El área Seguridad de la Competencia Digital: un estudio con método mixto en alumnado gallego de Educación Primaria

E. Vila-Couñago, U. Fernández-Regueira, y E. Pernas-Morado

***Title*— The Security area of the Digital Competence: a mixed method study in Galician primary education students.**

***Abstract*— This paper aims to evaluate the security area of digital competence in pre-adolescents schooled in primary education and understand the processes that interfere with the development of that area. A mixed research methodology is used through an exploratory sequential type design with a first qualitative phase (multiple case study) and a second quantitative phase (assessment test about security). Among the results obtained, highlights the family influence on the subcompetence of health protection, which is the one that worries families the most and in which the students get the highest score in the test carried out.**

***Index Terms*— Digital Competence, Digital divide, Digital security, Mixed Method Research.**

I. Introducción

El impacto de las nuevas tecnologías en las sociedades ha generado cambios en todos los ámbitos de la vida; de modo que la competencia digital (CD) se presenta como uno de los aprendizajes demandados por la sociedad contemporánea. Una situación que se evidencia y magnifica a raíz de los últimos acontecimientos, marcados por el confinamiento y las diferentes medidas adoptadas por los gobiernos a raíz de la crisis sanitaria propiciada por el COVID-19. La CD se torna ahora imprescindible para ejercer el teletrabajo, la teleformación, el ocio y también para mantener la conexión con la actualidad y los seres queridos. La falta de acceso y competencias amplifican hoy los riesgos que diversos autores ya apuntaban ante la brecha digital [1], [2]: desigualdades en función del género, desintegración social, marginación institucional, pérdida de nichos de socialización, infoxicación o alarma social, entre otros.

En este contexto, se han movilizado de urgencia diversas medidas y herramientas en diferentes sectores, entre ellos el educativo, con el objeto de continuar con la actividad diaria en este nuevo escenario. Si bien en el contexto actual se hacen eco preocupaciones relativas al acceso y la competencia instrumental –cuestiones básicas para garantizar la continuidad de la actividad educativa–, es necesario mantener en el centro del debate que la capacidad de realizar un uso inteligente, crítico y reflexivo de estas tecnologías se circunscribe en la interconexión y negociación entre las oportunidades y riesgos que entrañan [3]. Una negociación que en estos tiempos –de amplia exposición a herramientas y tecnologías adoptadas con urgencia y rapidez, normalización a nivel mundial de la recolección de datos con nuevos propósitos añadidos a los hasta ahora conocidos y la atención dirigida hacia la salud– plantea la e-seguridad y la CD en esta dimensión como prioridad.

II. La competencia digital de las y los preadolescentes: la dimensión seguridad

Este estudio adopta como marco de referencia el Proyecto DIGCOMP [4], cuya definición de la CD hace alusión a un aprendizaje que implica el empoderamiento cognitivo y la transferencia de los conocimientos a través del uso de herramientas digitales en diferentes contextos [5] de forma efectiva, eficiente, apropiada, crítica, creativa, autónoma, flexible, ética y reflexiva [4] para la resolución de problemas reales. En la CD se identifican cinco dimensiones: informacional, de comunicación, creación de contenido, seguridad y resolución de problemas. A su vez, estas áreas agrupan un total de 21 subcompetencias.

Los antecedentes manifiestan que es la dimensión relativa a la seguridad la que causa una mayor preocupación a las familias e instituciones que trabajan con menores en lo relativo a las tecnologías [3], [6], [7], [8], [9], [10]. Esta contempla cuatro subcompetencias [4]:

- La protección de dispositivos. Supone comprender los riesgos y amenazas en línea, conocer y ser capaz de adoptar medidas de seguridad para proteger los dispositivos y evitar el fraude en el uso de contraseñas, mostrando una actitud positiva pero realista en torno a los riesgos del uso en línea de las nuevas tecnologías.
- La protección de datos personales. Implica la comprensión de los términos y condiciones de privacidad, así como la garantía y protección de la misma a través del cuidado de los datos compartidos y la creación de la identidad digital propia y de otros/as, evitando situaciones de *ciberbullying*.
- La protección de la salud. Supone conocer y actuar conforme los riesgos de las nuevas tecnologías para la salud psicológica y física. Así como la relación

Esther Vila-Couñago es profesora ayudante doctora en el Dpto. de Pedagoxía e Didáctica (Área de Didáctica e Org. Escolar) en la Facultade de Ciencias da Educación de la Universidade de Santiago de Compostela (e-mail: esther.vila@usc.es). ORCID: 0000-0001-6407-463X.

Uxía Fernández-Regueira es estudiante predoctoral en la USC y profesora invitada en la Universidade de Vigo (e-mail: uxiafernandez.regueira@usc.es). ORCID: 0000-0003-2738-182X.

Eulogio Pernas-Morado es profesor en el Dpto. de Pedagoxía e Didáctica (Área de Didáctica e Org. Escolar) en la Facultade de Ciencias da Educación de la Universidade de Santiago de Compostela (e-mail: eulogio.pernas@usc.es). ORCID: 0000-0002-3311-2063.

DOI (Digital Object Identifier) Pendiente

existente entre la propia actuación y el bienestar de las/os demás.

- La protección del medio ambiente. Implica la conciencia sobre la relación existente entre el desarrollo tecnológico y el medioambiente; actuando de forma consecuente y eficiente.

Una versión posterior, denominada DIGCOMP 2.0 [11] introduce algunos cambios en esas cuatro subcompetencias. Entre ellos, la segunda de ellas pasa a denominarse "Protección de la privacidad y de los datos personales en entornos digitales", añadiendo aspectos relativos a la comprensión de cómo se usan y comparten los datos de identificación e información personal, así como al funcionamiento de las políticas de privacidad de las plataformas y redes sociales o a la gestión de la identidad digital. Además, el ciberacoso, el riesgo en la red que afecta a un mayor número de niñas y niños de entre 9 y 12 años [9], se considera en la subcompetencia referida a la salud; a la cual se añaden habilidades destinadas a favorecer la inclusión a través de herramientas digitales.

La legislación educativa actual alude a la necesidad de abordar la seguridad para el adecuado desarrollo de la CD [12], [13]. En este marco, la seguridad se entiende como el conocimiento de los riesgos que entraña la tecnología y la disposición de estrategias para evitarlos: la protección de la información y el reconocimiento de aspectos adictivos. El *ciberbullying* y otros fenómenos de riesgo no se recogen o se sobreentienden implícitos en la dimensión comunicación. Tampoco se recogen la protección de los dispositivos o del medio ambiente. Cuestiones de relevancia como la creación, cuidado y gestión de identidades digitales, propias y ajenas, quedan excluidas del currículo. Si bien la seguridad es una de las cuestiones que más preocupa a familias e instituciones, la formación en esta dimensión de la CD es todavía una tarea pendiente que requiere de una mayor y mejor formación [6] para el uso seguro y responsable de las nuevas tecnologías e Internet.

Las investigaciones previas sobre e-seguridad revelan la concienciación y buenas actitudes hacia la seguridad [6], [14], [15]. En el caso del alumnado español, la percepción de su CD en esta dimensión es superior a la manifestada en otras y se sitúa por encima de la media europea [14]. En cambio, las investigaciones citadas señalan, en contraste con la autopercepción del alumnado, el bajo desempeño en prácticas relacionadas con el uso seguro y responsable en Internet. Las y los jóvenes parecen tener conocimientos sobre situaciones de riesgo y conciencia sobre prácticas adecuadas como: no dar información personal, promover la protección y cuidado de la imagen virtual propia y de los otros, y mostrar un comportamiento apropiado en entornos digitales, como apuntan los hallazgos de las investigaciones realizadas con alumnado universitario [15] y de enseñanzas básicas [5]. En contraste con estos datos, se observa que prácticas tales como el uso de contraseñas seguras o la aplicación de protocolos para cambiarlas, así como mantener en privado los propios nombres de usuario/a, no son prácticas comunes [7], [15].

Muestran preocupación por la privacidad a través de las características de su cuenta o la concepción binaria sobre los "amigos", incluso tan restrictivas que socavan las potencialidades de las redes sociales [3]. Cerca de la mitad de los menores de entre 9 y 12 años (45%) mantienen un perfil privado [9]; y diversas investigaciones [7], [9] ponen de manifiesto que la mayoría de preadolescentes de entre 11 y 12 (74%) dice aceptar peticiones de amistad solo de personas conocidas y que el contacto con desconocidos se produce mayoritariamente a través de mensajería instantánea y redes sociales, no en el espacio físico. En cambio, en estos perfiles es común que los menores publiquen fotos de sí mismos/as, información personal como apellidos, número de teléfono o su escuela [8], lo que supone dificultades para conocer cómo gestionar la privacidad *online* y la identidad digital.

Del mismo modo, en lo relativo a la salud y el impacto medioambiental de las tecnologías, hay estudios con alumnado universitario que sugieren ciertas contradicciones entre el conocimiento del que disponen y la práctica [16]: dicen estar concienciados con las adicciones a dispositivos, los efectos psicológicos o sobre el bienestar físico, pero reconocen la dependencia a estos. Y del mismo modo, si bien manifiestan conciencia con respecto al consumo eléctrico de los dispositivos que emplean y el coste medioambiental de la producción de los mismos, ítems relativos al reciclaje de dispositivos obtienen puntuaciones bajas y reconocen no pensar en el medioambiente cuando compran, sustituyen o usan dispositivos electrónicos.

Los datos de las investigaciones sugieren una disonancia entre la percepción de la CD y las prácticas que las y los jóvenes realizan en contextos digitales. Por tanto, se pone en entredicho la capacidad de establecer una negociación consciente entre posibilidades y riesgos en la red. Si bien existen múltiples investigaciones que abordan la seguridad digital, son escasas las que estudian las competencias relativas a esta área. Del mismo modo, las investigaciones mayoritarias recogen la percepción de las y los jóvenes, pero no evalúan su CD. Y son escasos los trabajos que lo hacen en el contexto de la educación primaria. Se manifiesta entonces la necesidad de conocer qué habilidades se desarrollan, cómo y cuándo lo hacen y quienes están influyendo en este proceso [17]. Así pues, con este trabajo se pretende evaluar la CD en el área de seguridad de jóvenes preadolescentes, en la etapa de escolarización primaria, analizando las distintas subcompetencias y facetas que la integran; así como comprender los procesos, contextos y personas que interfieren en el desarrollo de la CD en el área de seguridad. La investigación que aquí se presenta forma parte del proyecto CDEPI "Competencia digital en estudiantes de educación obligatoria. Entornos sociofamiliares, procesos de apropiación y propuestas de e-inclusión", llevado a cabo en las Comunidades Autónomas de Castilla y León, Galicia y Madrid.

III. Método

Este estudio se caracteriza por el empleo de una metodología mixta de investigación: en concreto, se lleva a cabo un diseño de tipo secuencial exploratorio [18], el cual combina una primera fase cualitativa y una segunda fase cuantitativa. En la primera fase se realiza un estudio de casos múltiple que permite profundizar en la comprensión y análisis del área de seguridad de la CD y, en la segunda fase,

se aplica una prueba de evaluación de la CD sobre seguridad, adaptada a la población objeto de estudio.

A. Fase 1: Estudio de Casos

Se trata de un estudio de casos múltiple de tipo analítico [19] y de diseño holístico [20]. Participan, bajo el principio de consentimiento informado, un total de ocho sujetos (seis correspondientes al proyecto de investigación CDEPI-Galicia y dos casos más que se incluyeron en una fase posterior de investigación), cuyos nombres ficticios son: Alfonso (Al), Antón (An), Catarina (Ca), Lucía (Lu), Bieito (Bi), Jaime (Ja), Pedro (Pe) y Elisa (El).

Previamente se aplicó un cuestionario elaborado *ad hoc* a 182 familias pertenecientes a cinco centros educativos de la Comunidad Autónoma de Galicia, con hijos/as que cursaban 6º curso de Educación Primaria, para –a partir de los datos recogidos– seleccionar a los/as participantes atendiendo a un criterio de máxima rentabilidad [21], abarcando entornos familiares con distinto capital cultural. Concretamente, dos casos son de nivel socioeconómico bajo (Bi y Ja), tres casos de nivel medio (Al, An y El) y tres casos de nivel alto (Ca, Lu y Pe). Algunos de los casos comparten el contexto familiar, dado que Alfonso y Antón son mellizos y Catarina y Lucía son gemelas.

La recogida de datos se llevó a cabo en el segundo y tercer trimestre del curso 2016-2017. Fueron fundamentalmente dos las técnicas de obtención de información utilizadas:

- Entrevistas en profundidad, con una duración aproximada de 1 hora, a los niños/as, a sus progenitores/as o tutores/as legales, al profesorado-tutor y en algunos casos también a los responsables de la dirección del centro educativo e incluso a amigos/as de los niños/as. Todas las entrevistas fueron realizadas, por lo general, en espacios del colegio, grabadas en audio y transcritas de manera íntegra y literal.
- Observación participante de los sujetos, fundamentalmente de los comportamientos de los niños/as ante determinadas tareas informáticas o juegos con su ordenador portátil o su tableta. La ejecución de estas actividades también fue grabada en vídeo para su análisis posterior.

Toda la información recogida se analizó con la ayuda del programa Atlas.ti 7 siguiendo un procedimiento mixto, inductivo-deductivo [22]: por una parte, se tuvo en cuenta el marco teórico aportado por el modelo DIGCOMP sobre las subcompetencias que conforman el área de seguridad; y, por otra, emergieron nuevas categorías a medida que se examinaban los datos, ampliando así el marco comprensivo de las categorías anteriores. Como último paso del proceso de análisis, se elaboraron varios informes que fueron entregados a las familias y a los centros educativos, permitiendo así contrastar la información extraída y validar las observaciones e interpretaciones realizadas.

En la presentación de los resultados, se incluyen citas textuales de los/as participantes, identificadas a través de las dos primeras iniciales del caso, pudiendo ir acompañadas de un código que designa a las demás personas entrevistadas: “Ma” para madre, “Pro” para progenitores (participan ambos), “Tu” para tutor/a y “Ab” para abuela. Se señala también el número de entrevista.

B. Fase 2: Aplicación Prueba ECODIES-Área Seguridad

En esta segunda fase, de naturaleza cuantitativa, se utiliza una prueba de evaluación de la CD elaborada por el grupo de investigación GITE de la Universidad de Salamanca –responsable de uno de los subproyectos de CDEPI– para el área de seguridad, construida a partir del marco europeo DIGCOMP y con base en un modelo, adaptado a las edades de los niños/as de 6º de Educación Primaria, de 72 indicadores de conocimientos, capacidades y actitudes definitorios de la CD sobre seguridad [23], [24].

Por un lado, la parte de la prueba referida a conocimientos y habilidades en el área de seguridad consta de 16 ítems con cuatro alternativas de respuesta, en la que sólo una de ellas es la correcta. Por otro lado, las actitudes se miden con 6 ítems a través de una escala tipo Likert con 5 alternativas de respuesta (1: muy en desacuerdo, 2: en desacuerdo, 3: indiferente, 4: de acuerdo, 5: muy de acuerdo). Se trata de una escala unidireccional donde los seis ítems están redactados de forma positiva (estar de acuerdo manifiesta una actitud favorable).

Para hallar la puntuación de cada sujeto en la prueba, las respuestas se codifican de forma dicotómica: 1 es respuesta correcta, 0 es respuesta incorrecta. Las respuestas de los ítems de actitudes son dicotomizadas: las categorías “muy de acuerdo” y “de acuerdo” asumen el valor 1 (actitud positiva) y “muy en desacuerdo”, “en desacuerdo” o “indiferente” asumen el valor 0 (actitud no positiva).

La prueba, presentada en una página web diseñada para tal fin, fue aplicada a lo largo del curso 2018-2019 a una muestra representativa de alumnado de 6º curso de Educación Primaria de centros públicos de Galicia atendiendo a tres criterios de estratificación: 1) tipo de provincia –atlántica o no atlántica–, 2) participación o no del centro educativo en un programa de inmersión tecnológica y 3) densidad poblacional del ayuntamiento –zona poco poblada, zona intermedia y zona densamente poblada–. La muestra quedó compuesta por 563 estudiantes.

Los análisis de los ítems se han realizado de forma diferenciada atendiendo a su tipología: tipo prueba objetiva y tipo escala Likert. Respecto a los ítems de la prueba objetiva, aunque se advierte que presentan diversos niveles de facilidad-dificultad, es mayor la representación de preguntas difíciles: 2 muy fáciles, 2 fáciles, 5 de dificultad media, 5 difíciles y 2 muy difíciles. El índice de discriminación de los ítems, basado en el procedimiento de los grupos extremos, es muy bueno, a excepción de los ítems 8 y 14. Se decide, pues, prescindir de ellos en el presente estudio por su excesiva dificultad y escaso poder discriminativo. En cuanto a los ítems de actitudes, se ha comprobado –entre otros análisis– su adecuada homogeneidad (correlación del ítem con el total calculado como suma de todos los ítems, menos el analizado), obteniendo valores que oscilan entre 0,35 y 0,54. La fiabilidad del conjunto de la prueba en el área de seguridad (ítems de conocimientos, capacidades y actitudes dicotomizadas), en términos de consistencia interna, muestra un valor aceptable (KR-20=0,77).

Para el presente trabajo, se han reorganizado los ítems de la prueba ECODIES del área de seguridad de forma que cada subcompetencia está integrada por ítems de conocimientos, capacidades y actitudes, de acuerdo con el

modelo DIGCOMP. La estructura empleada se recoge en la Tabla I.

Las puntuaciones obtenidas en cada una de las subcompetencias son el resultado de sumar el número de respuestas correctas en los correspondientes ítems. Estas puntuaciones fueron calculadas en base 10 para poder establecer comparaciones entre las subcompetencias. Así mismo, se calcularon las puntuaciones para las tres facetas de la CD en el área de seguridad: conocimientos (5 ítems), capacidades (9 ítems) y actitudes (6 ítems).

Se llevaron a cabo análisis descriptivos univariables (porcentajes, medidas de tendencia central y medidas de dispersión), utilizando el paquete estadístico SPSS, versión 25. Además, debido a la falta de normalidad de la distribución de las respuestas –comprobada a través de la prueba de Kolmogorov-Smirnov (Sig.=0,00)–, se empleó la Prueba de Friedman para conocer si existen diferencias significativas entre las puntuaciones obtenidas en las diferentes subcompetencias y facetas de la CD en el área de seguridad.

TABLA I.
ESTRUCTURA POR SUBCOMPETENCIAS E ÍTEMS

Subcompetencia Protección de dispositivos
1. Sabe qué hacer cuando un dispositivo se infecta con un virus (conocimiento).
2. Sabe poner una contraseña segura (capacidad).
3. Usa el antivirus en el ordenador (capacidad).
4. Conoce normas para poner contraseñas (capacidad).
17. Considera que sólo se deben compartir las contraseñas con los padres o tutores (actitudes).
21. En lugares públicos procura utilizar la wifi cuando es segura (actitudes).
Subcompetencia Protección de datos personales
5. Sabe que una vez se publica algo en Internet se pierde el control (conocimiento).
6. Conoce las consecuencias de que descubran su contraseña (conocimiento).
7. Identifica las publicaciones que pueden poner en peligro su identidad (capacidad).
19. Considera que subir fotos a Internet y compartir información personal y familiar puede ser peligroso (actitudes).
Subcompetencia Protección de la salud
9. Sabe cómo evitar problemas de acoso a través de Internet (conocimiento).
10. Juega con los amigos *online* de forma positiva (capacidad).
11. Mantiene una postura correcta cuando usa dispositivos digitales (capacidad).
12. Navega por Internet sin perder el tiempo (capacidad).
16. Es capaz de dejar de jugar si se siente nervioso (capacidad).
18. Es consciente de que las tecnologías pueden crear adicción (actitudes).
Subcompetencia Protección del medio ambiente
13. Sabe que el consumo de dispositivos tiene impacto en el medio ambiente (conocimiento).
15. Ahorra energía en el uso de los dispositivos (capacidad).
20. Valora los dispositivos tecnológicos que respetan el medio ambiente (actitudes).
22. Es consciente de que los recursos naturales con los que se fabrican los móviles son limitados y pueden agotarse (actitudes).

IV. Resultados

Al evaluar –mediante la prueba ECODIES– el área de seguridad en su conjunto, las puntuaciones del alumnado reflejan un nivel medio (X=6,86; S=1,91; Md=7,50). La subcompetencia que el alumnado tiene más desarrollada es la relativa a la protección de la salud (X=7,13; S=2,48). Como se observa en la Fig. 1, sus respuestas se concentran en mayor medida en las puntuaciones más altas (Md=8,33). En las demás subcompetencias se obtienen puntuaciones promedio más bajas, por este orden: protección del entorno (X=6,84; S=2,70; Md=7,50), de datos personales (X=6,73; S=2,89; Md=7,50) y de dispositivos (X=6,69; S=2,26; Md=6,67). Se encuentran diferencias significativas entre las subcompetencias de protección de dispositivos y protección de la salud (Sig.=0,00) y entre las de protección de datos personales y protección de la salud (Sig.=0,03).

Respecto a las facetas de la CD, las puntuaciones más altas se obtienen en los ítems de actitudes (X=8,48; S=2,13; Md=10), cuya distribución de respuestas es muy homogénea (ver Fig. 2): el 75,5% del alumnado se sitúa entre las puntuaciones 8,33 y 10. Se obtienen puntuaciones más bajas en los ítems de conocimientos (X=6,54; S=2,92; Md=6) y capacidades (X=5,95; S=2,29; Md=6,67). Entre los tres aspectos analizados se dan diferencias significativas (Sig.=0,00 en los tres contrastes).

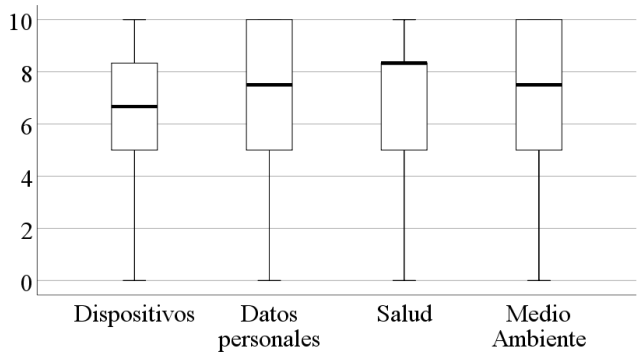

Fig. 1. Puntuaciones en las subcompetencias del área de seguridad.

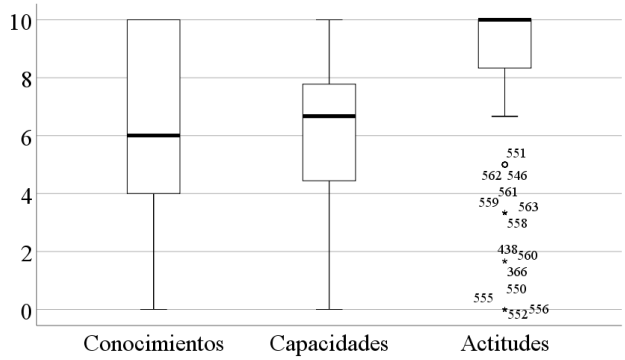

Fig. 2. Puntuaciones en las facetas de la CD en el área de seguridad.

A. Subcompetencia Protección de Dispositivos

De los 3 "núcleos" que componen la subcompetencia relacionada con la protección de dispositivos (gestión de contraseñas, protección frente a virus y acceso a redes wifi), la necesidad de pasar el antivirus (ítem 1) es el que muestra un porcentaje más alto: un 81,7% del alumnado sabe que cuando un dispositivo se infecta con un virus debe pasar inmediatamente el antivirus. Los resultados caen de manera llamativa en lo que se refiere a la prevención contra los virus, ya que solo un 52,9% afirma que de vez en cuando abre el antivirus y examina el disco duro (ítem 3), mientras un preocupante 16% no usa programas antivirus por no haberlos necesitado nunca.

Los casos manifiestan una evidente dualidad que concuerda con los datos recogidos a través de la prueba ECODIES, al tener claro que deben usar el antivirus una vez que el equipo está afectado, por un lado, y ser descuidados en la prevención frente a los virus informáticos, por otro. Esta contradicción se observa ya en el contexto familiar; los padres de Catarina no saben siquiera si el equipo que emplea su hija (el que le proporciona su colegio), tiene instalado un antivirus: "*me da la impresión de que eso no es algo que queda de su mano...* (...) *Jamás les oí hablar nada de eso...*" (Ca_Pro-2). Y ocurre exactamente lo mismo con los padres de Pedro, quienes tienen mucha confianza en las habilidades de su hijo "*Descarga, instala, borra, actualiza…*" (Pe-1), pero afirman que no tiene instalado antivirus y que no "controla" sobre el mantenimiento del ordenador. Algo que se contradice cuando en la misma entrevista afirman que, en realidad, el antivirus ya "le venía montado" en el ordenador, porque ya se preocuparon ellos (los padres) de esos aspectos. Los testimonios de ambas familias, de capital sociocultural alto, contrastan con la preocupación manifiesta en torno al uso de las tecnologías digitales que hacen sus hijas/os cuando se alude a otras áreas de la CD.

Es llamativa la situación de Antón cuyo ordenador *"cogió un virus"* (An-1), mientras el padre descargaba música (en el ordenador propiedad de los niños, no en el que les proporciona el colegio). Hecho que podría ser frecuente, ya que la madre indica irónicamente que es "*experto en baixar virus*" (An_Pro-2) y evidencia en su testimonio tener escasos conocimientos en la materia, al afirmar "*Realmente... Para o Linux non hai virus*" (An_Pro-2), cuando se refiere al portátil del colegio (dotado de sistema operativo Linux).

Algunos casos manifiestan desconocimiento o despreocupación ante este tema; así Elisa, afirma con tranquilidad tener virus en su ordenador al mostrar a la entrevistadora el procedimiento que sigue para descargar vídeos; o confunde una app de protección antirrobo, denominada Cerberus, que se encontró ya instalada en su móvil, con un antivirus propiamente dicho.

Por su parte, la gestión de contraseñas –el segundo de los núcleos mencionados dentro de la subcompetencia protección de dispositivos– presenta unos resultados de la prueba ECODIES no demasiado alentadores en lo que a seguridad se refiere: tan solo un 46,5% elegiría una contraseña segura para su dispositivo (ítem 2), en concreto las iniciales de su cantante favorito/a y el año en el que nació; mientras el resto (más de la mitad), elegiría opciones evidentemente menos seguras (desde su DNI, a su propio nombre y fecha de nacimiento o la dirección de su domicilio). Los resultados mejoran en lo que se refiere a las normas que siguen para crear contraseñas (ítem 4): el 60,9% escoge aquellas con muchos y variados caracteres, frente al 24,2% que las elige cortas (para recordarlas mejor), el 8,3% que usa solo minúsculas o el 6,6% que emplea solo letras.

Si nos vamos a los casos, solo Elisa comenta con claridad tener una contraseña "*muy difícil*", e incluso no le importa que la entrevistadora la mire mientras la teclea "*porque tiene mucha letra*" (El-2). Claro que esas cautelas tal vez no sirvan de mucho, ya que la niña le confiesa a la entrevistadora que guarda todas sus contraseñas anotadas dentro de la funda del móvil a pesar de que "*las sé de memoria*" (El-2). Nadie sabe que las tiene ahí, ni siquiera sus padres (ella misma, como hace mucho que las anotó en ese lugar, casi ni se acordaba).

Lucía, por su parte, parece priorizar la necesidad de que la contraseña sea sencilla *"porque si no, nos olvidamos"* (Lu-2), además de usar la misma para la wifi que para acceder a su correo electrónico, antes que priorizar la seguridad usando una combinación más segura.

En cuanto a las actitudes (ítem 17), un elevado 75,5% está de acuerdo o muy de acuerdo con que solo se deben compartir las contraseñas con sus padres o tutores, frente a un 15,1% que está en desacuerdo o muy en desacuerdo. Si vamos a los casos, comprobamos como la madre de Antón corrobora que sus hijos le dicen sus contraseñas. Lucía también comparte sus contraseñas con sus padres y con la profesora, así como con su hermana gemela, Catarina; pero mientras Lucía afirma que sus compañeros/as de clase no conocen las de los demás, Catarina comenta que se dicen las contraseñas entre amigas.

Jaime muestra ambivalencias: no tiene problema en que su padre sepa sus contraseñas –con el que comparte tardes de videojuegos– y es perfectamente consciente de los riesgos de compartir sus cuentas con otra persona, aunque sea un "*amigo*" de juegos *online*, "*porque a lo mejor, después se queda con mi cuenta, me borra juegos, no sé*" (Ja-1); incluso aunque ello supusiera ventajas, como subir de nivel en un videojuego. Sin embargo, sobre las medidas que toma con sus contraseñas en otros dispositivos, como el ordenador, Jaime no parece ser tan cauto y afirma no usarlas. Por su parte, Elisa es consciente de que compartir sus contraseñas con los compañeros comporta riesgos: "*pueden entrarte y jaqueártela, por ejemplo*" (El-2), aunque ella sí conoce la de algunos porque "*la van diciendo por ahí*".

Por último, el acceso a redes wifi, que constituye el tercer núcleo de la subcompetencia protección de dispositivos, presenta un porcentaje elevado, 83,7%, en lo relativo al uso de la wifi en lugares públicos cuando es segura, mientras solo un 5,6% se muestra en desacuerdo o muy en desacuerdo. En este sentido, en el conjunto de los casos solo tenemos constancia del acceso a una wifi pública en concreto, la de sus centros escolares, probablemente la única que gran parte del alumnado que participó en ECODIES conoce. Esto puede haber influido en los resultados, al no tener razones para desconfiar de la seguridad de sus contraseñas; a pesar de que su estructura sea fácilmente predecible para cada alumno de la misma clase, lo que hace sencillo averiguar la del resto: "*la sabe todo el mundo*" (Pe-1). Son escasas las alusiones al wifi y estas no se dirigen tanto a la seguridad como a los problemas de conectividad en los centros, como se evidenció al intentar conectar el equipo de Jaime durante una entrevista, o como manifiestan Pedro y su familia.

B. Subcompetencia Protección de Datos Personales

Los aspectos abordados giran en torno al control percibido por el alumnado de sus publicaciones en Internet, la configuración de la privacidad de las cuentas, las consecuencias de que otros/as sepan sus contraseñas y el tipo de publicaciones que ponen en peligro su identidad.

El 50,4% del alumnado sabe que una vez que se publica

algo en Internet, como pueden ser fotos o datos sobre la familia o la casa, se pierde el control sobre ello (ítem 5). Por el contrario, un 26,3% considera que son ellos/as quienes controlan la información y la pueden borrar cuando quieran; un 18,5% piensa que sus publicaciones sólo las verán sus verdaderos/as amigos/as y un 4,8% cree que esa información no afecta en ningún caso a su futuro ni al de su familia.

De acuerdo con el testimonio de la profesora-tutora de Catarina y Lucía, la mayor parte de su alumnado tiene cuenta propia en Facebook e Instagram "*a pesar de que o outro día aínda tivemos aquí un... Non sei, bueno, un oficial da Garda Civil... Falándolles da seguridade en Internet… Dicíndolles que hasta que tiveran catorce anos que non podían ter*" (Ca_Tu-1). El alumnado desconoce la edad mínima para darse de alta en las distintas plataformas o mismamente violan conscientemente las condiciones de uso de estos servicios, creando un perfil con datos inventados o basándose en los de otra persona: "*Claro, porque eles para probar… entonces poñen primeiro os meus datos, e despois din «esto funciona, o vamos facer cos nosos»"*(An_Ma-1). Además, el alumnado demuestra conocimientos y habilidades muy básicas relacionadas con las configuraciones de privacidad de las cuentas. Elisa llegó a tener un perfil personal en Google+, sin saber que era público: *"la sorpresa fue por un WhatsApp que mantuvo ella. «Yo tengo tantos seguidores» (...) Entonces, vimos que lo tenía en abierto, que* [se] *podía acceder"* (El_Pro-1).

En las publicaciones del alumnado en Internet media el contexto familiar. Por un lado, hay familias, como la de Catarina y Lucía, que les niegan el acceso a estos entornos digitales. Ídem para Pedro: *"Es una norma. No me dejarán hasta que tenga, creo que quince años, o catorce"* (Pe-1). La familia de Bieito también prohíbe tajantemente su uso. Su hermana mediana, de 13 años, se saltó las reglas, con el consecuente castigo: cierre de la cuenta de Instagram y sin acceso al móvil durante cuatro semanas. Por otro lado, hay familias como la de Elisa o Antón y Alfonso que permiten usar redes sociales, bajo la norma categórica de no subir fotos personales –aunque los progenitores no son total conocedores de todas las aplicaciones y redes que utilizan sus hijos/as–: "*Claro, dicíanme… «Mamá, podemos tal…?» E eu: «Mira, total andades co ordenador … bueno, vale. O que si, procurade non poñer fotos vosas…»*" (An_Ma-1).

En cuanto a las consecuencias de que otras personas descubran la contraseña personal de uno/a mismo/a, el estudio cuantitativo muestra que el 65,2% del alumnado sí que las conocen, sabiendo que pueden llegar a enviar mensajes haciéndose pasar por ellos/as, leer los mensajes que han recibido de cualquiera de sus contactos o incluso cambiar su contraseña y, por ende, no poder volver a ver sus propios mensajes (ítem 6). El estudio de casos ha permitido identificar la poca aplicación de este conocimiento sobre las contraseñas relativas a la plataforma E-Dixgal empleada en el ámbito escolar, con base en la común asunción de que no contiene ningún contenido importante y que presenta lo mismo para todo el grupo-clase. Sin embargo, con las cuentas de otras plataformas digitales y redes sociales que utiliza el alumnado fuera del contexto escolar, sí se advierte una mayor conciencia de las posibles consecuencias que conlleva divulgar su contraseña o que otras personas la descubran: "*Pueden, pues, poner una foto, que a ti no te parezca bien, por ejemplo*" (El-2). Elisa, a pesar de que conoce contraseñas de algunos compañeros, comprende y respeta su privacidad: *"a mí no me gustaría que me entraran en el mío"* (El-2).

En cambio, el caso de Bieito se caracteriza por no disponer de cuentas digitales propias. Curiosamente, utiliza cuentas heredadas de Gmail –a través del teléfono móvil que le han dado sin previamente restablecer los datos de fábrica del dispositivo– y abre los correos electrónicos destinados al anterior propietario, vulnerando la protección de datos de la otra persona, sin ni siquiera ser conocedor de las implicaciones de sus propios actos.

El estudio cuantitativo también revela que el 61,8% del alumnado identifica las publicaciones que pueden poner en peligro su identidad (ítem 7), como una fotografía en la puerta de la casa en la que aparezca el número y nombre de la calle, una entrada en un blog en el que se facilite el número de teléfono o una fotografía de las vacaciones del último verano. No obstante, aumenta en 30 puntos porcentuales (91,7%) el alumnado que considera que subir fotos a Internet y compartir información personal y familiar puede ser peligroso (ítem 19), existiendo un 8,3% que muestra una actitud indiferente o en desacuerdo con este hecho.

En este sentido, Elisa cuida determinados detalles en la difusión de su imagen y es consciente de la importancia de la privacidad de los datos personales en Internet: "*esta es la foto que tengo, ¿no?* [se refiere a una cuenta de correo electrónico] *Que no se me ve, a propósito, que se me ve la espalda"* (El-2). Tiene como hábito buscarse a sí misma en Google para comprobar que no está publicada ninguna imagen suya en la que se le reconozca. Se constata que todo este celo que envuelve sus prácticas está fundado en el control y preocupación parental por asegurar la protección de sus datos personales y evitar posibles peligros que pueda traer consigo compartir información: *"Tiene todos privados* [vídeos que crea con la aplicación Musical.ly] *(…) Porque no sabes ni quién lo ve. Ni cómo lo va a utilizar"* (El_Pro-1). Pero, a veces, Elisa no actúa con prudencia: "*sí que se me ve la cara, pero no es para tanto* [hablando de la foto de perfil de Instagram]" (El-1). Actitud despreocupada que adopta en otras prácticas como la visita de páginas no seguras para descargar canciones, en donde le saltan de forma constante pantallas emergentes y *banners* que ella identifica como negativos, pero sin saber qué riesgos entrañan.

Pedro sabe perfectamente qué información personal no hay que facilitar en la red, aunque, contradictoriamente, utiliza su cuenta de Gmail a menudo para subscribirse a juegos y a canales de YouTube. En ocasiones, sí parece mostrarse más consciente de la protección de datos personales y, para acceder a algún juego, incluso introduce cuentas de correo electrónico que no existen. Al comunicarse con los miembros del clan a través del chat propio de Clash Royale y Clash of Clans, asegura que "*No decimos ninguna cosa personal, ni nada de eso*", "*Ni siquiera decimos nuestros nombres*" (Pe-1). Además, pone de manifiesto los riesgos de proporcionar información personal en las redes sociales por la posibilidad de caer en peligrosos retos virales: "*Se llama «El Reto de la Ballena Azul», (...) para poder aceptarlo tienes que darle tu nombre,*

tus apellidos y tu dirección, y... Si no completas el reto, matan a tu familia" (Pe-1).

Por su parte, Jaime verbaliza que está al tanto de los riesgos de Internet. En efecto, no utiliza su nombre personal en sus cuentas de YouTube o GTA, pero cuando se le pregunta el motivo concreto, no tiene elaborado un discurso sólido al respecto: *"No sé, nunca se me dio por poner el nombre*", *"Todos ponen nombres inventados"* (Ja-5). Lo cual sugiere que esta práctica guarda más relación con la configuración de su identidad como *gamer* que con la seguridad en la red.

Por último, Alfonso y Antón son conscientes de la necesidad de proteger su información personal, con algunas reservas. En una de las entrevistas realizadas a Alfonso, nos enseña su Instagram, manifestando preocupación por una foto de una tercera persona que tiene publicada en su perfil privado: *"teño que borrar unha foto porque según Laura* [nombre ficticio], *unha nena pódeme denunciar por poñer unha foto de WhatsApp*" (Al-1). Bien porque no sabe, bien porque se olvida, no elimina la referida foto a lo largo de las diferentes sesiones mantenidas con él.

Los casos estudiados muestran, pues, falta de congruencia entre lo que creen y dicen y lo que realmente saben y hacen, en correspondencia con los resultados arrojados por la prueba ECODIES, como se ha indicado: mayor puntuación en actitudes (ítem 19) que en capacidades (ítem 7).

C. Subcompetencia Protección de la Salud

Se alude a las competencias que se poseen para garantizar el bienestar psicológico, que engloba la calidad de las relaciones que se establecen en la red, el tiempo de dedicación y la calidad del mismo, así como el bienestar físico.

En el análisis de los casos se observa que la preocupación principal de las familias relativa a esta subcompetencia versa sobre la variable espacio–tiempo. Esta aparece transversalmente en todos los casos, en forma de norma, conducta de algún/a miembro de la familia o a través del discurso; y sobre ella recae en mayor medida el peso de la seguridad tanto psicológica como física de las y los jóvenes. Destaca en los casos caracterizados por un capital socioeconómico medio, donde la dotación de acceso y la preocupación por los tiempos es una constante en el discurso. La familia de Elisa, articula normas estrictas para su control, asegurando que *"Por semana no tiene el móvil, se le da el viernes, después de que venga del cole, y se lo requiso entre comidas"* (El_Pro-1). La familia de Antón y Alfonso también restringe el uso durante la semana y, a pesar de que establece normas más laxas que en ocasiones se incumplen, llega a instalar herramientas de control parental destinadas a limitar el tiempo de exposición, *"Porque senón eles estarían seguido (...) no da casa téñolle o con... control parental, basicamente para que non estén conectados todo o día"* (An_Pro-1).

A pesar de que no siempre existen normas explícitas para regular los tiempos y momentos de uso en todas las familias, se detecta algún tipo de control por parte de algún/a familiar, como en el caso de Bieito, cuya hermana interviene retirando el dispositivo ante la falta de competencia en el hogar, surgiendo normas laxas: *"No, se la pido el abuelo y él me deja* [en alusión a la consola]. *Por la semana, no"* (Bi-2). Incluso en el caso en el que no se retira el dispositivo existe una reflexión explícita en torno al tiempo de dedicación que permiten a partir de una negociación previa entre las potencialidades de estas tecnologías y los riesgos que detectan. La familia de Jaime no detecta riesgos suficientes que justifiquen limitar el tiempo de juego, que consideran positivo para su TDAH (Trastorno por Déficit de Atención e Hiperactividad). Una decisión que es objeto de discusión entre su madre y su tutora escolar.

En aquellas familias con un capital sociocultural alto, la preocupación se dirige hacia el tipo de uso que se hace de los dispositivos, tratando de garantizar que el tiempo dedicado impacta positivamente en el desarrollo de los/las jóvenes y prescindiendo o reduciendo otros posibles usos. Esto se manifiesta a través de la restricción, que en el caso de las gemelas lleva a la negación de cualquier uso no académico, a excepción de mini juegos en los que participan de forma esporádica o el contacto con familia extensa. En el caso de Pedro, se produce a través de la supervisión y promoción de otros usos, facilitando el acceso al ocio y a determinados juegos, pero no a de redes sociales.

Se evidencia en los casos una preocupación sobre si este uso se interpone o no en otras obligaciones como el estudio; o si el uso excesivo puede derivar en consecuencias negativas para las/os jóvenes. Del mismo modo, la prueba ECODIES revela la existencia de una conciencia del alumnado en torno a la posibilidad de generar adicciones al uso de dispositivos. Un 90,2% del alumnado manifiesta que es consciente de que las tecnologías pueden crear adicción (ítem 18) y solo un 9,8% muestra su desacuerdo o su indiferencia ante esta aseveración.

Desde la articulación de normas rígidas y elaboradas, como es el caso de Elisa, hasta la consideración de que el balance riesgo-beneficio es positivo y por ende no necesita intervención, como es el caso de Jaime, no existen alusiones a una regulación de los tiempos que nazca del interés de la o el joven, porque considere que dedica un tiempo excesivo o sienta que tiene conductas relacionadas con la adicción.

De acuerdo con los resultados de la prueba ECODIES, un 63,6% del alumnado es capaz de dejar de jugar si se siente nervioso (ítem 16). En el lado opuesto, un 16% sigue jugando porque considera que un poco de estrés y nerviosismo sirve para mejorar su rendimiento en el juego; un 8,2% sigue jugando aunque su rendimiento sea menor y un 12,3% nunca se plantearía dejar el juego por esa razón. Del mismo modo, en lo que respecta a la deportividad, el 82,1% de los alumnos/as juega con los amigos/as *online* de forma positiva (ítem 10), ya que consiguen mantener buenas relaciones con ellos/as aunque vayan perdiendo en el juego.

Las niñas que configuran los casos no son jugadoras y en caso de jugar a algún videojuego, es frecuente que participen en propuestas enfocadas en el juego simbólico (Elisa, "imagina ser") o la resolución de actividades basadas en el conductismo (gemelas, puzzles y tetris), que no proponen un problema o meta a resolver de forma estratégica y que propician escasas posibilidades de juego *online* (Elisa, Just Dance en la Wii, sin cámara). En los jóvenes jugadores sí que se acostumbra a colaborar o competir con otras personas (Jaime con el GTA o los gemelos y Pablo con el Clash Royale); y en esta práctica se detectan habilidades relativas a la gestión del nerviosismo

en el juego y la deportividad. Jaime señala como su primo *"a veces se pica y tira el mando al suelo"* (Ja-3) y manifiesta que él no tiene esta conducta, aunque se enfada si no logra "*pasar una fase*", dice "*voy a jugar a la* tablet" (Ja-3) para relajarse.

Se observa que la práctica de jugar *online* interfiere en las tensiones existentes en las familias entre la seguridad y el control, interpelando al sentimiento de desprotección de las y los jóvenes en el contexto virtual. La interacción con desconocidos causa ambivalencias en el entorno familiar. Algunas familias valoran la experiencia de poder aproximarse a otras personas y a culturas diferentes: *"él me decía: «mamá, es que conocí a un niño mejicano y me dijo que en su país esto es así, así, así»"* (Ja_Ma-1), lo cual es interpretado como una oportunidad de aprendizaje: *"Claro, y él va cogiendo conocimientos, entonces, ¿por qué le voy a restringir eso? Pues prefiero que esté, a lo mejor, hablando* online *con esos niños que le pueden aportar algo y no viendo... Shin Chan en la tele"* (Ja_Ma-1). Otras familias hacen énfasis en los riesgos que se ocultan tras esta práctica, por lo que abogan por la prohibición de hablar con desconocidos en el juego o en las redes sociales. Esta preocupación en el caso de la familia de Elisa lleva al control de las conversaciones que mantiene la joven a través de sus dispositivos: *"intentamos ver todos los mensajes. Tenemos con ella un acuerdo que no puede borrar mensajes (...) y que nosotros tenemos que saber las contraseñas y poder acceder a todo lo que tiene en el móvil"* (El_Pro-1); y la prohibición de jugar *online* empleando micrófono y cámara*: "no nos gusta que… que con la cámara pues puedan* [grabarla...]*… no"* (El_Pro-1).

La intervención familiar se centra en el permiso o en la prohibición de la práctica a partir de su negociación entre potencialidades y riesgos, pero no se repara en la información de la que disponen las/os jóvenes para discernir entre conocidos y desconocidos. Aunque en algunos casos, como el de Pedro, se explicitan prácticas ligadas a la protección de datos personales en chats de videojuegos *online;* el concepto "desconocido" se presenta de forma ambigua en los casos y se observa cómo generan estrategias propias para discernir de quien se pueden fiar y de quien no. Antón y Alfonso parecen tener una mirada diferenciada entre aquellos desconocidos vinculados a intereses comunes, con los que sí se comunican a través de chats de juegos *"non conozco a xente. Pero cáenme ben…"* (An-1); y aquellos desconocidos con los que aparentemente no comparten un interés común, lo que le otorga rango de "desconocido". Elisa, por otra banda, adopta la edad aparente de la persona y sus amistades como criterio para distinguir entre conocidos y desconocidos. Pues para ella el desconocido no es aquel que no conoce personalmente, sino aquel que se considera como potencialmente peligroso. Por ello, acepta como conocidas a personas de su edad que parezcan asistir al instituto al que irá ella el siguiente año o a quienes tengan un trato de amistad con sus amigas/os o conocidas/os. Actúa a través del bloqueo cuando personas que no encajan en estas reglas tratan de interactuar con ella, *"hace poco, una, una, mmm es que no sé qué eran, porque había dos personas en una foto y me dice: «Hola». Y yo le digo: «¿Quién eres?» «Alguien, ¿qué tal?». Y yo, no te tengo, hay dos personas así que son bastante mayores. No me voy a… lo bloquee. (...) Además la foto también estaba así un chico así bastante grande por así… que tendría treinta y pico y tenía una chica al lado y yo… esto no son niños ni nada"* (El-1). Si bien esta estrategia puede resultar útil, no repara en que la identidad digital que observa en la red pueda ser simulada, llegando a admitir *"me tienen que poner, por ejemplo: «Soy ta, ta, ta, de* [cita como ejemplo el nombre de parroquias cercanas y el colegio]*… íbamos juntos a la guardería». Si me dicen eso aún me lo creo"* (El-1).

Las y los jóvenes hacen uso de estas estrategias para salvaguardarse y las consideran valiosas y de utilidad. Esto encaja con los valores obtenidos en la prueba, según la cual el 68,7% de los alumnos/as sabe cómo evitar problemas de acoso a través de Internet (ítem 9), ya que no se fían de personas que no conocen y que quieren contactar con ellos/as. Pero la ambigüedad en torno a la persona desconocida sugiere que los conocimientos y competencias que poseen al respecto podrían ser endebles y exponerles a posibles engaños. Además, este código no concurre nunca con la escuela, ni se menciona en las entrevistas a tutoras/es; únicamente se puede intuir que se podría haber dotado de alguna información al respecto en este escenario a través de la tutora de Catarina y Lucía, quien habla de una charla impartida por la Guardia Civil. El enfoque legal y del delito justificaría la identificación de la persona desconocida de la que desconfiar, con concepciones previas en torno a quién podría ser un potencial agresor o agresora.

En lo relativo al aprovechamiento de tiempo, en la prueba se recoge que el 57,5% del alumnado navega por Internet sin perder el tiempo (ítem 12), yendo directamente a la información que necesita para terminar cuanto antes. Sin embargo, un 14,9% suele tardar bastante porque encuentra páginas divertidas con las que se entretiene; un 11,9% termina leyendo o viendo vídeos que no tienen nada que ver con la información que buscaba y un 15,6% del alumnado revisa normalmente muchas páginas, pero no termina de encontrar lo que quería. Sobre esta cuestión, son escasas las referencias explícitas en los casos, a pesar de que sí se detectan alusiones a la navegación a través de hipervínculos en plataformas como YouTube. En el caso de Elisa es una práctica frecuente, incluso afirma que el contenido que consume es aquel que figura en las recomendaciones de otros vídeos.

Del mismo modo, son pocas las referencias a la salud física. Si bien el 65,9% del alumnado mantiene una postura correcta cuando usa dispositivos digitales (ítem 11) –de acuerdo con los datos recogidos por la prueba ECODIES–, tanto en el escenario familiar, como el escolar o el del grupo de iguales, esta preocupación en torno a la seguridad se sitúa en un segundo plano frente a otras relativas a la salud.

D. Subcompetencia Protección del Medio Ambiente

Esta subcompetencia obtiene el segundo valor medio más alto en la dimensión seguridad. En contraste, no existen referencias explícitas a esta subcompetencia, ni por niños/as, ni por padres o tutores/as. Por lo que se interpreta que esta subcompetencia no está dotada de la consideración que reciben otras, en torno a las que se desata un gran debate.

De acuerdo con la prueba ECODIES, un 61,1% del alumnado sabe que el consumo de dispositivos tiene

impacto en el medio ambiente por generar basura difícil de reciclar (ítem 13). Un 44,6% de los/as estudiantes sabe ahorrar energía en el uso de los dispositivos (ítem 15), de forma que si se encuentran realizando un trabajo en el ordenador, que aún no han terminado, y tienen que ausentarse por cierto tiempo, usan la opción "suspender" para ahorrar energía. Por el contrario, un 19,5% del alumnado deja el ordenador encendido porque en poco tiempo volverá; un 29% opta por apagar solo la pantalla y un 6,9% deja encendido el ordenador sin cuestionarse esta acción.

Un 86,5% del alumnado valora los dispositivos tecnológicos que respetan el medio ambiente (ítem 20). Concretamente, un 61,5% y un 25% del alumnado responde a esta afirmación en las categorías "muy de acuerdo" y "de acuerdo", respectivamente. Así mismo, un 81,5% del alumnado es consciente de que los recursos naturales con los que se fabrican los móviles son limitados y pueden agotarse (ítem 22). Por el contrario, un 18,5% de los/as estudiantes se muestran indiferentes o en desacuerdo con esta problemática.

Se observa, en el plano actitudinal, como la variable del impacto ambiental no se contempla en el cambio de dispositivos. Elisa manifiesta el deseo de cambiar su móvil, que posee desde hace un año, por otro mejor; a pesar de que se deduce que este es perfectamente útil, tanto por su testimonio como por las observaciones realizadas en el uso del dispositivo. Incluso no parece tener argumentos para justificar la elección del dispositivo que quiere comprar, más allá de la presión social hacia el consumismo o la posesión de dispositivos de alta gama: *"El que todo el mundo quiere (...) es el iPhone*" (El-3). Se observa cómo la joven estima hasta qué precio cree que puede llegar pidiendo un móvil nuevo, eligiendo la gama más alta dentro de las posibilidades familiares, "*Yo quiero el seis plus (...) Porque el siete no me gusta y porque el cinco me parece muy pequeño*" (El-3), sin contemplar, ni conocer en profundidad, las características del dispositivo que desea. Por ende, no aflora en ningún momento la responsabilidad medioambiental como motivo para no hacer el cambio, o el consumo energético del dispositivo como criterio de elección de uno nuevo.

La economía juega un papel antagónico en familias con un menor capital socioeconómico, dando lugar a prácticas positivas para el medioambiente, como es la herencia digital. Es el caso de Bieito y su teléfono móvil *"Doullo seu… seu tío, seu padriño. Tiña a tarjeta..., era usado* (...) *Haberá un ano, se o hai"* (Bi_Ab-1). Si bien esta práctica favorece el medioambiente, no se lleva a cabo de forma premeditada y consciente, sino que es producto de la falta de recursos para hacerse con nuevos dispositivos.

V. Conclusión

Los resultados obtenidos, tanto en la prueba ECODIES como en el estudio de casos, ponen de manifiesto una mayor predisposición del alumnado (actitudes) que conocimientos y capacidades reales sobre cuestiones relacionadas con la seguridad. Destaca la protección de la salud como la subcompetencia en la que muestran un mayor dominio y, a su vez, la que supone una mayor preocupación parental; lo cual manifiesta la influencia de las familias en el desarrollo de la CD de las y los jóvenes.

La preocupación de la familia en torno a la protección de la salud no parte de una alta CD, sino de la preocupación parental de proteger a sus hijas/os [25], que lleva a las familias a intervenir casi de forma instintiva; haciendo hincapié en fenómenos concretos y con repercusión mediática (adicción, *sexting*, c*iberbullying*…), sin reparar en el conjunto de prácticas relativas a la seguridad que favorecen o propician estos fenómenos (privacidad en la red, virus, gestión de contraseñas…). El discurso familiar se materializa en las y los jóvenes en actitudes positivas, pero presentan lagunas, contradicciones en su práctica y ambigüedades conceptuales, que afloran en los casos y los resultados de la prueba.

A juzgar por la información extraída del análisis de los casos, la escuela tampoco está garantizando el desarrollo de esta área. Descuida la seguridad en los propios dispositivos que se usan en el aula, tanto en lo que se refiere al uso de programas antivirus como a la gestión de contraseñas o el acceso al wifi. La privacidad y salud se cede a otras instituciones como las fuerzas de seguridad, que acuden a las escuelas con un fin informativo y un enfoque legalista o centrado en el delito. Y la protección del medio ambiente no se contempla en el currículo como parte de la CD. De hecho, en el desarrollo de las entrevistas tampoco ha emergido con fuerza esta subcompetencia relativa a la protección del entorno y, por tanto, no se ha profundizado suficientemente en ella, siendo esta una limitación de nuestro estudio que requiere de una mayor atención en futuras investigaciones.

Este estudio cuestiona la capacidad de las y los jóvenes de hacer un uso inteligente, crítico y reflexivo de las nuevas tecnologías [3] en materia de seguridad; y pone de relieve la influencia del escenario familiar frente a la escuela en el desarrollo de la CD, favoreciendo la brecha digital y la desigualdad [1], [2]. Conclusiones inquietantes en los tiempos que corren y que invitan a repensar el lugar de la CD en las escuelas una vez superada la crisis.

Agradecimientos

Proyecto de investigación "Competencia digital en Estudiantes de Educación Obligatoria. Entornos socio-familiares, procesos de apropiación y propuestas de e-inclusión" (EDU2015-67975-C3-1-P) financiado por el Ministerio de Economía y Competitividad y por el Fondo Europeo de Desarrollo Regional (FEDER).

Referencias

[1] A. Alonso-Ferreiro, U. Regueira, and M. H. Zapico-Barbeito, "Actitudes de alumnado preadolescente ante la seguridad digital: un análisis desde la perspectiva de género", *RED. Revista Educación a Distancia*, vol. 19, no. 61, pp. 1-29, Nov. 2019.

[2] A. Gewerc and F. Fraga-Varela, "Competencia digital e inclusión social: cuando las condiciones socioculturales se imponen. In Gewerc, A. and Martínez-Piñeiro, E. (Coords.), Competencia digital y preadolescencia. Los desafíos de la e-inclusión (pp. 21-42). Madrid, Spain: Síntesis, 2019.

[3] S. Livingstone, Internet literacy: "Young people's negotiation of new online opportunities". In McPherson, T. (Ed.), Unexpected outcomes and innovative uses of digital media by youth. MacArthur Foundation

Series on Digital Media and Learning (pp. 101-121). Cambridge, Mass., USA: MIT Press, 2008.
[4] A. Ferrari, DIGCOMP: A Framework for Developing and Understanding Digital Competence in Europe. Sevilla, Spain: Joint Research Centre, Institute for Prospective Technological Studies, 2013.
[5] A. Alonso-Ferreiro, Competencia Digital y Escuela. Estudio de Caso Etnográfico en dos CEIP de Galicia (Universidade de Santiago de Compostela). 2016.
[6] F. Annansingh and T. Veli, "An investigation into risks awareness and e-safety needs of children on the internet", *Interactive Technology and Smart Education*, vol. 13, no. 2, pp. 147-165, 2016.
[7] J. Byrne, D. Kardefelt-Winther, S. Livingstone, and M. Stoilova, Global Kids Online research synthesis, 2015–2016. UNICEF, 2016.
[8] J. Fernández-Montalvo, A. Peñalva, and I. Irazabal, "Hábitos de uso y conductas de riesgo en Internet en la preadolescencia", *Comunicar: Revista Científica de Comunicación y Educación*, vol. 22, no. 44, pp. 113-121, 2015.
[9] M. Garmendia, E. Jiménez, M. A. Casado, and G. Mascheroni, Net Children Go Mobile: Riesgos y oportunidades en internet y el uso de dispositivos móviles entre menores españoles (2010-2015). Madrid, Spain: Red.es/Universidad del PaísVasco, 2016.
[10] S. Livingstone, EU Kids Online: Findings, methods, recommendations. London, UK: EU Kids Online, 2014.
[11] S. Carretero, R. Vuorikari, and Y. Punie, The Digital Competence Framework for Citizens. With eight proficiency levels and examples of use (No EUR 28558 EN), 2017.
[12] Orden ECD/65/2015, de 21 de enero, por la que se describen las relaciones entre las competencias, los contenidos y los criterios de evaluación de la educación primaria, la educación secundaria obligatoria y el bachillerato, *BOE*, no. 25, 2015.
[13] Consellería de Cultura, Educación y Ord. Univ., Decreto 105/2014, de 4 de septiembre, por el que se establece el currículo de la educación primaria en la Comunidad Autónoma de Galicia, *DOG*, no. 171, 2014.
[14] ESSIE, Survey of schools. ICT in Education. Bechmarking Acces, Use and Attitudes to Technology in Europe's Schools, 2013.
[15] M. J. Gallego-Arrufat, N. Torres-Hernández, and T. Pessoa, "Competencia de futuros docentes en el área de seguridad digital", *Comunicar: Revista Científica de Comunicación y Educación*, vol. 27, no. 61, pp. 57-67, 2019.
[16] B. Castillejos, C. Torres, and A. Lagunes, "La seguridad en las competencias digitales de los millennials", *Apertura*, Vol. 8, no. 2, pp. 54-69, 2016.
[17] E. Martínez-Piñeiro, A. Gewerc, and A. Rodríguez-Groba, "Nivel de competencia digital del alumnado de educación primaria en Galicia. La influencia sociofamiliar", *Revista de Educación a Distancia*, vol. 19, no. 61, pp. 1-25, Nov. 2019.
[18] J. W. Creswell and V. L. Plano, Designing and conducting mixed methods research (3ª ed.). Thousand Oaks, CA, USA: Sage, 2018.
[19] X. Coller, Estudio de casos (2ª ed.). Madrid, Spain: CIS, 2005.
[20] R. K. Yin, Case study research. Design and methods (4ª ed.). Londres, UK: Sage, 2009.
[21] R. E. Stake, Investigación con estudio de casos (5ª ed.). Madrid, Spain: Morata, 2010.
[22] J. C. Tójar, Investigación cualitativa. Comprender y actuar. Madrid, Spain: La Muralla, 2006.
[23] A. García-Valcárcel, et al., Modelo de indicadores para evaluar la competencia digital de los estudiantes tomando como referencia el modelo DIGCOMP (INCODIES), 2019. [Online]. Available: https://gredos.usal.es/jspui/handle/10366/139409 [Accessed: 05-17-2020].
[24] A. García-Valcárcel, L. Salvador, S. Casillas, and V. Basilotta, "Evaluación de las competencias digitales sobre seguridad de los estudiantes de Educación Básica", *Revista De Educación a Distancia*, vol. 19, no. 61, pp. 1-34, Nov. 2019.
[25] D. Buckingham, Crecer en la era de los medios electrónicos. Madrid, Spain: Morata, 2002.

.

Esther Vila-Couñago es Licenciada en Pedagogía y doctora en Educación por la Universidade de Santiago de Compostela (USC). Actualmente es profesora ayudante doctora en el Departamento de Pedagoxía e Didáctica (Área de Didáctica e Organización Escolar), en la Facultade de Ciencias da Educación de la USC. Ha participado en publicaciones centradas en la medición y evaluación educativa y en proyectos de investigación sobre servicios de orientación profesional, calidad de los centros docentes, competencia en el lenguaje escrito y competencia digital en estudiantes de educación obligatoria.

Uxía Fernández-Regueira es graduada en Pedagogía, es estudiante predoctoral en la USC, en el marco del Programa de Equidad e Innovación en la Educación; y profesora invitada en la Universidade de Vigo. Sus líneas de investigación abordan la tecnología educativa, la competencia digital y la implicación del género en la apropiación tecnológica. Ha participado en un proyecto nacional. Posee un capítulo de libro, dos artículos y comunicaciones a congresos con impacto en el campo educativo.

Eulogio Pernas-Morado es Maestro y licenciado en Filosofía y Ciencias de la Educación en 1991. Actualmente es profesor del Dpto. de Pedagoxía e Didáctica de la USC y director de la revista *Innovación Educativa*, publicada por el Servizo de Publicaciones de la USC. Como miembro del Grupo de Investigación Stellae desde su fundación, es autor de diversos artículos, libros y otras publicaciones en torno a temas focalizados en las tecnologías aplicadas a la educación, entornos virtuales de enseñanza y aprendizaje y medios y recursos didácticos.