https://doi.org/10.1344/REYD2024.30.44082

Educar y proteger: análisis de la educación en ciberseguridad para combatir la ciberdelincuencia

Educar i protegir: anàlisi de l'educació en ciberseguretat per a combatre la ciberdelinqüència

Educate and protect: analysis of cybersecurity education to combat cybercrime

Alberto Beltran Muñoz

Doctor en Criminología

Universidad de Granada, España

ORCID: https://orcid.org/0000-0001-7776-2204

Email: albertobeltran@correo.ugr.es

Resumen: La ciberdelincuencia es un problema en aumento que afecta a toda la ciudadanía. Actualmente, se están poniendo en marcha planes educativos para educar a la población y poder disminuir esas tasas de victimización. El objetivo de este estudio es analizar las relaciones entre los conocimientos en ciberseguridad y ciberamenazas, la vulnerabilidad y la victimización. Al mismo tiempo, también se ha estudiado la influencia de la educación y variables sociodemográficas sobre las anteriores variables. Para ello, se ha administrado un cuestionario a una muestra de 229 personas de distintos puntos del territorio español. Los resultados muestran que la educación mejora los conocimientos y consigue disminuir la vulnerabilidad y victimización ante la ciberdelincuencia. Además el sexo, la edad y la procedencia también tienen una relación directa con las variables. Este estudio demuestra la importancia de los programas educativos en ciberseguridad y su influencia para poder mejorar la protección de la ciudadanía.

Palabras clave: ciberseguridad, ciberdelito, vulnerabilidad, victimización, educación.

Resum: La ciberdelinqüència és un problema en augment que afecta a tota la ciutadania. Actualment, s'estan posant en marxa plans educatius per a educar a la població i poder disminuir aquestes taxes de victimització. L'objectiu d'aquest estudi és analitzar les relacions entre els coneixements en ciberseguretat i ciberamenazas, la vulnerabilitat i la victimització. Al mateix temps, també s'ha estudiat la influència de l'educació i variables sociodemogràfiques sobre les anteriors variables. Per a això, s'ha administrat un qüestionari a una mostra de 229 persones de diferents punts del territori espanyol. Els resultats mostren que l'educació millora els coneixements i aconsegueix disminuir la vulnerabilitat i victimització davant la ciberdelinqüència. A més el sexe, l'edat i la procedència també tenen una relació directa amb les variables. Aquest estudi demostra la importància dels programes educatius en ciberseguretat i la seva influència per a poder millorar la protecció de la ciutadania.

Paraules clau: ciberseguretat, ciberdelicte, vulnerabilitat, victimització, educació.

Abstract: Cybercrime is a growing problem that affects all citizens. Currently, educational plans are being implemented to educate the population in order to decrease these victimization rates. The aim of this study is to analyze the relationships between knowledge of cybersecurity and cyberthreats, vulnerability and victimization. At the same time, the influence of education and sociodemographic variables on the above variables has also been studied. To this end, a questionnaire was administered to a sample of 229 people from different parts of Spain. The results show that education improves knowledge and reduces vulnerability and victimization to cybercrime. In addition, gender, age and origin also have a direct relationship with the variables. This study demonstrates the importance of educational programs in cybersecurity and their influence in improving citizen protection.

Keywords: cybersecurity, cybercrime, vulnerability, victimization, education.

1. INTRODUCCIÓN

La ciberdelincuencia y la vulnerabilidad en el ciberespacio son problemas que van en aumento en nuestra sociedad, afectan a un gran número de personas y tiene un gran impacto en la ciudadanía. Según el Departamento de Seguridad Nacional (DSN, 2019) la vulnerabilidad en el ciberespacio llega a ser calificada como uno de los principales riesgos para nuestro desarrollo como nación. Supone un gran riesgo para la seguridad de nuestros datos personales, de las actividades comerciales y un perjuicio económico para quienes lo sufren. Además, en el Estudio sobre percepción y nivel de confianza en España (ONTSI, 2024), se encontró que en el último semestre de 2022, el 57,8% de las personas afirma haber sufrido un incidente de seguridad. En cuanto al fraude en la red, el porcentaje de quienes lo han sufrido es del 67,5%, y hasta el 90% sienten que necesitan formación en ciberseguridad. También va en aumento el "phishing", que consiste en usar el engaño para manipular a las víctimas y conseguir infectarles el dispositivo o robar información.

Existe un reconocimiento en la literatura de que los factores de comportamiento humano son la clave para combatir el ciberdelito (Oluwaseun et al., 2024; Hadlington & Chivers, 2018). Aunque la tecnología de la información es usada masivamente por toda la sociedad a nivel mundial, es necesario enseñar los temas de seguridad de la información para evitar que se conviertan en víctimas de la ciberdelincuencia (Muniesa et al., 2023). Los resultados encontrados por Fernández-Montalvo et al. (2015) también suponen una señal de alarma e indican la necesidad de establecer programas preventivos para el uso seguro de Internet. Se trata de conseguir que el uso de Internet encuentre un espacio natural en las actividades del sujeto, evitando los riesgos y peligros derivados de una utilización indiscriminada y sin criterios específicos. La baja capacidad para conseguir encontrar y enjuiciar a los ciberdelincuentes, hace necesario mejorar la protección de las potenciales víctimas.

Los hábitos de ciberseguridad, también denominado ciberhigiene, suele desempeñar un papel importante en victimización. Algunos ejemplos de estos hábitos son emplear cortafuegos y aplicaciones antivirus. Los individuos con buena ciberhigiene siguen las mejores prácticas de seguridad y protegen su información personal (Cain et al., 2018). En su investigación, estudiaron los conocimientos de ciberseguridad, sobre las ciberamenazas y sus comportamientos

relacionados con la ciberhigiene. Además, incluyeron variables como formación y experiencia previas, el impacto de la edad, el sexo y la victimización. En sus resultados, destacan la importancia de la educación y los conocimientos y de tener en cuenta las variables demográficas implicadas. Dentro de los conocimientos, existen algunos básicos como: detectar el phishing, recursos a los que acudir en caso de ser víctimas, las ciberamenazas existentes, las ciberestafas más habituales o la creación de contraseñas seguras.

En el estudio de Zwilling et al. (2020), analizaron las relaciones entre la concienciación, los conocimientos y el comportamiento en materia de ciberseguridad con las herramientas de protección. Encontraron que los internautas poseen una concienciación adecuada sobre las ciberamenazas, pero sólo aplican medidas de protección mínimas, por lo general relativamente comunes y sencillas. Los resultados del estudio también muestran que un mayor conocimiento cibernético está relacionado con el nivel de ciberconciencia. Además, la concienciación también está relacionada con las herramientas de protección. Así pues, los encuestados con más conocimientos de ciberseguridad toman más medidas para prevenir los ataques, especialmente cuando las herramientas de defensa son sencillas. También descubrieron que el conocimiento de la ciberseguridad y el uso de Internet estaban relacionados con las actividades de protección a través de la mediación de la concienciación sobre la ciberseguridad. Estos resultados ponen de relieve el importante papel de la educación de ciberseguridad para motivar a los usuarios a adoptar conductas proactivas.

En Drew (2020), se ha estudiado la educación para la prevención de la delincuencia centrada en aumentar los conocimientos y su eficacia en reducir la victimización. Encontraron la necesidad de incluir elementos clave que puedan tener un impacto significativo y real en el uso de la autoprotección. Estos tienen un impacto significativo y real en el uso de comportamientos y estrategias de autoprotección. Educar a los individuos resulta ser un método útil para fomentar la autoprotección y un mayor uso de los métodos de prevención, reduciendo así la probabilidad de victimización. Por lo tanto, existe una relación entre educación, conocimientos y vulnerabilidad que es de interés estudiar para poder prevenir la ciberdelincuencia.

Existen evidencias de diferencias entre los distintos colectivos de la sociedad en su capacidad para defenderse. Un ejemplo claro es la edad, factor generador de la denominada “brecha

digital", en este caso, de forma intergeneracional. Se ha encontrado que las personas mayores presentan menores conocimientos y capacidades para defenderse en el ámbito digital frente a las más jóvenes (Ramadhani et al., 2020). En Gudiño (2018) hablan de la desprotección de los mayores ante los riesgos a los que se ven expuestos en uso diario de las nuevas tecnología. Entre los factores de vulnerabilidad encontraron: el aislamiento social, los problemas de salud cognitivos, físicos y mentales; el nivel de riqueza, las habilidades o conocimientos limitados en ciberseguridad. En cuanto a la prevención, la intervención directa con las personas mayores reduce los riesgos de ciberdelincuencia, la mejora de la concienciación y las habilidades (Burton et al, 2022). Se han desarrollado programas exitosos donde se aprenden las técnicas de seguridad y las medidas de protección desde un nivel inicial, explicando a personas de la tercera edad sobre estafas mediante phishing por correo electrónico (Cook et al., 2011) y redes sociales (Alwanain et al., 2020).

Dentro de los distintos colectivos, también encontramos a los nativos digitales, que son aquellos que han crecido con las nuevas tecnologías. Aunque la usan a diario, algunos estudios sobre población escolar, encontraron que casi el 30% del alumnado no había recibido ningún tipo de formación o información previa a la actuación formativa de ciberseguridad (Gamito et al., 2020). A pesar de ello, la formación general en el ámbito digital y la agilidad en el uso de TICs debería ser un factor positivo en relación a los conocimientos y una menor vulnerabilidad. También se han encontrado diferencias según el sexo, siendo los hombres los que obtienen mejores resultados en conocimientos y menor vulnerabilidad (Cain et al., 2018). En cuanto a la procedencia, no hay estudios que investiguen la incidencia sobre la población migrante en España y su capacitación para defenderse. La población migrante, solicitante de asilo, refugiada y apátrida, en muchos casos, proviene de países donde no hay alfabetización digital, por lo tanto, también sería una población de mayor riesgo en el ciberespacio.

En este estudio, se busca dar respuesta a si la educación en ciberseguridad y los conocimientos reducen la vulnerabilidad, victimización y factores sociodemográficos. Concretamente, nos planteamos la siguiente pregunta de investigación ¿Puede la educación en ciberseguridad y los conocimientos sobre este tema reducir la vulnerabilidad y la victimización? Para ello, se han planteado un total de 4 objetivos de investigación:

- Objetivo 1: Comprobar los niveles de vulnerabilidad, victimización, educación, sensación de seguridad y conocimientos en ciberseguridad/ciberdelincuencia.

- Objetivo 2: Averiguar la relación existente entre el nivel de conocimientos, vulnerabilidad, victimización y educación.

- Objetivo 3: Estudiar la influencia de las variables sociodemográficas (sexo, edad y procedencia) en los conocimientos, vulnerabilidad y victimización.

- Objetivo 4: Estudiar la influencia que tiene la educación en ciberseguridad en los conocimientos, vulnerabilidad y victimización.

2. METODOLOGÍA

La metodología implementada ha sido el estudio observacional por método de encuesta. Se ha empleado un cuestionario dividido en 4 secciones. La primera sección incluyen las variables sociodemográficas (4 preguntas); la segunda preguntas para evaluar los conocimientos (8 preguntas); la tercera contiene preguntas para evaluar la vulnerabilidad (10 preguntas); la última sección contiene preguntas referidas a la educación, la victimización y la autopercepción de seguridad (4). Para la validez del cuestionario se ha hecho una consulta a jueces expertos e incluido conceptos clave del ámbito. Posteriormente, se administró a una muestra piloto para obtener un primer feedback. Para el análisis de fiabilidad se han realizado pruebas de Alfa de Cronbach, obteniendo una puntuación de 0,725. Este indicador muestra la consistencia interna de la herramienta empleada. Teniendo en cuenta que el mínimo aceptable para la fiabilidad es de 0,7, encontramos que el instrumento es apto para la evaluación de interés.

La plataforma empleada para el cuestionario es GoogleForms, que permite un diseño fácil con múltiples opciones, recibir las respuestas automaticamente y enviar por distintas vías el enlace de acceso. Se ha tratado de una muestra incidental mediante el envío masivo por distintos medios y tomando datos de residencia para controlar la variable territorial. La muestra obtenida es de un total de N=229. En la Tabla 2.1 se muestran los porcentajes según sexo (48,9% hombres y

48,5% mujeres) y de edad, divididos en tres rangos según sean nativos digitales (48%) y no nativos digitales (51.9%). Este último grupo, se ha subdividido entre población adulta (43,2%) y tercera edad (8,7%). Finalmente, en la variable "colectivo por procedencia", se muestra el porcentaje de personas nacionales (81,7%) y extranjeras (migrantes, solicitantes de asilo, refugiados y apátridas) con un 18,3%.

TABLA 2.1 Datos sociodemográficos

Sexo

	N	%
Hombres	112	48,9%
Mujeres	111	48,5%
Sin especificar	6	2,6%

Edad

	N	%
Menores de 35	110	48,0%
Entre 35 y 65	99	43,2%
Mayores de 65	20	8,7%

Colectivo por procedencia

	N	%
Nacionales	187	81,7%
Extranjeros	42	18,3%

En cuanto a las variables planteadas, son las siguientes:

VI Sexo: Variable Nominal- Dicotómica. Hombres; Mujeres.

VI Edad: Variable nominal

- Colectivo 1 Nativos digitales (Menores de 35)
- Colectivo 2 No-Nativos digitales (Mayores de 35 y menores de 65)
- Colectivo 3 No-Nativos digitales (Mayores de 65)

VI Procedencia Variable Nominal

- Colectivo 1 Nacionales.
- Colectivo 2 Población extranjera: migrantes, solicitantes de asilo, refugiados y apátridas.

VI Educación en ciberseguridad/ciberdelincuencia: Si ha recibido formación/cursos en ciberseguridad y/o ciberamenazas. Variable Ordinal.

VI Nivel de conocimientos: conocimiento sobre las amenazas y formas de ciberdelincuencia, así como las medidas de ciberseguridad necesarias para protegerse. Variable Cuantitativa Discreta.

VD Vulnerabilidad: Se entiende por vulnerable cuando el individuo no pone en marcha medidas de protección. No basta solo con tener conocimiento (el cómo defenderse), sino también emprender acciones para evitar ser víctima. Por lo tanto, la vulnerabilidad tiene un componente de concienciación y esfuerzo sumado a la educación. La puntuación 0 corresponde con una alta vulnerabilidad y 10 una escasa vulnerabilidad. Variable Dicotómica

VD Victimización: Si en algún momento ha sufrido algún tipo de ciberdelito y una o varias veces. La idea de víctima de ciberdelito es amplia, y puede incluir, por ejemplo, el sufrir malware en cualquier dispositivo, una ciberestafa o el robo de información. Ordinal

VD Autopercepción de seguridad: Si el individuo se considera seguro para afrontar posibles ciberdelitos. Ordinal

3. RESULTADOS

3.1 Niveles de vulnerabilidad, victimización, educación, sensación de seguridad y conocimientos en ciberseguridad/ciberdelincuencia.

En la Tabla 3.1 se muestran los datos descriptivos. Se debe tener en cuenta que la vulnerabilidad se ha tratado de forma invertida, siendo la puntuación 0 la correspondiente a una persona vulnerable y 10 una persona con alta capacidad para defenderse. Se puede observar que la media en conocimientos apenas alcanza el 4,89, siendo la puntuación máxima de 16 y una desviación del 3.66. Solo el 12,3% supera la puntuación de 10, estando la mayor parte de los individuos por debajo de ese valor. En vulnerabilidad la media es 5.51, siendo la puntuación máxima 10, por lo tanto, se encuentra en unos valores medios de protección. La mayor parte de los individuos se encuentran entre 3 puntos y 8 puntos en vulnerabilidad (84,3%). En cuanto a la desviación, presenta un valor de 2.11.

Analizando los datos de victimización, el 60.7% afirman no haber sido nunca víctima de ningún tipo de ciberdelito, mientras que el resto afirma haber sido víctima al menos en una ocasión. De los que afirman haber sido víctimas, la mayor parte lo fueron en una sola ocasión con un 31% del total. Por otra parte, analizando los datos en educación, el 60,7% de las personas consultadas afirman no haber recibido nunca ningún tipo de formación, frente al 39,3% que sí la ha recibido. En cuanto a la sensación de inseguridad, es mayoritaria, encontrando que el 57% de las personas se sienten poco o muy poco seguras, frente al 24,5% que sí se sienten seguras. También existe un porcentaje muy bajo que afirman sentirse muy seguras, tan solo el 4,4%. El restante de los consultados (18,5%) no sabrían decirlo. La puntuación media es de 1,66 sobre 4.

TABLA 3.1 Estadísticos Descriptivos

Estadísticos Descriptivos

		Conocimientos de ciberseguridad básica	Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Víctima de ciberdelito	Educación en ciberseguridad	Sensación de seguridad
N	Válido	229	229	229	229	229
Media		4,89	5,51	1,49	1,66	1,66
Desviación		3,669	2,112	,698	,927	1,119
Mínimo		0	0	1	1	0
Máximo		15	10	4	4	4

Nivel de conocimientos de ciberseguridad básica

	N	%
0	21	9,2%
1	18	7,9%
2	28	12,2%
3	32	14,0%
4	26	11,4%
5	22	9,6%
6	15	6,6%
7	17	7,4%
8	10	4,4%
9	12	5,2%
10	7	3,1%

Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)

	N	%
0	1	0,4%
1	8	3,5%
2	14	6,1%
3	20	8,7%
4	24	10,5%
5	41	17,9%
6	37	16,2%
7	47	20,5%
8	24	10,5%
9	8	3,5%

Víctima de ciberdelito

	N	%
Nunca	139	60,7%
1 vez	71	31,0%
2 o 3 veces	15	6,6%
Más de 3 veces	4	1,7%

Educación en ciberseguridad

	N	%
No	139	60,7%
Poca formación	42	18,3%
Algo de formación	36	15,7%
Mucha formación	12	5,2%

Sensación de seguridad

	N	%

11	7	3,1%
12	2	0,9%
13	5	2,2%
14	3	1,3%
15	4	1,7%

10	5	2,2%

No sabe	41	17,9%
Muy poco seguro	63	27,5%
Poco seguro	69	30,1%
Algo seguro	46	20,1%
Muy seguro	10	4,4%

De las cuestiones relacionados con conocimientos (Tabla 3.2), la mayor parte de la ciudadanía (80,7%) afirma no conocer instituciones específicas en caso de ser víctimas de ciberdelitos. Tras ser preguntadas específicamente por el INCIBE, el OSI y el IS4K, el 72,1% de las personas consultadas no conocen ninguna de ellas. De las que conocen, encabezan la lista el Incibe (23,6%), seguido por el OSI (8,7%) y el IS4K (3,1%).La mayor parte afirman conocer el Phishing (76,5%), pero cuando se hace una pregunta de evaluación sobre en qué consiste este ciberdelito, tan solo el 44,8% acierta. El porcentaje es aún menor cuando se pregunta sobre cómo detectarlo (37,1%). En cuanto a la estafa relacionada con el Bizum, el 37,1% caería en la estafa, mientras que el 62,9% sería capaz de evitarla.

En las cuestiones relacionadas con vulnerabilidad, tan solo el 27,9% afirma de disponer antivirus en el móvil, frente al 72,1% que carecen de él. En cuanto al uso de las VPN (Virtual Private Network), el porcentaje es similar, 69% no dispone de él. Más de la mitad de las personas (55,9%) afirman hacer copias de seguridad periódicas de su información. Sobre las contraseñas, el 79% es capaz de reconocer una contraseña segura (8 caracteres, con números, letras, mayúsculas, minúsculas y símbolos), sin embargo, el 31,9% afirma no usarlas. Además, el 80,3% de los encuestados afirma repetir contraseñas en distintos sitios. Por último, el 45,4% se conectan a conexiones wifi que no requieran contraseñas.

TABLA 3.2 Principales resultados de cuestionario

Cuestiones destacadas	Resultados
En caso de sufrir un ciberataque o sufrir un ciberdelito ¿sabrías con qué institución específica (además de la policía) ponerte en contacto?	19,3% si 80,7% no
Ante la pregunta de ¿Qué tipos de ciberdelitos que conoces?	76,5% Phishing
¿Qué es el phishing?	44,8% acierta
¿Cómo detectar el phishing?	37,1% acierta
¿Cuál de estas instituciones públicas de ciberseguridad conoces?	72,1% no conoce ninguna 23,6% Incibe 8,7% OSI 3,1% IS4K

Te envían una solicitud de Bizum ¿recibes o te cobran el cargo?	62,9% acierta 37,1% caería en la estafa
¿Tienes antivirus en el móvil?	27,9% sí tiene 72,1% no tiene
¿Haces copias de seguridad de forma periódica?	55,9% sí
¿Usas VPN (virtual private network) en el ordenador?	69% no usa
¿Cual de las siguientes contraseñas es más segura?	79% acierta
Usas contraseñas seguras: 8 caracteres, con números, letras, mayúsculas, minúsculas y símbolos.	31,9% no las usa
¿Repites contraseñas en distintos sitios?	80,3% las repite
¿Alguna vez te conectas a wifi pública que no requiere contraseña?	45,4% se conectan

3.2 Relación existente entre el nivel de conocimientos, vulnerabilidad, victimización y educación.

Una vez realizado el análisis estadístico (Spearman) para las variables conocimientos, vulnerabilidad, victimización y educación, se encontró una alta correlación entre dichas variables (Tabla 3.3). La variable conocimientos obtiene un coeficiente de correlación significativo de 0,438 con la variable vulnerabilidad (Sig. <0,001); con la variable victimización obtiene una relación significativa negativa de -0,172 (Sig. 0,009); con la variable educación tiene la correlación más fuerte de las tres, con 0,537 de coeficiente (Sig. <0,001). La vulnerabilidad tiene una correlación significativa con la variable educación del 0,330 (Sig. <0,001), sin embargo, su relación con la victimización no es significativa (Sig. 0,127). La victimización tiene una relación negativa y significativa con la variable educación, obteniendo un coeficiente de -0,177 (Sig. 0,007).

TABLA 3.3 Correlaciones entre conocimientos, vulnerabilidad, victimización y educación en ciberseguridad

Correlaciones

			Conocimientos de ciberseguridad básica	Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Víctima de ciberdelito	Educación
Rho de Spearman	Nivel de conocimientos de ciberseguridad básica	Coeficiente de correlación		,438**	-,172**	,537**
		Sig. (bilateral)		<,001	,009	<,001
	Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Coeficiente de correlación	,438**		-,101	,330**
		Sig. (bilateral)	<,001		,127	<,001
	Víctima de ciberdelito	Coeficiente de correlación	-,172**	-,101		-,177**
		Sig. (bilateral)	,009	,127		,007
	Educación en ciberseguridad	Coeficiente de correlación	,537**	,330**	-,177**	
		Sig. (bilateral)	<,001	<,001	,007	.

**. La correlación es significativa en el nivel 0,01 (bilateral).

3.3 Influencia de las variables sociodemográficas sobre los conocimientos, vulnerabilidad y victimización.

Se han obtenido los siguientes resultados en relación a la variable sexo (Tabla 3.4) . En primer lugar, existen diferencias significativas entre los conocimientos según el sexo, con una t de 4,904 (Sig. <0,001). La media de conocimientos en hombres es mayor que el de las mujeres. Los hombres obtienen una media de 5,97 frente al 3,69 de las mujeres. El resto de variables, vulnerabilidad y victimización, no obtienen diferencias significativas (Sig. 0,255 y 0,384 respectivamente). Por lo tanto, los datos muestran que no existe una influencia de la variable sexo sobre vulnerabilidad y victimización, pero sí sobre los conocimientos en ciberseguridad básica.

TABLA 3.4 Estadísticos variable Sexo

	Sexo	N	Media	Desviación estándar
Nivel de conocimientos de ciberseguridad básica	Hombres	112	5,97	3,976
	Mujeres	111	3,69	2,872
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Hombres	112	5,53	2,009
	Mujeres	111	5,45	2,206
Víctima de ciberdelito	Hombres	112	1,46	,684
	Mujeres	111	1,53	,724

Prueba t de muestras independientes

	Prueba de Levene de igualdad de varianzas		Prueba t para la igualdad de medias				
					Significación		
	F	Sig.	t	gl	P de un factor	P de dos factores	Diferencia de medias
Conocimientos de ciberseguridad básica	12,422	<,001	4,904	221	<,001	<,001	2,280
Nivel de vulnerabilidad	1,303	,255	,270	221	,394	,787	,076
Víctima de ciberdelito	,761	,384	-,713	221	,238	,476	-,067

La tabla 3.5 muestra los resultados en relación a la procedencia de los participantes y la prueba t de muestras independientes. Se han dividido en nacionales y extranjeros. En la variable conocimientos, se han hallado diferencias significativas entre los grupos, con una t de 3,341 y una significación de <0,001. Los nacionales obtienen mejores resultados que los extranjeros, con una puntuación media de 5,26 de los nacionales frente al 3,21 de los extranjeros. También se han encontrado diferencias significativas en la variable vulnerabilidad, con una t de 4,871 y una significación de <0,001. Al igual que en el anterior caso, los nacionales obtienen una mejor puntuación de vulnerabilidad. Los nacionales tienen una media de 5,82 frente al 4,14 de los extranjeros. Finalmente, la procedencia resultó no ser significativa en la victimización.

TABLA 3.5 Estadísticos variable Procedencia

	Procedencia	N	Media	Desviación estándar
Nivel de conocimientos de ciberseguridad básica	Nacionales	187	5,26	3,685
	Extranjeros	42	3,21	3,120
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Nacionales	187	5,82	1,860
	Extranjeros	42	4,14	2,600
Víctima de ciberdelito	Nacionales	187	1,50	,721
	Extranjeros	42	1,45	,593

Prueba t de muestras independientes

	Prueba de Levene de igualdad de varianzas		prueba t para la igualdad de medias				
					Significación		
	F	Sig.	t	gl	P de un factor	P de dos factores	Diferencia de medias
Conocimientos de ciberseguridad básica	5,281	,022	3,341	227	<,001	<,001	2,048
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	13,735	<,001	4,871	227	<,001	<,001	1,675
Víctima de ciberdelito	1,497	,222	,421	227	,337	,674	,050

La tabla 3.6 muestra los resultados de la variable edad y del análisis Anova. En la variable conocimientos se ha encontrado diferencias significativas entre los 3 grupos en los que se ha dividido la muestra según su edad. Se ha obtenido una puntuación F de 16,268 y una significación de <0,001. El grupo que ha obtenido mejores resultados es el de menores de 35, con una puntuación media de 5,97, el siguiente es el del rango 35-65, que obtiene una media de 4,36. Por último, los mayores de 65, tienen una media de 1,5. También la variable vulnerabilidad muestra resultados significativos. Tiene un F de 13,306 y una significación de <0,001. La media de los menores de 35 y del rango de 35-65 muestran medias muy similares con 5,74 y 5,71 respectivamente. El grupo mayor de 65 tiene una media de 3,30, la menor de los 3 grupos. Finalmente, la variable victimización no tiene resultados significativos en relación a la edad. Obtiene una F de 3.93 y una significación de 0,021.

TABLA 3.6 Estadísticos variable Edad

		N	Media
Nivel de conocimientos de ciberseguridad básica	Menores de 35	110	5,97
	Entre 35 y 65	99	4,36
	Mayores de 65	20	1,50
	Total	229	4,89
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Menores de 35	110	5,74
	Entre 35 y 65	99	5,71
	Mayores de 65	20	3,30
	Total	229	5,51
Víctima de ciberdelito	Menores de 35	110	1,36
	Entre 35 y 65	99	1,60
	Mayores de 65	20	1,70
	Total	229	1,49

ANOVA

		gl	F	Sig.
Nivel de conocimientos de ciberseguridad básica	Entre grupos	2	16,268	<,001
	Total	228		
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Entre grupos	2	13,306	<,001
	Total	228		
Víctima de ciberdelito	Entre grupos	2	3,939	,021
	Total	228		

3.4 Influencia de la educación en ciberseguridad sobre los conocimientos, vulnerabilidad y victimización.

En relación a la tabla 3.7, se muestra el efecto de la educación en ciberseguridad sobre las variables objeto de estudio. En la variable conocimientos, se encontró una F 34,765 y una significación de <0,001. Las personas que recibieron educación en ciberseguridad tienen una media de conocimientos mayor que aquellas que no. La media de las que no recibieron educación es de 3,28 frente a las que recibieron mucha 8,75. Las que recibieron algo tienen 7,86 y las que tuvieron poca 6.55. En cuanto al nivel de vulnerabilidad, también resultó ser significativa con una F de 10,833 y una significación de <0,001. Las personas que no recibieron educación tienen una media de vulnerabilidad de 4,91. De las que sí recibieron, obtienen medias

muy similares de vulnerabilidad en los distintos niveles de educación (Poca=6,38; Algo=6.36; Mucha=6,83). En relación a la variable victimización, se encontró que existen diferencias débiles (F de 3,516) pero significativas (Sig. 0,016). Los individuos que no han recibido nunca educación en ciberseguridad tienen una media mayor en victimización que el resto (1,58). Aquellas que tienen mucha formación obtienen una media de 1,08, las que han recibido algo 1,53 y las que tuvieron poca 1,29.

TABLA 3.7 Estadísticos variable educación

		N	Media	Desviación estándar
Nivel de conocimientos de ciberseguridad básica	No	139	3,28	2,551
	Poca formación	42	6,55	3,270
	Algo de formación	36	7,86	3,796
	Mucha formación	12	8,75	4,827
	Total	229	4,89	3,669
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	No	139	4,91	2,198
	Poca formación	42	6,38	1,413
	Algo de formación	36	6,36	1,775
	Mucha formación	12	6,83	1,642
	Total	229	5,51	2,112
Víctima de ciberdelito	No	139	1,58	,711
	Poca formación	42	1,29	,596
	Algo de formación	36	1,53	,774
	Mucha formación	12	1,08	,289
	Total	229	1,49	,698

ANOVA

		gl	Media cuadrática	F	Sig.
Nivel de conocimientos de ciberseguridad básica	Entre grupos	3	324,010	34,765	<,001
	Total	228			
Nivel de vulnerabilidad (0=vulnerable ; 10 = no vulnerable)	Entre grupos	3	42,794	10,833	<,001
	Total	228			
Víctima de ciberdelito	Entre grupos	3	1,660	3,516	,016
	Total	228			

4. DISCUSIÓN Y CONCLUSIONES

Tras analizar los resultados obtenidos, se ha encontrado un nivel bajo de conocimientos en la población consultada. Dichos conocimientos aportan una capacitación que permite a los individuos defenderse, sin embargo, esa carencia encontrada les deja en una situación de mayor vulnerabilidad. Además, los niveles de educación son bajos, ya que el 60% nunca la recibió ningún tipo de formación. El 39,3% que sí la recibió también es bajo si lo comparamos con el 81% de Cain et al., (2018), pero más aproximado al 30% de Gamito et al., (2020). El porcentaje de victimización es elevado (60,7%) en comparación a otros estudios, 24% - 30% (Díaz, 2023; Emm, 2023). Un ejemplo sería la victimización por Phishing, que en otros estudios alcanza el 25% (Emm, 2023). En cuanto a la sensación de seguridad, apenas el 24,5% afirma sentirse segura. Este sentimiento generalizado puede deberse a que, al plantearse las cuestiones sobre ciberamenazas, los individuos han sido más conscientes del desconocimiento que tienen sobre el tema.

Son preocupantes algunos resultados de hábitos en ciberseguridad, por ejemplo, el escaso uso de antivirus en el teléfono móvil (72,1% no tiene). Contrasta con el uso de antivirus en el ordenador, ya que en Cain et al. (2018) encontraron que entre el 47% y el 78% disponen de él y lo actualizan con regularidad. También destaca el desconocimiento de instituciones como el Incibe, la OSI y el IS4K. Estas instituciones son las encargadas de brindar información, materiales didácticos y educación a la población general, sin embargo, no están consiguiendo llegar a la ciudadanía. Cabría cuestionarse si las campañas implementadas por estas instituciones son efectivas cuando la mayor parte de la población afirma no conocerlas. Por último, el 37,1% de la población consultada caería en la estafa del Bizum, lo que indica que desconocen aspectos básicos de esta plataforma de pagos y que puede llevarles a ser víctimas de este tipo de delitos.

Para el segundo objetivo de estudio, se confirmó que existe relación directa entre conocimientos y vulnerabilidad. Aquellos individuos con un mayor de nivel de vulnerabilidad presentan menores conocimientos. Lo mismo sucede al contrario, aquellas personas con más conocimientos tienen una menor vulnerabilidad. Estos datos señalan la importancia de mejorar los conocimientos en ciberseguridad para disminuir la vulnerabilidad ante las ciberamenazas Sobre la cuestión de si existe una relación inversa entre conocimiento y victimización por

ciberdelito, también se han encontrado diferencias significativas. Cuanto mayor es el conocimiento que presentan los individuos, menor es la tasa de victimización, reforzando así la importancia de los conocimientos para evitar ser víctima de la ciberdelincuencia.

También se han encontrado diferencias significativas entre conocimientos y educación, hallando que a mayor nivel de educación, mejores conocimientos. Por el contrario, aquellos individuos que no han recibido educación en ciberseguridad, presentan las menores tasas de conocimientos. En el análisis de correlaciones entre vulnerabilidad y educación, también se han obtenido resultados significativos, encontrando que a una mayor educación, existe una menor vulnerabilidad. Los resultados coinciden con Zwilling et al. (2020) y Drew (2020) sobre la mejora de la protección mediante la educación y los conocimientos en ciberseguridad. Las importancia de estos resultados reside en el peso que tiene la educación como forma de prevención de la ciberdelincuencia en la población general.

Finalmente, se encontró una relación significativa entre victimización y educación. A un mayor nivel de educación, se reduce la victimización y viceversa. Sorprendentemente, los niveles de victimización no se correlacionan con los de vulnerabilidad. En estudios anteriores, se examinó si el hecho de haber sido víctima en el pasado afectaba a la ciberhigiene (Cain et al., 2018). Presumiblemente, después de haber sido atacados, los usuarios se comportarían de forma más segura en el futuro y sabrían cómo evitar los ataques (menos vulnerables), pero esta postura no recibió apoyo empírico. El hecho de que un usuario haya sufrido ataques en el pasado no influían en su vulnerabilidad actual. Por lo tanto, esos resultados estarían en la misma línea que los obtenidos en este estudio, ausencia de relación significativa entre vulnerabilidad y victimización.

En relación al objetivo 3, se analizó la influencia de las variables sociodemográficas (sexo, edad y procedencia) con las variables objeto de estudio: vulnerabilidad, conocimientos y victimización. Los resultados hallados apuntan a que existen diferencias significativas en la variable sexo, encontrando mayores conocimientos en hombres que en mujeres. En relación a la procedencia, estas diferencias consisten en que las personas nacionales tienen mejores resultados que las extranjeras. Las extranjeras obtienen peores tasas de conocimientos y son más vulnerables, por lo que demuestra una situación de desventaja frente a los nacionales. Por su

parte, en la variable edad, los nativos digitales muestran mejores resultados de educación, conocimientos y vulnerabilidad que los no-nativos digitales. Este hecho se explica en que los jóvenes son los que más saben de tecnología y están más preparados. Los resultados encontrados contrastan con el estudio de Cain et al., (2018), en el que los usuarios de más edad tendían a comportarse de forma más segura que los más jóvenes.

Para responder al cuarto objetivo de investigación encontramos que existe una influencia positiva de la educación sobre los conocimientos, e inversa sobre la vulnerabilidad y la victimización. Las que recibieron educación en ciberseguridad tienen más conocimientos que las que no la recibieron, son menos vulnerables y tienen menores tasas de victimización. Sobre el tipo de educación, también es llamativo que apenas el 17% incluía formación sobre ciberseguridad y ciberamenazas. El resto de individuos recibieron educación sobre alguno de los 2 aspectos en solitario. Como limitaciones, señalar que las cuestiones relacionadas con la educación, la victimización y la sensación de seguridad se hicieron de forma genérica sin especificar formas concretas. De cara a futuras investigaciones, sería interesante profundizar en las diferencias según tipos de victimización, analizar mejor los niveles de educación y consultar de una forma más extensa sobre la sensación de seguridad.

Como conclusiones, se puede afirmar que se confirmó así la hipótesis de que recibir educación mejora los conocimientos y reduce la vulnerabilidad y la victimización. Actualmente, se defiende la idea de que la mayor parte de la población debe tener estos conocimientos mínimos en ciberseguridad, sin embargo, los resultados demuestran que una parte importante de individuos consultados carecen de ellos. También se muestra fundamental la atención a las personas mayores de 65 y las personas extranjeras, que son la población más vulnerable ante las ciberamenazas. Además, otra consecuencia de no recibir educación en ciberseguridad es que puede generar una sensación de inseguridad, tal y como se ha detectado. Por lo tanto, para reducir la victimización, la vulnerabilidad y la sensación de inseguridad, se deben aumentar los esfuerzos de las instituciones en fomentar y mejorar la educación en ciberseguridad, concienciar sobre las ciberamenazas y prestar una mayor atención a los colectivos menos protegidos.

BIBLIOGRAFÍA

Alwanain, M., I. (2020). Phishing Awareness and Elderly Users in Social Media. *International Journal of Computer Science and Network Security*, *20*(9), 114-119. https://doi.org/10.22937/IJCSNS.2020.20.09.14

Burton, A., Cooper, C., Dar, A., Mathews, L., & Tripathi, K. (2022). Exploring how, why and in what contexts older adults are at risk of financial cybercrime victimisation: a realist review. Exp. Gerontol. 159, 111678 https://doi.org/10.1016/j.exger.2021.111678

Cain, A., Edwards, M., & Still, J. (2018). An exploratory study of cyber hygiene behaviors and knowledge. Old Dominion University, Department of Psychology, Norfolk, VA 23529, USA

Cook, D., Szewczyk, P., & Sansurooah, K. (2011). Seniors Language Paradigms: 21st century jargon and the impact on computer security and financial transactions for senior citizens. Paper presented at the 9th Australian Information Security and Management Conference, Citigate Hotel, Perth, Western Australia

Díaz, J. D. (2023). La seguridad cibernética y los estudios actuales. Recuperado de https://www.researchgate.net/profile/Juan-Diaz-Aparicio/publication/369790828_La_seguridad_cibernetica_y_los_estudios_actuales/links/642cd1f24e83cd0e2f8df8a2/La-seguridad-cibernetica-y-los-estudios-actuales.pdf

Drew, J.M. (2020). A study of cybercrime victimisation and prevention: exploring the use of online crime prevention behaviours and strategies. Journal of Criminological Research, Policy and Practice. Recuperado de: http://hdl.handle.net/10072/393427

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

Emm, D., (2023). Ignorance is Bliss: Most adults are leaving themselves open to cybercrime, despite knowing the dangers. Kaspersky Report. Recuperado de:

https://media.kasperskydaily.com/wp-content/uploads/sites/86/2023/04/24175910/Kaspersky-Adult-consumer-Report-v5.pdf

Fernández-Montalvo, J., Peñalva, A., & Irazabal, I. (2015). Hábitos de uso y conductas de riesgo en Internet en la preadolescencia. Comunicar, XXII(44),113-120.[fecha de Consulta 9 de Marzo de 2022]. ISSN: 1134-3478. Recuperado de: https://www.redalyc.org/articulo.oa?id=15832806012

Gamito, R., Aristizabal, P., Vizcarra, M., & León, I. (2020) Seguridad y protección digital de la infancia: retos de la escuela del siglo XXI. Educar , vol. 56(1) 219-237

Gudiño, D. (2018). Los riesgos de las redes sociales y su prevención en los mayores. Servicio de Publicaciones de la Universidad de Extremadura, 855-866

Hadlington, L. & Chivers, S. (2018). Segmentation analysis of susceptibility to cybercrime: Exploring individual differences in information security awareness and personality factors. Policing: A Journal of Policy and Practice, April, 1-14

Muniesa, P., Herrera, D., Guerrero, J., Martínez, F., Rubio, M., Gil, V., Santiago, A., & Gómez, M.A. (2023). 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/export/sites/default/.galleries/galeria-de-prensa/documentos-y-multimedia/balances-e-informes/2023/Informe-Cibercriminalidad_2023.pdf

Oluwaseun, T., Kuzankah S., Onimisi S., Oluwatoyin A., & Olanipekun A. (2024). A review of Cybersecurity strategies in modern organizations: examining the evolution and effectiveness of cybersecurity measures for data protection. *Computer Science & IT Research Journal*, *5*(1), 1-25. https://doi.org/10.51594/csitrj.v5i1.699

ONTSI (Observatorio Nacional de Tecnología y Sociedad). (2024). Cómo se protege a la ciudadanía ante los ciberriesgos. Estudio sobre percepción y nivel de confianza en España. Observaciber. Recuperado de: https://www.ontsi.es/es/publicaciones/Como-se-protege-la-ciudadania-de-los-ciberriesgos-Estudio-sobre-percepcion-y-nivel-de

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F., & Basim, H.N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study, Journal of Computer Information Systems, DOI: 10.1080/08874417.2020.1712269