

# TRABAJO FIN DE MÁSTER



## UCAM

UNIVERSIDAD CATÓLICA  
DE MURCIA

### FACULTAD DE CIENCIAS SOCIALES Y DE LA COMUNICACIÓN

Máster Universitario en Formación del Profesorado de  
Educación Secundaria Obligatoria y Bachillerato, Formación  
Profesional y Enseñanzas de Idiomas

### CIBERSEGURIDAD Y FOMENTO DE BUENOS HÁBITOS EN EL USO DE LAS TIC EN ALUMNADO DE SECUNDARIA MEDIANTE AULA INVERTIDA

Autor:

D. Eduardo Turmo Durán

[https://youtu.be/-4w\\_BU76FAc](https://youtu.be/-4w_BU76FAc)

Director:

D. Juan Miguel Navarro Ruiz

Murcia, 7 de mayo de 2021







# TRABAJO FIN DE MÁSTER



## UCAM

UNIVERSIDAD CATÓLICA  
DE MURCIA

### FACULTAD DE CIENCIAS SOCIALES Y DE LA COMUNICACIÓN

Máster Universitario en Formación del Profesorado de  
Educación Secundaria Obligatoria y Bachillerato, Formación  
Profesional y Enseñanzas de Idiomas

### CIBERSEGURIDAD Y FOMENTO DE BUENOS HÁBITOS EN EL USO DE LAS TIC EN ALUMNADO DE SECUNDARIA MEDIANTE AULA INVERTIDA

Autor:

D. Eduardo Turmo Durán

[https://youtu.be/-4w\\_BU76FAc](https://youtu.be/-4w_BU76FAc)

Director:

D. Juan Miguel Navarro Ruiz

Murcia, 7 de mayo de 2021



## **AUTORIZACIÓN PARA LA EDICIÓN ELECTRÓNICA Y DIVULGACIÓN EN ACCESO ABIERTO DE DOCUMENTOS EN EL REPOSITORIO INSTITUCIONAL DE LA UNIVERSIDAD CATÓLICA DE MURCIA**

El autor, D. Eduardo Turmo Durán (██████████) como Alumno de la UNIVERSIDAD CATÓLICA DE MURCIA, **DECLARA** que es el titular de los derechos de propiedad intelectual objeto de la presente cesión en relación con la obra “CIBERSEGURIDAD Y FOMENTO DE BUENOS HÁBITOS EN EL USO DE LAS TIC EN ALUMNADO DE SECUNDARIA MEDIANTE AULA INVERTIDA” (Trabajo Fin de Máster), que ésta es una obra original y que ostenta la condición de autor en el sentido que otorga la Ley de la Propiedad Intelectual como único titular o cotitular de la obra.

En caso de ser cotitular, el autor (firmante) declara asimismo que cuenta con el consentimiento de los restantes titulares para hacer la presente cesión. En caso de previa cesión a terceros de derechos de explotación de la obra, el autor declara que tiene la oportuna autorización de dichos titulares de derechos a los fines de esta cesión o bien que retiene la facultad de ceder estos derechos en la forma prevista en la presente cesión y así lo acredita.

### **2º. Objeto y fines de la cesión**

Con el fin de dar la máxima difusión a la obra citada a través del Repositorio institucional de la Universidad y hacer posible su utilización de *forma libre y gratuita* por todos los usuarios del repositorio, el autor **CEDE** a la Universidad Católica de Murcia **de forma gratuita y no exclusiva**, por el máximo plazo legal y con ámbito universal, los derechos de reproducción, distribución, comunicación pública, incluido el derecho de puesta a disposición electrónica, y transformación sobre la obra indicada tal y como se describen en la Ley de Propiedad Intelectual.

### **3º. Condiciones de la cesión**

Sin perjuicio de la titularidad de la obra, que sigue correspondiendo a su autor, la cesión de derechos contemplada en esta licencia permite al repositorio institucional:

- a) Transformarla en la medida en que ello sea necesario para adaptarla a cualquier tecnología susceptible de incorporación a internet; realizar las adaptaciones necesarias para hacer posible la utilización de la obra en formatos electrónicos, así como incorporar los metadatos necesarios para realizar el registro de la obra e incorporar también “marcas de agua” o cualquier otro sistema de seguridad o de protección.
- b) Reproducirla en un soporte digital para su incorporación a una base de datos electrónica, incluyendo el derecho de reproducir y almacenar la obra en servidores, a los efectos de garantizar su seguridad, conservación y preservar el formato.
- c) Distribuir a los usuarios copias electrónicas de la obra en un soporte digital.
- d) Su comunicación pública y su puesta a disposición a través de un archivo abierto institucional, accesible de modo libre y gratuito a través de Internet.

### **4º. Derechos del autor**

El autor, en tanto que titular de una obra que cede con carácter no exclusivo a la Universidad por medio de su registro en el Repositorio Institucional tiene derecho a:

- a) A que la Universidad identifique claramente su nombre como el autor o propietario de los derechos del documento.
- b) Comunicar y dar publicidad a la obra en la versión que ceda y en otras posteriores a través de cualquier medio. El autor es libre de comunicar y dar publicidad a la obra, en esta y en posteriores versiones, a través de los medios que estime oportunos.
- c) Solicitar la retirada de la obra del repositorio por causa justificada. A tal fin deberá ponerse en contacto con el responsable del mismo.
- d) Recibir notificación fehaciente de cualquier reclamación que puedan formular terceras

personas en relación con la obra y, en particular, de reclamaciones relativas a los derechos de propiedad intelectual sobre ella.

#### **5º. Deberes del autor**

El autor se compromete a:

- a) Garantizar que el compromiso que adquiere mediante el presente escrito no infringe ningún derecho de terceros, ya sean de propiedad industrial, intelectual o cualquier otro.
- b) Garantizar que el contenido de las obras no atenta contra los derechos al honor, a la intimidad y a la imagen de terceros.
- c) Asumir toda reclamación o responsabilidad, incluyendo las indemnizaciones por daños, que pudieran ejercitarse contra la Universidad por terceros que vieran infringidos sus derechos e intereses a causa de la cesión.
- d) Asumir la responsabilidad en el caso de que las instituciones fueran condenadas por infracción de derechos derivada de las obras objeto de la cesión.

#### **6º. Fines y funcionamiento del Repositorio Institucional**

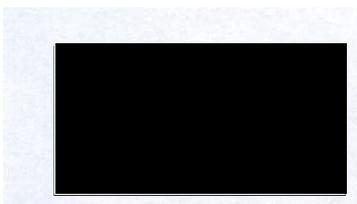
La obra se pondrá a disposición de los usuarios para que hagan de ella un uso justo y respetuoso con los derechos del autor, según lo permitido por la legislación aplicable, sea con fines de estudio, investigación, o cualquier otro fin lícito, y de acuerdo a las condiciones establecidas en la licencia de uso –modalidad “reconocimiento-no comercial-sin obra derivada” de modo que las obras puedan ser distribuidas, copiadas y exhibidas siempre que se cite su autoría, no se obtenga beneficio comercial, y no se realicen obras derivadas. Con dicha finalidad, la Universidad asume los siguientes deberes y se reserva las siguientes facultades:

##### a) Deberes del repositorio Institucional:

- La Universidad informará a los usuarios del archivo sobre los usos permitidos, y no garantiza ni asume responsabilidad alguna por otras formas en que los usuarios hagan un uso posterior de las obras no conforme con la legislación vigente. El uso posterior, más allá de la copia privada, requerirá que se cite la fuente y se reconozca la autoría, que no se obtenga beneficio comercial, y que no se realicen obras derivadas.
  - La Universidad no revisará el contenido de las obras, que en todo caso permanecerá bajo la responsabilidad exclusiva del autor y no estará obligada a ejercitar acciones legales en nombre del autor en el supuesto de infracciones a derechos de propiedad intelectual derivados del depósito y archivo de las obras. El autor renuncia a cualquier reclamación frente a la Universidad por las formas no ajustadas a la legislación vigente en que los usuarios hagan uso de las obras.
  - La Universidad adoptará las medidas necesarias para la preservación de la obra en un futuro.
- b) Derechos que se reserva el Repositorio institucional respecto de las obras en él registradas:
- Retirar la obra, previa notificación al autor, en supuestos suficientemente justificados, o en caso de reclamaciones de terceros.

Murcia, a 7 de Mayo de 2021

#### **ACEPTA**



Fdo. Eduardo Turmo Durán





## ÍNDICE

1. JUSTIFICACIÓN .....	13
2. MARCO TEÓRICO .....	16
3. OBJETIVOS.....	22
3.1 OBJETIVO GENERAL.....	22
3.2 OBJETIVOS ESPECÍFICOS.....	22
4. METODOLOGÍA .....	23
4.1 DESCRIPCIÓN DEL PROYECTO .....	25
4.2 CONTENIDOS .....	26
4.3 TEMPORALIZACIÓN .....	27
4.4 ACTIVIDADES .....	31
4.5 RECURSOS .....	43
5. EVALUACIÓN .....	46
6. REFLEXIÓN Y VAORACIÓN FINAL .....	49
7. REFERENCIAS BIBLIOGRÁFICAS.....	52
8. ANEXOS.....	55

## ÍNDICE DE FIGURAS Y TABLAS

TABLA 1. BLOQUES DE CONTENIDOS DE LA ASIGNATURA DE TECNOLOGÍA EN 4º ESO.....	17
TABLA 2. BLOQUE 1: TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN.....	18
TABLA 3. FASE DE INICIO EN LA TEMPORALIZACIÓN DEL PROYECTO.....	28
TABLA 4. FASE DE DESARROLLO EN LA TEMPORALIZACIÓN DEL PROYECTO.....	30
TABLA 5. FASE DE EVALUACIÓN EN LA TEMPORALIZACIÓN DEL PROYECTO.....	32
TABLA 6. TAREAS PREVIAS A CLASE EN AULA INVERTIDA O FLIPPED CLASSROOM.....	33
TABLA 7. TAREAS DURANTE LA CLASE EN AULA INVERTIDA O FLIPPED CLASSROOM.....	33
TABLA 8. TAREAS DESPUÉS DE CLASE EN AULA INVERTIDA O FLIPPED CLASSROOM.....	34
TABLA 9. RESUMEN DE LAS ACTIVIDADES A REALIZAR EN LAS SESIONES DE AULA INVERTIDA...35	
FIGURA 1. AULA INVERTIDA O FLIPPED CLASSROOM.....	25
FIGURA 2. FUNCIONAMIENTO DEL AULA INVERTIDA O FLIPPED CLASSROOM.....	25
FIGURA 3. EJEMPLO DE REGISTRO DE ACTIVIDAD DE CUENTA DE GOOGLE.....	38
FIGURA 4. EJEMPLO DE REGISTRO CRONOLÓGICO DE UBICACIONES DE CUENTA DE GOOGLE...38	
FIGURA 5. PLATAFORMA DE APRENDIZAJE: GOOGLE CLASSROOM.....	44

## 1. JUSTIFICACIÓN

En los últimos tiempos el uso de las Tecnologías de la Información y la Comunicación (TIC) se ha generalizado de una forma que no podríamos imaginar hace no mucho, sobre todo en el caso de los dispositivos móviles. Esto es debido a las mejoras en los estándares de telefonía móvil, con la introducción del 3G, 4G y, en la actualidad, el inicio del despliegue del 5G, que ha provocado que podamos navegar por Internet desde cualquier lugar, con unas velocidades que antes estaban reservadas sólo a las conexiones mediante cable.

Por otro lado, y como consecuencia de lo anteriormente comentado, la evolución de los teléfonos móviles a smartphones ha hecho que prácticamente todos, a partir de una determinada edad, tengamos uno y lo usemos a diario para una gran variedad de cometidos. Porque ya no solo lo podemos usar para llamar o enviar algún mensaje, sino que además de esto, nos sirve para conectarnos a Internet y poder consultar las noticias, la previsión meteorológica, el correo electrónico, nuestras redes sociales (RRSS) o hacer uso de multitud de aplicaciones que tenemos instaladas en ellos para casi cualquier propósito.

Esto nos facilita la vida en muchos aspectos, pero también debemos de tener en cuenta que nos acarrea una serie de riesgos e inconvenientes, que no todo el mundo conoce o no es capaz de calibrar su alcance. Por este motivo, creo que es necesario tener una formación mínima en el ámbito de la ciberseguridad, aunque sea a nivel de usuario, para no tener que lamentarnos luego. En el caso de los adolescentes no es diferente, y en mi opinión, lo considero más importante aún si cabe, porque cada vez es más temprana la edad a la que tienen su propio ordenador o teléfono móvil.

Desde hace algún tiempo, me he dado cuenta que en mi entorno ocurre lo que comentaba anteriormente, no todo el mundo es consciente de los riesgos que puede suponer un uso inadecuado de las TIC. Sobre todo, recibo consultas, en algunos casos con preocupación y angustia, de familiares y amigos con hijos en edad adolescente que empiezan a introducirse en este nuevo mundo que es para ellos la tecnología e Internet. Como Ingeniero Técnico de Telecomunicación que soy, y apasionado de las tecnologías, siempre me ha encantado poder

asesorar, investigar y divulgar mis conocimientos al respecto a quien me lo solicita, para de esta forma tratar de evitar los posibles riesgos.

Cuando comencé el Practicum en un centro educativo de mi localidad, pude comprobar que esto no era una simple percepción mía relacionada con mi entorno. Durante el periodo de prácticas en el centro he podido observar, y también me han confirmado distintos profesores y la responsable del departamento de orientación, que entre muchos de los alumnos y alumnas se dan conductas poco apropiadas en el uso de las TIC. He podido ver en muchas ocasiones un exceso de atención o casi dependencia de los móviles (teniendo que llamarles la atención para dejen de usarlos durante las clases), así como comentarios y dudas que me han formulado sobre sus cuentas de correo electrónico, apps o publicaciones en RRSS en el ámbito precisamente de la asignatura de TIC II, de la que he impartido algunas clases.

Gracias a esto, he podido constatar que una mayoría del alumnado tiene una serie de carencias importantes en lo referido a la competencia digital, ya que no conocen los riesgos que pueden tener determinadas conductas en la sociedad multiconectada actual en la que vivimos. Además, hablando con ellos también he podido comprobar que muchas de las recomendaciones que les he dado, por ejemplo, respecto a la configuración de privacidad de sus cuentas de Google, RRSS o apps, no las han recibido nunca por parte de sus padres y madres, ya que, según ellos, solo se limitan a ponerles límites de tiempo al uso del móvil o el ordenador. Aunque se les considera nativos digitales, igual que aprendieron a caminar, a comer o relacionarse, también es necesario enseñarles unas rutinas o buenos hábitos digitales para el uso de Internet.

Por todo esto, tras confirmar con mi tutor de prácticas que él también observa estas carencias, y que sería muy positivo diseñar una serie de acciones que pudieran solventarlas, decidí que la elaboración de este Trabajo de Fin de Máster (TFM) fuera en esa línea. En primer lugar, se pretende que el alumnado conozca los riesgos inherentes al uso de las TIC y se tratará de concienciar sobre la importancia de tomar medidas frente a éstos. En mi opinión, esto será lo primordial, porque si no se conoce un peligro, no tomamos las medidas de protección oportunas, y es entonces cuando estamos realmente en riesgo. Y,

después, fomentaremos una serie de buenas prácticas en el ámbito de la ciberseguridad, para que tengan instrumentos o habilidades para desenvolverse en el mundo digital de forma responsable y lo más segura posible.

Todo esto lo llevaremos a cabo en la asignatura de Tecnología de 4º de Enseñanza Secundaria Obligatoria (ESO), ya que considero que es importante tratar estos temas a una edad temprana, pero lo suficientemente madura como para comprender el significado real y la importancia que tienen. Se hará desarrollando los contenidos del currículo de Seguridad Informática, dentro del bloque I: Tecnologías de la Información y la Comunicación, mediante una metodología de aula invertida.

Utilizando esta metodología, favorecemos el aprendizaje significativo de una competencia transversal, como es la competencia digital. Hay que tener en cuenta que el aula invertida no funciona en todos los contextos, ni en todos los grupos, ya que para obtener los resultados que esperamos se requiere una implicación e interés previo por parte del alumnado. La idea es enfocar esta temática desde un punto de vista que atrae a la mayoría de los adolescentes, como son las RRSS e Internet. De esta forma, conseguiremos un plus de motivación y que se produzca un aprendizaje más duradero en el tiempo, porque ha sido construido por los propios alumnos y alumnas, debido a que el trabajo previo en casa no les resultará tedioso y se hará más atractivo.

## 2. MARCO TEÓRICO

### 2.1 NORMATIVA VIGENTE

A la hora de desarrollar la propuesta educativa de este TFM, es importante tener el claro el marco legal de aplicación, en este caso para la asignatura de Tecnología en 4º de ESO.

En el Real Decreto 1105/2014, de 26 de diciembre, se establece en currículo básico la para las asignaturas de Enseñanza Secundaria Obligatoria y Bachillerato. En este Real Decreto se especifica que la asignatura de Tecnología, en el curso de 4º de ESO, tiene los siguientes 6 bloques de contenidos:

TECNOLOGÍA EN 4º DE ESO	
Bloque 1	Tecnologías de la información y la comunicación
Bloque 2	Instalaciones en viviendas
Bloque 3	Electrónica
Bloque 4	Control y Robótica
Bloque 5	Neumática e hidráulica
Bloque 6	Tecnología y sociedad

**Tabla 1. Bloques de contenidos de la asignatura de Tecnología en 4º ESO**

A nivel autonómico, es el decreto nº 220/2015, de 2 de septiembre de 2015, el que concreta los contenidos específicos de estos bloques generales del Currículo en la Enseñanza Secundaria Obligatoria en la Región de Murcia. Para el bloque 1 tendríamos los contenidos, criterios de evaluación y estándares de aprendizaje evaluables que se pueden ver en la Tabla 2. En el caso que nos ocupa, habrá que fijarse en el punto de los contenidos referente a la “Seguridad informática”. A su vez, en los criterios de evaluación, el punto 2 es “Acceder a servicios de intercambio y publicación de información digital con criterios de seguridad y uso responsable”. Y en los estándares de aprendizaje, el punto 2.2 será “Conoce las medidas de seguridad aplicables a cada situación de riesgo”.

CONTENIDOS	CRITERIOS DE EVALUACIÓN	ESTANDARES DE APRENDIZAJE EVALUABLES
-Elementos y dispositivos de comunicación alámbrica e inalámbrica. -Tipología de redes. -Publicación e intercambio de información en medios digitales. -Conceptos básicos e introducción a los lenguajes de programación. <b>-Seguridad informática.</b> -Software de adquisición e interpretación de datos.	1. Analizar los elementos y sistemas que configuran la comunicación alámbrica e inalámbrica.	1.1. Describe los elementos y sistemas fundamentales que se utilizan en la comunicación alámbrica e inalámbrica.  1.2. Describe las formas de conexión en la comunicación entre dispositivos digitales.
	<b>2. Acceder a servicios de intercambio y publicación de información digital con criterios de seguridad y uso responsable.</b>	2.1. Localiza, intercambia y publica información a través de Internet empleando servicios de localización, comunicación intergrupala y gestores de transmisión de sonido, imagen y datos.
		<b>2.2. Conoce las medidas de seguridad aplicables a cada situación de riesgo.</b>
	3. Elaborar sencillos programas informáticos.	3.1. Desarrolla un sencillo programa informático para resolver problemas utilizando un lenguaje de programación.
	4. Utilizar equipos informáticos.	4.1. Utiliza el ordenador como herramienta de adquisición e interpretación de datos, y como realimentación de otros procesos con los datos obtenidos.

**Tabla 2. Bloque 1: Tecnologías de la información y la comunicación**

## 2.2 FUNDAMENTOS TEÓRICOS Y CONCEPTUALES

Referente a la ciberseguridad, o seguridad informática, y la concienciación de los riesgos inherentes al uso de las TIC para alumnos y alumnas de secundaria hay numerosos estudios y planes de diferentes comunidades autónomas, incluso ya existen algunos orientados al alumnado de los últimos cursos de primaria, como Ciberprotégete o Ciber expert@ (Gomez et al., 2020).

Lo más importante a la hora de concienciar a los adolescentes con respecto a la ciberseguridad es que tengan claro cuales son los riesgos a los que se enfrentan. En primer lugar, el riesgo para su privacidad, especialmente en el uso de las redes sociales (RRSS). En un estudio realizado se pone de manifiesto que:

Muchos adolescentes utilizan ampliamente las redes sociales para incrementar su sociabilidad sin ser conscientes del valor de la información compartida y de los riesgos potenciales existentes relacionados con su privacidad y seguridad en la red. La utilización indebida o la divulgación sin permiso de la información privada de los usuarios puede tener

consecuencias no deseadas en la vida de las personas. (Argente et al., 2017, p. 107)

Y estos riesgos se puede clasificar en tres tipos según Vanderhoven et al. (2014), como son de contenido, de contacto y comerciales. Los primeros son los relacionados con contenido inapropiado o mensajes de odio, que requieren por parte de los adolescentes una capacidad de crítica consolidada. Los de contacto son los que más alarma causan porque son los más obvios, y pueden desembocar en prácticas como el ciberbullying (o ciberacoso), grooming o sexting. Por último, los comerciales incluyen el uso no autorizado de datos personales, que pueden ser utilizados por terceras empresas para hacer un seguimiento de los hábitos de consumo del individuo y ofrecerle anuncios personalizados según sus gustos o preferencias que incitan a la compra compulsiva.

El segundo lugar, las adicciones tecnológicas en la adolescencia son otro de los riesgos más importantes en el uso de las TIC. Como indica Montañés (2017), esta etapa se caracteriza por una gran vulnerabilidad ante esta o cualquier tipo de adicciones, debido a que hay determinadas zonas del cerebro relacionadas con la autorregulación de la conducta que no están todavía completamente desarrolladas. Esto tiene unos claros síntomas que deben de tenerse en cuenta si son observados, como son, necesidad de usar las tecnologías cada vez más veces o más tiempo, malestar o enfado en caso de no poder usarlas, dificultad para dejar de usarlas si las tiene a mano, son un impedimento para actividades normales como la alimentación o unas horas mínimas de sueño, si producen problemas familiares derivado de su exceso o uso inadecuado, y si se produce pérdida de interés por otras actividades que antes eran gratificantes.

Otro riesgo a tener en cuenta hoy en día son las ciberestafas, que tiene como práctica habitual el phishing (en todas sus variantes). Según Domínguez (2019) los ataques phishing constituyen un mecanismo criminal que utiliza técnicas de ingeniería social y subterfugio técnico para sustraer a los usuarios datos de identidad personal o incluso credenciales de sus cuentas bancarias.

Por desgracia, ninguna entidad o persona está libre de esta amenaza, de manera que hay que planificar una serie de medidas de prevención. Por ejemplo, la primera medida que toman las empresas, y la que mejores resultados tiene, es capacitar a su personal para ser capaz de reconocer este tipo de ataques.

Como se ha mencionado anteriormente, hay fenómenos especialmente peligrosos y de actualidad como el ciberbullying o ciberacoso, el grooming o el sexting. El ciberbullying o ciberacoso puede definirse de acuerdo con Hernández Prados et al. (2007) como el uso de cualquiera de las posibilidades que ofrecen las TIC para hostigar con ensañamiento a una víctima de acoso escolar, haciendo uso de la violencia física o psicológica sobre ella. El grooming en cambio no es violencia entre iguales como en el caso anterior, puesto que un adulto suplanta la identidad de un menor para acosar a otro menor, normalmente con intenciones sexuales, según algunos autores, de la siguiente forma:

Una estrategia básica -e intencional- de acercamiento al menor y configuraría una etapa previa de “cortejo” o seducción mediante la cual el ciberabusador trata de ganarse la confianza de su víctima y establecer con ella un vínculo afectivo que le sitúe en la situación de superioridad idónea para la manipulación y el control emocional del menor, además de asegurarle el silencio de la víctima. (Juan et al., 2014, p. 215)

Por último, el sexting no es un problema de seguridad informática en si mismo, es una práctica de riesgo. Según Pérez et al. (2011) “el sexting consiste en la difusión o publicación de contenidos (principalmente fotografías o videos) de tipo sexual, producidos por el propio remitente, utilizando para ello el teléfono móvil u otro dispositivo tecnológico” (p. 4).

Hay numerosos estudios que ponen de manifiesto la escasa percepción del riesgo que tienen los adolescentes ante todo esto, así como el abuso que hacen de las TIC, pero es destacable el realizado por Gairín y Mercader (2018) con 1194 alumnos de entre 12 y 17 años de Andalucía, Cataluña y Madrid. En los resultados del mismo pueden verse como el 38% utiliza el móvil más de 6 horas durante el fin de semana y un 37% el ordenador durante más de 3 horas. El alumnado entre los 15 y los 17 años presenta una mayor incidencia en las

conductas de riesgo, el 54,2% tiene contacto con desconocidos, el 41,7% afirma que envía mensajes de burla a otros y el 25,7% comparte imágenes y videos de otros sin consentimiento.

Por lo anteriormente expuesto, se deduce la necesidad de implementar actividades de concienciación y formativas sobre esta temática. De hecho, por lo general, este tipo de proyectos suelen tener una buena aceptación, como se deduce, por ejemplo, de los resultados obtenidos por Prats et al. (2018) en sus Talleres para el uso saludable de Internet y las RRSS, en los que se observa una opinión por parte de los alumnos muy positiva al respecto, considerándolos muy útiles e importantes, siendo muy participativos en debates y dinámicas de grupo, aumentando su grado de concienciación y expresando la necesidad de seguir teniendo talleres o formaciones de este tipo de forma regular.

### **2.3 METODOLOGÍA, ESTRATEGIA DE APRENDIZAJE Y RECURSOS CONCRETOS**

Para llevar a cabo la propuesta de este TFM se usará como metodología el modelo pedagógico de aula invertida o Flipped Classroom. La elección se hace después de leer varios artículos en los que se pone de manifiesto sus ventajas y los buenos resultados obtenidos con el uso de esta metodología.

El estudio realizado por Lucena et al. (2019) pone de manifiesto que “las distintas investigaciones que componen la muestra de estudio verifican en su mayoría que el método de aula invertida mejora el rendimiento académico de los estudiantes” (p. 16).

Por otro lado, de acuerdo con Villalba de Benito et al. (2018) gracias a este enfoque centrado en el estudiante, éste puede asimilar los temas con más profundidad a través de un enfoque activo y más significativo para el aprendizaje.

Además del aula invertida, se proponen actividades grupales que favorecen también estrategias de aprendizaje cooperativo, ya que como indican González y Carrillo (2016) “la fusión de metodologías activas como el Aprendizaje Cooperativo, con la Flipped Classroom y las TIC, permiten dirigir el

proceso de enseñanza - aprendizaje hacia la adquisición de conocimientos y procedimientos mucho más significativos" (p. 43).

Y, como ponen de manifiesto Johnson et al. (1999), la cooperación fomenta la motivación para alcanzar los objetivos, genera relaciones interpersonales más positivas y favorece una mejor salud mental que los modelos competitivo o individualista. Pero el docente tendrá que decidir cuales serán sus objetivos, la formación de los grupos y los roles dentro de cada grupo, como disponer el aula y que materiales didácticos que se usarán. Después, deberá explicar en que consiste trabajar de forma cooperativa, asignará tareas claras a cada miembro y tendrá que transmitir el significado de lo que es la responsabilidad tanto individual, como dentro del grupo. Y, por último, no hay que olvidar que el docente deberá coordinar, supervisar e intervenir cuando sea necesario durante todo el proceso, así como evaluarlo y fomentar la autocrítica por parte del alumnado, para ver como funcionaron sus grupos de aprendizaje.

Para llevar a cabo la metodología de aula invertida, se hace imprescindible el uso de las TIC como recurso concreto. Por tanto, como indican Sagrà y Guàrdia (2005), el docente necesitará producir o seleccionar contenidos y materiales que el alumnado tendrá que trabajar previamente. Para ello tendrá que usar algún tipo de plataforma o aula virtual (tipo Moodle, Google Classroom o del propio centro) para publicar y distribuir dichos materiales. Esto lleva consigo posteriormente tareas de mantenimiento, administración de sistemas, revisión y actualización de los contenidos en la plataforma elegida, así como apoyo técnico al alumnado.

### **3. OBJETIVOS**

Mediante este TFM se pretende alcanzar una serie de objetivos que se detallan a continuación. Se ha especificado un objetivo general, así como unos objetivos secundarios que ayudan y complementan la consecución del principal.

#### **3.1 OBJETIVO GENERAL**

- El objetivo principal es concienciar al alumnado de 4º de ESO sobre la importancia de tener unas nociones básicas sobre ciberseguridad y fomentar unos buenos hábitos en el uso de las TIC, mediante la metodología de aula invertida.

#### **3.2 OBJETIVOS ESPECÍFICOS**

Una vez definido el objetivo general, se procede a continuación a definir los distintos objetivos específicos que servirán para dar cada uno de los pasos necesarios para la consecución del objetivo principal:

- Valorar nuestra privacidad y saber que es la identidad digital. Solo de este modo se puede interaccionar con otros de forma adecuada a través del mundo virtual de Internet. Esto se conseguirá mediante actividades en las que el alumnado analizará publicaciones propias en RRSS y sus configuraciones de privacidad. (OE1).
- Conocer los riesgos a los que se expone el usuario cuando hace uso de las TIC en general, y las RRSS en particular (adicción a la tecnología, ciberestafas, grooming, sexting o ciberacoso), mediante el visionado de videos con experimentos o experiencias reales y el posterior debate en clase. (OE2).
- Fomentar buenos hábitos tecnológicos para salvaguardar nuestras relaciones personales en el mundo real, nuestra salud mental y nuestra intimidad, mediante una reflexión grupal de todos los conceptos expuestos anteriormente. (OE3).

#### **4. METODOLOGÍA**

El modelo pedagógico de aula invertida o Flipped Classroom fue creado por Bergmann J. y Sams A. en el año 2007, consiste en invertir algunos de los procesos tradicionales de aprendizaje fuera del aula, y otros que se hacían en casa, pasan a desarrollarse en el aula. Usando los videos grabados de sus clases para los alumnos que no habían podido asistir presencialmente por enfermedad, o cualquier otro motivo, se dieron cuenta que esta forma de trabajar la podían extrapolar a la totalidad de los alumnos. De esta manera, el tiempo en clase se podía utilizar de manera diferente, realizando otro tipo de actividades, facilitándose así la adquisición de conocimientos de forma significativa y práctica.

En esta metodología, en el proceso de enseñanza y aprendizaje se diferencian dos partes:

- Tiempo no presencial o en casa: al contrario que con el modelo tradicional, esta parte se produce antes de asistir a clase. En ella el alumnado visualiza videos, analiza los recursos facilitados por el profesor e investiga sobre el tema a tratar posteriormente en clase. Cada cual puede marcar su propio ritmo a la hora de asimilar los contenidos teóricos o pasivos.
- Tiempo presencial o en clase: se realizarán actividades grupales e individuales, debates, puestas en común, dudas y aclaraciones por parte del profesor. De esta forma, el alumnado podrá aplicar los conceptos previamente adquiridos, reflexionar y comprender, y así se genera conocimiento de forma constructiva.



Figura 1. Aula invertida o Flipped Classroom.

Nota: Adaptado de *Clase invertida*, de Nuria Sánchez Marcos, 2018, Diarium (<https://diarium.usal.es/nuriasama/2018/03/05/clase-invertida/>)

Como se puede deducir de la definición de esta metodología, para que tenga éxito puede y debe apoyarse también en una estrategia de aprendizaje colaborativo. Mediante el desarrollo de actividades tanto individuales como grupales, a la hora de construir conocimiento, el alumnado puede contar con la colaboración de sus compañeros, con el profesor y su entorno. De acuerdo con Lucero (2003), el aprendizaje en ambientes colaborativos fomenta el desarrollo de habilidades individuales y grupales, a partir de la discusión o el debate a la hora de investigar sobre nuevos conceptos, y siendo cada uno responsable de su aprendizaje. Se busca que este ambiente sea diverso en posibilidades y opiniones, para que así se propicie el crecimiento del grupo.

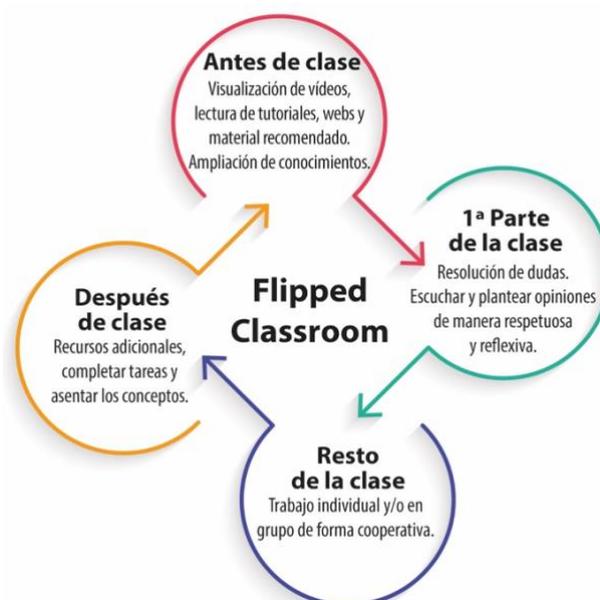


Figura 2. Funcionamiento del aula invertida o Flipped Classroom

A la hora de poner en práctica el aula invertida, como se ha comentado anteriormente, se hace imprescindible el uso de recursos TIC, para que el profesorado pueda compartir con el alumnado la información previa, videos, etc. Hoy en día existen numerosas plataformas, gestores de aulas o aulas virtuales diseñadas para este cometido (Moodle o Classroom de Google, por ejemplo), así como herramientas de documentos compartidos o colaborativos (Evernote o GDrive de Google). El profesor sube en estas plataformas el contenido o recursos que considere oportunos, y los alumnos pueden plantear dudas o sugerencias a través de los servicios de mensajería que tienen algunas de ellas o mediante redes sociales. Además, para compartir videos o conferencias también tenemos varias plataformas disponibles (Vimeo, Wistia, dailymotion o TED), pero actualmente Youtube, y su versión educativa Youtube Edu, son las que más contenido ofrecen y más usuarios tienen.

Por último, cabe destacar el papel del profesor en este nuevo modelo. Tal y como indica Berenguer-Albaladejo (2016), el profesor actúa como organizador o guía en el proceso de aprendizaje, seleccionando los contenidos que debe estudiar, asimilar y retener, poniéndolos a su disposición y estando constantemente en comunicación con el alumno, que es el que debe colaborar e implicarse activamente en su propio aprendizaje.

#### **4.1 DESCRIPCIÓN DEL PROYECTO**

Mediante la realización de este proyecto se pretende subsanar las deficiencias encontradas en el ámbito de la competencia digital del alumnado, en concreto, las relacionadas con la ciberseguridad y malos hábitos en el uso de las TIC y redes sociales. Además, trataremos de ampliar el margen de actuación hacia el resto del personal docente, al tratarse de una competencia transversal. Así como al ámbito de las familias, pues es un trabajo de todos y todas, y deben de estar también correctamente informadas y concienciadas.

## 4.2 CONTENIDOS

Como se ha mencionado anteriormente en el marco teórico, los contenidos de la asignatura de Tecnología de 4º de ESO en la región de Murcia se dividen en 6 bloques (según el Real Decreto nº 1105/2014 y el decreto autonómico nº 220/2015). En el primero de ellos, Tecnologías de la Información y la Comunicación, hay un epígrafe referido a la Seguridad Informática. Dentro de este epígrafe, según los criterios de evaluación y los estándares de aprendizaje concretos para este bloque, se especifican a continuación los contenidos específicos a tratar en este proyecto:

- Privacidad e identidad digital: en esta primera parte se explicará que es la privacidad en Internet, la responsabilidad que tiene cada usuario al respecto, como se tiene que actuar para protegerla y que mecanismos existen para ello. Se verán las distintas opciones que existen para configurar la privacidad en dos plataformas que tenemos todos (cuenta de Google o usuario de Apple), así como de la aplicación de redes sociales más popular actualmente entre adolescentes (Instagram).

Por otro lado, se expondrá el concepto de identidad digital o reputación online, y se verá su importancia y hasta donde llega, así como las implicaciones legales que tiene todo esto, tanto para menores de edad, como para personas de más de 18 años.

- Riesgos y conductas inadecuadas en el uso de las TIC e Internet: En esta segunda parte, se expondrán los distintos tipos de malware, virus y amenazas silenciosas que existen en Internet, y se verá como protegerse de ellos. Además, se abordarán los conceptos de ciberbullying, grooming y sexting, y se distinguirán los distintos tipos de ciberestafas y sus formas más habituales.
- Buenas prácticas o hábitos tecnológicos: en este último bloque temático, una vez vistos los anteriores, se consensuarán de forma reflexiva una serie de buenas prácticas o hábitos tecnológicos. Esto se hará de forma conjunta entre todo el alumnado, con la participación del docente como guía o facilitador.

### 4.3 TEMPORALIZACIÓN

Para que el desarrollo del proyecto consiga los objetivos que perseguimos, habrá que planificar previamente de forma reflexiva y pausada las fases en las que consistirá. En este apartado de temporalización se detallan cada una de estas fases, que serán las siguientes:

- Fase de inicio o preparación

CONTENIDOS	ACTIVIDAD	DURACIÓN	OBJETIVO
Planificación del proyecto y uso de la nueva metodología	Búsqueda de recursos y planificación de sesiones	240'	Correcto funcionamiento del proyecto
Resumen de los contenidos del proyecto y nociones básicas de ciberseguridad	Sesión 1: destinada al personal docente	90'	Implicar al resto del personal docente y capacitarlo. OE1, OE3
Presentación de la metodología de aula invertida o Flipped Classroom. Información sobre riesgos para los adolescentes en el uso de las TIC y nociones básicas de ciberseguridad	Sesión 2: destinada a familias	90'	Informar a las familias, concienciarlas de la importancia del proyecto y buscar su implicación. OE2, OE3

**Tabla 3. Fase de inicio en la temporalización del proyecto**

En primer lugar, se tendrá que pensar bien como aplicamos los contenidos anteriormente descritos mediante la metodología de aula invertida. Planificaremos el número de sesiones necesarias para cada apartado, y habrá que buscar o elaborar los recursos para cada uno de ellos, videos, tutoriales y lecturas sugeridas, así como elegir la plataforma donde alojarlos para que sean accesibles al alumnado, y

para que puedan trabajarlos antes de la clase presencial correspondiente.

Una vez completadas estas primeras tareas, vamos a proceder a presentar el proyecto a los demás implicados dentro de la comunidad educativa. Se planificarán dos sesiones formativas/explicativas de una hora y media (90') destinadas a:

- Resto del personal docente del centro: al tratar el proyecto una deficiencia detectada de una de las competencias transversales, como es la competencia digital, necesitaremos la implicación de los demás profesores y profesoras. En esta sesión, se procederá a realizar un resumen de los contenidos a tratar, así como unas nociones básicas de los aspectos más importantes. De este modo, se trabajará en la misma línea desde todos los ámbitos del centro.
- Familias de los alumnos y alumnas: en este caso, la orientación de la sesión será algo diferente. En ella presentaremos en primer lugar la metodología de aula invertida a las familias. Es importante este punto, ya que al salirse del modelo "clásico" de docencia puede generar rechazo. La colaboración de las familias es básica, una vez que se les presente la nueva metodología, y todos los beneficios que tiene en el proceso de enseñanza y aprendizaje de sus hijos e hijas, probablemente las posibles reticencias desaparecerán. En segundo lugar, esta sesión tratará de concienciar sobre los riesgos que existen para sus hijos e hijas en el uso de las TIC e Internet, sin alarmar ni generar miedo, pero desde un enfoque informativo, ya que en muchos casos desconocen este tipo riesgos. Después, al igual que al resto de compañeros y compañeras docentes, procederemos a presentar los contenidos más importantes que vamos a tratar, y a sugerir una serie de recursos online por si quieren profundizar en el tema. Como, por ejemplo, la web del Instituto Nacional de Ciberseguridad ([www.incibe.es](http://www.incibe.es)), u otros portales corporativos específicos de esta misma institución,

como [www.is4k.es](http://www.is4k.es) (Internet Segura For Kids) o [www.osi.es](http://www.osi.es) (Oficina de Seguridad del Internauta). Por último, se informará de que los datos que se utilicen de sus hijos e hijas tendrán una finalidad exclusivamente educativa, y se pedirá su autorización para ello.

- Fase de desarrollo o implementación

CONTENIDOS	SESIONES	DURACIÓN	OBJETIVOS
Introducción a la metodología de aula invertida	Sesión 1	50'	Que el alumnado conozca la nueva metodología
Privacidad en Internet e identidad digital	Sesión 2	50'	OE1
Riesgos 1: malware y amenazas silenciosas. Ciberestafas	Sesión 3	50'	OE2
Riesgos 2: Cyberbullying, grooming y sexting	Sesión 4	50'	OE2
Buenos hábitos tecnológicos	Sesión 5	50'	OE3

**Tabla 4. Fase de desarrollo en la temporalización del proyecto**

Esta fase será la que ocupe una mayor duración en el tiempo, en ella se desarrollarán cinco sesiones de 50 minutos en el aula, en las que se tratarán los distintos aspectos:

- Sesión 1: presentación del proyecto en el aula, como funciona el aula invertida y el aprendizaje cooperativo. Composición de

los grupos de trabajo, acondicionamiento del aula y redistribución del espacio.

- Sesión 2: en esta sesión se tratará la privacidad en Internet y la identidad digital. Una vez analizado los contenidos previos facilitados por el docente, se realizarán una serie de actividades individuales y grupales sobre configuración de privacidad de cuentas de usuario de Google, Apple e Instagram, así como el impacto real de una publicación en RRSS.
- Sesión 3: esta será la primera de las dos sesiones que destinaremos a ver los riesgos y conductas no adecuadas en el uso de las TIC e Internet. En concreto, abordaremos el tema del malware y las amenazas silenciosas, el uso de antivirus y sus tipos, así como las ciberestafas. La actividad que se realizará en clase será un juego de puntuación por grupos, tipo concurso de preguntas y respuestas, con varias posibles opciones.
- Sesión 4: en esta segunda sesión sobre los riesgos se verá otros distintos fenómenos como son el ciberbullying, grooming y sexting. Presentando a los alumnos y alumnas una serie de cuestiones previas, la parte práctica de esta sesión se enfocará a modo de debate.
- Sesión 5: en esta sesión, una vez visto todo lo anterior, así como unos nuevos recursos específicos para ella, se tratará de hacer una reflexión de grupo en la que consensuemos una serie de buenos hábitos tecnológicos relacionados con la ciberseguridad. Esta sesión será grabada, para visionarla posteriormente en el proceso de evaluación del proyecto.

- Fase de cierre o evaluación

METODO EVALUACIÓN	SESIONES	OBJETIVOS
Cuestionarios inicial y final	Sesiones 1 y 5	OE1, OE3

Registro observación	Todas	OE3
Pruebas trampa	Durante las sesiones y después	OE2
Cuestionarios globales	Sesión 6	Evaluación alumnado

**Tabla 5. Fase de evaluación en la temporalización del proyecto**

En esta última fase se analizará por un lado el resultado del proyecto, es decir, si hemos conseguido los objetivos que perseguíamos. Esto se detallará más adelante en su apartado correspondiente, pero se hará principalmente mediante estos tres métodos:

- Cuestionario inicial y otro final, para ver la evolución de sus conocimientos y percepciones.
- Registro de observación y visionado de la última sesión en clase, grabada a tal efecto.
- Envío de e-mails y solicitudes de contactos por RRSS “trampa”, para ver de manera práctica si son capaces de aplicar lo tratado en clase sobre ciberestafas, malware, grooming, etc.

Y, por otro lado, también se evaluará los conocimientos, habilidades y competencias adquiridas por el alumnado en una sexta, y última, sesión en el aula, donde se realizarán dos cuestionarios o pruebas con este propósito.

#### **4.4 ACTIVIDADES**

De manera general, tanto el alumnado como el profesorado, tienen que realizar una serie de actividades o tareas antes, durante y después de clase cuando se usa la metodología de aula invertida. A grandes rasgos, estas actividades serían las siguientes:

Antes de clase:

TAREAS DEL PROFESOR/A	TAREAS DEL ALUMNO/A
Definir el funcionamiento del aula invertida, así como los objetivos de cada aprendizaje, y que el alumnado lo entienda fácilmente.	Estar abierto a esta nueva metodología, entender su funcionamiento y como se van a llegar a los objetivos marcados.
Seleccionar, buscar y/o crear los contenidos adecuados para que los alumnos puedan trabajar en casa previamente, en función de los objetivos que perseguimos.	Trabajar los contenidos seleccionados (videos y demás recursos), investigar por su cuenta para ampliar conocimientos y tener la soltura suficiente en su manejo cuando lleguen a clase.
Desarrollar las tareas que luego se llevarán a cabo en clase, en función de los objetivos marcados al inicio.	

**Tabla 6. Tareas previas a clase en Aula Invertida o Flipped Classroom**

Durante la clase:

TAREAS DEL PROFESOR/A	TAREAS DEL ALUMNO/A
Resolver las dudas y hacer un repaso de los nuevos conceptos.	Plantear sus posibles dudas y conclusiones a las que haya llegado por sí mismos.
Guiar el proceso de aprendizaje y ver si ha habido dificultades, apoyar de forma individual si hay alguien rezagado.	Escuchar y plantear opiniones con una actitud respetuosa y reflexiva, asentando de esta manera el proceso de aprendizaje.
Plantear la parte práctica en la que se trabajarán los conceptos y competencias concretas.	Ser participativo/a y tener una actitud cooperativa con el resto de compañeros/as de clase y grupo.

**Tabla 7. Tareas durante la clase en Aula Invertida o Flipped Classroom**

Después de clase:

TAREAS DEL PROFESOR/A	TAREAS DEL ALUMNO/A
Seguir en contacto con el alumnado para resolver posibles dudas y facilitar nuevos recursos, en caso de que sea necesario.	Seguir trabajando los recursos facilitados por el profesor para afianzar los conceptos y competencias trabajadas en clase.
Corregir, evaluar y dar feedback al alumnado sobre las actividades prácticas realizadas. Analizar sus progresos de forma individualizada	Hacer un uso de la plataforma de aprendizaje no solo pasivo (leer, consultar y visionar), sino también activo, compartiendo contenido que haya obtenido investigando y que pueda ayudar a los compañeros/as.

**Tabla 8. Tareas después de clase en Aula Invertida o Flipped Classroom**

En nuestro caso particular, en la fase de desarrollo o implementación se han planificado cinco sesiones en el aula. En ellas se realizarán una serie de actividades antes, durante y después de las sesiones, que se han diseñado en función de los objetivos perseguidos en cada una de ellas. Se presenta, en primer lugar, una tabla a modo de resumen de las mismas, con los contenidos a tratar en cada una de ellas, las actividades a desarrollar cada día, duración de las sesiones y objetivos específicos de las mismas. En segundo lugar, a continuación de la tabla resumen, se puede ver de forma detallada todo lo expuesto anteriormente, así como los recursos que se podrían utilizar en cada una de las sesiones programadas.

SESIONES	CONTENIDOS	PRÁCTICA	OBJETIVO
Sesión 1 (50')	Introducción a la metodología de aula Invertida o Flipped Classroom	<ul style="list-style-type: none"> <li>- Formación de grupos</li> <li>- Redistribución de mobiliario</li> <li>- Realización de test de conocimientos previos sobre ciberseguridad</li> </ul>	Que el alumnado conozca la nueva metodología
Sesión 2 (50')	Privacidad en Internet e identidad digital	<ul style="list-style-type: none"> <li>- Individual: configurar las opciones de privacidad de una cuenta de Google o Apple, y una cuenta de Instagram</li> <li>- Grupal: elegir una publicación en RRSS y analizar su alcance. Reflexionar sobre cuestiones de privacidad e identidad digital</li> </ul>	OE1
Sesión 3 (50')	Riesgos 1: malware y amenazas silenciosas. Ciberestafas	-Grupal: juego de preguntas y respuestas sobre el malware, sus tipos y ciberestafas	OE2
Sesión 4 (50')	Riesgos 2: Cyberbullying, grooming y sexting	-Debate sobre cyberbullying, grooming y sexting, que se articula a través de una serie de cuestiones relacionadas con los temas a tratar	OE2
Sesión 5 (50')	Buenos hábitos tecnológicos	<ul style="list-style-type: none"> <li>- Asamblea de clase en la que, de forma conjunta, se reflexionará sobre el conjunto de buenos hábitos tecnológicos que se deben tener</li> <li>- Cuestionario final sobre ciberseguridad para ver el grado de concienciación alcanzado y los conocimientos adquiridos</li> </ul>	OE3

**Tabla 9. Resumen de las actividades a realizar en las sesiones de aula invertida**

- **Sesión 1:**

- Objetivo de la sesión: que el alumnado entienda la nueva forma de trabajar, los objetivos y los medios que se van a usar para conseguirlos.
- Antes de la clase: al ser la primera sesión, el alumnado no tiene que realizar ninguna tarea previa.
- Durante la clase: se realizarán las siguientes tareas que se detallan a continuación.
  - Presentar el proyecto en el aula, explicar la metodología de aula invertida y la estrategia de aprendizaje cooperativo, así como la temática a tratar y como vamos a distribuir contenidos.
  - Formación de grupos de trabajo, en los que cada uno tiene un rol y unas funciones determinadas, que tienen que quedar claras desde el primer momento.
  - Redistribución del mobiliario del aula, de manera que las mesas y las sillas se dispongan en grupos de 5-6 personas, pero dejando espacio suficiente para pasar entre ellas y que desde cualquier lugar de la clase se pueda ver la pizarra/proyección.
  - Cuestionario sobre ciberseguridad para ver los conocimientos previos del alumnado
- Después de la clase:
  - Consolidar los grupos de trabajo, establecer las normas y modos de comunicación entre sus integrantes.
  - El docente posibilitará el visionado de una serie de videos en la plataforma de aprendizaje, así como enlaces de interés para ampliar y entender mejor su funcionamiento explicado en clase.
  - Ejemplos de recursos:
    - <https://youtu.be/R16HT9oeg9I>

- <https://youtu.be/UqTF5xgQMos>
- <https://www.theflippedclassroom.es>
- <https://domingochica.com>

- **Sesión 2:**

- Objetivo de la sesión: valorar nuestra privacidad en Internet y saber como protegerla. Conocer el concepto de identidad digital y reflexionar sobre ella, así como analizar nuestro rastro en la red. (OE1).
- Antes de la clase: visionado de los siguientes videos y lectura del material adjunto sobre la privacidad, la identidad digital y sus repercusiones legales en menores:
  - ¿Por qué me vigilan, si no soy nadie?  
<https://youtu.be/NPE7i8wuupk>
  - Privacidad. IS4K  
<https://www.is4k.es/necesitas-saber/privacidad>
  - ¿Eres la misma persona en redes sociales?  
<https://youtu.be/6K0wtyDI2u4>
  - Tu identidad digital. OSI  
<https://www.osi.es/es/actualidad/blog/2011/06/21/tu-identidad-digital>
- Durante la clase:
  - Resolver dudas y repasar los aspectos principales de los contenidos facilitados por el profesor.
  - Actividad individual: buscar donde se configuran las principales cuentas de usuario que tiene la mayoría de los adolescentes (Google, Apple e Instagram). Analiza que configuración tienes, qué se guarda sobre ti, qué se puede ver y quien lo puede ver.  
Por ejemplo, para una cuenta de Google (myactivity.google.com):
    - Gestionar mi cuenta de Google

- Datos y personalización
- Actividad (Webs, apps y búsquedas) y Cronología (ubicaciones)

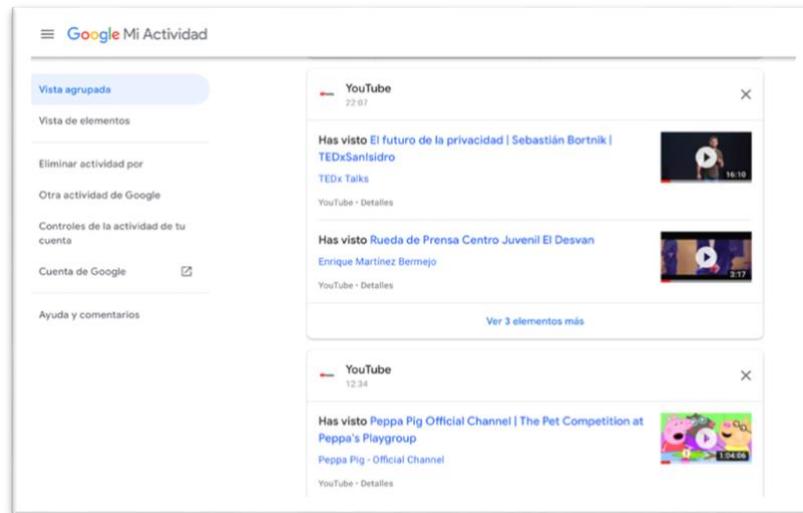


Figura 3. Ejemplo de registro de actividad de cuenta de Google

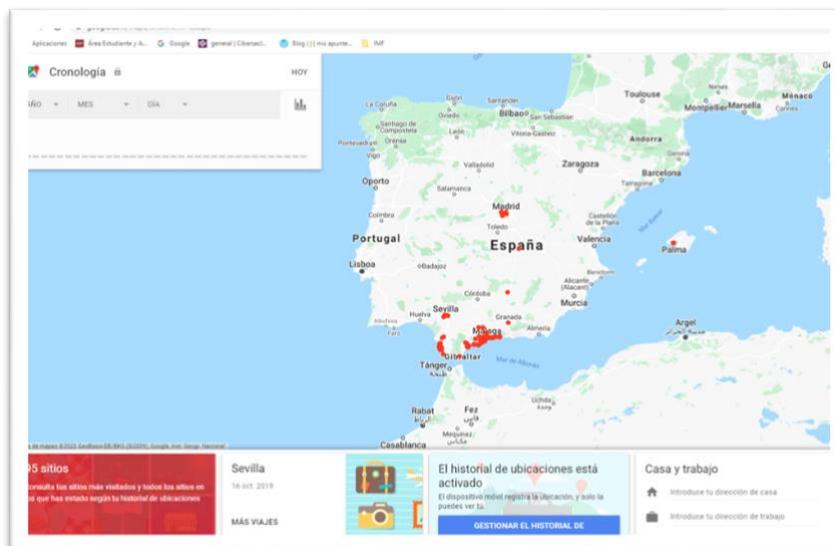


Figura 4. Ejemplo de registro cronológico de ubicaciones de cuenta de Google

- Actividad grupal: se elige una publicación de RRSS de cualquiera de los miembros del grupo, en función de los contactos que tiene y la configuración de privacidad, analicemos cuanta gente puede llegar a verla, ¿son muchas personas? ¿lo habías pensado alguna vez?

Reflexionar y discutir sobre las siguientes cuestiones con los compañeros del grupo:

- Privacidad: ¿Pondrías una foto tuya en la puerta del instituto? ¿Qué tipo de foto? ¿Y una disfrazado?
- Identidad digital: ¿Qué es para tí la identidad digital? ¿Coincide siempre con la identidad real? ¿Por qué? ¿Qué herramienta tenemos disponible para configurar alertas que nos avisan si alguno de los datos personales que indiques aparecen en Internet?

Analizar si se tienen buenos hábitos de privacidad, en caso contrario, ¿en qué aspectos se podría mejorar?

- Después de la clase: revisar lo visto en clase y, a través de la plataforma de aprendizaje, visualizar y leer los siguientes recursos. Plantear las posibles dudas que surjan a través de la plataforma. Si han encontrado algo, compartir contenido que pueda ayudar a los compañeros.

- El futuro de la privacidad:  
<https://youtu.be/TjsCyfkKPk0>
- Ojo con tus datos (hasta el minuto 14:10):  
<https://www.rtve.es/alcanta/videos/documentos-tv/documentos-tv-ojo-tus-datos/2270048/>
- Reputación online:  
<https://www.osi.es/es/actualidad/blog/2013/08/09/tu-reputacion-online-es-muy-importante-cuidala>
- Los menores y las redes sociales (Legalitas):  
<https://www.legalitas.com/abogados-para-particulares/actualidad/articulos-juridicos/contenidos/Los-menores-y-las-redes-sociales>

- **Sesión 3:**

- Objetivo de la sesión: conocer los riesgos a los que los usuarios se exponen cuando hacen uso de las TIC y RRSS. (OE2).
  
- Antes de la clase: el alumnado tendrá que trabajar el siguiente material, hacer anotaciones de lo que consideren más importante y, si lo desean, investigar por su cuenta desde fuentes fiables.
  - ¿Qué es el malware?  
<https://youtu.be/Md9ergKwZ3Y>
  - Tipos de malware  
<https://youtu.be/A6FAgk2QDiM>
  - Malware, tipos y como evitarlo  
<https://www.xataka.com/basics/malware-que-que-tipos-hay-como-evitarlos>
  - Ciberestafas:  
<https://youtu.be/cp8uFVnJ16c>  
<https://youtu.be/Jr5rMLXzxt4>
  - Ciberdelincuentes, ¿quiénes son?  
<https://www.osi.es/es/campanas/los-ciberdelincuentes-quiénes-son>
  
- Durante la clase:
  - Resolver dudas y revisar los conceptos más importantes de esta sesión.
  - Actividad grupal: se realizará un concurso de preguntas y respuestas por equipos. En la pizarra digital o proyector se visualizarán las preguntas y las posibles opciones de repuesta, en las que deberán:
    - Diferenciar tipos de malware.
    - Elegir entre varias opciones para evitarlo.
    - Viendo casos de e-mails reales, diferenciar si son estafas o peticiones normales.

- Después de la clase: revisar lo visto en clase, usar la plataforma para dudas y compartir contenido con los compañeros. Analizar el siguiente contenido:
  - Fraudes online dirigidos a menores:
    - <https://www.is4k.es/fraudes-online>
  - Seguridad en Internet: menores y “malware”:
    - [https://www.consumoresponde.es/art%C3%ADculos/seguridad\\_en\\_internet\\_menores\\_y\\_malware](https://www.consumoresponde.es/art%C3%ADculos/seguridad_en_internet_menores_y_malware)
  
- **Sesión 4:**
  - Objetivo de la sesión: conocer los riesgos a los que los usuarios se exponen cuando hacen uso de las TIC y RRSS, en concreto el ciberbullying, grooming y sexting. (OE2).
  
  - Antes de la clase: el alumnado deberá trabajar los siguientes materiales, anotar sus reflexiones personales y los sentimientos que han experimentado al ver las situaciones de los videos.
    - Ciberbullying
      - <https://www.is4k.es/necesitas-saber/ciberacoso-escolar>
      - <https://youtu.be/mDF0KQ1Gags>
      - [https://youtu.be/KI\\_Vh30-E6g](https://youtu.be/KI_Vh30-E6g)
    - Grooming
      - <https://www.is4k.es/necesitas-saber/grooming>
      - <https://youtu.be/UPVU0XK6zq0>
    - Sexting
      - <https://www.is4k.es/necesitas-saber/sexting>
      - <https://youtu.be/qKs7qnHvY2U>
  
  - Durante la clase: una vez trabajado el material facilitado por el profesor, procederemos a:
    - Resolver dudas y se abre un turno de palabra en el que cada uno podrá expresar, si lo desea, sus reflexiones personales y sentimientos experimentados al ver los videos.

- Actividad grupal: debate sobre ciberbullying, grooming y sexting. Se articulará respecto a las siguientes cuestiones, que se comentarán primero por grupos, y luego se debatirá con el resto de la clase.

¿Has sufrido bullying o ciberbullying? ¿Lo has presenciado? ¿Cómo reaccionaste y cómo te gustaría haber reaccionado?

¿Has quedado con desconocidos con los que has contacto por Internet o RRSS? ¿Conoces a alguien que lo haga? ¿Qué opinas sobre esto? ¿Lo ves peligroso?

Si tienes pareja ¿le has dado tu contraseña del móvil o RRSS? ¿Te parece normal hacerlo? ¿Te pide que le envíes fotos o videos? Si no te apetece ¿qué le contestas?

- Después de la clase: releer lo trabajado en clase, plantear posibles dudas o reflexiones en la plataforma y compartir contenido con los compañeros y compañeras si se considera oportuno. Visualizar los siguientes videos:
  - Educación en la era del 'sexting' y 'ciberbullying':  
<https://youtu.be/Jjf7oUUDqNw>
  - Peligros en RRSS para niños, niñas y adolescentes:  
<https://youtu.be/G8iciqvXnmk>

#### - **Sesión 5:**

- Objetivo de la sesión: fomentar buenos hábitos tecnológicos para salvaguardar nuestras relaciones personales en el mundo real, nuestra salud mental y nuestra intimidad, evitando en la medida de lo posible los riesgos expuestos en sesiones anteriores. (OE3).

- Antes de la clase: leer el siguiente material en la plataforma y sacar las ideas que se consideren más importantes:
  - <https://www.is4k.es/jovenes>
  - [https://www.elconfidencial.com/tecnologia/2017-01-01/profesor-silicon-valley-adictos-movil-instagram-facebook\\_1310897/](https://www.elconfidencial.com/tecnologia/2017-01-01/profesor-silicon-valley-adictos-movil-instagram-facebook_1310897/)
  - [https://www.elconfidencial.com/alma-corazon-vida/2016-12-05/adiccion-movil-silicon-valley\\_1290118/](https://www.elconfidencial.com/alma-corazon-vida/2016-12-05/adiccion-movil-silicon-valley_1290118/)
  
- Durante la clase: en esta última sesión, la dinámica será un poco diferente, se realizarán las siguientes tareas:
  - Se plantearán y resolverán las posibles dudas surgidas en el estudio del material previo.
  - Se llevará a cabo una asamblea de clase en la que se intentará, mediante una reflexión grupal de todos los conceptos expuestos anteriormente, recopilar el conjunto más importante de buenas prácticas en el uso de la TIC y RRSS para salvaguardar nuestra intimidad y evitar las conductas de riesgo.
  - Cuestionario final sobre ciberseguridad para ver los conocimientos adquiridos durante este proceso y el grado de concienciación alcanzado.
  
- Después de la clase: después de esta última sesión, los alumnos y alumnas podrán revisar o volver a leer cualquiera de los recursos que tienen disponibles en la plataforma, plantear nuevas dudas, terminar las tareas que tengan pendientes y hacer las últimas aportaciones para el resto de compañeros y compañeras.

## 4.5 RECURSOS

Para el desarrollo de la metodología de aula invertida o Flipped Classroom será imprescindible el uso de diversos recursos TIC, que detallamos a continuación:

- Plataforma de aprendizaje:

Será básico este recurso porque nos ayudará a compartir los contenidos que el alumnado tiene que consultar antes y después de clase. Además, a través de ella se podrán plantear las dudas, el alumnado puede compartir otros contenidos o experiencias que puedan servir a los compañeros y compañeras y, también, nos facilita un canal de comunicación permanente entre profesor y alumnado. En nuestro caso, se ha elegido Google Classroom, que es una aplicación gratuita del paquete educativo de Google. En ella, además de todo lo anterior, se podrán subir las actividades realizadas por los alumnos y alumnas para ser evaluadas por el profesor, y nos permite realizar test/exámenes online, si lo deseamos, así como publicar las calificaciones de cada una de las pruebas. Se puede acceder desde el siguiente enlace (con un correo de dominio @ucam):

<https://classroom.google.com/c/Mjl1NDE4NDMzMzE1?cjc=hocabbi>

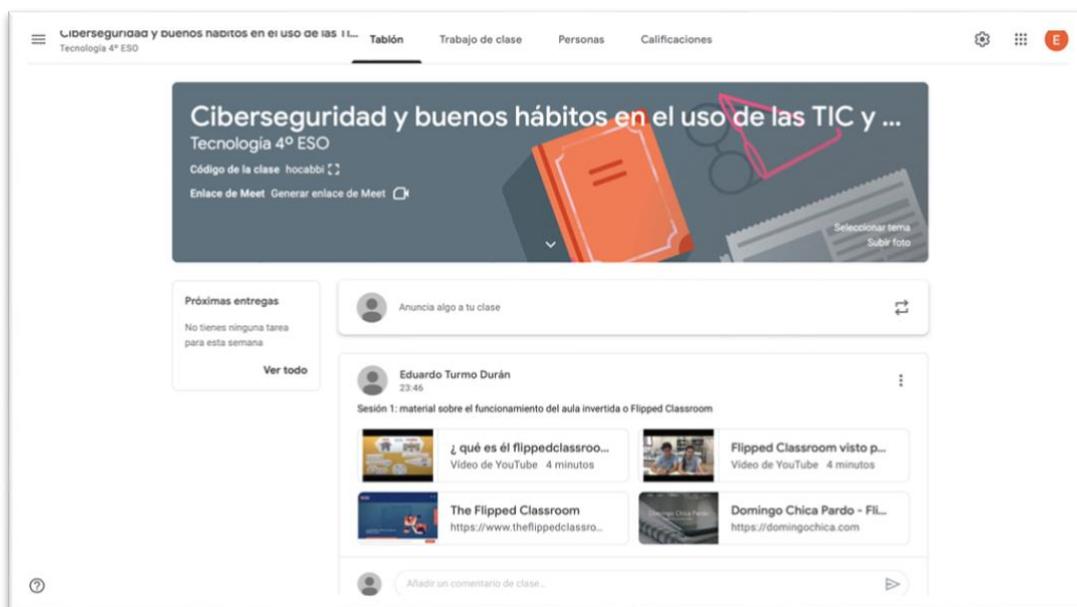


Figura 5. Plataforma de aprendizaje: Google Classroom

- Aplicaciones para generar contenidos:

En el caso de que se necesiten crear contenidos, existen numerosas aplicaciones, tanto gratuitas, como de pago, que se podrán usar dependiendo de lo que se desee elaborar:

- Tutorial en texto: Word, Documentos de Google, Pages (Apple) o cualquier otro editor de texto.
- Presentación: Power Point (Windows), Keynote (Apple) o Presentaciones de Google son las más utilizadas.
- Encuestas o exámenes: Formularios de Google nos sirve para esta función, y da los resultados de forma automática.
- Subir videos a Internet: las plataformas de video más populares, y que además tienen más contenidos y usuarios actualmente son Youtube o Vimeo.
- Edición de video: para este propósito hay multitud de aplicaciones disponibles, las más usuales pueden ser Movie Maker (Windows), iMovie (Apple), Adobe Premiere o VideoPad, por ejemplo.
- Mapas conceptuales: para la elaboración de este recurso se puede usar CmapTools o Canva.

- Pizarra digital o proyector en clase:

Esto no es un requisito imprescindible para llevar a cabo el proyecto, pero si que facilitará mucho el desarrollo de las clases, porque podremos visionar videos con ejemplos, casos reales o experimentos sociales relacionados con el tema que se esté tratando. Hoy en día, en casi todos los centros tienen, como mínimo, un aula acondicionada con este tipo de tecnología.

- Conexión a Internet y dispositivo electrónico, como puede ser un ordenador, tablet o smartphone:

Estos recursos serán necesarios tanto para el profesorado, como para el alumnado, pero no debería ser un problema, ya que actualmente prácticamente todo el mundo dispone de ellos. De todas formas, si no fuera así, el aula de informática de los centros educativos está disponible para que el alumnado que no dispone de ordenador o conexión a Internet en casa puedan hacer uso de ella.

## 5. EVALUACIÓN

Este apartado consta de dos propósitos principales, en primer lugar, averiguar si se ha conseguido el objetivo principal del proyecto, y esto se hará evaluando a su vez la consecución de los objetivos secundarios, que nos llevarán a lograr el principal. Y, en segundo lugar, se pretende evaluar al alumnado, para ver si han alcanzado los conocimientos, habilidades o competencias necesarias.

El encargado de esta evaluación será el profesor de Tecnología que desarrollará el proyecto y estará en contacto directo con el alumnado en todo momento.

Se partía de una deficiencia detectada en la competencia digital del alumnado. La mayoría no eran conscientes de practicar conductas de riesgo o poco seguras en el uso de las TIC y RRSS. Además, no valoran debidamente su privacidad en Internet y no son conscientes de lo que significa su identidad digital. Por este motivo, se propuso tratar de concienciar sobre los riesgos existentes, así como fomentar unos buenos hábitos en el uso de la tecnología. Para ello, se recuerdan a continuación cuales eran los objetivos secundarios del proyecto:

- Valorar nuestra privacidad y saber que es la identidad digital. Solo de este modo se puede interaccionar con otros de forma adecuada a través del mundo virtual de Internet. Esto se conseguirá mediante actividades en las que el alumnado analizará publicaciones propias en RRSS y sus configuraciones de privacidad. (OE1).
- Conocer los riesgos a los que se expone el usuario cuando hace uso de las TIC en general, y las RRSS en particular (adicción a la tecnología, ciberestafas, grooming, sexting o ciberacoso), mediante el visionado de videos con experimentos o experiencias reales y el posterior debate en clase. (OE2).
- Fomentar buenos hábitos tecnológicos para salvaguardar nuestras relaciones personales en el mundo real, nuestra salud mental y

nuestra intimidad, mediante una reflexión grupal de todos los conceptos expuestos anteriormente. (OE3).

De esta forma, para valorar la consecución o no de estos objetivos planteados en primera instancia, realizaremos una evaluación formativa que constará de 3 fases, al inicio del proyecto, durante el proyecto y al final del mismo. Para ello se utilizarán estos 3 métodos:

- Cuestionario inicial y cuestionario final: con esto podremos comprobar el nivel de conocimientos y concienciación del alumnado antes de comenzar, y al finalizar el proceso, se podrá comprobar la evolución de sus conocimientos y percepciones realizando un cuestionario final. Estos cuestionarios se pueden ver en el apartado de Anexos o en los siguientes enlaces de Googles Forms:
  - o Cuestionario inicial (Anexo 1):  
<https://forms.gle/RiCaiqazz2EidAXj8>
  - o Cuestionario final (Anexo 2)  
<https://forms.gle/br633YLKNJohUx4e9>

En el Anexo 3 se puede observar también una Rúbrica para la evaluación de este proyecto basado en aula invertida.

- Registro de observación: mediante esta herramienta iremos anotando de forma sistemática, por ejemplo, las actitudes, comportamientos, comentarios y dudas que el alumnado irá teniendo, de esta forma, se puede averiguar si están alcanzando o no las competencias y conocimientos necesarios. Además, se realizará el visionado de la última sesión en clase, que será grabada con este objetivo. En esta sesión la actividad principal es una asamblea de clase, en la que se tratará de consensuar entre todos una serie de medidas o buenos hábitos en el uso de las TIC y RRSS. Por tanto, esta grabación también será muy útil a la hora de evaluar los progresos del alumnado en la materia.

- Envío de correos electrónicos y solicitud de contacto por RRSS “trampa”: este último punto puede considerarse una práctica innovadora, ya que durante el transcurso de las cinco sesiones que dura el proyecto para el alumnado, y después de éstas, se les enviará una serie de correos electrónicos simulando ofertas o grandes descuentos, solicitud para el restablecimiento de su contraseña de Instagram o solicitudes ficticias para contactar por RRSS. De esta manera, se podrá comprobar de forma práctica si son capaces de darse cuenta de que dichas solicitudes podrían ser ciberestafas, así como prácticas de phishing o de grooming.

Para terminar, la evaluación del alumnado se llevará a cabo en una sexta y última sesión en el aula, en la que tendrán que completar dos cuestionarios de Googles Forms de 25 minutos cada uno:

- Cuestionario o prueba de conocimientos: en éste se evaluará los conocimientos, competencias y habilidades adquiridas de forma individual. Tendrá una estructura muy parecida a la parte práctica de la sesión 3, serán preguntas con varias opciones de respuesta sobre todo lo abordado, con los conceptos básicos, con ejemplos y situaciones que podrían ser reales.
- Cuestionario de coevaluación: como la mayoría de las actividades se realizarán en grupo, de este modo los alumnos y alumnas evaluarán el desempeño, colaboración e implicación de sus propios compañeros.

Con estos dos cuestionarios, junto con la entrega de las distintas prácticas a través de la plataforma y el trabajo realizado día a día en clase, el profesor podrá evaluar de manera global a cada uno de los alumnos y alumnas.

## 6. REFLEXIÓN Y VALORACIÓN FINAL

Para terminar, en este apartado se van a exponer una reflexión y valoración final, así como las conclusiones más importantes que se pueden sacar una vez desarrollado este proyecto.

- Aspectos clave del proyecto:

Como punto fuerte del proyecto destacaríamos que la temática de Internet, RRSS, móviles y demás aspectos tecnológicos tiene muy buena aceptación entre los adolescentes. Son cuestiones que les motivan, usan a diario y sobre las que suelen investigar por si mismos.

Por otro lado, puede ser una circunstancia que sirva para ampliar conocimientos y competencias, no solo por parte del alumnado, sino también para los adultos. Habrá padres, madres y resto del profesorado que tampoco sean conscientes de los riesgos que corren, no solo sus hijos e hijas, sino ellos mismos en el uso diario de las TIC. De manera que también puede ser una gran oportunidad para aprender juntos, padres, madres, hijos e hijas, como proteger nuestra privacidad en Internet, evitar los posibles riesgos y tener hábitos adecuados con el uso de la tecnología.

- Viabilidad:

Para sacar adelante este proyecto solo hará falta proponérselo, ya que los recursos necesarios para ello están disponibles en casi todos los centros en los que se quiera implementar. Si, además, contamos con la participación e implicación del resto de la comunidad educativa, seguramente será un éxito.

También puede ser extrapolable a otras asignaturas posteriores como TIC I y TIC II en Bachillerato, en las que la edad del alumnado es superior y se podría profundizar en ciertos temas o darles otro enfoque.

- Utilidad:  
Como se ha comentado anteriormente, la utilidad y necesidad que tienen propuestas de este tipo considero que son bastante importantes. Porque es una cuestión que nos afecta a todos hoy en día, cuanto antes tengan los alumnos y alumnas unas nociones básicas de ciberseguridad, mejor será tanto para el desarrollo de la competencia digital, como para su propio desarrollo personal. Pudiendo prevenir muchas situaciones desagradables que podrían ocurrir en caso contrario, así como prevenir futuros problemas de adicciones a la tecnología.
  
- Innovación:  
Los dos aspectos innovadores de este TFM considero que son, por un lado, la utilización de la metodología de aula invertida o Flipped Classroom para conseguir un aprendizaje significativo adaptado al ritmo de cada alumno o alumna. Y, por otro lado, en el apartado de evaluación, el envío de correos electrónicos y solicitudes de contacto a través de RRSS ficticios o “trampa”. Esto es un método de evaluación que ellos no esperan, y que les hará poner en práctica las competencias que deben de haber adquirido durante el desarrollo del proyecto, y si no las tienen todavía, ellos mismos se darán cuenta sin necesidad de sufrir las consecuencias reales.
  
- Desarrollo futuro:  
Esta propuesta es susceptible de ser ampliada en el futuro, o en otras asignaturas, en muchos aspectos. Se podría alargar en el tiempo la formación al profesorado y familias, si se ve que tienen buena acogida, para lograr una mayor implicación y mejorar sus conocimientos sobre ciberseguridad. También se podría aumentar el número de sesiones con el alumnado, para tratar más aspectos relacionados con la ciberseguridad o entrar más en detalle en los que se proponen en este proyecto.

Pero, en general, considero que se han tratado los temas o aspectos más importantes referentes a la ciberseguridad, privacidad en Internet, identidad digital, riesgos y fomento de buenos hábitos tecnológicos, en un periodo de tiempo razonable, y con una serie de actividades que se adaptan a la edad del alumnado a las que van dirigidas.

## 7. REFERENCIAS BIBLIOGRÁFICAS

### BIBLIOGRAFÍA:

- Argente, E., Vivancos, E., Alemany, J., & García-Fornes, A. (2017). Educando en privacidad en el uso de las redes sociales. *Education in the knowledge society*, 18(2), 107-126.
- Berenguer-Albaladejo, C. (2016). Acerca de la utilidad del aula invertida o flipped classroom.
- Bergmann, J., & Sams, A. (2014). Dale la vuelta a tu clase. *Madrid: Ediciones SM*.
- Dominguez, A. H. (2019). Sistema para la detección de ataques PHISHING utilizando correo electrónico. *Telemática*, 17(2), 60-70.
- Gairín Sallán, J., & Mercader, C. (2018). Usos y abusos de las TIC en los adolescentes.
- Gomez, R. G., Llorente, P. A., Morales, M. T. V., & Hernández, I. L. (2020). Seguridad y protección digital de la infancia: retos de la escuela del siglo XXI. *Educar*, 56(1), 219-237.
- González Fernández, N. & Carrillo Jácome, G.A. (2016). El Aprendizaje Cooperativo y la Flipped Classroom: una pareja ideal mediada por las TIC. *Aularia: Revista Digital de Comunicación*, vol. 5 (número 2), pp. 43-48.
- Guàrdia Ortiz, L., & Sangrà Morer, A. (2005). Diseño instruccional y objetos de aprendizaje; hacia un modelo para el diseño de actividades de evaluación del aprendizaje online.
- Hernández Prados, M., & Solano Fernández, I. M. (2007). Cyberbullying, un problema de acoso escolar. *Revista Iberoamericana de Educación a distancia*.

- Johnson, D. W., Johnson, R. T., & Holubec, E. J. (1999). El aprendizaje cooperativo en el aula.
- Juan, I. M., Vayá, E. J. C., & García, M. S. (2014). Victimización infantil sexual online: online grooming, ciberabuso y ciberacoso sexual. *Delitos sexuales contra menores: abordaje psicológico, jurídico y policial*, 203-224.
- Lucena, F. J. H., Díaz, I. A., Rodríguez, J. M. R., & Marín, J. A. M. (2019). Influencia del aula invertida en el rendimiento académico. Una revisión sistemática. *Campus Virtuales*, 8(1), 9-18.
- Lucero, M. M. (2003). Entre el trabajo colaborativo y el aprendizaje colaborativo. *Revista iberoamericana de Educación*, 33(1), 1-21.
- Montañés, M. C. (2017). Prevención de las adicciones tecnológicas en la adolescencia. *Padres y Maestros/Journal of Parents and Teachers*, (369), 53-59.
- Pérez, P., Flores, J., de la Fuente, S., Álvarez, E., García, L., y Gutiérrez, C. (2011) Guía sobre adolescencia y sexting: qué es y cómo prevenirlo. Observatorio de la Seguridad de la Información de INTECO y PantallasAmigas.
- Prats, M. À., Torres-Rodríguez, A., Oberst, U., & Carbonell, X. (2018). Diseño y aplicación de talleres educativos para el uso saludable de internet y redes sociales en la adolescencia: descripción de un estudio piloto. *Píxel-Bit. Revista de Medios y Educación*, (52), 111-124.
- Vanderhoven, E., Schellens, T., & Valcke, M. (2014). Enseñar a los adolescentes los riesgos de las redes sociales: una propuesta de intervención en Secundaria. *Comunicar: Revista científica iberoamericana de comunicación y educación*, (43), 123-132.

Villalba de Benito, M. T., Castilla Cebrian, G., Martínez Requejo, S., Jiménez García, E., Hartyányi, M., Sedivine, B., ... & Tauchmanova, V. (2018). Innovación en la educación profesional. Flipped classroom en la práctica.

#### **WEBGRAFÍA:**

Instituto Nacional de Ciberseguridad. Ministerio de Asuntos Económicos y Transformación Digital. [www.incibe.es](http://www.incibe.es)

Internet Segura For Kids (Portal INCIBE). Ministerio de Asuntos Económicos y Transformación Digital. [www.is4k.es](http://www.is4k.es)

Oficina de Seguridad del Internauta (Portal INCIBE). Ministerio de Asuntos Económicos y Transformación Digital. [www.osi.es](http://www.osi.es)

## 8. ANEXOS

### ANEXO 1: CUESTIONARIO INICIAL (EVALUACIÓN)



#### Cuestionario inicial: Ciberseguridad

Cuestionario sobre ciberseguridad y hábitos de uso de las TIC entre adolescentes

1. ¿Qué edad tienes?

- 12 años
- 13 años
- 14 años
- 15 años
- 16 años
- 17 años

2. ¿Cuál es tu sexo?

- Mujer
- Hombre
- Prefiero no decirlo

3. ¿A qué edad tuviste tu primer móvil (smartphone)?

- A los 12 años o antes
- A los 13 años
- A los 14 años
- A los 15 años o después

4. ¿Cuántas cuentas de correo electrónico tienes?

- Ninguna
- 1
- 2
- 3
- Más de 3

5. ¿Cuántas aplicaciones tienes instaladas en tu móvil?

- Menos de 10
- Entre 10 y 20
- Entre 21 y 30
- Más de 30

6. ¿Cuántos perfiles tienes en redes sociales? Marca los que corresponda

- Instagram
- Tik Tok
- Twitter
- Snapchat
- Twitch
- Facebook
- Otro: \_\_\_\_\_

7. ¿Qué importancia tiene para ti publicar regularmente imágenes o videos (tuyos o de amigos/as) en redes sociales?

- 1      2      3      4      5
- Poco importante                        Muy importante

8. ¿Te has arrepentido alguna vez de algo que has publicado en redes sociales o se ha enfadado contigo algún amigo/a por este motivo?

- No
- Me ha pasado alguna vez
- Me pasa con frecuencia

9. ¿Has contactado con alguien desconocido a través de redes sociales, o conoces a algún amigo/a que lo haya hecho?

- Una vez lo hice (o conozco alguien que lo hizo)
- Lo hago habitualmente (o conozco a alguien que lo hace)
- Nunca

10. Si al salir de casa te das cuenta de que te has olvidado el móvil, ¿te vuelves a por él?

- Siempre
- Si, pero solo si espero una llamada de mis padres o algún amigo/a
- No, si voy a volver pronto
- Nunca

11. Si estás fuera de casa, tu móvil tiene poca batería y no tienes como cargarlo, ¿cómo te sientes?

- Liberado/a, así no tengo que estar pendiente de quien me escribe o me llama
- Me da igual, ya lo cargaré cuando llegue
- Preocupado hasta que no encuentre un enchufe/cargador
- Pensando en volver a casa lo antes posible
- Otro: \_\_\_\_\_

12. Si lo deseases ¿podrías borrar de internet de forma definitiva cualquier imagen o video de ti mismo?

- Si, por supuesto
- Si, pero solo si lo he subido yo mismo
- No se puede

13. ¿Sabes lo que es la identidad digital?

- Es la información que internet muestra sobre nosotros, y que voluntariamente hemos subido nosotros mismos
- Es la información sobre nosotros que hay disponible en internet, subida por nosotros mismos o nuestro círculo de confianza
- Es la información sobre nosotros que hay en internet, subida por nosotros mismos, familiares, amigos o cualquier otra persona/entidad

14. ¿Sabes lo que es el RGPD?

- Es la Regla General Para Derechos fundamentales, es una normativa a nivel mundial
- Es el Reglamento General de Protección de Datos, es una norma a nivel europeo
- Es la Regulación Genérica de Protección de Digital, es una norma a nivel estatal

15. ¿Te has descargado alguna vez aplicaciones de tiendas no oficiales (fuera de Google Play y App Store)?

- Si
- No

16. Aunque la aplicación esté en tiendas oficiales (Google Play y App Store), ¿has verificado alguna vez su fiabilidad, por ejemplo, haciendo una búsqueda en Google?

- Si
- No

17. ¿Lees los términos y condiciones al bajarte una aplicación?

- Siempre
- A veces
- Una vez lo intenté
- Nunca

18. ¿Cuántas contraseñas tienes para tus aplicaciones, cuentas de correo electrónico y redes sociales?

- Una para todo
- Varias contraseñas diferentes que voy combinando
- Una diferente para cada cosa

19. Si el sistema te lo permitiese, ¿usarías contraseñas simples en lugar de una segura (longitud determinada, mayúsculas, minúsculas y/o caracteres especiales)?

- Sí
- A veces
- No

20. ¿Qué opinión tienes sobre los sistemas de verificación en 2 pasos para acceder a algunas cuentas de correo electrónico o aplicaciones?

- Es necesario y positivo para nuestra seguridad
- Es un poco rollo, porque se tarda mucho en entrar
- Si de mi dependiera, lo eliminaría
- No sé lo que es

21. ¿Has revisado o modificado alguna vez las condiciones de privacidad de tus aplicaciones o cuentas de correo?

- Nunca
- Una vez lo hice
- Cada vez que me descargo una app

22. ¿Tienes instalado algún antivirus en el móvil?

- Sí
- No

23. ¿Actualizas regularmente el sistema operativo y aplicaciones del móvil?

- Sí, cada vez que sale una actualización
- Sí, de vez en cuando
- Nunca

24. ¿Usas el modo de navegación oculto en internet?

- Siempre
- A veces, depende del servicio de internet
- Nunca

Enviar

## ANEXO 2: CUESTIONARIO FINAL (EVALUACIÓN)



### Cuestionario final: Ciberseguridad

Cuestionario sobre ciberseguridad y hábitos de uso de las TIC entre adolescentes

1. ¿Qué edad tienes?

- 12 años
- 14 años
- 15 años
- 16 años
- 17 años

2. ¿Cuál es tu sexo?

- Mujer
- Hombre
- Prefiero no decirlo

3. ¿A qué edad tuviste tu primer móvil (smartphone)?

- A los 12 años o antes
- A los 13 años
- A los 14 años
- A los 15 años o después

4. ¿Cuántas cuentas de correo electrónico tienes?

- Ninguna
- 1
- 2
- 3
- Más de 3

5. ¿Cuántas aplicaciones tienes instaladas en tu móvil?

- Menos de 10
- Entre 10 y 20
- Entre 21 y 30
- Más de 30

6. ¿Cuántos perfiles tienes en redes sociales? Marca los que corresponda

- Instagram
- Tik Tok
- Twitter
- Snapchapp
- Twitch
- Facebook
- Otro: \_\_\_\_\_

7. ¿Qué importancia tiene para ti publicar regularmente imágenes o videos (tuyos o de amigos/as) en redes sociales?

- 1      2      3      4      5
- Poco importante                        Muy importante

8. Desde que empezamos a tratar este tema en clase ¿te has arrepentido de alguna publicación en redes sociales o se ha enfadado contigo algún amigo/a por este motivo?

- No
- Me ha pasado alguna vez
- Me pasa con frecuencia

9. A partir de ahora ¿cómo de probable es que contactes con alguien desconocido a través de redes sociales?

- 1      2      3      4      5
- Nada probable                        Muy probable

10. Si al salir de casa te das cuenta de que te has olvidado el móvil, ¿te vuelves a por él?

- Siempre
- Si, pero solo si espero una llamada de mis padres o algún amigo/a
- No, si voy a volver pronto
- Nunca

11. Si estás fuera de casa, tu móvil tiene poca batería y no tienes como cargarlo, ¿cómo te sientes?

- Liberado/a, así no tengo que estar pendiente de quien me escribe o me llama
- Me da igual, ya lo cargaré cuando llegue
- Preocupado hasta que no encuentre un enchufe/cargador
- Pensando en volver a casa lo antes posible
- Otro: \_\_\_\_\_

12. Si lo desearas ¿podrías borrar de internet de forma definitiva cualquier imagen o video de ti mismo?

- Si, por supuesto
- Si, pero solo si lo he subido yo mismo
- No se puede

13. ¿Sabes lo que es la identidad digital?

- Es la información que internet muestra sobre nosotros, y que voluntariamente hemos subido nosotros mismos
- Es la información sobre nosotros que hay disponible en internet, subida por nosotros mismos o nuestro círculo de confianza
- Es la información sobre nosotros que hay en internet, subida por nosotros mismos, familiares, amigos o cualquier otra persona/entidad

14. ¿Sabes lo que es el RGPD?

- Es la Regla General Para Derechos fundamentales, es una normativa a nivel mundial
- Es el Reglamento General de Protección de Datos, es una norma a nivel europeo
- Es la Regulación Genérica de Protección de Digital, es una norma a nivel estatal

15. A partir de ahora ¿cómo de probable es que te descargues alguna aplicación de tiendas no oficiales (fuera de Google Play y App Store)?

- 1      2      3      4      5
- Nada probable                        Muy probable

16. Aunque una aplicación esté en tiendas oficiales (Google Play y App Store), ¿cómo de probable es que compruebes a partir de ahora su fiabilidad, por ejemplo, haciendo una búsqueda en Google?

- 1      2      3      4      5
- Nada probable                        Muy probable

17. A partir de ahora ¿leerás los términos y condiciones al bajarte una aplicación?

- Siempre
- A veces
- Nunca

18. A partir de ahora ¿cómo de probable es que cuando te bajes una nueva aplicación le pongas una contraseña que ya usas en otra?

- 1      2      3      4      5
- Nada probable                        Muy probable

19. Después de lo visto en clase, si el sistema te lo permitiese, ¿usarías contraseñas simples en lugar de una segura (longitud determinada, mayúsculas, minúsculas y/o caracteres especiales)?

- Sí
- A veces
- No

20. ¿Qué opinión tienes ahora sobre los sistemas de verificación en 2 pasos para acceder a algunas cuentas de correo electrónico o aplicaciones?

- Es necesario y positivo para nuestra seguridad
- Es un poco rollo, porque se tarda mucho en entrar
- Si de mí dependiera, lo eliminaría
- No sé lo que es

21. A partir de ahora ¿cómo de probable es que revises o modifiques alguna vez las condiciones de privacidad de tus aplicaciones o cuentas de correo?

- 1      2      3      4      5
- Nada probable                        Muy probable

22. ¿Tienes instalado algún antivirus en el móvil?

- Sí
- No

23. A partir de ahora ¿actualizarás regularmente el sistema operativo y aplicaciones del móvil?

- Sí, cada vez que sale una actualización
- Sí, de vez en cuando
- Nunca

24. ¿Cómo de probable es que uses el modo de navegación oculto en internet a partir de ahora?

- 1      2      3      4      5
- Nada probable                        Muy probable

Enviar

ANEXO 3: RÚBRICA PARA LA EVALUACIÓN DEL PROYECTO BASADO EN AULA INVERTIDA

A EVALUAR	EXCELENTE	BIEN	CORRECTO	INSUFICIENTE
<p><b>CONTENIDOS</b></p> <p>Privacidad, riesgos de las TICs y buenos hábitos tecnológicos</p>	<p>Comprendo los conceptos trabajados y soy consciente de su importancia. Soy capaz de solucionar las prácticas.</p>	<p>Comprendo los conceptos trabajados, pero no soy consciente de su importancia. Soy capaz de solucionar las prácticas.</p>	<p>Comprendo los conceptos trabajados, pero soy consciente de su importancia. No soy capaz de solucionar las prácticas de forma autónoma.</p>	<p>No comprendo los conceptos trabajados, no soy consciente de su importancia. No soy capaz de solucionar las prácticas.</p>
<p><b>PRÁCTICAS</b></p>	<p>He resuelto las prácticas fácilmente y me ayudaron a reforzar los aspectos más importantes.</p>	<p>He resuelto las prácticas sin dificultad.</p>	<p>Las prácticas tenían una alta dificultad.</p>	<p>Las prácticas eran poco interesantes e inapropiadas.</p>
<p><b>USO DE LAS TICs</b></p> <p>Plataforma de aprendizaje</p>	<p>Navego sin problemas por la plataforma, descargo de el material, planteo dudas y comparto información con mis compañeros y compañeras fácilmente.</p>	<p>Navego sin problemas por la plataforma y descargo de el material, pero a veces me cuesta plantear dudas y compartir información con mis compañeros y compañeras.</p>	<p>Navego sin problemas por la plataforma y descargo de el material. Pero tengo dificultad para compartir contenido o participar en ella.</p>	<p>Me cuesta navegar por la plataforma, descargar material y compartir contenido en ella.</p>
<p><b>OPINIÓN DEL ALUMNADO</b></p>	<p>Esta metodología me resultado motivadora y me he sentido participe del proceso de aprendizaje.</p>	<p>Esta metodología me ha gustado y me gustaría que se usara más.</p>	<p>Esta metodología me ha parecido positiva en algunos aspectos, en otros no.</p>	<p>No me ha gustado nada esta metodología, prefiero el método de siempre.</p>

# ANEXO 4: MAPA CONCEPTUAL TFM

