1.5. Protección de Datos Personales, Privacidad, Seguridad y Bienestar Digital

Introducción

La última competencia del Área 1. Compromiso profesional del Marco Digital Docente. está orientada al **desarrollo del compromiso docente con este objetivo y se ejercita a través de cuatro ejes:**

1. la protección de datos personales, de la privacidad y de los derechos digitales;
2. la seguridad en el acceso a los dispositivos, sistemas y redes;
3. el uso responsable y sostenible de los recursos digitales desde el punto de vista medioambiental y
4. las medidas orientadas a garantizar la salud física y mental.

Un elemento fundamental para el desarrollo de esta competencia es la **protección de datos personales,** pues es una obligación que contrae todo docente en el desempeño de sus responsabilidades y su ejercicio está sujeto al deber de sigilo y debe ser completo desde un primer momento, por lo que no se puede graduar, en ningún caso, su aplicación.

Los **contenidos** que integran esta competencia son:

- Legislación sobre protección de datos personales, privacidad y garantías y derechos digitales en el ámbito educativo.
- Seguridad en el acceso, almacenaje y recuperación de la información.
- Bienestar digital y uso responsable, saludable y sostenible de los recursos digitales

El **nivel B2 de esta competencia** demanda una "*Colaboración en la evaluación de los planes y protocolos del centro relacionados con la protección de datos personales, la privacidad, la seguridad, los derechos digitales y el bienestar al utilizar las tecnologías digitales*". Se logra cumpliendo los siguientes **requisitos**

- 1*.5.B2.1. Colabora en el diseño y la evaluación de los protocolos para la aplicación de las medidas establecidas por la A. E. o los titulares del centro sobre protección de datos personales y garantías de derechos digitales de acuerdo con la normativa vigente.*
- *1.5.B2.2. Contribuye al diseño del plan de convivencia en lo relativo al uso de las tecnologías digitales y a su impacto en el bienestar físico y psicológico del alumnado.*
- *1.5.B2.3. Colabora en la inclusión, en el plan digital de centro, de actuaciones que promuevan la sostenibilidad medioambiental en el uso de los recursos digitales y su posterior seguimiento.*
- *1.5.B2.4. Ayuda, de manera informal, a otros docentes de su centro en la aplicación de las medidas sobre protección de datos personales*

Sintetizando: ¿Colaboro con el equipo directivo en el diseño y evaluación de cualquier iniciativa relacionada con la seguridad, la protección de datos, la garantía de los derechos digitales, el bienestar físico y psicológico del alumnado y la sostenibilidad medioambiental relacionados con el uso de tecnologías digitales?

Aquí vemos **ejemplos de como llevarlo a cabo**:

- Para aquellos servicios o funcionalidades no ofrecidos por la A. E. o los titulares del centro:
  a)Selecciono las tecnologías digitales en función de criterios de privacidad y protección de datos personales garantizando que dichos recursos no recaban ningún tipo de datos personales.
  b)Solicito autorización previa si dichas aplicaciones recaban algún tipo de dato personal.
- Aporto ideas para integrar en el plan de mejora la inclusión y seguimiento de actuaciones que promuevan la sostenibilidad medioambiental (optimización del consumo de energía, control del gasto de impresión, criterios para la sustitución de dispositivos, etc.).
- Ayudo a otros compañeros a identificar los riesgos, para la protección de datos personales o los derechos y garantías digitales del alumnado, que pueden derivarse del uso de alguna aplicación o servicio web.
- Utilizo el cifrado de documentos de texto que contengan datos personales mientras deban estar en mi posesión dentro del flujo de trabajo establecido por las A. E. o los titulares del centro.

Seguridad y privacidad en internet

Decálogo: 10 pasos hacia la ciberseguridad de Aragonesa de Servicios Telemáticos

Actualmente usamos diariamente las nuevas tecnologías tanto en casa como en el trabajo y, en este escenario, desde la **perspectiva de la seguridad de la información, hemos de tener mayor cuidado** pues, como empleados públicos que gestionamos información en primera persona somos el primer perímetro de seguridad de los datos que manejamos.

> De ahí, que sea clave nuestra implicación en la **gestión segura de la información**, desde la adopción de pautas de comportamiento seguro con las tecnologías hasta la integración de medidas de mejora de la seguridad de la información con la que trabajamos.

A continuación, te presentamos **el Decálogo** que nos recomienda seguir el medio técnico del Gobierno de Aragón, Aragonesa de Servicios Telemáticos:

- **Puesto de trabajo.** Mantén la mesa “limpia” de papeles que contengan información sensible. Bloquea la sesión de tu equipo cuando abandones tu puesto. Es sencillo, pulsa a la vez [Tecla Windows + tecla L], tu equipo bloqueará la sesión automáticamente.

- **Dispositivos.** Es mejor que no modifiques la configuración de tus dispositivos si no estás plenamente seguro de lo que quieres modificar. Es arriesgado conectar dispositivos USB no confiables y no está permitido instalar aplicaciones no autorizadas. En tus dispositivos móviles establece una clave de acceso y activa la opción de bloqueo automático.

- **Uso de Equipos No Corporativos.** No manejes información corporativa en equipos de acceso público y, si accedes al correo del Gobierno de Aragón desde tu equipo personal, no descargues ficheros al equipo.

- **Gestión de Credenciales.** No compartas tus credenciales de acceso (usuario y contraseña). Tus credenciales deben ser únicas e intransferibles. No utilices tus credenciales de acceso corporativas en aplicaciones de uso personal porque pueden verse expuestas. No apuntes tus credenciales en lugares visibles.

- **Correo Electrónico.** Fíjate en el emisor del correo y elimina todo correo sospechoso que recibas. Evita los correos en cadena, es decir el reenvío de correos que van dirigidos a un gran número de personas.

- **Navegación.** Evita acceder a páginas webs no confiables y no pinches en enlaces (links) sospechosos. Es preferible escribir la dirección directamente en la barra del navegador y fijarse de que realmente accedes a donde quieres acceder.

- **Viaja Seguro.** Procura no transportar información sensible en dispositivos extraíbles. Si lo haces, cifra la información. No manejes información sensible en redes WIFI no confiables.

- **Protección de la información.** Realiza copias de seguridad de aquella información sensible que sólo esté alojada en tus dispositivos. Más vale un ‘por si acaso’ que un ‘no pensé’.

- **Fugas de Información.** No facilites información sensible si no estás seguro de quién es el receptor de la misma. Destruye la información sensible en formato papel (y si es con una destructora del papel, mejor). En todo caso, no la tires a la papelera.

- **Tú eres la Clave.** Si detectas cualquier actividad sospechosa o un funcionamiento anómalo de tu equipo, avisa al 4100.

Amenazas internas

En este apartado trataremos de dar respuesta al siguiente indicador del marco:

> 1.5.B2.2. Contribuye al diseño del plan de convivencia en lo relativo al uso de las tecnologías digitales y a su impacto en el bienestar físico y psicológico del alumnado.

> *"Conoce a tu enemigo y conócete a ti mismo, y saldrás triunfador en mil batallas."* Sun-Tzu, el Arte de la Guerra

Como ya hemos visto, las redes están llenas de potenciales peligros y amenazas externas pero, ¿qué pasa cuando la amenaza no es externa? A continuación vamos a ver los peligros de la adicción a Internet y los riesgos que conlleva para nuestra salud y bienestar digital.

Uso y consumo de tecnologías digitales

Este punto es muy importante, ya que **está directamente relacionado con nuestra salud.** El uso cada día más asiduo de las redes para la gestión prácticamente de cualquier cosa, hace que **a lo largo del día repitamos movimientos de forma continua** y mantengamos una **postura ergonómica relacionada con el dispositivo que usamos**. Esto significa que que **si el movimiento que repetimos es forzoso, a lo largo de los días desarrollemos una lesión** y acaba por condicionar nuestro estado de ánimo en el trabajo.

Es por ello que hay que **tener en cuenta los siguientes aspectos para tener** un uso sano de las tecnologías:

- **Aspecto postural**. Destacando la postura de la zona cervical y dorsal de la columna vertebral.
- **Aspecto visual**. En el que se destaca el uso prematuro de procedimientos de corrección de la graduación visual del menor por el uso de dispositivos digitales.
- **Aspecto mental**. Éste último es el que más preocupación produce en la sociedad actual, destacando:
  - El uso excesivo de dispositivos digitales, ya que el fin último es el consumo máximo de publicidad personalizada o encubierta por medio de influencers, la segmentación de perfiles para realizar acciones de marketing.

- El ciberacoso o “bullying”, en el que se incluyen la difusión o recepción de bulos o fraudes que provocan desinformación o alarma social, el consumo o generación de discursos de odio, irrespetuosos o agresivos que pueden promover ideas extremistas, generando actitudes intolerantes o violentas y la pertenencia a comunidades que promueven conductas dañinas, trastornos alimenticios, autolesiones o consumo de drogas.

https://www.youtube.com/embed/cojLhNcBdBU

Youtube. Tu vida en las RRSS tiene público. Orange España

Adicción a la tecnología

Como ya hemos visto, las tecnologías digitales han venido para facilitarnos la vida, pudiendo ser de gran ayuda tanto en nuestro entorno laboral como en nuestro ocio. No obstante, su uso excesivo puede suponer un gran problema de salud y bienestar.

Las adicciones, hoy en día, suponen un gran problema de salud y no todas tienen por que ser a sustancias. El DSM-V, (manual de diagnóstico de trastornos mentales) ya ha incluido una sección de "Adicciones no relacionadas a sustancias", así como la OMS, que ya reconoce en su clasificación Internacional de Enfermedades (CIE) el "trastorno por videojuegos".

Señales de Alarma o Red Flags

Cuando una de estas adicciones se presenta, la persona adicta en cuestión puede presentar síntomas a los que hemos de prestar atención como:

- Uso excesivo de las TIC, llegando a perder la noción del tiempo.
- Empeoramiento del rendimiento laboral/escolar
- Apatía hacia otro tipo de actividades.
- Aislamiento social.
- Ansiedad cuando no se están utilizando tecnologías digitales.
- Salud descuidada (sueño, alimentación).
- Síndrome de abstinencia (irritabilidad al no utilizar las tecnologías digitales)

Consecuencias de la adicción a la tecnología

La adicción a las tecnologías digitales, como cualquier otra adicción, supone consecuencias en los planos social, psicológico, y físico.

En el **plano psicológico** se produce una gran inestabilidad emocional, con estados que pueden pasar de la depresión a la agresividad.

En el **plano social** encontramos las siguientes consecuencias: aislamiento social o limitando las relaciones personales a aquellas relacionadas con la adicción, falta de sinceridad con amigos y familiares, no cumplir objetivos ya sean domésticos, laborales o escolares.

En cuanto al **plano fisiológico** encontramos fatiga ocular por el uso de pantallas, fatiga mental y dolores de cabeza por el constante flujo de información así como cansancio y obesidad como consecuencia de un gran número de horas realizando esta actividad sedentaria. Además, los ciclos de sueño se ven alterados, produciendo irritabilidad e, incluso, alteraciones inmunitarias.

> Este es un contenido extensible al módulo 6 dada la vulnerabilidad del alumnado a las tecnologías digitales. Para obtener más recursos para trabajar en el aula visita: tudecideseninternet.es , portal para los más jóvenes de la Agencia Española de Protección de Datos (AEPD) donde encontrarás videos como el siguiente, para trabajar en el aula:

https://www.youtube.com/embed/tLYumn3qo5g

Youtube. UN CRACK DEL BMX (Versión larga). Agencia Española de Protección de Datos.

Adicción al móvil

También conocida como **nomofobia** (*del inglés NO-MObile-phone phobia)* hace referencia a la fobia irracional a no disponer del teléfono móvil físicamente o disponer de él pero sin sus funcionalidades (batería, cobertura), imposibilitando el acceso a la información y actualizaciones que este nos ofrece en redes sociales o servicios de mensajería. Este se enmarcaría dentro de la adicción a la tecnología y sus consecuencias son muy similares: irascibilidad, ansiedad y estrés.

Hemos de prestar atención a las siguientes **señales de alerta** para empezar a plantearnos si una persona tiene adicción al móvil.

- Más interacciones virtuales que reales (Whatsapp, RRSS...)

- El dispositivo es lo primero y lo último que atiendo cada día.
- Angustia, ansiedad e irritabilidad cuando no se puede disponer de las prestaciones del móvil (olvidado, sin batería o sin cobertura).

> SI quieres saber algunos tips de aplicaciones que nos ayudan a controlar nuestro tiempo, mira este vídeo en clave de humor sobre la adicción a los dispositivos:

https://www.youtube.com/embed/3khh4fiA6Xs

Adicción a los videojuegos

Práctica y uso excesivo y compulsivo de los videojuegos. Como todas las actividades, comienza a ser considerada adicción cuando afecta a los hábitos fundamentales del individuo en su día a día.

Como la adicción a la tecnología, interfiere en nuestra vida afectando al espacio y al tiempo dedicado a estas, dañando nuestras interaccione sociales y afectando a nuestra salud física y mental.

Además, los videojuegos, se basan en principios propios de la ludopatía clásica, que los hacen más adictivos como el feedback inmediato, haciendo que el cerebro genere dopamina, sensación placentera.

También se desarrollan en escenarios fantásticos alejados de la realidad.

Derecho a la desconexión digital

Los dispositivos digitales con conexión a internet, han supuesto una gran ayuda en el mundo laboral facilitando opciones como el **teletrabajo,** concepto que empezó a cobrar fuerza durante el primer año de la pandemia por COVID-19 en nuestro país.

Algo tan novedoso, albergaba muchos pros y contras, y entre ellos estaba un elemento que desconocíamos: la desconexión digital.

El hecho de estar confinados y sin un horario establecido de trabajo, hizo que este se extendiera a lo largo de toda la jornada (24 horas), lo que, a la larga, generó situaciones de estrés y ansiedad. No obstante, esta situación ya había sido contemplada en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales:

> **Artículo 88. Derecho a la desconexión digital en el ámbito laboral.**
>
> 1. Los trabajadores y los empleados públicos tendrán derecho a la desconexión digital a fin de garantizar, fuera del tiempo de trabajo legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar."

¿Cómo conseguirlo?

Hay varios tips y herramientas que nos ayudarán a conseguir este propósito (que a veces se vuelve bastante dificil):

1. **Establece y delimita tu horario laboral,** fuera de este, no deberías prestar atención a e-mails o llamadas laborales.
2. Establece **canales para URGENCIAS** de tipo laboral, y lo de urgencias lo escribimos así con mayúsculas, no para cualquier actividad.
3. Aunque ya has establecido un horario laboral, estaría bien que te obligues a tener **periodos sin dispositivos tecnológicos** (PC o smartphone) así como socializar con los tuyos.
4. Utiliza las facilidades que te ofrecen los dispositivos: **Modo no molestar, horario de notificaciones.**.. Para esto, aunque muchos terminales ya disponen de su propio configurador de horario, han surgido distintas apps como OFFTIME, que permite **bloquear un buen número de aplicaciones o llamadas entrantes** que sepas que te pueden molestar o incluso establecer un horario de bloqueo. Puedes conocer más apps para la desconexión digital pulsando aquí.
5. **Separa tu vida laboral de tu vida personal**: Procura no utilizar cuentas personales para asuntos laborales.

Amenazas externas

Phishing, qué es y cómo evitarlo

> El **phishing es una de las estafas con mayor trayectoria** y mejor conocidas de Internet. Es un tipo de fraude que se da en las telecomunicaciones y que emplea trucos de ingeniería social para obtener datos privados de sus víctimas. La diferencia entre Spam y Phishing es clara: el Spam es correo basura, no es más que un montón de anuncios no deseados. **El phishing por otro lado, tiene como finalidad robar tus datos y utilizarlos contra ti.**

La **mayor parte del phishing puede dar como resultado el robo de identidades o de dinero, y también es una técnica eficaz para el espionaje industrial y el robo de datos**. “Algunos hackers llegan incluso a crear perfiles falsos en redes sociales, invierten un tiempo en desarrollar una relación con las posibles víctimas y esperan a que exista confianza para hacer saltar la trampa”.

Un ataque de phishing tiene 3 componentes:

1. El ataque **se realiza mediante comunicaciones electrónicas, como un correo electrónico, un SMS o una llamada de teléfono.**
2. El atacante **se hace pasar por una persona u organización** de confianza.
3. El **objetivo es obtener información personal confidencial**, como credenciales de inicio de sesión o números de tarjeta de crédito.

> Como a veces es difícil detectarlo, aquí te dejamos una serie de **características y trucos que pueden funcionar** para **detectar** un intento de **phishing:**

- Sé **precavido ante los correos** que aparentan ser de entidades bancarias o servicios conocidos (Dropbox, Facebook, Google Drive, Apple ID, Correos y Telégrafos, Agencia Tributaria, etc.) con mensajes que no esperabas, que son alarmistas o extraños.
- **Sospecha si hay errores gramaticales en el texto,** pueden haber utilizado un traductor automático para la redacción del mensaje trampa. Ningún servicio con cierta reputación enviará mensajes mal redactados.
- Si recibes **comunicaciones anónimas del tipo “Estimado cliente”, “Notificación a usuario” o “Querido amigo”,** es un indicio que te debe poner en alerta.

- **Si el mensaje te obliga a tomar una decisión de manera inminente o en unas pocas horas, es mala seña**l. Contrasta directamente si la urgencia es real o no directamente con el servicio o consultando otras fuentes de información de confianza: la OSI, Policía, Guardia Civil, etc.
- **Revisa si el texto del enlace que facilitan en el mensaje coincide con la dirección a la que apunta,** y que ésta corresponda con la URL del servicio legítimo.
- **Un servicio con cierto prestigio utilizará sus propios dominios para las direcciones de email corporativas**. Si recibes la comunicación desde un buzón de correo tipo @gmail.com, @outlook.com o cualquier otro similar, sospecha.
- Aplica la **ecuación: solicitud de datos bancarios + datos personales** = fraude.

Ciberacoso

UNICEF lo define como:

> Ciberacoso es acoso o intimidación por medio de las tecnologías digitales. Puede ocurrir en las redes sociales, las plataformas de mensajería, las plataformas de juegos y los teléfonos móviles. Es un comportamiento que se repite y que busca atemorizar, enfadar o humillar a otras personas.
>
> - **Difundir mentiras o publicar fotografías** o videos vergonzosos de alguien en las redes sociales.
> - **Enviar mensajes, imágenes o videos hirientes**, abusivos o amenazantes a través de plataformas de mensajería
> - **Hacerse pasar por otra persona** y enviar mensajes agresivos en nombre de dicha persona o a través de cuentas falsas.

Y por último, en el caso de que nuestro alumnado reciba el tan temido ciberacoso hay que enseñarles a gestionarlo:

- En un primer momento hay que **crear un clima de confianza con el menor** en el que entienda que se le escucha y se le apoya, evitando culpabilizar a nadie.
- Hay que **guardar evidencias** de la situación generada mediante capturas de pantalla de los mensajes, fotografías o vídeos.
- **Contactar con las Fuerzas y Cuerpos de Seguridad** en caso de reiteración, gravedad o ilegalidad del comportamiento.

IS4K de INCIBE. Ciberacoso escolar.

> INCIBE es el Instituto Nacional de Ciberseguridad y tiene una web específica para el uso seguro en menores (IS4K). En ella se puede obtener más información sobre ciberacoso escolar en el siguiente enlace.

Sexting

Etimológicamente proviene de los anglicismos SEX (sexo) y TEXTING (mensajería de texto) y hace referencia a la producción y difusión de contenido sexual mediante aplicaciones de mensajería digital.

Estudios nacionales afirma que el 31% de los menores de entre 11 y 16 años ha recibido ha recibido mensajes sexuales de algún tipo principalmente por servicios de mensajería instantánea, habiendo aumentado exponencialmente frente al 10% del año 2010.
Entre sus características encontramos:

- Uso de medios digitales para la producción.
- Contenido erótico/sexual
- Protagonistas identificables en el contenido difundido.
- Naturaleza privada en su origen.

Pero pese a ser contenidos privados, pueden ser difundidos debido a:
- Pérdida del dispositivo
- Fallo de seguridad
- Haber sido enviado a un destinatario erróneo
- O difusión posterior por parte del receptor del mensaje sin estar autorizado.

Esto puede acarrear consecuencias como:
- **Sextorsión**: Utilización de material privado de contenido sexual para chantajear.
- **Ciberbulling o Ciberacoso**
- **Grooming**: Forma de acoso en la que un adulto contacta con un menor con el fín de ganarse su confianza para posteriormente involucrarle en una actividad sexual.
- **Pornovenganza**: difusión de contenido íntimo en redes sociales o servicios de mensajería sin consentimiento del protagonista.

Todas estas actuaciones conllevarán a la exigencia de
-**Responsabilidad en materia de protección de datos** por difusión de datos sensibles sin consentimiento.
-**Responsabilidad civil**: por daños y perjuicios materiales y morales, con su consecuente sanción administrativa e indemnización
-Responsabilidad penal: la grabación y difusión de imágenes o vídeos sin consentimiento podrá ser constitutiva de delito, sancionable con penas de hasta 5 años de prisión. Y de **uno a tres meses para quienes difundan, revelen o cedan a terceros sin consentimiento de la víctima**.

https://www.youtube.com/embed/s_O1FlEc1xk

Youtube. No puedes compartirlas sin su consentimiento #RevengePorn. Pantallas Amigas

> Para saber más, échale un ojo al libro de "*Convivencia segura en la red, ciberayudantes*"

Tratamiento de los datos personales en los centros educativos y personas que intervienen

¿Qué es el tratamiento de datos?

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

Resumiendo, es **cualquier actuación que se haga sobre datos personales**, y podrá ser considerada un tratamiento de datos personales.

Fuente propia

Desde la tramitación de los procesos de **admisión del alumnado**, los centros educativos tratan información personal del alumno para proporcionarle los servicios de educación y orientación, que se traduce en acciones muy diversas realizadas por parte de diferentes intervinientes: las autoridades educativas estatales y autonómicas, el centro docente, los órganos de gobierno y participación de los centros, los integrantes de la comunidad educativa (profesorado, alumnado, familias...), con finalidades tan distintas como la confección de los **expedientes académicos**, la **gestión de los comedores** y **transporte escolares**, la **concesión de ayudas para estos conceptos y para material curricular**, la concesión de **premios académicos**, la organización y promoción de actividades educativas, **culturales, deportivas** y de ocio, la evaluación académica, la **orientación del alumnado con necesidades educativas** especiales o específicas, la corrección disciplinaria. Para ello se recogen y registran datos personales, se captan y difunden imágenes del alumnado y profesorado, se organizan eventos, se utilizan recursos didácticos digitales, se comunican datos a diversas instituciones...

Todo ello implica el **tratamiento de un considerable volumen de datos personales** que afectan a toda la comunidad educativa. Este tratamiento se realiza en diversos **formatos, en papel, a través de aplicaciones informáticas,** por medio de empresas externas, con y sin transferencias internacionales de datos.

Por otra parte, algunos de estos datos deberán destruirse tras finalizar el curso escolar o tras agotarse la finalidad de su tratamiento, pero otros se mantienen por tiempo indefinido en los gestores y repositorios de expedientes académicos. Cada uno de estos medios y cada uno de estos períodos de conservación tiene unos riesgos específicos para la protección de datos que debemos

tener en cuenta.

Por lo tanto, desde el origen de un tratamiento hasta su supresión se realizan determinadas operaciones con los datos personales. Cada operación tiene unas reglas básicas que afectan al diseño de cualquier proyecto, al registro del tratamiento, a la transparencia e información a los interesados, a la gestión del tratamiento por el propio responsable o a través de otra persona encargada, al sistema informático utilizado y las medidas de seguridad aplicables, así como a la gestión de los incidentes o brechas de seguridad, al ejercicio de derechos o a cómo conservar y destruir adecuadamente los datos una vez agotada su finalidad.

Infografía Quién es quién. Fuente AEPD.

Responsable

Persona física o jurídica, autoridad pública, servicio u organismo que solo o con otros determine los fines y medios del tratamiento.
En los tratamientos educativos realizados por los centros educativos públicos, son responsables,

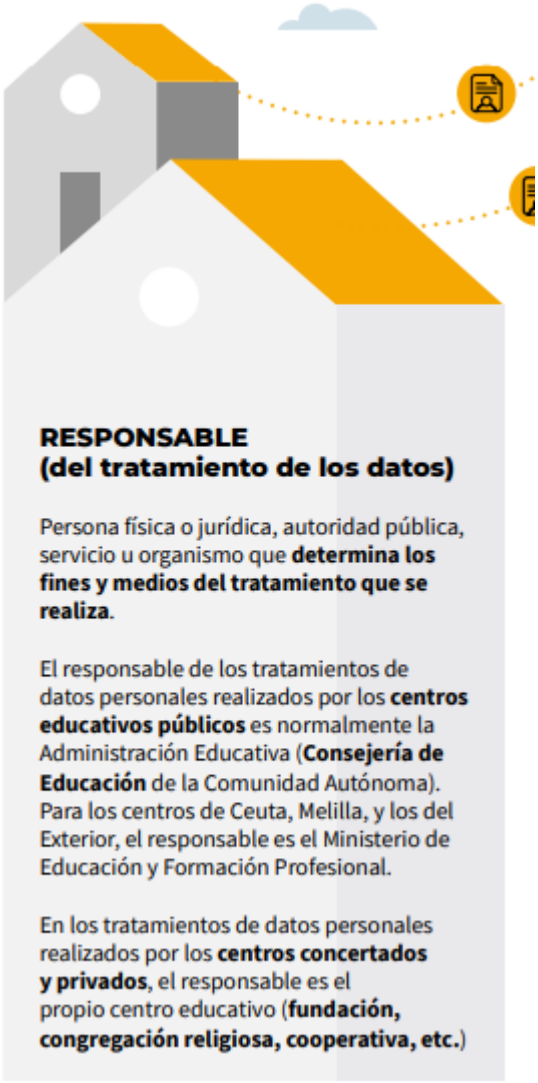
habitualmente, los órganos administrativos de la **Consejería de Educación** o del Ministerio de Educación en su ámbito de actuación respectivo, aunque actúen en muchos tratamientos a través de los centros docentes o de otro personal. El tratamiento de los datos por estas personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable no se considera cesión o comunicación de datos, porque estas personas actúan en nombre del responsable.

El **registro de actividades de tratamiento (RAT)** en las Administraciones Públicas (incluidos los centros docentes) es público y debe ser accesible por medios electrónicos (art. 31.2 LOPDGDD). En los centros públicos, normalmente será **la Consejería de Educación la que se encargue de actualizar ese RAT,** en su caso, con el asesoramiento de los Delegados de Protección de Datos, a quienes deben comunicarse por el responsable las modificaciones, adiciones o supresiones que se hagan en el RAT.

Modificación de la imagen de Mohamed Hassan en Pixabay.

> A continuación se muestran dos ejemplos de RAT de los Departamentos de Educación de Valencia (enlace) y de Educación de Madrid (enlace), donde se desglosan los diferente tipos de actividades y agente involucrados.

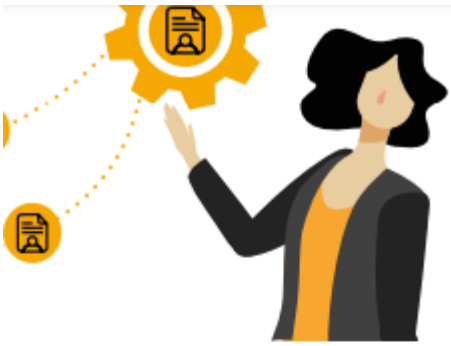
En los centros concertados y privados son responsables los titulares de los propios Centros



Fuente AEPD

Encargado del tratamiento

Persona física o jurídica, autoridad, servicio u organismo que **trata los datos por cuenta del responsable.** Al igual que en el caso de los responsables del tratamiento, **el encargado puede actuar por sí mismo o a través de otras personas que actúan bajo su autoridad directa**. Además, el encargado puede subencargar el tratamiento a otras personas o entidades que actúan siguiendo las instrucciones del encargado principal (y a su vez, ambos, siempre deben actuar en el marco de las instrucciones fijadas por el responsable).
El encargado de tratamiento debe ofrecer las garantías suficientes de aplicación de medidas técnicas y organizativas adecuadas para garantizar la protección de datos y su seguridad.
El encargo requiere la firma de un contrato. En resumen, los encargados asumen la mayor parte de las obligaciones de los responsables con respecto al encargo realizado, pero actúan por cuenta de estos y siguiendo sus instrucciones, fijadas en el acto jurídico correspondiente.



ENCARGADO
(del tratamiento de los datos)

Persona física o jurídica, autoridad, servicio u organismo que **trata los datos por cuenta del responsable**. El responsable determina a quién le encarga el tratamiento que se va a llevar a cabo. Debe ser elegido por éste únicamente **entre los que ofrezcan garantías suficientes** de cumplimiento de la normativa de protección de datos.

El encargado siempre debe actuar en el marco de las instrucciones fijadas por el responsable.

El flujo de datos personales entre el responsable y el encargado no constituye una cesión de datos.

Ejemplos de encargados en el ámbito educativo: prestadores de servicios tecnológicos, empresas que gestionan el comedor escolar, la ruta escolar, las actividades extraescolares, etc.

Fuente AEPD

Delegado de protección de datos

El DPD tiene funciones principales de **supervisión del cumplimiento de la legislación sobre protección de datos**, **asesoramiento a responsables y encargados** en esta materia de protección de datos, cooperación e interlocución con la autoridad de control respectiva, participación en las reclamaciones de los interesados, evaluaciones de impacto y en otros asuntos encomendados a los responsables de los tratamientos.

El DPD puede formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

DELEGADO DE PROTECCIÓN DE DATOS (DPD)

Figura que debe designar el responsable **de forma obligatoria** para todos los centros educativos que ofrecen enseñanzas en cualquiera de los niveles establecidos en la legislación reguladora del derecho a la educación.

Funciones**, entre otras, del **DPD
Asesorar e informar al responsable sobre la aplicación de la normativa de protección de datos y supervisar su cumplimiento.

Interlocutor con las personas afectadas para cualquier cuestión de protección de datos, lo que incluye **dudas**, tanto de las familias como de profesionales de la educación, así como **quejas y reclamaciones**.

El DPD será nombrado por la Administración Educativa correspondiente cuando sea esta la responsable del tratamiento de datos en centros de titularidad pública y, en caso de centros privados o concertados, por el centro educativo.

Fuente AEPD

La LOPDGDD especifica los responsables y encargados que deberán designar un DPD, mencionándose entre ellos los centros docentes que ofrezcan enseñanzas en cualquiera de los niveles educativos. **Esto no significa que cada centro docente deba tener un DPD distinto, sino que todos los centros deben tener un DPD**. A estos efectos, el artículo 37.3 RGPD establece que cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, «se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño».

agencia española protección datos

Contactos DPD Educación CC.AA.

COMUNIDAD/CIUDAD AUTÓNOMA	E-mail del DPD
Andalucía [1] (Autoridad de control propia)	DPD.CED@JUNTADEANDALUCIA.ES
Aragón	PROTECCIONDATOSECD@ARAGON.ES
Asturias	DPD-PRESIDENCIA@ASTURIAS.ORG
Baleares	PROTECCIODADES@DPD.CAIB.ES
Canarias	VEUD.EDUCACION@GOBIERNODECANARIAS.ORG
Cantabria	DPDCENTROSDOCENTES@EDUCANTABRIA.ES
Castilla-La Mancha	PROTECCIONDATOS@JCCM.ES
Castilla y León	DPD.EDUCACION@JCYL.ES
Cataluña [2] (Autoridad de control propia)	DPD.PRESIDENCIA@gencat.cat
Extremadura	DPD@JUNTAEX.ES
Galicia	DPD.CULTURA.EDUCACION@XUNTA.GAL
La Rioja	DELEGADAPD@LARIOJA.ORG
Madrid	PROTECCIONDATOS.EDUCACION@MADRID.ORG
Murcia	DPD.CENTROS@MURCIAEDUCA.ES
Navarra	DPD@NAVARRA.ES
País Vasco [3] (Autoridad de control propia)	DPD-DBO@AVPD.EUS
Valencia	DPD@GVA.ES
Ceuta y Melilla	DPD MINISTERIO DE EDUCACIÓN Y F.P. DPD@EDUCACION.GOB.ES

Fuente AEPD

Los centros concertados y privados también están obligados a tener su propio DPD, si bien, entre varios centros pueden compartir uno.

Interesado

Es la **persona física titular (propietaria) de los datos personales**. Es importante recordar que los responsables o encargados de tratamiento tratan (administran) los datos de los interesados, pero los datos pertenecen únicamente a cada persona física identificada o identificable a la que se refieren.

Fuente AEPD

Además a los interesados les ampara la normativa de protección de datos y le otorga una serie de derechos, los cuales los puede ejercer dirigiéndose ante quien está tratando sus datos (responsable). Los derechos son los siguientes:

- Derecho de información
- Derecho de rectificación
- Derecho de oposición
- Derecho a la limitación de tratamiento
- Derecho de acceso
- Derecho de supresión
- Derecho de portabilidad

Fuente AEPD

Destinatario

Es la persona física o jurídica, autoridad u organismo **a quien se comuniquen (cedan) los datos personales**, ya sea esta persona otro responsable o un tercero.
La cesión de datos será una transferencia internacional cuando el destinatario de los datos está establecido en países fuera del Espacio Económico Europeo (los países de la Unión Europea más Liechtenstein, Islandia y Noruega). En caso de transferencia internacional, el RGPD exige garantías o requisitos adicionales para el tratamiento de datos personales.

Tercero

Es la persona física o jurídica, autoridad, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Autoridad de control

La autoridad pública independiente establecida por un Estado miembro de la UE con arreglo a lo dispuesto en el artículo 51 RGPD. Se llama «autoridad de control interesada» a la autoridad de control a la que afecta el tratamiento de datos personales.
La **Agencia Española de Protección de Datos (AEPD)** es una autoridad administrativa independiente de ámbito estatal, con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones y se relaciona con el Gobierno a través del Ministerio de Justicia.

Agencia Española de Protección de Datos. Fuente AEPD

Tiene atribuidos los poderes y funciones, los más relevantes son las potestades de investigación e inspección, la atención de reclamaciones, la potestad sancionadora, dictar criterios y circulares obligatorias, los planes de auditoría preventiva y directrices.

¿Cuál es el protocolo de actuación en caso de tener una brecha de seguridad?: El **responsable** debe notificar a la correspondiente **autoridad de control** (AEPD) a través del **DPD** en un plazo muy reducido (**72 horas** desde que se tenga conocimiento del incidente), así como la adopción de las medidas cautelares que procedan para evitar perjuicios mayores en la privacidad y, en algunos casos, la notificación del incidente producido también a los **interesados**.

Una ejemplo de plantilla para ir constatando los acuerdos y compromisos del centro puede ser esta.

RESPONSABLE

- La **Consejería de Educación de la DGA** es la responsable en nuestro centro educativo público y tiene que actualizar el registro de actividades de tratamient (RAT).

ENCARGADO

- La **dirección del centro** educativo es habitualmente quien ostenta este cargo, y trata los datos por cuenta del responsable.

DELEGADO DE PROTECCIÓN DE DATOS

- La persona designada por el Departamento de Educación en Aragón tiene el siguiente contacto: **PROTECCIONDATOSECD@ARAGON.ES**

INTERESADOS

- El **alumnado** es el propietario de sus datos, cuando son menores de 14 años, lo tutores legales son los que dan el consentimiento en su nombre, pero los datos son del alumnado. Respecto a sus datos tienen derecho de información, rectificación, oposición, limitación de tratamiento, acceso, supresión y portabilidad

DESTINATARIO

- El **centro educativo**, dependiente del Departamento de Educación, es el organismo al que ceden los datos los interesados.

TERCEROS

- Cualquier persona física o jurídica, autoridad, servicio u organismo autorizado p la Consejería de Educación o dirección. Por ejemplo empresa encargada del comedor escolar o empresa de actividades extraescolares.

AUTORIDAD DE CONTROL

- La Agencia Española de Protección de Datos (AEPD)

Más información sobre protección de datos en centros educativos pulsando aquí.

Protección de datos en centros educativos. Guía 2023

El cifrado de documentos

Existen **diversas formas de cifrar documentos en educación** para proteger su confidencialidad y privacidad. Algunas de las técnicas más comunes son:

Contraseñas

Es posible utilizar **contraseñas para proteger los documentos**. Para ello, se puede utilizar una aplicación de software de procesamiento de texto que permita agregar una contraseña para abrir y modificar el documento. De esta forma, solo las personas autorizadas que tengan la contraseña podrán acceder al contenido del documento.

EJEMPLOS DE CONTRASEÑAS QUE NO DEBEMOS UTILIZAR

Ejemplo de cifrado de documentos
Office Google Docs

Cifrado de archivos

También es posible cifrar los archivos de los documentos utilizando **herramientas de cifrado de archivos.** Estas herramientas convierten los archivos en un formato ilegible sin la clave de descifrado, lo que protege la información confidencial del acceso no autorizado.

Por otro lado, los servicios en la nube cada vez son más populares ya que nos permiten alojar gran cantidad de información que no queremos perder con la tranquilidad de que siempre va a estar ahí. Pero a veces surgen fallos de seguridad que ponen en riesgo nuestra privacidad, de manera que, para evitar problemas, lo mejor que podemos hacer es **cifrar nuestros archivos antes de subirlos a la nube.**

Ejemplos de cifrado de archivos

Encriptación de Windows y en la nube

Herramientas de cifrado de archivos (entrono Windows)

Encripatador de datos (entrono iOS)

> Es importante recordar que, independientemente del método de cifrado utilizado, se deben establecer políticas de seguridad claras y asegurarse de que todas las partes involucradas comprendan y sigan estas políticas.