6.2. Comunicación, colaboración y ciudadanía digital.

- 6.2.0. Introducción.
- Final
- Ciudadanía Digital
- Huella digital

Copyright 2026

6.2.0. Introducción.

Esta competencia 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.

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.

Copyright 2026

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.

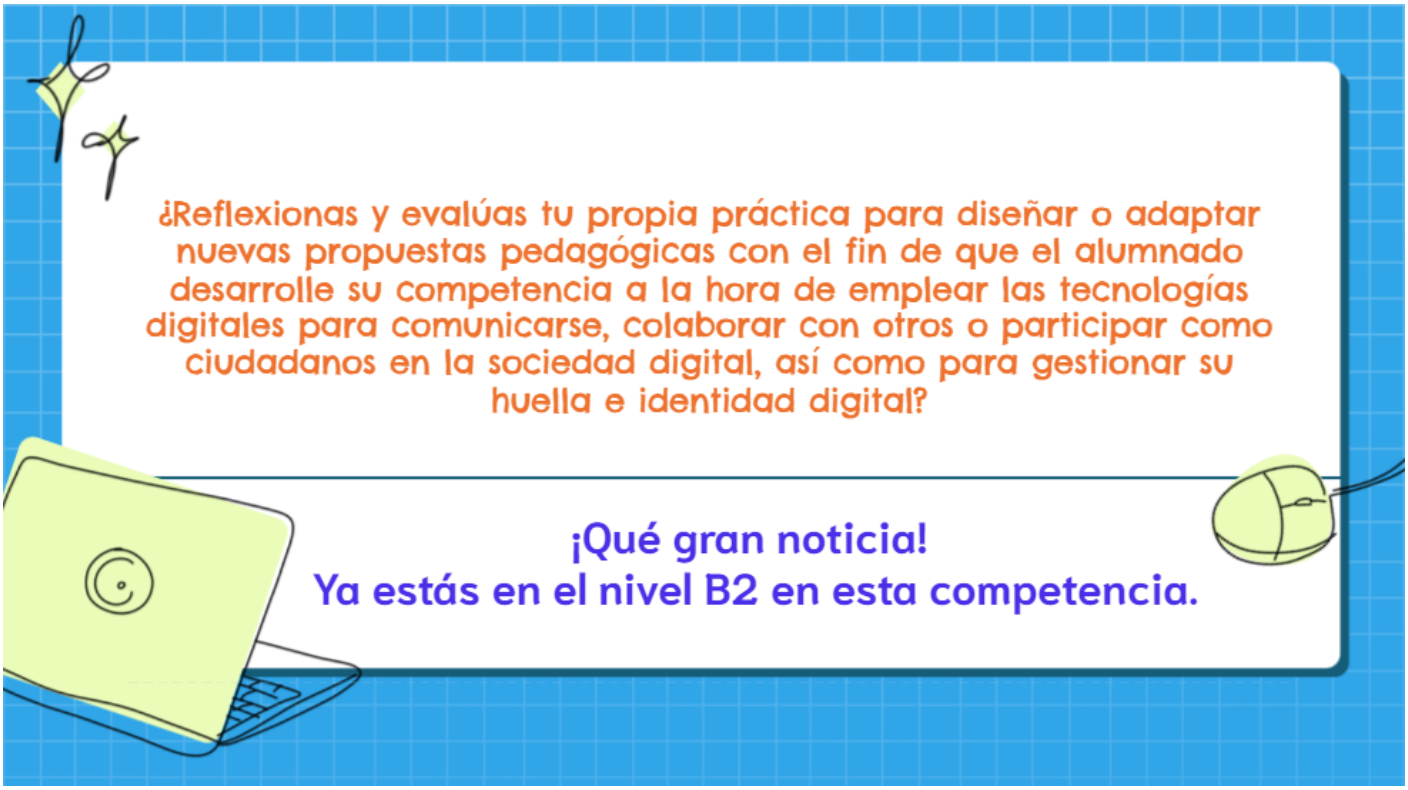
Los **contenidos** necesarios para el desarrollo de esta competencia docente son:

- **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

Según el MRCDD un docente con nivel B2 en esta competencia...	
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.

Copyright 2026

Final



Copyright 2026

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:

Copyright 2026

- 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 trasmitir 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.

Copyright 2026

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,

Copyright 2026

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 muchas 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: compraventa 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.

Copyright 2026

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.

Copyright 2026

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, cada 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

Copyright 2026

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 phising, 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.

Copyright 2026

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 (Phising).
- 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/)

Copyright 2026

Huella digital

Huella digital:

La huella digital es el rastro de información que dejamos en Internet a través de nuestra navegación y actividades en línea. Esta huella contribuye a nuestra identidad digital, que es la información sobre nosotros que se puede encontrar en Internet y que puede afectar positiva o negativamente a nuestra reputación en línea. Es imposible no dejar una huella digital, incluso si somos solo espectadores pasivos en línea. Muchos de estos datos se recopilan de manera pasiva e inconsciente, a través de cookies y otras técnicas de seguimiento. Sin embargo, también proporcionamos datos de manera activa y consciente al registrarnos en servicios y aplicaciones en línea. Es posible controlar nuestra huella digital mediante el uso de herramientas y aplicaciones específicas y leyendo las políticas de privacidad y cookies antes de aceptarlas.

Identidad digital:

La identidad digital es la información que se encuentra en internet sobre una persona, ya sea de forma directa o indirecta. Esta información puede ser interpretada a través de datos o metadatos, y puede ser vista por máquinas o por otras personas a través de buscadores como Google. Muchas veces, la información que compartimos en las redes sociales es deliberadamente pública, pero esto afecta nuestra privacidad y reputación en línea. Es importante ser conscientes de nuestra identidad digital y tratar de influir en ella de manera positiva, ya que gestionar nuestra identidad digital es una competencia digital básica que todos deberíamos desarrollar.

Egosurfing:

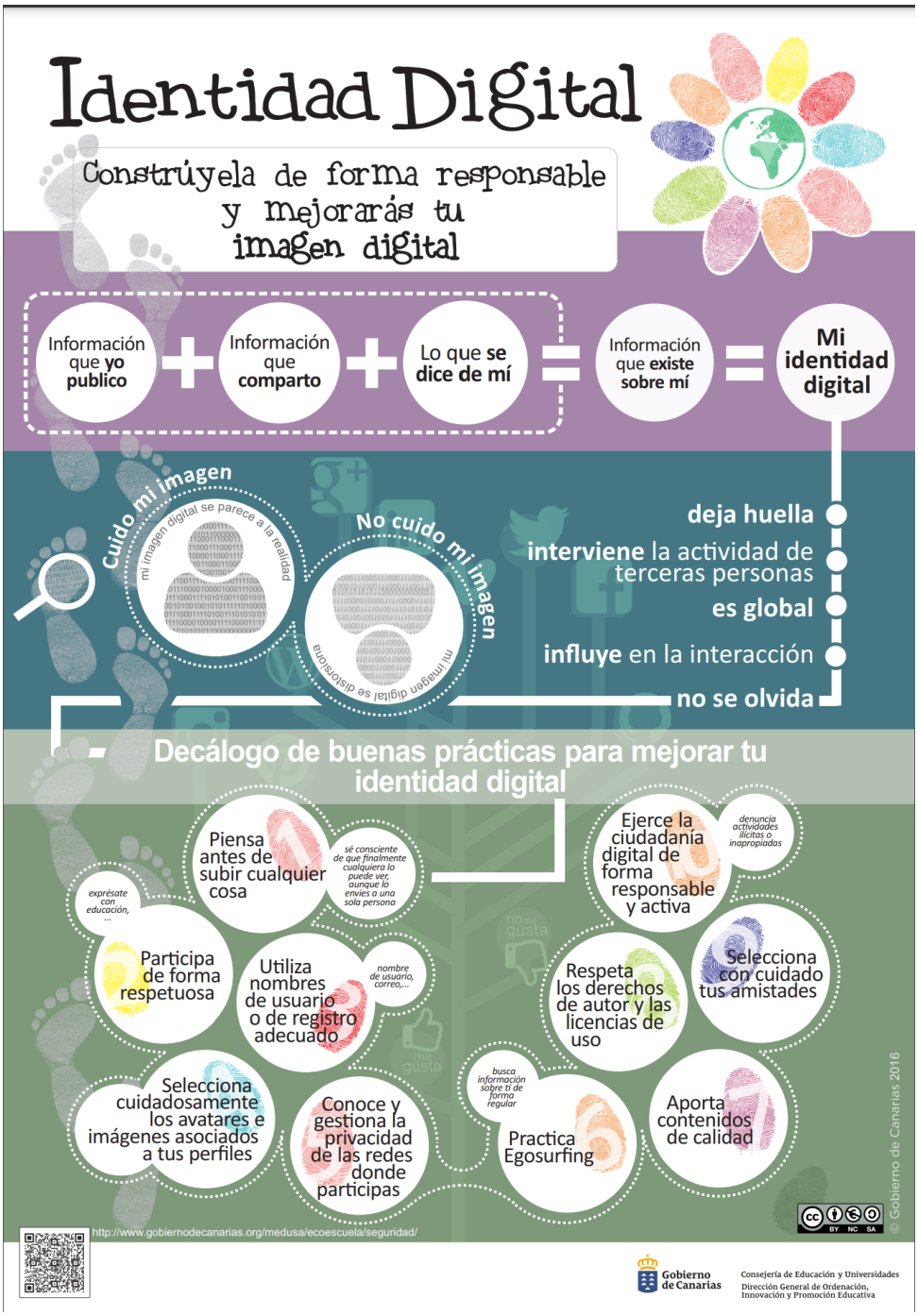
El *egosurfing* es el acto de buscar información sobre uno mismo en Internet. Es una forma de monitorear la reputación en línea, ya que permite a las personas conocer cómo se presentan a sí mismas en la red y cómo son percibidas por otros. El egosurfing puede ayudar a detectar contenido inapropiado o inexacto y tomar medidas para corregirlo o eliminarlo. También puede ayudar a las personas a ser más conscientes de su presencia en línea y tomar medidas para gestionar su identidad digital.

Es imprescindible que nuestro alumnado comprenda la gran **diferencia** que existe entre un **perfil profesional y uno personal en las RR.SS**. Como hemos explicado anteriormente, nos encontramos en un momento de nuestra historia en el que la conectividad y la digitalización han cobrado una importancia capital. Empresas y organizaciones van a consultar nuestros datos,

Copyright 2026

nuestra “identidad digital”. Está en nuestras manos ayudar a las nuevas generaciones en la creación de un perfil apto para el público profesional, en el cual sean ellos mismos los curadores del contenido personal que comparten.

Dividir ambos perfiles les permitirá filtrar la información que quieren compartir dependiendo del público potencial.



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