4. Uso responsable y bienestar digital

Introducción.

Uno de los grandes problemas que se encuentra el docente **al ayudar a usar las TIC por parte del alumnado es: ¿Hará un uso responsable de ellas? ¿Harán un buen uso de las redes sociales en el momento que las tengan? ¿Sufrirán o harán sufrir el tan temido 'bullying?**

Como docente hay que preguntarse si somos capaces de dejar la puerta de nuestra casa abierta durante todo el día y la respuesta suele ser: "No". Si preguntas por qué no se queda abierta la puerta es porque pueden entrar a robar. Si se hace la misma pregunta pero relacionada con las tecnologías digitales sería si tienes contraseña en tu ordenador, tableta, teléfono móvil, etc... y puede que haya gente que te diga que no tiene ninguna contraseña. En el momento que otra persona disponga de ese dispositivo sin contraseña o con la contraseña guardada por defecto va a disponer de multitud de tus datos personales y profesionales. Hoy en día mucha de nuestra información está guardada en servidores, lo que se hace llamar "la nube" para poder disponer de ella en cualquier momento por lo que **hay que enseñar a nuestro alumnado a tener guardada toda la información que dispone en dispositivos digitales mediante sistemas de contraseña.**

> Esta competencia digital docente está íntimamente **relacionada con la competencia digital docente 1.5 'Protección de datos personales, privacidad, seguridad y bienestar digital'** del MRCDD.

Privacidad.

Una vez que ya se es consciente del uso obligatorio de contraseñas en nuestros dispositivos tenemos que saber que hay sistemas informáticos que descifran nuestras contraseñas en segundos por lo que hay que utilizar contraseñas seguras. La **creación de contraseñas seguras** implica utilizar como **mínimo 12 caracteres** entre los que se tienen que incluir **letras mayúsculas, minúsculas, números y al menos un carácter especial (!, ¡, -, _, *, etc)**. Mantener una gran seguridad en el uso de contraseñas implica, por último, **cambiar las contraseñas cada 3 meses**. Este trabajo supone estar dedicados al uso de contraseñas seguras mucho tiempo por lo que se aconseja el uso de un **gestor de contraseñas**.

> Cada uno de los equipos digitales que se encuentra en un centro educativo es usado a lo largo de un día por multitud de personas, ya sea por parte del profesorado, alumnado o personal no docente, por lo que es recomendable recordar a toda la comunidad educativa la importancia de salir de las aplicaciones y páginas web en las que haya que entrar por medio de contraseñas y no dejarlas ni memorizadas ni abiertas. A su vez el centro puede usar configuraciones en los sistemas operativos para evitar estas situaciones.

> En Aragón se ha desarrollado el Sistema Operativo VITALINUX, basado en el sistema operativo LUBUNTU, para su uso en centros educativos. Este Sistema Operativo permite configurar cada ordenador de cada centro educativo para que pueda guardar su propio nivel de privacidad a nivel de contraseñas. Para más información pincha en el siguiente enlace.

A nivel de privacidad y datos personales hay que destacar que el alumnado que estudia en los centros educativos, en su mayoría, es menor de edad por lo que hay que proteger la identidad del menor. Los centros educativos y los docentes deben tener especial cuidado a la hora de usar los datos personales del alumnado. Hay que informar, y obtener el permiso de los padres o tutores legales del menor, del uso que se pueden hacer de esos datos en los distintos entornos digitales en los que el centro educativo puede participar. A continuación se destacan los posibles entornos en los que un centro educativo puede hacer uso de datos personales del alumnado:

- El **entorno docente**, ejemplos son los documentos digitales para impartir docencia y el blog de aula.
- El **entorno de las redes sociales y webs propias del profesorado y del centro educativo**, en los que se pueden incluir los listados del alumnado y su propia imagen.
- El **entorno de otras webs corporativas del Gobierno de Aragón y el Ministerio de Educación y Formación Profesional** al haber participado en proyectos o visitas educativas destacables.

Freepik. Privacidad online. 8photo. (CC BY-SA)

Uso y consumo de tecnologías digitales.

Para realizar un uso y consumo de las tecnologías digitales y las redes sociales hay que destacar a nuestro alumnado que debe tener en cuenta tres aspectos:

- **Aspecto postural**. Destacando la postura de la zona cervical y dorsal de la columna vertebral.
- **Aspecto visual**. En el que se destaca el uso prematuro de procedimientos de corrección de la graduación visual del menor por el uso de dispositivos digitales.
- **Aspecto mental**. Éste último es el que más preocupación produce en la sociedad actual, destacando:
  - El uso excesivo de dispositivos digitales, ya que el fin último es el consumo máximo de publicidad personalizada o encubierta por medio de influencers, la segmentación de perfiles para realizar acciones de marketing.
  - El ciberacoso o “bullying”, en el que se incluyen la difusión o recepción de bulos o fraudes que provocan desinformación o alarma social, el consumo o generación de discursos de odio, irrespetuosos o agresivos que pueden promover ideas extremistas, generando actitudes intolerantes o violentas y la pertenencia a comunidades que promueven conductas dañinas, trastornos alimenticios, autolesiones o consumo de drogas.

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

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

Uso responsable de las Redes Sociales

El uso responsable de redes sociales de forma segura y positiva incluye los siguientes puntos:

- La **elección de la red social adecuada a la edad y a su madurez del menor** mediante:
  - La **selección de un perfil privado** en la configuración de la cuenta de la red social.
  - La **limitación de la visibilidad de sus publicaciones** solo a sus contactos.
  - La **limitación de la recepción de mensajes y comentarios** solo a sus contactos.
  - La **prohibición de la recepción de publicidad personalizada**.
- **La creación de una buena identidad digital**, realizando publicaciones en las que se respeten a sí mismos y a los demás. (por ejemplo, pidiendo permiso para publicar fotos de los demás).
- **La administración correcta de las solicitudes de amistad**, limitando esas solicitudes a compañeros de clase o familiares de su edad y a sus padres o tutores legales, siendo estos últimos junto con el profesorado los que les enseñen a aprender a distinguir qué solicitudes pueden ser de riesgo.

https://www.youtube.com/embed/rNmXiYY9iHA

Youtube. Identidad digital: ¿quiénes somos en las redes sociales?. OSI (Oficina de Seguridad del Internauta)

Ciberacoso.

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.

Listado de términos y palabras clave

¿Qué palabras o términos clave están intrínsecamente relacionados con la competencia 6.4? En esta página se ofrece un listado de términos y palabras clave que ayudan a comprender la dimensión de esta competencia.

PALABRAS CLAVE	
fraude digital riesgos ciberacoso RGPD Derechos Digitales biométrico restringir acceso adicción 2FA autenticador	PDC entorno digital perfil de usuario geoetiquetado contraseña des/encriptar AEPD cookies ciberseguridad RR.SS.

¿Cómo podría trabajar la competencia 6.4 en mi aula en un nivel A2?

En esta página se exponen **dos ejemplos** que se pueden llevar a cabo en nuestras aulas. Para realizar una distinción de etapa, el primero de los ejemplos estará destinado a cursos como Educación Infantil o Educación Primaria, mientras que el segundo, a etapas contextualizadas en aulas de Educación Secundaria, Bachillerato o Formación Profesional.

Freepik. Digitalización del futuro. Rawpixel.com (CC BY-SA)

EDUCACIÓN INFANTIL Y EDUCACIÓN PRIMARIA

Cada vez es más normal el uso de plataformas educativas en los centros de educación infantil y educación primaria y el alumnado debe registrarse para utilizar los recursos que le comparte su profesorado en las distintas asignaturas.

Por ello, la actividad a realizar consiste en organizar en el aula, en pequeños grupos de alumnado que se conozca bien, una dinámica para adivinar las contraseñas que utilizan. De manera que sensibilicemos sobre la necesidad de crear contraseñas robustas.

Freepik. Seguridad en la red. 8photo (CC

EDUCACIÓN SECUNDARIA, BACHILLERATO Y FORMACIÓN PROFESIONAL

Continuando con la idea del bloque de educación infantil y primaria la actividad propuesta consiste en ayudar a configurar los perfiles de usuario del alumnado de mi tutoría a la vez que configuro mi perfil de profesorado en la plataforma educativa (entorno virtual de aprendizaje, EVA) del centro siguiendo las pautas recogidas en el Plan Digital de Centro y en el protocolo proporcionado a tal efecto.

Freepik. Configuración de una video llamada. rawpixel.com (CC BY-SA)