



Programa de Jornadas Escolares

Promoción del uso seguro y responsable de
Internet entre los menores

Privacidad, identidad digital y reputación

Unidad Didáctica y contenidos de apoyo al docente

Licencia de contenidos



La presente publicación pertenece a **INCIBE (Instituto Nacional de Ciberseguridad)** y está bajo una licencia **Reconocimiento-No Comercial-Compartir Igual 4.0 Internacional de Creative Commons**. Por esta razón está permitido copiar, distribuir y comunicar públicamente esta obra bajo las condiciones siguientes:

- **Reconocimiento.** El contenido de esta publicación se puede reproducir total o parcialmente por terceros, citando su procedencia y haciendo referencia expresa tanto a **INCIBE** y la iniciativa **Internet Segura for Kids (IS4K)** como a sus sitios web: <https://www.incibe.es> y <https://www.is4k.es>. Dicho reconocimiento no podrá en ningún caso sugerir que INCIBE presta apoyo a dicho tercero o apoya el uso que hace de su obra.
- **Uso No Comercial.** El material original y los trabajos derivados pueden ser distribuidos, copiados y exhibidos mientras su uso no tenga fines comerciales.
- **Compartir Igual.** Si altera o transforma esta obra, o genera una obra derivada, sólo puede distribuirla bajo esta misma licencia.

Al reutilizar o distribuir la obra, tiene que dejar bien claro los términos de la licencia de esta obra. Alguna de estas condiciones puede no aplicarse si se obtiene el permiso de INCIBE como titular de los derechos de autor.

Texto completo de la licencia: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.es> ES

La presente publicación sólo refleja las opiniones del autor. La Comisión Europea no es responsable de ningún uso que pudiera hacerse de la información que contiene.

CONTENIDO

1. Presentación de la Unidad Didáctica.....	4
2. Ficha descriptiva.....	4
3. Temporalización y secuenciación.....	6
4. Orientaciones didácticas	6
4.1. Metodología	6
4.2. Recursos	7
4.3. Descripción de las actividades a abordar.....	7
4.3.1. Actividad 01: Introducción a la privacidad, identidad y reputación	7
4.3.2. Actividad 02: Gran Hermano	9
4.3.3. Actividad 03. Riesgos vinculados a la construcción de identidad digital negativa.....	11
4.3.4. Actividad 04. “Egosurfing”	12
4.3.5. Actividad 05. “Construyendo mi identidad digital positiva”	13
4.3.6. Actividad 06. “Autoevaluación”	13
4.4. Criterios de evaluación.....	14
5. Marco teórico de apoyo al docente	15
6. Bibliografía / Documentación complementaria	18
7. Anexo1. Test de autoevaluación	20
8. Anexo 2. Respuestas al Test de autoevaluación	21
9. Anexo 3. Recursos asociados	22

1. Presentación de la Unidad Didáctica

Por lo general es difícil para muchos pre-adolescentes pensar en términos de futuro cuando se trata de acciones que quieren tomar hoy. El planteamiento de esta Unidad Didáctica parte de la necesidad de ser conscientes de preservar su privacidad en la red y conocer los beneficios y los riesgos asociados a la identidad digital, para evitar, entre otros aspectos, que nadie les suplante (usurpación de la identidad digital) y construir una identidad digital que no les perjudique ahora o en el futuro.

Los contenidos de esta temática y su metodología asociada deben enfocarse a que el alumnado aprenda a respetar su privacidad y la de los demás. Se focalizará la atención en el rastro que cada uno de nosotros va dejando en la red, se mostrará mediante ejemplos prácticos cómo nuestras publicaciones, o publicaciones de otras personas referidas a nosotros, forman parte de la construcción de nuestra identidad digital y se ofrecerán pautas para una correcta configuración de la privacidad de los servicios interactivos que utilizamos, así como, de su revisión y actualización constante.

2. Ficha descriptiva

Destinatarios		Alumnado de 6º de Primaria y ESO.
Duración		2 sesiones de 50 minutos.
Objetivos didácticos	General	Conocer los conceptos de privacidad, identidad digital y reputación y sus implicaciones para la vida personal y profesional presente y futura.
	Específicos	• Entender el concepto de privacidad. • Entender el concepto de identidad digital y de reputación online. • Comprender los principales riesgos vinculados a una gestión no adecuada de la privacidad. • Tomar conciencia sobre la importancia de la identidad digital, tanto en la actualidad como y de cara al futuro. • Aprender a gestionar nuestra identidad digital de forma positiva.
Contenidos de aprendizaje		• Conceptos de privacidad e imágenes y privacidad de terceros. • Conceptos de identidad digital y reputación digital. • Factores determinantes de la reputación digital. • Importancia y consecuencias positivas y negativas de la información que se comparte en la Red. • Riesgos vinculados a la identidad y la reputación digital. • Identidad digital positiva.

Áreas competenciales	Digitales*	Área Comunicación (nº 2): Comunicarse en entornos digitales, compartir recursos por medio de herramientas en red, conectar con otros y colaborar mediante herramientas digitales, interaccionar y participar en comunidades y redes, concienciación intercultural. Y en concreto con la competencia: • Gestión de la identidad digital (nº 2.6): Crear, adaptar y gestionar una o varias identidades digitales, ser capaz de proteger la propia reputación digital y de gestionar los datos generados a través de las diversas cuentas y aplicaciones utilizadas. Área Seguridad (nº 4): Protección de información y datos personales, protección de la identidad digital, medidas de seguridad, uso responsable y seguro. Y en concreto con la competencia: • Protección de datos personales (nº 4.2). Entender los términos habituales de uso de los programas y servicios digitales, proteger activamente los datos personales, respetar la privacidad de los demás, protegerse a sí mismo de amenazas, fraudes y ciberacoso. <i>*Referencia «Marco Común de la Competencia Digital Docente» INTEF (Instituto de Tecnologías Educativas y de Formación del Profesorado) (2013)</i>
	Clave	• Competencias en comunicación Lingüística (CCL): el alumnado aprenderá a utilizar adecuadamente vocabulario relacionado con la temática (privacidad; identidad digital, reputación online). • Aprender a aprender (CPAA): el alumnado adquirirá habilidades para que, de manera autónoma, sea capaz de identificar los riesgos de seguridad vinculados con la privacidad en nuevos servicios y para comenzar a construir de forma positiva su identidad digital como elemento motivador para preservar y seguir desarrollando una buena gestión de la privacidad y de su reputación online. • Sociales y cívicas (SCS): el alumnado aprenderá a comunicarse de una manera constructiva y segura en el entorno digital comprendiendo códigos de conducta en este ámbito y su repercusión positiva y/o negativa tanto para él como para terceros.

3. Temporalización y secuenciación

Sesión	Contenido / actividad	Duración	Metodología
Sesión 01	Actividad 01 (Introducción a privacidad, identidad y reputación)	25 min.	Expositiva e interrogativa
	Actividad 02 (Vídeo sobre privacidad)	25 min.	Vídeo y Debate
Sesión 02	Actividad 03 (Riesgos vinculados a la identidad y reputación digital)	10 min.	Expositiva e interrogativa
	Actividad 04 (Búsqueda en Internet)	20 min.	Ejercicio práctico individual
	Actividad 05 (Identidad Digital positiva)	10 min.	Expositiva e interrogativa
	Actividad 06 (Autoevaluación)	10 min.	Autoevaluación individual

4. Orientaciones didácticas

4.1. Metodología

En esta Unidad Didáctica el formador realizará las exposiciones combinando el método **expositivo**¹ y el **interrogativo**². El método expositivo centrado en la transmisión de información, facilita ésta de forma rápida y generalizada. El método interrogativo se centrará más en la aplicación práctica del contenido a trabajar, basado en el proceso de comunicación que se establece entre docente y el alumnado, a través de preguntas que motiven a la participación y la reflexión y/o a orientar al profesor en el conocimiento de partida del alumnado sobre la materia a tratar.

Actuará también como facilitador de una sesión participativa utilizando el **debate**³ y la visualización de los vídeos con objeto de animar a compartir información, ideas, inquietudes, dudas, buscando en todo momento promover un entorno que favorezca la motivación del alumnado.

¹ **METODOLOGÍA EXPOSITIVA:** centrada en la transmisión de información, posibilita la transmisión de conocimientos ya estructurados, facilitando demostraciones de tipo verbal y la transmisión de información y conocimiento, de manera rápida y generalizada.

² **METODOLOGÍA INTERROGATIVA:** centrada en el proceso de aplicación del contenido a trabajar, basada en el proceso de comunicación que se establece entre docente y grupo, a través de **la pregunta**. Esta se convierte en elemento dinamizador, que desencadena el proceso de enseñanza aprendizaje.

³ **EL DEBATE EN EL AULA:** nos permite estimular el análisis y el cambio de actitudes por medio de la presentación de distintos puntos de vista

Esta metodología promoverá la construcción del conocimiento a partir de la permanente reflexión del alumnado, siempre orientada por aquél, asesorando y facilitando recursos e información y procurando poner ejemplos vinculados a la realidad objetiva del perfil del alumnado destinatario. El formador utilizará un lenguaje acorde con el nivel de conocimientos previstos en el alumnado destinatario, con objeto de un entendimiento claro de las actividades propuestas, contribuyendo a su buen desarrollo.

La actividad 05 previa a la autoevaluación, se programa con el objeto de desarrollar en el alumnado la capacidad de toma de decisiones partiendo de los conocimientos adquiridos en torno a su privacidad.

4.2. Recursos

Recursos requeridos para el desarrollo de la Unidad Didáctica:

- Recursos logísticos:
 - Ordenador con conexión a Internet para el docente, conectado a un proyector VGA o pizarra electrónica.
 - Pizarra o papelógrafo.
 - Ordenadores con conexión para actividades del alumnado (al menos 1 ordenador por cada 2 alumnos) capacitados para la emisión de vídeo y altavoces (tipo auricular/cascos, para la escucha individual).
- Recursos didácticos:
 - Presentación de contenidos dirigida a los menores, que acompaña a la presente Unidad Didáctica.
 - Sitios web, imágenes y vídeos. Referidos en el apartado 6. Bibliografía /Documentación complementaria.

4.3. Descripción de las actividades a abordar

4.3.1. Actividad 01: Introducción a la privacidad, identidad y reputación

Descripción	Se plantea una exposición inicial sobre los conceptos de: • Privacidad e imágenes, privacidad de terceros. • Identidad y reputación digital y factores determinantes. • Identidad digital frente a identidad personal.
Metodología	Expositiva e interrogativa.
Duración	25 minutos.
Recomendaciones	Para ello se puede recurrir a un interrogatorio dirigido , mediante el que se puede realizar una evaluación inicial y comprobar el nivel de conocimientos previo del alumnado, detectar concepciones equivocadas, lagunas de conocimiento, etc. Asimismo, el desarrollo del interrogatorio puede

permitirnos hacer que sean los propios alumnos/as quienes pasen a definir dichos conceptos, aclarar sus dudas en común, ponerse ejemplos reales, etc. Se plantean algunos ejemplos:

- **¿Pondrías una foto tuya a la puerta del instituto?, ¿qué foto pondrías?, ¿y una disfrazado?**

El concepto de privacidad es subjetivo, cada persona debe encontrar un equilibrio entre los beneficios de exponerse públicamente y los riesgos de tal exposición. Lo importante es que la gente tome la decisión de manera informada, siendo consciente de los riesgos que asume al publicarla. Por el mismo motivo, hay que ser respetuoso con las fotos de terceros (una foto en una fiesta puede que a alguien le parezca estupenda para que la vea cualquiera, pero otra persona puede considerarla privada y no querer que se muestre).

- **¿Qué os parecería conseguir el teléfono de una popular presentadora de televisión?, ¿sabéis que publicó su número en Twitter?, ¿os imagináis lo que pasó?**

3689 llamadas, 1623 sms, 258 mensajes de voz, 6384 mensajes de WhatsApp... Conviene pensarse dos veces si lo que vamos a compartir es lo que de verdad queremos, si damos información de más (como en este caso), si nos puede hacer daño a futuro (o a otras personas).

- **¿Os acordáis del futbolista fichado y despedido por el Barça en unas horas?, ¿recordáis el caso?, ¿por qué pasó todo?**

Según lo que publicamos y lo que publican los demás, la gente con la que nos relacionamos, lo que nos “gusta”, etc. creamos (consciente o inconscientemente) una imagen de nosotros en Internet (identidad digital) que provoca en los demás una valoración (reputación digital). No se trata de que sea mejor o peor, sino de que seamos conscientes de que todo lo que hacemos en Internet (o dicen de nosotros) contribuye a nuestra imagen y reputación.

- **¿Conocéis a alguien que haya tenido algún enfado con sus amigos por algo que ha dicho en el WhatsApp, o publicado en Facebook?**

Cuando nos comunicamos por Internet perdemos contacto con la otra persona por lo que es muy fácil que haya malentendidos y enfados. Por eso, es importante no reaccionar exageradamente y tratar de ponerse en la piel de la otra persona. Recordar, lo que decimos en Internet marca nuestra imagen y nos puede pasar factura si llega a nuestros padres, a nuestra pareja, a nuestros futuros empleadores, etc.

Complementariamente se puede realizar una **exposición** de carácter sensibilizador apoyándose en la presentación de la charla dirigida al alumnado sobre “Privacidad, identidad digital y reputación”. En este caso, se recomienda seguir las pautas indicadas en la guía para el docente asociada a dicha presentación.

4.3.2. Actividad 02: Gran Hermano

Descripción	Debate sobre privacidad: Visualización de vídeos que muestren diferentes situaciones de pérdida de privacidad con el objetivo de motivar hacia el debate, la reflexión y llegar a conclusiones.
Metodología	Vídeo y Debate.
Duración	25 minutos.
Recomendaciones	Los vídeos propuestos permiten trabajar la privacidad desde diferentes puntos de vista y son perfectamente adecuados para los niveles educativos propuestos. • <u>Tu vida entera está en Internet... y pueden usarla contra ti</u> Este vídeo forma parte de una campaña publicitaria con el objetivo de llamar la atención del peligro que conlleva compartir la vida privada en Internet. Se invitó a participar a personas anónimas que paseaban por la calle, Dave, un supuesto adivino con dotes paranormales iba a hablarles sobre su vida. En realidad se trataba de un actor que a través de un minúsculo micrófono en su oído recibía información de un grupo de hackers que buscaban información sobre la vida de los visitantes a través de lo que ellos mismos habían publicado en sus redes sociales. ○ ¿Cuál fue el precio de su casa? ○ ¿Cuánto dinero hay en su cuenta bancaria? ○ ¿Cuánto gastó en ropa y en bebida el mes pasado? ○ ¿Cuál es el número de su tarjeta bancaria? Son algunas de las preguntas que el adivino Dave sabe responder de las personas que tiene delante. <u>Pregunta de reflexión:</u> ¿Qué información se podría descubrir sobre nosotros en función de la información que publicamos en nuestras redes sociales? • <u>Privacidad de la Información (permisos aplicaciones móviles).</u> Para utilizar algunas de las aplicaciones más populares en nuestro móvil cedemos excesivos permisos sobre nuestra información personal: ○ Acceso a tu localización exacta. ○ Enviar mensajes y/o realizar llamadas sin la mediación del usuario. ○ Cambiar nuestras contraseñas. ○ Leer nuestro registro de llamadas. ○ Historial de navegación. ○ Acceder a nuestras fotos y archivos multimedia.

Pregunta de reflexión: ¿Sabemos qué permisos hemos cedido por utilizar las aplicaciones que tenemos descargadas en nuestro Smartphone? ¿Cuál es nuestra opinión sobre el acceso por parte de terceros a nuestros datos?

En sistemas Android accediendo a Ajustes > Aplicaciones podemos comprobar los permisos a los que puede acceder cada aplicación que tenemos descargada.

Los usuarios de iPhone pueden bloquear el acceso de las aplicaciones a sus fotos, contactos o funciones del GPS accediendo a Ajustes > Privacidad.

- Si todo estaba perfecto... ¿Qué falló?

Vídeo desarrollado por chicos y chicas de 12 a 18 años en el marco de un concurso “Tecnología Sí. Conéctate con responsabilidad” que tiene por objetivo premiar cortos que aborden aspectos relacionados con el uso seguro de la tecnología.

Este vídeo en concreto aborda la importancia de la entrevista de trabajo y como la imprudencia, la ignorancia sobre privacidad, identidad digital y reputación online y la falta de conocimiento a la hora de utilizar la tecnología puede perjudicarnos seriamente ante la posibilidad de obtener un empleo.

***Observaciones:** el sonido de este vídeo no es óptimo pero el hecho de que tanto su guionaje como realización esté elaborado por menores y dirigido precisamente a menores hace que consideremos relevante incluirlo. Es un ejemplo de cómo los propios menores pueden participar de manera activa en el desarrollo de materiales dirigidos a ellos mismos, observando cómo son capaces de dar consejos certeros cuando se les pide reflexión y análisis, utilizando su propio lenguaje, de forma que los resultados pueden llegar a ser mejor acogidos por sus iguales.

La función del docente será la de moderador y dinamizador favoreciendo la interacción entre el alumnado. Se puede orientar hacia la reflexión de otro tipo de situaciones más próximas a la realidad del alumnado, por ejemplo, en lugar de una entrevista de trabajo la misma situación puede darse para entrar en un equipo de fútbol, baloncesto para entrar en un coro o en cualquier otro tipo de asociación que realice una mínima selección de sus miembros e incluso a la hora de ligar o buscar pareja.

La proyección de cualquiera de los vídeos incluidos ha de servir para motivar al alumnado para iniciar un debate en torno a la importancia la identidad digital y el cuidado de la privacidad.

Se proponen algunos ítems para favorecer la reflexión y debate:

- ¿Qué les sucede a los protagonistas de los vídeos?
- ¿Cuáles creéis que son los motivos?
- ¿Crees que esta situación podría afectar a alguien que conocéis? ¿por

	qué? • ¿Qué aconsejaríais cambiar al personaje del vídeo sobre cómo construye su identidad digital? El alumnado debe llegar a un consenso en torno a la importancia de cuidar la identidad digital, y de la utilización adecuada de la tecnología. Se deberá llegar a un consenso en la elección de al menos 4 recomendaciones para evitar la pérdida de privacidad y una mala construcción de nuestra identidad digital. El profesorado deberá reconducir las conclusiones en caso de que no se ajusten al objetivo buscado. Las recomendaciones buscadas deben estar en relación con aspectos como: • Leer las condiciones y políticas de privacidad antes de aceptar crear un perfil al abrir una cuenta en una red social. • Configurar adecuadamente las opciones de privacidad al crear el perfil. • Revisar periódicamente las opciones de privacidad de nuestro perfil. • Controlar lo que se publica.
--	--

4.3.3. Actividad 03. Riesgos vinculados a la construcción de identidad digital negativa

Descripción	Se plantea una exposición sobre los riesgos vinculados a una construcción negativa de la identidad digital: • Amenazas a la privacidad. • Usurpación de identidad. • Amenazas a la reputación online.
Metodología	Expositiva e interrogativa.
Duración	10 minutos.
Recomendaciones	Tomar como punto de partida las conclusiones obtenidas del debate anterior. El alumnado ya está en disposición de aportar algunos de los riesgos que se solicitan. El profesorado reconducirá las exposiciones aclarando dudas y complementando la información de al menos los 3 aspectos destacados como riesgos vinculados a una construcción negativa de la identidad digital. En este caso se planearán ejemplos de casos reales: • La última estafa tecnológica: los falsos mensajes de WhatsApp Falsos correos electrónicos generalmente con un mensaje de vos o vídeo adjunto aparentemente enviados en nombre de WhatsApp y que incluyen un troyano de alto riesgo. • Dos detenidos por acceder a redes wifi de otras personas y amenazar e insultar a sus contactos

	Nuestra privacidad puede verse afectada de muchas maneras, por ejemplo, si alguien consigue hackear nuestra wifi como en el ejemplo de la noticia, cuanto más si utilizamos wifis públicas abiertas, es decir sin contraseña, en estos casos toda la información que transmitimos puede ser interceptada por cualquiera, por este motivo, nunca se debe transmitir información privada a través de redes que no son de nuestra confianza. • <u>"Detenida una joven de 18 años por usurpar el perfil de otra persona en una red social"</u> Usurpación de identidad. • <u>"Despedida de su empresa por un comentario racista en Twitter"</u> Amenazas a la reputación online. El caso de <i>Justine Sacco</i> es un ejemplo real de las consecuencias profesionales que puede conllevar un mal uso de las redes sociales. Apenas tenía seguidores pero una broma racista la convirtió en tendencia mundial. Su fulminante despido fue aplaudido en las redes.
--	--

4.3.4. Actividad 04. "Egosurfing"

Descripción	Ejercicio práctico individual: Investigar sobre lo que Internet sabe sobre nosotros mismos.
Metodología	Ejercicio práctico individual.
Duración	20 minutos.
Recomendaciones	El alumnado realizará una búsqueda en Internet poniendo su nombre y apellidos incluso ciudad en el buscador. Por ejemplo, incluir en el buscador de Google "nombre y apellidos" and "ciudad" and "Nombre del colegio"; o bien incluir en el buscador: site: webredsocia "nombre y apellidos". Encontraremos nuestros perfiles en redes sociales, imágenes, etc. De esta forma el alumnado puede ser consciente de la información publicada sobre él mismo en Internet y obtener una imagen de su reputación online. El profesorado debe orientar al alumnado en que observe como parte de los resultados obtenidos son debidos a lo que nosotros mismo publicamos sobre nosotros. En algunos casos se podrá observar también comentarios de otras personas sobre nosotros, bien amigos y/o conocidos o incluso otro tipo de entidades como un periódico cuando nos hizo por ejemplo una entrevista en la fiesta del colegio. El profesorado también debe orientar al alumnado en la necesidad de que periódicamente realice esta práctica para tener un poco más controlada nuestra identidad digital. Esta actividad debe realizarse de forma individual.

4.3.5. Actividad 05. “Construyendo mi identidad digital positiva”

Descripción	Elaborar una breve estrategia personalizada con el objetivo de mejorar la construcción de su identidad digital.
Metodología	Expositiva e interrogativa.
Duración	10 minutos.
Recomendaciones	Después de haber realizado la actividad anterior, el alumnado estará en disposición de elaborar una breve estrategia encaminada a mejorar la construcción de su identidad digital o sencillamente mantener una buena identidad digital. Esta actividad se realizará en pequeños grupos y posteriormente se pondrán en común las 4 o 5 estrategias elaboradas con la totalidad de la clase. Esta actividad servirá de repaso de todo lo aprendido puesto que el alumnado deberá reflexionar sobre todo lo visto a lo largo de las dos sesiones de trabajo. Una estrategia para una construcción positiva de la identidad digital debería abordar aspectos como: • Configurar las opciones de privacidad de mis redes sociales. • Revisar periódicamente las opciones de privacidad de mis redes sociales. • Utilizar contraseñas seguras y no compartirlas. • Utilizar un patrón de desbloqueo en mi móvil. • Valorar cuando tener activado servicios como la geolocalización. • Revisar los permisos que solicitan las aplicaciones que instalo en mi Smartphone. • Cuidar especialmente mi privacidad, no ofreciendo excesivos datos personales. • Hacer trimestralmente una búsqueda con mi nombre y apellidos en Internet (egosurfing) y además activar alertas de Google con mi “nombre.apellidos”. • Tener presente: “pensar antes de publicar”. • Utilizar un lenguaje correcto.

4.3.6. Actividad 06. “Autoevaluación”

Descripción	Test de autoevaluación individual.
Metodología	Autoevaluación individual.
Duración	10 minutos.

Recomendaciones	Se elaborará un test de autoevaluación sencillo (de uso individual), que evalúe los criterios marcados en el siguiente epígrafe (Criterios de evaluación), facilitando la verificación de que el alumnado ha entendido y asimilado conceptos y buenas prácticas relacionados con cada uno de los contenidos trabajados.
------------------------	---

4.4. Criterios de evaluación

Se ha elaborado un [Test de Autoevaluación](#) relacionado con las competencias alineadas con la UD tomando como referencia el [Marco Común de Competencia Digital Docente](#)⁴.

En el [Anexo 2](#) se dispone de las respuestas correctas.

El test de autoevaluación se ha elaborado con el objetivo de que el alumnado compruebe los conocimientos adquiridos sobre privacidad, identidad y reputación online como actividad final.

Se sugiere al docente que el test de autoevaluación también puede ser utilizado al inicio y al final. Al inicio como actividad nº 0, con objeto de que el alumnado sea consciente de los conocimientos que tiene sobre la temática y al final estableciendo una comparativa y observando los avances obtenidos tras la realización de todas las actividades.

También podemos pedir a los alumnos que aporte alguna pregunta que podríamos incluir en el test, desafiar a sus compañeros siempre es un reto atractivo para el alumnado, de esta manera fomentaremos su curiosidad y espíritu competitivo en beneficio del aprendizaje.

La resolución del test de forma grupal preguntando a los alumnos los motivos de escoger cada respuesta nos puede facilitar hacer más atractiva la actividad.

La evaluación atenderá al interés y participación del alumnado en las actividades planteadas.

⁴ [Marco Común de Competencia Digital Docente V 2.0](#)

5. Marco teórico de apoyo al docente

La **Privacidad** se puede definir como el ámbito de la vida personal que se tiene derecho a proteger de cualquier intromisión. La privacidad nos proporciona seguridad, nos resguarda de la mirada de los otros. La privacidad es necesaria, las personas tenemos diferentes facetas y en cada una de ellas nuestra privacidad es diferente, es decir no nos comportamos de la misma manera con nuestros amigos, que con nuestros profesores, nuestros padres o nuestra pareja. Nosotros elegimos el grado de privacidad de cada una de nuestras relaciones y gracias a esto podemos tener relaciones sociales enriquecedoras y variadas que nos permiten desarrollarnos como personas. La privacidad también tiene que ver con aquello que se comparte solo con uno mismo.

La privacidad nos da seguridad, nos permite tener parcelas de intimidad para hacer cosas que no haríamos en público, estar relajados, no tener que cuidar nuestra apariencia.

En definitiva, nuestra información privada dicen mucho sobre nosotros o sobre nuestra familia, entorno, etc. En función de la cantidad de datos que facilitemos expondremos en mayor o menor medida nuestra vida privada, que puede ser utilizada para fines que nos pueden perjudicar.

Un exceso de información sobre nosotros nos hace más vulnerables.

De la misma manera que debemos ser cuidadosos con la gestión de nuestra privacidad, deberemos serlo con la privacidad de los demás.

La información que hace referencia a nuestros gustos, aficiones, creencias, etc. también forma parte de nuestra privacidad. Al igual que nuestros datos personales como la dirección donde vivimos, el número de móvil, dirección de correo electrónico, nuestra imagen (vídeos, fotos), incluso nuestra voz son datos personales. También, son datos personales los relacionados con la salud -enfermedades, pruebas médicas o tratamientos-, los datos bancarios como el número de cuenta o de tarjeta, los datos asociados a nuestra vida laboral como por ejemplo el salario, los datos biométricos son las huellas dactilares, etc.

Los datos personales están protegidos ⁵por la (LOPD) Ley Orgánica de Protección de datos y eso quiere decir que nadie puede hacer un uso fraudulento de ellos. Pero somos nosotros los que debemos protegerlos.

Las personas utilizamos diferentes identidades parciales en función de las diferentes actividades que desarrollamos online. Cada identidad parcial está sustentada por un servicio o aplicación de Internet. Por ejemplo, podemos tener nuestro perfil en Facebook, Twitter, subir fotos a Instagram, crear vídeos en YouTube, participar en diferentes foros o blog del colegio... En cada uno de estos servicios vamos creando una identidad digital y parcial de nosotros, que pueden estar o no relacionadas con el resto.

Cuando navegamos por Internet, realizamos búsquedas, etc. también vamos dejando rastro aunque no dejemos aparentemente nuestros datos en ningún formulario es lo que se llama huella digital.

La suma de todas estas identidades parciales permite construir una identidad digital y una imagen de la persona en Internet.

⁵ El 28 de enero se celebra el Día de la protección de datos con el objetivo de concienciar sobre la importancia de la privacidad y la protección de datos personales. Puede ser oportuno vincular la realización de esta Unidad Didáctica en el marco de esta celebración.

En base a esta información, proyectamos una imagen que es como nos ven los demás. Y esta imagen que puede resultar positiva o negativa, es lo que llamamos reputación online.

El concepto de identidad y reputación se debe abordar desde la toma de conciencia de que estar en el ciberespacio significa una identidad virtual para poder interactuar. Al mismo tiempo la construcción de la identidad digital conlleva una responsabilidad que se debe asumir como una competencia más de la sociedad actual.

Debemos centrar la atención en el rastro que cada uno de nosotros va dejando en Internet sobre su propia vida y en los comentarios que realizamos sobre los demás. Entender, tanto nuestras propias publicaciones como las publicaciones ajenas referidas a nosotros, como parte de la construcción de nuestra identidad digital.

Características de la identidad digital/reputación online

La propiedad de la Identidad: En la vida fuera de Internet es la persona adulta la que controla su Identidad: si quiere modificar su apariencia, cambiar de amigos, tener una vida social activa o, por el contrario, permanecer en un área privada.

En la red parte de esos rasgos que nos diferencian como personas pasan a estar gestionados por compañías privadas. En este detalle reside la importancia de leer detenidamente las condiciones de uso, ya que podemos estar cediendo el control de más datos de los que deseamos.

La perdurabilidad: Mientras que en la vida diaria una persona puede con mayor o menor facilidad poner fin o modificar alguno de los rasgos diferenciadores que conforman su identidad, en Internet borrar el rastro que van dejando nuestras decisiones no es siempre tan fácil.

El acceso: En la vida off-line cuando por ejemplo conocemos a una persona procuramos dar nuestra mejor imagen, si acudimos a una entrevista de trabajo, para entrar en una universidad o para pertenecer a una asociación que nos pueda interesar, somos conscientes de que la persona que tenemos en frente se está formando una impresión de nosotros, tanto por nuestra imagen, como por lo que decimos. Por el contrario en Internet, nosotros no sabemos cuándo alguien nos puede buscar para saber más de nosotros.

Junto al riesgo de configurar una reputación negativa existen otros riesgos vinculados a una mala gestión de la privacidad. La principal es que nos hace más vulnerables a otros riesgos como el ciberacoso, los fraudes.... A continuación se apuntan algunos:

- Mal uso que puedan hacer otras personas con el exceso de información que publicamos sobre nosotros mismos o sobre otras personas.
- Suplantación de nuestra identidad. Si una persona obtiene muchos datos personales nuestros puede hacerse pasar por nosotros o incluso abrir un perfil en una red social con nuestros datos o cometer fraudes con nuestros datos.
- Una de las modalidades de ciberacoso más utilizadas es el ataque a nuestra reputación online, por ejemplo con difusión de fotos/grabaciones que dañan la imagen de la persona.
- Uso comercial de nuestra información personal por parte de empresas, servicios y/o aplicaciones.

Por estos motivos se hace necesario realizar esfuerzos encaminados a entender la importancia de preservar la privacidad y construir una identidad digital positiva. Con este objetivo se exponen a continuación una serie de recomendaciones que deberíamos intentar convertir en hábitos:

1. **Utilizar contraseñas seguras y no compartirlas.** La contraseña es personal e intransferible, es decir no debemos decírsela a nadie. Una contraseña segura no debe contener ninguna

información relacionada con nosotros, no debe contener nuestro nombre, ni nuestra edad, año de nacimiento, nombre de nuestro perro...), debe tener un mínimo de 8 caracteres incluyendo mayúsculas, minúsculas, dígitos y caracteres especiales. Es muy importante igualmente que utilicemos diferentes contraseñas para los diversos servicios y/o aplicaciones de los que somos usuarios.

2. **Utilizar patrones de seguridad.** Es increíble la cantidad de datos que llevamos en nuestro smartphone (datos/imágenes personales, datos que afectan a nuestra privacidad, incluso datos que pueden afectar a la privacidad de terceros).
3. **Revisar los permisos que solicitan las aplicaciones que se instalan en el smartphone:** poner en una balanza el servicio que nos da esa aplicación y los permisos que cedemos.
4. **Informarse sobre las condiciones y políticas de privacidad antes de aceptar crear un perfil al abrir una cuenta en una red social.** Tomarse el tiempo necesario para comprender los términos, la información que comparten y como protegen nuestra privacidad frente a terceros.
5. **Configurar adecuadamente las opciones de privacidad al crear el perfil.** Ante cualquier duda, las principales redes sociales tienen **centros de seguridad** donde poder encontrar información para resolver dudas.
6. **Revisar periódicamente las opciones de privacidad de nuestro perfil.** Las redes sociales cambian sus parámetros de privacidad o su política de privacidad y no siempre avisan por lo que podemos pensar que tenemos bien configurada las opciones de privacidad y no ser así, es una buena práctica revisar cada cierto tiempo las opciones de privacidad de nuestras redes sociales.
7. **Conectarse a páginas seguras para transacciones importantes o informaciones sensibles.** Son aquellas que empiezan por https. Todos los bancos tienen este protocolo pero ahora también algunas redes sociales lo tienen, al activar el cifrado toda la información que enviemos será encriptada y en caso de ser interceptada no será legible. Es muy útil cuando nos conectamos desde fuera de casa.
8. **Valorar cuando tener activado servicios como la geolocalización.** Ya que estaríamos transmitiendo nuestra ubicación e incluso hábitos de desplazamiento. Además los Smartphone y la mayoría de las cámaras digitales actuales registran la posición GPS del lugar donde se toma una determinada foto y esa información se añade a los metadatos de la misma, quedando accesible a cualquiera a quien hagamos llegar la foto. La mejor solución pasa por deshabilitar en general la conexión GPS cuando no se esté utilizando
9. **No publicar excesiva información personal. Y tener presente: “pensar antes de publicar”.** No por aparecer esta recomendación la última es la menos importante, todo lo contrario, subir una fotografía comprometida o realizar un comentario polémico tal vez pueda pasar desapercibido en el presente, pero puede pasarnos factura en el futuro. Es necesario que pensemos siempre en las consecuencias que puede suponer tanto para nuestra reputación online como para la de los demás.

6. Bibliografía / Documentación complementaria

- [Adivino Dave. Vídeo sobre privacidad en redes sociales.](#)
- [Si todo estaba perfecto... ¿qué falló? Vídeo sobre reputación online.](#)
- [Privacidad de la información. Vídeo sobre permisos y aplicaciones móviles.](#)
- [Identidad digital, privacidad y reputación. Vídeo Voluntad Digital.](#)
- [Artículo “En Internet cuida tu privacidad”. OSI Oficina de Seguridad del Internauta.](#)
- [Artículo “Tu identidad digital”. OSI Oficina de Seguridad del Internauta.](#)
- [Artículo “Tu reputación online es muy importante ¡Cuidala!”. OSI Oficina de Seguridad del Internauta.](#)
- [Vídeo “Ojo con tus datos”. Documentos TV.](#)
- [Artículo “Tendencias 2014: El desafío de la privacidad en Internet”. ESET Latinoamérica.](#)
- [“Derecho a la protección de datos”. AGPD - Agencia Española de Protección de Datos.](#)
- [Canal YouTube de OSI Oficina de Seguridad del Internauta.](#)
- [Guía de privacidad y seguridad en Internet de la Agencia Española de Protección de Datos \(AGPD\) y la Oficina de Seguridad del Internauta \(OSI\).](#)
- [Página de Internet Segura for Kids \(IS4K\) sobre Privacidad.](#)
- [Preguntas frecuentes en la Línea de Ayuda de Internet Segura for Kids \(IS4K\).](#)

Internet Segura for Kids <http://www.is4k.es>

Página web del Centro de Seguridad en Internet para menores en España. Incluye:

- La información que **“necesitas saber”** sobre privacidad, ciberacoso escolar, sexting, contenido inapropiado, uso y configuración segura, mediación parental.
- Artículos de interés y actualidad en el **“blog”**.
- Guías, juegos, herramientas de control parental y otros recursos **“de utilidad”**.
- Información de **“programas”** de sensibilización para un uso seguro y responsable de Internet por los menores.
- Una **“línea de ayuda”** con una serie de preguntas frecuentes y un contacto para resolver dudas.

CONTACTO | ENCUESTA | AGENDA | BOLETINES

is4k INTERNET
SEGURA
FOR KiDS

LÍNEA DE AYUDA

BLOG

INICIO • NECESITAS SABER • DE UTILIDAD • PROGRAMAS • SOBRE NOSOTROS



FAMILIAS • EDUCADORES

7. Anexo1. Test de autoevaluación

1.- La identidad digital es el conjunto de información sobre una persona que podemos encontrar en Internet.

- ☐ Verdadero
☐ Falso

2.- ¿Cuál de estas acciones no es tan importante para tu reputación online?

- ☐ a) Lo que publico en redes sociales (aficiones musicales, fotos de viajes, comentarios en blog...)
☐ b) Lo que hago cuando estoy por la calle o en el parque con mis amigos.
☐ c) Los “Me gusta” que pongo en las fotos y publicaciones de mis amigos en redes sociales.
☐ d) Las fotos en las que me etiquetan mis amigos y conocidos.

3.- Verdadero o falso. La identidad digital se caracteriza por su perdurabilidad.

- ☐ Verdadero
☐ Falso

4.- Señala la opción incorrecta de entre las que se presentan a continuación:

- ☐ a) Es muy importante que lea detenidamente las condiciones de uso antes de registrarme en un servicio.
☐ b) En el mundo digital los datos de mi identidad pasan a estar gestionados por compañías privadas.
☐ c) En las condiciones de uso de los diferentes servicios online se suelen utilizar jergas legales fáciles de comprender.
☐ d) Soy yo como usuario de un servicio quien tiene la responsabilidad de conocer hasta qué punto estoy dejando de controlar aspectos de mi vida personal.

5.- Verdadero o falso. Una aplicación que me bajé para escuchar música y a la que he dado permiso para interactuar con mi red social puede afectar a mi privacidad, pues puede estar ofreciendo información que en mi red social no estaba habilitada, al sincronizarse las plataformas:

- ☐ Verdadero
☐ Falso

6.- Señala la opción incorrecta. Los riesgos en la gestión de la identidad digital y reputación online son:

- ☐ a) Usurpación de la identidad
☐ b) Malware y virus en el ordenador
☐ c) Amenazas para la privacidad

7.- Señala la opción incorrecta. Para controlar mi identidad digital es necesario:

- ☐ a) Configurar adecuadamente las opciones de privacidad al crear mi perfil.
☐ b) Tener muchas publicaciones, al menos publicar todos los días algo sobre cualquier tema.
☐ c) Revisar periódicamente las opciones de privacidad de mi perfil.
☐ d) Leer las condiciones y políticas de privacidad antes de aceptar crear mi perfil al abrir una cuenta en una red social.
☐ e) Controlar lo que publico.

8.- Es responsabilidad de las redes sociales configurar los perfiles de sus usuarios para reducir el riesgo de que la información se utilice con fines malintencionados.

- ☐ Verdadero
☐ Falso

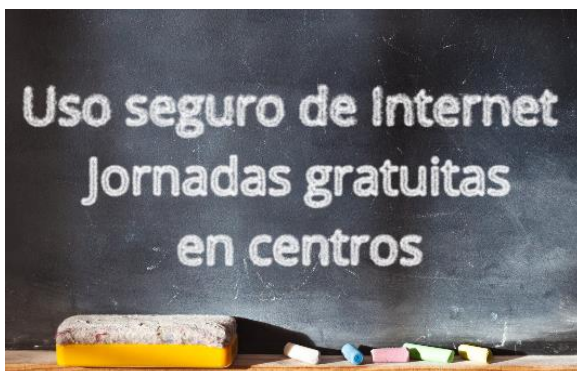
8. Anexo 2. Respuestas al Test de autoevaluación

1. **Verdadero.** Efectivamente, debemos entender que tanto nuestras propias publicaciones como las publicaciones ajenas referidas a nosotros forman parte de la construcción de nuestra identidad digital.
2. **Opción B.** No olvides que es la suma de todos los pasos que damos en la red lo que permite construir una identidad digital y en base a esta información, proyectar una imagen que podrá ser positiva o negativa (es como nos ven los demás) lo que llamamos reputación Online.
3. **Verdadero.** Efectivamente, en Internet borrar el rastro que van dejando nuestras decisiones no es siempre tan fácil.
4. **Opción C.** Has acertado. A pesar de las recomendaciones de las autoridades de protección de datos de utilizar un lenguaje sencillo y fácilmente comprensible todavía encontramos que en el mayor parte de los casos su redacción es difícil de comprender, aun así, es nuestra obligación leer antes de aceptar porque podemos estar poniendo nuestra privacidad y seguridad en peligro.
5. **Verdadero.** Efectivamente, la sincronización supone muchas ventajas pero también supone un peligro para tu privacidad, verifica siempre a que das derecho cuando te bajas una nueva aplicación.
6. **Opción B:** Los riesgos de una mala gestión de tu identidad digital están más relacionados con las amenazas a tu privacidad, el riesgo de usurpación de tu identidad y lógicamente con ofrecer a los demás una reputación online negativa.
7. **Opción B.** Para controlar mi identidad digital precisamente es muy necesario reflexionar sobre lo que voy a publicar, así que la mejor recomendación es “pensar siempre antes de publicar”.
8. **Falso.** Has acertado. Es nuestra responsabilidad no sólo configurar las opciones de privacidad más adecuadas para proteger mi privacidad, sino además, revisarlas periódicamente porque a veces las redes sociales actualizan las opciones de privacidad disponibles, lo que puede hacer que cambie la configuración que yo había establecido previamente.

9. Anexo 3. Recursos asociados

Recursos asociados a esta Unidad Didáctica disponibles para su futura utilización por los docentes:

- Presentación charla sensibilización dirigida al alumnado.
- Guía de preparación. Charla sensibilización dirigida al alumnado.



Toda la información del programa de Jornadas Escolares está disponible en la sección [programas](#) del portal [IS4K](#).