FORMACIÓN ENIDENTIDAD DIGITAL SEGURA EN ADULTOS

Grado en Pedagogía

Autor: Jesús Márquez Papaleo

Tutora: Raquel Sánchez Barragán

Modalidad de propuesta de creación de recursos educativos, formativos o didácticos

Resumen

En el presente documento se detalla un Trabajo de Fin de Grado (T.F.G) donde se recopila gran parte de la literatura científica acerca de la identidad digital y su gestión de manera segura y cívica siendo los adultos la población diana. Del mismo modo, se hace un breve alegato de qué planes tienen las autoridades mundiales como la Organización de las Naciones Unidas con los Objetivos de Desarrollo Sostenible y los diferentes planes de actuación de las diversas organizaciones europeas como españolas en relación con la identidad digital de la ciudadanía, analizando acerca de qué visión tienen sobre la identidad digital y que planes fomentan su uso. En segundo lugar, se entrega como recurso, una acción formativa de veinte horas de formación, diseñado desde el Exelearning (software de diseño de contenidos educativos) para fomentar entre la población adulta, la gestión segura de sus identidades digitales en la red. Dicha acción formativa permite una navegación sencilla para reducir la brecha digital de la población adulta y se publicará en https://identidad-digital-segura.on.drv.tw/Identidad_Digital/

Palabras claves

Alfabetización Tecnológica, Educación Tecnológica, Identidad Digital, Objetivos de Desarrollo Sostenible, Blockchain, Ciberseguridad.

Abstract:

This document details a Final Degree Project (T.F.G) where a large part of the scientific literature on digital identity and its management in a safe and civic manner is compiled, with adults being the target population. In the same way, a brief statement about what plans world authorities, such as the United Nations Organization, have according to the Sustainable Development Goals, the different action plans of the various European and Spanish organizations in relation to the digital identity of the citizenship, analysing what vision they have about digital identity and what plans encourage its use. Secondly, twenty hours training action, designed from Exelearning (educational content design software) is delivered as a resource to encourage the safe management of their digital identities on the network among the adult population. This training action allows an easy navigation, that helps to reduce the digital gap of the adult population. It will be published "https://identidad-digital-segura.on.drv.tw/Identidad_Digital/" website.

Keywords

Technological Literacy, Technology Education, Digital Identity, Sustainable Development Goals, Blockchain, Cybersecurity.

ÍNDICE

1. INTRODUCCIÓN Y JUSTIFICACIÓN

Nos encontramos en un momento determinante en la historia donde la disrupción tecnológica juega un gran papel en la transformación digital y social en la que el mundo está inmersa, la cual, se encuentra mucho más avanzada que las propias leyes internacionales que abogan por la protección y seguridad a los internautas. Vivimos en una era donde de las diez mayores empresas del mundo, siete son tecnológicas, y donde el podio lo comparten los tres gigantes norteamericanos de internet; como son Alphabet (empresa que entre sus servicios se encuentra el buscador Google), Microsoft, y a la cabeza, la multinacional del logo con la manzana mordida, Apple.

En una sociedad del conocimiento donde los países más desarrollados hablan del "derecho a internet" como un derecho básico de libertad y democracia; y donde el comercio electrónico cada vez es más habitual, nuestra presencia en la red aumenta día tras día a través de nuestros movimientos en la red, o lo que comúnmente se conoce como "huella digital". Por tanto, la formación en identidad digital es imprescindible para la ciudadanía digital del presente y el futuro. Desde la educación, debemos diseñar experiencias de aprendizaje que fomenten en la sociedad el ser consecuentes con el rastro digital que dejamos en internet y cuál es la imagen que dejamos de nosotros mismos en la red.

2. MARCO TEÓRICO

2.1. Introducción.

Tras la época de pandemia por Sars_Covs_2, la Unión Europea ha establecido una nueva hoja de ruta no solo en política económica sino en toda su política interior. Hablamos de la transformación de todo el tejido europeo hacia energías más limpias, sociedades más democráticas, medidas para la inclusión de personas desfavorecidas y hacia la transformación digital (Comisión Europea y la Dirección General de Redes de Comunicación, Contenido y Tecnologías, 2021).

Las pretensiones de Europa son claras, es necesario que sus ciudadanos adquieran competencias digitales, no solo porque la pandemia haya acelerado el proceso hacia el teletrabajo o para hacer la vida más fácil a sus ciudadanos con las compras online, socializar, etcétera; es el punto de partida hacia sociedades digitalmente competentes e inteligentes, consiste en generar una sociedad democrática y accesible en el espacio virtual.

Sin embargo, estas medidas entrañan riesgos para la población. Vivimos una situación compleja y abrumadora, donde gran parte de la población no conoce cómo funcionan las tecnologías digitales y su uso se restringe a actividades muy básicas como socializar a través de redes sociales y efectuar algún tipo de búsqueda por la red.

Este modelo de empleo de las TIC (Tecnologías de la Información y Comunicación) deja entreabierta la puerta a recibir ciberataques y otras amenazas (como hablaremos más adelante) que afectan a los individuos y las empresas. Según Ausín y Robles Carrillo (2021), con la llegada del "internet de las cosas" va a suponer una mayor expansión del consumo y una mayor exposición de nuestros datos personales, generando un descontrol de nuestra huella digital y de quienes somos por todo internet. Las autoras conectan todas las bondades de la información que cedemos, ya que se utilizará en los ámbitos sociales, movilidad, finanzas, entre otros. Sin embargo, ¿para qué otros fines pueden ser utilizados nuestros datos por parte de empresas y estados?

Asimismo, dado que son nuestros datos personales ¿es igualitario el servicio gratuito por la exposición de datos personales? ¿Qué estamos dispuestos a pagar en caso de no ofrecerlos? ¿Disponer de la información de lo que hacen con nuestros datos personales no les parece un derecho fundamental? Normalmente, si perdemos la cartera, llamamos para cancelar la tarjeta del banco por miedo a que nos roben el dinero, o vamos a comisaría para denunciar el robo de nuestros datos ¿por qué no ocurre igual en internet?

Defendemos el derecho a la protección de los datos personales, no solo desde las leyes fundamentales de la privacidad, sino desde el derecho a la libertad sin control. Hurtados Martos (2020) plantea que poseer una identidad digital es un derecho fundamental para la libertad individual ya que esta es la que da acceso sin restricción a los derechos y servicios básicos de hoy día, tales como el derecho a una educación (inscripción escolar), derecho a

sufragio, a atención médica, y a un largo etcétera, lo cual hace que a nivel legislativo, sea difícil de redactar sin coartar la libertad que ofrece la red online.

Por ello, Fernández Burgueño (2012) habla de que la protección jurídica hacia la identidad digital es cada vez mayor, es un derecho de cada persona física a existir en internet en cualquiera de las maneras y poder llevar una vida tanto offline como online. Asimismo, contempla un derecho fundamental que como su nombre indica, ha sido olvidado, y es el derecho al olvido, el cual permite un enorme control del individuo físico sobre la información que conforma la identidad y reputación online de la persona.

Tal y como indican Ausín y Robles Carrillo (2021), la revolución tecnológica debe ir acompañada de una revolución jurídica y ética. La tecnología parte de estar al servicio de la humanidad y los conceptos de justicia y ética, son constructos sociales plenamente subjetivos y que dependen de cada cultura o civilización. Por tanto, hablamos de que las tecnologías deben adaptarse a los cambios y a las necesidades actuales para que puedan ser eficaces.

Desde una visión más pedagógica, Muñoz-Rodríguez, Torrijos Fincias, Serrate González y Murciano Hueso (2020) contemplan la necesidad de diseñar acciones formativas socio-educativas para dar lugar a aprendizajes en habilidades sociales y comunicativas en el entorno virtual, proporcionando la oportunidad de educar a una ciudadanía digital en valores democráticos.

2.2. Identidad digital.

2.2.1. Conceptualización de la identidad digital.

El término de Identidad Digital se empieza a acuñar en 1990 cuando comienzan a utilizarse los ordenadores personales, sin embargo, según Pérez Subías (2012), con la llegada de las redes sociales y los smartphones, se despliega todo un grueso de investigaciones sobre esta idea. El autor argumenta sus afirmaciones justificando que estas nuevas tecnologías impulsan todo un sistema de conexiones digitales las cuales permiten interactuar entre distintas identidades para socializar, colaborar y ser totalmente omnipresentes.

Los autores muestran una gran diversidad de concepciones de lo que realmente es la identidad digital, aunque todos concluyen en ser una construcción compleja (Giones-Valls y Serrat-Brustenga, 2010) de datos tanto intrínsecos de la persona física o jurídica (Fernández Burgueño, 2012) como parte de un sistema social (Giones-Valls y Serrat-Brustenga (2010) y Merchán Murillo (2021)).

Esta información personal, tal y como puede ser la huella digital, se guardan en ficheros que adquieren características de longitud fija a través de un *hash* (método de encriptación de la información), los cuales son completamente únicos de cada entidad, y que por tanto, permite que dentro de los sistemas electrónicos (tal y como veremos más adelante con el *Blockchain*), el usuario sea identificado de manera segura (Merchán Murillo, 2021).

En la actualidad, la identidad digital no logra limitarse dentro del sistema cibernético ya que algunos autores como Fernández Burgueño (2012) y Hurtados Martos (2020) también la identifican en el *offline*. Este último, desglosa el concepto desde la información *offline* del sujeto, la huella digital que este tiene y la reputación *online* que le precede. Por otro lado, Giones-Valls y Serrat-Brustenga (2010) es más holístico, y la taxonomiza en la suma de quiénes queremos ser, cómo queremos que nos perciban y el cómo nos perciben, siendo más relevante la imagen que queremos dar a terceras personas, estando muy en sintonía con las ideas de Fernández Burgueño (2012).

Por último, autores internacionales como Rodgers y Scott, 2008, citado en Engeness, 2020)) que la identidad digital (de los docentes, aunque puede extrapolarse a todos los ámbitos), es una competencia digital (citado de Instefjord and Munthe (2017) y Røkenes and Krumsvik (2016)) que puede estar influenciada por los contextos, por las relaciones o interacciones, por el tiempo y por el significado del cual dotemos a nuestra propia identidad. Por tanto, el mismo autor cita de Gorospe et al (2015) y de Robson (2018), que hablamos de un concepto en constante cambio y fluctuación, por el cual, puede llegar a reinterpretarse todo el sistema de valores de la persona o entidad conforme más interactúan.

2.2.2. Características de la identidad digital.

Según Allison, Currall, Moss y Stuart (2005) se detalla que la identidad digital posee los mismos elementos, y que, pueden llegar a ser equiparables a la identidad personal o

psicológica, tan solo que en el mundo digital, todo el proceso de interacción y almacenaje de la información se desarrolla más eficientemente debido a las Tecnologías de la información y la comunicación (TIC).

Según otros autores como Castañeda y Camacho (2012), podríamos fragmentar la identidad digital en tres partes:

- Parte personal: Se le confiere la importancia a qué parte de mí muestro a los demás.
- Parte social A: Basada en quienes son las personas que configuran mi identidad personal o pertenecen a nuestra red de aprendizaje. Son aquellas personas (otras identidades digitales) que "seguimos" en redes sociales, y con las que compartimos aficiones, gustos…en definitiva, con quienes tenemos un contacto digital estrecho.
- Parte social B: Enfocada en las identidades que son o fueron influidas por nosotros, ya sean o no personas íntimas. Nosotros somos los que "distribuimos la información", aunque, se puede llegar a dar el caso que sus "voces" tengan un mayor impacto en la red y podamos ser susceptibles a presentar una mala "imagen" personal en Internet.

Según la Biblioteca Universitaria de la Universidad de Alicante (2018), encontramos siete características que caracterizan a la identidad digital:

- Es esencialmente social, ya que su construcción se asienta en la navegación e interacción con el resto de usuarios.
- Como vimos en la parte social B de Castañeda y Camacho (2012), la información puede ser muy volátil, por lo que la identidad digital es algo subjetivo, cada persona lee e interpreta en función de sus esquemas de pensamiento. Asimismo, hablamos de que es compuesta ya que no solo se compone por la información de una persona sino que se construye desde la interacción con el resto de identidades.
- Las define como valiosas ya que puede resultar de utilidad a las empresas.
- La identidad digital no solo actúa en el ámbito cibernético sino que también puede tener efectos en la vida real.
- Está en constante evolución por lo que decimos que la identidad digital es dinámica.

2.2.3. Construcción de la identidad digital.

Para Pérez Subías (2012) es fundamental para gestionar de manera adecuada nuestra identidad digital el ser conocedores de cómo se genera o construye, ya que somos agentes activos de nuestra propia identidad por lo que somos imprescindibles para su diseño y conformación, además, tal proceso de reflexión, es una oportunidad de aprendizaje propio.

Por otro lado, el mismo autor hace referencia a que podemos tomar distintas medidas a la hora de construirla con mayor o menor privacidad, siendo el caso de poder mantener distintos perfiles en internet los cuales no se encuentren entrecruzados ((Canevacci (2004), Aparici y Osuna Acedo (2013), Nagy y Koles (2014) y Antón Cuadrado y Levratto (2021)). Asimismo, la persona física es el elemento diferencial que decide en qué webs o aplicaciones nos registramos y que niveles de privacidad nos interesa.

En consonancia a estas ideas, Giones-Valls y Serrat-Brustenga (2010) afirman que nuestra identidad digital llega a construirse a través de la participación activa en internet, aportando contenidos a las redes sociales o con la creación de recursos digitales. La clave de la buena gestión de nuestra identidad es que haya homogeneidad entre la corpórea y la cibernética, aunque nuestra identidad puede verse alterada por el desarrollo de las nuevas tecnologías y por la actitud que mantenemos en la red. Tal y como indica Antón Cuadrado y Levratto (2021) citando a Hall, (2003), el intercambio de información y las conexiones entre distintos perfiles hace que nuestra identidad cambie en menor o mayor medida.

Por ende, Ausín y Robles Carrillo (2021) determinan que la construcción de la identidad digital se da gracias a un proceso de “datificación” donde nuestra actividad se transforma en datos que las computadoras pueden manejar para que puedan ser medidos, integrados y analizados por una inteligencia artificial. Este proceso corre al cargo de una IMS (Identification Management System) donde se integra un operativo para la identificación y gestión de la propia identidad digital de cada individuo u organización de manera segura (Hansen, Schwartz y Cooper, 2008, citado por Hurtados Martos, 2020). Este sistema es el encargado de la autorización de acceso a aplicaciones y webs en las que estamos inscritos y nos permite navegar por las mismas.

Según Ausín y Robles Carrillo (2021), la digitalización de estos datos, logra darse gracias los avances tecnológicos, los cuales permiten recoger información tales como:

- Nuestra geo-localización.
- Las interacciones que tenemos con otros usuarios, donde mostramos nuestros pensamientos, emociones y otros intangibles.
- Datos biológicos (huella dactilar, los pasos que damos, el ritmo del corazón, oxigeno en sangre, etc.) e incluso nuestros hábitos y rutinas.
- Información personal e íntima, gracias a los chips que poseen los dispositivos de uso cotidiano (el llamado Internet de las Cosas), los cuales registran nuestra actividad diaria y nos crean un perfil ajustado a nosotros, detectando nuestras necesidades y ofreciéndonos recursos e información relevante.

2.2.4. Amenazas a la identidad digital en la red.

De todo esto, podemos apreciar que el ritmo de innovación que están desarrollando las industrias tecnológicas es vertiginoso, lo cual, resulta muy beneficioso para facilitar la vida de las personas como para generar un mayor bienestar en ellas. Sin embargo, el acceso a las nuevas tecnologías se ve mermado por las deficiencias de la ciudadanía en competencias digitales (Giones-Valls y Serrat-Brustenga, 2010), de ahí nace el término comúnmente conocido como brecha digital. Supone no solo un problema de malestar por aislamiento o exclusión sino de como afirma Hurtados Martos (2020), se trata de una problemática que roza lo ético y legal para la ciudadanía, planteando serios problemas de gestión de la identidad digital de manera eficaz para la participación ciudadana en la red para aquellos colectivos más vulnerables los cuales sean analfabetos digitales.

Asimismo, un hecho que ha tenido una enorme repercusión ciudadana, legal y mediática en los tribunales tanto europeos como americanos, fue por la venta por parte de empresas como *Facebook*[1] (actualmente *Meta*) de sus datos de usuarios, principalmente con el objetivo de lucrarse a costa de su enorme fuerza como red social. Según el Incibe[2] (2016), este tipo de actividad económica daña a la imagen y al prestigio de la empresa ya que hablamos de información comprometida y confidencial.

[1] Colomé, J. P. (2018, 20 diciembre). Facebook compartía datos sensibles de sus usuarios con más de 150 grandes empresas. ElPai-s.com. https://elpais.com/tecnologia/2018/12/19/actualidad/1545221673_589059.html
[2] Instituto Nacional de Ciberseguridad

En contraposición, podría darse otro tipo de pérdidas de la información, y esta vez, ocurre de manera no autorizada. Estas pueden darse a través del espionaje industrial donde se usan ciberataques con virus, malwares u otros tipos de ataque como los DDos[3] (ataque de denegación de servicio), que permiten el robo de información sensible de los equipos de la organización o como en el último caso, son capaces de cerrar el acceso para la autentificación del usuario. Ante estas amenazas, las empresas deben formar a sus empleados en ciberseguridad como medida de prevención y de mitigación de ciberataques (Hurtados Martos, 2020).

En lo que respecta a los usuarios, según el Incibe (2016) la gran amenaza que atenta contra la propia identidad digital es la suplantación de la identidad digital. Esta no solo puede darse de manera individual sino que puede llegar a atentar contra organizaciones tanto públicas como privadas[4]. Este tipo de ciberdelincuencia se da en mayor medida por dos tipos de técnicas:

- El phishing[5]: El ciberdelincuente es un estafador, el cual usurpa la identidad de empresas de confianza para la mayoría de la población. Su técnica se basa en el envío de emails, SMS, entre otros medios, con la peculiaridad de que suplanta las imágenes oficiales y enlaces web muy similares a las de la empresa víctima con el pretexto de que accedamos a su enlace o introduzcamos datos confidenciales, para así, apoderarse de nuestra identidad digital y poder realizar sus actividades maliciosas e ilícitas.
- El *pharming*: En este caso, la amenaza ya está en nuestro dispositivo electrónico. El atacante cambia el mecanismo que hace que cuando nosotros buscamos la web original (la de nuestro banco, por ejemplo), esos mecanismos se activan y te redirigen hacia una web muy similar.

Por último, el Incibe (2016) destaca otro método de dañar de manera más sencilla que los anteriores, las redes sociales y el poco control de las identidades digitales en ellas. Como hemos podido ver, la reputación o imagen que tienen los demás de nosotros forma parte de nuestra propia identidad. ¿Qué implica todo esto? Significa que todos somos susceptibles que

[3] Hidalgo Pérez, M. (2021, 22 noviembre). Un ciberataque mantiene en jaque a distintos medios de comunicación españoles desde el viernes. Elpais.com. https://elpais.com/tecnologia/2021-11-22/un-ciberataque-mantiene-en-jaque-a-distintos-medios-de-comunicacion-espanoles-desde-el-viernes.html

[4] Lázaro, F. (2022, 28 febrero). Hackean la página de Instagram del Estado Mayor de la Defensa. Elmundo.es. https://www.elmundo.es/espana/2022/02/28/621c93fee4d4d8eb228b45c1.html

[5] Refojos, M. (2021, 12 febrero). España, a la cabeza mundial en engaños, estafas y fraudes online. elperiodico. https://www.elperiodico.com/es/activos/innovadores/20210212/espana-cabeza-mundial-enganos-estafas-11513245

personas nos ataquen directamente a través de *trolls* (al español, podría traducirse como troleros o bromistas), *outofcontext* (fuera de contexto en inglés), entre otro tipo de prácticas muy habituales en las redes, que influyen de manera negativa en nuestra imagen digital y que puede ir a mayores, intensificando las burlas, insultos y otras formas de odio hacia una persona o entidad en particular.

2.3. Gestión de la identidad digital eficaz y segura.

Ante semejante nivel de amenaza, es muy entendible que ciertas personas tengan terror al uso de Internet, pero este tipo de acciones ilegales no nos suceden a todos y se reducen en gran medida si la ciudadanía presenta conocimientos en competencia digital, más específicamente en la gestión eficaz de sus identidades digitales. Esto plantea un reto educativo (Hipólito Ruiz, Fernández Ortega y Gil Higuera, 2017) pero es necesario abordarlo para lograr la participación social plena en el entorno digital y el fomento de pautas de desarrollo de una identidad digital segura.

Para Ausín y Robles Carrillo (2021), para dicho proceso de aprendizaje, se requiere de una reflexión crítica que implique el diálogo ético entre cada comunidad. Principalmente, entre dos grandes cuestiones, la privacidad en la red (y el derecho al olvido) y el derecho a internet y a formar parte de este.

Por otro lado, Incibe (2016) recomienda algunas pautas que ayudan a prevenir las amenazas en las redes sociales, por ello, ha creado una guía de buenas prácticas, entre las cuales se muestran:

a) Cambio de contraseña frecuentemente.
b) Tener cuidado con las imágenes y nombres que mostramos en las redes.
c) No escribir tus opiniones como si fueran las únicas válidas sino tratar de ser asertivo.
d) Evitar dar opiniones políticas, religiosas e ideológicas.
e) Resulta recomendable realizar críticas constructivas y evitar las destructivas sin criterio ni razón.
f) Rehusar las discusiones en las redes sociales.

g) No mostrar información personal (no solo datos sino también dónde vives, dónde compras, donde trabajas…)

Asimismo, se destacan las recomendaciones para gestionar eficazmente la identidad digital de Giones-Valls y Serrat-Brustenga (2010). Entre ellas se encuentran que:

- La identidad digital es una habilidad que debe desarrollarse y aprender con una actitud positiva por la participación de la cultura digital, siendo siempre reflexivos de qué alcance tiene nuestra actividad para los otros y qué es lo que queremos aportar a la comunidad.
- Participar desde un tema en el que seamos "expertos", temas que nos gusten, sepamos mucho y/o estemos experimentados en ellos. Esto nos ayudará a ganar visibilidad por gente afín a nosotros y a ganar reputación.
- No aportar datos personales y solo darlos tras cerciorarse que el lugar es seguro o a personas cercanas de confianza.

2.3.1. La seguridad del *Blockchain*.

El *Blockchain* surge en 2009 con el surgimiento de la criptomoneda *Bitcoin*. Esta consiste en una cadena de bloques donde cada bloque presenta tres caras (PlayGround, 2018):

1) La información: Todos los datos que presenta el bloque (autor, fechas, cantidad si hablamos de dinero…)
2) El *Hash* del bloque: es el número de identificación del bloque. Este forma en función del contenido del bloque. Si el contenido cambia, el hash también lo hace.
3) El *Hash* del bloque anterior y posterior: Esto hace que se permita crear una cadena o un puzle, permiten la interconexión entre bloques.

Se trata de un sistema que permite la vigilancia y criptografía basada en redes de bloques donde se controla cada movimiento de manera individualizada. Esta tecnología es en la actualidad prácticamente invulnerable debido a la dificultad que entraña su descodificación. Asimismo, se le suma a que si los diferentes bloques que forman las redes, detectan algún gesto extraño o un cambio de información, el acceso al bloque se elimina ya que el hash del bloque y sus interconectores con el anterior y posterior bloque, cambia.

Según Millar (2018) citado en Merchán Murillo (2021) lo define como un registro autorizado para todos y cada uno de los usuarios de *Blockchain*, los cuales tienen "copias" (Merchán Murillo, 2021) encriptadas en sus ordenadores, lo cual hace que no exista necesidad de que la autorización se lleve a cabo por organismos gubernamentales o entidades globales.

Tras esto, conocemos cómo funciona pero no qué relación tiene el *Blockchain* con la gestión de las identidades digitales. Su respuesta es sencilla, Para Hurtados Martos (2020) esta tecnología genera una estructura unificada, operables a escala mundial y completamente segura ante fraudes de identidad cibernéticos, aportando seguridad a usuarios, entidades y el *Internet of Things*.

Otras de las grandes ventajas que ofrece según Baars (2016, citado en Hurtados Martos, 2020) es que por las propiedades naturales del sistema, se genera un sistema de identificación robusto y confiable, gracias en parte, a los avances en criptografía digital y el desarrollo de nuevas herramientas de gestión de identidad digital, enfocándose en el concepto de identidad digital descentralizada (del inglés, *DID*).

2.3.2. La visibilidad.

Para Giones-Valls y Serrat-Brustenga (2010, pp.5), la visibilidad se define por "toda actividad que genera el individuo en la red" y puede darse tanto de manera positiva como negativa. Esta puede crearse por uno mismo (a través de publicaciones) o por terceros (comentarios acerca de ti).

Asimismo, la visibilidad de la identidad digital es perfectamente medible a partir de la red de contactos que posee, sus seguidores, según qué tipo de contenidos publicamos y el tráfico que genera la cuenta (Urbalab Gandía, s. f.). Por tanto, debemos reflexionar cuál es nuestra marca personal y qué queremos mostrar de nosotros (Giones-Valls y Serrat-Brustenga, 2010) ya que nuestro comportamiento nos puede reportar valoraciones positivas como negativas.

2.3.3. La reputación.

Antes de comenzar con la reputación, habría que hacer un inciso para diferenciar a la huella de la sombra digital, además de a la reputación o identidad online. Autores como Golder y

Macy (2014) citado de Hurtados Martos (2020) asocian la huella digital a todos los datos e información que se añade en internet por parte de un usuario. En sintonía, se encuentran Byarugaba Agaba, Akindès y Bengtsson, (2016) citados una vez más en Hurtados Matos (2020) donde determinan que la sombra digital son los rastros que dejamos en la red en forma de *metadatos*[6]y que aportan trazabilidad de las interconexiones en la red.

Por tanto, la identidad online (o reputación o identidad 2.0) es la respuesta que nos da la red donde se muestra qué percepción tienen los demás de nosotros en función de nuestras publicaciones. Como hemos comentado, el qué piensan de nosotros (la reputación) es tan solo una parte de nuestra identidad digital y en consecuencia, es necesaria su matización para evitar errores terminológicos.

Para Lerderman (2008) citado en Fernández Burgueño (2012), la reputación es de las partes que más varían en nuestra identidad digital ya que los algoritmos de las redes sociales fluctúan en favor de conectar a cada persona con más usuarios a parte de los de su red cercana de contacto, lo que genera que la persona participe más en la red social y pase de consumidor a prosumidor (hacer del usuario un sujeto activo y por ende, un creador de contenido), además de consumidor de esta.

La esencia interconectada de internet puede hacer que ciertas identidades digitales se "viralicen", pudiendo llegar a ser muy mediáticas, siendo la reputación tanto beneficiosa como maliciosa para la persona física. Incibe (2016) apuesta por la monitorización de esta por parte de cada ciudadano y apoya el surgimiento de aplicaciones que clasifican y analizan la información para ayudar a mejorar la experiencia online del usuario.

2.3.4. La privacidad

Tal y como indica Aced et al (2009b) citado de Giones-Valls y Serrat-Brustenga (2010), la privacidad es uno de los elementos más importantes a tener en cuenta a la hora de la creación de perfiles en internet y por tanto, en la exposición de nuestra identidad digital tal vez de manera masiva.

[6] Conjunto de datos que hablan que proporcionan micro-información sobre otros datos mayores.

Debemos tener en cuenta que antes de comenzar en una red social, las plataformas nos piden nombre y apellidos, fecha de nacimiento, email o teléfono, una foto, etc. Alguno de estos datos luego son visibles a desconocidos, cosa que nos hace ser vulnerables tanto en el mundo digital como el analógico.

A esto le sumamos los datos que aportamos sin conocimiento como cómo comemos, qué nos gusta, que deporte hacemos, que serie seguimos, fotos de nuestros padres, nuestros hijos u otros familiares, y sin fin de elementos que son altamente personales e íntimos.

Por último, Giones-Valls y Serrat-Brustenga (2010) hace referencia a que también damos nuestro consentimiento a los proveedores de servicios web, aportando de manera inconsciente, nuestras conexiones, nuestro número de IP, donde prestamos mayor atención y clicamos, nuestra posición política, etc.

Ante esto, la Agencia Estatal Boletín Oficial del Estado. (2020, 11 noviembre) promulgó la "Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza". En el título tres denominado como "obligaciones de los prestadores de servicios electrónicos de confianza", se detallan los artículos del 8 al 11, donde se contempla la protección de los datos personales y las obligaciones, responsabilidades y limitaciones de los prestadores de servicios de confianza, con la intención de proteger bajo el paraguas legal, los datos de los usuarios españoles y limitar la exposición de estas.

2.3.5. La identidad digital soberana.

Continuando con las ideas de Baars (2016) sobre la creación de un sistema como el Blockchain, el cual permite una mejor gestión de la identidad digital más descentralizada. En realidad este pensamiento ha sido fruto de un largo proceso de desarrollo y una evolución no solo tecnológica sino humanista, donde se trata de satisfacer tres necesidades (Tobin y Reed, 2017):

1. Seguridad en cuestión de privacidad.
2. Control de la identidad digital y sobre con qué o quién compartimos nuestros datos.
3. Portabilidad.

Figura 1

Evolución de los modelos de identidad digital desde sus inicios hasta hoy.

Nota. Tobin y Reed (2017).

Para Tobin y Reed (2017), el primer modelo fue el centralizado y a día de hoy, es aún el mayoritario. Esto implica que una sola empresa o la plataforma se reserva todos nuestros datos para la portabilidad dentro de su propio dominio. El segundo modelo se le llamó federación[7], ya que permitía un mayor grado de portabilidad de la identidad digital hacia otros servicios ajenos a la empresa que lo emite.

Fue en 2008 cuando Kim Cameron, Reinhard Posch y Kai Rannenberg abren la puerta a una nueva concepción de la gestión de la identidad digital y por tanto a un nuevo modelo. El usuario pasa a ser el centro del sistema de gestión de las identidades digitales y es él el que tiene que guardar su información y gestionar a quién o quiénes proporcionársela.

La cuarta fase o modelo, es la más actual. Hablamos de la identidad digital soberana (self-sovereignidentity o SSI). Para ello, volvemos a rescatar las palabras de Baars (2016) citado en Hurtados Martos (2020) donde el autor considera que se trata de:

> Un sistema de identificación que permite a la persona que lo usa, de forma segura y legal, utilizar una identidad digital universal única para controlar la trasferencia y uso de los datos de los cuales es titular. Consiste en una identidad manejable, portable y de por vida para cualquier persona, entidad u objeto que no depende de ninguna autoridad centralizada proveedora de identidad y que nunca puede ser arrebatada ya que la identidad está basada en los principios de mismidad e ipseidad. (pp.118-119)

[7]Un ejemplo claro es el del programa OASIS perteneciente a la empresa SAML, el cual permite la autentificación de las identidades digitales entre dominios.

Es por este modelo que Allen (2016), fiel seguidor de este modelo, ha creado diez principios específicos para el uso de esta identidad soberana:

a) Existencia: Las identidades deben existir tanto en el plano real como el digital.
b) Control: Es el control de la propia identidad digital por parte de la persona física.
c) Acceso: Disponer de un acceso completo a sus datos personales.
d) Transparencia: El sistema debe ser transparente y de código abierto.
e) Persistencia: Las identidades deben ser duraderas pero sin contradecir el derecho al olvido.
f) Portabilidad: La información debe ser transportable por la persona y no debe ser obstruida o mantenida por terceros.
g) Interoperabilidad: Tener el mayor uso posible.
h) Consentimiento: Deben estar de acuerdo con el consentimiento de los datos y su uso.
i) Minimización: Evitar que se viralicen y divulguen datos de las identidades digitales.
j) Protección: Proteger el derecho de acceso a internet y ser partícipes de este.

2.4. Identidad digital y los Objetivos de Desarrollo Sostenible.

Los Objetivos de Desarrollo Sostenible nacieron en 2015 y fueron propuestos 17 objetivos por las Naciones Unidas para solventar las diferentes problemáticas en las que estamos envueltos la humanidad tales como el cambio climático, las desigualdades, la pobreza, la justicia y la paz mundial.

Al enfocarnos en un medio tan holístico como es el de internet, resulta muy difícil limitar los medios de acción con cada objetivo. Sin embargo, existen tres objetivos que demuestran ser esenciales en el uso de la identidad digital.

2.4.1. Objetivo 4: Educación de calidad

Este objetivo entraña garantizar una educación inclusiva y de calidad, promoviendo oportunidades de aprendizaje tales como la acción formativa que se endosa en este proyecto. Como sabemos, la educación digital dota no solo a menores sino a toda una población a adaptarse a la nueva era digital y a los cambios que surgen en las sociedades digitales

(Vicepresidencia Primera de Gobierno y Ministerio de Asuntos Económicos y Transformación Digital, 2021), que resultan ser aprendizajes para toda la vida.

Tal y como indica Hipólito Ruiz, Fernández Ortega y Gil Higuera (2017, pp.576)"La adquisición de competencias digitales es uno de los principios fundamentales para la adecuada promoción del sujeto en el entorno virtual". La pedagogía tiene una gran baza de trabajo ya que son necesarios para que el proceso educativo desarrolle el aprendizaje no sólo contenido técnico sino también axiológico de las tecnologías, asimismo, se requiere de la promoción de habilidades reflexivas y habilidades comunicativas que favorezcan los valores democráticos dentro de las comunidades digitales.

2.4.2. Objetivo 10: Reducción de las desigualdades

Tal y como indica Castells (2010), ex-ministro de universidades en España; Internet ha pasado a ser el tejido de la ciudadanía mundial, no es solo un medio sino un modo de organización social. Esto implica que las estructuras sociales comienzan a emerger dentro de las sociedades digitales, implicando por tanto, que el no acceso a un proceso de identificación digital en la red es una forma de exclusión de colectivos vulnerables. Asimismo, cada entidad debe ser un agente activo demostrando su participación en la red con el deber de hacerlo bajo los valores democráticos según corresponda su sociedad, aunque mostrando un pensamiento crítico (Hipólito Ruiz, Fernández Ortega y Gil Higuera, 2017).

Este movimiento cibernético tiene un enorme potencial en la destrucción de las barreras temporales o físicas que ocurren en el mundo corpóreo, los sistemas de identificación digital son la herramienta con el potencial para reducir enormemente la brecha digital mundial, ya que gracias a las TIC, los ciudadanos del mundo tienen un mayor acceso a la información y tienen los medios digitales a su disposición para actuar en la red en defensa de sus derechos a la libertad de opinión y a construir cultura digital (Hurtados Martos, 2020).

2.4.3. Objetivo 16: Promover sociedades justas, pacíficas e inclusivas

Continuando con estas ideas, las Naciones Unidas (2022) determinaron en sus objetivos específicos 16.7 enfocado en "Garantizar la adopción en todos los niveles de decisiones inclusivas, participativas y representativas que respondan a las necesidades" y en el 16.10, el

cual busca “Garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con las leyes nacionales y los acuerdos internacionales”.

Se requiere de la posesión de una identidad digital no sólo segura sino accesible a todos para conformar los derechos más esenciales de sus ciudadanos. Sin embargo, el objetivo 16.9 sólo engloba que "De aquí a 2030, proporcionar acceso a una identidad jurídica para todos, en particular mediante el registro de nacimientos", desestimando la importancia del derecho a internet y la importancia de participar en él.

2.4.4. Otros objetivos e influencia menos patente.

Para el ODS 1 basado en el fin de la pobreza, la identidad digital permite no solo la participación social sino también te da acceso a recursos financieros (como fondos de ayuda social), asimismo, poseer una identidad digital legal, te permite el acceso servicios básicos como la gestión online de propiedades o algunos servicios financieros.

Además, la gestión de una identidad digital cumple con el ODS 3 “salud y bienestar”, ya que permite el acceso a servicios de salud universal. Por otro lado, el tener tu propia voz a través de medios digitales permite la igualdad de género (ODS 5), especialmente en países menos desarrollados en materia de igualdad. Igualmente, permite la auto-gestión financiera necesaria para el empoderamiento femenino (Buvinic y O’Donnell, 2016, citado en Hurtados Martos, 2020) y el acceso igualitario al mercado de trabajo (ODS 8).

2.5. Europa en la década digital. El camino de la digitalización europea para 2030 en relación con las políticas de desarrollo de la identidad digital.

En lo que respecta al panorama europeo, La Unión Europea están implementados distintos programas de no solo recuperación económica sino también de desarrollo tecnológico para sus empresas y sus ciudadanos. Uno de estos programas se le llama “Programa Europa Digital 2021-2027” y se fundamenta en desarrollar las nuevas tecnologías como la Inteligencia Artificial, informática de alto rendimiento, ciberseguridad y el fomento de las

competencias digitales especializadas (Vicepresidencia Primera de Gobierno y Ministerio de Asuntos Económicos y Transformación Digital, 2021), entre ellas, las competencias destinadas a la gestión de las identidades digitales.

.

La Comisión Europea y la Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2021, pp.14-15) abre a la sociedad digital la capacidad de beneficiarse de los derechos fundamentales europeístas como son la libertad de expresión, la libertad de comercio (especialmente el digital), protección de los datos personales y la privacidad y el derecho intelectual.

En este momento, es necesario realizar un breve inciso de qué es la competencia digital para los organismos gubernamentales. Es por ello que se recoge de Ferrari (2013, citado de Arruti, Paños-Castro y Korres, 2021, pp.30), ya que aglutina en un mismo concepto la visión de la Unión Europea y de España. La definición es la siguiente:

> "conjunto de conocimientos, habilidades, actitudes, estrategias, valores y concienciación que se requieren cuando se usan las TIC y los medios digitales para realizar tareas, solucionar problemas, comunicar, gestionar información, colaborar, crear y compartir contenido y construir conocimiento de modo efectivo, eficiente, apropiado, crítico, creativo, autónomo, flexible, ético y reflexivo para el trabajo, el ocio, la participación, el aprendizaje, la socialización, el consumo y el empoderamiento."

Cerrado este paréntesis, existe otro plan que surgió a medida que tratamos de superar la pandemia y es el Plan de Recuperación presentado por la Comisión Europea para afrontar la era post- COVID-19 (Vicepresidencia Primera de Gobierno y Ministerio de Asuntos Económicos y Transformación Digital, 2021). Este plan resalta la especial importancia de la formación en competencias digitales y sostenibles para lograr a su vez el Plan de Acción de Educación Digital y una Nueva Agenda de Capacidades para Europa.

Asimismo, la presidenta Úrsula von der Leyen destacó durante el discurso del Estado de la Unión en 2020 que se debe garantizar la soberanía digital hasta 2030 gracias a los objetivos propuestos en los diferentes programas (Comisión Europea en España, s. f.). El objetivo es que se pueda crear un sistema inclusivo para participar en la vida democrática, se ofrezcan

servicios y herramientas digitales, dentro de una infraestructura segura, la cual proteja la privacidad de sus usuarios. Asimismo, se plantea la creación de un sistema de identidad fiable totalmente bajo control de los usuarios que permita el uso pleno de los servicios públicos a nivel europeo (Comisión Europea y Dirección General de Redes de Comunicación, Contenido y Tecnologías, 2021).

2.5.1. Políticas digitales europeas en España.

Por parte de la Vicepresidencia Primera de Gobierno y Ministerio de Asuntos Económicos y Transformación Digital (2021), el fomento del aprendizaje de las competencias digitales en España, es su mayor estandarte de desarrollo económico. Marca como un enclave estratégico la creación de un "Plan de Recuperación, Transformación y Resiliencia", muy similares a los europeos, donde la transición ecológica y el desarrollo digital sea su mayor fuente de futuros empleos y bienestar, añadiéndose a la problemática de la España vaciada.

La Comisión Europea inspecciona todos los desarrollos en política de transformación digital y desarrollo tecnológico con el Índice de la Economía y la Sociedad Digitales (DESI)[8] . En el informe de 2019, nuestro país se posicionaba en el puesto enésimo de los veintiocho países miembros participantes. La Comisión Europea en España (s. f.) preveía un cambio mayor en España, el cual se ha visto en el último DESI en 2021, donde este país ha ascendido al noveno puesto, superando la media europea en el apartado general y en cada uno de sus índices específicos (Comisión Europea, 2021a).

Por otro lado, para el Eurobarómetro de 2019, se entrevistó a 26,475 personas, de las cuales, 1,014 entrevistas fueron a la población española sobre la digitalización y el control de la información personal, la identidad digital y los servicios online (entre otros) dentro de la Unión Europea (Comisión Europea, 2019) Los resultados mostraron que el 67% de la población española consideraría muy útil disponer de un identificador digital único y seguro. Además, los datos con el resto de países de la Unión Europea se encuentran en consonancia siendo los resultados (64%).

[8] Comisión Europea. (2021b, 12 noviembre). DESI. ShapingEurope's Digital Future. Recuperado 6 de marzo de 2022, de https://digital-strategy.ec.europa.eu/en/policies/desi

Por último, según la Comisión Europea (2021b) también en España se publicó en 2020 un primer modelo de Gestión de Identidades Descentralizadas basadas en el Blockchain y otras tecnologías en colaboración con el país germano para la creación de un proyecto piloto europeo de identidad digital autosuficiente[9].

2.6. Marco de Competencias Digitales para la Ciudadanía (DigComp).

En el año 2006, según Arruti, Paños-Castro y Korres (2021), el parlamento europeo y el consejo europeo detallaron hasta ocho competencias digitales básicas para la vida, por tanto, desarrollaron un marco de referencia europeo denominado DigComp y otro individual para España, llamado INTEF.

El DigComp es una herramienta diseñada para mejorar las competencias digitales de la ciudadanía. Su primera publicación fue en 2013 y se ha convertido en un marco de referencia europeo para todos los países de la Unión Europea. No fue hasta 2016, cuando se implantó el DigComp 2.0. (Carretero Gómez, Vuorikari, Punie y AUPEX (2018))

Sin embargo, la última versión es el denominado DigComp 2.1 el cual busca el desarrollo de hasta ocho niveles de competencia digital en cada una de las cinco áreas de competencia donde se desarrolla. El objetivo de este modelo no es más que el de servir de ayuda a profesionales interesados en la implementación de estas competencias. (Carretero Gómez, Vuorikari, Punie y AUPEX (2018).

2.7. DigComp 2.1. Versión traducida al español por Carretero Gómez, Vuorikari, Punie y AUPEX (2018).

Casillas-Martín, Cabezas-González y García-Valcárcel Muñoz-Repiso (2022) realizaron un cuadro que resume la estructura de las competencias digitales del DigComp 2.1. En él, se nombraban las cinco áreas generales (excluyendo las micro-competencias que comprenden a cada una de las generales), los cuatro niveles de aptitud (con dos subniveles por nivel) y los

[9] Administración Electrónica. (2021, 3 junio). Portal de Administración Electrónica (PAe). administracionelectronica.gob.es. Recuperado 6 de marzo de 2022, de https://administracionelectronica.gob.es/general/error.htm;jsessionid=558EB00F2851C86E9161C061EA960663.node1_paeaplic

tres ámbitos de implementación de cada micro-competencia como son los de conocimiento (conceptual), capacidad (procedimental) y actitud (actitudinal).

Cuadro 1.

Estructura del DigComp 2.1.

Áreas	Niveles	Ámbitos
1. Información y alfabetización informacional. 2.Comunicación y colaboración 3.Creación de contenidos digitales 4.Seguridad 5.Resolución de problemas	1. Básico 2. Intermedio 3. Avanzado 4. Altamente especializado (dos subniveles por cada nivel)	1. Conocimiento 2. Capacidad 3. Actitud

Nota. Casillas-Martín, Cabezas-González y García-Valcárcel Muñoz-Repiso (2022)

2.7.1. Área de competencia número 2. Comunicación y colaboración online. Por Carretero Gómez, Vuorikari, Punie y AUPEX (2018)

El área de competencia 2 se denomina “comunicación y colaboración online” y destaca por ser el que más apartados presenta dentro de este DigComp 2.1. Las micro-áreas que presenta son las de:

- Interactuar a través de tecnologías digitales: Se enfoca en la interacción que se genera entre diversos dispositivos electrónicos y las aplicaciones que conllevan. Además de entender su distribución y gestión de la comunicación digital.
- Compartir a través de tecnologías digitales: Afronta el reto de compartir información con el resto de usuarios, ser prosumidor de contenido y recursos y tener habilidades de difusión de la información de manera que se respete el citado.
- Compromisos de la ciudadanía a través de tecnologías digitales: Su focalización es la de empoderar a la ciudadanía y hacerla partícipe de las tecnologías digitales adecuadas a sus necesidades.
- Colaboración a través de las tecnologías digitales: Su óptica es la de usar herramientas digitales para colaborar entre entidades y la creación conjunta de información y recursos.

- Comportamiento en la red: Destinada a conocer las *netiquette* o normas de comportamiento en entornos digitales, adoptando estrategias comunicativas diversas en función del público al que se dirige.
- Gestión de la identidad digital: Su orientación la describiremos a continuación, pero podemos adelantar que plantea la creación y gestión de una o varias identidades digitales con el objetivo de proteger la reputación de la persona a través del uso diferentes tecnologías, espacios y servicios digitales.

2.7.1.1. Apartado 2.6. Gestión de la identidad digital a través de los niveles de actitud.

Como ya sabemos, cada una de las micro-áreas se dividen en cuatro niveles con dos subniveles cada uno, por tanto, realizaremos un pequeño resumen comenzando a desarrollar desde el nivel básico en adelante.

A nivel básico

Se trata del nivel más simple y se destaca por el reconocer una identidad digital, describir alguna forma de proteger nuestra reputación online y reconocer que informaciones básicas estamos aportando a la red.

A nivel intermedio

Pasa por detectar diferentes identidades digitales, analizar y explicar diferentes formas de protección de la reputación online, describir en mayor medida la información que generamos según qué herramienta, servicio o entorno digital nos encontremos y poder manejarla.

A nivel avanzado

A este nivel ya podríamos ayudar a otras personas, ya que se fundamenta en saber manejar las identidades digitales y poder explicarlas a los demás, aplicar diferentes formas de proteger la reputación online y saber utilizar y modificar la información que generamos.

A nivel altamente especializado

Es el nivel más complejo de todos ya que requiere de la capacidad de resolución de problemas complejos con la identidad digital y la reputación online, emplear nuestros conocimientos técnicos para guiar a otros en la gestión de su identidad digital y el ser creativos para poder aportar ideas y procesos en el entorno donde nos desenvolvemos.

3. OBJETIVOS TFG

El objetivo general del presente trabajo es:

Diseñar un paquete formativo online abierto sobre identidad digital para personas adultas donde puedan alcanzar mayores destrezas digitales según los niveles de aptitud que se muestran el Marco de Competencias para la Ciudadanía DigComp 2.1.

Como objetivos específicos, los cuales son intrínsecos a este:

- Conocer la postura común de los países de la Unión Europea respecto a la identidad digital y la relación de esta con los Objetivos de Desarrollo Sostenible.
- Crear contenidos multimedia que facilite la accesibilidad del conocimiento a la población adulta y mejorar la comprensión de estos a través de actividades online de autoformación que capaciten a los usuarios a adquirir competencias relacionadas con la Identidad Digital.
- Fomentar actitudes seguras en la red de la ciudadanía española en edad adulta para lograr mayor conocimiento de internet, en ciberseguridad y en sus identidades sociales.

4. METODOLOGÍA

4.1. Fases de realización del TFG

El presente proyecto se encuentra dividido en cinco fases de desarrollo tutorizadas regularmente.

Cuadro 2.

Fases de realización del TFG. Diseño propio.

Fases	Guión didáctico	Guión técnico
Fase 1	● Selección de la necesidad educativa. ● Objetivos del proyecto ● Justificación del proyecto	● Selección del programa de creación de contenidos "exelearning" frente a otros.
Fase 2	● Diseño del marco teórico.	● Búsqueda de información en bases de datos científicas y páginas webs oficiales.
Fase 3	● Selección de metodología, objetivos específicos de la formación, competencias digitales implicadas y el método de evaluación a través del modelo de Kirkpatrick (1999, 2004).	● Primeros bocetos de la columna vertebral de la acción formativa.
Fase 4	● Diseño y creación de las actividades planteadas para la acción formativa.	● Creación de actividades de respuesta automática y de reflexión. ● Enriquecimiento de la acción formativa a través de distintos formatos multimedia (imágenes, videos, hiperenlaces, esquemas, ejercicios interactivos…)
Fase 5	● Entrega del proyecto	● Activación de la acción formativa en la web.

5. CREACIÓN DE UNA ACCIÓN FORMATIVA DIGITAL

5.1. Descripción del recurso formativo.

El recurso desarrollado consiste en una acción formativa completamente online y asíncrona, que entre sus características destacan su flexibilidad horaria y el fomento del trabajo autónomo adecuándose al tiempo y al ritmo de aprendizaje de cada uno. Sin embargo, requiere de tener voluntad, constancia y de autoexigencia para poder completarlo de manera adecuada.

La navegación a través del botón "siguiente" o a través del panel izquierdo es sencilla e intuitiva y no requiere de haber realizado una formación previa sobre su uso. La duración estimada de la formación es de 20 horas y se encontrará plenamente disponible en https://identidad-digital-segura.on.drv.tw/Identidad_Digital/ . Sin embargo, se recomienda proponer horarios regulares en horas apropiadas, evitando realizar la formación durante la noche.

En cuanto al grupo diana al que está enfocada esta formación, se trata de personas adultas entendiéndose un amplio rango de entre los 18 y 60 años, aunque al ser abierto y gratuito, puede llegar a extenderse en mayor o menor medida.

5.2. Objetivos

Entre los objetivos que plantea esta acción formativa son los de:

- Contribuir al conocimiento y la difusión de la relevancia de la identidad digital en el público adulto dentro de un contexto cibernético, para procurar mayor autocontrol y seguridad en la gestión eficaz de una o varias identidades digitales.
- Mostrar los diferentes programas europeos que contemplan la identidad digital dentro de sus propuestas y que relación tienen con los ODS.
- Promover las buenas prácticas en internet en lo que respecta al comportamiento de la población adulta en las redes sociales.

5.3. Competencias

Asimismo, se detallan las competencias que se pondrán a prueba durante la realización de la acción formativa. Se encuentran las siguientes:

Para el INTEF (2017) podríamos dividir las competencias clave para la gestión de la identidad digital segura en dos grandes bloques:

A. Gestión de la identidad digital. Comparte características con el DigComp 2.1 (Carretero Gómez, Vuorikari, Punie y AUPEX, 2018) e implica las siguientes competencias.

    a. Competencia general: Crear y gestionar una o varias identidades digitales, protegiendo su reputación digital y gestionar los datos de diferentes cuentas.

Cuadro 3.

Competencias específicas de gestión de la identidad.

Competencias específicas		
Nivel básico	**Nivel intermedio**	**Nivel avanzado**
Ser conocedor de los beneficios y riesgos que conlleva la identidad digital.	Crear diferentes identidades digitales y rastrear su huella digital. Gestionar la información que ofrecemos en las diversas identidades.	Gestión de diferentes identidades digitales en función del contexto y la finalidad. Capacidad para supervisar la información que producimos en interacción online y saber cómo protegernos a nosotros y a los demás.

Nota. Carretero Gómez, Vuorikari, Punie y AUPEX (2018)

B. Protección de datos personales e identidad digital.

a. Competencia general: Ser conocedor de la terminología usada en los diferentes servicios digitales, proteger nuestros datos digitales y la privacidad de los demás, además de desarrollar medidas para autoprotegerse de amenazas, fraudes y el ciberacoso.

Cuadro 4.

Competencias específicas en la protección de datos personales e identidad digital.

Competencias específicas		
Nivel básico	**Nivel intermedio**	**Nivel avanzado**
Es consciente del entorno donde es seguro compartir información y donde no.	Sabe cómo proteger su privacidad en línea y la de los demás. Reflexiona acerca de las estrategias de protección va a implantar.	Cambia a menudo la configuración de privacidad de determinados servicios en línea. Investiga y/o comparte información de cómo proteger la información sensible.

Nota. Carretero Gómez, Vuorikari, Punie y AUPEX (2018)

5.4. Temporalización

La acción formativa tiene asignada unas 20 horas de teleformación totales divididas de la siguiente manera:

- Bloque 1 “Acotación de la identidad digital”: 6 horas
- Bloque 2 “Gestión de la identidad digital eficaz y segura”: 6 horas
- Bloque 3 “Identidad digital y los Objetivos de Desarrollo Sostenible”: 5 horas
- Bloque 4 “Europa en la década digital”: 2 horas

- Bloque 5 “Evaluación por DigComp 2.1”: Este bloque está dividido en tres niveles de evaluación de competencia. Se aconseja empezar por el nivel básico hasta alcanzar el nivel que cada usuario quiera ponerse a prueba.
    - Nivel básico: 1 hora
    - Nivel intermedio: 2 horas
    - Nivel avanzado: 2 horas

5.5. Actividades

Las actividades a desarrollar son muy numerosas y se repiten, por tanto, se divide entre los tipos de actividades que encontraremos en la acción formativa online según Marcelo, Yot, Murillo y Mayor (2015):

Actividad asimilativa: Contenido en vídeo	
Objetivos	• Visualizar los vídeos insertados en la acción formativa. • Comprender los mensajes, instrucciones o ideas expuestas en los videos.
Desarrollo	Conforme avancen en la acción formativa se encontrarán con diferentes videos que hablarán de las distintas temáticas de cada apartado. Tan solo tienen que darle al *play* y dedicarles atención y comprensión a lo que ven y oyen.
Temporalización	De 2 a 10 minutos aprox.
Ubicación y denominación	**Unidad 1: Acotación de la identidad digital.** • Página de inicio: TEDx Talks. (2016, 3 marzo). El derecho al olvido | Teresa Rodríguez de las Heras | TEDxUPValència [Vídeo]. YouTube. https://www.youtube.com/watch?v=FkjMaJ8aNQA • Características de la identidad digital: Universidadurjc. (2018, 3 septiembre). *Módulo 1. Identidad digital* [Vídeo]. YouTube.

https://www.youtube.com/watch?v=SN5zBwVPktM

- Construcción de la identidad digital: LagartoShowOk. (2019, 28 octubre). *Qué hacen con nuestros datos en internet* [Vídeo]. YouTube. https://www.youtube.com/watch?v=oB8LYJtHcPw

- Amenazas a la identidad digital en la red:
    - ComputerHoy.com. (2019, 5 enero). ¿Qué es Phishing? [Vídeo]. YouTube. https://www.youtube.com/watch?v=Esde5ek_Yao

    - Banco Central. (2014, 8 septiembre). ¿Qué es el pharming? [Vídeo]. YouTube. https://www.youtube.com/watch?v=k3b5xzB3dds

Unidad 2: Gestión de la identidad digital eficaz y segura.

- La seguridad del Blockchain: Solo Para Inteligentes. (2018, 28 marzo). ¿QUÉ es y CÓMO funciona el BLOCKCHAIN? en 6 MINUTOS. TIENES QUE SABERLO ¡YA! [Vídeo]. YouTube. https://www.youtube.com/watch?v=C5NZnD12yjg

- La reputación: Entorno Simple. (2020, 7 mayo). Sombra, Huella, Identidad DIGITAL - Reputación digital y stalkers - #ESimple [Vídeo]. YouTube. https://www.youtube.com/watch?v=NarEyDYDCqU
- La privacidad: BBC News Mundo. (2018, 6 febrero). Cómo proteger tus datos en Internet [Vídeo]. YouTube. https://www.youtube.com/watch?v=XnhB7_5tLr8

- La identidad digital soberana: Blockchain Federal Argentina. (2019, 26 septiembre). *¿Qué es Blockchain? Capítulo 8: Identidad Digital Soberana* [Vídeo]. YouTube.

	https://www.youtube.com/watch?v=yG_m7XKqA28 **Unidad 3: Identidad digital y los Objetivos de Desarrollo Sostenible.** • Página de inicio: UNESCO en español. (2017, 26 enero). *Los Objetivos de Desarrollo Sostenible - qué son y cómo alcanzarlos* [Vídeo]. YouTube. https://www.youtube.com/watch?v=MCKH5xk8X-g **Unidad 4: Europa en la década digital.** • El camino de la digitalización europea para 2030 en relación con las políticas de desarrollo de la identidad digital: @CDTI_innovacion. (2020, 9 diciembre). Presentación de las Líneas estratégicas del programa Horizonte Europa 2021–2027 [Vídeo]. YouTube. https://www.youtube.com/watch?v=a2w62exE0Gw • Políticas digitales europeas en España: o Asuntos Económicos y Transformación Digital. (2021, 23 febrero). Plan Nacional de Competencias Digitales. España Digital 2025 [Vídeo]. YouTube. https://youtu.be/BdQ4Fw9uwg8 o Ayuntamiento de Madrid. (2021, 22 junio). Plan de Recuperación, Transformación y Resiliencia [Vídeo]. YouTube. https://www.youtube.com/watch?v=Vgo3wIkVvh0 **Unidad 5: Evaluación por DigComp 2.1** • Nivel avanzado: OSIseguridad. (2015b, noviembre 6). Cómo utilizar el egosurfing para proteger tu privacidad [Vídeo]. YouTube. https://www.youtube.com/watch?v=JOli4tNRelY

Actividad asimilativa: Esquemas	
Objetivos	● Clarificar las ideas desarrolladas para una mejor comprensión y estructuración del conocimiento.
Desarrollo	En el transcurso de la formación, el alumnado se encontrará con distintos esquemas los cuales podrán analizar y facilitar la comprensión de lo leído.
Temporalización	Indefinida.
Ubicación y denominación en la acción formativa	Se encuentra al inicio de la formación y se denomina “Estructura de la formación”

Actividad de gestión de la información: Inserción de textos y webs anexas	
Objetivos	● Proporcionar un mayor conocimiento extendiendo la información más allá de la acción formativa. ● Promocionar diferentes webs que fomenten la gestión segura de la identidad digital.
Desarrollo	Se trata de una actividad de lectura optativa para seguir mejorando o fortalecer las ideas principales. El contenido se mostrará a través de hiperenlaces que darán acceso directo a la visualización del contenido.
Temporalización	Indefinida

Actividad de gestión de la información: Podcast	
Objetivos	● Proporcionar un mayor conocimiento extendiendo la información más allá de la acción formativa. ● Reflexionar acerca de cómo de visible queremos que sea nuestra identidad digital.
Desarrollo	Consiste en escuchar un pequeño podcast de menos de 5 minutos donde explican cuáles son las ventajas y desventajas de la visibilidad online.
Temporalización	7-10 minutos.
Referencias bibliográficas	Paz C. (anfitrión). (2018). *Ventajas y desventajas de la Visibilidad On-Line* [Podcast]. Soundcloud. https://soundcloud.com/carmenpaz/podcast-38-ventajas-y-desventajas-de-la-visibilidad-on-line?utm_source=clipboard&utm_medium=text&utm_campaign=social_sharing

- Actividades comunicativas: Son aquellas actividades que están diseñadas para contestar (de forma asíncrona) a través del foro externo diseñado y que se encuentra anexado a la acción formativa.

Actividad comunicativa: Participación en foro	
Objetivos	● Enriquecerse de las reflexiones de otros estudiantes. ● Crear sus propias conclusiones acerca de diversos temas y compartirlas con los otros.
Desarrollo	Dentro del apartado “reflexiona y comparte” se evocará una cuestión relacionada con el tema que requerirá de la participación del usuario en el foro, el cual accederá a través de un hiperenlace.

Temporalización	5 - 20 minutos por participación.
Ubicación y denominación en la acción formativa	El acceso a cada sección del foro se redirige a través de hiperenlaces en cada una de las actividades. Aquí dejo el acceso general a todas sus secciones.

- Actividades evaluativas: Las usamos para evaluar al alumnado. El bloque cinco conforma distintos grupos de actividades divididos por niveles de competencias en identidad digital. Asimismo, en cada módulo, aparece la rúbrica en el inicio con lo que deberían aprender en cada módulo.

Actividad tipo evaluativas: Rosco	
Objetivos	• Evaluar el glosario específico necesario para el resto de la formación. • Recalcar conocimientos clave de la unidad 1.
Desarrollo	Es un juego de autocompletar muy famoso. El juego te proporciona una pista y la letra de inicio de la palabra por acertar. Por ejemplo, con la letra “c” y la pista “A los objetos cotidianos que tienen acceso a la red, pertenecen al Internet de las…”; el alumno/a pondrá la respuesta “cosas” en el caso de acertar. En el caso negativo, recibirá un feedback al instante.
Temporalización	La duración es de 5 minutos
Ubicación y denominación en la acción formativa	Test final de la unidad 1.

Actividad tipo evaluativas: Verdadero o falso	
Objetivos	● Valorar el nivel de comprensión de la segunda unidad didáctica.
Desarrollo	El procedimiento es muy sencillo. Aparecen 9 afirmaciones recalcadas en negrita, cada una tiene las opciones de verdadero o falso, el alumno seleccionará cual corresponda. En caso de error, recibirá un feedback automático donde se le explica cuál es el error.
Temporalización	5-10 minutos
Ubicación y denominación en la acción formativa	Test final de la unidad 2.

Actividad tipo evaluativas: Prueba de nivel básico	
Objetivos	● Reconocer una identidad digital. ● Describir formas simples de proteger la reputación. ● Detectar qué información generamos a través de nuestras búsquedas y publicaciones en redes.
Desarrollo	Las actividades planteadas son actividades de creación propia y están diseñadas para poner a prueba las competencias correspondientes al nivel básico. Entre las actividades encontramos: 1. Nombra una de tus identidades digitales y describe al menos tres formas de proteger tu reputación en la identidad digital que has nombrado. 2. Analiza tu identidad digital nombrada e indaga sobre tus búsquedas, tus gustos, a quienes sigues, dónde comentas, etc. Menciona al menos tres acciones o medidas que tomarás a partir de ahora para no mostrar información sensible en esta identidad digital.
Temporalización	60 minutos

Ubicación y denominación en la acción formativa	Dentro de la unidad didáctica 5, apartado de práctica de “nivel básico”.

Actividad tipo evaluativas: Prueba de nivel intermedio	
Objetivos	● Mostrar las distintas identidades digitales que poseemos. ● Analizar formas específicas de proteger la reputación online en esas identidades digitales. ● Manejar la información que generamos a través de herramientas, servicios o entornos digitales.
Desarrollo	Las actividades planteadas son actividades de creación propia y están diseñadas para poner a prueba las competencias correspondientes al nivel intermedio. Entre las actividades encontramos: 1. Detecta distintas identidades digitales en blogs, webs, correos electrónicos, redes sociales y en fotos o videos. Después determina una medida de protección de la reputación online por cada una de ellas. 2. Analiza tus redes sociales y busca posibles fallas en la seguridad de tu identidad digital, en especial de la reputación online. Puede empezar a buscar en tus videos e imágenes que compartes o en los comentarios que hayan sido hirientes hacia otros usuarios. Una vez los hayas localizado, ¿Qué puedes hacer para solucionarlo? ¡Compártelo en el foro con nosotros!
Temporalización	120 minutos

Ubicación y denominación en la acción formativa	Dentro de la unidad didáctica 5, apartado de práctica de "nivel intermedio".

Actividad tipo evaluativas: Prueba de nivel avanzado	
Objetivos	● Gestionar y utilizar varias identidades digitales. ● Explicar la forma adecuadamente proteger la reputación online. ● Utilizar y ser capaz de modificar la información que generamos en los entornos digitales.
Desarrollo	Las actividades planteadas son actividades de creación propia y están diseñadas para poner a prueba las competencias correspondientes al nivel avanzado. Entre las actividades encontramos: 1. Nombra tres herramientas, servicios o entornos digitales por internet que nos ayuden a gestionar diferentes identidades digitales. Explica las características que ofrecen cada una y justifica con cuál te quedarías. 2. Practica el egosurfing. ¿Conoces el término? Cuéntanos en el foro: ¿qué te ha aparecido al buscar sobre ti? ¿cómo vas a solucionarlo? Te dejamos este video muy clarificador que te ayudará a entender este método de proteger nuestra reputación digital y qué medidas puedes optar en el caso de encontrarte una sorpresa desagradable. La actividad contiene este video de Youtube para acercar este nuevo término al usuario. OSIseguridad. (2015, 6 noviembre). *Cómo utilizar el egosurfing para proteger tu privacidad* [Vídeo]. YouTube. https://www.youtube.com/watch?v=JOli4tNRelY&t=1s
Temporalización	120 minutos
Ubicación y denominación en la acción formativa	Dentro de la unidad didáctica 5, apartado de práctica de "nivel avanzado".

5.6. Aspectos a tener en cuenta.

A la hora de realizar la formación, es necesario tener ciertos criterios:

1. La acción formativa es completamente gratuita y abierta a todos los que quieran formarse en identidad digital segura. Por tanto, pueden acceder a ella tantas veces como quieran y realizar la formación todas las veces que deseen los usuarios.
2. Es totalmente imprescindible tener conexión a internet desde el momento en el que se accede a la formación.
3. Se recomienda el uso de un ordenador o tabletas para tener una mejor experiencia de aprendizaje, sin embargo, también es compatible con smartphones.
4. Se recomienda organizar el tiempo de manera individual y planificar las horas de aprendizaje.
5. Se aconseja tomar nota no solo del temario en texto sino también de toda la información multimedia recogida en la formación.
6. La acción tutorial solo se encontrará activa hasta el 23 de diciembre de 2022.
7. No se recomienda realizar la formación por debajo de las horas recomendadas por cada módulo ni finalizarlas en un solo día. Se aconseja cumplir con un calendario de al menos tres días desde su comienzo sin superar las ocho horas por día.
8. Una vez finalizado no se obtendrá ningún certificado o título que acredite haber superado la acción formativa.

5.7. Evaluación de los aprendizajes.

Considerando la Ley 30/2015, de 9 de septiembre, por la que se regula el Sistema de Formación Profesional para el Empleo en el Ámbito Laboral, se establecen las bases que sustentan el compromiso de la entidad que ofrece la formación a ejecutar diversas medidas de evaluación permanente, de calidad, de impacto y de satisfacción de los usuarios beneficiarios de la formación.

Por tanto, si consideramos la propuesta de Kirpatrick (1999, 2004) citado en Garín (2014) ya que nos ofrece un enfoque evaluativo mixto para ayudarnos a determinar la calidad de la formación y de los aprendizajes.

1. Nivel de reacción: Mide el grado de satisfacción de los participantes con la acción formativa. Asimismo, contempla que la acción formativa no sufra de un alto grado de absentismo. Por tanto, se ha desarrollado una encuesta de satisfacción a la conclusión de la formación que podrá ser entregada de forma optativa.

2. Nivel de aprendizaje: Evalúa las habilidades, conocimientos y actitudes logradas en la acción formativa. El hecho de ser una formación online plantea el reto de no únicamente enfrascarse en el saber o conocer sino de también potenciar las carencias frente a las formaciones presenciales, las cuales permiten mayor práctica y un formador presencial que traslade su saber ser (componente actitudinal). Por ello, se ejecutarán las siguientes evaluaciones:

    a. Rúbrica por nivel de competencia: Más enfocada en que el alumnado sea autónomo y tenga en consideración como mejorar su experiencia de aprendizaje para que estos lleguen a ser más significativos. Dentro de cada nivel de competencia del bloque 5, se mostrará al inicio una rúbrica para que los estudiantes tengan orientaciones acerca de qué y cómo deberían de darse las prácticas.
    b. Actividades de respuesta automática: Cada apartado de cada módulo presenta actividades interactivas que generan la respuesta correcta automática una vez se haya cumplimentado. Marcando en rojo los errores y justificando la respuesta para una mayor comprensión del error por parte del alumnado. Asimismo, al completar cada módulo habrá una actividad final a modo de cuestionario que funciona de la misma manera que las anteriores.
    c. Actividades prácticas evaluables disponibles al final de cada módulo y dentro de cada sección del bloque 5.Este tipo de actividades suscitan a la reflexión sobre el saber, el saber ser y el saber hacer acerca de la propia identidad digital y la de los demás.

3. Nivel de conducta: Plantea la evaluación de los cambios conductuales y en los hábitos en la vida del participante a largo plazo. Para contemplar estos cambios, a los usuarios que hayan podido dejar su teléfono o correo electrónico en la encuesta de satisfacción, se les realizará una pequeña entrevista que consta de las siguientes preguntas:
    a. ¿Qué tal? ¿Cómo se encuentra?
    b. ¿Qué cree usted que ha cambiado tras la formación?
    c. ¿Continúa contento con la formación que realizó?
    d. ¿Qué tal su nivel en identidad digital? ¿Piensa en volver a hacer la formación o mejorar su nivel competencial?
    e. ¿Han adquirido nuevos hábitos tras la formación?
    f. ¿Habrá mayor facilidad en las gestiones de la identidad digital relacionadas con el empleo?
    g. ¿Crees que han obtenido nuevos aprendizajes inferidos indirectamente por las formaciones?
    h. Tras dejar pasar todo este tiempo ¿Qué crees que le falta a nuestra formación? ¿En qué formaciones estaríais interesados de cara a un futuro próximo?

4. Nivel de resultados: Contempla el cómputo total de las evaluaciones hacia el usuario y la evaluación de la acción formativa en sí, como la calidad, el impacto alcanzado, próximas mejoras de esta, etc. Por ende, la mejor manera es la realización de una memoria en diciembre de 2023. El motivo de la fecha es la finalización del seguimiento el 23 de diciembre de 2022, la recopilación de los datos (la entrevista no se realiza hasta 6 meses después de la conclusión de este), el análisis y la expedición de los resultados de impacto de la acción formativa.

6. RESULTADOS Y CONCLUSIONES

En adelante, se presentan las características más bondadosas de este proyecto y las que requieren de algún tipo de cambio y necesitan ser perfeccionadas. Entre los puntos más fuertes de este proyecto son:

a) Dotar de difusión a la identidad digital entre la población española: Por desgracia, la identidad digital no ha cobrado fuerza en España a pesar de que está muy integrada en

nuestra vida cotidiana, contemplemos el hecho de tener una cuenta en Google o Facebook y las micro-identidades que implica todo ello. Este proyecto da visibilidad a la identidad digital no solo teóricamente sino que le aporta un sentido práctico y actitudinal y promueve un conocimiento más macro que dota a los estudiantes de herramientas para su gestión y la promoción de la seguridad.

b) Creación de un recurso digital: El diseño y creación de un recurso digital tiene tanto beneficios como inconvenientes, sin embargo, el hecho de promover la concienciación sobre las virtudes de la era digital dentro de una formación también digital nos permite un alto grado de complementariedad, favoreciendo además la inserción de todo tipo de herramientas pedagógicas digitales que favorezcan los aprendizajes significativos junto con un bajo nivel de absentismo.

Este apartado cumple con el objetivo general de este proyecto, en cual se dictaba lo siguiente: "Diseñar un paquete formativo online abierto en identidad digital para personas adultas donde puedan alcanzar mayores destrezas digitales según los niveles de aptitud que se muestran el Marco de Competencias para la Ciudadanía DigComp 2.1." Se puede acceder a la formación a través del siguiente enlace.

Dentro de la acción formativa, contemplamos los objetivos específicos ya que por ejemplo, limitamos el contenido escrito y priorizamos contenido multimedia, el apoyo visual ayuda a la comprensión y favorece la accesibilidad del conocimiento de la identidad digital en los adultos. También se responde a los objetivos donde se detalla la creciente postura de los organismos europeos y españoles con la identidad digital, además de su relación con los Objetivos de Desarrollo Sostenible.

La principal dificultad es la de trasladar las actitudes seguras al estudiantado. La ciberseguridad es una de las asignaturas pendientes de la población española, diversos estudios lo confirman, sin embargo, el objetivo propuesto fue tenido en cuenta y en todas las prácticas evaluativas contempla un apartado de ciberseguridad. Asimismo, tiene un apartado propio dentro de la acción formativa de la unidad primera, el cual es bastante extenso en comparación con otros apartados.

Por último, entre los puntos menos ventajosos de este proyecto, aun sabiendo que las acciones formativas online y gratuitas tienen acceso abierto a cualquiera que desee aprender, y por tanto, menos barreras al conocimiento y mayor capacidad para llegar a un gran público gracias a internet, el apartado de difusión de este proyecto es el más vago. En futuros proyectos debemos abordar como publicitar la acción formativa y dar mayores incentivos para que otras personas las realicen.

7. REFERENCIAS BIBLIOGRÁFICAS

Agencia Estatal Boletín Oficial del Estado. (2020, 11 noviembre). Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. Boe.es. Recuperado 12 de febrero de 2022, de https://www.boe.es/eli/es/l/2020/11/11/6

Allen, C. (2016, 26 abril). The Path to Self-Sovereign Identity. Lifewithalacrity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

Allison, A., Currall, J., Moss, M., y Stuart, S. (2005). Digital identity matters. Journal of the American Society for Information Science and Technology, 56(4), 364–372. https://doi.org/10.1002/asi.20112

Antón Cuadrado, R., y Levratto, V. (2021). La construcción de la identidad digital en las redes sociales: un estudio cuantitativo en Argentina y España. La imagen como elemento determinante en la identidad y acción digital. Revista Latinoamericana de Estudios sobre Cuerpos, Emociones y Sociedad, 36(13), 23–33. http://www.relaces.com.ar/index.php/relaces/article/view/448/428

Aparici, R., y Osuna-Acedo, S. (2013). La Cultura de la Participación. Revista Mediterránea de Comunicación, 4(2), 137–148. https://doi.org/10.14198/medcom2013.4.2.07

Arruti, A., Paños-Castro, J., &Korres, O. (2021). Análisis de contenido de la competencia digital en distintos marcos legislativos. Aloma: Revista de Psicología, Ciències de

l'Educació i de l'Esport, 38(2), 149–156. https://doi.org/10.51698/aloma.2020.38.2.149-156

Ausín, T., y Robles Carrillo, M. (2021). Ética y derecho en la revolución digital. Revista Diecisiete: Investigación Interdisciplinar para los Objetivos de Desarrollo Sostenible., 04(abril 2021), 15–28. https://doi.org/10.36852/2695-4427_2021_04.00

Baars, D., Moonen, H., van Sinderen, M., y Steenbergen, R. (2016, octubre). Towards Self-Sovereign Identity using Blockchain Technology (TFM). Rabobank. University of Twente. https://essay.utwente.nl/71274/

Biblioteca Universitaria de la Universidad de Alicante (2018, 14 septiembre). RUA: CI2 Básico (curso 2017–2018). Bloque 3. Identidad digital. Rua.ua. Recuperado 26 de febrero de 2022, de http://rua.ua.es/dspace/handle/10045/79589

Boletín Oficial del Estado. (2015, 10 septiembre). BOE.es - BOE-A-2015-9734 Ley 30/2015, de 9 de septiembre, por la que se regula el Sistema de Formación Profesional para el empleo en el ámbito laboral. boe.es. Recuperado 27 de marzo de 2022, de https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-9734

Canevacci, M. (2004). Etnografía web e identidades avatar. Nómadas, 21, 138–151. https://www.redalyc.org/pdf/1051/105117678012.pdf

Carretero Gómez, S., Vuorikari, R., Punie, Y., y AUPEX. (2018). DigComp 2.1: El marco de competencias digitales para ciudadanos con ocho niveles de competencia y ejemplos de uso. Editamás editorial. https://doi.org/10.2760/38842

Casillas-Martín, S., Cabezas-González, M., y García-Valcárcel Muñoz-Repiso, A. (2022). Influencia de variables sociofamiliares en la competencia digital en comunicación y colaboración: [Influence of socio-familial variables on digital competence in communication and collaboration]. Pixel-Bit, Revista de Medios y Educación, 63, 7–33. https://doi.org/10.12795/pixelbit.84595

Castañeda, L., y Camacho, M. (2012). Desvelando nuestra identidad digital. El Profesional de la Información, 21(4), 354–360. https://doi.org/10.3145/epi.2012.jul.04

Comisión Europea y Dirección General de Redes de Comunicación, Contenido y Tecnologías. (2021, marzo). Comunicación de la comisión al parlamento europeo, al consejo, al comité económico y social europeo y al comité de las regiones. Brújula Digital 2030: el enfoque de Europa para el Decenio Digital (N.o 52021DC0118). EUR-Lex. https://eur-lex.europa.eu/legal-content/es/TXT/?uri=CELEX%3A52021DC0118

Comisión Europea en España. (s. f.). Políticas digitales de la UE en España. Comisión Europea. Representación en España. Recuperado 12 de febrero de 2022, de https://spain.representation.ec.europa.eu/estrategias-y-prioridades/politicas-clave-de-la-ue-en-espana/politicas-digitales-de-la-ue-en-espana_es

Comisión Europea. (2019, diciembre). Eurobarómetro Especial. El efecto de la digitalización en nuestra vida diaria. (N.o 503). https://www.ospi.es/export/sites/ospi/documents/documentos/Eurobarometro_Digitalizacion_factsheet_Es_es.pdf

Comisión Europea. (2021). Índice de la Economía y la Sociedad Digitales (DESI) 2021. https://digital-strategy.ec.europa.eu/en/policies/countries-digitisation-performance

Engeness, I. (2020). Developing teachers' digital identity: towards the pedagogic design principles of digital environments to enhance students' learning in the 21st century. European Journal of Teacher Education, 44(1), 96–114. https://doi.org/10.1080/02619768.2020.1849129

Fernández Burgueño, P. (2012). Aspectos jurídicos de la identidad digital y la reputación online. adComunica: revista científica de estrategias, tendencias e innovación en comunicación, 3, 125–142. https://doi.org/10.6035/2174-0992.2012.3.8

GairínSallán, J. (2014). La Evaluación Del Impacto En Programas De Formación. Revista Iberoamericana sobre Calidad, Eficacia y Cambio en Educación, 8(5), 19–43. https://www.redalyc.org/pdf/551/55119084002.pdf

Giones-Valls, A., y Serrat-Brustenga, M. (2010). La gestión de la identidad digital: una nueva habilidad informacional y digital. *BiD: textos universitarios de biblioteconomía y documentación*, *24*(junio), 1–15. https://doi.org/10.1344/105.000001544

Hipólito Ruiz, N., Fernández Ortega, S., y Gil Higuera., N. (2017). Las TIC para, cómo y con la Educación Social. La Gestión de la identidad digital como competencia desde la Educación Social. RES: Revista de Educación Social, 24(Enero), 571–578. https://eduso.net/res/wp-content/uploads/documentos/986.pdf

Hurtados Martos, J. A. (2020). *La identidad digital, una herramienta para el desarrollo sostenible* [Trabajo Fin de Grado, Universidad de Córdoba]. https://www.uco.es/docencia_derecho/index.php/RAYDEM/article/viewFile/219/272

Identidad digital auto-soberana. (2021, 6 diciembre). En Wikipedia. https://es.wikipedia.org/wiki/Identidad_digital_auto-soberana

Incibe (Instituto Nacional de Ciberseguridad) (2016, marzo). Ciberseguridad en la identidad digital y la reputación online. Una guía de aproximación para el empresario. https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_ciberseguridad_identidad_online_metad_0.pdf

INTEF. (2017, septiembre). Marco común de competencia digital docente (Octubre, 2017). https://aprende.intef.es/sites/default/files/2018-05/2017_1020_Marco-Com%C3%BAn-de-Competencia-Digital-Docente.pdf

Marcelo, C., Yot, C., Murillo, P., y Mayor, C. (2015). Actividades de aprendizaje con tecnologías en la universidad. ¿Qué uso hacen los profesores? Profesorado, revista de currículum y formación del profesorado., 20(3), 283–312. https://recyt.fecyt.es/index.php/profesorado/article/view/54614

Merchán Murillo, A. (2021). Identidad digital Blockchain e Inteligencia Artificial: aspectos jurídicos de presente y futuro a debate. IUS ET SCIENTIA, 1(7), 183–203. https://doi.org/10.12795/ietscientia.2021.i01.12

Muñoz-Rodríguez, J. M., Torrijos Fincias, P., Serrate González, S., & Murciano Hueso, A. (2020). Entornos digitales, conectividad y educación. Percepción y gestión del tiempo en la construcción de la identidad digital de la juventud. Revista Española de Pedagogía, 78(277), 457–475. https://doi.org/10.22550/rep78-3-2020-07

Naciones Unidas. (2022, 3 febrero). 17 objetivos para transformar nuestro mundo. Objetivos de Desarrollo Sostenible. https://www.un.org/sustainabledevelopment/es/

Nagy, P., y Koles, B. (2014). The digital transformation of human identity. Convergence: The International Journal of Research into New Media Technologies, 20(3), 276–292. https://doi.org/10.1177/1354856514531532

Pérez Subías, M. (2012, 31 mayo). Identidad digital. Revista TELOS (Revista de Pensamiento, Sociedad y Tecnología), 91(Abril-Junio 2012). https://telos.fundaciontelefonica.com/archivo/numero091/identidad-digital/?output=pdf

PlayGround. (2018, 30 marzo). Qué es «Blockchain» en 5 minutos [Vídeo]. Youtube. https://www.youtube.com/watch?v=Yn8WGaO__ak

Tobin, A., & Reed, D. (2017). The Inevitable Rise of Self-Sovereign Identity. sovrin.org. https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf

Urbalab Gandía. (s. f.). Visibilidad. urbalabgandia.com. Recuperado 4 de marzo de 2022, de https://www.urbalabgandia.com/wp-content/uploads/autoaprenentatge-en-linia/16.Generacion_identidad_digital/visibilidad.html

Vicepresidencia Primera de Gobierno y Ministerio de Asuntos Económicos y Transformación Digital. (2021, enero). PLAN NACIONAL DE COMPETENCIAS DIGITALES.

Ministerio de Asuntos Económicos y Transformación Digital. https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_nacional_de_competencias_digitales.pdf

8. ANEXOS

8.1. Guía de usuario para acceder a la Teleformación.

Se ha realizado una guía para el acceso a la acción formativa y otra que explica cómo desenvolverse por ella. Se puede acceder a través del siguiente enlace.