Análisis de expertos sobre la educación en ciberseguridad dirigida a población no-técnica

Alberto Beltrán Muñoz[1], Manuel G. Jiménez-Torres[2]

[1] *Universidad de Granada. Coordinador de proyecto de investigación en CEAR Alicante*.

[2] *Universidad de Granada, Departamento de Personalidad, Evaluación y Tratamiento Psicológico*.

Beltrán Muños, Alberto y Jiménez-Torres, Manuel G. (2023). Análisis de expertos sobre la educación en ciberseguridad dirigida a población no técnica. *Revista Electrónica de Criminología, 08-07*. 1-10.

RESUMEN: En este estudio se ha consultado a 10 expertos del ámbito de la educación en ciberseguridad para conocer sus opiniones y percepciones. Se les ha planteado 3 cuestiones de desarrollo y 6 de tipo likert, con un cuestionario final para calificar de validez de los expertos. Las cuestiones van referidas a la educación de la población no-técnica y la situación actual en torno a ella. Se ha encontrado consenso en torno a la falta de concienciación, conocimientos y preparación de la ciudadanía en materia de ciberseguridad y ciberdelincuencia. También la falta de más equipos interdisciplinares y personal de áreas no-técnicas a la hora de afrontar los retos de la ciberseguridad. Se ha identificado una falta de adaptación de la educación a las nuevas necesidades. También se detectó la necesidad de mejorar las campañas educativas y de actualizar de las medidas implantadas. Consecuencia de todo ello, se visibiliza la necesidad de reajustar las campañas de divulgación y la actualización constante de las estrategias educativas.

PALABRAS CLAVE: Ciberseguridad; ciberdelito; educación; concienciación; interdisciplinariedad.

EXPERT ANALYSIS OF CYBERSECURITY EDUCATION AIMED AT NON-TECHNICAL POPULATION.

ABSTRACT: In this study, 10 experts in the field of cybersecurity education were consulted for their opinions and perceptions. They were asked 3 developmental questions and 6 likert-type questions, with a final questionnaire to qualify the experts' validity. The questions refer to the education of the non-technical population and the current situation regarding it. Consensus has been found around the lack of awareness, knowledge and preparation of citizens in cybersecurity and cybercrime. Also the lack of more interdisciplinary teams and personnel from non-technical areas when facing the challenges of cybersecurity. A lack of adaptation of education to new needs was identified. The need to improve educational campaigns and update the measures implemented was also detected. As a result of all this, the need to readjust the dissemination campaigns and the constant updating of educational strategies became apparent.

KEYWORDS: Cybersecurity; cybercrime; education; awareness; interdisciplinarity.

FECHA RECEPCIÓN REC: 26/03/2023

FECHA PUBLICACIÓN REC: 30/12/2023

AUTOR/A CORRESPONDENCIA: Alberto Beltrán Muñoz, albertobeltran@correo.ugr.es

SUMARIO 1. Introducción, 2. Metodología, 2.1 Diseño, 2.2 Instrumento, 2.3 Participantes, 3. Resultados. 4. Discusión. 5. Conclusiones.

1. Introducción

En la última década, el impacto de la Cibercriminalidad va aumentando año tras año tal y como se demuestra con el aumento de hechos conocidos. La proporción dentro del conjunto de la criminalidad también está creciendo: se ha pasado del año 2016, de un 4,6%, al año 2020 con el 16,3%. En el mismo periodo, 2016-2020, se ha mantenido constante el aumento de los delitos informáticos, de hecho, solo en el 2020, se ha conocido un total de 287.963 hechos, lo que supone un 31,9% más con respecto al 2019 (ONTSI, 2022). Queda claro que la ciberdelincuencia es un problema en auge y, como se suele repetir en el ámbito, el factor humano es el eslabón más débil pero también el más importante. Es más necesario que nunca buscar un conocimiento amplio y comprensión abierta sobre las distintas formas de cibedelincuencia a las que se enfrenta nuestra sociedad, especialmente aquellas nuevas y emergentes (DSN, 2019).

Estas nueva forma de delincuencia, la ciberdelincuencia, es un fenómeno complejo y global que requiere un enfoque interdisciplinar para abordar cualquier planteamiento de respuesta contra el mismo (López et al., 2021; Ghernaouti-Helie, 2009). Este punto es determinante y requiere de análisis, especialmente para responder a la pregunta de "¿Se está realmente abordando de forma interdisciplinar con presencia de ramas de las Ciencias Sociales? o por el contrario ¿Nos encontramos en un ámbito donde la mayor parte de profesionales son de áreas STEAM (Ciencia, Tecnología, Ingeniería, Artes y Matemáticas) con enfoques únicamente técnicos?". Dentro del enfoque interdisciplinar, tiene especial importancia la presencia de ciencias relacionadas con la conducta humana porque cuando hablamos de ciberdelincuencia y víctimas, hablamos de conductas. Tal y como se afirma en ONTSI (2022), "las costumbres online determinan en gran medida la exposición a los ataques". Existe un reconocimiento en la literatura de que los factores de comportamiento humano son la clave para combatir el ciberdelito (Hadlington & Chivers, 2018).

Si nos vamos a los datos de 2020 sobre hábitos y conductas de la ciudadanía, España ya se encuentra en el puesto número 7 de viviendas con acceso a internet de toda la UE (López et al., 2021). Algunas de las conductas más destacables según la ONTSI (2022) son: el acceso a contenidos digitales gratuitos desde webs no oficiales, la descarga e instalación de software, el comercio online y las transacciones no verificables. También, de las personas consultadas en dicho estudio, el 41,1% declara realizar alguna conducta de riesgo a sabiendas; un 59,7% afirma haber sufrido un incidente de seguridad en el último semestre de 2021; el 14,2% manifiesta haber sufrido el ataque de virus o *malware* y alrededor del 14% reconocen haberse quedado sin acceso a servicios debido a ciberataques. De lo anterior se desprende que, a nivel de conductas, existe un problema extendido en la ciudadanía, pero cuando nos vamos al por qué y, concretamente, a la preparación de la ciudadanía, nos encontramos los siguientes datos: Tan solo el 6,6% de internautas se considera totalmente preparado o preparada para afrontar los desafíos de seguridad. El 27,3% manifiesta estar bastante preparado o preparada mientras que el 37,8% declara que lo está suficientemente. El 21,3% se consideran algo preparados y el 6,8% nada preparado (ONTSI, 2022).

A consecuencia de lo anterior ha surgido una mayor conciencia sobre la necesidad de educación en ciberseguridad dirigida a la ciudadanía y población-no técnica. Junto con esta educación en ciberseguridad, y muy ligada a ella, se encuentra la educación en ciberdelincuencia. Consiste en aquella educación dirigida a dar a conocer los peligros de la red, las ciberamenazas y las distintas formas de los ciberdelitos. Por lo tanto, educar y concienciar se hacen más necesarios que nunca y es por todo ello que las instituciones públicas han promovido la cultura de prevención de la cibercriminalidad entre la ciudadanía y empresas. El Ministerio del Interior ha elaborado y puesto en marcha un Plan Estratégico contra la Cibercriminalidad que se articula en torno a seis ejes estratégicos, entre los que están la cultura de prevención de la cibercriminalidad y la potenciación de capacidades (ANDS, 2021).

La educación se muestra una herramienta eficaz a la hora de prevenir y proporcionar herramientas a la ciudadanía, pero también implica una serie de cualidades intrínsecas. Tal y como plantea Ghernaouti-Helie (2009), los programas educativos específicos deben ser eficaces y estar disponibles para cada tipo de población objetivo, por un lado, a responsables políticos, profesionales de la justicia y la policía, gestores, profesionales de las TIC, y por otra parte, a los usuarios finales (incluidos niños y ancianos). Al igual que otros autores, defienden la introducción de conocimientos relacionados con la seguridad informática en los planes de estudio de todos los niveles educativos (Árpád, I., 2013). Cabe preguntarse si las estrategias educativas están siendo adaptadas al siglo

XXI, qué tipo de perfiles profesionales están implicados y cómo mejorar dichas estrategias. La finalidad de esta investigación es responder a estas cuestiones, estableciendo los siguientes objetivos de investigación:

> O1 – Conocer la situación en materia de educación en ciberseguridad dirigida a la población general.
> O2 – Analizar los perfiles profesionales y académicos de los agentes implicados en materia de ciberseguridad.
> O3 – Analizar posibles puntos de mejora en las actuales políticas y proyectos implementados.

En cuanto a las preguntas de investigación, se han planteado las siguientes:

1. Pregunta de investigación: ¿Qué aspectos o qué puntos se podrían mejorar en la educación en ciberseguridad orientada a la población general?
2. Pregunta de investigación: En la organización a la que pertenecen los expertos, ¿trabajan personas provenientes de titulaciones técnicas como informática, telecomunicaciones, TIC, ingenierías, etc.? ¿Y de áreas de ciencias sociales como psicología, sociología, criminología, ciencias de la educación, etc.?
3. Pregunta de investigación: ¿Hay una representación proporcional entre perfiles de titulaciones técnicas y de las ciencias sociales en el ámbito de la educación en ciberseguridad?
4. Pregunta de investigación: ¿Tiene la población general unos conocimientos, preparación y capacidades mínimas en ciberseguridad? ¿Y concienciación sobre la ciberdelincuencia?
5. Pregunta de investigación: ¿Cree que los esfuerzos que se están realizando para educar a la población son proporcionales al avance del ciberdelito y sus técnicas?
6. Pregunta de investigación: ¿La educación en ciberseguridad se está orientando demasiado hacia personal técnico y menos a la población general?
7. Pregunta de investigación: ¿Los proyectos educativos que se están poniendo en marcha, están siendo adaptados y actualizados en las novedades educativas y las técnicas didácticas?

Para alcanzar los objetivos, se ha realizado una consulta a expertos en la materia para que puedan transmitir su opinión de un modo sistemático y estructurado. En la sección de metodología, se describe de forma detallada el procedimiento que se ha puesto en marcha, la justificación del método, el diseño, instrumento y participantes. En resultados, se han detallado de un modo organizado y en profundidad las respuestas de forma separada. En la sección discusión, se debate la cuestión de la educación en ciberseguridad, sus retos, puntos débiles y posibilidades de mejora. Finalmente, en las conclusiones, se han detallado las ideas finales, depuradas y sintetizadas, las limitaciones y algunas propuestas para futuras investigaciones.

2. Metodología

2.1 Diseño

La metodología de juicio de expertos es una técnica que se usa con diversas finalidades "una opinión informada de personas con trayectoria en el tema, que son reconocidas por otros como expertos cualificados, y que pueden dar información, evidencia, juicios y valoraciones" (Escobar & Cuervo, 2008). Es relevante que los jueces sean conocedores del área de conocimiento del que van a dar su opinión. Los jueces expertos son personas que emiten su juicio sobre determinada cuestión y no personal jurisdiccional. El conocimiento puede venir dado, tanto por su experiencia laboral, como por su formación académica. Por lo tanto, para la selección, se debe tener en consideración su educación, ocupación y experiencia y, una vez cerrada la lista, establecer la comunicación para poder realizar la tarea de valoración.

> "*La evaluación mediante el juicio de experto consiste en solicitar a una serie de personas la demanda de un juicio hacia un objeto, un instrumento, un material de enseñanza, o su opinión respecto a un aspecto concreto.*" (Cabero-Almenara & Llorente, 2013)

Entre las ventajas que presenta esta metodología, se encuentran: la calidad de las respuestas que conseguimos sobre el área de estudio en cuestión, el nivel de profundización sobre la temática, facilidad y rapidez para obtener la información, la facilidad a nivel técnico para llevar a cabo la investigación, la diversidad de medios para poder hacer la recogida de información y también la posibilidad de obtener información y datos actualizados sobre el objeto de estudio. Para la aplicación del método y poder garantizar los mejores resultados, lo hemos dividido en cuatro etapas:

1. Cálculo del número de expertos.

2. Confección de la lista de posibles candidatos y envío de los cuestionarios.

3. Selección de los expertos.

4. Recepción de las respuestas y procesamiento de los resultados.

En lo que se refiere al número de expertos finales que deben ser utilizados, cabe señalar que no hay un

acuerdo unánime para su determinación, aunque en líneas generales, suelen oscilar entre 15 y 30 (Escobar-Pérez & Cuervo-Martínez, 2008) "Al escoger un número de expertos menor que nueve, el error medio grupal comienza a aumentar considerablemente. Para un número de expertos mayor de 25 el error medio grupal es prácticamente nulo, lo que significa que escoger un número de expertos mayor complica el trabajo y no mejora significativamente los resultados. De igual forma, se puede determinar que la cantidad óptima de expertos a consultar para la aplicación del método oscila entre 15 y 25" (García & Fernández, 2008). Es un criterio avalado por la experiencia de diferentes autores en la actividad docente investigativa y por la aplicación de este método en investigaciones por más de 25 años.

Las formas de poner en acción la estrategia del juicio de experto son diversas, como las presenciales, las entrevistas o el método Delphi, donde se desarrollan las propuestas de conjunto buscando un acuerdo (Robles & Rojas, 2015). En este estudio, se ha seleccionado la "Agregación individual de los expertos", que consiste en obtener la información de manera individual de cada uno de ellos, sin que estos se encuentren en contacto.

En referencia a la selección de expertos, inicialmente se elaboró una lista de posibles candidatos a encuestar. Se realizó un análisis de la información disponible respecto a la competencia de cada uno de ellos, teniendo en consideración sus condiciones de trabajo y las posibilidades reales de participación. Una vez realizada la lista, se les les hizo llegar anticipadamente el cuestionario junto con los instrumentos para evaluar su capacitación en el tema. Por lo tanto, el procedimiento empleado para esta selección de los expertos ha sido estructurados (frente a otros que procedimientos que carecen de estructura o filtros) Para ello, se emplearon 2 criterios de selección: el biograma y el de competencia experta. La decisión de emplear una combinación de 2 técnicas se tomó para dar una mayor fiabilidad a la hora de hacer la selección.

a) Biograma: Se basa en realizar una biografía del experto en la que se pueden incorporar diferentes aspectos: lugar donde trabaja, años de experiencia, actividades desarrolladas, acciones formativas llevadas a cabo, experiencia en investigación, experiencia en la producción de TIC, años de trabajo, lugares dónde ha trabajado, entre otros. A partir de este biograma, se justifica la selección del experto por parte del investigador. En este caso, se estableció como mecanismo de adecuación del experto que conformen alguno de los siguientes perfiles: haber realizado estudios teóricos o empíricos sobre ciberseguridad/ciberdelincuencia ; haber realizado estudios teóricos o empíricos sobre educación vinculada a ciberseguridad/ciberdelincuencia; ser profesional relacionado con la ciberseguridad/ciberdelincuencia; ser docente de acciones formativas relacionado con el objeto de estudio; participar o haber participado en políticas públicas relacionadas con educación en ciberseguridad/ciberdelincuencia.

b) Una vez elaborada la lista de posibles expertos y confirmada la voluntariedad de estos a participar, se procedió a la calificación con la finalidad de determinar el grado de competencia en el tema que se quiere investigar. El método consiste en usar la autovaloración que la persona realiza en diferentes aspectos e indicadores. En base a ello, se establece un valor que es empleado para seleccionar a los expertos. Entre estos procedimientos, el de mayor significación es el denominado "competencia del experto en el tema (C)" (García & Fernández, 2008). Se obtiene mediante la opinión de los propios expertos hacen sobre su conocimiento y las fuentes a partir de las cuales argumentan y justifican su conocimiento.

Para determinar esta competencia (C); se hizo un cálculo a partir de la opinión del experto sobre su nivel de conocimiento acerca del problema planteado y de las fuentes que le permitan argumentar sus criterios. El cálculo se estableció en la expresión C =1/ 2 (Cc +Ca) donde:

Cc.: Coeficiente de conocimiento o información que tiene el experto acerca del tema. Calculado a partir de la valoración del propio experto en la escala del 0 al 10 y multiplicado por 0,1.

Ca : Coeficiente de argumentación o fundamentación de los criterios de los expertos

Tabla 1. Calificación por argumentación del criterio

Argumentación del criterio		
N°	Aspecto por calificar	Valor
1	Análisis teóricos realizados por el experto	0.3
2	Experiencia obtenida	0.5
3	Trabajos de autores nacionales	0.05
4	Trabajos de autores extranjeros	0.05
5	Conocimiento propio del estado del problema en el extranjero	0.05
6	Intuición del experto	0.05

Fuente: García & Fernández, 2008

Para evaluar el coeficiente de competencia, se empleó el siguiente criterio:

- Sí C está entre 0,8 y 1, el coeficiente de competencia es alto.
- Sí C está entre 0,5 y 0,8 el coeficiente de competencia es medio.
- Sí C está entre 0,25 y 0,5 el coeficiente de competencia es bajo.

En la consulta se incluye la autovaloración y la fuente de argumentación. Posteriormente, en el procesamiento de las encuestas de selección, se obtuvo el coeficiente de competencia del experto, garantizando así una selección estructurada y justificada. Por último, en la fase final del proceso de consulta a los expertos, se elaboran las conclusiones del juicio. Se debe estimar la presencia de variables individuales como la personalidad o las habilidades sociales de los jueces, que pueden generar sesgos a favor de uno o varios aspectos del mismo (Robles & Rojas, 2015).

2.2 Instrumento

En cuanto a los instrumentos de recogida de información en el juicio de experto, de todo el amplio abanico de herramientas que permiten recoger la información de una manera cuantitativa, hemos seleccionado los cuestionarios. El motivo es que permiten dar una información más detallada y extendida. Se han incluido 3 preguntas de desarrollo, una tabla de valoración de 6 preguntas para poder cruzar los datos de una forma numérica, la tabla de argumentación del criterio y una valoración numérica de autocalificación del experto.

2.3 Participantes

El número total de expertos consultados asciende a un total de 42, de los cuales han remitido el cuestionario cumplimentado un total de 10. La identidad se ha anonimizado empleando códigos del E1 al E10 y asignándolos de forma aleatoria. Entre los expertos se encuentran personas de dilatada experiencia y en sectores clave, tanto hombres como mujeres. Muchos de ellos pertenecen a un ámbito principalmente académico, mientras que una parte pequeña son de áreas más prácticas y de intervención directa en el área de estudio.

3. Resultados

En la Tabla 2 se pueden observar los coeficientes de competencia, a través de los cuales se puede determinar la calidad de la argumentación y medir de un modo cuantitativo el nivel de las personas consultadas. Los resultados se obtienen a partir de la autocalificación y la calificación de argumentación que, según el tipo de argumentación, recibirá una puntuación u otra (Tabla1). De los 10 jueces expertos, 3 tienen una puntuación de (C) Alto, ya que son mayores de 0.8, mientras que los otros 7 se encuentran en un nivel medio (entre 0.5 y 0.8). En cuanto a la media total es de 0.7475, por lo que es un nivel medio y cercano al alto, pero sin alcanzarlo (0.8). Por todo ello, se puede afirmar que los distintos jueces expertos tienen una competencia válida para poder respaldar las respuestas aportadas a las preguntas planteadas.

Tabla 2. Coeficiente de competencia de los jueces expertos

	Autocalificación	**Calificación de argumentación**	**Coeficiente de competencia C =1/ 2 (Cc +Ca)**	**Coeficiente (C)**
E1	9	0.5	0.5*(9*0.1+0.5)= 0.7	(C) Medio
E2	9	0.55	0.5*(9*0.1+0.55)=0.725	(C) Medio
E3	9	0.55	0.5*(9*0.1+0.55)=0.7258	(C) Medio
E4	9	0.95	0.5*(9*0.1+0.95)=0.925	(C) Alto
E5	10	0.6	0.5*(10*0.1+0.6)=0.8	(C) Alto
E6	7	0.55	0.5*(7*0.1+0.55)=0.625	(C) Medio
E7	8	0.9	0.5*(8*0.1+0.9)=0.85	(C) Alto
E8	9	0.55	0.5*(9*0.1+0.55)=0.725	(C) Medio
E9	8	0.55	0.5*(8*0.1+0.55)=0.675	(C) Medio
E10	9	0.55	0.5*(9*0.1+0.55)=0.725	(C) Medio
Total	Media: 8,7	6.65	Media 0.7475	(C) Medio

Fuente: Elaboración propia

A continuación, se exponen los resultados encontrados a las preguntas planteadas a los jueces expertos:

Pregunta 1 ¿Qué aspectos o qué puntos cree que se podrían mejorar en la educación en ciberseguridad orientada a la población general?

- E1 señala los conocimientos, la concienciación y las fakes news como elementos claves a tratar. También la importancia de la huella digital, las estafas y las prisas sumadas al desconocimiento.
- E2 señala la sencillez (adaptar los conceptos a la ciudadanía, hacerla entendible). También usa el concepto "democratizar" los conceptos para que sean accesibles a todo el mundo. Fomentar el interés en la ciudadanía que, tal y como indica, las personas atribuyen la responsabilidad a los otros.
- E3 señala que se debe ayudar a detectar estafas como elemento central de la ciberdelincuencia. También afirma que se necesita más información de acceso seguro a Internet, navegación segura, protección de datos, cookies, rastros, etc. Se centra, por lo tanto, en medidas concretas de protección.
- E4 señala que se debe hacer comprender (concienciar) sobre las amenazas que existen y el impacto que puedan tener en sus vidas. Para este experto, la ciudadanía también debería estar en constante actualización, aprendiendo siempre las nuevas medidas de protección, tener una actitud proactiva y también concienciar en la autoprotección.
- E5 señala los riesgos asociados a las TIC: vulneración de privacidad y uso fraudulento. También apunta a que la ciudadanía debe conocer las instituciones a las que acudir en caso de sufrir un riesgo asociado a la ciberseguridad.
- E6 señala en primer lugar la importancia de la huella digital, la falta de concienciación en la población a la hora de publicar información de sus propias vidas en RRSS sin pararse a pensar en las consecuencias. Además, el problema no parece ser solamente que suban su propia información privada, sino que también suben información de sus propios hijos/as.
- E7 señala la necesidad de difusión y accesibilidad de acciones formativas, con una especial atención a los/as jóvenes.
- E8 señala un aspecto clave, el de una especial atención a los perfiles vulnerables "susceptibles de sufrir ataques". También señala, al igual que otros expertos, la necesidad de más campañas por parte de las instituciones públicas. El tercer elemento que resalta es el de la necesidad de actuar sobre la brecha digital existente.
- E9 señala que un elemento de gran peso con relación a la educación. Indica que los proyectos de formación implementados deben ser impartidos por personas que tengan experiencias prácticas. Se destaca la importancia de tener conocimientos prácticos sobre la materia y no solamente académicos para una mayor conexión con la realidad de la ciberseguridad. Estos conocimientos prácticos pueden ser así transmitidos a las personas a las que se dirige la educación.
- E10 señala a la necesidad de mejorar en la divulgación de cara a la ciudadanía, sobre todo en lo que se refiere a la autoprotección y las medidas de seguridad que ponen en marcha las personas. Por último, indica que un punto a mejorar es la falta de recursos y medios.

Pregunta 2: en su organización ¿Trabajan personas provenientes de titulaciones técnicas como informática, telecomunicaciones, TIC, ingenierías, etc.? ¿Y de áreas de ciencias sociales como psicología, sociología, criminología, ciencias de la educación, etc.?

- E1 "Provienen de ambos sectores, tanto técnicos como no técnicos."
- E2 "Sí, hay profesionales de diversas áreas, tanto técnicas como sociales."
- E3 "En mi organización son todos informáticos."
- E4 "Sí, trabajo en una universidad. Sí, por el mismo motivo."
- E5 "Sí, de todo tipo. Asimismo, existen perfiles no técnicos dedicados a la ciberseguridad como economistas, periodistas, abogados, entre otros."
- E6 "Sí"
- E7 "Sí, de ambas áreas. Es una Universidad."
- E8 "En mi entorno suelo ser el único con titulación en informática. El resto de mis compañeros son distintas disciplinas educativas, trabajo social, sociosanitario, etc."
- E9 "Trabajo con gente que viene de titulaciones técnicas y también de ciencias sociales ya que estoy en un ámbito educativo."
- E10 "Trabajamos mayoritariamente de las primeras."

Pregunta 3: ¿Considera que en el ámbito de la educación en ciberseguridad hay una representación proporcional entre perfiles de titulaciones técnicas y de las ciencias sociales?

- E1: Este experto responde negativamente y reafirma la idea de que la mayoría de los perfiles son de tipo técnicos. "No, actualmente la educación en ciberseguridad, y la conciencia que tiene la mayoría de la sociedad, abarca perfiles técnicos."

- E2: De nuevo, va en la misma dirección de la dominancia de las áreas técnicas. También apunta a un cambio en el futuro, con una disminución progresiva. "No, domina las áreas técnicas, aunque creo que esta diferencia tenderá a disminuir con el paso del tiempo. Regulaciones como el RGPD va generando interés en la ciberseguridad a perfiles como abogados y los sistemas de gestión como las ISO 27001, ISO 22301 y el Esquema Nacional de Seguridad permiten a profesionales de otras titulaciones de ciencias acercarse a la ciberseguridad de manera gradual."
- E3: "Creo que no, creo que la ciberseguridad se imparte en titulaciones muy concretas y relacionadas con la materia y que no es una enseñanza de ámbito general ni que se imparta en todas las titulaciones. Podría impartirse más en titulaciones de ciencias sociales."
- E4: "No, de momento suelen tener más peso los perfiles técnicos."
- E5: "Aún no las hay, se entiende la ciberseguridad como una disciplina técnica y no es exclusiva de este ámbito."
- E6: Este experto señala un punto interesante y es que, según el tipo de organización, la situación será una u otra. En el caso de este experto, al pertenecer a una ONG dirigida a la educación, los perfiles prioritarios son de tipo social, pero también afirma que en las anteriores organizaciones eran mayoritarios los perfiles técnicos. "No, los profesionales técnicos son menos numerosos que los de ciencias sociales, pero también es debido al tipo de empresa, es una ONG que se dedica a la educación. Cuando he trabajado en otras empresas, los perfiles técnicos siempre han sido menores a los perfiles humanistas."
- E7: "Hay demasiados técnicos y menos perfiles de sociales."
- E8: En este caso, la percepción del experto es contraria a casi la totalidad de los expertos. Según señala, hay pocos perfiles técnicos y en general desconocen aspectos clave. "Para nada, cada vez que hablo con mis compañeros del tema me doy cuenta de que no saben casi nada de ello..."
- E9: "No, en temas de ciberseguridad la exigencia son carreras técnicas, no obstante, conozco algún perfil que viene de otras ramas y se ha redirigido al mundo de la ciberseguridad, bien con un máster de ello, o con certificaciones de ciberseguridad."
- E10: "No, sobre todo de técnicas."

En la Tabla 3 se pueden ver los resultados totales de las respuestas a las 6 preguntas tipo likert. En general, las respuestas de los expertos son bastante homogénea y en la misma dirección. Las puntuaciones mínimas en cifras absolutas son de 10 y la máxima de 50. En las puntuaciones medias la mínima es de 1 y la máxima de 5. En la primera pregunta, la media es de 1.7, por lo que se puede afirmar que, según los expertos, la sociedad carece de capacidades mínimas en ciberseguridad. En la segunda tenemos un 1,5, así que está en la misma línea de la primera pregunta. Entienden que la población no está preparada debidamente para enfrentarse a los riesgos del ciberespacio y a los ciberdelitos. En la tercera tenemos una puntación de 1.6, afirmando así que los esfuerzos por educar a la población en ciberseguridad son insuficientes frente al ciberdelito.

A partir de las puntuaciones a la pregunta 4 (1,5), se puede afirmar que valoran una falta de concienciación sobre los peligros de la ciberdelincuencia por parte de la población. En la pregunta 5 tenemos la puntuación más alta (3.1), siendo aun así un punto medio de la escala (entre 1 y 5). Se podría decir que no existe acuerdo sobre la cuestión de si se está orientando excesivamente hacia personal técnico frente a la población general. Por último, están en desacuerdo sobre la cuestión de si los proyectos educativos están siendo adaptados y actualizados a las novedades educativas y técnicas didácticas (2,1).

Tabla 3. Valoración de los expertos sobre las preguntas planteadas

Valoración de los expertos tipo Likert (del 1 al 5), siendo: 1 En total desacuerdo/ 2 En desacuerdo / 3 Indiferente / 4 De acuerdo /5 Totalmente de acuerdo			
Pregunta planteada	**Suma**	**Media**	**Desv.**
1. ¿Cree que actualmente la población general tiene unos conocimientos y capacidades mínimas en ciberseguridad?	17	1,7	,948
2. ¿Cree que se está preparando a la población general lo suficiente para enfrentarse a los riesgos del ciberespacio y a los ciberdelitos?	15	1,5	,527
3. ¿Cree que los esfuerzos que se están realizando para educar a la población son proporcionales al avance del ciberdelito y sus técnicas?	16	1,6	1,264
4. ¿Cree que la población general está suficientemente concienciada de los peligros de la ciberdelincuencia?	15	1,5	,500
5. ¿Cree que la educación en ciberseguridad se está orientando demasiado hacia personal técnico y menos a la población general (es decir, a un ámbito académico y profesional y no tanto a la ciudadanía)?	31	3,1	1,286
6. ¿Cree que los proyectos educativos que se están poniendo en marcha, están siendo adaptados y actualizados en las novedades educativas y las técnicas didácticas?	21	2,1	,875
Valores mínimos y máximos	10-50	1-5	

Fuente: Elaboración propia

4. DISCUSIÓN

Tras el análisis de los resultados nos encontramos con varios puntos que son a destacar. En primer lugar, que existe una visión general sobre la falta de concienciación, de conocimientos y de preparación de la población general frente a la ciberdelincuencia (pregunta 1, 2, 3 y 4 tipo likert). Es un punto de especial relevancia ya que, tal y como se ha expuesto en el informe de la ONSTI (2022) y de López et al. (2021), se afirma que el crecimiento de la ciberdelincuencia se va acelerando, cada día es mayor y con una mayor incidencia en la población general. El consenso de los expertos también va de acorde a dichos informes cuando se informa de la autopercepción de la población y su propia falta de capacitación para protegerse. En cuanto a las altas tasas de conductas de riesgo (ONSTI, 2022), van en línea con los resultados encontrados en este estudio, donde los jueces expertos afirman en la pregunta 4 (Likert) que la ciudadanía no está concienciada sobre la problemática.

Actualmente, se han puesto en marcha diversas campañas de concienciación, sin embargo, tenemos también los resultados encontrados en el informe anual elaborado por la ONTSI (2022). Dicho informe señala que las campañas no llegan bien a la ciudadanía ya que el 48,8% de las personas consultadas declara no conocer ninguna en concreto. Precisamente uno de los expertos (E5), en la pregunta de desarrollo 1, va en esta misma línea cuando defiende que "*La ciudadanía debe conocer las instituciones a las que acudir en caso de sufrir un riesgo asociado a la ciberseguridad*". Las campañas deben arrojar luz a la ciudadanía para conocer los medios públicos a su disposición para prevenir y actuar ante un ciberataque. Sobre las formas en que se podría mejorar en la educación en ciberseguridad (pregunta 1 de desarrollo), las opiniones son variadas, aunque con algunos patrones en común. Es habitual incluir la mejora y aumento de campañas y divulgación. Esta afirmación es coherente con lo dicho anteriormente, ya que las campañas no están llegando correctamente a la ciudadanía. Por todo ello, sería necesario aumentarlas y mejorarlas.

Es común a prácticamente a todos los expertos la importancia de la concienciación sobre las ciberamenazas y no solamente la adquisición de medidas de autoprotección. La relevancia de este dato reside en que la concienciación está directamente relacionada con el conocimiento y el comportamiento online (Zwilling et al., 2022). En este punto, la educación puede suponer un punto de partida desde el cual mejorar la conciencia. La educación aporta conocimientos para protegernos, pero también una mayor comprensión sobre la amenaza, cómo detectarla y cuál puede ser el origen de la victimización. Con relación a las amenazas, los expertos señalaron las estafas como un elemento de especial preocupación y en incluirlo como elemento clave a la hora de educar a la población.

En cuanto a colectivos y población diana, fueron 2 los expertos que señalaran a grupos específicos. En el primer caso, se señala a la población joven como de especial importancia para recibir la educación. En el segundo caso, se habla de perfiles más vulnerables, precisamente aquellos a los que se ha redirigido la ciberdelincuencia tras los años del COVID-19, tal y como señala Miró (2021). Existirían colectivos con una mayor necesidad de educación y para los que sería necesario personalizar la educación. Es en este punto donde entrarían las ciencias de la educación para poder adaptarse a los distintos perfiles según sus características (niños, jóvenes, adultos, personas mayores, diversidad intelectual y funcional, población migrante, etc.). En cuanto a quiénes tienen que educar, uno de los expertos (E9) en la pregunta de desarrollo 1, señala la importancia de que tengan conocimientos prácticos y no solamente teóricos o académicos. Esta indicación reafirma la importancia de la cercanía entre profesionales y ciudadanía, en la misma línea que el experto E2 en la pregunta de desarrollo 1, donde habla de "democratizar" la educación en ciberseguridad.

Abordando la cuestión de los perfiles técnicos o relacionados con las ciencias sociales (pregunta 2 de desarrollo), podemos observar que mayoritariamente los perfiles en las organizaciones de los expertos son variados o mixtos. Solamente 2 afirman que son predominantemente informáticos/técnicos. Estos últimos irían en la línea de Sánchez et al., (2022), quienes señalan que los equipos y expertos encargados de la ciberseguridad tienen un perfil técnico, con una alta preparación en informática, pero no sobre el comportamiento humano, la incidencia de la cultura y la formación. También se debe resaltar que, la afirmación de los expertos sobre perfiles multidisciplinares en su entorno de trabajo (8 de 10), puede ser debido a que muchos/as pertenecen a instituciones universitarias y académicas, donde es habitual que haya todo tipo de perfiles.

La pregunta 3 de desarrollo reafirma lo anteriormente dicho, ya que, aunque casi todos/as afirman que en su institución están presentes distintos tipos de perfiles, cuando se les pregunta "*¿Considera que en el ámbito de la educación en ciberseguridad hay una representación proporcional entre perfiles de titulaciones técnicas y de las ciencias sociales?*", la respuesta mayoritaria es negativa, que son mayoritariamente técnicos. De hecho, uno de los expertos argumenta su respuesta en la línea de lo

anteriormente expuesto que, los perfiles técnicos o mixtos, se agrupan según las organizaciones: por una parte, ONGs, Universidades, etc. con perfiles variados y con representación de CCSS, mientras que en otras serían predominantes las técnicas.

El análisis de estas 2 cuestiones tiene su importancia en que cuando hablamos de educación en ciberseguridad, cibercrimen, víctimas, concienciación, etc. hablamos de criminología, psicología, educación, ciencias políticas, derecho, etc. Sin embargo, en muchas ocasiones nos encontramos que los autores provienen exclusivamente de ciencias de la computación o informática (Sánchez et al., 2022). Es en este punto donde hay que resaltar el hecho de que la ciberdelincuencia es un fenómeno complejo que requiere un enfoque interdisciplinar (López et al., 2021; Ghernaouti-Helie, 2009). Las respuestas de los expertos apuntan en la misma dirección de forma general, a pesar de que afirman trabajar en entornos con una presencia de profesionales variada.

Finalmente, otro punto de especial interés es el encontrado a raíz de los resultados de la pregunta 6 (Likert). Se señala la falta de adaptación de las técnicas empleadas para educar. Aunque existen novedades e innovaciones, no se están poniendo en marcha a un nivel práctico. Desde las ciencias de la educación y ramas relacionadas, se investiga y se prueban nuevas formas enseñanza, con una fuerte implementación de las TIC, la gamificación y la simulación (Zhang-Kennedy & Chiasson, 2021; Coenraad et al., 2020). Dichas innovaciones deben ser puestas a disposición de la educación en ciberseguridad en el terreno práctico. También con relación a esto nos encontramos las respuestas a la pregunta 3 (likert) donde los expertos están en desacuerdo con que los esfuerzos que se están realizando para educar a la población son proporcionales al avance del ciberdelito y sus técnicas. Se desprende de estas ideas la necesidad de readaptar las estrategias educativas a las novedades de la ciberdelincuencia. Del mismo modo que si fuese una carrera tecnológica, la autoprotección debe tener siempre puesta la mirada en las nuevas formas de ciberataques.

5. CONCLUSIONES

En esta investigación se ha consultado a expertos en el ámbito de la educación en ciberseguridad para conocer sus opiniones y percepciones basadas en amplia experiencia y formación. Se les ha planteado 3 cuestiones de desarrollo y 6 de tipo likert, con un cuestionario final para calificación de validez como expertos. De las respuestas obtenidas se muestra una realidad que no se corresponde con las necesidades a las que se enfrenta la sociedad. En primer lugar, aunque son necesarios perfiles procedentes de distintas áreas, incluidas las Ciencias Sociales, la realidad es que por lo general predominan los perfiles técnicos. La falta de equipos interdisciplinares con personas procedentes de derecho, criminología, psicología, sociología o ciencias de la educación pueden provocar una carencia de otras perspectivas o conocimientos de gran importancia a la hora de abordar la ciberdelincuencia.

También se puede afirmar que la percepción de los expertos sobre la ciudadanía es clara: existe una gran falta de concienciación, conocimientos y preparación por parte de las personas no-técnicas para protegerse a sí mismas y a sus familias. Esta carencia se refleja en las estadísticas de ciberdelincuencia, que van en aumento cada año y con previsiones de que a la larga los delitos online puedan superar a los tradicionales (offline). A esto se añade la falta de adaptar las técnicas y estrategias educativas al ámbito y aumentar la educación dirigida a la población general, no solo la dirigida a personal técnico o avanzado. En cuanto a las propuestas de mejora, hay consenso sobre que se deben mejorar y aumentar las campañas de divulgación dirigidas a la población, incluyendo información sobre ciberamenazas y ciberdelitos (con especial atención a las estafas), medidas de autoprotección y una atención a determinados perfiles.

Por último, analizando todos los resultados de forma conjunta, existe una idea general compartida por los expertos: hay una falta de más y mejores estrategias de educación, más divulgación y visibilización de la problemática, una mejor adaptación de los medios educativos y más énfasis en concienciar sobre las ciberamenazas. Las políticas y estrategias que se implementan por parte de las instituciones son las responsables directas a la hora de mejorar esta autoprotección. Por lo tanto, es de especial relevancia que la administración pública esté actualizada y pueda reajustar su respuesta de acorde con la realidad vigente, por ejemplo, reformulando las campañas de divulgación o mejorando las técnicas educativas. En caso contrario, esa necesidad detectada se convertirá en victimización con el paso del tiempo.

Las limitaciones del estudio fueron la escasa participación de los expertos consultados y posibles sesgos en las preguntas. De los 42 expertos a los que se les envió el cuestionario, tan solo 10 respondieron. La redacción de las preguntas de investigación puede siempre pueden incluir sesgos al dirigir la investigación (y en este caso las respuestas de los expertos) a unas determinadas posiciones u opiniones. Con todo, las implicaciones de este estudio son relevantes de cara a la mejora de las posibles mejoras en la educación en ciberseguridad y la concienciación ante la ciberdelincuencia. Se debe destacar la problemática de la excesiva orientación de la educación hacia personal técnico y a un nivel avanzado frente a la educación básica a la ciudadanía general. Para futuras

investigaciones, sería interesante profundizar en formas concretas de mejorar las campañas de educación en ciberseguridad y en cómo redefinir las estrategias actuales. También ampliar la información sobre metodologías concretas que perfeccionen la enseñanza y el aprendizaje de ciberseguridad en la población general.

Referencias

ANDS (Asociación Nacional de Directores de Seguridad). (2021). Plan Estratégico contra la Cibercriminalidad. *Asociación Nacional de Directores de Seguridad*. Recuperado de https://directoresdeseguridad.es/2021/03/16/plan-estrategico-contra-la-cibercriminalidad/

Árpád, I. (2013). A Greater Involvement of Education in Fight Against Cybercrime. *Procedia - Social and Behavioral Sciences*, 83, 371–377. Doi: https://doi.org/10.1016/J.SBSPRO.2013.06.073

Cabero-Almenara, J., & Llorente, M. (2013). La aplicación del juicio de experto como técnica de evaluación de las tecnologías de la información y comunicación (TIC). *Eduweb*, 7(2), 11–22. Recuperado de http://tecnologiaedu.us.es/tecnoedu/images/stories/jca107.pdf

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation and Gaming*, *51*(5), 586–611. https://doi.org/10.1177/1046878120933312

DSN. (2019). Estrategia Nacional de Ciberseguridad 2019. *Departamento de Seguridad Nacional, España*. Recuperado de: https://www.dsn.gob.es/es/documento/estrategia-nacional-ciberseguridad-2019

Escobar-Pérez, J., & Cuervo-Martínez, Á. (2008). Validez de contenido y Juicio de Expertos: Una Aproximación a Su Utilización. *Avances En Medición*, 6, 27–36 . Recuperado de https://www.researchgate.net/publication/302438451_Validez_de_contenido_y_juicio_de_expertos_Una_aproximacion_a_su_utilizacion

García, L., & Fernández, S. J. (2008). Procedimiento de aplicación del trabajo creativo en grupo de expertos. *Ingeniería Energética, XXIX* (2),46-50. Consultado el 16 de Abril de 2022. Recuperado de https://www.redalyc.org/articulo.oa?id=329127758006

Ghernaouti-Helie, S. (2009). An Inclusive Information Society Needs a Global Approach of Information Security. *2009 International Conference on Availability, Reliability and Security*, 658-662. DOI: 10.1109/ARES.2009.127

Hadlington, L., & Chivers, S. (2020). Segmentation Analysis of Susceptibility to Cybercrime: Exploring Individual Differences in Information Security Awareness and Personality Factors. *Policing: A Journal of Policy and Practice*, 14, 479-492. DOI:10.1093/police/pay027

López, J., Sánchez, F., Herrera, D., Martínez, F., Rubio, M., Gil, V., Santiago, A.M., & Gómez, M.A . (2021). Informe sobre la Cibercriminalidad en España. Dirección General de Coordinación y Estudios Secretaría de Estado de Seguridad . Ministerio del Interior, España. Recuperado de https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

Miró, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP. Revista de Internet, Derecho y Política*, núm. 32 (marzo). UOC. http://dx.doi.org/10.7238/idp.v0i32.373815

ONTSI (Observatorio Nacional de Tecnología y Sociedad). (2022). Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. *Observaciber*. Recuperado de https://www.observaciber.es/sites/observaciber/files/media/documents/ciudadaniaciberriesgos_abril2022_1.pdf

Robles, P. & Rojas, M. (2015). La validación por juicio de expertos: dos investigaciones cualitativas en Lingüística aplicada. *Revista Nebrija de Lingüística Aplicada* (2015) 18. Recuperado de: https://www.nebrija.com/revista-linguistica/files/articulosPDF/articulo_55002aca89c37.pdf

Sánchez, F., Martínez, J.E., & Téllez, A. (2022). La seguridad en el ciberespacio desde una perspectiva sociocultural. *Methaodos Revista De Ciencias Sociales*, *10*(2), 243–258. https://doi.org/10.17502/mrcs.v10i2.577

Zhang-Kennedy, L., & Chiasson, S. (2021). A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education. *ACM Computing Surveys*, *54*(1), 1–39. https://doi.org/10.1145/3427920

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. *Journal of Computer Information Systems*, *62*(1), 82–97. https://doi.org/10.1080/08874417.2020.1712269