Actas del Congreso Iberoamericano de Docentes

Un instrumento de evaluación de la formación del profesorado en materia de ciberseguridad

Noemí De Castro-

Cristina López Gómez

ISBN: 978-84-948417-0-5

Edita **Asociación Formación IB**.

Coordinación editorial: **Joaquín Asenjo Pérez, Óscar Macías Álvarez, Patricia Ávalo Ortega y Yoel Yucra Beisaga**

Año de edición: **2018**

Presidente del Comité Científico: **César Bernal.**

El I Congreso Iberoamericano de Docentes se ha celebrado organizado conjuntamente por la Universidad de Cádiz y la Asociación Formación IB con el apoyo del Ayuntamiento de Algeciras y la Asociación Diverciencia entre otras instituciones.

http://congreso.formacionib.org

red iberoamericana de docentes

UCA Universidad de Cádiz

formaciónib

Un instrumento de evaluación de la formación del profesorado en materia de ciberseguridad

Noemí DeCastro-García[1]* y Crístina López Gómez[2]*

*Universidad de León

[1]ncasg@unileon.es; [2]clopeg04@estudiantes.unileon.es

Resumen

En el contexto actual, la educación está inmersa en continuos y numerosos cambios, principalmente relacionados con la inclusión en las aulas de las tecnologías de la información y la comunicación. Estos recursos pueden suponer una serie de riesgos y consecuencias desconocidos para los usuarios en la mayoría de las ocasiones. A partir de la necesidad de incorporar la ciberseguridad en los centros educativos, en el presente trabajo se presenta un instrumento combinado de evaluación que sirve para valorar el grado de concienciación y formación que el profesorado tiene en materia de ciberseguridad. La herramienta se centra en cinco dimensiones clave en el ámbito educativo. La validez de contenido del instrumento se ha estimado mediante un juicio de expertos.

Introducción

En la actual sociedad del conocimiento las tecnologías de la información y la comunicación (TIC) se integran en la educación desde diferentes ámbitos: la digitalización de las instituciones educativas, el desarrollo en el alumnado de competencias digitales, recursos didácticos interactivos y/o las nuevas plataformas de interacción entre los agentes involucrados. Cada una de estas perspectivas implica diferentes riesgos que crecen a medida que aumenta el interés en los datos generados, evolucionan a la vez que las amenazas en la red, y ponen en riesgo la imagen, información e incluso, la seguridad física y mental de los usuarios.

Ante la realidad descrita, se hace necesario emprender estrategias que aseguren que se cumplen los criterios de calidad y seguridad requeridos en la escuela. Es necesario, por ejemplo, que los centros educativos cuenten con la instalación de un software de filtrado y protección de contenidos inadecuados para la web para proporcionar a los/as estudiantes una experiencia digital segura (Smoothwall, 2011; Giant, 2016). Por otra parte, se ha de prestar especial atención al control de las tecnologías móviles y su uso (Department for Education, 2012). Además, las leyes internacionales de protección de datos establecen que cualquier organismo que tenga responsabilidad sobre la administración educativa ha de implantar una normativa de seguridad en Internet para los menores que tenga como función controlar el acceso de

los jóvenes a contenidos inapropiados o potencialmente dañinos, garantizar la seguridad de los jóvenes y profesorado al utilizar las TIC, así como proteger a los menores de actividades que sean ilegales. Por último, el ciberacoso o cyberbulling es un problema íntimamente ligado con la ciberseguridad y altamente relevante en el contexto docente (Belsey, 2005; Giménez-Gualdo, Arnaiz-Sánchez, Cerezo-Ramírez y Prodócimo, 2018; Yudes-Gómez, Baridon-Chauvie y González-Cabrera, 2018).

Por las razones descritas es recomendable que los miembros de la comunidad educativa posean una formación básica en nuevas tecnologías, protección de datos y riesgos en la red (Giant, 2016). Como primer paso, se ha de comenzar por estudiar cuál es y a qué nivel está la formación docente general en materia de ciberseguridad. En esta línea de investigación se enmarca este trabajo cuyo objetivo principal es elaborar un instrumento de evaluación que permita extraer conclusiones sobre la concienciación y formación que tiene el profesorado en ciberseguridad. La elaboración del instrumento de evaluación se ha hecho en base a las cinco dimensiones de la ciberseguridad que están más estrechamente relacionadas con la labor profesional docente diaria según la formación especializada para educadores propuesta por el Instituto Nacional de Ciberseguridad de España (INCIBE, 2018) y la búsqueda sistemática realizada en diferentes fuentes de información.

La estimación de validez de contenido se ha realizado a través de juicio de expertos (Skjong y Wentworht, 2000; Escobar y Cuervo, 2008). Se han valorado los resultados y se ha propuesto un instrumento final mejorado combinado que incluye un test informativo de respuesta cerrada con 5 preguntas, y una rúbrica de evaluación con 20 descriptores divididos en 5 bloques cuya escala de valoración es de 5 niveles.

Método

Procedimiento

Este trabajo se ha realizado con una metodología de investigación mixta cuasi-experimental.

La herramienta se ha elaborado siguiendo las sugerencias de Gatica-Lara y Uribarren-Berrueta (2013), y Herman, Aschbacher y Winters (1992).

Participantes

La elección de los expertos se ha basado en su reputación en la comunidad, la disponibilidad y la motivación para participar (Skjong y Wentworht, 2000). La herramienta fue enviada a cuatro expertos: del ámbito de la ciberseguridad, del educativo, y dos que se encontraban en la intersección de ambos campos. Tenían entre entre 6 y 20 años de experiencia.

Materiales y recogida de información

La valoración de los expertos se recogió mediante una planilla que tomaba como base la propuesta en Escobar y Cuervo (2008). Con ella se han medido diferentes categorías de los descriptores: claridad, coherencia, relevancia, claridad, suficiencia de los niveles u opciones de respuesta, comentarios y sugerencias.

La planilla fue enviada a los expertos a través de correo electrónico explicándoles cuál era el objetivo de la valoración, las instrucciones de cumplimentación y una descripción sobre el significado de cada valoración en cada ítem.

Análisis de datos

Existen diferentes métodos para la estimación de la validez de contenido de un instrumento de evaluación mediante juicio de expertos (Pedrosa, Suárez y García, 2013). En base a las características de la investigación, el método para la estimación de la validez de contenido del instrumento de evaluación ha sido el coeficiente de validez de contenido (CVC) de Hernández-Nieto (2002). Se ha tomado como umbral de mantenimiento de ítems aquellos con un CVC superior a 0.80 (Hernández Nieto, 2002). Además, se ha elaborado un registro con las sugerencias y comentarios más comunes entre los expertos.

Resultados y propuesta

El instrumento inicial tenía dos partes: un test informativo cerrado con una sola opción correcta (Parte I), y una rúbrica de evaluación (Parte II). Ambas se basan en la evaluación de cinco dimensiones clave: privacidad, seguridad, ciber acoso, actuación y respuesta ante incidentes, y formación y concienciación en ciberseguridad. El cuestionario tenía 4 preguntas cerradas con una sola opción correcta. La rúbrica de evaluación tiene 5 bloques de evaluación con un total de 20 descriptores (4,4,4,3 y 5, respectivamente).

Resultados del juicio de expertos

Como podemos observar en la figura 1, ninguna de las preguntas del test superó el umbral establecido en términos de claridad. Entre las sugerencias más destacadas estuvieron la modificación en la redacción de las preguntas, correcciones de erratas y precisión terminológica.

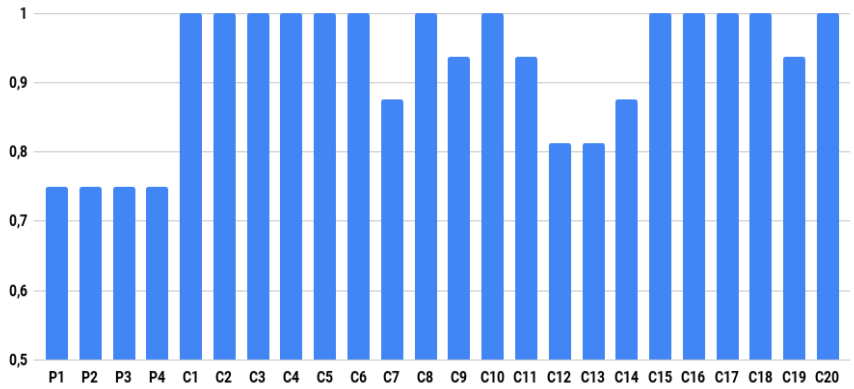

Figura 1. CVC de claridad de cada criterio.

La información de la figura 2 concluye que el 12.5% de los ítems no superó el umbral marcado en relevancia. La sugerencia más frecuente estaba relacionada con la concreción y adición de determinados conceptos ausentes.

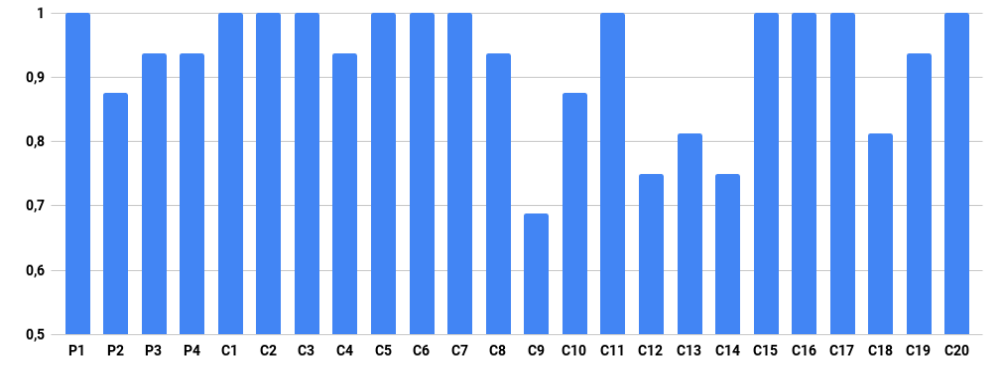

Figura 2. CVC de relevancia de cada criterio.

La figura 3 muestra que el 100% de los ítems superó el umbral marcado para la coherencia del criterio.

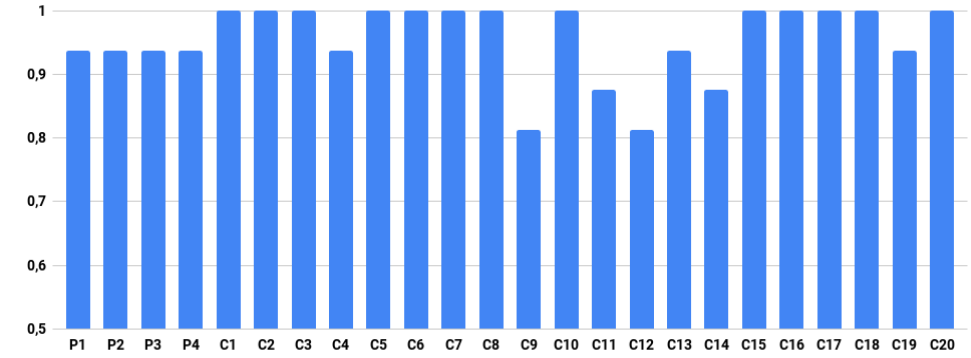

Figura 3. CVC de coherencia de cada criterio.

El análisis mostrado en la figura 4 concluye que el 33.3 % no superó el umbral establecido en claridad de los niveles. Los comentarios de los expertos remarcaron la necesidad de concretar los términos usados.

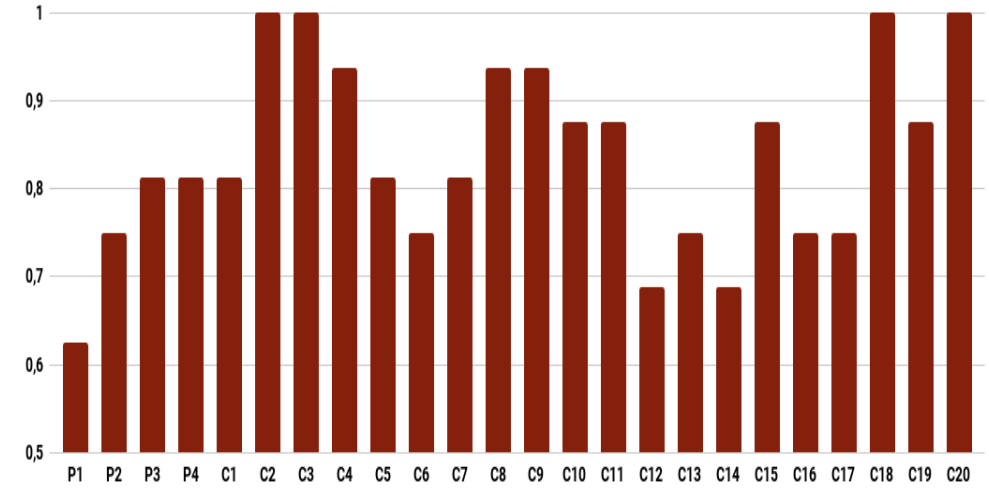

Figura 4. CVC de la claridad de los niveles de respuesta

La información de la figura 5 muestra que el 29.16 % de los niveles no superaban el umbral de adecuación, destacando que ninguno de los pertenecientes al bloque del test lo superó. Las sugerencias mayoritarias remarcaron la necesidad de que los niveles fueran completamente disjuntos entre sí. Además, se encontró más de una opción correcta en P1,P2,P3 y P4. Por otra parte, se recomendó intercambiar el orden de algunos niveles en C5 y C17.

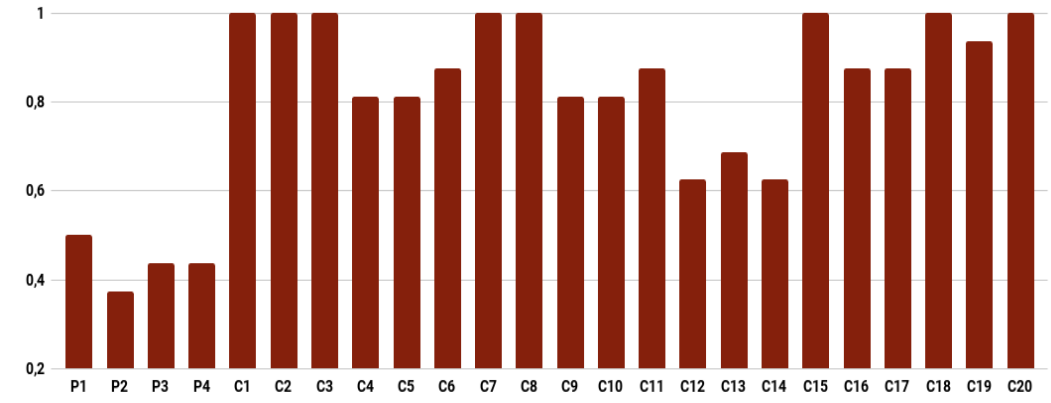

Figura 5. CVC de la adecuación de los niveles de respuesta

Por último, otra sugerencia significativa fue la recomendación de modificar en el cuestionario los términos de seguridad por ciberseguridad, y el de seguridad por sistemas de autenticación y controles de acceso. Además, se añadieron dos preguntas más.

Propuesta final

El instrumento de evaluación propuesto se encuentra en el Anexo.

Conclusiones

En este trabajo se presenta un instrumento de evaluación para analizar el nivel de formación y concienciación docente en ciberseguridad. Se ha creado una herramienta combinada, y compuesta por una rúbrica de evaluación y un test informativo cerrado, validada mediante juicio de expertos.

Los resultados obtenidos con la aplicación de esta herramienta a diferentes centros educativos y agentes involucrados aportará puntos clave para proponer líneas de actuación que permitan adecuar la formación en ciberseguridad a los criterios de calidad requeridos en la sociedad actual.

Referencias bibliográficas

Belsey B (2005). *Cyberbullying: An emerging threat to the "always on" generation.* Recuperado de http://www.cyberbullying.ca

Department for Education (2012). *Principles of E-Safety*: *Mobile and Wi-fi Technologies in Educational Settings*. Londres: DfE.

Escobar, J., y Cuervo, A. (2008). Validez de contenido y juicio de expertos: una aproximación a su utilización. *Avances en Medición, 6,* 27-36.

Gatica-Lara, F., y Uribarren-Berrueta, T. D. N. J. (2013). ¿Cómo elaborar una rúbrica?

Investigación en educación médica,2(5), 61-65.

Giant, N. (2016). *Ciber-seguridad para la i-Generación. Usos y riesgos de las redes sociales y sus aplicaciones.* Madrid: Narcea, S.A de Ediciones.

Giménez-Gualdo, A., Arnaiz-Sánchez, P., Cerezo-Ramírez, F. y Prodócimo, E. (2018). Percepción de docentes y estudiantes sobre el ciberacoso. Estrategias de intervención y afrontamiento en Educación Primaria y Secundaria. *Comunicar, 56*, 29-38. https://doi.org/10.3916/C56-2018-03

Herman, J.L., Aschbacher, P.R., y Winters, L. (1992). A practical guide to alternative assessment. Alexandria, VA: Association for Supervision and Curriculum Development. (ERIC Document Reproduction Service No. ED352389)

Hernández-Nieto, R. A. (2002), *Contributions to Statistical Analysis*. Mérida, Venezuela: Universidad de Los Andes.

Instituto Nacional de Ciberseguridad, INCIBE (2018), Internet Segura for Kids (IS4K), Recuperado de https://www.is4k.es

Pedrosa, I., Suárez, J., y García, E. (2013). Evidencias sobre la validez de contenidos: avances teóricos y métodos para su estimación. *Acción Psicológica, 10* (2), 3-18.

Skong. R. y Wentworth, B. (2000). *Expert Judgement and risk perception.* Recuperado de http://research.dnv.com/skj/Papers/SkjWen.pdf

Smoothwall (2011). e-*Safety in Education: A Discussion Document on Standards, Liability and the Implications of Local Control*. Leeds: Smoothwall UK.

Yudes-Gómez, C., Baridon-Chauvie, D. y González-Cabrera, J. (2018). Ciberacoso y uso problemático de Internet en Colombia, Uruguay y España: Un estudio transcultural]. *Comunicar, 56*, 49-58. https://doi.org/10.3916/C56-2018-05

Anexo

En la tabla 1 y las figuras 6-11 se muestra el instrumento de evaluación propuesto.

Tabla 1.
Parte I: Test informativo

Bloque 0: ¿Sabes lo que es…?	
Pregunta 1 ¿Qué es la privacidad en la web?	1. Está relacionada sólo con la protección de datos personales. 2. Permite controlar quién puede tener acceso a la información que posee un determinado usuario que se conecta a internet. 3. Permite controlar quién puede tener acceso a la información que posee un determinado usuario que se conecta a internet, y está relacionada con la protección de datos personales. 4. Es una forma de acoso que tiene lugar en internet y redes sociales. Además es una amenaza que se da en la actualidad y puede provocar que un niño o adolescente se sienta amenazado, acosado, humillado y avergonzado por otro niño o adolescente. 5. La opción 2,3 y 4 son verdaderas.
Pregunta 2 ¿Qué es un sistema de autenticación?	1. Es aquel que garantiza la seguridad de tus dispositivos tecnológicos. 2. Es aquel que tiene como uso el proceso de confirmar que algo (o alguien) es quien dice ser, fomentando la seguridad y el acceso la información. 3. La 1 y la 2 son verdaderas. 4. Consiste en un conjunto de políticas, prácticas y tecnología que evitan los ataques a las redes y a los recursos accesibles de la red. 5. La 1 es verdadera.
Pregunta 3. ¿Qué es el ciberacoso o cyberbullin g?	1. Es una forma de acoso que tiene lugar sólo en la calle 2. Es una forma de acoso que tiene lugar en internet y redes sociales. 3. Es una forma de acoso que tiene lugar en internet y redes sociales. Además es una amenaza que se da en la actualidad y puede provocar que un niño o adolescente se sienta amenazado, acosado, humillado y avergonzado por otro niño o adolescente. 4. La opción 2 y 3 son verdaderas. 5. Es un conjunto de políticas, prácticas y tecnología que evitan los ataques a las redes y a los recursos accesibles de la red.
Pregunta 4. ¿Qué es la ciberseguri dad,	1. Consiste en un conjunto de políticas, prácticas y tecnología que evitan los ataques en las redes. 2. Se basa en la protección de la información digital, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información.

/seguridad en la Web?	3. Está organizada sobre un conjunto de políticas, prácticas y tecnología que evitan los ataques a las redes y a los recursos accesibles de la red. Junto con la protección de la privacidad y de garantizar que el uso de esa red sea óptimo y que los propios usuarios posean únicamente derechos que les han sido concedidos. 4. Permite controlar quien puede tener acceso a la información que posee un determinado usuario que se conecta a Internet, y está relacionada con la protección de tus datos personales. 5. Todas las anteriores son verdaderas.
Pregunta 5. ¿Qué es el programa de Cibercooperantes?	1. **Promueve la colaboración de personas particulares interesadas en la divulgación de la ciberseguridad a través de charlas de sensibilización** 2. **Cuenta con centros que requieren de formación en ciberseguridad, destinado a niños, jóvenes, padres, madres y educadores.** 3. Se basa en la protección de la información digital, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información. 4. La 1 y la 2 son verdaderas. 5. Es aquel programa que tiene como uso el proceso de confirmar que algo (o alguien) es quien dice ser, fomentando la seguridad y el acceso la información.

Criterios	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4
Bloque I: Privacidad					
1. ¿Sabes si el centro educativo cuenta con software informáticos para proteger la privacidad de la información relativa, tanto de los estudiantes, como de la propia institución educativa?	No tengo conocimiento sobre la existencia de este tipo de programas informáticos en el centro educativo.	El centro educativo no cuenta con este tipo de programas informáticos.	El centro educativo cuenta con algún programa informático de este tipo, pero no hace un uso efectivo del mismo.	El centro educativo cuenta con programas informáticos de este tipo, pero no existe un control habitual sobre el funcionamiento de los mismos.	El centro educativo utiliza gran variedad de programas informáticos de este tipo y, además, tiene un control frecuente sobre los mismos.
2. En base a la plataforma web educativa de la que disponga el centro educativo, como blogs, redes sociales o Moodle, ¿cuál es su política de actuación para compartir adecuadamente las fotos de sus estudiantes menores de edad, evitando conflictos legales?	No tengo conocimiento sobre que haya que tomar ningún tipo de medida con respecto a imágenes o fotografías de los estudiantes.	Comparto las fotos de los alumnos en la web sin tomar ninguna medida específica.	Comparto las fotos de los alumnos en la web pixelando los rostros.	Comparto las fotos de los alumnos en la web tomando medidas específicas, como el cifrado de las fotografías, o el pixelado de los rostros.	Comparto las fotos de los alumnos en la web tomando medidas específicas: el cifrado de las fotografías, el pixelado de los rostros y presto especial atención a que no se pueda deducir información conflictiva como la hora en la que los estudiantes se encuentran en un lugar concreto.
3. ¿Sabe qué medidas se han de tomar en la gestión y almacenamiento las fotos de sus estudiantes para evitar y prevenir conflictos legales?	No tengo conocimiento sobre que haya que tomar ninguna medida de seguridad en la gestión y almacenamiento de dichas imágenes.	Guardo las imágenes de los menores sin seguridad, ya que considero que no es importante.	Guardo y almaceno las imágenes de los menores en equipos que disponen de medidas de seguridad, ya que considero que es importante.	Guardo las imágenes de los menores de manera cifrada, pero no tengo en cuenta la seguridad de los dispositivos de almacenamiento de éstas.	Guardo las imágenes de los menores de manera cifrada y en dispositivos que tienen medidas de seguridad de acceso añadidas.
4. ¿Se pide autorización expresa a las familias cuando se suben fotos de los menores de edad a las diferentes plataformas web o redes sociales del centro?	No tengo conocimiento sobre el funcionamiento de dicha autorización parental.	No se pide autorización a las familias y/o tutores.	Sí, se tiene en cuenta la autorización de los padres y/o tutores, pero en más de una ocasión no se ha solicitado.	Sí se pide autorización a las familias. Además este consentimiento se hace por escrito, para poder guardarlo como justificante.	Sí, se pide autorización por escrito a las familias informando a las mismas de sus derechos que se recogen en la Ley de Protección de datos del menor, para evitar conflictos legales. Además este consentimiento se hace por escrito para poder guardarlo como justificante y existe un procedimiento de revisión periódica y de mejora continua.

Figura 6. Bloque I de Parte II.

Bloque II: Sistemas de autenticación y controles de acceso					
5. ¿Utilizas una contraseña de acceso o patrón para acceder tanto a tus dispositivos como a la información que contengan los mismos?	No tengo conocimiento sobre lo que es una contraseña de acceso.	No dispongo de una contraseña de acceso, ya que considero que no es importante.	Sí que dispongo de una contraseña de acceso, y es la misma para todos mis dispositivos y cuentas de correo electrónico.	Sí que dispongo de una contraseña de acceso y la(s) tengo apuntada(s) de manera visible y/o pública. (Por ejemplo, al lado del ordenador). Pero las contraseñas que utilizo son iguales en todos los dispositivos.	Sí que dispongo de una contraseña de acceso, la mantengo en secreto y hay un cambio de contraseñas cada cierto tiempo.
6. ¿Utilizas una contraseña de acceso fuerte para acceder tanto a tus dispositivos como a la información que contengan los mismos?	No tengo conocimiento sobre lo que es una contraseña de este tipo.	Sí que dispongo de una contraseña de acceso, pero la misma es de carácter débil y de fácil acceso y es la misma para todos los dispositivos y cuentas de correo.	Sí que dispongo de un sistema de contraseñas teniendo un carácter fuerte, pero es la misma para todos mis equipos y cuentas de correo electrónico.	Sí que dispongo de una contraseña de acceso, pero la misma es de carácter débil y de fácil acceso, aunque tengo contraseñas diferentes para cada dispositivo y/o cuentas de correo.	Sí que dispongo de una contraseña de acceso de carácter fuerte, y es diferente para cada dispositivo y cuenta de correo, y se cambian a lo largo del tiempo.
7. Las contraseñas de acceso que tienen los dispositivos informáticos del centro educativo, ¿son de carácter fuerte?	No tengo conocimiento sobre lo que es una contraseña de este tipo.	Sí que disponen de una contraseña de acceso, pero la misma es de carácter débil y de fácil acceso. Además, es la misma para todos los miembros de la institución.	Sí que disponen de un sistema de contraseñas teniendo un carácter fuerte, pero es la misma para todos los miembros de la institución.	Sí que disponen de una contraseña de acceso, pero la misma es de carácter débil y de fácil acceso. Sin embargo existen contraseñas diferentes para cada miembro de la institución.	Sí que disponen de una contraseña de acceso de carácter fuerte, y es diferente para cada miembro de la institución.
8. ¿El centro educativo tiene instalado un sistema de autenticación, tanto en los ordenadores como en la plataforma Web?	Desconozco si el centro tiene instalado un sistema de autenticación	El centro no cuenta con un sistema de autenticación ni en los dispositivos informáticos ni en la plataforma educativa.	El centro no cuenta con un sistema de autenticación pero sí utiliza sistemas de contraseñas para controlar la seguridad de acceso.	Sí, cuenta con un sistema de autenticación que garantiza la seguridad del acceso a la información pero sólo en los dispositivos informáticos.	Sí, cuenta con un sistema de autenticación que garantiza la seguridad del acceso a la información, tanto en los dispositivos informáticos, como en la plataforma servicios vía web.

Figura 7. Bloque I de Parte II.

Bloque III: Ciberacoso o cyberbulling					
9. ¿Comprende plenamente los riesgos e implicaciones que supone el ciberacoso para la comunidad educativa (estudiantes y/o profesores)?.	No sé cuáles son los riesgos del ciberacoso en general, tanto por parte de la víctima como del acosador.	Conozco, de manera superficial, los riesgos emocionales y psicológicos que causa el ciberacoso para aquellas víctimas que lo sufren y su acosador.	Conozco, de manera suficiente, los riesgos emocionales y psicológicos que causa el ciberacoso tanto por parte de la víctima como del acosador.	Conozco, de manera completa, los riesgos emocionales y psicológicos que causa el ciberacoso, tanto por parte de la víctima como del acosador.	Conozco, de manera profunda, los riesgos e implicaciones (emocionales, psicológicas y legales) del ciberacoso, tanto por parte de la víctima, como del acosador.
10.¿Cómo se han tratado los casos de ciberacoso en tu centro educativo?	No tengo constancia, ni he mostrado interés por si ha habido algún caso de ciberacoso en el centro educativo.	Tengo constancia de que no ha habido ningún caso en el centro educativo de ciberacoso.	Tengo constancia de que sí hay algún caso de ciberacoso pero no me he implicado para solucionarlo.	Tengo constancia de que ha habido algún caso de ciberacoso relacionado con miembros de la comunidad educativa del centro, y se han tomado medidas pero no se ha seguido ningún protocolo especial.	Tengo constancia de que sí ha habido casos de ciberacoso en el centro educativo, y se han tomado medidas (según protocolos de actuación de buenas prácticas) para solventarlo.
11. ¿Crees que es necesario que los docentes se impliquen en la detección y prevención del ciberacoso de los estudiantes de su centro educativo para protegerlos? En caso de que sí, ¿Hay un protocolo de actuación?	Considero que no es necesario que los docentes se impliquen en la detección y la prevención del ciberacoso de los estudiantes de ningún centro educativo.	Considero que sí es necesario que los docentes se impliquen en la detección y la prevención del ciberacoso de los estudiantes de su centro educativo, pero no existe un protocolo de actuación.	Considero que sí que es necesario que los docentes se impliquen en la detección y la prevención del ciberacoso de los estudiantes del centro educativo, pero tendrían que ser las familias las que se encargarán en mayor medida del problema.	Considero que es necesario que los docentes se impliquen en la detección y la prevención del ciberacoso de los estudiantes frente a estas amenazas, y que lo hagan junto a las familias.	Considero que sí que es necesario que los docentes se impliquen en la detección y la prevención del ciberacoso de los estudiantes, incluyendo a las familias y trabajando en el centro educativo con profesionales del ámbito siguiendo un protocolo de actuación.

Figura 8. Bloque III de Parte II.

Bloque IV: Actuación ante los incidentes					
12. Una vez que surgen un incidente relacionado con la ciberseguridad en el centro educativo tanto para hackear la Web como un caso de ciberacoso, ¿hay programas de apoyo para evitar que vuelvan a suceder estos incidentes y combatir sus consecuencias?	No tengo constancia de que haya habido ningún incidente de estos tipos en el centro educativo.	Aunque tenga constancia de que haya habido algún incidente de estos tipos, no tengo información sobre sí hay programas de apoyo o si se han tomado medidas preventivas.	Aunque tenga constancia de que haya habido algún incidente relacionado con estos tipos, no hay programas de apoyo ni se toman medidas preventivas.	Tengo constancia de que haya habido algún incidente de este tipo, y hay medidas preventivas pero no hay programas de apoyo, o hay programas de apoyo pero no se toman medidas preventivas.	Tengo constancia de que haya habido algún incidente de este tipo, y además, se cuenta con programas de apoyo y a la vez con la ayuda de medidas preventivas.
13. Cuando surgen incidentes relacionados con la ciberseguridad tanto en lo que se refiere a hackear la Web como un caso de ciberacoso en el centro educativo, ¿se investigan y se deja un registro de las incidencias?	No tengo constancia de que haya habido ningún incidente de estos tipos en el centro educativo.	Aunque tenga constancia de que haya habido algún incidente relacionado con la ciberseguridad, no tengo información sobre sí se deja ningún registro de los mismos o si se investigan.	Cuando surgen estos incidentes no se deja ningún registro de los mismos y tampoco se investigan.	Cuando surgen estos incidentes se deja un registro de los mismos, pero no se investigan, o se investigan pero no de deja ningún registro de los mismos.	Cuando surgen estos incidentes se deja registro de los mismos y se investigan.
14. Cuando surgen incidentes relacionados con la ciberseguridad, sobretodo sí se basa en un problema de ciberacoso en el centro educativo ¿se ha informado a las familias?	No tengo constancia de que haya habido ningún incidente de estos tipos en el centro educativo.	Aunque tenga constancia de que haya habido algún incidente relacionado con el ciberacoso, no tengo información sobre si hay información a las familias del centro educativo.	Cuando surgen estos incidentes no se informa a las familias de los estudiantes del centro educativo, a no ser que sea imprescindible para solicitar alguna autorización.	Cuando surgen estos incidentes no se informa a todas las familias de los estudiantes del centro educativo, sólo a aquellas familias de los estudiantes que estén implicados en el incidente.	Cuando surgen estos incidentes no se informa a todas las familias de los estudiantes del centro educativo, sólo a aquellas familias de los estudiantes que están implicados en el incidente, dejando además un registro firmado del mismo.

Figura 9. Bloque IV de Parte II.

Bloque V: Formación y concienciación en ciberseguridad					
15. ¿Has recibido formación sobre ciberseguridad?	No he recibido formación sobre la ciberseguridad.	He recibido algo de formación sobre la ciberseguridad en un charla dada en el centro educativo.	He recibido poca formación en ciberseguridad, durante cursos de duración mínima.	He recibido formación en ciberseguridad, ya que he acudido a numerosos cursos relacionados con el ámbito.	He recibido mucha formación en ciberseguridad, ya que he acudido a numerosos cursos sobre ello y el propio centro educativo nos da charlas informativas y de preparación cada poco.
16. ¿Crees que los centros educativos deberían tomar medidas para formar a los docentes sobre la ciberseguridad?. Por ejemplo, acudiendo a profesionales del sector de la ciberseguridad para la formación.	No creo que la ciberseguridad sea un aspecto a considerar en el ámbito educativo.	Considero que los centros educativos no deberían implicarse en la formación a los docentes sobre ciberseguridad.	Considero que los centros educativos sí deberían implicarse en la formación de los docentes en ciberseguridad, pero no de una manera activa ya que la responsabilidad principal en este ámbito debería recaer en las familias.	Considero que el centro debería formar a los docentes sobre la ciberseguridad, realizando talleres de prevención y concienciación para que se den a conocer los riesgos a los que pueden estar expuestos.	Considero que el centro educativo debería formar a los docentes sobre la ciberseguridad, realizando talleres de prevención y concienciación para que se den a conocer los riesgos a los que pueden estar expuestos. Además, debería impartirse más cursos de formación, charlas informativas y talleres de seguridad y privacidad, así como teniendo en cuanta las leyes de protección de datos para toda la comunidad educativa.
17. ¿Crees que los centros educativos deberían tomar medidas para concienciar a las familias sobre la importancia de la ciberseguridad?	No creo que la ciberseguridad sea un aspecto a considerar en el ámbito educativo.	Considero que los centros educativos no deberían implicarse en la concienciación a las familias sobre la importancia de la ciberseguridad.	Considero que los centros educativos sí deberían implicarse en la concienciación a las familias sobre la importancia de la ciberseguridad pero no de una manera activa ya que la responsabilidad principal en este ámbito debería ser de la propia familia.	Considero que el centro educativo debería implicarse en la concienciación a las familias sobre la importancia de la ciberseguridad, realizando talleres de prevención con profesionales que ayuden a que se den a conocer los riesgos a los que pueden estar expuestos los estudiantes.	Considero que el centro educativo debería implicarse en la concienciación a las familias sobre la importancia de la ciberseguridad, realizando talleres de prevención con profesionales que ayuden a que se den a conocer los riesgos a los que pueden estar expuestos los estudiantes. Además, deberían impartirse más cursos de formación, charlas informativas y talleres de seguridad y privacidad, teniendo en cuenta las leyes de protección de datos para toda la comunidad educativa.

Figura 10. Bloque V de Parte II (1)

18. ¿Crees que los centros educativos deberían tomar medidas para concienciar a los estudiantes sobre la importancia de la ciberseguridad?	No creo que la ciberseguridad sea un aspecto a considerar en el ámbito educativo.	Considero que los centros educativos no deberían implicarse en la concienciación al alumnado sobre la importancia de la ciberseguridad.	Considero que los centros educativos sí deberían implicarse en la concienciación del alumnado sobre la importancia de la ciberseguridad pero no de una manera activa ya que la responsabilidad principal en este ámbito debería ser de los padres o tutores.	Considero que el centro educativo debería implicarse en la concienciación del alumnado sobre la importancia de la ciberseguridad, realizando talleres de prevención con profesionales que ayuden a que se den a conocer los riesgos a los que pueden estas expuestos.	Considero que el centro educativo debería implicarse en la concienciación del alumnado sobre la importancia de la ciberseguridad, realizando talleres de prevención y concienciación para que se den a conocer los riesgos a los que pueden estar expuestos. Además, deberían impartirse cursos de formación, charlas informativas y talleres de seguridad y privacidad, teniendo en cuenta las leyes de protección de datos para toda la comunidad educativa.
19. ¿Crees que los docentes deberían tomar medidas para concienciar a sus estudiantes sobre la importancia de la ciberseguridad?	No creo que la ciberseguridad sea un aspecto a considerar en el ámbito educativo.	Creo que la concienciación en ciberseguridad en responsabilidad de las familias, o de otros sectores, y no del centro educativo.	Creo que el centro educativo ha de tomar medidas para la concienciación en ciberseguridad de los estudiantes, pero no ha de ser responsabilidad docente.	Creo que el docente ha de participar en la concienciación en ciberseguridad de los estudiantes, pero no ha de implicarse de manera activa ni dar formación.	Creo que el docente ha de participar de manera pro activa en la concienciación en ciberseguridad de los estudiantes.
20. ¿Crees que actualmente la formación en ciberseguridad debería ser obligatoria en el ámbito educativo?	No creo que la ciberseguridad sea un aspecto a considerar en el ámbito educativo.	Creo que la ciberseguridad puede ser un aspecto a considerar en la formación docente pero de manera transversal y solo para aquellos ciclos educativos con estudiantes de secundaria.	Creo que la ciberseguridad puede ser un aspecto a considerar en la formación docente pero de manera transversal.	Creo que la formación en ciberseguridad ha se der obligatoria actualmente en la carrera docente.	Creo que la formación docente en ciberseguridad actualmente es esencial para toda la comunidad educativa y, por lo tanto, debería ser una formación obligatoria en la carrera docente.

Figura *11.* Bloque V de Parte II (2)

21. ¿Saben dónde encontrar información sobre formación o sobre contenidos de ciberseguridad? ¿Conocen el programa de cibercooperantes?	No tengo constancia de donde poder encontrar este tipo de información y no conozco el programa de cibercooperantes.	Me han dado cierta información de sitios donde poder obtener formación en ciberseguridad pero no me he informado por completo. Además no conozco el programa de cibercooperantes.	Sí tengo constancia de dónde encontrar información sobre contenidos en ciberseguridad, pero solo empleo una seria de sitios Web que no son fiables por completo. No conozco el programa de cibercooperantes.	Sí tengo constancia de dónde encontrar información sobre contenidos en ciberseguridad, además utilizo el programa de cibercooperantes para tener un contenido más completo.	Sí tengo constancia de dónde encontrar información sobre contenidos en ciberseguridad utilizo el programa de cibercooperantes para tener un contenido más completo, y además lo trasmito a mis compañeros.

Figura *12.* Bloque V de Parte II (3)