

# Competencia 6.2. Comunicación, colaboración y ciudadanía digital

- 0. Introducción y palabras claves:
- 1. Comunicación y Colaboración
- 2 Ciudadanía Digital
- 3 Identidad Digital
- 4 Huella Digital
- 5 ¿Y si usamos las Redes Sociales en el aula?

# 0. Introducción y palabras claves:

Esta competencia es la segunda competencia del área 6 y se centra en la **capacidad del docente para crear situaciones de enseñanza-aprendizaje en las que el alumnado desarrolle sus competencias comunicativas, de colaboración y participación ciudadana**, tanto en el ámbito educativo como en el social. Se espera que el docente haya adquirido, por su parte, estas mismas competencias y las pueda modelizar.

La **edad del alumnado puede condicionar de forma significativa el tipo de acciones educativas que pueda emprender un docente**. En general, todo el trabajo desarrollado en las etapas de educación infantil y educación primaria tendría carácter propedéutico, mientras que las desarrolladas en las etapas posteriores, podrían disponer de una aplicación práctica directa.

Esto es debido a que en el artículo 7. Consentimiento en los menores de edad de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales se establece que *“El tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de catorce años”*, es decir, a partir de esa edad los menores pueden voluntariamente ceder sus datos para registrarse en una plataforma o red social y, en cualquier caso, dependerá de las normas del servicio al que quiera acceder o de la regulación estatal o europea.

Esto supone que muchos de los adolescentes se pueden encontrar ya registrados en RR. SS. o plataformas similares y se hace especialmente necesaria su formación para que esa participación la puedan desarrollar con suficientes garantías. En cualquier caso, se deberá **potenciar que el alumnado sea capaz de realizar un análisis crítico** de estos servicios y valore la necesidad de su utilización en función de sus necesidades, sus valores, su bienestar personal y los riesgos y beneficios asociados a su uso.

En estos procesos de comunicación e intercambio o en la utilización de cualquier servicio de Internet, **el alumnado debe ser consciente de la “huella digital” que deja a través de las operaciones que realiza y de su comportamiento**, de que se puede hacer un seguimiento pormenorizado de ella y que es prácticamente imposible tener el control de esa información una vez que se ha realizado cualquier acción, lo que, de una forma u otra, podría afectar a su “reputación digital” y a aspectos presentes y futuros de su vida. Esta huella forma parte de la identidad digital, junto con los "perfiles" que se construyen de una forma más deliberada y consciente en las redes sociales y plataformas de intercambio o publicación de contenidos de cualquier tipo. La concepción, por tanto, del proceso de construcción responsable de la identidad digital es amplia, forman parte de ella también los "perfiles" que terceros puedan crear a partir de las páginas que se visitan, los servicios que se contratan, las compras que se realizan, los datos y

metadatos de los contenidos que se comparten, nuestras redes de contactos o los datos de nuestros dispositivos. Todo ello, y las inferencias que puedan realizarse a partir de dichos datos, conforma la identidad o identidades de los internautas.

Por último, la **ciudadanía digital** exige la participación ciudadana segura a través de los servicios que pueden ofrecer las administraciones públicas e instituciones privadas, por lo que el alumnado, aun no disponiendo de la edad necesaria, en algunos casos, deberá conocer la existencia y el uso de los certificados digitales, sistemas de firma y autenticación y de otras medidas de seguridad asociadas a su identidad digital.

Los **contenidos** que integran esta competencia son:

- Estrategias pedagógicas para el desarrollo de la competencia digital del alumnado.
- Tecnologías digitales que permiten comunicar, interactuar, compartir y colaborar.
- Huella digital, reputación, identidad digital e ingeniería social.
- Participación ciudadana a través de las tecnologías digitales.
- Normas de comportamiento en los procesos de comunicación y colaboración en entornos digitales

Los **indicadores del MRCDD** en esta competencia establecen que en el nivel B2 un docente:

- **6.2.B2.1.** *Reflexiona y evalúa su propia práctica para diseñar o adaptar nuevas propuestas pedagógicas con el fin de que el alumnado desarrolle su competencia a la hora de emplear las tecnologías digitales para comunicarse, colaborar con otros o participar como ciudadanos en la sociedad digital, así como para gestionar su huella e identidad digital.*
- **6.2.B2.2.** *Aplica sus conocimientos sociológicos, psicológicos y técnicos sobre las tecnologías para la comunicación, la colaboración y la participación para adaptar su utilización por parte del alumnado a contextos cambiantes.*

Algunas **acciones** en las que se manifiesta esta competencia son:

- Desarrollo, con el fin de mejorar mi práctica docente, diseños didácticos que ayuden al alumnado a comunicarse por medio de herramientas digitales aplicando y respetando sus propias normas de comportamiento y comunicación, a través del intercambio de mensajes a través de redes multiculturales.
- Configuro el blog de aula para que el alumnado trabaje colaborativamente en la creación de unas normas de etiqueta digital respetando la diversidad y las ideas de los demás.
- Planteo a mi alumnado, en clase de Filosofía o de Valores éticos y cívicos, una actividad para reflexionar sobre la concepción de la propia identidad y sobre la construcción de la personalidad en la que se haga necesario realizar un análisis comparativo de los datos seleccionados en el perfilado para personalizar los servicios de dos tipos de empresas distintas, una que ofrece un motor de búsqueda de contenidos (“eres lo que visionas”) y otra que proporciona una red social de comunicación (“eres lo que compartes”).
- Propongo a mi alumnado completar los cuadrantes de una "ventana de Johari" a partir de su actividad en los entornos digitales para identifiquen qué tipo de datos se situarían en

cada uno de los cuadrantes y para que analicen su interacción dentro de una red social o grupo de colaboración virtual.

- Pido a mi alumnado que, en pequeños grupos, elabore un listado de derechos digitales. Una vez elaborados, se comparan con los derechos y principios digitales que la Comisión Europea propone incluir en una declaración institucional como parte de las acciones incluidas bajo la iniciativa “La Década Digital de Europa: metas digitales para 2030”.
- He diseñado, con una herramienta de autor, un simulador que permite configurar de forma ficticia un perfil personal y vuelco los datos en una plantilla de documento de texto para que el alumnado sea consciente de la información que cede cuando realiza este tipo de procesos.
- Configuro el blog de clase para que el alumnado pueda calificar las aportaciones de otros compañeros y compañeras con un like o dislike y analizar sus efectos, ofreciendo sistemas alternativos de valoración.
- He creado un vídeo didáctico en el que explico a mi alumnado cómo configurar las opciones de privacidad de las cuentas en redes sociales.
- Participo con mi alumnado en un proyecto de colaboración escolar de ámbito autonómico consistente en la recopilación de datos sobre los índices de contaminación en las distintas localidades para construir, con el apoyo de un centro de investigación ubicado en el territorio, una web informativa y de sensibilización y elaborar modelos para simular distintas evoluciones en función del comportamiento de la ciudadanía.

<b>PALABRAS CLAVE</b>		
ciudadanía digital	derechos y deberes digitales	identidad digital
reputación digital	Redes Sociales	responsabilidad
autoprotección	comunicación y colaboración digital	huella digital

# 1. Comunicación y Colaboración

## Comunicación y Colaboración

Como hemos visto anteriormente, las tecnologías digitales han favorecido mediante diversas herramientas a la **comunicación** interpersonal así como el **trabajo colaborativo** entre los docentes.

Esta cultura de comunicación y colaboración digital es la que hemos de transferir a nuestro alumnado ya sea mediante herramientas para la comunicación como el **correo electrónico o el entorno virtual de aprendizaje** así como las herramientas colaborativas tales como los **documentos compartidos o los gestores de tareas**.

- Comunicación organizativa.
- Participación, Colaboración y Coordinación Profesional.

## ¿Qué deben saber nuestros alumnos sobre la comunicación y colaboración digital?

### Interacción a través de medios digitales

- Los menores interactúan a través de una gran variedad de plataformas digitales, por eso es necesario que comprendan cuáles son los medios de comunicación digitales apropiados para cada contexto.
- Y es que no es lo mismo comunicarse a través de una plataforma educativa, WhatsApp, o una red social como Twitter. Cada espacio tiene sus normas de conducta, derechos, deberes, obligaciones y peligros.
- Los menores deben aprender qué plataforma utilizar en base a sus necesidades, cómo hacerlo de manera responsable, y cómo actuar para evitar los riesgos a los que se exponen en cada medio.

### Compartir a través de medios digitales

- Una vez que los menores hacen uso de Internet, están expuestos a ser víctimas de robos de información o del uso de su propio contenido como arma contra ellos mismos u otros. Por eso deben aprender a compartir datos, información y contenido digital de manera apropiada y segura. Evitando que personas desconocidas o peligrosas tengan acceso a su información.

- Además, dentro de estas competencias digitales para menores, es importante que conozcan las prácticas de referencia y atribución de los contenidos en Internet, de esta forma evitarán meterse en problemas legales por apropiación de contenido con derechos de autor.

## Participar como ciudadanos digitales

- Internet ha permitido a todas las personas participar en la sociedad mediante el uso de servicios digitales públicos y privados. Así como de buscar oportunidades de auto-empoderamiento y de ciudadanía participativa a través de las tecnologías digitales apropiadas.
- Los menores pueden formar parte activa de la sociedad e implicarse en temas de trascendencia como la política, y los movimientos sociales. Pero para ello, deben saber donde y cómo hacerlo.

## Colaboración empleando tecnologías digitales

- Uno de los grandes beneficios que ha traído Internet con él es el de poder compartir los conocimientos de todo el mundo en un mismo lugar. Esto ha permitido acercar a personas con los mismos intereses y crear procesos colaborativos para la construcción y creación de recursos y conocimientos. Un gran espacio común donde los menores pueden aprender a tener una visión más amplia de los temas.

## Normas de conducta y Netiqueta

- Todo lo que se publica en Internet permanece ahí para siempre y tiene repercusiones en la vida real. Si tenemos en cuenta esto, y para garantizar un uso responsable y seguro de Internet, los menores deben aprender a estar al tanto de las normas conductuales y de los conocimientos técnicos mientras se utilizan las tecnologías digitales y la interacción en entornos digitales.
- También es necesario que sepan adaptar las estrategias de comunicación al público específico y conocer la diversidad cultural y generacional en entornos digitales.

## Gestión de la identidad y la reputación digital

- La identidad digital es la versión que existe online de cada persona y se crea a partir de la actividad que se tiene en Internet a través de los años. La identidad digital se construye a través de lo que el alumnado sube a internet, y aquello en lo que aparece o es etiquetado.
- La reputación digital es la imagen que se crea el resto de los usuarios de una persona a través de su identidad digital, la reputación puede ser positiva o negativa.
- Una mala identidad digital propia puede acabar perjudicando en la vida real. Por eso es importante que desde niños aprendan a crear y gestionar una o varias identidades digitales, proteger la propia reputación y manejar los datos que producen a través de varias herramientas, entornos y servicios digitales.

Extraído de: <https://gaptain.com/blog/competencias-digitales-para-menores-comunicacion-y-colaboracion/>

# 2 Ciudadanía Digital

La ciudadanía digital puede definirse cómo las normas de comportamiento que conciernen al uso de la tecnología. Estas normas se organizan en 9 áreas generales de comportamiento que tratan de recoger toda la complejidad del concepto y las implicaciones derivadas del buen y mal uso de la tecnología.

## **1. Netiqueta: (etiqueta) estándares de conducta o manera de proceder con medios electrónicos.**

El uso que hacemos los docentes de los medios electrónicos, nuestro comportamiento en las comunicaciones, etc. sirven como modelos que pueden inspirar al alumnado.

En algunos casos las pautas de actuación no están consensuadas, no hay unas normas de uso claras, o la adhesión a esas normas es baja, por lo que es importante dar ejemplos de buen uso.

También hay que tener en cuenta que la adopción de nuevas tecnologías y modos de comunicación puede suponer que la adopción de las mismas rompa con normas y códigos de conducta previamente establecidos y comúnmente aceptados. Por ejemplo: un 42% de estudiantes indican que responderían a una llamada de móvil si sonaba mientras estaban en una conversación cara a cara con otra persona.

A continuación van algunos ejemplos tanto de Netiqueta inapropiada, como de estrategias para favorecer una buena netiqueta.

### **Netiqueta inapropiada:**

- El alumnado emplea dispositivos digitales durante las clases para hacer cosas no relacionadas con la tarea del aula.
- El alumnado escribe correos con el cuerpo del mensaje en el asunto y todo en mayúsculas.
- El alumnado contacta a través de Redes Sociales a profesorado para preguntar dudas a las 11 de la noche de un sábado.

### **Estrategias:**

- Elaborar y publicar un documento de Política de Uso Aceptable de dispositivos digitales en el centro.
- Utilizar casos o escenarios para ilustrar formas adecuadas e inadecuadas para utilizar la tecnología.

- En colaboración con el alumnado y las familias, diseñar modelos de uso adecuados de la tecnología dentro y fuera del aula.

## 2. Comunicación: intercambio electrónico de información.

Los móviles, la mensajería instantánea y el correo electrónico han transformado las formas en las que se comunican los usuarios de la tecnología. Estas formas de comunicación han creado una nueva estructura social de quién, cómo y cuándo, interactúan las personas. Los estudiantes deben aprender a diferenciar cuál es la forma de comunicación más adecuada para una circunstancia determinada. Por ejemplo, la comunicación cara a cara es más efectiva que la comunicación electrónica cuando los temas que se van a tratar involucran información delicada, personal o negativa. La comunicación electrónica es eficiente y efectiva para transmitir información básica.

### Comunicación inapropiada

- Exclusión de personas concretas de los grupos de comunicación del grupo-clase por motivos de afinidad, manteniendo en los mismos a personas que no aportan contenidos relevantes o que directamente aportan contenidos ofensivos.
- Empleo de las comunicaciones para difundir contenidos falsos, sesgados o perjudiciales para otros miembros de la comunidad educativa.

### Estrategias:

- Modelar el uso adecuado de la comunicación electrónica: enviar mensajes que vayan al grano y evitar el uso de palabras comprimidas, abreviaciones, modismos, *slang*, etc.
- Estimular a los estudiantes para que se comuniquen digitalmente sólo cuando sea necesario, la comunicación cara a cara sigue siendo primordial para evitar malentendidos.
- Hacer uso racional de las comunicaciones digitales en cuanto a momentos y longitud de los mensajes.
- Usar dispositivos digitales en el aula únicamente con propósitos educativos. Por ejemplo, para acceder a información en tiempo real en la resolución de dudas, realización de tareas digitales, etc.

## 3. Educación: el proceso de enseñar y aprender sobre tecnología y su utilización.

La utilización de la tecnología en la educación es cada día más frecuente. Sin embargo, la enseñanza de cómo se utiliza esta de una manera correcta y coherente no se ha desarrollado de la misma forma. Cuando se enseña utilizando la tecnología, la mayoría de las veces no se incluye la instrucción de cuáles son los usos apropiados y los inapropiados. Una manera de favorecer una educación en el uso de la tecnología es comenzar con tareas muy limitadas y

dirigidas.

### **Educación inapropiada:**

- No se evita el uso de dispositivos móviles como herramientas para realizar trampas en pruebas y exámenes.
- No se forma al alumnado en el uso de la tecnología para contrastar informaciones, referenciar fuentes y origen de elementos multimedia empleados, seleccionar recursos, etc.

### **Educación apropiada:**

- Diseñar actividades y tareas que permitan a los estudiantes utilizar dispositivos digitales del centro, o sus propios dispositivos digitales (ordenador, portátil, tablet, smartphone, etc.) para acceder, guardar y compartir información de manera responsable.
- Estimular a los estudiantes a que encuentren usos nuevos y alternativos para Internet y otras tecnologías digitales.
- Ofrecer oportunidades de aprendizaje en las que se utilicen distintas facetas de la tecnología (ej: sitios web, chats, plataformas de elearning, foros de discusión, etc).
- Enseñar alfabetización digital mediante proyectos que se lleven a cabo con tecnología (ej: identificar, acceder, aplicar y crear información).

## **4. Acceso: participación electrónica plena en la sociedad.**

La tecnología ofrece muchas oportunidades para que gran número de personas accedan y utilicen formas alternativas de comunicación; pero no todo el alumnado y sus familias tienen la capacidad para usar o acceder las herramientas de la nueva sociedad digital.

A veces nos encontramos con que estas oportunidades solamente están disponibles para un limitado grupo de alumnado; aunque el costo de la tecnología está disminuyendo rápidamente y el acceso a la tecnología sea cada vez más sencillo. La disparidad en la idoneidad de dispositivos no ayuda, ya que para el trabajo relacionado con la escuela (manejo del EVA, comunicación asíncrona, elaboración de textos o presentaciones, etc.) un teléfono inteligente no es suficiente y hace falta otro dispositivo, como una tableta, un ordenador, etc.

Todavía existe mucha disparidad en el mundo entre los que tienen acceso a la tecnología y los que no lo tienen.

### **Acceso inapropiado:**

- La escuela ignora o subestima las necesidades tecnológicas de grupos marginados.
- Los encargados de la educación no ofrecen tecnologías especializadas para poblaciones especiales y por lo general aducen "falta de fondos".
- La escuela fracasa en compensar a los estudiantes que no tienen acceso a la tecnología en sus casas.

- Los docentes evitan realizar proyectos o tareas que involucren tecnología por temor a que no los puedan hacer los estudiantes carentes de acceso.
- No se contempla el uso de la tecnología como facilitadora de acceso al alumnado que presenta características diferenciadas.

### **Estrategias:**

- Identificar estudiantes que tengan circunstancias y necesidades especiales y explorar formas de acomodarlos o buscar alternativas a sus necesidades tecnológicas.
- Promover la creación de sitios web con accesibilidad plena, que puedan ser navegados por todas las personas sean cuales sean sus circunstancias y dispositivos en uso.
- Promover el acceso tecnológico para todos los estudiantes, independientemente de las discapacidades que tengan.
- Establecer tiempos y espacios en los centros educativos para facilitar a los estudiantes que no tienen acceso a la tecnología en sus casas, para que puedan utilizarla en el centro con el fin de realizar trabajos o tareas.
- Diseñar actividades, tareas, proyectos, etc. con la accesibilidad en mente, ya sea con adaptaciones de acceso, de itinerario, etc. Tener en cuenta siempre las distintas circunstancias de nuestro alumnado cuando programemos para no dejar a nadie atrás, incluyendo esto en los agrupamientos que realicemos, si es necesario.

## **5. Comercio: compra-venta electrónica de bienes y servicios.**

Aunque pensemos que nuestro alumnado es demasiado joven para acceder a servicios de compra-venta online, en la mayoría de los juegos online en los que participan, así como en muchas de las aplicaciones que emplean, hay contenidos que sólo pueden desbloquearse mediante transacciones electrónicas.

Es una de nuestras tareas la de enseñarles a relacionarse con el comercio electrónico, a valorar si las transacciones realmente merecen la pena en su relación coste-beneficio, y alertarles de los modelos de compras aleatorias (*loot crates*, sobres de recompensas, etc.) que pueden llevar a la adicción y al juego online desde la infancia mediante mecanismos de recompensa similares a los de los juegos de azar.

### **Comercio electrónico inapropiado:**

- El alumnado adquiere packs cosméticos o otro tipo de DLCs en juegos online con dinero real y sin control parental.
- El alumnado compra recompensas aleatorias en juegos y plataformas online con dinero real y sin control parental.
- El alumnado realiza compras en línea sin saber cómo proteger adecuadamente su identidad (robo de identidad), o sus cuentas o tarjetas de crédito.
- El alumnado compra en tiendas online guiado únicamente por ofertas que son demasiado buenas para ser verdad, exponiéndose a posibles fraudes de producto, uso

fraudulento de sus datos personales, o uso fraudulento de sus datos bancarios.

- El alumnado se deja llevar por compras por impulso abocados por el bombardeo de publicidad dirigida que reciben a través de las apps (TikTok, Facebook, Instagram, etc.)

### **Estrategias:**

- Involucrar a los estudiantes en un diálogo sobre el uso de la tecnología para comprar objetos y servicios.
- Estimular la participación de los estudiantes en una discusión en la que se expongan experiencias buenas y malas de las compras en línea.
- Solicitar al alumnado que indague sobre estrategias de compra comparativas y que las analicen.
- Enseñar a los estudiantes el peligro que tiene el robo de identidades y de qué manera pueden protegerse.
- Favorecer entre el alumnado una actitud crítica ante la adquisición de bienes online, especialmente los intangibles (DLCs, *Loot Crates*, Packs cosméticos, recompensas aleatorias, etc.) y la relación coste-beneficio de dichos bienes.

## **6. Responsabilidad: responsabilidad por hechos y acciones en los medios electrónicos.**

Desde que son pequeños, se le facilita al alumnado localizar y descargar recursos de Internet. Sin embargo, se obvia una formación sobre lo que es apropiado y lo que no lo es, qué es legal o ilegal cuando usan Internet.

Así es fácil encontrarse alumnos/as de Secundaria, Bachillerato o incluso Universidad que utilizan software comercial no licenciado, música o libros digitales descargados de forma ilegal, etc. sin tener ninguna conciencia de haber hecho nada ilegal.

Las entidades educativas tenemos que ser ejemplo en el uso de elementos multimedia y software con la consabida licencia, o si permite su uso libre, con la debida atribución y referenciación.

### **Responsabilidad inadecuada:**

- Los estudiantes descargan o consumen en streaming ilegalmente contenido multimedia proveniente de fuentes no fiables.
- Para proyectos de clase, los estudiantes copian contenidos y/o material multimedia de Internet y no reconocen la autoría del mismo.
- El alumnado utiliza software comercial no licenciado en sus dispositivos y/o no conoce alternativas legales como la adquisición de licencias de estudiante, software alternativo sin licencia, etc.

### **Estrategias:**

- Que el alumnado se familiarice desde el comienzo con el uso de software que no es privativo en el centro educativo, con el uso de material multimedia a través de plataformas legales, etc.
- Facilitar del uso de software libre.
- Promover entre los estudiantes un diálogo en el que se discuta lo que ellos sienten cuando los materiales que ellos han realizado se descargan sin su permiso.
- Fomentar la discusión sobre las percepciones de los estudiantes respecto al uso ético y no ético de la tecnología.
- Discutir acerca del uso honrado y las leyes sobre derechos de autor.

## **7. Derechos: las libertades que tienen todas las personas en el mundo digital.**

Cuando los estudiantes, generan o publican cualquier cosa digitalmente, ellos están amparados por la misma protección de derechos de autor que tiene cualquier otro productor de contenidos. No detenerse solamente en los derechos de autor, también en sus derechos como ciudadanos digitales, en especial relacionados con los puntos 2 y 5 anteriormente desarrollados.

### **Derechos inadecuados:**

- La institución no protege los derechos de los usuarios que trabajan con la tecnología de la escuela.
- El centro educativo no respeta el derecho de la protección de los datos del alumnado y sus familias.
- Los estudiantes violan las políticas de uso establecidas por la escuela porque las perciben como injustas.

### **Estrategias:**

- Informar a los docentes sobre los derechos digitales de los estudiantes, en especial aquellos relacionados con sus datos personales.
- Informar a los estudiantes sobre sus derechos y deberes como ciudadanos digitales y como miembros de la comunidad educativa del centro a través de un documento de Política de Uso Aceptable.
- Fomentar la discusión por parte de la comunidad escolar de las razones para el establecimiento de políticas respecto a la tecnología, involucrándola en el desarrollo de dichas políticas y los documentos que las recogen.
- Promover el que los estudiantes intercambien opiniones acerca del uso de la tecnología en la escuela y fuera de ella.
- Establecer unas personas de confianza y referencia (personal docente y alumnado) a quien pueda acudir el alumnado en caso de duda sobre sus derechos y obligaciones digitales.

## 8. Ergonomía: bienestar físico en un mundo tecnológico digital.

Cada vez está más presente en la sociedad el daño que el uso abusivo de la tecnología está acarreando tanto a nivel físico como psicológico; por ello el alumnado debe de ser consciente de estos daños que puede ocasionar el abuso de la tecnología.

A nivel físico aparecen cosas como el síndrome del túnel carpiano, contracturas en cuello y hombros, desarrollo de "chepa" por malas posturas, problemas de visión, etc., todos ellos son problemas comunes en las actividades relacionadas con la tecnología. A nivel mental la ansiedad por desconexión, la pérdida de atención, la falta de sueño, etc. son otros de los problemas que aparecen con el abuso de la tecnología. Tampoco podemos obviar los accidentes causados por distracciones por uso de la tecnología: caídas, golpes con mobiliario urbano, atropellos, caída de dispositivos sobre el rostro, etc.

Los educadores deben fomentar que los estudiantes utilicen la tecnología de manera responsable con el fin de prevenir lesiones físicas y/o afecciones mentales. Debemos promover que en el centro se trabaje con la ergonomía apropiada, dentro de las circunstancias, y así ayudar a evitar problemas futuros relacionados con el uso inadecuado de la tecnología.

### **Ergonomía inadecuada:**

- Los docentes ignoran los efectos físicos perjudiciales del uso inadecuado de la tecnología por parte del alumnado.
- Los docentes no enseñan ergonomía cuando los estudiantes utilizan la tecnología.
- Se emplea mobiliario no adaptado al tamaño del alumnado a la hora de emplear tecnología.
- No se ofrecen momentos de descanso durante el uso de la tecnología en el centro.
- Se ignoran las condiciones lumínicas necesarias para poder trabajar de manera cómoda con la tecnología.

### **Estrategias:**

- Explorar sitios web dedicados a la ergonomía para informarse sobre nuevas formas de usar la tecnología con seguridad.
- Asegurarse de que las aulas están bien iluminadas y que el mobiliario es el adecuado para usar la tecnología en forma segura.
- Informar al alumnado de los problemas físicos a largo plazo que pueden generar ciertos usos inadecuados de la tecnología.
- Fomentar el uso de la tecnología con pausas, enseñando estiramientos y otras estrategias que puedan aliviar la carga física del uso de la tecnología.

## 9. Riesgo: precauciones para garantizar la seguridad en los medios electrónicos

Cada vez se guarda electrónicamente mayor cantidad de información de carácter confidencial por lo que se debe generar la estrategia correspondiente para protegerla.

Ante la proliferación del almacenamiento remoto, la primera capa de seguridad tiene que ser la generación de contraseñas seguras, así como un almacenamiento seguro de las mismas que permita un acceso rápido a ellas.

Para la segunda capa de seguridad el alumnado debe aprender a proteger sus dispositivos frente amenazas como el malware, estrategias de phishing, etc. Proteger el equipo personal no solamente indica responsabilidad de parte del usuario sino que responde a la necesidad de proteger la comunidad. Por ejemplo, manteniendo actualizado el antivirus.

Una última capa de seguridad es la de generar copias de seguridad de nuestros datos digitales que queremos conservar y almacenarlas de manera segura y responsable mediante unidades externas, preferentemente encriptadas.

Finalmente la seguridad va más allá de la protección de los equipos. Incluye protegernos a nosotros mismos y a otros de influencias externas que pueden causarnos daños físicos.

### **Seguridad inadecuada:**

- El alumnado comparte de manera pública y publicada sus contraseñas de accesos a los servicios online del centro (Cuentas de correo, EVAs u otros servicios online).
- Alumnado y profesorado emplean unidades externas sin revisarlas mediante software antivirus.
- Alumnado y profesorado comparten información sensible en respuestas a mensajes sospechosos recibidos a través de medios digitales (Phishing).
- Alumnado y profesorado asumen que no hay ninguna necesidad de proteger los datos electrónicos.
- Alumnado y profesorado no mantiene actualizado el software o los parches que protegen de los virus, en sus dispositivos.
- El alumnado no protege su identidad cuando usa correos electrónicos, participa en salas de conversaciones (chats) o mensajería instantánea.

### **Estrategias:**

- Ponerse en contacto con organizaciones especializadas para obtener materiales que le indiquen cómo proteger los usuarios, realizando formaciones específicas en autoprotección digital.
- Desarrollo por parte del centro educativo de unos protocolos de protección digital (Firewall, talleres de protección de datos, etc.).
- Desarrollar píldoras formativas para profesorado, alumnado y familias sobre estrategias de generación, almacenamiento y protección de contraseñas.
- Enseñar a los estudiantes a realizar copia de seguridad de la información y a proteger sus equipos de daños.
- Enseñar a los estudiantes, utilizando software legal, cómo comprobar la ausencia de malware en sus dispositivos.

Tenemos que tener en cuenta que la ciudadanía digital es un derecho universal recogido por la UNESCO en la reformulación de sus derechos a e-derechos de los niños y las niñas.

b0aa737c

Fuente: Raúl Diego (<https://www.rauldiego.es/la-importancia-de-educar-en-la-ciudadania-digital/>)

# 3 Identidad Digital

## ¿Qué es la Identidad Digital?

La Identidad Digital es el conjunto de **informaciones publicadas en Internet sobre mí** y que componen la imagen que los demás tienen de mí: datos personales, imágenes, noticias, comentarios, gustos, amistades, aficiones, etc. Estas informaciones no son únicamente aquellas que yo comparto voluntariamente, **también son** aquellas informaciones, datos, imágenes, etc. que **otras personas o instituciones comparten** sobre mí, etiquetándome, nombrándome, etc., por lo que **se construye socialmente**.

Todos estos datos me describen en Internet ante los demás y **determinan mi reputación digital**, es decir, **la opinión que los demás tienen de mí en la red**.

Esta identidad puede construirse sin que se corresponda exactamente con la realidad, ya que suele presentar una realidad sesgada; sin embargo lo que se hace bajo esa identidad digital tiene sus consecuencias en el mundo real y viceversa.

## ¿Cuáles son sus características?

Nuestro alumnado tiene que conocer que la identidad digital tiene una serie de características que hacen que tenga múltiples facetas y ángulos, y que, en su caso, su identidad digital lleva generándose prácticamente desde el nacimiento; las **características de la identidad digital** son:

- **Social.** Se construye navegando por las redes sociales a partir del reconocimiento de los demás sin ni siquiera llegar a comprobar si esa identidad es real o no.
- **Subjetiva.** Depende de cómo los demás perciban a esa persona a través de las informaciones que genera.
- **Valiosa.** A veces personas y empresas navegan por las redes sociales para investigar la identidad digital de un candidato y tomar decisiones sobre él/ella.
- **Indirecta.** No permite conocer a la persona directamente sino las referencias publicadas de esa persona.
- **Compuesta.** La identidad digital se construye por las aportaciones de la misma persona y también por otras personas sin la participación o consentimiento del mismo.
- **Real.** La información de la identidad digital puede producir efectos positivos y negativos en el mundo real.
- **Dinámica.** La identidad digital no es una foto instantánea sino que está en constante cambio o modificación.

## Gestión de la Identidad Digital

El alumnado debe aprender a gestionar su identidad digital desde la infancia, **en colaboración con los adultos responsables de su crianza y educación**, para ir tomando poco a poco las riendas de dicha gestión cuando se alcanza la adolescencia y aparecen los perfiles individuales en redes sociales.

Un conocimiento previo sobre esta gestión de su identidad digital les permitirá **ser más reflexivos** a la hora de realizar distintas acciones que pueden suponer un impacto negativo a su reputación digital. Aprendiendo que no se debe de huir de la actividad en redes sociales, sino que esta no tiene que estar marcada por la impulsividad a la hora de compartir, tanto contenidos propios, como contenidos de otras personas. Deben recordar que la identidad digital se construye socialmente, y que lo que subimos sobre otra persona, puede afectar a su identidad y su reputación digital también.

## ¿Cómo se construye la Identidad Digital?

Parte de la identidad digital de nuestro alumnado viene marcada por la actividad en redes sociales de sus familiares, nos podemos encontrar alumnado con una gran huella digital prácticamente desde el nacimiento, con un reguero de fotos y publicaciones en distintas redes sociales, en especial en Facebook, Instagram y TikTok.

Para este alumnado, el compartir absolutamente todo en las redes sociales será lo normal, lo cual puede resultar complicado a la hora de hacer una gestión eficaz de la identidad digital.

Como hemos dicho anteriormente la identidad digital se

Nuestro alumnado va a construir su identidad digital a través de tres canales principalmente:

### Redes sociales

Nuestro alumnado suele ser ávido usuario de redes sociales, en las que tendrá (al menos) un perfil por red, aunque **es usual que cuenten con varios perfiles**: un perfil público compartido con familiares y amigos, un perfil privado compartido con un círculo restringido de amistades al margen de la familia, y un perfil que se emplea para curiosear los perfiles de otras personas de manera más anónima.

La **identidad digital** de nuestro alumnado **se construirá preferentemente a través de los perfiles públicos, y de acceso limitado** que tienen en distintas redes sociales y en los que se muestra, comparte imágenes y vídeos de acceso más o menos público. Estas redes suelen ser: Instagram, TikTok; y en menor medida Facebook, Youtube y Twitter.

Un fenómeno que se está dando en los últimos años y que es más complicado de gestionar son los "directos", conexiones a través de Twitch, Instagram o TikTok en los que se está durante mucho rato haciendo y diciendo cosas, y en los que es casi imposible una edición a posteriori, y en los que otras personas pueden grabar lo que están emitiendo.

No hay que olvidar que **las aplicaciones de mensajería instantánea (Whatsapp, Telegram, etc.) son también redes sociales**, y que, aunque nuestro alumnado considere que son vehículos de comunicación privada, tanto las imágenes, como las conversaciones permanecen, y pueden ser empleadas por otras personas para perjudicar su identidad y su

reputación digital.

Como docentes podemos sugerirles una serie de **conductas de autoprotección** a la hora de compartir contenidos en las distintas redes sociales, que cuentan con opciones de configuración que pueden ayudar a mantener un mayor control sobre su identidad digital.

No hemos de olvidar que **las convenciones sociales y de uso** de algunas de estas plataformas **cambian según el país o el idioma** de las personas con las que se estén comunicando y ello también puede afectar a la construcción de esa identidad digital de nuestro alumnado. Como docentes de idiomas podemos ayudarles a evitar problemas a la hora de interactuar en estas redes sociales; siempre siendo conscientes de que si hacemos una apología del uso de redes sociales debe de ser siempre desde un punto de vista educativo y positivo: encontrar recursos, favorecer la interacción en la segunda lengua, profundización en aficiones positivas, etc.

### Correo Electrónico y otras plataformas de comunicación

Nuestro alumnado también construye su identidad digital en sus **comunicaciones a través del correo electrónico y otras plataformas de comunicación**; ya sean las comunicaciones internas a través de los dominios de correo electrónico del centro educativo, los Entornos Virtuales de Aprendizaje o las plataformas de gestión y comunicación como SIGAD.

Una comunicación eficaz, con un registro apropiado y concisa será clave para que su aporte sea positivo a la identidad digital de nuestro alumnado; por ello se puede trabajar desde las áreas de Lengua y de Idiomas la comunicación en este formato, cada vez más imperante ante la carta manuscrita, según los distintos destinatarios a los que se dirige la comunicación.

## Relación de la Identidad Digital y la Identidad Analógica

Ambas identidades **están relacionadas y pueden tener una gran influencia sobre la otra**, ya que lo que hace nuestro alumnado en el mundo "desconectado" puede salpicar al mundo digital y viceversa. Todos conocemos conflictos que han comenzado en el patio y han explotado en redes; o que empezaron como una bronca en redes, y han terminado en una pelea a gritos e insultos en el patio.

Tanto la identidad digital como la identidad analógica **están influenciadas por los distintos aspectos que las configuran**, así las afinidades musicales, deportivas, sociales, religiosas, ideológicas, etc. que tiene nuestro alumnado y que muestran en sus entornos digitales afectan a sus relaciones sociales fuera del entorno digital.

Por ejemplo un alumno tremendamente forofa de un equipo de fútbol, que consume y comparte imágenes y vídeos de los ultras de dicho equipo en sus redes sociales, puede rechazar o incluso tener algún conflicto con un compañero o compañera de clase que sea fan de otro equipo rival, o

que le reproche el usar esos contenidos no apropiados.

## Visibilidad en entornos digitales

Nuestro alumnado emplea **las métricas de las Redes Sociales**: número de seguidores, cantidad de "me gustas" de una publicación, cantidad de comentarios e interacciones, interacción con personas famosas en redes, etc. como elementos **para medir su visibilidad**, lo lejos que llega lo que suben a las redes; y esa carrera por tener más de todo lo anterior puede hacerles caer en publicar contenido que resulte perjudicial para su identidad digital, como puede ser contenido polémico, sexualizado, etc.

Desde el mundo educativo tenemos que **poner en valor aquellos perfiles de redes que tienen una alta visibilidad y que aportan contenido de calidad** en dichas redes; para ello es interesante que los docentes de idiomas conozcamos algunos perfiles de redes que sirvan como ejemplo a la hora de hablar de visibilidad positiva, frente a visibilidad negativa.

## Reputación en entornos digitales

La reputación de las personas es la imagen que otros se hacen de esa persona, en este caso la reputación en entornos digitales es la imagen que los otros se hacen de una persona en función de todos los contenidos que configuran su identidad digital.

Nuestro alumnado, especialmente a través de lo que comparte en redes sociales, puede tener una gran influencia en la reputación que van a tener en los entornos digitales, generando una identidad digital que lleve mayoritariamente hacia una **reputación positiva o negativa** en función de aquello que va subiendo a redes, junto a lo que otras personas suben sobre ellos y ellas. Así pueden forjarse una **reputación positiva** como personas deportistas, activas, responsables, solidarias, etc. o pueden generarse una **reputación negativa** como personas problemáticas, que abusan del alcohol, conflictivas, etc.

Es importante hacer entender al alumnado que todo **lo que se sube a internet permanecerá allí para siempre**, y que **la gestión de una reputación negativa es muy complicada**. Además, de que la reputación que se labran desde el comienzo de su actividad en redes puede tener **influencia en situaciones en el futuro, como la búsqueda de empleo**, así que algo que parece que no va a tener relevancia en la adolescencia (imágenes o vídeos inapropiados, comentarios de odio hacia colectivos o personas, participación en situaciones de ciberacoso, etc.) pueden tener un recorrido muy largo que puede afectarles muchos años más tarde.

El trabajo de fomento de una reputación digital positiva se puede hacer a través del trabajo con ejemplos como los citados anteriormente o con páginas específicas que trabajan temas como la identidad digital o la protección de datos del alumnado en el idioma objetivo, como la iniciativa [Be Internet Awesome With Google](#), que tiene multitud de idiomas para escoger.

## Gestión de la Identidad Digital

Como hemos dicho anteriormente la identidad digital no se genera exclusivamente de manera individual, sino que también tiene un componente social, y una manera de reducir la capacidad de

impacto de dicho componente social es aprovechar las opciones de privacidad que ofrecen las Redes Sociales.

Una formación y acompañamiento a la hora de establecer los **límites a la interacción que se puede realizar con los perfiles de nuestro alumnado en Redes Sociales** puede ayudarles a aprender a gestionar su identidad digital, siempre explicando por qué deberían de adaptarlos y dejándoles la última palabra a ellos; pero no podemos quedarnos sólo ahí.

Otra medida de autoprotección de la identidad digital es la de **no aceptar solicitudes de amistad de perfiles anónimos, de personas que no conocen o de perfiles sospechosos;** ya que dichos perfiles pueden ser de personas que buscan acercamientos sexuales (groomers), de personas que buscan robarles los datos y suplantar su identidad (phising), de personas que buscan métodos para atacar (ciberbullies), etc. Además, esos perfiles añadidos como amistades, también pueden etiquetar al alumnado en publicaciones y perjudicar su identidad y reputación digitales.

Por último una gestión segura de contraseñas permite también mantener segura la identidad digital, ya que hará más complicado el secuestro de los perfiles de nuestro alumnado.

## **Recursos para trabajar la Identidad Digital**

Encontrar infografías como la siguiente del Gobierno de Canarias pero en el idioma en el que impartimos nuestras clases puede ser un magnífico recurso para concienciar al alumnado a la vez que se trabaja la segunda lengua con un propósito claro y en un contexto que la mayoría de nuestro alumnado conoce.

**Infografía sobre Identidad Digital del Gobierno de Canarias**

# Identidad Digital



Constrúyela de forma responsable  
y mejorarás tu  
imagen digital

Información  
que yo  
publico

Información  
que  
comparto

Lo que se  
dice de mí

Información  
que existe  
sobre mí

Mi  
identidad  
digital

Cuido mi imagen

mi imagen digital se parece a la realidad

No cuido mi imagen  
mi imagen digital se desvirtúa

deja huella

interviene la actividad de  
terceras personas

es global

influye en la interacción

no se olvida

Decálogo de buenas prácticas para mejorar tu  
identidad digital

Piensa  
antes de  
subir cualquier  
cosa

sé consciente  
de que finalmente  
cualquiera lo  
puede ver,  
aunque lo  
envíes a una  
sola persona

Ejerce la  
ciudadanía  
digital de  
forma  
responsable  
y activa

denuncia  
actividades  
ilícitas o  
inapropiadas

Participa  
de forma  
respetuosa

expresate  
con  
educación,  
...

Utiliza  
nombres  
de usuario  
o de registro  
adecuado

nombre  
de usuario,  
correo,...

Respetar  
los derechos  
de autor y las  
licencias de  
uso

Selecciona  
con cuidado  
tus amistades

Selecciona  
cuidadosamente  
los avatares e  
imágenes asociadas  
a tus perfiles

Conoce y  
gestiona la  
privacidad  
de las redes  
donde  
participas

busca  
información  
sobre ti de  
forma  
regular

Practica  
Egosurfing

Aporta  
contenidos  
de calidad



<http://www.gobiernodecanarias.org/medusa/ecoesuela/seguridad/>



© Gobierno de Canarias 2016



Gobierno  
de Canarias

Consejería de Educación y Universidades  
Dirección General de Ordenación,  
Innovación y Promoción Educativa

Gobierno de Canarias. Identidad digital. (CC BY-SA)

## Materiales para trabajar la Identidad Digital en Primaria en español

El mago de las redes sociales: En ocasiones, los poderes adivinatorios tienen menos misterio del que puede parecer, basta con no configurar nuestra privacidad en RRSS.

<https://www.youtube.com/embed/IVvfx0GT5sk>

## Videos de la Agencia Española de Protección de Datos: Tú controlas en internet.

[https://www.youtube.com/embed/D57vDI7w\\_mA](https://www.youtube.com/embed/D57vDI7w_mA)

<https://www.youtube.com/embed/-x1-hdcF2TU>

## Materiales para trabajar la Identidad Digital en secundaria en español

A continuación, os compartimos una **propuesta didáctica**, con animaciones y guías llamada Pilar y su celular, producida y diseñada por PantallasAmigas.

“Pilar y su Celular” es un programa educativo concebido para ayudar a madres, padres, docentes y profesionales del mundo educativo en general en la tarea de acompañar a las y los más pequeños (**8 a 12 años**) en el inicio del **uso autónomo, responsable y saludable del smartphone**.

### **Pilar y su celular: Historias para contar**

Videos para trabajar la privacidad en RRSS en secundaria:

<https://www.youtube.com/embed/Ak3qp4qRAiY>

[https://www.youtube.com/embed/4xyAnL\\_yNFA](https://www.youtube.com/embed/4xyAnL_yNFA)

## Recopilación de vídeos sobre uso de redes sociales en jóvenes y adolescentes

Aquí tienes una recopilación de vídeos, de la iniciativa "Por un uso Love de la tecnología" de una empresa de telecomunicaciones junto con la Agencia Española de Protección de Datos y el INCIBE (Instituto Nacional para la Ciberseguridad), que pueden ayudar a tu alumnado a reflexionar sobre el uso que dan a las redes sociales y lo expuesto de su identidad digital y cómo puede afectar eso a su reputación digital.

<https://www.youtube.com/embed/UPVU0XK6zq0>

<https://www.youtube.com/embed/6K0wtyDI2u4>

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

<https://www.youtube.com/embed/0qCWQTS04i0>

<https://www.youtube.com/embed/efjLymGz3U0>

<https://www.youtube.com/embed/11Q-z4AjEtk>

<https://www.youtube.com/embed/s-3M2e366M4>

<https://www.youtube.com/embed/rpnLvDPpzd0>

<https://www.youtube.com/embed/lw1TaPifnDI>

<https://www.youtube.com/embed/WzmmhBCtm8fs>

[https://www.youtube.com/embed/sE-a\\_hAQmug](https://www.youtube.com/embed/sE-a_hAQmug)

<https://www.youtube.com/embed/XCPxLQUEU1I>

<https://www.youtube.com/embed/d9dfuU2CRT0>

<https://www.youtube.com/embed/czGoaAhrPEc>

Recuerda que en el Capítulo 5 del libro del Área 1 te proporcionamos una serie de recursos en distintos idiomas para trabajar la importancia de la ciberseguridad y de un manejo responsable de las redes sociales, en distintos idiomas.

# 4 Huella Digital

## Huella digital: significado y definición

Una huella digital (a veces llamada sombra digital o huella electrónica) se refiere al **rastro de datos que dejas cuando usas Internet**. Esto incluye los sitios web que visitas y los correos electrónicos y la información que envías en línea. Se puede usar una huella digital para rastrear las actividades y los dispositivos en línea de una persona. Los usuarios de Internet crean su huella digital de forma activa o pasiva.

## ¿Qué es una huella digital?

Siempre que utilizamos Internet, dejas un rastro de información conocido como tu huella digital. **Una huella digital crece de muchas maneras: por ejemplo, cuando publicas en redes sociales, te suscribes a un boletín informativo, dejas una reseña en línea o compras en línea.**

En ocasiones, **no siempre es obvio que estás contribuyendo a tu huella digital**. Por ejemplo, los sitios web pueden rastrear tu actividad instalando cookies en tu dispositivo, y las aplicaciones pueden recopilar tus datos sin que lo sepas. Una vez que permites que una organización acceda a tu información, esta podría vender o compartir tus datos con terceros. Y lo que es peor, tu información personal podría verse comprometida como parte de una filtración de datos.

A menudo se escuchan los términos “activo” y “pasivo” en relación con las huellas digitales:

- Una **huella digital activa** ocurre cuando el usuario compartió deliberadamente información sobre sí mismo (por ejemplo, mediante la publicación o participación en sitios de redes sociales o foros en línea). Si un usuario inicia sesión en un sitio web a través de un nombre de usuario o perfil registrado, cualquier publicación que realice forma parte de su huella digital activa. Otras actividades que contribuyen a las huellas digitales activas incluyen completar un formulario en línea (como suscribirse a un boletín informativo) o aceptar cookies en tu navegador.
- Se crea una **huella digital pasiva** cuando se recopila información sobre el usuario sin que este sea consciente de que está sucediendo. Por ejemplo, esto ocurre cuando los sitios web recopilan información sobre cuántas veces los visitan los usuarios, de dónde vienen y cuál es su dirección IP. Este es un proceso oculto, por ende los usuarios pueden no saber que está ocurriendo. Otros ejemplos de huellas pasivas incluyen sitios de redes sociales y anunciantes que recopilan las veces que pones “me gusta”, compartes y comentas para crear un perfil sobre ti y enviarte contenido específico.

<https://www.youtube.com/embed/tLYumn3qo5g>

[https://www.youtube.com/embed/fLKPsy2\\_2Og](https://www.youtube.com/embed/fLKPsy2_2Og)

<https://www.youtube.com/embed/fb506ebswb8>

## ¿Por qué son importantes las huellas digitales?

Las **huellas digitales son importantes por los siguientes motivos:**

- Son relativamente permanentes y, una vez que los datos son públicos (o incluso semipúblicos, como puede ser en el caso de las publicaciones de Facebook), el propietario tiene poco control sobre cómo los usarán los demás.
- Una huella digital puede determinar la reputación digital de una persona, la cual ahora es casi tan importante como su reputación fuera de Internet.
- Los empleadores pueden verificar las huellas digitales de sus empleados potenciales, especialmente sus redes sociales, antes de tomar decisiones de contratación. Los colegios y universidades también pueden verificar las huellas digitales de sus posibles estudiantes antes de aceptarlos.
- Las palabras y fotos que publiques en línea pueden malinterpretarse o modificarse, lo que podría provocar una ofensa involuntaria.
- El contenido destinado a un grupo privado puede extenderse a un círculo más amplio, lo cual podría dañar relaciones y amistades.
- Los cibercriminales pueden aprovecharse de tu huella digital, utilizándola para fines como el **phishing** para acceder a la cuenta o crear identidades falsas basadas en tus datos.

Por estas razones, vale la pena considerar lo que dice tu huella digital sobre ti. Muchas personas intentan administrar su huella digital siendo cautelosas con sus actividades en línea para controlar los datos que se pueden recopilar en primer lugar.

## Ejemplos de huella digital

Un usuario de Internet podría tener cientos de elementos como parte de su huella digital. Algunas de las formas en las que los usuarios aumentan su huella digital incluyen lo siguiente:

### Compras en línea

- Realizar compras en sitios web de comercio electrónico
- Registrarse para recibir cupones o crear una cuenta
- Descargar y utilizar aplicaciones de compras
- Registrarse en los boletines de noticias de una marca

## Banca en línea

- Usar una aplicación de banca móvil
- Comprar o vender acciones
- Suscribirse a blogs y publicaciones financieras
- Abrir una cuenta de tarjeta de crédito

## Redes sociales

- Usar las redes sociales en tu computadora o dispositivos
- Iniciar sesión en otros sitios web con tus credenciales de redes sociales
- Conectarse con amigos y contactos
- Compartir información, datos y fotos con tus contactos
- Unirse a un sitio o una aplicación de citas

## Leer las noticias

- Suscribirse a una fuente de noticias en línea
- Ver artículos en una aplicación de noticias
- Registrarse para recibir el boletín informativo de una publicación
- Volver a publicar los artículos y la información que has leído

## Salud y ejercicios

- Usar rastreadores deportivos
- Usar aplicaciones para recibir atención médica
- Registrar tu dirección de correo electrónico en un gimnasio
- Suscribirte a blogs de salud y fitness

## Protege tu huella digital

Debido a que los empleadores, las universidades y otras entidades pueden buscar tu identidad en línea, es una buena idea tener en cuenta tu huella digital. A continuación, se ofrecen algunos consejos para proteger tus datos personales y administrar tu reputación en línea.

- Utiliza buscadores para comprobar tu huella digital
- Reduce la cantidad de fuentes de información que te mencionan
- Limita la cantidad de datos que compartes
- Vuelve a verificar tu configuración de privacidad
- Evita compartir demasiado en las redes sociales

- Evita los sitios web inseguros
- Evita divulgar datos privados en redes Wi-Fi públicas
- Elimina las cuentas antiguas
- Crea contraseñas seguras y utiliza un administrador de contraseñas
- No inicies sesión con Facebook
- Mantén actualizado el software
- Revisa tu uso de dispositivos móviles
- Piensa antes de hacer una publicación
- Actúa rápido después de una filtración

Extraído de: <https://latam.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>

# 5 ¿Y si usamos las Redes Sociales en el aula?

Las redes sociales se han convertido en la principal vía de comunicación para los jóvenes estudiantes. Según el Estudio Anual de Redes Sociales 2019 de IAB, el perfil de estudiante que más utiliza las redes sociales lo encontramos en las universidades (46%), seguido muy de cerca por los estudiantes de educación secundaria (40%). Además, el rango de edad de 16-30 años ya representa un 31% del total de usuarios de redes sociales de nuestro país.

Que Instagram, Twitter o Snapchat estén presentes en el aula no debe sorprendernos. Ahora bien, ¿y si pudiéramos aprovecharlas para hacer más divertidas y productivas las clases?

## Aquí van algunos beneficios del uso de las redes sociales en el aula

- Fomentan la participación de nuestros alumnos. Además, les permite interaccionar entre ellos, hacer equipo y generar debate.
- Formación. Las redes sociales ayudan a mejorar las competencias y conocimientos tecnológicos de los alumnos. La demanda de nuevos perfiles digitales en el mercado nos muestra cómo el manejo de herramientas relacionadas con estas plataformas puede ayudarles a la inserción laboral.
- Identidad digital. Desde la docencia podemos ayudar a los alumnos a crear correctamente su identidad digital, enseñándoles la importancia de la privacidad o cómo pueden evitar posibles casos de ciberacoso.

Debemos de ser conscientes de que el uso de las Redes Sociales puede resultar estimulante para el alumnado, especialmente en secundaria, pero el uso de estas redes debe tener un **claro objetivo pedagógico**, no debiendo ser un fin de la actividad, sino un medio para alcanzar los objetivos didácticos de la misma.

No podemos olvidar que nos debemos a la protección de la imagen y los datos personales de nuestro alumnado, por lo que, además de respetar en todo momento la **Política de Uso Aceptable y la Política de Comunicación** que establezca nuestro centro, deberíamos realizar **publicaciones** en redes exclusivamente a través de **los perfiles propios del centro educativo**. Si es necesario, se puede solicitar la creación de un perfil específico para el área o departamento en cuestión, pero siempre siguiendo las líneas marcadas por los documentos que hemos citado y que serán nuestra referencia.

Si en nuestro centro no existen esos documentos, deberemos consultar con el Equipo Directivo la manera de proceder antes de decidir publicar en Redes Sociales ningún tipo de contenido.

En el curso de Aularagon de Community Manager Educativo encontraremos multitud de recomendaciones sobre la gestión de las Redes Sociales del centro y cómo deberían ser las publicaciones que se hagan en las mismas.

Tenemos que ser especialmente vigilantes del uso que se hace de la imagen del alumnado, o de su trabajo, en las Redes Sociales, ya que, cada vez más, nos encontramos con docentes en las redes que emplean al alumnado como un elemento para reforzar su marca personal, para mostrar lo buenos que son los materiales que generan y luego ponen a disposición de quien quiera comprarlos en su tienda virtual, o para demostrar lo "guays y enrollados" que son, en especial en TikTok.