la normativa de la Unión Europea en materia de protección de datos. (s. f.). Recuperado 6 de septiembre de 2023, de Boe.es website: https://www.boe.es/buscar/act.php?id=BOE-A-2018-10751

[3] BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (s. f.-a). Recuperado 6 de septiembre de 2023, de Boe.es website: https://www.boe.es/eli/es/lo/2018/12/05/3/con

[4] BOE-A-2018-16673 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. (s. f.-b). Recuperado 6 de septiembre de 2023, de Boe.es website: https://www.boe.es/eli/es/lo/2018/12/05/3

[5] BOE.es - DOUE-L-2016-80807 Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (s. f.). Recuperado 6 de septiembre de 2023, de Boe.es website: https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

[6] Confidencialidad, N., & Protección De Datos, Y. (s. f.). MODELO DE CLAÚSULA PARA CONTRATOS DE ENCARGA- DOS DEL TRATAMIENTO. Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/clausulas-contratos-encargado-tratamiento.pdf

[7] Gestión del riesgo y evaluación de impacto en tratamientos de datos personales. (s. f.). Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf

[8] GUíAS SECTORiALES AEPD I Guía para centros educativos. (s. f.). Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/guia-centros-educativos.pdf

[9] Juan, C. J. (s. f.). Gabinete Jurídico. Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/2015-0065.pdf

[10] Junio, V. (s. f.). Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo. Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/orientaciones-evaluacion-impacto-desarrollo-normativo.pdf

[11] (S. f.-a). Recuperado 6 de septiembre de 2023, de Gva.es website: https://portal.edu.gva.es/pladigital/wp-content/uploads/sites/1192/2022/03/Tratamiento-de-Datos-en-Centros-Educativos.pdf

[12] (S. f.-b). Recuperado 6 de septiembre de 2023, de Madrid.org website: https://site.educa.madrid.org/ies.ciudaddejaen.madrid//wp-content/uploads/ies.ciudaddejaen.madrid/2022/10/Instrucciones-Proteccion-de-Datos-V2.1.pdf

[13] (S. f.-c). Recuperado 6 de septiembre de 2023, de Archive.org website: https://web.archive.org/web/20091210192125/https://www.agpd.es/portalweb/index-ides-idphp.php

[14] (S. f.-d). Recuperado 6 de septiembre de 2023, de Gob.es website: https://www.educacionyfp.gob.es/dam/jcr:a54d26cd-e431-4970-a45d-aadf572b9964/rat-mefp.pdf

[16] (S. f.-e). Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/2019-0002.pdf

[17] (S. f.-f). Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/convenio-marco-aepd-mecd.pdf

[18] Una breve guía del RGPD para los centros educativos y el profesorado. (s. f.). Recuperado 6 de septiembre de 2023, de SchoolEducationGateway website: https://www.schooleducationgateway.eu/es/pub/resources/tutorials/brief-gdpr-guide-for-schools.htm

[20] Barcelona. (s. f.). Guía de protección de datos para los colegios profesionales y consejos de colegios. Recuperado 6 de septiembre de 2023, de Gencat.cat website: https://apdcat.gencat.cat/web/.content/03-documentacio/documents/guia-col-professionals/apdcat_Guia-colegis-professionals_ES.pdf

[21] Guía sobre el uso de videocámaras para seguridad y otras finalidades. (s. f.). Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/guia-videovigilancia.pdf

[22] Protección de datos - Consejería de Desarrollo Educativo y Formación Profesional. (s. f.). Recuperado 6 de septiembre de 2023, de Juntadeandalucia.es website: https://www.juntadeandalucia.es/educacion/portals/web/ced/centros/seguridad-y-proteccion-de-datos/proteccion-de-datos/-/novedades/detalle/NEMEN06dlVTF/proteccion-de-datos-videovigilancia

[23] (S. f.). Recuperado 6 de septiembre de 2023, de Aepd.es website: https://www.aepd.es/es/documento/cartel-videovigilancia.pdf

[24] ¿Pueden los colegios tomar imágenes de los alumnos durante su actividad escolar? ¿Y subirlas a internet? (s. f.). Recuperado 6 de septiembre de 2023, de AEPD website: https://www.aepd.es/es/prensa-y-comunicacion/blog/pueden-los-colegios-tomar-imagenes-de-los-alumnos-durante-su-actividad

[25] Docentes y su importancia para la protección de datos y la privacidad. (s. f.). Recuperado 6 de septiembre de 2023, de AEPD website: https://www.aepd.es/es/prensa-y-comunicacion/blog/docentes-y-su-importancia-para-la-proteccion-de-datos-y-la-privacidad

[26] de la pandemia por el Covid-, D. el I. (s. f.). 10 claves sobre la protección de datos personales en los centros educativos en tiempos del Covid-19. Recuperado 6 de septiembre de 2023, de Ccoo.es website: https://exterior.fe.ccoo.es/7856f10ef7cf5e15096e6629ba167f34000063.pdf

[27] Información Adicional de Protección de Datos en el Tratamiento de datos para la Gestión de la inscripción de profesores de Primaria y Secundaria de la enseñanza reglada para participar en el concurso escolar. (s. f.). Recuperado 6 de septiembre de

2023, de Gob.es website: https://www.consumo.gob.es/es/protecci-n-de-datos-personales/pdatos-dg-consumo/consumoescolar

[28] (S. f.-b). Recuperado 6 de septiembre de 2023, de Gob.es website: https://www.consumo.gob.es/sites/consumo.gob.es/files/formulario_dd-pd_mc.pdf

13. Bibliografía

[1] Domínguez, A. G. (2004). *Tratamiento de datos personales y derechos fundamentales*. Librería-Editorial Dykinson.

[2] Gómez, E. P., & López, A. S.-C. (2007). *La protección de datos en los centros de enseñanza: recomendaciones para cumplir el régimen jurídico*. Sanchez-Crespo Abogados y Consultores.

[3] Reigada, Antonio. (2006). *La publicación de datos de profesores y alumnos y la privacidad personal: acerca de la protección de datos personales en las Universidades.* Revista de Derecho Político. 10.5944/rdp.67.2006.8999.