

# 5. Protección de datos personales, privacidad, seguridad y bienestar digital

En el capítulo final, adoptaremos y evaluaremos las medidas sobre protección de datos, privacidad, seguridad, derechos digitales y bienestar digital aplicadas en el centro educativo.

A través de la 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.

- [1. Tratamiento de datos personales en centros educativos](#)
- [2. Seguridad y privacidad en Internet](#)
  - [2.1. Amenazas internas](#)
  - [2.2. Amenazas externas](#)

# 1. Tratamiento de datos personales en centros educativos

## ¿Qué es el tratamiento de datos personales?

Es 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, **cualquier actuación que se haga sobre datos personales** podemos considerarlo un tratamiento de datos personales.

## CUÁLES SON TUS DERECHOS DE PROTECCIÓN DE DATOS

La normativa de protección de datos te otorga una serie de derechos. Para ejercerlos, debes dirigirte ante quien está tratando tus datos ("responsable")





### Derecho de información

El responsable siempre debe identificarse, informarte para qué se utilizan tus datos y además decirte:

- La razón por la que tus datos son necesarios
- Hasta cuándo los conservará
- Cómo puedes ejercer tus derechos de protección de datos
- Cuál es la base jurídica del tratamiento
- Si los va a ceder a terceros o transferir a otros países
- Si los van a utilizar para elaborar perfiles tienes **derecho a oponerte si se adoptan decisiones automatizadas** que te afecten jurídicamente o de manera similar



### Derecho de rectificación

Te permite corregir tus datos o completarlos si son inexactos o incompletos.



### Derecho a la limitación de tratamiento

Permite solicitar la suspensión del tratamiento de tus datos cuando:

- Impugnes su exactitud, durante el período en el que se comprueba
- Te opongas al tratamiento, mientras se verifica si prevalece el interés legítimo del responsable
- El tratamiento sea ilícito, pero te opones a su supresión y en su lugar solicitas que se limite
- Cuando los necesites para la formulación, ejercicio o defensa de reclamaciones



### Derecho de oposición

Puedes oponerte a que una entidad trate tus datos:

- Por motivos personales salvo que el responsable acredite un interés legítimo
- Cuando el tratamiento tenga por objeto el marketing directo



### Derecho de supresión ("derecho al olvido")

Puedes solicitar la eliminación de tus datos personales cuando:

- Ya no sean necesarios para los fines para los que se recogieron
- Retires el consentimiento que diste, siempre que no haya otra causa que legitime el tratamiento
- Tus datos hayan sido tratados ilícitamente
- Te hayas opuesto a su tratamiento y no prevalezca el interés legítimo, o si el tratamiento tuviera por objeto el marketing directo
- Deban suprimirse para cumplir una obligación legal
- Se hayan obtenido siendo menor de edad en relación con los servicios de la sociedad de la información



### Derecho a la portabilidad

Cuando el tratamiento esté basado en tu consentimiento o en la ejecución de un contrato, y se efectúa por medios automatizados, puedes recibir tus datos en un formato que permita transmitirlos a otro responsable.

**Más información sobre tus derechos y cómo ejercerlos en:**  
<https://www.aepd.es/es/derechos-y-deberes/conoce-tus-derechos>

 [www.aepd.es](http://www.aepd.es)
 [AEPD\\_es](https://twitter.com/AEPD_es)

Noviembre 2021

Infografía. *Cuáles son tus derechos de protección de datos.* [AEPD.](https://www.aepd.es)

**En los centros educativos, debemos extremar las precauciones,** puesto que trabajamos con un gran volumen de datos.

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 instituciones:


- 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...)

Todo ello 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.

Por lo que, se recogen y registran múltiples 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.

**Para profundizar más**, te proponemos que veas la siguiente **EDUcharla** 

<https://www.youtube.com/embed/ZICN29pU-cc>

Youtube. "La protección de datos en los centros educativos" INTEF.

**¿Quién es quién en el tratamiento de datos personales en un centro educativo?**

## QUIÉN ES QUIÉN en el tratamiento de datos personales en tu centro educativo



### INTERESADO/A

Es la **persona física titular** (propietaria) de los datos personales.

Los datos **pertenecen** únicamente a cada **persona física** identificada o identificable a la que se refieren (alumnado, profesorado, progenitores, personal de administración y servicios, proveedores, etc.)

Si los datos tratados corresponden a menores de 14 años, sus progenitores o tutores legales, en su caso, prestarán el consentimiento en su nombre, pero los datos personales son de los/las menores.

### RESPONSABLE (del tratamiento de los datos)

Persona física o jurídica, autoridad pública, servicio u organismo que **determina los fines y medios del tratamiento que se realiza**.

El responsable de los tratamientos de datos personales realizados por los **centros educativos públicos** es normalmente la Administración Educativa (**Consejería de Educación** de la Comunidad Autónoma). Para los centros de Ceuta, Melilla, y los del Exterior, el responsable es el Ministerio de Educación y Formación Profesional.

En los tratamientos de datos personales realizados por los **centros concertados y privados**, el responsable es el propio centro educativo (**fundación, congregación religiosa, cooperativa, etc.**)

### 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.



### 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.

Infografía. *Quién es quién en el tratamiento de datos personales en tu centro educativo.* [AEPD.](http://www.aepd.es)

Si quieres saber más sobre protección de datos en centros educativos pulsa [aquí](#).

## 2. 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.

## 2.1. Amenazas internas

### Uso y consumo de tecnologías digitales

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 **si el movimiento que repetimos es forzoso, a lo largo de los días desarrollamos 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.

### Adicción a la tecnología

<https://giphy.com/embed/QYWva5M1nBfLcT46Vr/video>

*Melt into your chair* de Boy Tillekens en [Giphy](#)





*legal o convencionalmente establecido, el respeto de su tiempo de descanso, permisos y vacaciones, así como de su intimidad personal y familiar."*

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

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.

Puedes conocer **más apps para la desconexión digital** pulsando [aquí](#).


## 2.2. Amenazas externas

### El Phishing

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.

Para saber más, te proponemos ver el siguiente vídeo 

<https://www.youtube.com/embed/uhzV5-iFb5E>

[Youtube](#). ¿Qué es el phishing? [INCIBE](#)

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 señal**. 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**.

En nuestro trabajo, tendremos que tener **mucho cuidado al revisar nuestras bandejas de entrada del correo corporativo**, por lo que te recomendamos leer la siguiente infografía para poder detectar los correos electrónicos maliciosos:



**Cómo identificar un correo electrónico malicioso**

Cientos de emails fraudulentos llegan a nuestras bandejas de correo y, aunque muchos son eliminados, otros consiguen su objetivo, ser leídos. Depende de nosotros saber cómo identificar un correo electrónico malicioso:

- 1 REMITENTE**  
¿Esperabas un email de esta persona/entidad?  
Comprueba que el email coincida con la persona o entidad remitente que dice ser o si está suplantando a alguien.
- 2 ASUNTO**  
¿Capta tu atención el asunto del correo?  
La mayoría de correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención. Ten en cuenta esta consideración.
- 3 OBJETIVO DEL MENSAJE**  
¿Cuál es el objetivo del correo?  
Una entidad de servicios como el banco, suministros del hogar (agua, gas) u otros nunca te pedirá tus datos personales por correo. Además, si es de carácter urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un fraude.
- 4 REDACCIÓN**  
¿Tiene errores ortográficos o parece una mala traducción de otro idioma?  
Revisa la redacción en busca de errores de ortografía o gramaticales. Además, si no está personalizado o parece una traducción automática, sospecha.
- 5 ENLACES**  
¿Los enlaces llevan a una página legítima?  
Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que redirige. Si no coincide o es una web sin certificado de seguridad (https://), no hagas clic.
- 6 ADJUNTOS**  
¿Contiene un archivo adjunto que no estabas esperando o es sospechoso?  
Analiza los adjuntos antes de abrirlos, puede tratarse de un malware. Los antivirus y analizadores de ficheros te ayudarán a identificar si están infectados.

Finalmente, **no olvides utilizar el sentido común y aplicar todos los contenidos que se encuentran en la OSI para convertirte en un usuario ciberseguro.**

¡Sigue estas pautas y disfruta de un correo electrónico libre de riesgos!

Mantente al día con nuestras campañas de concienciación para estar informado.  
**¡Es nuestra mejor defensa!**  
[www.incibe.es](http://www.incibe.es) | [www.osi.es](http://www.osi.es)

Infografía. *Cómo identificar un correo electrónico malicioso.* [INCIBE](http://www.incibe.es).

## El 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](#).

**INCIBE** es el Instituto Nacional de Ciberseguridad y tiene una web específica para el uso seguro en menores (IS4K). En ella puedes obtener más información sobre **[ciberacoso escolar](#)**.

## Sexting

[https://www.youtube.com/embed/s\\_O1FIEc1xk](https://www.youtube.com/embed/s_O1FIEc1xk)

[Youtube](#). No puedes compartirlas sin su consentimiento #RevengePorn. [Pantallas Amigas](#)

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.

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
- 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)
- **Ciberbullying o Ciberacoso**
- **Grooming** (forma de acoso en la que un adulto contacta con un menor con el fin 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)

Para saber más, échale un ojo al libro de "[\*\*Convivencia segura en la red, ciberayudantes\*\*](#)"