Protección de Datos. Profesorado SAED, PTSC y Orientadores

Parte I

Ponente:
Herminia Gil Pérez.
Jefa del Servicio de Protección de Datos de la Delegación de Protección de Datos en la Consejería de Educación y Juventud 917200468

Protecciondatos.educacion@madrid.org

www.dpd.educa2.madrid.org

PARTES I Y II

1. Legislación relacionada con la educación y la protección a menores.
2. La responsabilidad del docente en la protección de datos personales e identidad digital de los alumnos.
3. Análisis y gestión de riesgos del tratamiento de datos sensibles.
4. La seguridad en el tratamiento informático de la información
5. El uso del correo electrónico, la mensajería instantánea y el Registro electrónico de la Administración.
6. El intercambio seguro de información.
7. EducaMadrid, un entorno fiable, confidencial y disponible ppara los docentes.

PRIMERA PARTE

1. Legislación relacionada con la educación y la protección a menores.
2. La responsabilidad del docente en la protección de datos personales e identidad digital de los alumnos.
3. Análisis y gestión de riesgos del tratamiento de datos sensibles

1. Legislación relacionada con la educación y la protección a menores.

Definiciones y conceptos
Contenido de los formularios

Normativa aplicable

- Reglamento General de Protección de Datos (RGPD) que entró en vigor el 25 de mayo de 2018.

- Ley Orgánica 3/2018 de 5 de diciembre, de Protección de Datos Personales garantía de los derechos digitales.

Normativa sectorial

- Ley Orgánica 2/2006, de 3 de mayo, de Educación (Disposición adicional vigesimotercera, sobre Protección de datos)
- Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica

Definiciones sobre protección de datos

- ***Datos de carácter personal*** : información
  - **numérica,** peso, altura, edad, matrícula
    - alfabética, Nombre, apellidos, titulación, profesión
      - **gráfica,** firma
        - fotográfica, nuestra imagen
          - **Acústica,** nuestra voz
          - **o de otro tipo** concerniente a personas físicas identificadas o identificables.
  - Son ***datos especialmente sensibles*** o de categoría especial los que revelan información sobre la esfera más íntima y personal, que puede hacernos más vulnerables: religión, creencias, salud, vida sexual, comisión de infracciones penales o administrativas.

https://www.youtube.com/watch?v=YNEAZihDLlc

Definiciones sobre protección de datos

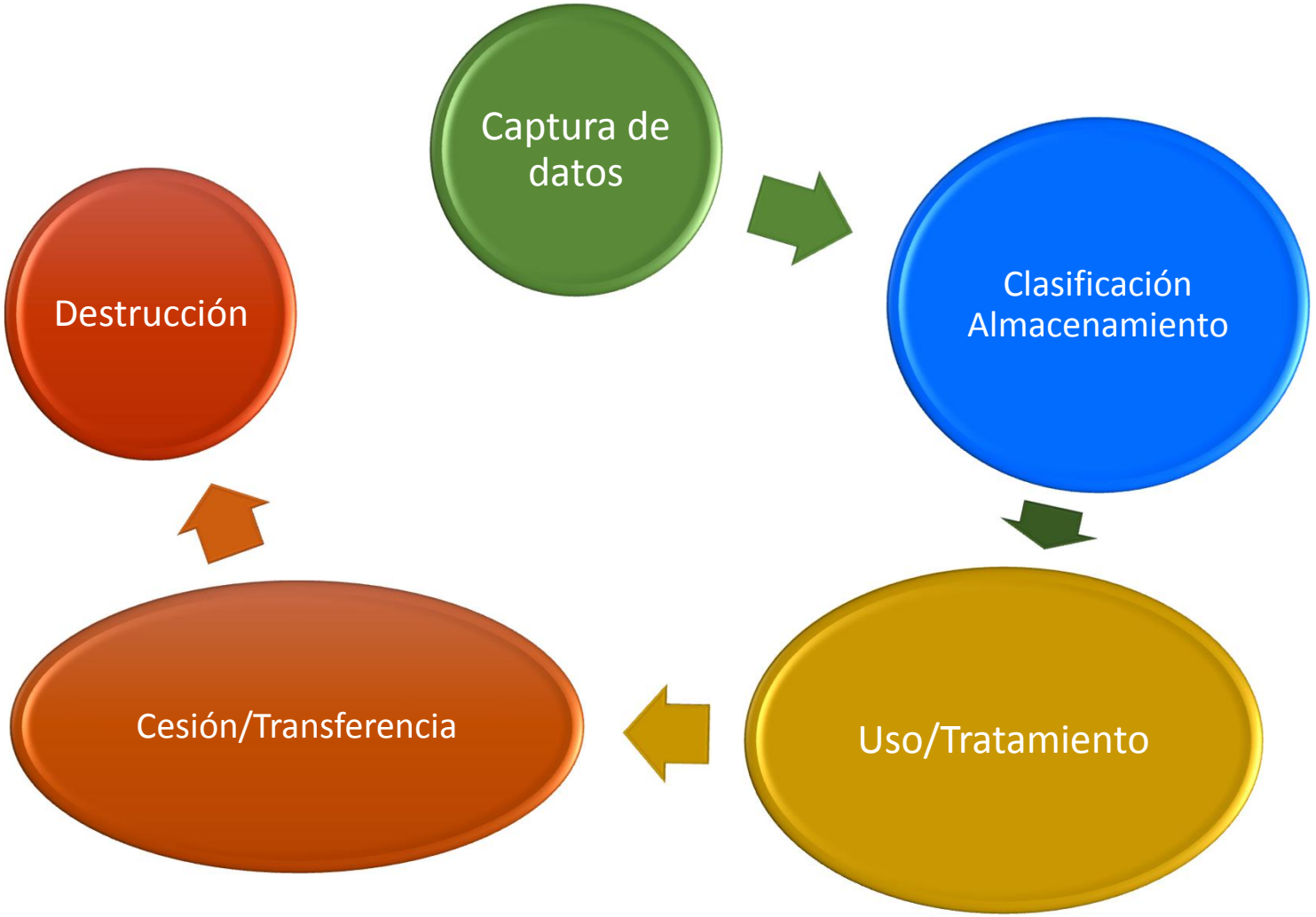
- *Tratamiento de datos* : cualquier operación o procedimiento técnico, sea o no automatizado, que implique la
  - recogida,
  - conservación,
  - modificación,
  - utilización,
  - cancelación,
  - grabación,
  - elaboración,
  - consulta,
  - bloqueo,
  - así como las **cesiones** de datos que resulten de comunicaciones, consultas, interconexiones y transferencias.

Definiciones sobre protección de datos

- *Persona identificable* : toda persona cuya identidad pueda determinarse, directa o indirectamente, mediante información referida a su
  - identidad física,
    - fisiológica,
      - psíquica,
        - económica,
          - cultural
            - o social.

  Una persona física no se considerará identificable si para ello se requiere plazos o actividades desproporcionados

Fases del ciclo de vida de los datos



Sujetos que intervienen en el ciclo de vida de los datos

Responsable

En las Administraciones Publicas, es el órgano administrativo, que **decide sobre la finalidad, contenido y uso del tratamiento**, aunque no lo realice materialmente. En la Comunidad de Madrid, las Direcciones Generales

Encargado de tratamiento

Es la persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, **trata datos personales por cuenta del responsable del tratamiento**, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio, por ejemplo:

MADRID DIGITAL

Delegado de Protección de Datos

- Funciones del Delegado de Protección de datos (artículos 37 y ss del RGPD)
  - Supervisar el cumplimiento del Reglamento y normativa en Protección de Datos, asignación de responsabilidades, la concienciación, formación del personal y auditorías correspondientes.

  - LOPDGDD artículo 34, obligación de designar de un delegado de protección de datos: en los Centros públicos de la Comunidad de Madrid lo designa la Consejería.

  - Artículo 36. El delegado actuará como interlocutor del responsable o encargado del tratamiento ante la Agencia Española de Protección de Datos. El delegado podrá inspeccionar los procedimientos y emitir recomendaciones en el ámbito de sus competencias

Legitimación para tratar los datos

Deber de informar sobre el tratamiento de datos personales

vs

consentimiento

El consentimiento es una más entre las causas para el tratamiento

Cuando exista

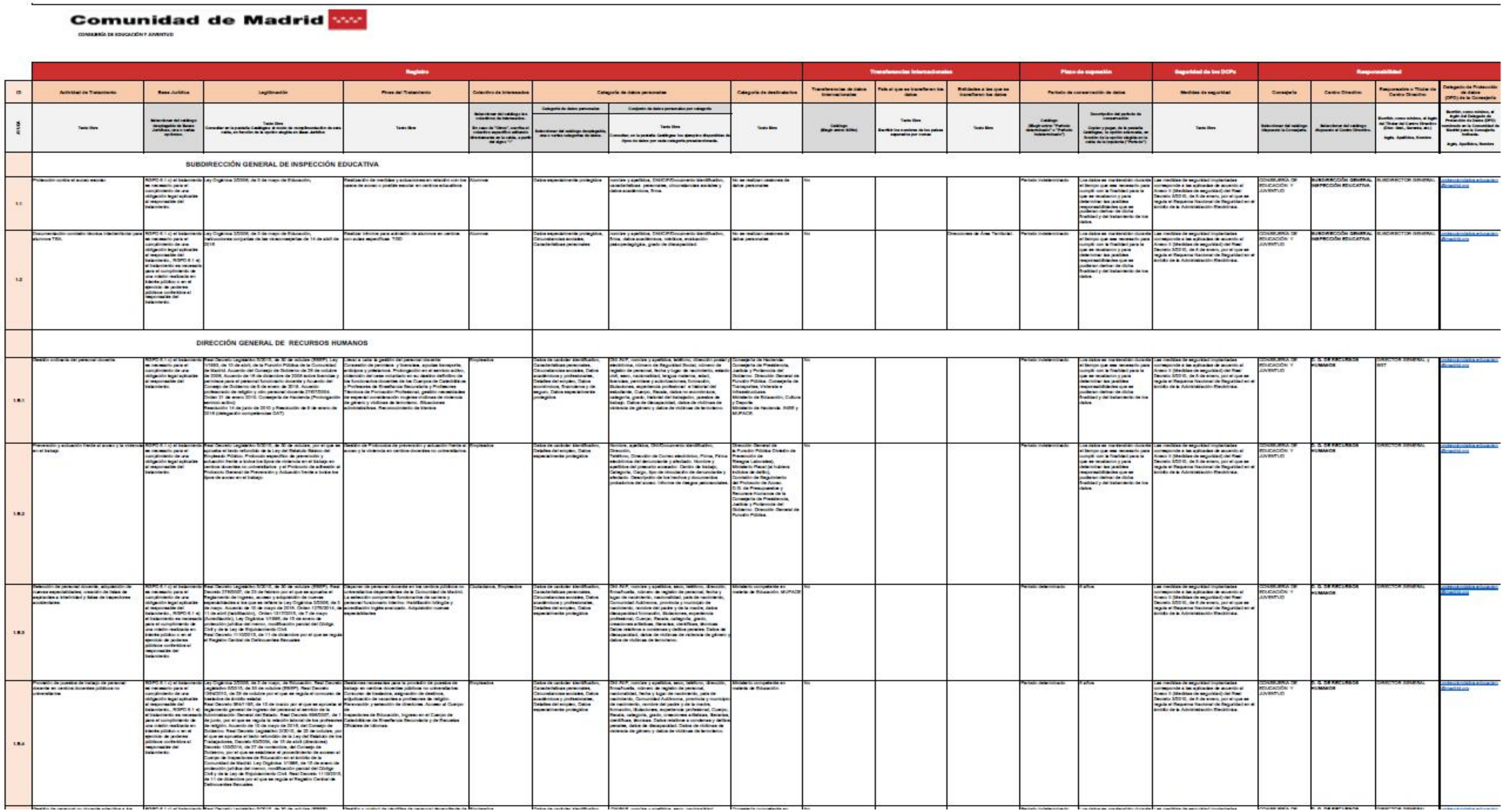
- un contrato o convenio,
- una obligación legal o
- una competencia otorgada por ley,

bastará con informar del tratamiento y no se solicitará el consentimiento, salvo para una finalidad distinta o complementaria de la del tratamiento principal

Las Administraciones Públicas, además de informar sobre el tratamiento que realizan de nuestros datos personales, deben publicar todos sus tratamientos en el **Registro de Actividades de Tratamiento** (RAT)

Registro de Actividades de Tratamiento (RAT) de la Consejería de Educación y Juventud

https://www.comunidad.madrid/gobierno/informacion-juridica-legislacion/proteccion-datos


Comunidad de Madrid
CONSEJERÍA DE EDUCACIÓN Y JUVENTUD
SUBDIRECCIÓN GENERAL DE INSPECCIÓN EDUCATIVA
DIRECCIÓN GENERAL DE RECURSOS HUMANOS

Comunidad de Madrid

- **Cada tratamiento del RAT contiene:**
  - Datos de contacto del responsable y del Delegado de Protección de Datos
  - Bases jurídicas y Fines del tratamiento
  - Categoría de interesados y categoría de los datos personales
  - Categoría de destinatarios
  - Cesiones y Transferencias a un tercer país
  - Plazos para la supresión de las diferentes categorías de datos
  - Medidas técnicas y organizativas de seguridad.

El contenido de cada actividad publicada en el RAT debe proporcionarse al ciudadano cuando rellena un formulario donde va a introducir sus datos personales.

- Por ejemplo, en los formularios de admisión, de matrícula o de recogida del consentimiento para actividades complementarias o extraescolares
- Pero también cuando disponemos de un sistema de video vigilancia debemos tener esa información a disposición del ciudadano

p://www.comunidad.madrid/sites/default/files/ca_educ_y_juv_-_clausula_ddi_videovig.pdf

Cuando los centros educativos realizan actividades complementarias o distintas de las que se recogen en el RAT de la Consejería competente en Educación, deben informar al ciudadano sobre los siguientes aspectos en el formulario de recogida de datos de:

- Identidad y contacto del responsable
- Datos de contacto del delegado de protección de datos
- Base jurídica y fines del tratamiento
- Destinatarios
- Plazo de conservación de los datos personales
- Ejercicios de derechos
- Reclamaciones ante la AEPD.

El RGPD **traslada el centro de gravedad al uso que se realiza del dato personal** (para qué y cómo se utiliza este)
Y se **refuerza el control del interesado sobre sus propios datos**

2. La responsabilidad del docente en la protección de datos personales e identidad digital de los alumnos.

La responsabilidad proactiva

El cambio del enfoque sobre los datos personales orienta la actividad del responsable a través del **Principio de responsabilidad proactiva** ("Accountability"), regulado en el RGPD.

La **proactividad** no significa sólo tomar la iniciativa, sino asumir la responsabilidad de hacer que las cosas sucedan; decidir en cada momento lo que queremos hacer, cómo lo vamos a hacer y ser capaces de **demostrarlo**.

https://youtu.be/GYYiaiSM9bE?t=16

https://www.youtube.com/watch?v=SCupWVzMGxE&t=12s

https://youtu.be/_DnY9OzXLBk

El responsable y el encargado deberán **implantar unas medidas técnicas y organizativas** apropiadas para demostrar que los tratamientos que realizan cumplen con el RGPD.

Estas medidas deberán ser **actualizadas y revisadas periódicamente** a través de procedimientos internos o externos de auditoría.

Con el cambio de enfoque, el RGPD persigue la **anticipación** a la infracción o lesión de derechos. Se busca el **cumplimiento con antelación** para evitar así la lesión o infracción del derecho o libertad del interesado.

Por tanto, es un cambio de enfoque con consecuencias reales, ya que **la falta de adopción de alguna de las medidas** u obligaciones establecidas por el RGPD **puede originar la imposición de una sanción**, sin que previamente exista una lesión de los derechos y libertades del afectado o interesado.

Régimen sancionador en las AAPP (art 77 LOPDGDD)

Resolución de **apercibimiento**.

Proponer la iniciación de **actuaciones disciplinarias**.

Amonestación con denominación del cargo responsable y publicación en BOE o Boletín que corresponda.

Comunicación al Defensor del Pueblo.

Publicación en página Web de la AEPD.

https://www.aepd.es/es/documento/ps-00334-2019.pdf

La AEPD impone una sanción de 10.000 € por publicar sin consentimiento

Las medidas de responsabilidad proactiva a las que hace referencia el RGPD se podrían resumir en las siguientes:

- Delegado de protección de datos
- Registro de actividades
- Medidas de protección de datos **desde el diseño**
- Medidas de protección de datos **por defecto**
- Medidas de seguridad adecuadas
- **Análisis de riesgos** y evaluaciones de impacto

3. Análisis y gestión de riesgos del tratamiento de datos sensibles

La huella y la identidad digital

Tratamiento de datos de menores

El interés superior del menor

¿Por qué es importante conocer los detalles del tratamiento de nuestros datos personales?

Debemos tomar conciencia sobre el control de nuestros datos personales, porque ofrecen mucha información sobre nosotros:

- quiénes somos,
- cómo contactarnos,
- revelan cómo nos comportamos,
- nuestras aficiones, preferencias y hábitos de consumo,
- y revelan información sobre nuestro entorno o familia

Por ello nos interesa proteger nuestra información personal …

- Porque en un contexto determinado nos puede perjudicar, por ejemplo, para optar a un puesto de trabajo.
- Para evitar que caiga en manos de personas malintencionadas que quieran utilizarla en nuestra contra
- O para que empresas u organizaciones no la utilicen de forma poco ética o fraudulenta

Qué ocurre con mis Datos:
Los tengo sólo yo, los estoy cediendo sin saberlo, se los quedan otros distintos a los que se los cedí…?

¿Por qué me vigilan, si no soy nadie? | Marta Peirano | TEDxMadrid

https://youtu.be/NPE7i8wuupk?t=13

El nombre TOR son las siglas de 'The Onion Router', el router Cebolla, y es posiblemente la principal y más conocida Darknet de Internet.

https://www.xataka.com/basics/red-tor-que-como-funciona-como-se-usa

Facebook sabe dónde estás sí o sí (aunque desactives la localización)

https://www.diariosur.es/tecnologia/gadgets/facebook-localiza-desactivado-20191220204142-ntrc.html

https://www.xataka.com/servicios/deep-web-dark-web-darknet-estas-diferencias

La huella digital

- Nuestra huella digital está formada por los rastros que dejamos al utilizar Internet.
- Comentarios en redes sociales, el uso de aplicaciones, registros de correo electrónico – todo esto forma parte de nuestro historial en línea y, potencialmente, puede ser visto por otras personas o almacenado en una base de datos.
- La huella digital es la **suma** de lo que **publicamos**, lo que **compartimos** y lo que **publican otros sobre nosotros**.

La identidad digital

- Es la imagen que proyectamos ante los demás a través de Internet. Esta imagen se forma partir los actos que generan nuestra huella digital.
- La identidad digital incorpora un componente psicológico, pues proporcionamos una información en conjunto que permite que seamos valorados o juzgados por otras personas e incluso por máquinas o algoritmos.

https://ementores.org/caja-de-herramientas/videos/huella-digital-nuestro-rastro-en-internet

¿Cómo dejamos nuestra huella digital?

Teléfonos móviles, tabletas y ordenadores portátiles

- Algunos sitios web generan un listado de los diferentes dispositivos que utilizamos para acceder a los mismos. Aunque muchas veces esto se utiliza como una forma de ayudarnos a proteger nuestras cuentas, es importante comprender qué información recogen sobre nuestros hábitos.

¿Cómo dejamos nuestra huella digital?

Sitios web y compras en línea

- Cada vez que visitamos un sitio web, revelamos información personal al dueño del sitio:
  - ✓ nuestra dirección IP, que puede incluir nuestra información geográfica;
  - ✓ el tipo de navegador y el sistema operativo que utilizamos;
  - ✓ a veces, el último sitio que hemos visitado.

¿Cómo dejamos nuestra huella digital?

Sitios web y compras en línea

- La visita a sitios web y las compras en línea dejan *cookies* que pueden seguir nuestro recorrido de un sitio a otro, permitiendo la entrega de anuncios personalizados.

Una cookie es una forma de conectar múltiples acciones realizadas por la misma persona para formar un hilo conectado.

¿Cómo dejamos nuestra huella digital?

Redes sociales

- Compartir información o hacer comentarios sin habernos preocupado por la configuración de privacidad de nuestro perfil, puede aumentar la visibilidad de nuestros datos

https://www.youtube.com/watch?v=vAeXTPocw3Q

Individualmente, cada huella es pequeña, pero juntas pueden formar un perfil sorprendentemente completo. Cuando varios sitios web deciden compartir entre sí esta información, surge la posibilidad de crear el perfil del usuario o usuaria, utilizando datos como los sitios que ha visitado, los productos que ha comprado o buscado, su dirección y cualquier otro dato que haya proporcionado a cualquiera de los sitios: su edad, sexo, salud, estado civil, empleo, información financiera... la lista incluye todo lo que alguna vez se haya compartido en Internet.

¿Cómo dejamos nuestra huella digital?

Lo que debes saber antes de compartir la foto del primer día de clase de tu hijo

https://www.bebesymas.com/ser-padres/antes-compartir-redes-foto-primer-dia-tu-hijo-piensa-su-seguridad

- **Cuando llegué a la adolescencia tomé conciencia de que mis padres habían compartido toda mi infancia en Internet**

https://www.xataka.com/especiales/cuando-llegue-a-adolescencia-tome-conciencia-que-mis-padres-habian-compartido-toda-mi-infancia-internet

Por qué tu sombra digital es alargada (y resulta mucho más importante y preocupante que tu huella)

https://www.xataka.com/privacidad/tu-sombra-digital-alargada-mucho-que-tu-huella

La sombra digital es la cantidad de información que queda de nosotros en diferentes sistemas (públicos o privados). Dichos datos pueden servir para que, de forma agregada, seamos identificados y por tanto perfilados en cuanto a nuestras preferencias, gustos o costumbres.

La reputación digital

- Nuestra identidad digital es una información cada vez más usada por los departamentos de Recursos Humanos en procesos selectivos de empleo y por los clientes para conocer una empresa

Existen servicios especializados que dan información sobre la reputación *online* de un individuo o una empresa (Brand Rain, Buzzmonitor, Social mention…).
Nuestra huella es nuestro escaparate, lo que conforma nuestra reputación *online*, por ello **es tan importante reflexionar sobre lo que publicamos de nosotros mismos como conocer lo que otros publican sobre nosotros**.

¿Cómo podemos proteger nuestra reputación personal?

- ✓ Concienciándonos,
- ✓ educándonos y
- ✓ tomando las medidas de protección a nuestro alcance

Debemos recordar que nuestra reputación en internet genera en los demás aceptación o rechazo, sin que podamos controlar la información sobre nosotros que circula libremente por internet

https://niltonnavarro.com/cosas-que-debes-borrar-en-redes-sociales

El tratamiento de datos de menores

Protección de los menores en Internet (Art. 84 de la LOPDGDD)

1. Los padres, madres, tutores, curadores o representantes legales **procurarán** que los menores de edad hagan un **uso equilibrado y responsable de los dispositivos digitales y de los servicios** de la sociedad de la información a fin de garantizar el adecuado desarrollo de su personalidad y preservar su dignidad y sus derechos fundamentales.

2. **La utilización o difusión de imágenes** o información personal de menores en las redes sociales y servicios de la sociedad de la información equivalentes que **puedan implicar una intromisión ilegítima en sus derechos fundamentales** determinará la intervención del Ministerio Fiscal, que instará las medidas cautelares y de protección previstas en la Ley Orgánica 1/1996, de 15 de enero, de Protección Jurídica del Menor (LOPJM)

Protección de los menores en Internet (Art. 4 de la LOPJM)

1. Los menores tienen derecho al honor, a la intimidad personal y familiar y a la propia imagen. Este derecho comprende también la inviolabilidad del domicilio familiar y de la correspondencia, así como del secreto de las comunicaciones.

2. La difusión de información o la utilización de imágenes o nombre de los menores en los medios de comunicación que puedan implicar una intromisión ilegítima en su intimidad, honra o reputación, o que sea contraria a sus intereses, determinará la intervención del Ministerio Fiscal, que instará de inmediato las medidas cautelares y de protección previstas en la Ley y solicitará las indemnizaciones que correspondan por los perjuicios causados.

3. Se considera **intromisión ilegítima en el derecho al honor, a la intimidad personal y familiar y a la propia imagen del menor**, cualquier **utilización de su imagen o su nombre** en los medios de comunicación **que pueda implicar menoscabo de su honra o reputación**, o que sea **contraria a sus intereses incluso si consta el consentimiento del menor o de sus representantes** legales.

El interés superior del menor

El interés superior del menor queda establecido por la siguiente normativa:

El artículo 2 de la Ley Orgánica 1/1996, de Protección Jurídica del Menor, introducida por la Ley Orgánica 8/2015, de 22 de julio, de Modificación del Sistema de Protección a la Infancia y a la Adolescencia:

"1. Todo menor tiene derecho a que su interés superior sea valorado y considerado como primordial en todas las acciones y decisiones que le conciernan, tanto en el ámbito público como privado.

En las medidas concernientes a los menores que adopten las instituciones, públicas o privadas, los Tribunales, o los órganos legislativos **primará el interés superior** de los mismos sobre cualquier otro interés legítimo que pudiera concurrir"

El interés superior del menor también está determinado por la jurisprudencia del Tribunal Supremo:

Derecho del niño a que su interés superior sea una consideración primordial que se evalúe y tenga en cuenta al sopesar distintos intereses.

Si una disposición jurídica admite más de una interpretación, se elegirá la interpretación que satisfaga de manera más efectiva el interés superior del niño

LOPDGDD. Artículo 92. Protección de datos de los menores en Internet.

Los centros educativos y cualesquiera personas físicas o jurídicas que desarrollen actividades en las que participen menores de edad **garantizarán** la protección del interés superior del menor y sus derechos fundamentales, **especialmente el derecho a la protección de datos personales, en la publicación o difusión de sus datos personales** a través de servicios de la sociedad de la información.

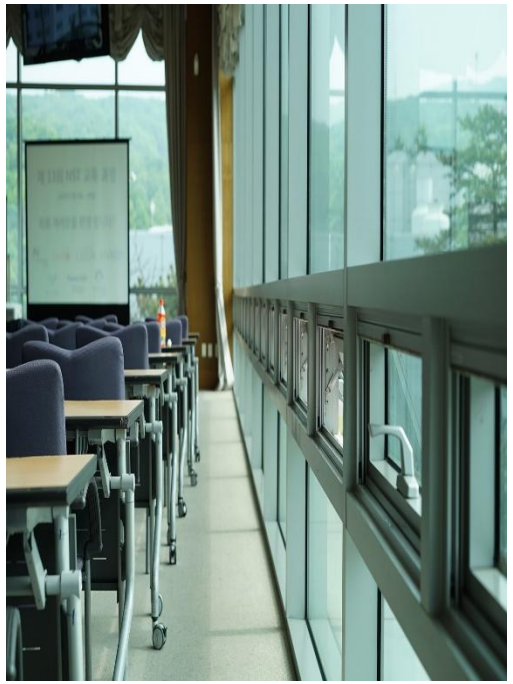
Derecho a la educación digital

Artículo 83. Derecho a la educación digital.

1. El sistema educativo garantizará la plena inserción del alumnado en la sociedad digital y el **aprendizaje** de un uso de los medios digitales que sea **seguro y respetuoso con la dignidad humana**, los valores constitucionales, los derechos fundamentales y, particularmente con el **respeto y la garantía de la intimidad personal y familiar y la protección de datos personales**.

2. Las Administraciones educativas deberán incluir en el diseño del bloque de asignaturas de libre configuración la competencia digital a la que se refiere el apartado anterior, así como los elementos relacionados con las situaciones de riesgo derivadas de la inadecuada utilización de las TIC, con especial atención a las situaciones de violencia en la red.

2. **El profesorado recibirá las competencias digitales y la formación necesaria para la enseñanza y transmisión de los valores y derechos referidos** en el apartado anterior



Vídeo Unicef

https://www.youtube.com/watch?v=WqBl2zyXI7g

Cuatro consejos básicos para compartir imágenes de nuestros hijos de forma segura

Fuente: https://www.bebesymas.com/ser-padres/antes-compartir-redes-foto-primer-dia-tu-hijo-piensa-su-seguridad

1) Desactivar la geolocalización

Muchas redes sociales añaden la ubicación del usuario al publicar la imagen en las redes sociales. Los padres deben asegurarse de que esta función esté desactivada para evitar divulgar su localización.

2) Configurar la privacidad

Solo hay que compartir fotos y otras publicaciones en redes sociales con un público privado. Facebook e Instagram, por ejemplo, permiten compartir información con aquellos usuarios confirmados como contactos, no obstante, todo lo que se publica en estas plataformas debe considerarse como información pública.

Cuatro consejos básicos para compartir imágenes de nuestros hijos de forma segura

3) No publicar fotos de otros sin autorización expresa

Se aconseja ser claros con amigos y familiares sobre las pautas para publicar las imágenes de nuestros hijos. Estas reglas pueden ayudar a evitar situaciones no deseadas en las que un miembro de la familia comparta fotografías sin el permiso explícito de los padres.

Por supuesto, esto incluye también no publicar fotos de amigos o compañeros de clase posando juntos. Son menores y su privacidad concierne a sus padres.

Estas mismas pautas básicas también deberían aplicarlas los propios padres para proteger a los niños de aquellas imágenes que puedan provocar ansiedad en el menor o que den paso al cyberbullying.

Cuatro consejos básicos para compartir imágenes de nuestros hijos de forma segura

4) Borrar toda huella personal

Es una buena opción pixelar el escudo o nombre del colegio en su uniforme o en el babi, para que sea ilegible, y así no se pueda localizar el lugar donde estudia el niño.

Antes de publicar la foto de nuestro hijo, pensemos en su seguridad y asegurémonos de que nuestras cuentas en las redes sociales solo pueden verlas nuestros contactos mas cercanos.

También podemos preguntar a los niños si les parece bien que publiquemos su foto. Porque aunque sean pequeños tienen ya opinión sobre qué les gusta y qué les molesta.

Las fotos perduran en el tiempo y los daños contra su autoestima, podrían aparecer más tarde. Incluso se habla de denunciar a los padres por el sharenting

Si nos concienciamos de los riesgos de una gestión inapropiada de nuestra privacidad y de la de los menores a nuestro cargo o de sus familias, habremos dado el primer paso para adoptar las medidas de seguridad más adecuadas.

De nada sirve disponer de los mecanismos más potentes de seguridad si no tenemos presente que deben aplicarse al conjunto de datos personales que garantice la dignidad humana y la intimidad personal y familiar.

GRACIAS