Mejora el PDC. Protección de datos personales, privacidad y seguridad

Privacidad y seguridad van de la mano

Privacidad y seguridad van de la mano

Riesgos de Internet

image.png

Internet es una herramienta poderosa que nos brinda una amplia gama de posibilidades, pero también conlleva ciertos riesgos que deben ser considerados por los centros educativos y las familias para proteger a los menores. Sobre todo desde la aparición y acceso a las redes sociales, entornos que les permiten abrir un perfil con datos personales para comunicarse y compartir información con otras personas, ya sea de forma pública o restringida.

Un ejemplo concreto en el ámbito educativo sería el de los **festivales de fin de curso, u otras actividades,** donde las familias toman fotos o graban vídeos. El centro educativo informará a los asistentes que esas fotos y vídeos son para uso exclusivo en el ámbito personal y doméstico y no deben de publicarse abiertamente en las redes sociales, puesto que se vulnera la protección de datos de los menores.

image.png

Fuente AEPD

Los riesgos más graves son aquellos que afectan a la integridad, tanto física como emocional, de los menores. No es fácil evitarlos, no son infrecuentes y, aunque no se produzca agresión física por parte de los acosadores, los efectos sobre la víctima pueden ser devastadores.

Dichos riesgos están relacionados con:

- La **publicación de datos personales:**

- **Suplantación de identidad**: cuando alguien se hace pasar por otra persona generalmente para cometer algún delito u obtener algún beneficio en nombre de otra persona de forma ilícita.

- **Engaño pederasta o *grooming***: Situación en la que un adulto se hace pasar por un menor para ponerse en contacto con un niño o niña, para luego ganarse su confianza y finalmente cometer algún tipo de abuso o chantaje sexual.

- Un **uso incorrecto de las redes sociales:**

- **Ciberacoso**: la realización de comentarios y publicaciones negativas o humillantes en redes sociales supone una forma de acoso en el entorno digital. Dar *me gusta*, compartir las burlas o no denunciarlas también implica ser cómplice.

- **Uso excesivo**: el no establecer límites de tiempo, descuidando otras actividades tan importantes como la comida, la actividad física o el descanso, puede generar en muchos casos síntomas de dependencia o adicción.

- El acceso a **contenidos inadecuados** puede exponer a los menores a bulos y fraudes, discursos de odio y publicaciones de comunidades peligrosas en las que se fomentan malos hábitos relacionados con desórdenes de alimentación, autolesión, consumo de drogas, etc.

A pesar de todo lo anterior, es posible usar internet y las redes sociales de manera positiva y segura, todo ello dependerá de cómo se utilicen y cómo sea la actitud del menor frente a ellas. Por ello nuestra labor, ya sea como docentes o como familiares, implica el ejercer de guías y acompañantes durante todo ese proceso.

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

logo.png

Privacidad y seguridad van de la mano

El factor humano

La seguridad y, por tanto, también la ciberseguridad en nuestro ámbito tienen como fin último la protección de los centros educativos y las personas que conforman la comunidad educativa a través de la protección de sus dispositivos y redes utilizando medidas organizativas, jurídicas y técnicas. Las medidas de ciberseguridad protegen los sistemas, redes y servicios de las administraciones públicas, las entidades privadas o, incluso, a nuestro entorno doméstico de ataques tecnológicos. Sin embargo, **la ciberseguridad no es un fin en sí mismo, sino un medio** para proteger a las organizaciones y a las personas.

El **factor humano** es el elemento clave que hay detrás de la cadena de garantías de la seguridad y, a la vez, el activo final a proteger. Sin embargo, si la información personal de cada individuo está expuesta, éste será vulnerable a ataques de ingeniería social específicamente dirigidos a sus debilidades. De esta forma, el atacante podrá alcanzar tanto a la organización como a los individuos, sorteando las protecciones tecnológicas.

image.png

Fuente Incibe

Durante el año 2020, el 85% de las brechas tecnológicas involucraron el factor humano. La realidad pone de manifiesto que el camino más fácil para comprometer una organización es conseguir que, desde dentro, se abran las puertas a los intrusos, o incluso que ejecute directamente las acciones que el intruso desea. Para conseguirlo se han desarrollado las técnicas de ingeniería social.

image.png

¿Qué es la ingeniería social?

Es la acción de **engañar o chantajear** a una persona para que revele información o emprenda una acción que pueda usarse para comprometer o afectar negativamente un sistema o una organización, en nuestro caso sería el entorno educativo. Se aprovechan de la forma de ser las personas, ya que ofrecemos facilidades a la ingeniería social con nuestras actitudes:

- **Todos queremos ayudar.**
- El primer movimiento es siempre de **confianza hacia el otro.**
- **No nos gusta decir NO.**

- A todos nos **gusta que nos alaben.**

Existen diferentes técnicas de ingeniería social:

image.png

Infografía del Incibe

> Una ejemplo de plantilla donde plasmar acuerdos y compromisos en materia de seguridad en el centro puede ser esta.image.png

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

logo.png

Protección de datos personales y privacidad

Protección de datos personales y privacidad

Ideas principales sobre los datos personales y privacidad

¿Qué es un dato personal?

DATO PERSONAL (Art.4.1 RGPD):
«Toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.»

Captura de pantalla_20230127_162002.png

Fuente propia

La lista recogida en el artículo anterior del RGPD no es exhaustiva. Por lo tanto, dato personal puede ser cualquier información que sirva para identificar a una persona física. Es decir, un dato identificativo como el nombre y apellidos, el DNI, una huella dactilar, un conjunto de rasgos físicos, un número de identificación escolar o la imagen o la voz que permitan la singularización del interesado.

image.png

Imagen de Christina Smith en Pixabay.

> Más información en la guía para centros educativos de la AEPD

Datos de especial protección

Los datos de menores de edad tienen una especial protección:
Según el RGPD los niños merecen una protección específica, ya que pueden ser menos conscientes de los riesgos, consecuencias,
garantías y derechos concernientes al tratamiento de datos personales. Dicha protección específica

debe aplicarse en particular, a la utilización de datos personales de niños con fines de mercadotecnia o elaboración de perfiles de personalidad o de usuario, y cuando se utilicen servicios ofrecidos directamente a un niño.

Diversas leyes otorgan a los menores de edad una especial protección y con el concepto de "interés superior del menor" se establecen obligaciones que afectan a las instituciones públicas y privadas y a todas las personas que traten con menores de edad, en orden a proteger sus derechos y libertades, entre ellos el de protección de datos personales.

Categorías especiales de datos

Son aquellos datos personales que revelan:

- **El origen étnico o racial**

En los centros a veces se reparten algunos cuestionarios elaborados por ejemplo en el ámbito de ayudas de la UE que incluyen preguntas relativas al origen étnico o racial (entre otras cuestiones reveladoras de las circunstancias sociales de los perceptores de las ayudas).

- **Las opiniones políticas**
- **Las convicciones religiosas o filosóficas**

En el servicio de comedor también se facilitan determinados datos por las familias sobre las restricciones o preferencias derivadas de la pertenencia a determinadas religiones.
La AEPD ha considerado sin embargo que «No tiene la consideración de categoría especial de datos o datos sensibles el que un alumno curse la asignatura de religión, ya que el mero hecho de cursar la misma no implica revelación de su confesión religiosa».

- **La afiliación sindical**

La información sobre la pertenencia a sindicatos de estudiantes es un ejemplo de tratamiento de datos reveladores de la afiliación
sindical.

- **Los datos genéticos**

Relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una
información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica.

- **Los datos biométricos**

Obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.

Los datos que se traten deben ser adecuados, pertinentes y proporcionados en función de su finalidad. Es decir, hay que realizar un
juicio de necesidad y proporcionalidad para descartar «que no haya otros medios menos intrusivos para ello y que de su tratamiento se deriven más beneficios para el interés general que perjuicios sobre otros bienes y valores».
La AEPD ha admitido la utilización de la huella dactilar para finalidades como el control de acceso al servicio de comedor en centros escolares con un gran número de alumnos, siempre que se adopten medidas que refuercen la confidencialidad de los datos como la conversión de la huella a un algoritmo, el cifrado de la información, la vinculación a un dato distinto de la identificación directa del alumno o la limitación de los protocolos de acceso a los datos.

> Para más información sobre datos biométricos pulsa aquí

- **Datos relativos a la salud**

Revelan la salud física o mental del alumnado, en el pasado, presente o futuro.

«Los centros educativos recaban en muchos casos, a través de sus servicios médicos o botiquines, datos de salud relacionados con las lesiones o enfermedades que pudieran sufrir los alumnos durante su estancia en el centro. También recogen datos de salud de los alumnos para el ejercicio de la función educativa, discapacidades físicas o psíquicas, por ejemplo del síndrome TDAH (trastorno por déficit de atención e hiperactividad).
Para prestar el servicio de comedor también es necesario recabar datos de salud que permitan conocer los alumnos que son celiacos, diabéticos o que padecen alergias alimentarias. También son datos de salud los contenidos en los informes psicopedagógicos de los alumnos»

- **Datos relativos a la vida sexual**
- **Datos relativos a la orientación sexual**

Para el cumplimiento de los principios y derechos de diversidad sexual y de género y la no discriminación, se han establecido en las
Comunidades Autónomas protocolos que obligan al tratamiento en los centros educativos de datos reveladores de la orientación sexual.

¿Cuáles pueden ser las primeras acciones para velar por los datos personales en un centro educativo, a la hora de

presentar datos a la comunidad educativa?

- **Seudonimización** es una medida utilizada para impedir la identificación del interesado por terceras personas, mediante la disociación de la identidad del interesado y del dato personal, sustituyendo la identidad real por un identificador ficticio (seudónimo) y manteniendo determinada información adicional separada que permite volver a realizar la identificación.
  Por ejemplo, si en un **listado que incluya el nombre y apellidos** de los alumnos con medidas educativas especiales, la dirección de un centro **sustituye la identificación por códigos individuales** de uso único que guarda de forma separada y segura en un repositorio, estaría aplicando una técnica de seudonimización, porque evita que terceras personas puedan identificarlos, pero las personas autorizadas podrían en cualquier momento volver a asociar cada código a cada alumno para identificarlos.
- **Anonimización** es un proceso que disocia de forma permanente la identidad y el dato, de forma que no permita volver a singularizar o identificar al interesado, que se oculta con un proceso irreversible. Por ejemplo, si en un listado Excel de calificaciones de todos los alumnos de un centro suprimimos las columnas que contienen los datos de identificación del alumnado para elaborar una estadística, si no existiese ninguna información adicional (característica física, un dato de localización o un rasgo cultural o biológico) que permita identificar qué alumno ha obtenido cada nota hemos aplicado un proceso de anonimización.

browser-g3907eff37_640.png

Imagen de Jan en Pixabay

- **Publicación de parte de los datos**. La Agencia Española de Protección de Datos nos transmite posibles criterios prácticos, como el que mostramos a continuación, a la hora de publicar listados tablones de anuncios o en sus comunicaciones digitales ante la necesidad legal de tener que dar información pública de la divulgación del documento nacional de identidad, para ello, seleccionaremos aleatoriamente el grupo de cuatro cifras numéricas que se van a publicar para la identificación de los interesados en las publicaciones de actos administrativos. El procedimiento para la determinación de forma aleatoria de las cuatro cifras numéricas a publicar del código de identificación de un interesado se realiza mediante el proceso de selección aleatoria en una bolsa opaca de una bola de entre cinco **bolas numeradas del 1 al 5**, si a bola resultante es la **número 4**, la publicación de documento nacional de identidad será de la siguiente forma:
  Dado un DNI con formato **12345678X**, se publicarán los dígitos que en el formato que ocupen las posiciones cuarta, quinta, sexta y séptima. En el ejemplo:

***4567**

Medidas preventivas, herramientas y configuraciones para proteger la privacidad

Para preservar nuestra privacidad deberemos de tener una serie de precauciones, configuraciones y herramientas concretas que nos ayuden a preservar nuestros datos y por tanto nuestra privacidad, debemos de tener muy presente:

- Mantener los dispositivos que utilicemos **actualizados.**
- **Protección frente accesos no deseados**. La primera barrera de seguridad son los patrones de desbloqueo y las contraseñas que tienen que ser robustas (difíciles de romper), no predecibles y secretas.
- **Cifrado del contenido** del dispositivo.
- **Gestión de contraseñas.**
- **Detección de accesos y/o usos no controlados** del dispositivo.

> Para más información y conocer más herramientas que nos ayudan a tener mayor privacidad pulsa en el siguiente enlace

- **Configurar las opciones de privacidad** de RR.SS., navegadores, sistemas operativos, aplicaciones de mensajería instantánea, etc.

> Para más información sobre configuraciones pulsa en el siguiente enlace

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

Protección de datos personales y privacidad

Principales leyes que respaldan la protección de datos

- **CONSTITUCIÓN ESPAÑOLA** (ART. 18 CE).

En el Art. 18 de la Constitución Española se garantiza:

1. El derecho al honor, a la intimidad personal y familiar y a la propia imagen.
2. El secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

> Para más información pulsa en el siguiente enlace

- REGLAMENTO (UE) 216/679, DE 27-4-2016, 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, RGPD**)

> Para más información pulsa en el siguiente enlace

- **LEY ORGÁNICA** 3/2018, DE 5 DE DICIEMBRE, DE **PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES** (**LOPDGDD**)

1. Está en vigor desde el 07/12/2018.
2. Completa y aplica el RGPD e incorpora un Título X dedicado a la “Garantía de los derechos digitales”, que desarrolla aspectos como el derecho a la educación digital, la protección de los menores en Internet o un nuevo catálogo de derechos de la “Era digital”, como los relacionados con internet y redes sociales o en el ámbito laboral y funcionarial.

> Para más información pulsa en el siguienteenlace

- LEY ORGÁNICA 2/2006, DE 3 DE MAYO, DE EDUCACIÓN (**LOE**), RECIENTEMENTE MODIFICADA POR LA LEY ORGÁNICA 3/2020, DE 29 DE DICIEMBRE (**LOMLOE**)

Disposición adicional vigesimotercera. Datos personales de los alumnos:

1. Los centros docentes podrán recabar datos necesarios para el ejercicio de su función educativa, que podrán hacer referencia al origen y ambiente familiar y social, a características o condiciones personales, al desarrollo y resultados de su escolarización, así como a aquellas otras circunstancias cuyo conocimiento sea estrictamente necesaria para la función docente y orientadora. Los padres o tutores y los propios alumnos deberán colaborar en la obtención de la información.
2. La incorporación de un alumno a un centro docente supondrá el tratamiento de sus datos y, en su caso, la cesión de datos procedentes del centro en el que hubiera estado escolarizado con anterioridad.
3. En el tratamiento de los datos del alumnado se aplicarán normas técnicas y organizativas que garanticen su seguridad y confidencialidad.
4. El profesorado y el resto del personal que acceda a datos personales y familiares o que afecten al honor e intimidad de los menores o sus familias quedará sujeto al deber de sigilo.

Artículo 111 bis. Tecnologías de la información y la comunicación. Esta disposición regula aspectos tan relevantes como:

- Los estándares que garanticen la interoperabilidad entre los distintos sistemas de información del Sistema Educativo Español y los distintos niveles de compatibilidad y seguridad en el tratamiento de los datos.
- El número identificativo para cada alumno o alumna, a fin de facilitar el intercambio de la información relevante con respeto de la privacidad y protección de datos personales.
- Los entornos virtuales de aprendizaje que se empleen en los centros docentes sostenidos con fondos públicos que deben permitir el acceso del alumnado, desde cualquier sitio y en cualquier momento, con respeto de la normativa de propiedad intelectual, privacidad y protección de datos personales y de los principios de accesibilidad universal y diseño para todas las personas y procurando su compatibilidad e interoperabilidad. Así mismo, se regulan las características de las plataformas digitales y tecnológicas ofrecidas por el Ministerio de Educación y Formación Profesional a toda la comunidad educativa.
- La obligación de las Administraciones educativas y de los equipos directivos de los centros de promover el uso de las tecnologías de la información y la comunicación (TIC) en el aula. También se obliga a establecer las condiciones que hagan posible la eliminación en el ámbito escolar de las situaciones de riesgo por la inadecuada utilización de las TIC, con

especial atención a las situaciones de violencia en la red.
- La obligación estatal de fijar los marcos de referencia de la competencia digital en la formación inicial y permanente del profesorado para el desarrollo de una cultura digital en los centros y en las aulas.
- La obligación de las Administraciones públicas de velar por el acceso de todos los estudiantes a los recursos digitales necesarios (para disminuir la denominada brecha digital).

Para más información pulsa en el siguiente enlace

Una ejemplo de plantilla de centro donde iremos anotando las legislación vigente en protección de datos puede ser esta:image.png

Protección de datos personales y privacidad

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.

image.png

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.

image.png

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.

6.png

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

Captura de pantalla_20221112_125027.png

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.

Captura de pantalla_20221112_125113.png

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.

Captura de pantalla_20221112_125149.png

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».

image.png

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.

Captura de pantalla_20221112_124956.pngFuente 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

image.png

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.

image.png

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.image.png

image.png

image.png

image.png

image.png

image.png

image.png

Protección de datos personales y privacidad

Principios en materia de protección de datos

Los principios en materia de protección de datos pretenden asegurar que se está actuando de forma adecuada para no verse comprometida la privacidad, en total son 9 los principios que los detallamos a continuación:

1. **Licitud** : el tratamiento solo es posible si concurren las condiciones previstas en los artículos 6.1 RGPD (condiciones de licitud) y siempre que se den las circunstancias del 9.2 RGPD, para el caso de las categorías especiales de datos.

2. **Lealtad** : debe haber coincidencia entre la información facilitada al interesado sobre el tratamiento y el tratamiento efectivamente realizado en cada momento.

3. **Transparencia** : debe cumplirse con los deberes de información de los artículos 12 al 14 del RGPD, en los que se prevé concretamente la información mínima que debe facilitarse a los interesados en todo tratamiento, y garantizar que toda información y comunicación relativa al tratamiento sea fácilmente accesible y fácil de entender y que se utiliza un lenguaje sencillo y claro. Así mismo, debe permitirse el acceso a la información , en los términos previstos en el RGPD.

4446588.jpg

Imagen de pikisuperstar en Freepik

4. **Limitación de la finalidad**: la recogida de datos se hará para fines determinados, explícitos y legítimos y el tratamiento posterior debe ser compatible con dichos fines, con la excepción prevista para el archivo, investigación y estadística (y para estas finalidades el art. 89 exige garantías adecuadas, entre ellas la minimización y seudonimización, cuando sea posible).
En todo caso, se debe garantizar la información del interesado sobre esos otros fines posteriores y sobre sus derechos, incluido el derecho de oposición.

imagen.png

Fuente propia

5. **Minimización de datos**: solo pueden tratarse los datos adecuados, pertinentes y necesarios para los fines del tratamiento.

Este principio está relacionado la protección de datos por defecto que también debe garantizar el responsable; con el principio de limitación de la finalidad, ya que solo es pertinente el tratamiento que se limita a la finalidad informada, así como con los principios de necesidad y proporcionalidad, en virtud de los cuales en los tratamientos siempre deberá buscarse la mínima incidencia posible en el derecho de protección de datos de forma que solo es adecuado el tratamiento que es proporcionado a la finalidad perseguida y siempre que esta finalidad no pudiera lograrse razonablemente por otros medios.

6. **Exactitud y calidad de los datos**: Los datos deben ser exactos y actualizados y ello exige adoptar todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos.
De acuerdo con la LOPDGDD, la inexactitud no es imputable al responsable del tratamiento cuando este haya adoptado todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que procedan, si los datos inexactos hubiesen sido obtenidos por el responsable:

- Directamente del afectado.
- De un mediador o intermediario en caso de que las normas aplicables al sector de actividad establecieran su posibilidad de intervención.
- De otro responsable en virtud del ejercicio por el afectado del derecho a la portabilidad.
- De un registro público.

7. **Limitación del plazo de conservación**: los datos deben mantenerse solo durante el tiempo necesario para los fines del tratamiento, salvo fines de archivo en interés público, investigación científica o histórica o estadísticos. Para ello es importante fijar plazos para la supresión y revisión periódica del tratamiento. Este principio también está relacionado con otros, como el de minimización, limitación de la finalidad y protección de datos por defecto.
En la conservación de datos en las Administraciones Públicas debe tenerse en cuenta la normativa sobre archivos y gestión de
documentos, aunque con frecuencia existe una gran indefinición en los plazos de conservación y una tendencia a conservar la información durante períodos superiores a los realmente necesarios. Por otra parte, las políticas de conservación o archivo deben tener en cuenta medidas de seguridad adecuadas, al igual que la supresión debe realizarse con seguridad.3255337.jpg

Imagen de storyset en Freepik

8. **Integridad y confidencialidad**: debe garantizarse una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

El RGPD se refiere a la seguridad del tratamiento de datos que debe garantizarse por el responsable y, en su caso, el encargado, mediante la adopción de medidas técnicas y organizativas proporcionadas, por ejemplo:

- La seudonimización y el cifrado de datos personales
- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios del tratamiento
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico
- Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Con respecto al deber de confidencialidad, la LOPDGDD establece este deber no solo para los responsables y encargados del tratamiento, sino para todas las personas que intervengan en cualquier fase de un tratamiento, manteniéndose aun después de finalizar la relación con el responsable o encargado. Además, esta obligación se establece con carácter complementario a los deberes de secreto profesional.

9. **Responsabilidad proactiva** : El responsable no solo debe cumplir los principios mencionados y otras obligaciones establecidas en el RGPD, sino que debe ser capaz de demostrarlo.
Este principio implica una inversión de la carga de la prueba que alcanza incluso a los procedimientos de infracción en materia de
protección de datos, en los que la "presunción de inocencia" es aplicable a quien demuestra que ha cumplido con sus obligaciones.
En la práctica, este principio se traduce en dos obligaciones atribuibles a los responsables:

- Una actitud preventiva y activa en el cumplimiento de sus deberes, que exige adoptar las medidas necesarias para garantizarlo.
- La necesidad de documentar las actuaciones realizadas en el cumplimiento de sus deberes.

imagen.png

Fuente propia

Protección de datos personales y privacidad

El consentimiento como condición de licitud

Captura de pantalla_20221114_210035.png

Fuente AEPD

Los tratamientos de **datos personales** realizados con una **finalidad estrictamente docente** u orientadora del alumnado (la mayoría de los tratamientos realizados por los centros educativos tienen esta finalidad), están directamente amparados o exigidos por la LOE y, por lo tanto, **no debe recabarse el consentimiento**, sino que este tratamiento viene impuesto **por el cumplimiento de obligaciones legales o de intereses públicos**, sin perjuicio de la obligación del responsable de informar adecuadamente a los interesados. Para el resto de supuestos diferentes a la finalidad docente y orientadora del alumno, la legislación anterior al RGPD partía del principio general de que el tratamiento de los datos de carácter personal, salvo excepciones, requería el consentimiento inequívoco del afectado.

Captura de pantalla_20221114_205449.png

Fuente AEPD

A partir del RGPD, el consentimiento es una más de las condiciones de licitud de los tratamientos, el artículo 6.1 del RGPD, según el cual, el tratamiento de datos debe basarse en alguna de las siguientes condiciones, que denominamos condiciones de licitud o bases de legitimación de los tratamientos de datos:

Art. 6.1.a) RGPD: el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos.

Captura de pantalla_20221114_205459.png

Fuente AEPD

De acuerdo con el RGPD, el consentimiento debe tener las siguientes características:

- **Manifestación de voluntad**: auténtica expresión de la voluntad del interesado.
- **Libre**: libre elección, sin sufrir perjuicio alguno, en el ámbito educativo, debe garantizarse que el interesado puede rechazar el tratamiento sin sufrir ningún perjuicio, ni quien consiente el tratamiento debe obtener un premio.
- **Específica**: No son válidos los consentimientos excesivamente genéricos. Por ejemplo, la AEPD ha admitido que se solicite el consentimiento para la captación o difusión de imágenes de actividades escolares al principio de curso, dado que la finalidad del tratamiento y sus características en estos casos suele ser la promoción de las actividades del centro, pero no son válidas las peticiones de consentimiento genéricas y no especificadas en el propio tratamiento.

Captura de pantalla_20221114_205518.png

Fuente AEPD

- **Informada**: Se debe facilitar a los interesados la información, se debe informar de la existencia del derecho a retirar el consentimiento en cualquier momento, esta información deberá facilitarse en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos.

Captura de pantalla_20221114_205508.png

Captura de pantalla_20221114_210013.png

Fuente AEPD

- **Demostrable**: El responsable debe ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales, debe conservar la prueba de dicha manifestación (documento con la declaración escrita, grabación con la declaración verbal, etc.)

Captura de pantalla_20221114_205924.png

Fuente AEPD

- **Consentimiento de los menores de edad**: La LOPDGDD establece la edad mínima para prestar el consentimiento en 14 años y requiere el consentimiento del titular de la patria potestad o tutela. Por ejemplo, es preciso el consentimiento para la difusión de los datos personales de los participantes en una actividad voluntaria, realizada con fines de promoción de un centro escolar.

Captura de pantalla_20221114_205403.png

Fuente AEPD

A continuación podéis pulsar en el siguiente enlace para ver un ejemplo para el alumnado entre 14-18 que son capaces de consentir por sí mismos.

image.png

Fuente AEPD

> Toda la información esta sintetizada en la siguiente infografía de la AEPD

Seguridad Digital

Seguridad Digital

Documentación y datos digitales

En el **centro educativo** podemos tener múltiples aspectos que se pueden convertir en amenazas a la hora de tener **brechas de seguridad** que afectan de forma sensible al correcto funcionamiento del centro, nos pueden llegar desde los propios miembros que conformamos la comunidad educativa, programas maliciosos, errores en la programación y posibles accidentes que pueden acontecer.

image.png

Imagen de Pedro González experto en Ciberseguridad

Si la amenaza se convierte en un ataque, la forma inmediata de detenerlo sería:

- **Desconexión del dispositivo de la red**
- **¿Apagarlo?**
- **Desconexión del router y switches del centro**
- **Llamar a soporte**

Por lo tanto en los centros educativos velaremos porque la información y los datos estén custodiados de forma segura y aplicaremos **medidas activas y pasivas** en lo concerniente a la **seguridad:**

image.png

Imagen de Pedro González, experto en Ciberseguridad

Papeles y datos digitales

- La información digital ocupa menos espacio, pero depende de la vida útil del soporte donde esté almacenada. Los papeles suelen durar más tiempo y, en muchos casos, es necesario conservar los **originales**, sobre todo en documentación que legalmente debemos conservar durante un tiempo determinado, o **documentos firmados**. Para ambos tipos de soporte, lo fundamental es que los almacenemos de forma segura y ordenada, y que las condiciones sean las adecuadas para que no se deterioren.

documentos-organizacion-adultos-jovenes.jpg

Imagen de Freepik

- El **centro educativo fijará qué dispositivos pueden utilizarse y controlarlos**. Por ello antes de usar ningún dispositivo personal como pendrives o discos externos o nuestros servicios en la nube personales (Dropbox, Google Drive, etc.), tendremos que preguntar al responsable, siendo recomendable el uso de los **servicios en la nube del centro**. Su uso indiscriminado puede dar lugar a riesgos importantes y a fugas de información.

image.png

Fuente Incibe

- Debemos asegurarnos que los soportes dónde guardamos la información se encuentran en buen estado y así no arriesgarnos a perder dicha información. Cuando seleccionamos un dispositivo de almacenamiento tenemos que conocer su vida útil para sustituirlo a tiempo y no perder la información que contiene.
- Las **condiciones del entorno** de los soportes donde guardamos la información resultan tan importantes como la seguridad de la información misma. Debemos procurar que se den las condiciones físicas (humedad, temperatura, etc.) adecuadas para que el soporte no se deteriore. También es importante que no esté al alcance de cualquiera y si es extraíble de no perderlo.

26769.jpg

Imagen de rawpixel.com en Freepik

- Aunque reciclar está muy bien, no debemos tirar la información así sin más ya que alguien podría recuperarla. Debemos asegurarnos que la información se destruya antes de deshacernos de ella y que sea imposible su reconstrucción. En la siguiente guía mostramos las pautas para un borrado seguro. Guía sobre el borrado seguro de la información
- **Política de copias de seguridad (Backups)**. Tendremos presente la regla 3-2-1: Siempre se deben realizar y **mantener tres copias** de seguridad de los datos a respaldar. Se utilizarán al menos **dos soportes distintos** para realizar estas copias y **uno de ellos tiene que estar siempre fuera del centro educativo** (en el entorno actual de trabajo, en la **nube**).

image.png

Imagen de Apen

A continuación presentamos un modelo de plantilla, donde podremos ir rellenando las medidas en materia de seguridad adoptadas en el centro.image.png

Financiado por el Ministerio de Educación y Formación Profesional y por la Unión Europea - NextGenerationEU

logo.png

Seguridad Digital

Dispositivos

Muchas pueden ser las actuaciones que en materia de seguridad se pueden aplicar en nuestros dispositivos digitales, a continuación se enumeran los más imprescindibles.

1.-Proteger el acceso a los dispositivos con contraseñas robustas

Para crear una **CONTRASEÑA** robusta tendremos en cuenta:

- Que tenga como **mínimo 12 caracteres**. Por ejemplo: cuentasegura
- Alternar **mayúsculas** y **minúsculas**. Ej: CuentaSegura
- Sustituir **letras por números** (a=1, e=2). : Ej: Cu2nt1s2gur1
- Añadir **caracteres especiales**. Ej: Cu2nt1s2gur1!
- **Personalizar** la contraseña para **cada servicio,** una para el inicio de sesión de un dispositivo y otra para el el correo electrónico, poniendo las iniciales en mayúsculas al principio y al final. Ej del correo electrónico: CCu2nt1s2gur1!E

log-in-g564c0a061_640.jpg

Imagen de Gerd Altmann en Pixabay

Y como medidas extra:

- **No las compartas** con nadie (ni amigos, ni familiares)
- Configurarlo de tal forma **que no se vean tus carácteres cuando los escribas**
- **Cámbialas cada cierto tiempo** (3 meses)
- **No repitas contraseñas en diferentes servicios** (@ corporativo, @ personal, RRSS,...)
- Si es posible configura la **verificación en dos pasos**
- Utiliza **gestores de contraseñas** para controlar todas tus claves. Si quieres conocer diferentes gestores de contraseñas gratuitos pulsa aquí.

> A continuación os proponemos dos propuestas para generar contraseñas de forma lúdica: "Mejora tus contraseñas". Construye contraseñas seguras jugando desarrollado por el Incibe y "Space Shelter": un juego para aprender a incrementar tu seguridad en Internet desarrollado por Google

2.- Importancia de las actualizaciones

Una actualización es un añadido o modificación realizada sobre los sistemas operativos o aplicaciones que tenemos instaladas en nuestros dispositivos, cuya misión es mejorar tanto aspectos de funcionalidad como de seguridad. Así, se corregirán las vulnerabilidades descubiertas y se contará con las últimas funciones implementadas por los desarrolladores.

Por tanto, si queremos mantener la seguridad de nuestros dispositivos, debemos:

- Vigilar el estado de actualización de todos nuestros dispositivos y aplicaciones.
- Elegir la opción de **actualizaciones automáticas** siempre que esté disponible.
- Instalar las actualizaciones **tan pronto como se publiquen**, especialmente las de los sistemas operativos, navegadores y programas antivirus.
- Ser **cuidadosos con las aplicaciones que instalamos**, huyendo de fuentes no confiables y vigilando los privilegios que les concedemos.
- Evitar usar aplicaciones y sistemas antiguos que ya no dispongan de actualizaciones de seguridad.
- Es recomendable no congelar los dispositivos ya que no es posible que se efectuen las actualizaciones de seguridad tando de los sistemas operativos como de las aplicaciones.

image.png

Fuente Incibe

Es importante no confundir tener una aplicación actualizada con tener la última versión. Podemos tener instalado y actualizado Windows 10, a pesar de no tratarse de la última versión de este sistema operativo. Los fabricantes no solo comercializan nuevas versiones que incorporan mejoras, sino que mantienen un largo periodo de tiempo las antiguas versiones a través de actualizaciones.

> En los siguientes enlaces encontrarás una recopilación de los sistemas, navegadores y programas más conocidos, que nos facilitarán la **actualización** de nuestros dispositivos:
>
> Cómo actualizar el **sistema operativo**, cómo actualizar los **navegadores**, cómo actualizar los **programas y aplicaciones**

Debemos huir de sitios “pirata”, especialmente de aquellos que ofrecen aplicaciones o servicios gratuitos o extremadamente baratos, por lo tanto instalemos **aplicaciones solo de fuentes de confianza y revisemos siempre los privilegios**, por si fuesen excesivos o innecesarios para el propósito al que están destinados.

3.- Cifrado de datos vulnerables.

El cifrado implica convertir texto con formato legible por humanos en un texto incomprensible, conocido como texto cifrado. En esencia, esto significa tomar datos legibles y cambiarlos para que se vean como algo aleatorio.

El cifrado implica utilizar una clave criptográfica. Podemos distinguir entre datos en transito y en reposo.

- **Cifrado de datos en tránsito** es cuando se mueven entre dispositivos, como es el caso entre redes privadas o por Interne, durante la trasferencia, los datos (cuando enviamos un Whatsapp, compra on-line,...) se encuentran en mayor riesgo debido a la necesidad de descifrar antes de transferir y a las vulnerabilidades del propio método de transferencia. Cifrar los datos durante la transferencia, conocido como cifrado integral, garantiza la protección de la privacidad de los datos, incluso si los interceptan.
- **Cifrado de datos en reposo** es cuando permanecen en un dispositivo de almacenamiento y no se usan o transfieren activamente. A menudo, los datos en reposo son menos vulnerables que los en tránsito debido a que las funciones de seguridad del dispositivo restringen el acceso. Cifrar los datos en reposo reduce las oportunidades para el robo de datos que propician los dispositivos perdidos o robados, o bien por compartir contraseñas u otorgar permisos por accidente

sl_031420_28950_06.jpg

Image by vectorjuice on Freepik

> Si quieres herramientas para el cifrado de datos pulsa en el siguiente enlace

4.- Antivirus activado y actualizado

Es fundamental tener el antivirus activado y actualizado para proteger los dispositivos de las distintas amenazas que circulan por Internet. Recordemos que un antivirus es un programa informático específicamente diseñado para detectar, bloquear y eliminar código malicioso (virus, troyanos, gusanos, etc.), pero para poder hacer su misión **debe estar activado**. Obviamente, no sirve de nada tener instalado en el equipo un antivirus si luego no está activo.

20945430.jpgImage by vectorjuice on Freepik

Pero aún hay más, también es necesario que el **antivirus esté actualizado**. La explicación a esto es muy sencilla. Cuando instalamos un antivirus en el dispositivo, éste es capaz de detectar los

virus existentes hasta ese momento. Es importante saber que los fabricantes de antivirus, a través del servicio de actualizaciones, lo que hacen es añadir a su base de datos, todos los nuevos virus que se descubren. Por tanto, si el usuario no actualiza la herramienta, los últimos virus podrán "colarse" en los dispositivos.

> Si quieres poder elegir entre diferentes antivirus y cleaners gratuitos puedes pulsar en el siguiente enlace

5. Configura el bloqueo automático del equipo cuando estás ausente o entra en reposo.

Cuando te levantes para descansar o no vayas a utilizar el ordenador en un rato, es importante bloquearlo, para que otras personas no tengan acceso a él. Los siguientes casos, son ejemplos de cuándo se bloquea el equipo:

- Dejar de teclear y usar el ratón por un tiempo definido según los ajustes.
- Tener un ordenador portátil y cerrar la tapa.
- Se bloquea manualmente.

Por ejemplo en los sistema Windows podemos hacerlo de diferentes formas:

- Desde el menú '**Inicio**', haz clic encima de tu nombre de usuario y luego en '**Bloquear**'.
- Usando el atajo de teclado **Windows + L** desde cualquier pantalla.
- Para portátiles, configura la suspensión cuando se cierra la tapa. Abre el menú '**Inicio**' y escribe '**Panel de control**'. Ábrelo y ve a '**Hardware y sonido**' > '**Opciones de energía**', y en esta ventana haz clic en '**Elegir el comportamiento del cierre de la tapa**' en la izquierda de la pantalla. Ahora configura las dos opciones marcadas en la imagen en '**Suspender**'.

image.png

Fuente Incibe

6.- Incorpora mecanismos seguros de desbloqueo

Hoy en día, tanto los teléfonos móviles, tablets como los ordenadores disponen de algún mecanismo para evitar que cualquier usuario pueda hacer uso de nuestro dispositivo, una de las primeras configuraciones de seguridad que realizamos cuando encendemos nuestro equipo es el **bloqueo de acceso**, ya sea mediante un PIN, un patrón o una clave de seguridad.

En los **ordenadores** existen varias opciones, aunque su disponibilidad dependerá del tipo de ordenador y de si tenemos permisos de administrador, las más comunes (en Windows) son:

- **Rostro de Windows Hello**: podremos utilizar nuestro rostro para bloquear/desbloquear nuestro equipo.
- **Huella digital de Windows** Hello: en este caso, utilizaremos nuestra huella dactilar.
- **PIN de Windows Hello**: podremos escoger un código PIN (clave numérica de al menos 4 caracteres), aunque es la opción menos segura.
- **Clave de seguridad**: se trata de una clave física, que se instala dentro de un dispositivo, como una memoria USB, y que necesitamos conectar al equipo para iniciar sesión.
- **Contraseña**: podremos cambiar la contraseña que creamos junto con la cuenta de usuario, es decir, la que utilizamos para desbloquear el ordenador.

image.png

Fuente propia

Por otro lado los dispositivos móviles (***smartphones o tablets***) cuentan también con una herramienta muy importante que es el sistema de bloqueo, una gran variedad de dispositivos utilizan el sistema de Android y la configuración del bloqueo de pantalla es el siguiente:

- **Patrón**: consiste en un dibujo trazado uniendo una serie de nueve puntos en forma de un cuadrado de 3x3. Es la opción menos segura, ya que cualquiera puede ver el trazo en la pantalla.
- **PIN**: se trata de una clave de al menos 4 dígitos. Te recomendamos no utilizar el mismo PIN de la tarjeta SIM o la del banco.
- **Contraseña**: se trata de una clave de al menos 4 dígitos y letras. Debemos utilizar una contraseña difícil de averiguar y única para el dispositivo.
- Desbloqueo con **huella dactilar**: nuestro dispositivo dispone de un lector de huella dactilar. Puede utilizarse para que una o varias huellas dactilares desbloqueen nuestro móvil o tablet simplemente poniendo el dedo sobre el lector de la huella.
- Desbloqueo **facial**: nuestro dispositivo es capaz de reconocer rostros mediante la cámara frontal. Podemos añadir nuestro rostro o el de otros usuarios como mecanismo de desbloqueo.
- Desbloquear con dispositivo **Bluetooth**: podremos utilizar otro dispositivo inteligente para desbloquear nuestro móvil o tablet, como una pulsera de actividad o reloj inteligente.

7. Instalar únicamente las aplicaciones necesarias, revisando privacidad y permisos

Tener muy claras las aplicaciones que vamos a utilizar y con que fines configurando convenientemente la privacidad y permisos que les damos a las mismas. Es conveniente actualizarlas desde los sitios oficiales y si ya no las utilizamos sería conveniente eliminarlas, pues pueden llegar a ser puertas de entrada de potenciales riesgos de nuestros dispositivos.

educational-gadf4e03eb_640.jpg

Imagen de edsys en Pixabay

Los **centros educativos tienen que analizar y consensuar las relación de aplicaciones** más adecuadas en el proceso de enseñanza y aprendizaje del alumnado en función del nivel educativo en el que se encuentren.

> Un posible modelo de plantilla, donde ir rellenando las medidas en materia de seguridad adoptadas en los dispositivos podría comenzar así.image.png

Seguridad Digital

Infraestructura de red y conectividad

Recomendaciones de seguridad en torno a conectividades y redes:

- Definir **distintas redes en el centro** en función de la sensibilidad de los datos con los que se trabaje y proteger cada una de ellas de de accesos no autorizados, lo mismo si se dispone de conexión wifi**.** Para ello es recomendable crear una **subred** para dirección / administración, otra para profesorado, y otra para alumnado.
- Las tomas que dan **acceso a la red por medio de cable Ethernet también se deberán proteger**, evitando que estas se encuentren en lugares públicos o con poco control.

5865576.jpg

Imagen de storyset en Freepik

- Definir pautas de uso y política de usuario/contraseña de la **red WIFI** del centro, por parte de todos los miembros de la comunidad educativa.

wifi-g5f862b6ec_640.png

Pixabay License

- **Controlar el DHCP.** El Protocolo de Configuración Dinámica de Host (DHCP) que es un protocolo de Internet que los equipos en red utilizan para obtener direcciones IP y otra información como la puerta de enlace predeterminada. Cuando el usuario se conecta a Internet, un equipo configurado como un servidor DHPC en el ISP le **asigna automáticamente una dirección IP**. Podría ser la misma dirección IP que tenía anteriormente o podría ser una nueva. Cuando se cierra una conexión a Internet que usa una dirección IP dinámica, el ISP puede asignar esa dirección IP a un usuario diferente. Por todos ello y con el fin de evitar vulnerabilidades, el centro educativo debe decidir sopesando la seguridad y las necesidades del centro, el tener habilitada / limitada la franja de IPs / deshabilitada, está configuración dinámica.

5118825.jpg

Imagen de storyset en Freepik

- Configuración del **Router** con criterios de seguridad (sino lo está, pueden espiar nuestras comunicaciones, utilizar la red para envío de spam, infectar los dispositivos conectados, reducir el ancho de banda,...), en los centros educativos sostenidos con fondos públicos, está **configuración viene por defecto definida por la administración educativa** y es la que realiza el soporte de los mismos, pero deberíamos de saber que aspectos de seguridad es conveniente conocer y si alguno podríamos personalizarlo para nuestro centro con la ayuda del servicio técnico que dispone la administración, por lo tanto tendremos en cuenta:
  - Asignar el mejor **protocolo de seguridad** posible en las conexiones Wifi, en estos momentos en los entornos educativos la mas segura y estable es el **WPA2**, pero ya se está hablando de la WPA3 aunque necesita ir adaptándose a la realidad educativa
  - **Cambiar u ocultar el nombre de la red o SSID**: Cuando modificamos las credenciales de acceso a nuestro router o a nuestra red wifi, estamos protegiéndolos de terceros evitando que puedan acceder a ellos. Para aumentar aún más la protección de nuestra red, es recomendable que cambiemos el nombre de nuestra red wifi (SSID)
  - **Filtrar las direcciones MAC**: Una práctica muy útil para mejorar la seguridad de nuestra conexión y protegerla de terceros es revisar eventualmente los dispositivos que están conectados a nuestra red y realizar un filtrado por dirección MAC, que es un identificador único que posee cada dispositivo. De esta forma, habilitaremos el acceso solo a aquellos dispositivos que conocemos y evitaremos que se conecten dispositivos desconocidos
  - **Desactivar el acceso remoto.** Si queremos evitar que se pueda entrar a nuestro router desde el exterior, es decir, desde otra red, tendremos que asegurarnos de que esta funcionalidad está desactivada

Wavy-C_Tech-05_Single-09.jpg

Imagen de vectorjuice en Freepik

  - **Desactivar el WPS o conexión rápida**: Los router y sus configuraciones de seguridad han evolucionado mucho a lo largo de los años. La funcionalidad WPS, por ejemplo, es una funcionalidad que, si bien resultaba muy útil a la hora de conectar dispositivos a la red, a día de hoy puede suponer una gran amenaza contra nuestra seguridad y privacidad. El WPS es un mecanismo creado para facilitar la conexión de dispositivos a nuestra red wifi. Aunque existen diversas formas mediante las cuales un dispositivo puede conectarse a una red inalámbrica utilizando, para ello, dicha funcionalidad, la más extendida de todas sigue siendo mediante una clave PIN.
  - **Puertos del router**. Los puertos del router se utilizan como un canal para establecer conexiones de diferentes aplicaciones con los correspondientes

servidores remotos para poder funcionar. Nuestro router es el encargado de transmitir la información que entra o sale de los dispositivos conectados a la red y la encamina, a través de router intermedios hasta su destino.

- **Crear una red para invitados**. Una red de invitados tiene como objetivo el permitir que varios dispositivos se conecten a nuestra conexión a Internet, pero permitiéndoles navegar en una red distinta a la de nuestros dispositivos habituales. De este modo, podrán acceder a nuestra conexión a Internet sin comprometer la seguridad de nuestra red principal y, sin que perdamos el control de los accesos.

A modo de resumen os dejamos un pequeño vídeo donde la OSI nos indican como proteger nuestra red

https://www.youtube.com/embed/POeuXk1UXHo

> Una posible plantilla donde ir escribiendo lo relacionado con infraestructura de red y conectividad comenzaría así.image.png

Seguridad Digital

Videovigilancia en los centros educativos

En los centros educativos con la intención de mejorar el nivel de convivencia, vandalismo y seguridad es lícito el instalar cámaras de vigilancia con unas condiciones muy concretas y con una serie de condicionantes:

- Antes de proceder a su instalación, el centro debe planificarla respetando la **privacidad y el derecho a la imagen de quienes resulten grabados** según la normativa vigente
- En centro educativo puede instalar las cámaras y no es necesario el consentimiento del alumnado o de sus representantes legales
- Debe de **informarse de la existencia de las cámaras**, por medio de carteles informativos, en lugar bien visible, en los accesos de la zona donde serán captadas las imágenes. Los carteles mostrarán la dirección del responsable del tratamiento, los interesados (estudiantes, profesores, familias y terceras personas) pueden ejercer sus derechos de acceso, supresión y/o limitación de tales imágenes.

cctv-security-camera-on-the-ceiling.jpg

Imagen de rawpixel.com en Freepik

- Únicamente tendrán **acceso** a las imágenes captadas las personas que designen los **responsables del centro educativo**
- Las imágenes almacenadas no pueden guardarse indefinidamente y se conservarán durante **30 días**, a menos que capten hechos presuntamente delictivos, en cuyo caso el centro dispone de 72 horas (desde la existencia de la grabación) para comunicar tales imágenes a las autoridades competentes (Fuerzas y Cuerpos de Seguridad del Estado; de las CCAA; Fiscalía de menores / autoridad judicial)
- **En ningún caso** se instalarán cámaras en espacios reservados: **baños, vestuarios, sala de descanso de docentes, etc**.
- La instalación de **cámaras en las aulas no es justificable** con fines de videovigilancia, ya que el control del alumnado está garantizado por los docentes que imparten las sesiones.

Una posible plantilla donde reflejar lo acordado respecto a la videovigilancia sería esta.
image.png

Seguridad Digital

Ciberseguridad para el alumnado

Muchas pueden ser las **actuaciones** que se pueden hacer para **concienciar al alumnado** para interiorizar la seguridad digital en las actuaciones de su día a día con los diferentes dispositivos. Nosotros como docentes podemos ayudar, formar y asesorar con una planificación de posibles actuaciones que vayan encaminadas a la prevención.

El adoptar hábitos en el día a día que estén en la dirección de un **buen uso y responsabilidad** con la tecnología ya hace que tengamos ese primera barrera de seguridad

> Más información en uso adecuado y responsabilidad del alumnado en el siguiente enlace

A continuación vamos a comentar algunas actuaciones para mejorar la ciberseguridad en el alumnado:

Jornadas formativas sobre ciberseguridad

Los centros educativos suelen concertar formaciones de prevención en muchas áreas, respecto a la seguridad, podemos contar con la participación de entidades que colaboran en la misión de divulgar y educar en las tecnologías digitales.

- Programa de Jornadas Escolares de IS4K

Las ‘Jornadas Escolares’ son de carácter **gratuito** y tienen por objetivo mejorar las competencias digitales en profesorado y alumnado de **Educación Primaria y Secundaria** para hacer un **uso seguro y responsable de Internet**.

image.png

> Más información en el siguiente enlace

- Plan director para la convivencia y mejora de la seguridad

El Plan director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos donde los cuerpos y fuerzas de seguridad del estado (Guardia Civil y Policía Nacional viene)n a los centros y nos ayudan en temas vinculados a internet, ciberacoso, redes sociales... y las responsabilidades civiles e incluso penales que tienen las actuaciones delictivas.

image.png

image.png

Además nos animan a descargarnos la aplicación Alertcops, con la que **cualquier persona**, con independencia de su idioma, origen o de sus discapacidades auditivas o vocales **pueda comunicar** a las Fuerzas y Cuerpos de Seguridad del Estado (**Policía y Guardia Civil) una alerta, información, dato o noticia sobre un acto delictivo** o incidencia de seguridad del que está siendo víctima o testigo.

image.png

> Más información en el siguiente enlace

- Realización de Talleres online

Como el de "**Día de intenet seguro**" realizado por el INCIBE, con actividades para fomentar, entre niños, jóvenes y sus entornos más cercanos, un uso seguro y positivo de las tecnologías digitales, promocionando sus competencias en esta materia y ayudándoles a ser respetuosos, críticos y creativos, en línea con los principios digitales europeos

image.png

> Más información de estos talleres en el siguiente enlace

Juegos que nos conciencian en seguridad digital

Muchos son los juegos que tenemos en internet que buscan aprender más sobre seguridad a modo de ejemplo hemos seleccionado

- Juego de Cyberscouts

Es un juego desarrollado por el INCIBE donde el alumnado aprende a proteger su identidad digital, a reconocer una buena contraseña, a identificar riesgos en internet, además de trabajarlo en clase puede hacerse posteriormente en familia consiguiendo adquirir conocimientos para hacer un uso más seguro de los servicios de Internet.

image.png

> Más información en el enlace

- Juego de Hackers vs Cybercrook

Juego desarrollado por INCIBE donde a través de las diferentes misiones, tendremos la oportunidad de aprender sobre la importancia de generar contraseñas seguras, la necesidad de realizar copias de seguridad, las precauciones al conectarte a redes wifi públicas y ¡muchas cosas más! Todo ello aderezado con la diversión de aprender jugando.

image.png

> Más información en el siguiente enlace

Instalación de la APP CONAN mobile

Finalmente vamos a presentar una **herramienta gratuita** avalada por el instituto nacional de ciberseguridad, de comprobación integral de la seguridad de nuestros **smartphones y tabletas**, que muestra soluciones a posibles riesgos a los que estamos expuestos y proporcionándonos algunos consejos que nos ayudarán a mejorar la seguridad de nuestros dispositivos.

Analizando vulnerabilidades a nivel de **configuración**: propiedades de configuración, redes Wifi inseguras, dispositivos bluetooth inseguros; a nivel de **aplicaciones**: maliciosas o sospechosas; a nivel de **permisos**: alto, medio, bajo, otros.

Además tiene un **servicio proactivo** de eventos relevantes que se están registrando en nuestro dispositivo (si estoy con mensajes de tarificación especial -servicios premium-, si mis aplicaciones tienen conexiones potencialmente peligrosas, información de la IP/dominio/localización geográfica)

https://www.youtube.com/embed/BOhfRa91HRg

> Plantilla de posibles actuaciones con el alumnado en materia de ciberseguridad.image.png

Seguridad Digital

La seguridad digital en el entorno familiar

Las familias tenemos la responsabilidad de conocer las situaciones de riesgo a la que están sometidas nuestros hijos cuando navegan por la red, para **ayudarles a disfrutar con seguridad**, como parte de nuestra labor de mediación parental. Por eso, es necesario saber el origen de estos riesgos y las medidas de protección a nuestro alcance.

image.png

¿Cómo reaccionaremos las familias desde casa ante los problemas de la Red?

1. ***Mantener la calma.*** Es normal sentir temor ante las posibles consecuencias de los problemas online, pero debemos ser conscientes de que en esos momentos los y las menores necesitan de nuestro apoyo, seguridad y confianza, evitando empeorar la situación, culpabilizándoles o sobrerreaccionando.
2. ***Guardar evidencias.*** Es recomendable no eliminar impulsivamente las pruebas del conflicto o problema, como imágenes, mensajes, perfiles de redes sociales o páginas web, sin consultar con un servicio especializado. De hecho, puede ser de utilidad tomar capturas de pantalla para ayudar a resolver el caso o esclarecer lo ocurrido, si posteriormente fueran borradas.
3. ***Buscar información y contactar con un profesional.*** Existen muchos servicios de ayuda en los que nos podemos apoyar para saber cómo actuar, ya que cada situación es distinta. Todas las redes sociales, juegos y la mayoría de las páginas web poseen centros de ayuda y seguridad y soporte técnico, que nos permiten contactar con los administradores, reportar un problema o solventar un conflicto.

• Conocer recursos online donde informarse las familias

En caso de necesitar conocer las últimas novedades sobre seguridad, las familias deben de conocer páginas fiables a las que poder recurrir. Por ejemplo la web

https://www.pantallasamigas.net/ desarrolla proyectos y recursos educativos para la capacitación del alumnado de forma que puedan desenvolverse de manera autónoma en Internet, siendo el objetivo final que desarrollen las habilidades y competencias digitales que les permitan participar

de forma activa, positiva y saludable en la Red.

image.png

Web de pantallas amigas

Además el **Instituto Nacional de Ciberseguridad** **(INCIBE)** pone a disposición de la comunidad educativa una serie de recursos, algunos de ellos a través de **Internet Segura for Kids** **(IS4K)** y de la **Oficina de Seguridad del Internauta** **(OSI) que son de gran ayuda, recordamos** **Línea de Ayuda 017**que es la línea de ayuda gratuita de ciberseguridad de INCIBE, operativa todos los días del año. Se atienden, entre otros, consultas de menores, madres y padres, profesores y otros profesionales de la educación.

image.png

- ## Redes Sociales

Estar al día en todo lo relativo a internet y tecnologías, para poder ayudar y acompañar a sus hijos o hijas en el buen uso de ellas. Por ejemplo en las manejo de las redes sociales

image-1670965551424.png

> Más información en el siguiente enlace

- ## Charlas formativas a las familias del Plan director para la convivencia y mejora de la seguridad

Las **familias suelen ser citadas** a charlas informativas para conocer de primera mano lo que van a escuchar sus hijos en los centros educativos y poder trabajar de forma colaborativa familias-centro-alumnado.

El Plan director para la convivencia y mejora de la seguridad en los centros educativos y sus entornos donde los cuerpos y fuerzas de seguridad del estado (Guardia Civil y Policía Nacional viene)n a los centros y nos ayudan en temas vinculados a internet, ciberacoso, redes sociales... y las responsabilidades civiles e incluso penales que tienen las actuaciones delictivas.

image.png

image.png

- ## Controles parentales como herramientas de seguridad

El **control parental** es una herramienta que permite a las familias controlar y limitar el contenido al que acceden los niños en internet, independientemente del dispositivo que usen (móviles, ordenadores, tablet, etc).

Entre las **funciones habituales** que suelen ofrecer este tipo de herramientas destacan: control web, control de aplicaciones, bloqueo de llamadas, tiempo de uso, alarmas, geolocalización o botón de emergencia.

Estas herramientas son un **complemento en nuestra labor de mediación parental**, siempre deben ir acompañadas de actividades digitales en familia que faciliten un clima de comunicación y confianza.

image.png

> Más información sobre controladores en los diferentes aparatos electrónicos en el siguiente enlace

- ## Utilizar los grupos de mensajería instantánea o Whatsapp entre familias como herramienta de ayuda en la convivencia y seguridad

Los grupos de mensajería instantánea son herramientas que pueden ser muy útiles a las familias para ayudarse a organizarse, y mantenerse en contacto en todo lo relacionado con el centro educativo, además puede servirnos con criterios de **seguridad**.

Es muy importante respetar una serie de normas para que el grupo aproveche el gran potencial, de lo que es tener información de primera mano, en lo que concierne a nuestros hijos.

En la siguiente imagen se indican 8 normas para el grupo del colegio.

image.png

Finalmente recordamos una recomendación de la Agencia Española de Protección de Datos (AEPD) exponiendo que, las **comunicaciones** entre profesores y padres de alumnos deben llevarse a cabo, preferentemente, a través de los medios puestos a disposición de ambos por el centro educativo **(plataformas educativas, correo electrónico** del centro,...).

pexels-anton-4132538.jpg

Foto de Anton en Pexels

El uso de aplicaciones de mensajería instantánea (como WhatsApp) entre profesores y padres o entre profesores y alumnos no se recomienda. No obstante, **en aquellos casos en los que el interés superior del menor estuviera comprometido**, como en caso de accidente o indisposición en una excursión escolar, y con la finalidad de **informar y tranquilizar a las familias**, titulares de la patria potestad, **se podrían captar imágenes y enviárselas.**

> Plantilla de posibles orientaciones a las familias en materia de ciberseguridad.image.png

Canales de ayuda

Canales de ayuda

Instituto Nacional de Ciberseguridad (INCIBE)

El **Instituto Nacional de Ciberseguridad** **(INCIBE)** pone a disposición de la comunidad educativa una serie de recursos, algunos de ellos a través de **Internet Segura for Kids** **(IS4K)** y de la **Oficina de Seguridad del Internauta** **(OSI)**:

- **Línea de Ayuda 017**: línea de ayuda gratuita de ciberseguridad de INCIBE, operativa todos los días del año. Se atienden, entre otros, consultas de menores, madres y padres, profesores y otros profesionales de la educación.
- **Educando en competencias digitales – CiberCOVID19**: página con diversos recursos con pautas para familias y educadores.
- **Consejos de ciberseguridad para el teletrabajo de docentes**: artículo con pautas para que los docentes puedan trabajar desde casa de forma cibersegura.
- **Ahora más que nunca, enseña a tus alumnos a identificar bulos y noticias falsas**: artículo con pautas sobre cómo trabajar en las clases virtuales la identificación de bulos y noticias falsas.
- **Materiales didácticos**: catálogo con diferentes recursos (unidades didácticas, presentaciones, actividades, etc.) sobre ciberseguridad.
- **Campañas:** **La ciberseguridad en tu mochila** y **Alfabetización mediática**.
- **Guía de privacidad y seguridad en Internet**: guía elaborada por OSI (INCIBE) y la AEPD, formada por 18 fichas que recogen los principales riesgos a los que nos exponemos al hacer uso de Internet así como las medidas de protección que debemos aplicar para evitarlos.
- **Guía para aprender a identificar fraudes *online***: guía compuesta por nueve fichas para ayudar a identificar los principales tipos de fraudes que existen en la red.
- **Canales de Youtube de OSI y de IS4K**: canales con vídeos sobre diferentes cuestiones relacionadas con la seguridad en Internet.
- **Avisos de ciberseguridad**: sección de la página web de OSI con noticias y avisos de ciberseguridad, de actualidad. Puedes suscribirte al boletín para estar al día de las últimas

novedades pinchando aquí.

Agencia Española de Protección de Datos (AEPD)

- **Canal Prioritario de la AEPD:** canal de la Agencia Española de Protección de Datos cuyo objetivo es ayudar a las víctimas de la violencia digital y evitar que aquellos contenidos, imágenes, audios o mensajes degradantes y humillantes que la ocasionan se sigan difundiendo a través de Internet. Se ha articulado, así, un procedimiento para solicitar su retirada de la red ofreciendo una rápida respuesta para situaciones excepcionalmente delicadas y gravosas.
- **Guía para centros educativos de la AEPD**: guía con pautas para un tratamiento correcto de los datos personales en centros educativos.
- **Tú decides en Internet**: web de la Agencia Española de Protección de Datos con diversas informaciones y recursos sobre protección de datos y menores.
- **Protección del menor en Internet. Recomendaciones para padres y tutores**: infografía con consejos y pautas para la protección de los menores en Internet.
- **Recomendaciones para proteger los datos personales en situaciones de movilidad y teletrabajo**
- **Decálogo de recursos de ayuda de la AEPD**

> Fuente INTEF