1234 “PASSWORD”: ESTUDIO SOBRE SEGURIDAD DIGITAL EN JÓVENES SALVADOREÑOS.

Eje temático del Congreso: Comunicación Digital

Autora:
Karla Ramos

Resumen

Esta ponencia presenta los resultados de un estudio realizado en El Salvador durante el año 2021, enfocado en prácticas de seguridad digital entre jóvenes de 16 a 24 años residentes en zonas urbanas y rurales. El objetivo era identificar las prácticas comunes en autogestión de sus datos. Se aplicó una metodología mixta a una muestra de 976 encuestados, y 28 jóvenes divididos en 3 grupos focales. Los resultados permitieron identificar las prácticas más comunes, falencias y debilidades. El estudio concluye en la necesidad de mejorar la seguridad para manejo de datos personales y la necesidad de desarrollar más el pensamiento crítico.

Palabras clave: Seguridad Digital, Alfabetización Mediática e Informacional, Jóvenes.

1. Introducción

La seguridad digital forma parte de esas habilidades y conocimiento que la UNESCO (2011a) plantea dentro de la Alfabetización Mediática e Informacional, las cuales identifica como esenciales para el desarrollo del pensamiento crítico y la eficaz relación con los mensajes y los medios (Unesco, 2011a).

Lo anterior pone de manifiesto un gran marco general y conceptual, que desde la perspectiva de Ferrés y Piscitelli, 2012; Durán Becerra y Lau 2020 debería articular otras dimensiones más específicas para su desarrollo, tales como las siguientes:

1. Informacional: la capacidad para acceder, evaluar, comprender críticamente la información. (Durán y Lau, 2020).

2. Digital: relacionada con el uso básico y avanzado de las TIC. Se refiere, entre otros aspectos, al diseño de soluciones y toma de decisiones estratégicas y reflexivas con las TIC (Durán y Lau, 2020).

3. Mediática: referida a hacer frente a un fenómeno complejo compaginando la cultura participativa con el desarrollo de la capacidad crítica (Ferrés, J., y Piscitelli, A.,2012). Es decir, al desarrollo de las habilidades y capacidades para el entendimiento del significado, funcionamiento y contexto de los medios; participación en redes, gobierno en línea y para tomar decisiones de seguridad, compartir conocimientos y comprender los aspectos éticos y legales del uso de los medios (Durán y Lau, 2020).

Esta última dimensión, es una de las que más se relaciona con la seguridad digital, la cual adquiere un significado de protección contra los problemas generados por el uso de las TIC (Barrow y Heywood-Everett, 2006, como se cita en Gallego et al., 2019), y está relacionada con la privacidad, integridad y también con promover, modelar y formar a los ciudadanos digitalmente responsables, para contrarrestar o minimizar riesgos de ingeniería social, conocida como la ciencia y arte del engaño a seres humanos, la cual se encuentra en aumento, Según el Reporte de Data Breach Investigations (Verizon 2018, como se cita en Conde, 2020) Algunos ejemplos donde se manifiesta son phishing (suplantación de identidad a través de e-mail falsos), smishing (fraude que se ejecuta a través de mensajes para incentivar hacer clics en sitios maliciosos), malware o software que se hacen pasar por legítimos, pretexting (práctica de presentarse como otra persona para obtener información privada (Sustama, 2022) entre otros.

En Centroamérica, algunos estudios han evidenciado el incremento en el interés y la relevancia de este tema para generar recomendaciones u orientaciones en materia de políticas públicas.

Uno de los primeros ejemplos es la investigación realizada por Castillejos, et al. (2016), quienes investigaron el tema de seguridad en las competencias digitales de los millenials en México. El estudio señaló que buena parte de estudiantes se mostraron prudentes al recibir mensajes desconocidos. El estudio también permitió conocer hábitos como el bloqueo de páginas de procedencia dudosa y modificación periódicas de sus contraseñas, además de mostrar el uso de tecnologías "verdes" como aporte innovador.

En Costa Rica, el Observatorio Centroamericano de Seguridad Digital de la Fundación Acceso (2019), desplegó una investigación sobre privacidad y vigilancia digital en El Salvador, y recomendó al país que se forme a personas ligadas a derechos humanos, a modo de generar sinergias para que las entidades y personas cuenten con un mejor estado de seguridad digital.

En la misma línea, la Fundación Comunicares (2021) presentó los resultados del estudio "Desde nuestra mirada", en el que se encontró, que el 28% de los jóvenes utilizó la misma contraseña en todas sus redes, y a la vez, el 54% abrió una nueva cuenta de Facebook debido a que olvidó su contraseña original. Sólo el 9% aduce

utilizar contraseñas combinando cuatro tipos de caracteres: mayúsculas, minúsculas, números y signos.

Si bien, estos estudios permiten conocer algunos indicios en la región, aún son necesarios más datos de fuentes primarias. Particularmente, en El Salvador, es importante indagar acerca de la temática tomando en consideración que los jóvenes salvadoreños representan el 54.1% de la población, según la Dirección General de Estadística y Censos (2019).

Este texto, representa una investigación enfocada en jóvenes salvadoreños de 16 a 24 años de zonas rurales y urbanas en El Salvador. Si bien, se trata de una aproximación inicial, se pretende:

a) Conocer las diversas prácticas y herramientas de protección digital utilizadas por los jóvenes

b) Generar datos con el propósito de desarrollar insumos para futuros planes de acción.

Se busca conocer con mayor detalle la situación local en materia de seguridad digital, respondiendo a la siguiente pregunta:

¿Qué prácticas y creencias sobre seguridad digital se pueden observar entre los jóvenes salvadoreños de 16 a 24 años en las zonas urbanas y rurales?

2. Metodología/planteamiento

Se utilizó un método mixto. Morse (2003) señala que una de sus principales ventajas es permitir el estudio de un fenómeno de forma más amplia y completa. Tashakkori y Teddli (1988) proponen una taxonomía de diseño mixto, de estatus equivalente donde para responder la pregunta de investigación, se conduce el estudio utilizando las aproximaciones cualitativas y cuantitativas, y los datos, se recogen en el mismo momento y se analizan de forma complementaria.

Para la recolección de datos, en lo cuantitativo, se utilizó un cuestionario en línea de respuestas cerradas. Y debido a que es difícil garantizar la aleatoriedad en la selección de los individuos, se utilizó un muestreo no probabilístico. La estrategia cualitativa de recogida de datos, fue la realización de 3 grupos focales en tres zonas principales de El Salvador.

Posteriormente, se analizaron los datos, los cuales según Hernández (2020), deben seguir los procedimientos propios de cada enfoque. En el caso de lo cuantitativo, se utilizó estadística descriptiva básica e inferencial, y lo cualitativo, a través de codificación por categorías. D modo que, para la lo cuantitativo, los datos se vaciaron, en una matriz de Excel, y seguidamente, se realizó por cada pregunta una

visibilización de la data obtenida, para posteriormente triangularla con lo encontrado dentro de las categorías cualitativas.

Las categorías de análisis se describen a continuación: Dispositivos-conexión, contraseñas, datos públicos, confianza en la web. Respecto al número de participantes, la elección propositiva o de juicio no parte de un número determinado, como lo define Patton (2001), "en este campo no hay reglas para decir el tamaño de la muestra y si hubiera que enunciar una, esta sería todo depende" (p.224).

Con base en lo anterior, se utilizó una muestra de la población salvadoreña, mayor de 16 años (a quienes se les pidió un consentimiento firmado por sus encargados legales) y menor de 25 años a quienes también se les pidió autorización para ser parte de este estudio.

Se aplicó el cuestionario a 976 jóvenes en 37 centros educativos, tanto públicos, como privados del área rural urbana. Y en los grupos focales, participaron 28 jóvenes de tres zonas diferentes del país.

2. Resultados

Por distribución geográfica, se tuvo jóvenes de 13 de los 14 departamentos de El Salvador: 29.9%, San Salvador; 21.6%, Santa Ana; 13.7%, San Miguel; 3.5%, La Libertad. Lo anterior, incluye zona rural y urbana.

Siguiendo los objetivos planteados, se generaron datos para conocer las prácticas y herramientas de protección digital utilizadas por los jóvenes. El detalle de estas, se agruparán en las categorías planteadas anterioriormente:

2.1. Dispositivos y conexión

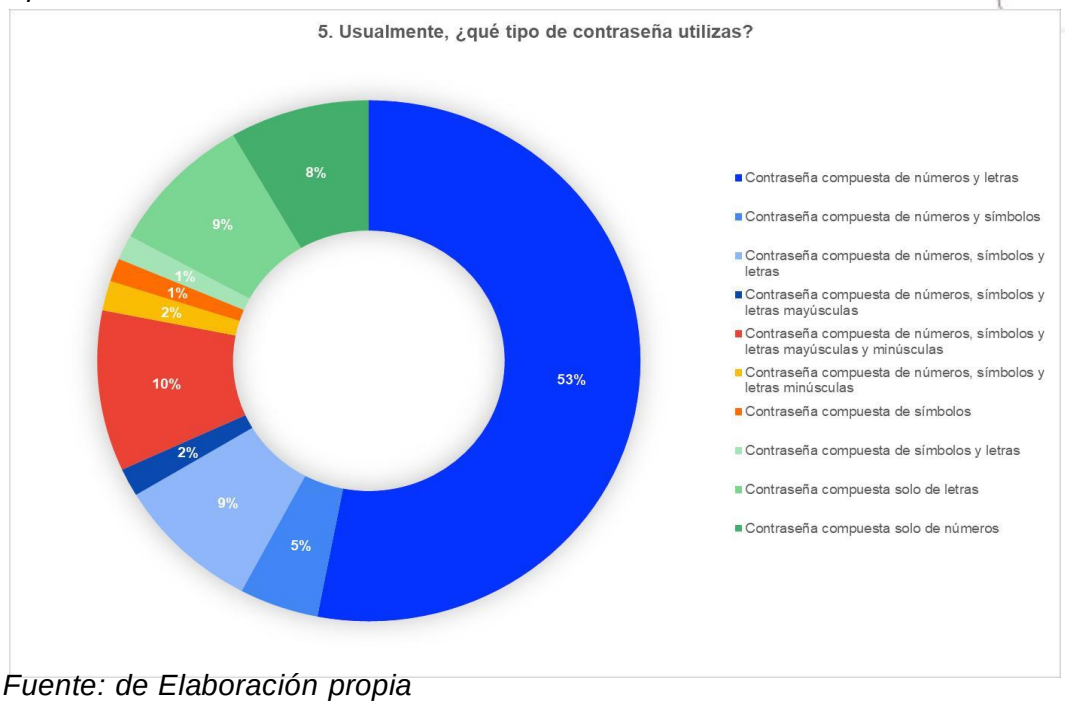
Con o sin internet, el celular (96.3%), la laptop (64.8 %) y la tablet (12.1%) constituyen las tecnologías de mayor uso.

Respecto al tiempo de conexión, el 70 % permanece en línea por más de tres horas. El internet residencial, es el que utiliza la mayoría, según respondieron, le sigue la modalidad prepaga y el pospago.

Las conexiones en los centros de estudio, parques o sitios públicos y los cibercafés también fueron registradas por los jóvenes, en menor frecuencia, como un punto de acceso a la red

2.2 Contraseñas

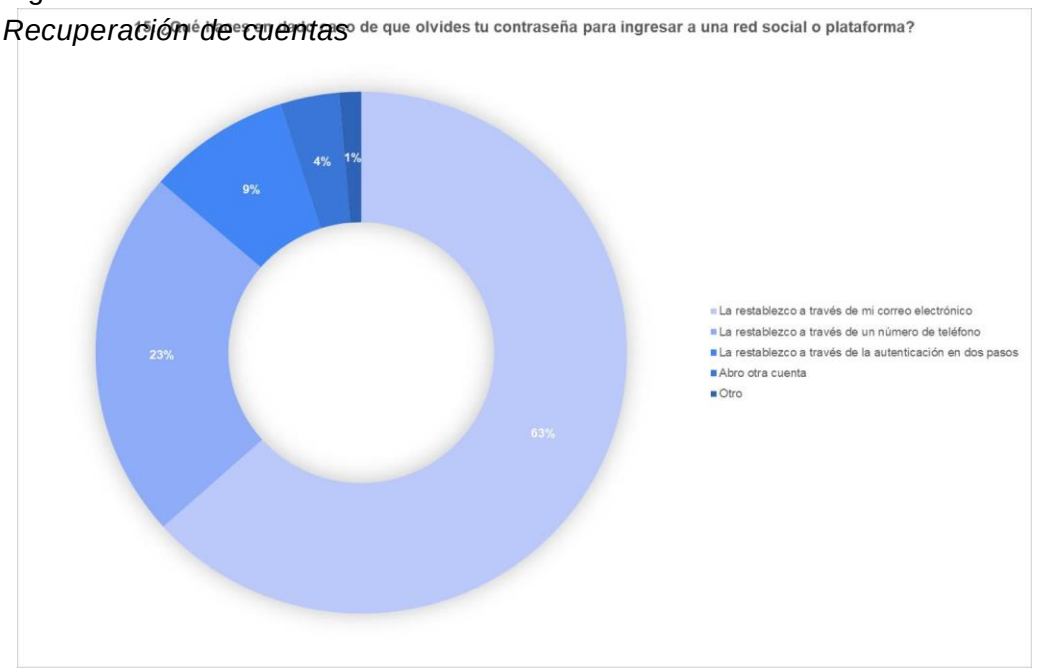
Figura 1.
Tipo de contraseña



Fuente: de Elaboración propia

Más del 61 % de jóvenes, usa contraseña no segura. Cuando las olvidan, seis de cada diez jóvenes, la restablecen por correo electrónico; el 9 %, por verificación en dos pasos, el resto, (23 %), lo hace a través de un número de teléfono.

Figura 2
Recuperación de cuentas



Fuente: elaboración propia

La respuesta de los encuestados, deja de lado la autenticación en dos pasos, por medio de la cual, sitios bancarios, redes sociales, videojuegos y plataformas de correo electrónico, deben comprobar de diferentes maneras la identidad de una persona, asegurando dos de ellas, (Marchal, 2019). Estas pueden ser a través de un código, huella digital, pregunta personal previamente guardada, entre otros. Los principales servidores como Google, Apple o Outlook recomiendan su implementación para reforzar los servicios web.

El 84.9%, no conoce alguna aplicación diseñada para la administración de contraseñas. Esto, representa una oportunidad de formación para las instituciones educativas, de tal modo que puedan profundizar en estas herramientas de ciberseguridad.

Solo el 31 % de los jóvenes, utiliza una contraseña distinta para cada cuenta que ha creado. A lo anterior, se suma otro elemento y es que, el 40 % nunca las actualiza. Los que sí lo hacen, se dividen entre los siguientes porcentajes: 26 %, cada seis meses y 10.0 %, trimestralmente.

Aunque el 70.0 % de los jóvenes dijo que no comparte su contraseña, los grupos focales mostraron que esto no es tan real. Los jóvenes saben que no es lo más recomendable compartirla; sin embargo, muchos la socializan con padres, amigos y parejas sentimentales, en ese orden.

A esto se agrega el hecho de que más de la mitad (53.5 %) indicó que también ha compartido sus dispositivos electrónicos con familiares y amigos cercanos; solo cuatro de cada diez no lo hacen.

2.3. Datos publicados

Figura 3.
Tipo de información publicada

Fuente: elaboración propia

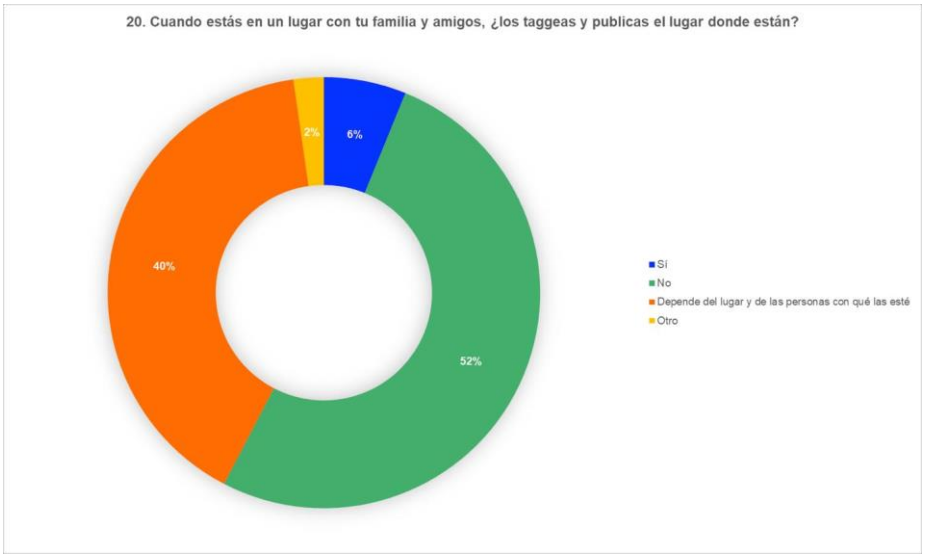
La mayoría, prefiere publicar el nombre, (42 %); lugar de residencia, (35 %); y dónde estudian, (35 %). El número de teléfono y el sitio de trabajo, (3.4 %), es lo que menos aparece en sus redes.

Los jóvenes encuestados, postean información verdadera, dependiendo de la situación y plataforma en la que se encuentren. Dos de cada diez, manifestaron nunca postear datos reales.

A lo anterior, se suman las menciones a amigos o familiares y, según lo encontrado, cuatro de cada diez, *taggea*n a sus contactos y publican su ubicación real.

Figura 4

Tags a cercanos



Fuente: elaboración propia

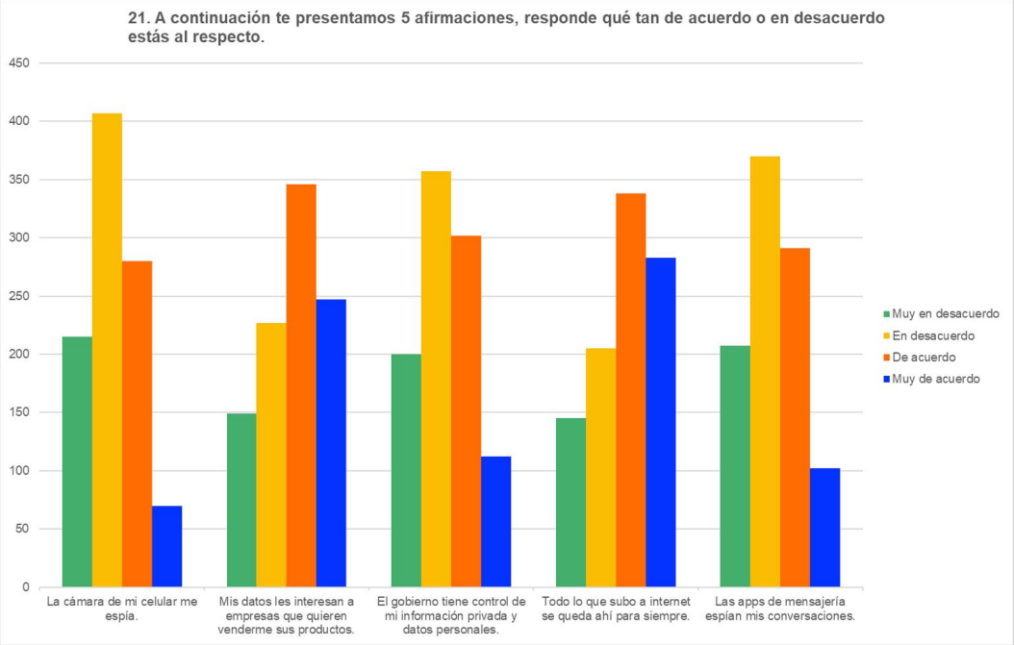
Al conversar con los jóvenes sobre publicar datos en tiempo real, varios mencionaron que esperan llegar a su casa, por razones de seguridad.
En el caso de la información que respaldan, cinco de diez, no lo hacen, ni saben que existen aplicaciones para ello. El resto manifiesta que sí.

2.4 Confianza en la web

En lo que más están en desacuerdo, es en creer que el Gobierno tenga control de su información privada y de sus datos personales. Tampoco creen que el teléfono y las apps de mensajería espíen o les interese sus conversaciones. Esto es un elemento que llama la atención porque la “apropiación” de los datos de los

ciudadanos ha ido in crescendo con el tiempo, (Ricoy Casas, 2018) y las vulneraciones son cotidianas.

Figura 5
Afirmaciones sobre confianza en la web



Fuente elaboración propia

Por otro lado, en lo que están más de acuerdo, es en que sus datos sí les interesan a las empresas que quieren venderles sus productos y también, la mayoría concuerda en que todo lo que se sube a la red, permanece ahí.

4. Discusión de resultados

4.1 Hijos de su tiempo

Los jóvenes salvadoreños, permanecen conectados en un 99 % a internet, con un dispositivo electrónico, un alto porcentaje muy característico de la cultura del siglo XXI, en la que se hace uso de las tecnologías para reemplazar estabilidad y fronteras por movimiento, experiencia por post experiencia, esfuerzo por diversión, profundidad por superficialidad, y colectividad por individualismo de masas (Baricco, 2008). Un mundo cuyos límites con el mundo físico, se han ido diluyendo, al punto que nuestro transitar, de uno al otro, es constante y cada vez menos perceptible.

4.2 Prácticas con deficiencias manifiestas

La mayoría de los jóvenes, utilizan contraseñas con bajos niveles de protección, es decir, el 53.0 %, las prefiere, únicamente, con números y letras. Además, ingresan con las mismas a sus diferentes cuentas.
Con esta práctica, están ignorando las recomendaciones que hacen entes competentes, quienes recomiendan la necesidad de incluir caracteres especiales

y símbolos, así como diferenciar los “password” en los correos, apps y cuentas bancarias.

Este hallazgo pone en evidencia una deficiencia en la dimensión digital ya que existe poco entendimiento del significado, funcionamiento y contexto de los medios para tomar decisiones de seguridad (Ferrés, J., y Piscitelli 2012).

4.2 Dimensión informacional presente de forma parcial

Los resultados encontrados, manifestaron que la competencia informacional (Becerra, et al., 2020), se aplica de forma parcial. Esto quiere decir que, los jóvenes poseen suficiente destreza técnica para acceder, evaluar y comprender aspectos del funcionamiento de dispositivos, pero con ausencia de muchos otros criterios. Esto toma relevancia en un entorno digital, donde los jóvenes manifiestan ser conscientes de la existencia de casos de estafas y robos de identidad como: phishing, malware, pretexting y smishing, que según Sustama (2022) son los más comunes dentro de la ingeniería social.

4.3 Violencia en la red y ciberataques

La violencia es un eje transversal presente en las relaciones mediadas por internet. Los resultados mostraron que existe un grupo considerable que espera llegar a un sitio seguro para poder publicar su ubicación, así como indicar las personas con quién estuvo. Algunos encuestados mencionaron conocer casos de bullying, suplantación de identidad, hackeos, grooming y otros.

4.4 La escuela, un actor indispensable

La mayoría de jóvenes manifestó saber de ciberseguridad a través de tareas o actividades dentro de los centros educativos. Así pues, se reafirma el papel de la escuela como agente constructor de pensamiento entre sus estudiantes.

Conclusiones

La seguridad digital, en clave de Alfabetización Mediática e Informacional, apunta al desarrollo del pensamiento crítico y la ciudadanía activa responsable, y se orienta más que a una instrumentalización de las tecnologías, a una práctica con conciencia contra los diversos ataques de la ingeniería social.

También se concluye, en la necesidad de pensar la seguridad digital en clave de Alfabetización Mediática e Informacional para saber cuestionar, poner distancia y renunciar a la primacía de las emociones en los hábitos de consumo de las audiencias, para salvaguardar la integridad de los usuarios. A la luz de los resultados, esta sigue siendo una materia pendiente, que debe seguirse abordando con plena consciencia de la complejidad del contexto.

Finalmente, el estudio resaltó la necesidad de educar en la comprensión de mensajes, publicidad, fuentes e intereses a las que estos responden. Pueden, además, echar mano de la Alfabetización Mediática e Informacional, tan

necesaria en el camino de la democracia y la justicia. Esto, con el fin de crear espectadores emancipados, como decía Rancière en favor de una educación liberadora; o, como enseñó el maestro Freire: una enseñanza que investiga, porque no hay enseñanza sin investigación, ni investigación sin enseñanza. Todos nosotros, sabemos algo; todos nosotros, ignoramos algo; por eso, aprendemos siempre.

5. Referencias

Acuña, J., Fulchi, L. A., y Sequera, M. (2017). L*a protección de datos personales en bases de datos públicas en Paraguay*. Tecnología y Comunidad. https://www.tedic.org/la-proteccion-de-datos-personales-en-bases-de-datos-publicas-en-paraguay/

Asociación Comunicares (2021). *Presentación de resultados: Desde Nuestra Mirada* [Diapositivas]. https://comunicares.com/archivo/presentacion-ejecutiva-exposicion-de-resultados-desde-nuestra-mirada

Castillejos López, B., Torres Gastelú, C. A., & Lagunes Domínguez, A. (2016). La seguridad en las competencias digitales de los millennials. *Apertura, 8(2), 54-69.*

Fundación Acceso (2019). Observatorio Centroamericano de Seguridad Digital https://www.acceso.or.cr/wp-content/uploads/2021/08/2019-OSD.pdf

Ferrés, J., y Piscitelli, A. (2012). La competencia mediática: Propuesta articulada de dimensiones e indicadores. *Luciérnaga Comunicación, 4(7), 72-79.*

Baricco, A. (2008). *Los bárbaros: ensayo sobre la mutación.* Barcelona: Anagrama, 2008. 254 p. Colección Argumentos.

Conde, J. (2021). Concientización en Ciberseguridad a través de Ataques de Ingeniería Social. *INF-FCPN-PGI Revista PGI*, (7), 62–64. https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/109

Dirección General de Estadística y Censos (DIGESTYC). (2020). Encuesta de Hogares de Propósitos Múltiples 2019.

Durán-Becerra, T., y Lau, J. (2020). MIL Competency Framework: Mapping Media and Information Competencies. *Anagramas: Rumbos y sentidos de la comunicación*, *19*(37), 49-67. https://doi.org/10.22395/angr.v19n37a3

Ferrés, J., y Piscitelli, A. (2012). La competencia mediática: propuesta articulada de dimensiones e indicadores. *Comunicar: Revista científica de comunicación y educación*, *19*(38), 75-81. https://doi.org/10.3916/C38-2012-02-08

Freire, P. (1968):Investigación y metodología de la investigación del tema generado. Santiago, marzo de 1968.

Gallego-Arrufat, M. J., Torres-Hernández, N., y Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. *Comunicar: Revista científica de comunicación y educación*, *27*(61), 57-67. https://doi.org/10.3916/C61-2019-05

Hernández-Sampieri, R., & Mendoza, C. (2020). *Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta*. Mcgraw-hill.

Morse, J. M. (2003). Principles of mixed methods and multimethod research design. In A. Tashakkori & C. Teddlie (Hrsg.), *Handbook of mixed methods in social and behavioural research* (S. 189–208).

Marchal, D. (2019). PSD2: Pagos más seguros a partir de ahora. *Red seguridad: revista especializada en seguridad de la información*, 86, 52-54. https://www.redseguridad.com/revistas/red/086/52/index.html#zoom=z

Patton, M. Q. (2001). *Qualitative research and evaluation and methods* (3a. ed.). Sage.

Rancière, J. (2010). *El espectador emancipado.* Buenos Aires: Bordes Manantial.

Ricoy Casas, R. M. (2018). Algunos ejemplos de espionaje y vulneración de la protección de datos a escala mundial. *Revista de la Escuela Jacobea de Posgrado*,
14, 51-68. https://www.jacobea.edu.mx/revista/numeros/numero14/3.-Rosa-Ricoy-Casas-Ejemplos-Espionaje-Vulneracion.pdf

Sustama, M.(2022). Análisis de las técnicas más usadas en la ingeniería social,*Universidad Piloto de Colombia.* http://repository.unipiloto.edu.co/handle/20.500.12277/12497

Tashakkori, A., Teddlie, C. *Mixed methodology: Combining qualitative and quantitative approaches* Thousand Oaks: Sage.

Unesco. (2011a). *Alfabetización Mediática e Informacional: Curriculum para Profesores*. Unesco. https://unesdoc.unesco.org/ark:/48223/pf0000216099