InGenio Journal
Revista de Ciencias de la Ingeniería de la Universidad Técnica Estatal de Quevedo
https://revistas.uteq.edu.ec/index.php/ingenio
e-ISSN: 2697-3642 - CC BY-NC-SA 4.0

Análisis de competencias en ciberseguridad de docentes en entornos virtuales de un IST en Guayas

(Analysis of cybersecurity Competence in Teachers in Virtual Environments at an IST in Guayas)

Karen Estacio
Instituto Superior Tecnológico ARGOS, Guayaquil, Ecuador
k_estacio@tecnologicoargos.edu.ec

Resumen: Esta investigación explora cómo la negligencia humana influye en el éxito de los ciberataques, considerándola el eslabón más débil en la seguridad de la información. Con el aumento de la educación virtual en instituciones educativas, los riesgos de ciberseguridad han crecido debido a la exposición de sistemas y datos sensibles. El estudio evalúa los conocimientos en ciberseguridad de los docentes de un Instituto Superior Tecnológico (IST) privado en Guayas, identificando brechas de seguridad sin proponer mejoras. Se utilizó un enfoque cuantitativo de tipo descriptivo con una encuesta validada por expertos en ciberseguridad y aplicada a 61 docentes. Los resultados mostraron un conocimiento satisfactorio en conceptos de ciberseguridad y buenas prácticas como el control de acceso físico y contraseñas robustas. Sin embargo, se identificaron áreas de mejora en la identificación de amenazas como el phishing y ransomware, subrayando la necesidad de formación especializada para reforzar las defensas contra estas amenazas en evolución.

Palabras clave: Ciberseguridad, entornos educativos virtuales, ciberdelito, Instituto Superior Tecnológico, amenaza cibernética.

Abstract: This research explores how human negligence influences the success of cyberattacks, considering it the weakest link in information security. With the rise of virtual education in educational institutions, cybersecurity risks have increased due to the exposure of systems and sensitive data. The study assesses the cybersecurity knowledge of teachers at a private Higher Technological Institute (HTI) in Guayas, identifying security gaps without proposing improvements. It employed a descriptive and quantitative approach with a survey validated by cybersecurity experts and applied to 61 teachers. The results showed satisfactory knowledge of cybersecurity concepts and good practices, such as physical access control and the use of strong passwords. However, areas for improvement were identified in recognizing threats such as phishing and ransomware, highlighting the need for specialized training to strengthen defenses against these evolving threats.

Keywords: Cybersecurity, virtual educational environments, cybercrime, Technological Higher Institute, cyber threat.

1. INTRODUCCIÓN

En la actualidad, una parte significativa de nuestra vida, tanto personal como profesional, se desenvuelve en el ámbito digital. Incluso profesionales o personas de campos de conocimiento diferentes a la ciberseguridad deben contar con habilidades mínimas de seguridad para resguardar tanto su información personal como la de la organización a la que pertenecen. La ciberseguridad también puede entenderse como la protección del hardware, el software, los datos y la información que existe en un sistema en línea, contra varios tipos de vulneraciones. El reconocimiento de la relevancia del conocimiento en ciberseguridad es generalizado en la actualidad; sin embargo, la aplicación generalizada de dicho conocimiento depende de las habilidades específicas en

DOI: https://doi.org/10.18779/ingenio.v8i2.981
Recibido (Received): 2024/10/09
Aceptado (Accepted): 2025/02/10

ciberseguridad que tenga la fuerza laboral. El principal inconveniente identificado en la actualidad radica en la carencia de estas destrezas en el personal de una empresa [1].

Aunado a lo mencionado, el delito cibernético es un término amplio y abarca actividades delictivas que involucran computadoras o redes informáticas. Esto hace cada vez más crucial la comprensión de las amenazas en el entorno digital para protegerse eficazmente contra los ciberataques [2].

A pesar de la importancia de instruir a los empleados sobre conciencia en ciberseguridad, esta formación no suple la adquisición de habilidades esenciales para fortalecer la defensa de las empresas frente a los ciberataques. Resulta imperativo que las empresas dirijan recursos hacia el desarrollo de competencias de ciberseguridad en todos los niveles, tanto entre los empleados como en los roles de liderazgo. Esta inversión no solo puede aliviar la carga financiera derivada de los ciberataques, sino que también contribuye a mantener la confianza de los consumidores en las marcas empresariales [3].

El informe sobre amenazas en América Latina de Kaspersky, que examinó datos desde junio de 2022 hasta julio de 2023, comparándolos con el mismo periodo del 2021 a 2022, revela que la actividad delictiva en la región se ha mantenido constante, mientras que los ataques de malware contra computadoras y dispositivos móviles han experimentado un aumento significativo del 617 % en los ataques de phishing, junto con un incremento del 50 % en troyanos bancarios [4].

En América Latina, de acuerdo con datos recolectados por Checkpoint [5], las organizaciones dedicadas a abordar los desafíos de seguridad informática mediante soluciones globalizadas reportan que, durante el tercer trimestre de 2022, cada entidad experimentó, en promedio, un total de 1.130 ataques por semana. El sector que más ataques recibe es el de educación e investigación, seguido del sector gubernamental y, por último, del de salud, siendo estos dos últimos los que han ocupado los primeros lugares de manera sostenida a lo largo del tiempo.

El incremento, tanto en la cantidad como en la sofisticación de las amenazas de seguridad o ciberamenazas en el entorno digital genera una creciente demanda de profesionales en ciberseguridad debidamente capacitados. La efectividad en la protección y disuasión de ciberataques se encuentra estrechamente vinculada con la preparación y competencia de los expertos en el terreno, así como con el nivel de ciberalfabetización y la conciencia general de la población [6].

La negligencia y la falta de preparación humana suelen contribuir al éxito de los ciberataques. Con frecuencia, se describe al humano como el eslabón más débil en la seguridad cibernética, una caracterización respaldada por investigadores. Esto se debe no solo a la falta de conocimiento, sino también a atributos psicológicos y sesgos cognitivos que pueden influir en el juicio de un individuo en lo que respecta a la gestión de la confianza [7].

Investigaciones recientes en ciberseguridad revelan que los ciberatacantes capturan 95 contraseñas por segundo, resultando en aproximadamente un robo anual de más de tres mil millones de cuentas. Además, solo el 20 % de los usuarios cambian sus contraseñas tras compromisos de seguridad, lo que subraya la urgencia de abordar esta amenaza constante en internet [7]. Con el incremento de los incidentes cibernéticos en el ámbito educativo, se destaca la relevancia de la ciberseguridad, ya que las instituciones académicas son ahora objetivos sensibles para los hackers, lo que evidencia la vulnerabilidad de los datos [8].

La adopción de la tecnología en las instituciones educativas no solo ha mejorado la cobertura de la educación a distancia, sino que también ha aumentado la gravedad de los riesgos de ciberseguridad experimentados por las escuelas y los estudiantes [9]. Durante la pandemia de COVID-19, muchas instituciones educativas se encontraron desprovistas de profesionales en informática, incapaces de brindar entrenamiento práctico sobre tecnología y los riesgos de

ciberataques a profesores y estudiantes. Posterior a la pandemia y con el avance de las tecnologías se puede constatar que, últimamente, destaca el gran desarrollo en materias TIC [10], nuestras rutinas diarias han cambiado y nos ha empujado a organizaciones e individuos a adoptar una nueva práctica como el trabajo y educación en entornos virtualizados y remotos, lo que significa que las personas pasan más tiempo en línea [11]. La falta de estrategias y recursos de mitigación, incluyendo profesionales de ciberseguridad y especialistas en informática, permite que los hackers roben información sensible de individuos, empresas y estudiantes de los servidores de las instituciones [12].

En Ecuador, según Ministerio de Telecomunicaciones y de la Sociedad de la Información [13] en el territorio, tanto entidades del sector público como del privado, junto con representantes de la sociedad civil y la academia, se encuentran inmersos en el proceso de construcción de la Política Nacional de Ciberseguridad (PNC). Dentro de los pilares fundamentales de esta política se destaca la cultura y educación en ciberseguridad.

Este pilar se fundamenta en la necesidad de establecer buenas prácticas y fortalecer el conocimiento de la población en materia de ciberseguridad, considerando que los usuarios constituyen el principal objetivo de protección [13]. En este sentido, se reconoce a las personas como la primera línea de defensa frente a los riesgos y amenazas presentes en el ciberespacio. Este enfoque no solo resguarda a los individuos, sino que también contribuye a la formación de una fuerza laboral preparada para hacer frente a los desafíos del entorno digital [3].

El objetivo general de la investigación es realizar una completa medición y evaluación de los conocimientos básicos en ciberseguridad entre los docentes de un Instituto Superior Tecnológico (IST) del sector privado en la provincia del Guayas, destacando su papel esencial en la enseñanza dentro de entornos virtuales. Se busca principalmente determinar la capacidad de estos profesionales para prevenir ciberataques y salvaguardar información crucial.

Para alcanzar el objetivo antes mencionado, se delimitaron objetivos específicos que abarcan diversas dimensiones. En primer lugar, analizar la familiaridad de los docentes con conceptos clave en el ámbito de la ciberseguridad. Seguidamente, se evaluará la comprensión que poseen respecto a las mejores prácticas de seguridad, poniendo énfasis en su aplicabilidad en entornos educativos virtuales. Asimismo, se llevará a cabo una medición precisa de la percepción de estos profesionales en relación con las amenazas cibernéticas que puedan afectar su labor docente.

Un aspecto clave de la investigación consistirá en identificar áreas específicas de mejora en los conocimientos y prácticas de ciberseguridad de los docentes. El objetivo final es identificar factores que permitan reducir la vulnerabilidad de la institución educativa ante posibles ataques y salvaguardar la integridad de la información en el ámbito educativo virtual.

Es relevante destacar, que los objetivos planteados se enfocan exclusivamente en la identificación de brechas de seguridad, la investigación prescinde de abordar la implementación de acciones para mejorar las prácticas de seguridad de la información y sus posibles implicaciones económicas.

2. MÉTODO

Para alcanzar los objetivos propuestos, se llevó a cabo una investigación de tipo descriptivo, con un diseño transversal y un enfoque cuantitativo que empleó variables cualitativas. El estudio se dividió en tres fases secuenciales que se explicarán en la siguiente sección. Este enfoque metodológico riguroso garantizó la recopilación de datos relevantes y la validación adecuada del instrumento de medición utilizado, proporcionando una base sólida para el análisis posterior de los resultados.

2.1 Desarrollo

En la primera fase, se utilizó una encuesta estructurada como instrumento principal para la recolección de datos. Esta encuesta abarcó temas clave de ciberseguridad, incluyendo conocimientos sobre amenazas cibernéticas, identificación de malware y gestión de contraseñas. La Tabla 1 presenta un desglose detallado de los temas, subtemas y los indicadores que se buscaban medir, los cuales se definieron tras una revisión exhaustiva de la literatura. La encuesta consta de once preguntas organizadas por tema, detalladas en la Tabla 2. Cada pregunta fue cuidadosamente diseñada y estructurada basándose en un análisis riguroso de la literatura disponible en bases de datos reconocidas como IEEE, ACM y ScienceDirect.

Tabla 1. Temas y subtemas de seguridad de gestión de seguridad de la información.

Tema	Subtemas	Resultados a medir	Autores
Conceptos básicos de ciberseguridad	Ciberseguridad	Comprender la definición básica de los componentes de la ciberseguridad y los delitos cibernéticos.	[14] [9]
	Ciberespacio	Identificar información de carácter sensible.	
	Delitos cibernéticos	Identificar consecuencias de un ciberataque.	
Seguridad física de dispositivos	Seguridad física de dispositivos móviles	Comprender requisitos para la seguridad en dispositivos móviles y PC.	[15] [16] [17] [15]
	Seguridad física de PC	Identificar funciones de seguridad integradas en dispositivos móviles y PC. Comprender la importancia de la actualización de seguridad en sistemas operativos de PC y dispositivos móviles.	
Uso y gestión de contraseñas	Requisitos de construcción de contraseñas	Comprender el requisito de una contraseña segura.	[16] [2] [14] [17] [8] [15]
	Riesgos asociados con gestión inadecuada de contraseñas	Identificar los riesgos de una contraseña débil en sistemas de información.	
Comunicación segura	Identificación de redes inalámbricas seguras	Comprender la importancia de acceder a los sistemas de información de la institución a través de redes alámbricas y/o inalámbricas seguras. Analizar los riesgos al acceder a los sistemas de información de la institución y compartir archivos a través de redes alámbricas y/o inalámbricas inseguras.	[2] [17] [14] [15]

Protección de malware	Definición o noción de malware.	Uso de antivirus para protección contra malware y virus en dispositivos móviles y PC.	[2] [14] [17] [15]
	Clasificación de malware.	Identificar las medidas preventivas para el malware.	
	Mejores prácticas para prevenir malware	Comprender los riesgos de abrir archivos adjuntos maliciosos	

En la segunda fase, se llevó a cabo la validación del cuestionario propuesto mediante la evaluación de un grupo de cuatro expertos, como recomienda Hernández-Nieto [17], la selección de los mismos fue del tipo intencionado, de modo que permitiera elegir cuidadosamente a los evaluadores con base en sus conocimientos, experiencia, experticia en el tema de estudio y evaluación de riesgos en seguridad de la información.

La tercera etapa se centró en la aplicación del cuestionario a un grupo de sesenta y un docentes de diversas áreas del conocimiento que imparten clases en modalidad online en un IST del sector privado, que posee cinco campus distribuidos geográficamente en la provincia del Guayas. El nombre de la institución no se revela en la presente investigación por motivos de confidencialidad; sin embargo, se obtuvo consentimiento informado por parte de las autoridades para ejecutar el estudio. La selección de la muestra se realizó de manera no probabilística por conveniencia, considerando la disponibilidad y accesibilidad de los participantes.

Se estableció comunicación con los cuatro expertos elegidos, mediante el envío de correos electrónicos, en el cual se le solicitó su valiosa contribución a la investigación, se adjuntaron el cuestionario y el formato de evaluación de pertinencia del cuestionario considerando siete criterios (ver Figura 1) [17]. Se explicó detalladamente los criterios de evaluación del instrumento y la escala de valoración, cada experto tuvo la oportunidad de expresar su consentimiento y aprobación para participar en la investigación.

Escala de Valores

1 = Inaceptable 2 = Deficiente 3 = Regular 4 = Bueno 5 = Excelente

Contenido			Evaluación				
Item	**Criterio**	**Observaciones**	**1**	**2**	**3**	**4**	**5**
1	Pertinencia		☐	☐	☐	☐	☐
	Claridad Conceptual		☐	☐	☐	☐	☐
	Redacción y Terminología		☐	☐	☐	☐	☐
	Respuesta Correcta		☐	☐	☐	☐	☐
	Distractores Apropiados		☐	☐	☐	☐	☐
	Niveles de Dificultad		☐	☐	☐	☐	☐
	Formato		☐	☐	☐	☐	☐

Figura 1. Formato de evaluación del instrumento por experto.
Fuente: Elaboración propia a partir de [18].

Tabla 2. Preguntas utilizadas en el cuestionario.

Ítem	Pregunta	Sección y tema relacionado
1	¿Cómo describiría a la ciberseguridad?	Conceptos básicos de ciberseguridad
2	En función de su conocimiento ¿Qué es un delito cibernético?	Conceptos básicos de ciberseguridad
3	Seleccione los tipos de amenazas cibernéticas que conoce	Conceptos básicos de ciberseguridad
4	¿Qué medida (s) de seguridad utiliza para proteger su dispositivo móvil?	Seguridad física de dispositivos
5	¿Qué medida (s) de seguridad utiliza para proteger su PC?	Seguridad física de dispositivos
6	Seleccione el/los tipos de contraseña que utiliza habitualmente para acceder a las plataformas institucionales	Uso y gestión de contraseñas
7	¿Con qué frecuencia realiza el cambio de contraseña de acceso a las plataformas de la institución?	Uso y gestión de contraseñas
8	Para acceder remotamente a la plataforma educativa de la institución utiliza:	Comunicación segura
9	¿Cuál (es) de las siguientes opciones describiría a un malware?	Protección de malware
10	Seleccione los tipos de malware que conoce:	Protección de malware
11	¿Con qué tipo de consecuencia relacionaría a un malware?	Protección de malware

Una vez que los expertos remitieron el formato de evaluación del cuestionario se procedió utilizar la fórmula de Coeficiente de Validez de Contenido (CVC) (ver Ecuación 1) que se define como el promedio de los Coeficientes de Validez de Contenido de cada pregunta de la encuesta. [18].

$$CVC = CVC_i - Pe_i \quad (1)$$

Donde CVC_i es resultado de la Ecuación 2.

$$CVC_i = \frac{M_x}{Vmax} \quad (2)$$

M_x representa la media del elemento en la puntuación dada por los expertos y $Vmax$ la puntuación máxima que el ítem podría alcanzar. Por otro lado, debe calcularse el error asignado a cada ítem (Pe_i), de este modo se reduce el posible sesgo introducido por alguno de los jueces, (ver Ecuación 3), siendo j el número de expertos participantes.

$$Pe_i = \left(\frac{1}{j}\right)^j \quad (3)$$

La implementación del cuestionario en línea se llevó a cabo mediante la aplicación Google Forms, y los datos resultantes fueron sometidos a un análisis estadístico utilizando Microsoft Excel. Este procedimiento facilitó la adquisición de la información esencial para el análisis dentro del marco de este estudio. El enlace al cuestionario fue enviado a los 61 docentes participantes a través del correo electrónico institucional, detallando el propósito de la investigación para su conocimiento. La encuesta se distribuyó respetando rigurosamente los principios éticos, garantizando el anonimato y la confidencialidad de los participantes. Antes de su participación, se obtuvo el consentimiento informado, asegurando la confidencialidad de las respuestas recopiladas.

3. DISCUSIÓN

3.1 Resultados de la validación del cuestionario

Los resultados obtenidos de la aplicación del formato de evaluación y validación del instrumento desarrollado para la presente investigación por parte de los expertos (ver Tabla 3), resultó poseer un Coeficiente de Validez de Contenido alto de 0,86 (superior a 0,8) conforme [17].

3.2 Resultados del cuestionario aplicado para determinar las medición y evaluación de los conocimientos básicos en ciberseguridad entre los docentes de un IST del sector privado en la provincia del Guayas que imparten clases en entornos virtuales.

El análisis de los resultados del cuestionario compartido a los docentes participantes revela estadísticamente mediante la interpretación de las frecuencias relativas de forma significativa sobre la percepción de los docentes en cuanto a la ciberseguridad (Figura 2). Se observa que el 33 % la asocia exclusivamente con la protección de la información, mientras que un 18 % la vincula tanto con la protección de sistemas como con medidas de seguridad en línea.

Es relevante señalar que el 59 % de los docentes evaluados eligió definir un delito cibernético como aquel cometido con la intención de dañar o interrumpir un sistema o red (Figura 3), mientras que, solo un 2 % manifestó desconocer la respuesta.

Tabla 3. Resultados de aplicación del Coeficientes de Validez de Contenido al instrumento.

Ítem	E1	E2	E3	E4	Sx_1	M_x	CVC_i	P_{ei}	CVC_{tc}
1	33	25	34	26	118	3,371	0,843	0,004	0,839
2	32	28	29	27	116	3,314	0,829	0,004	0,825
3	30	25	35	28	118	3,371	0,843	0,004	0,839
4	34	29	35	28	126	3,600	0,900	0,004	0,896
5	33	32	31	28	124	3,543	0,886	0,004	0,882
6	33	27	34	35	129	3,686	0,921	0,004	0,918
7	28	27	28	32	115	3,286	0,821	0,004	0,818
8	35	30	28	28	121	3,457	0,864	0,004	0,860
9	35	34	28	30	127	3,629	0,907	0,004	0,903
10	31	28	28	29	116	3,314	0,829	0,004	0,825
11	27	35	28	32	122	3,486	0,871	0,004	0,868
Coeficiente de Validez de Contenido									**0,861**

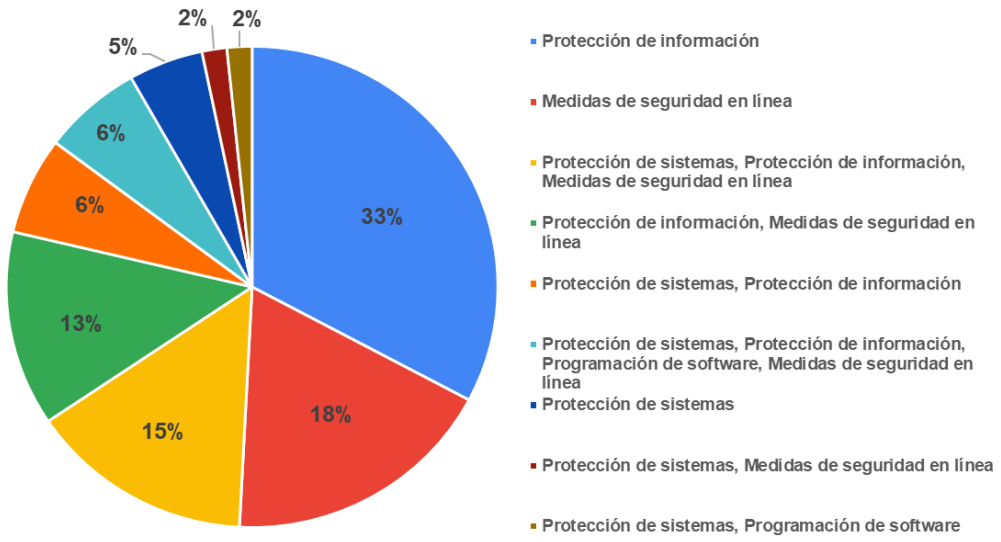

Figura. 2. Descripción de la ciberseguridad por parte de los encuestados.

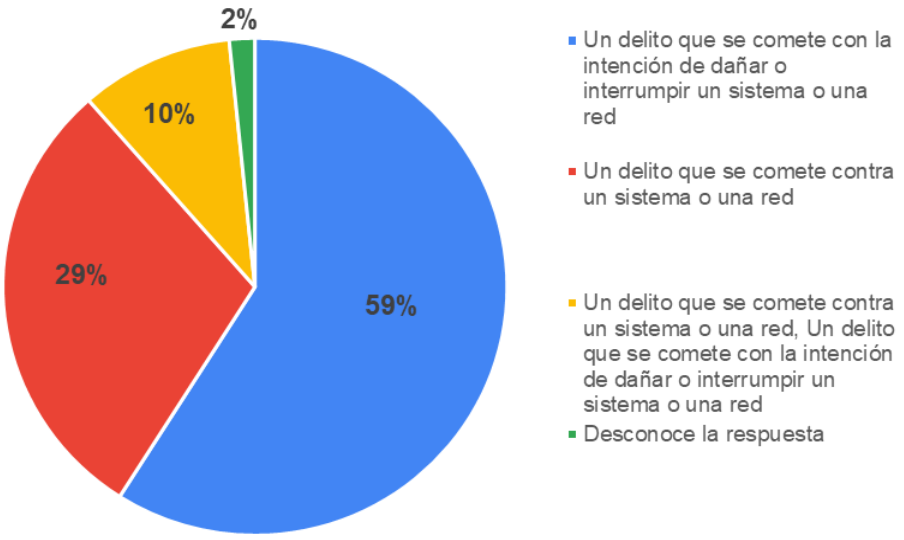

Figura 3. Percepción de la descripción delito cibernético.

En lo que respecta a la pregunta sobre los tipos de delitos cibernéticos, se proporcionó una lista de opciones de selección múltiple (Figura 4). El 95 % de los participantes seleccionó robo de información, el 72 % optó por ciber espionaje, y el 70 % eligió fraude.

En la primera sección, "Conceptos básicos de ciberseguridad" (Tabla 2), los resultados obtenidos revelan que los participantes demuestran un nivel de conocimiento satisfactorio en relación con los conceptos asociados a la ciberseguridad y el delito cibernético. Sin embargo, al abordar la identificación de tipos específicos de amenazas en el ciberespacio, que podrían tener repercusiones significativas, como lo es el phishing, se observa que solo 39 docentes lo seleccionaron, asimismo, 33 de ellos optó por malware.

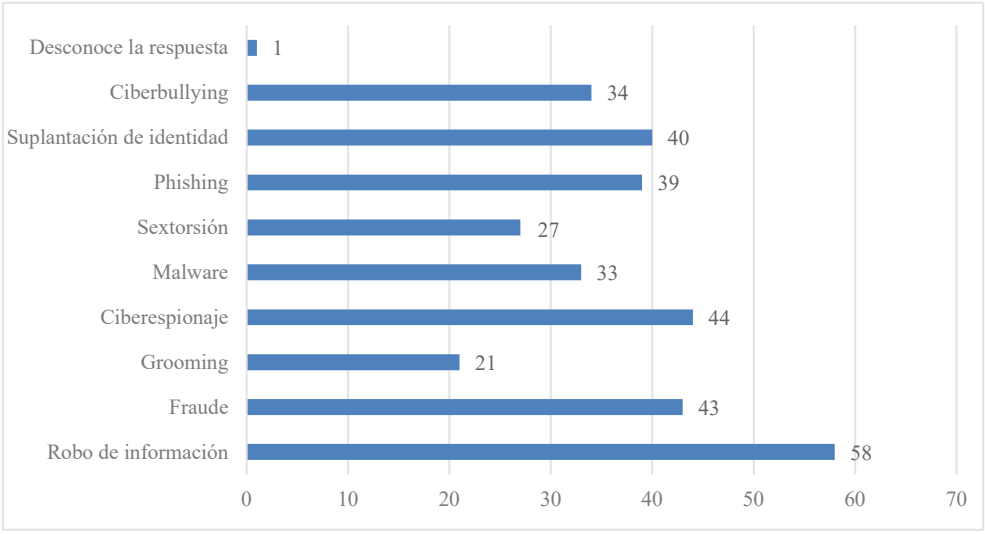

Figura. 4. Tipos de amenazas cibernéticas que conocen los encuestados.

La Figura 5 detalla los resultados destinados a evaluar las medidas de seguridad implicadas a la protección de los dispositivos móviles considerando que dicho dispositivo le permite al docente conectarse hacia las plataformas institucionales que albergan información confidencial y sensible,

el 70 % utiliza un código PIN o un patrón para desbloquear su dispositivo, mientras que el 56 % seleccionaron activar autenticación de dos factores al igual que actualizar el sistema operativo.

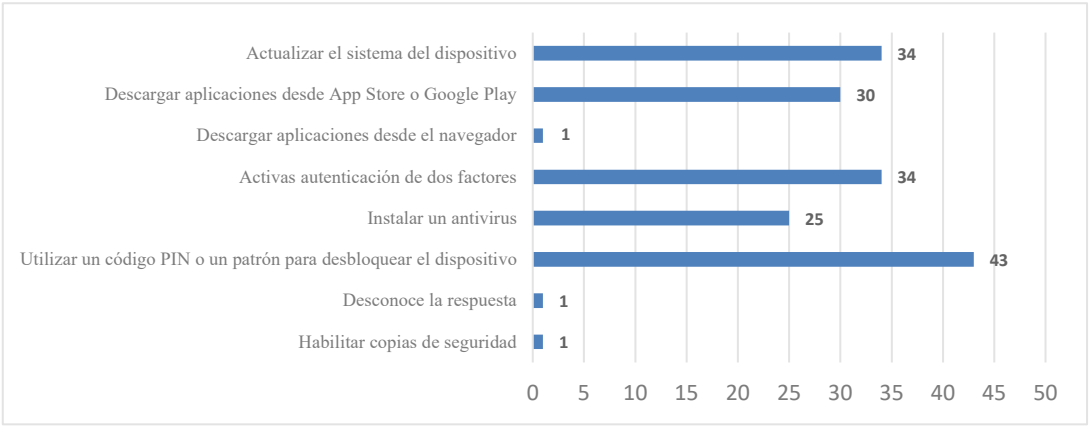

Figura 5. Medida (s) de seguridad utilizadas para proteger dispositivos móviles.

En cuanto a las medidas de seguridad destinadas a proteger la PC durante las conexiones a plataformas institucionales, se formuló una pregunta de selección múltiple (Figura 6). El 83 % de los participantes optaron por la instalación de un antivirus, el 25 % seleccionaron la actualización del sistema operativo y la utilización de un firewall. Al analizar la sección dedicada a la "Seguridad física de dispositivos" (Figura 5) y (Figura 6), se puede interpretar un alto grado de aplicación de estas medidas por parte de los participantes.

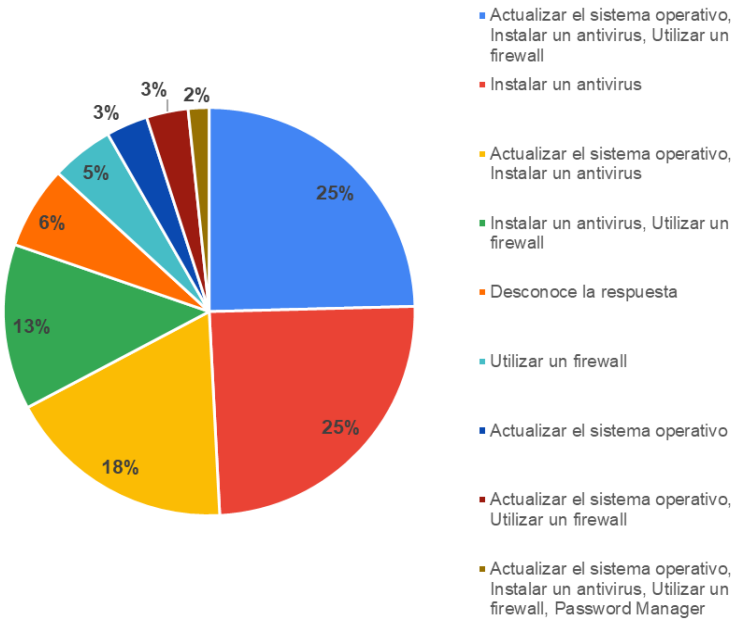

Figura 6. Medida (s) de seguridad utilizadas para proteger la PC.

En la sección dedicada al "Uso y gestión de Contraseñas" (Tabla 2), se llevó a cabo una evaluación específica de los requisitos de construcción de contraseñas. A través del cuestionario, se solicitó a los participantes seleccionar los tipos de contraseñas que emplean. Es relevante resaltar que un considerable 88 % de los encuestados opta por contraseñas que incluyen una combinación de letras, números y símbolos, lo cual sugiere una práctica robusta en la creación de

contraseñas. Por otro lado, únicamente un 5 % indicó utilizar fechas importantes como parte de sus contraseñas (Figura 7). Este hallazgo resalta la prevalencia de prácticas de seguridad sólidas al construir contraseñas entre la mayoría de los participantes, con una precaución hacia el uso de información personal y confidencial significativa.

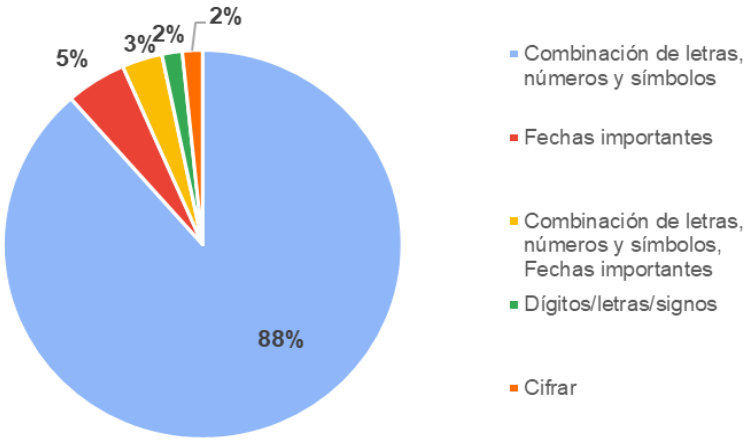

Figura 7. Tipos de contraseña que utiliza habitualmente para acceder a las plataformas institucionales.

En lo que respecta a la frecuencia de cambio o actualización de contraseñas (Figura 8), se observaron diversas prácticas entre los participantes. Un 29 % de ellos opta por llevar a cabo esta actualización anualmente, mientras que un 25 % lo hace únicamente una vez desde la asignación inicial de la contraseña temporal o por defecto. De manera preocupante, un 10 % de los participantes admitió nunca haber realizado la actualización de su contraseña, prefiriendo mantener la contraseña asignada por defecto. Este último hallazgo destaca la importancia de concientizar sobre la necesidad de prácticas regulares de cambio de contraseñas para fortalecer la seguridad en el acceso a plataformas y sistemas institucionales.

Dentro de la sección dedicada a la "Comunicación Segura", se abordó específicamente el tipo de red que los docentes emplean al conectarse a las plataformas institucionales desde ubicaciones remotas (Figura 9). El 89 % de los participantes indicó seleccionar la red wifi de su hogar, señalando una preferencia notoria por la familiaridad y confiabilidad de esta conexión. Además, el 53 % expresó su preferencia por conectarse específicamente a través de la red wifi doméstica, mientras que un 38 % opta por utilizar datos móviles para esta finalidad.

Estos resultados revelan un patrón interesante en el comportamiento de conexión remota de los docentes, destacando la preeminencia de la red wifi del hogar como la elección principal. Asimismo, es alentador observar que un porcentaje significativo evita el uso de redes públicas para el acceso remoto, lo cual indica una conciencia de seguridad y una práctica prudente entre los participantes.

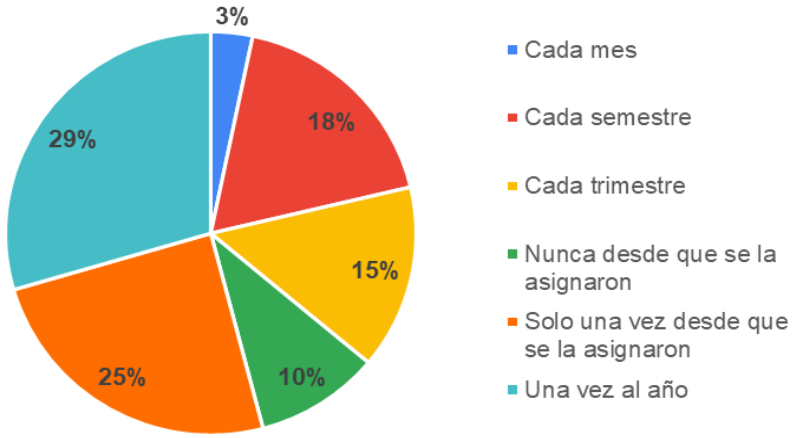

Figura 8. Frecuencia de cambio de contraseña de acceso a las plataformas de la institución.

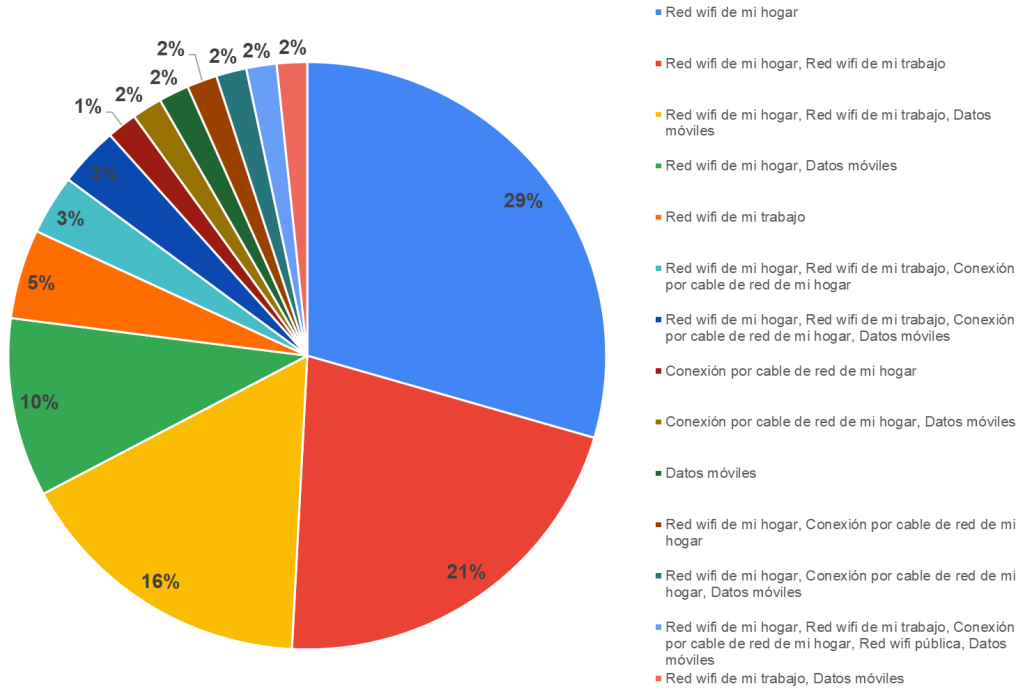

Figura 9. Tipo de red que utilizan encuestados para acceder remotamente a la plataforma educativa de la institución.

La sección sobre "Protección de Malware" se diseñó para evaluar la comprensión del malware y su prevención. Las preguntas 10 a 12 se centraron en este aspecto (Tabla 2). La Figura 10 revela que un notable 84 % de los participantes identifica el malware como un software malicioso, mientras que el 41 % lo asocia con software que roba información. Solo un pequeño 7 % desconoce la respuesta.

Estos resultados evidencian un entendimiento generalizado entre los participantes sobre la naturaleza maliciosa del malware, con una mayoría que lo identifica como un tipo de software con intenciones nocivas. La asociación con el robo de información también resalta la conciencia de las amenazas asociadas al malware por parte de un porcentaje significativo de los encuestados.

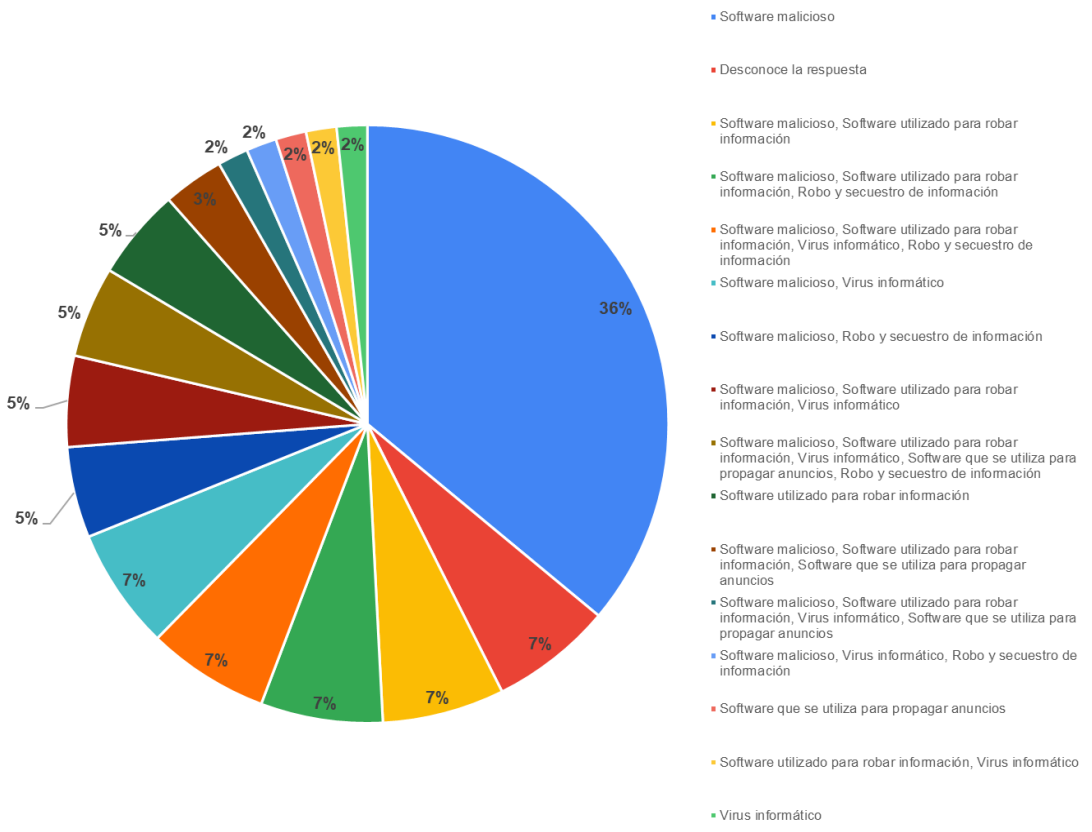

Figura 10. Descripción de un malware según los encuestados.

Al solicitar a los participantes que identifiquen los tipos de malware que conocen mediante una selección múltiple, se encontró que 47 docentes seleccionaron troyanos. Por otro lado, 9 indicaron desconocer la respuesta (Figura 11).

Estos resultados evidencian un conocimiento sustancial entre los participantes sobre tipos particulares de malware, con una notoria preeminencia en la comprensión de los troyanos. La diversidad de opciones seleccionadas resalta la variabilidad en los conocimientos sobre amenazas de malware entre los encuestados, siendo notable que solo el 33 % tiene conocimientos sobre el ransomware. Este tipo de malware es especialmente peligroso, ya que secuestra información mediante extorsiones con fines económicos, siendo importante la concientización sobre esta amenaza crítica.

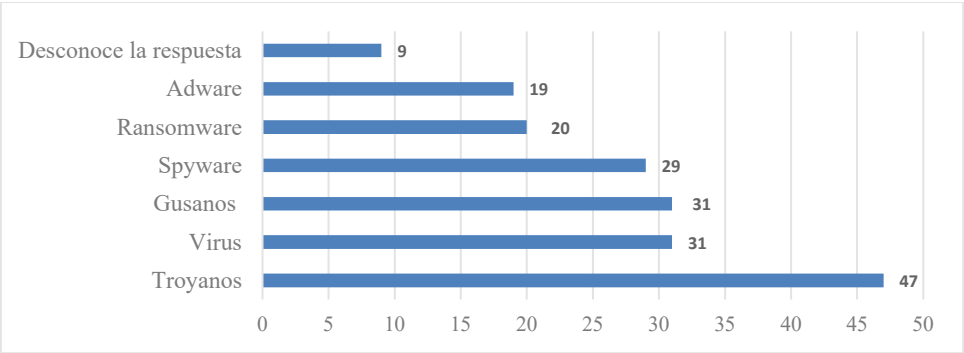

Figura 11. Tipos de malware que conocen los encuestados.

En cuanto a las consecuencias asociadas al malware, las cifras más destacadas revelan que el 44 % de los encuestados identificaron daño a los sistemas informáticos como una consecuencia relevante, mientras que el 15 % señaló el robo de información (Figura 12). De manera preocupante, solo un 3 % seleccionó la interrupción del negocio y la pérdida de productividad como posibles consecuencias.

Estos resultados plantean inquietudes, ya que la baja identificación de la conexión entre los riesgos graves de un ataque de malware y las posibles repercusiones en la operación y productividad de la institución destaca la necesidad de una mayor conciencia sobre la importancia de protegerse contra estas amenazas para garantizar el funcionamiento ininterrumpido de la institución.

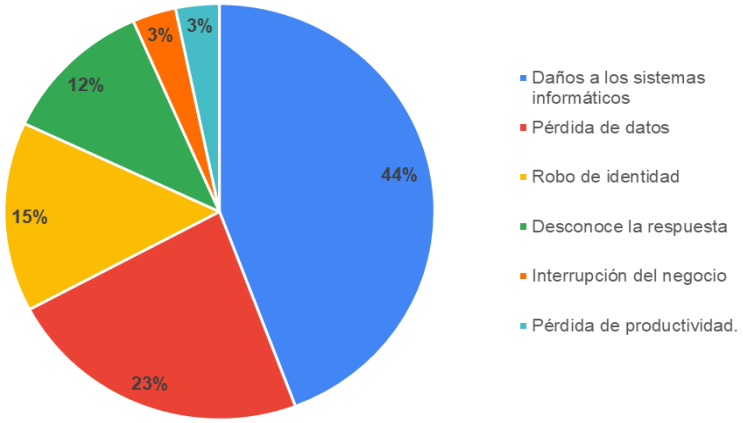

Figura 12. Tipo de consecuencia relacionada a un malware según los encuestados.

4. CONCLUSIONES

Los resultados del estudio permiten concluir que, entre el grupo de docentes participantes, existe una comprensión generalizada de los conceptos básicos de ciberseguridad, lo que sugiere una familiaridad con temas fundamentales como la importancia de las contraseñas seguras, el control de acceso a los sistemas y las medidas de protección física. Sin embargo, a pesar de este conocimiento general, se identificaron áreas críticas de mejora, particularmente en la conciencia y el reconocimiento de amenazas específicas, como el phishing, el ransomware y otros tipos de ciberataques avanzados que se han vuelto más comunes en los últimos años.

Esta brecha de conocimiento sugiere que, si bien los docentes tienen un entendimiento básico de cómo proteger la información, hay un déficit en su capacidad para identificar y responder a amenazas más sofisticadas que evolucionan constantemente en el panorama digital, relacionadas a extorsiones y secuestro de información que podría detener la operación y actividades de la Institución Académica.

Los resultados destacan que la mayoría de los docentes utiliza contraseñas seguras y adopta medidas de seguridad física en dispositivos. Sin embargo, existe un espacio para mejorar la frecuencia de cambio de contraseñas y la comprensión de las consecuencias institucionales, por materialización del malware relacionado a suplantación de identidad. En la sección de conexiones y acceso a la red, es alentador mencionar que la mayoría de los docentes prefiere conexiones seguras al acceder a plataformas institucionales, evitando redes públicas.

Este estudio proporciona una visión valiosa sobre la preparación en ciberseguridad de los docentes en entornos virtuales de distintas áreas del conocimiento en formación académica. Aunque se demuestre un entendimiento medianamente alto, la continua formación y

concientización son esenciales para mantenerse al día con las amenazas emergentes y fortalecer las defensas en un mundo digital en constante cambio. El análisis de implementación de programas de capacitación específicos puede mejorar significativamente la resiliencia contra ciberataques, asegurando un entorno educativo virtual más seguro y protegido.

Aunque esta investigación no abordó directamente la implementación de acciones para mejorar las prácticas de seguridad de la información ni sus posibles implicaciones económicas, se sugiere que, con base en los resultados obtenidos, se elaboren políticas de seguridad de la información orientadas a cubrir las brechas identificadas. Estas políticas deberían contemplar medidas claras y aplicables que fortalezcan la gestión de riesgos, aumenten la concienciación y garanticen un enfoque sostenible para proteger los activos digitales de la institución académica.

REFERENCIAS

[1] B. J. Blažič, "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training", *Technol. Soc.*, vol. 67, pp. 101769, nov. 2021. [Online]. Available: https://doi.org/10.1016/j.techsoc.2021.101769

[2] P. Zaqueu, and T. Mawela, "Factors Contributing to Cybersecurity Awareness, Education and Training", in Proceedings of NEMISA Digital Skills Conference 2023: Scaling Data Skills For Multidisciplinary Impact, pp. 69-58, 2023. [Online]. Available: https://doi.org/10.29007/l4ph

[3] M. Adams, and M. Makramalla, "Cybersecurity Skills Training: An Attacker-Centric Gamified Approach", *Technol. Innov. Manag. Rev*, vol. 5, no. 1, pp. 5-14, jan. 2015. [Online]. Available: https://pdfs.semanticscholar.org/2053/f0a9b61a83e861c00e656c9f53fd9b086930.pdf

[4] "Cómo proteger tus datos en línea usando un gestor de contraseñas", Kaspersky, 2023. [En línea]. Disponible en: https://www.kaspersky.es/resource-center/preemptive-safety/protecting-your-data-online-password-manager

[5] "Check Point Research: Third quarter of 2022 reveals increase in cyberattacks and unexpected developments in global trends", Check Point Research Team, 2022. [Online]. Available: https://blog.checkpoint.com/2022/10/26/third-quarter-of-2022-reveals-increase-in-cyberattacks

[6] A. Brilingaitė, L. Bukauskas, and A. Juozapavičius, "A framework for competence development and assessment in hybrid cybersecurity exercises", *Comput. Secur.*, vol. 88, pp. 101607, jan. 2020. [Online]. Available: https://doi.org/10.1016/j.cose.2019.101607

[7] A. A. Garba, F. Jeribi, I. Al-Shourbaji, M. Alhameed, F. Reegu, and S. Alim, "An Approach To Weigh Cybersecurity Awareness Questions In Academic Institutions Based On Principle Component Analysis: A Case Study Of Saudi Arabia", vol. 10 no. 4, apr. 2021. [Online]. Available: https://www.ijstr.org/final-print/apr2021/An-Approach-To-Weigh-Cybersecurity-Awareness-Questions-In-Academic-Institutions-Based-On-Principle-Component-Analysis-A-Case-Study-Of-Saudi-Arabia.pdf

[8] I. L. Suarez Cruz, A. Escobar Díaz, y H. Vacca González, "Unidades de climatización para centro de datos", *Rev. Vínculos*, vol. 16, no. 1, pp. 128-147, jun. 2019. [En línea]. Disponible en: https://doi.org/10.14483/2322939X.15273

[9] Z. Yan, Y. Xue, and Y. Lou, "Risk and protective factors for intuitive and rational judgment of cybersecurity risks in a large sample of K-12 students and teachers", *Comput. Hum. Behav.*, vol. 121, pp. 106791, aug. 2021. [Online]. Available: https://doi.org/10.1016/j.chb.2021.106791.

[10] M. J. Garrido Antón, y Á. García-Collantes, "El impacto de las tecnologías de la información y la comunicación en la educación. La importancia de la formación, la información y la sensibilización", *Rev. Tecnol. Cienc. y Educ*, pp. 155-182, jan. 2022. [En línea]. Disponible en: https://doi.org/10.51302/tce.2022.660

[11] "Sector de Desarrollo de la UIT: Fomento de la transformación digital mundial", ITU, 2023. [En línea]. Disponible en: https://www.itu.int/es/mediacentre/backgrounders/Pages/itu-d-driving-ict-led-development-worldwide.aspx

[12] W. J. Triplett, "Addressing Cybersecurity Challenges in Education", *Int. J. STEM Educ. Sustain.*, vol. 3, no. 1, pp. 47-67, jan. 2023. [Online]. Available: https://www.researchgate.net/publication/366844898_Addressing_Cybersecurity_Challenges_in_Education

[13] "Plan Nacional de Telecomunicaciones y Tecnologías de Información del Ecuador 2022-2025", Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2021. [En línea]. Disponible en: https://www.telecomunicaciones.gob.ec/wp-content/uploads/2022/06/Plan-de-Servicio-Universal-signed-signed-signed-signed-signed.pdf

[14] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia", *Information*, vol. 12, no. 10, pp. 417, oct, 2021. [Online]. Available: https://doi.org/10.3390/info12100417.

[15] L. Kraus, V. Švábenský, M. Horák, V. Matyás, J. Vykopal, and P. Celeda, "Want to Raise Cybersecurity Awareness? Start with Future IT Professionals", en *Proceedings of the 2023 Conference on Innovation and Technology in Computer Science Education V. 1*, Turku Finland: ACM, jun, 2023, pp. 236-242. [Online]. Available: https://doi.org/10.1145/3587102.3588862.

[16] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training", in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, Bangkok: IEEE, may 2012, pp. 256-262. [Online]. Available: https://doi.org/10.1109/CYBER.2012.6392562.

[17] M. Choi, Y. Levy, and H. Anat, "The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse", in Proceedings of the Eighth Pre-ICIS Workshop on Information Security and Privacy, Milano, December 14, 2013. [Online]. Available: https://aisel.aisnet.org/wisp2012/29/

[18] I. Pedrosa, J. Juarros-Basterretxea, A. Robles-Fernández, J. Basteiro, y E. García-Cueto, "Pruebas de bondad de ajuste en distribuciones simétricas, ¿qué estadístico utilizar?", *Univ. Psychol.*, vol. 14, no. 1, oct. 2014. [En línea]. Disponible en: https://doi.org/10.11144/Javeriana.upsy14-1.pbad