REALIDAD
Revista de Ciencias Sociales y Humanidades

Revista Realidad No. 166, Julio-Diciembre de 2025, pp. 144-158.
URL: https://revistas.uca.edu.sv/index.php/realidad
DOI: https://doi.org/ 10.51378/realidad.vi166.9781
e-ISSN: 2520-0526 / ISSN: 1991-3516

# Otro extraño en la sombra: Un acercamiento a las características del cibercriminal

## *Another Stranger in the Shadows: An Approach to the Characteristics of the Cybercriminal*

**Carlos Iván Orellana**[1]
Universidad Centroamericana José Simeón Cañas
El Salvador
corellana@uca.edu.sv
ORCID: https://orcid.org/0000-0002-4936-867X

**Adilio Carrillo**[2]
Universidad Centroamericana José Simeón Cañas
El Salvador
acarrillo@uca.edu.sv
ORCID: https://orcid.org/0000-0002-1956-1137
Fecha de recepción: 28 de octubre de 2024
Fecha de aceptación: 20 de febrero de 2025

**Resumen:** A pesar del auge del cibercrimen aún se desconoce mucho de la experiencia social y las manifestaciones de esta forma de inseguridad, especialmente, las características del perpetrador. Con el empleo de un cuestionario en línea llenado por 315 adultos salvadoreños, se encontró que existen situaciones de victimización junto a una percepción de incremento del cibercrimen. Además, un diferencial semántico mostró que la representación del cibercriminal adopta tendencialmente características como ser una persona sofisticada, con alta escolaridad, de clase alta o, de manera relevante, no pertenecer a pandillas. De esta manera, mientras que se argumenta que en el país existen condiciones cibercriminógenas –en buena medida instigadas por el gobierno de turno– esta investigación ofrece pistas de que la representación del cibercriminal se aparta de la del pandillero, la figura criminal emblemática nacional de los últimos 35 años. El cibercriminal encontraría ya su lugar propio como un nuevo extraño sombrío en el imaginario salvadoreño.

**Palabras clave:** crimen, perpetrador, inseguridad ciudadana, violencia, representación

***Abstract:*** *Despite the rise of cybercrime, many aspects remain unknown about the social experience and manifestations of this form of insecurity, especially the characteristics of the perpetrator. Using an online questionnaire filled out by 315 Salvadoran adults, cases of victimization and a perception of increased cybercrime were found. In addition, a semantic differential showed that the representation of the cybercriminal tends to adopt characteristics such as being a*

1 Doctor en Ciencias Sociales. Profesor e investigador del Departamento de Psicología y Salud Pública y director de la Maestría en Intervención Social de la Universidad Centroamericana José Simeón Cañas (UCA).

2 Maestro en Ciencia Política, con estudios en Seguridad y Desarrollo Nacional por el Colegio de Altos Estudios Estratégicos de la Fuerza Armada de El Salvador (FAES). Profesor e investigador del Departamento de Sociología y Ciencias Políticas de la Universidad Centroamericana José Simeón Cañas (UCA).

*sophisticated person, with high schooling, upper class, or, relevantly, not belonging to gangs. Thus, while it is argued that cybercriminogenic conditions exist in the country –largely instigated by the government in power– this research offers cues that the representation of the cybercriminal takes distance from the gang member´s, the national emblematic criminal figure of the past 35 years. The cybercriminal has now found his own place as a new shadowy stranger in the Salvadoran imaginary.*

***Keywords:*** *crime, offender, citizen insecurity, violence, representation*

## 1. Introducción

El cibercrimen constituye una realidad global cuyas manifestaciones afectan a gobiernos, empresas, organizaciones y personas particulares. Se considera un fenómeno cuyo crecimiento e impacto sobrepasa ya el provocado por el crimen convencional, que se entrecruza con el crimen organizado, mientras se potencia en sociedades en las que predominan altos niveles de precariedad e inseguridad ciudadana (Oficina de las Naciones Unidas contra la Droga y el Delito [UNODC], 2013, 2022; World Economic Forum, 2022). Tales condiciones retratan el caso de países como El Salvador, en el que coexisten añejas y profundas vulnerabilidades socioeconómicas –exclusión, informalidad laboral, bajos salarios, brechas digitales y de género– con condiciones criminales cambiantes, violencia cotidiana, corrupción y graves violaciones a derechos humanos (Cristosal, 2024; Departamento de Economía de la Universidad Centroamericana José Simeón Cañas, 2022; Fundación de Estudios para la Aplicación del Derecho [FESPAD], 2021).

La irrupción de la pandemia a finales de 2019 complejizó los problemas aludidos alrededor del mundo, pero con especial resonancia en países en vías de desarrollo. La emergencia sanitaria propició la digitalización acelerada de las sociedades (educación, comercio, vínculos, etc.), proceso que arrojó a las personas a nuevos riesgos y vulnerabilidades, entre las que destaca la inseguridad en y desde el ciberespacio (Mahadevan, 2020; World Economic Forum, 2022). La pandemia agudizó la fragilidad socioeconómica y trajo consigo mutaciones criminógenas favorables para el ejercicio de la violencia y, de manera notable, la violencia contra las mujeres (International Crisis Group, 2020; ONU Mujeres, 2021). Asimismo, a esta circunstancia de crisis socioeconómica y sanitaria se sumó otra de corte político, al constatarse el retroceso de la democracia en varios países del mundo (United Nations Development Programme [UNDP], 2024).

Precisamente, desde 2019, El Salvador viene experimentando un proceso de deterioro democrático que se ha cristalizado en un régimen autocrático (Nord *et al.*, 2024). Estas condiciones, además de las persecuciones a opositores, militarización y restricción de derechos humanos que estos procesos regresivos conllevan, también han propiciado un caldo de cultivo favorable para la cibercriminalidad. En poco menos de un quinquenio en el poder, el nuevo gobierno se ha caracterizado por el empleo masivo de las redes sociales para comunicarse, activamente hacer propaganda e intentar manipular a la población (Kinosian, 2022); autorizó una criptomoneda –el Bitcoin– como "moneda" de curso legal y promovió el uso de una *wallet* gubernamental –la Chivo Wallet– a través de un incentivo económico cuya implementación estuvo marcada por numerosas irregularidades y estafas (Alvarado, 2022); ha incurrido en espionaje cibernético de periodistas y activistas considerados como opositores (Gavarrete, 2022); llevó a cabo negociaciones con las pandillas mientras que, con el pretexto de combatirlas, ha mantenido vigente un régimen de excepción por más de dos años y medio que ha vulnerado derechos y libertades ciudadanas (Cristosal, 2024; International Crisis Group, 2022; Instituto Universitario de Opinión Pública [IUDOP], 2022). El freno súbito de las pandillas, uno de los principales factores criminógenos de los últimos 30 años, a través de llenar las calles con policías y soldados, detiene el cometimiento de sus crímenes, pero también propende a la adaptación de la criminalidad hacia opciones más sofisticadas, ajenas a las calles, como las que pueden darse en el ciberespacio.

Las condiciones descritas bosquejan un contexto socioeconómico, político y digital efervescente. En Latinoamérica, los cibercrímenes han subido como la espuma (Diazgranados, 2021). Por lo apuntado anteriormente, esta modalidad de inseguridad se encuentra igualmente en auge en El Salvador. En 2021, en vinculación con la implementación del Bitcoin y la Chivo Wallet, se habría producido un incremento del 700% en la incidencia de los cibercrímenes hasta contabilizar 9,790 delitos informáticos en el país, según las autoridades de seguridad. Las autoridades, por cierto, han declarado reserva sobre las cifras de delitos informáticos desde 2022, mientras parecen resultar inermes ante el embate de esta forma de criminalidad (Bernal, 2024a). Así lo demuestra la vulneración nada menos que de los sistemas de seguridad de ejércitos y corporaciones policiales de varios países latinoamericanos, incluyendo los de El Salvador, por parte de un grupo de hackers autodenominado "Guacamaya", acaecida en 2021 (Bernal, 2022) y, más recientemente, el hurto y filtración de bases de datos con información personal de ciudadanos, así como de correos de la Policía Nacional Civil (PNC) y la Fuerza Armada de El Salvador (FAES) (Bernal, 2024b).

Quiere decir que, mientras la ciberseguridad constituye una preocupación para gobiernos, empresas y sistemas, la cibercriminalidad o los delitos cibernéticos constituyen, además, una inquietud especial para el ciudadano de a pie. Hoy en día, dada la conexión permanente de las personas ciudadanas, estas se ven constantemente expuestas a llegar a ser victimizadas en un medio técnicamente complejo como el de las redes. En Estados Unidos el miedo a ser víctima de un ciberdelito ya supera el temor a ser víctima de un acto delincuencial convencional (Brenan, 2018).

Tanto la incidencia de los delitos informáticos como el temor a los mismos ya se detecta en países centroamericanos y del caribe, incluyendo El Salvador. Vargas y Vargas (2023), a partir de una muestra no representativa de 3000 personas de 18 años o más provenientes de Guatemala, Honduras, El Salvador, Costa Rica y República Dominicana, encontraron que los cibercrímenes más prevalentes en la región son el ciberacoso, *malware*, hackeo de email, hackeo de redes y *ransomware*[3]. Asimismo, que esta forma de criminalidad acaece especialmente en las zonas urbanas más que en las rurales, que se reporta polivictimización y que destacan mayoritariamente como víctimas los individuos con edades entre 18 y 24 años –los considerados "nativos digitales"– y adultos jóvenes con edades arriba de 24 y hasta 34 años. En lo que concierne al caso salvadoreño, durante las elecciones internas previas a los eventos electorales de 2024, se consignaron altos niveles de violencia hacia mujeres activas en política. En cuatro meses de elecciones internas de los partidos políticos en contienda se produjeron más de 52,000 ataques a personas políticas a través de las redes sociales X (entonces Twitter) y de Facebook, siendo el 63% de estos dirigidos contra mujeres políticas (Asociación Nacional de Regidoras, Síndicas y Alcaldesas Salvadoreñas [ANDRYSAS], 2024).

Por su lado, Orellana y Carrillo (2023) identificaron la existencia de altos niveles de miedo al cibercrimen en una muestra de personas adultas salvadoreñas. Estos autores constatan que el miedo es más alto en la medida en que la persona es mujer, tiene menos de 25 años, estudia y trabaja, si conoce a víctimas de delincuencia y de ciberdelincuencia y si cree que el cibercrimen ha aumentado. En esta investigación, el miedo al delito convencional constituyó, entre otros, el principal predictor estadístico del miedo al cibercrimen y se identificaron dos dimensiones de miedo al cibercrimen: el ciberfraude y la invasión a la intimidad. En este último, compuesto por cibercrímenes como el acoso sexual, personal y laboral, extorsión con información o imágenes personales y espionaje, el género –siempre ser mujer– constituyó un factor predictor relevante.

El cibercrimen se ve fortalecido por la confluencia de distintos factores posibilitadores –adicionales a la peculiaridad local de los ya mencionados propiciados por el gobierno de turno–, como la existencia de altos niveles de crimen convencional, las brechas digitales, y debido a

3 Ver las definiciones de estos cibercrímenes en Vargas y Vargas (2023, pp. 15-17).

las adaptaciones que los criminales comunes y los mismos cibercriminales habrían realizado antes y debido a la digitalización forzosa y acelerada impelida por la pandemia (Carbajal, 2022; Miró Llinares, 2021; UNODC, 2013). A pesar del escenario descrito, los estudios de opinión y las investigaciones en el país, continúan escudriñando exclusivamente la inseguridad que acaece en el mundo "físico" o fuera de línea, en el barrio, y en la que operan perpetradores de manera directa. De esta manera incurren en la "falacia de la desconexión" (Orellana y Carrillo, 2023, p. 32), es decir, que parten de una perspectiva pre-digital sobre la violencia criminal según la cual el ciudadano común se encuentra desconectado de la red y por tanto solo expuesto a criminalidad convencional.

### 1.1. El cibercriminal como extraño

Por todo lo expuesto, no debe extrañar que la literatura disponible ya consigne algunas características *reales* o usuales del cibercriminal, tales como ser un hombre, usualmente atravesando la adultez joven (20-40 años) (Cámara Arroyo, 2020; López Gutiérrez *et al.*, 2022; Lee, 2007). De manera llamativa, Vargas y Vargas (2023) identificaron que, de la muestra de 3000 personas centroamericanas y del caribe que participaron en su estudio, 1,213 –40%– fue víctima de al menos un ciberdelito, la mayoría provenía del triángulo norte, y de esta cantidad, aproximadamente un 20% conocía al victimario (en ese momento era un amigo, pareja o trabajaban juntos).

Entre todas estas características posibles, destaca la pericia técnica. Tal como documenta Cámara Arroyo (2020), la clasificación del perfil de un cibercriminal puede ser amplia, compleja y hasta responder a idiosincrasias subculturales (*Cyberpunks*, *White Hat Hackers,* entre muchos otros). No obstante, se puede decir que el atributo pericial permite distinguir cibercriminales especializados –este sería el caso de los *hackers* de todo tipo– y cibercriminales no especializados. Entre estos últimos existiría una panoplia de individuos en búsqueda de réditos –prestigio, entretención, imágenes o dinero– a través de sus más o menos variados, aunque rudimentarios conocimientos informáticos.

Nos es difícil suponer que la atribución de sofisticación personal ligada a la competencia técnico-informática constituyen las condiciones *sine qua non* de la representación social de un cibercriminal. No obstante, no se puede afirmar que estos sean rasgos uniformes y menos que los mismos agoten el perfil construido de un ciberdelincuente. Algo similar se puede decir del género. Por ejemplo, en el ámbito escolar, con los recursos que puede disponer a su edad una adolescente, aunque se mantiene la tendencia mayoritariamente masculina en la perpetración de distintas formas de *ciberbullying*, igualmente las jóvenes incurren en este comportamiento usualmente a través de formas de indirectas de acoso (Morales-Arjona *et al.*, 2020; Romo-Tobón *et al.*, 2020), y en el mismo contexto salvadoreño, algunas estafas en línea han sido llevadas a cabo por mujeres con conocimientos de redes sociales bastante elementales (Ayala, 2024; Marroquín, 2023).

Quiere decir que la figura de un cibercriminal dista de presentar contornos definidos, especialmente en condiciones en las que igualmente hace falta protegerse e imaginar criminales de carne y hueso. La decidida presencia del cibercrimen como amenaza a la seguridad personal en la sociedad salvadoreña actual hace presuponer que esta convive con representaciones académicas y populares de criminales ajenos al mundo digital. Porque, en la galería histórica nacional de parias y delincuentes –indígenas, comunistas, vagos, guerrilleros, corruptos, entre otros–, existe un profundo enraizamiento de preconcepciones "fuertes", físicas o corporizadas que, de forma dominante y quizás debido a las dinámicas sociales del último cuarto de siglo, terminaron encontrando rápidamente en la figura del pandillero su particular representación frecuente (Martel Trigueros, 2006). Pero ahora, la figura novedosa, pero "etérea", mediáticamente construida, carente de un retrato robot preciso y hasta contraintuitiva del cibercriminal (es decir, joven, capaz de victimizar simultáneamente a muchos) encontraría dificultades

representacionales. Así parece confirmarse de manera implícita al constatar que la literatura que analiza al cibercriminal, si acaso, suele subsumirlo bajo la categoría difusa de "delincuente motivado" (*motivated offender*), uno de los eslabones de la Teoría de Actividades Rutinarias (o RAT, por sus siglás en inglés, *Routine Activity Theory*) que se emplea con mucha frecuencia para estudiar el cibercrimen (Henson *et al.*, 2016; Orellana y Carrillo, 2023).

Con bastante seguridad, este proceso de mutación en los imaginarios criminógenos no es exclusivo de El Salvador. Sin embargo, dada la añeja historia de violencia en este pequeño país centroamericano, es posible verificar este proceso. Algo similar habría ocurrido en la posguerra salvadoreña de la década de 1990 cuando, progresivamente, la figura del "guerrillero" o las acciones de guerra, como los "enfrentamientos" o las "masacres" de la década previa, fueron dando paso al surgimiento de actores violentos sin rostro ni emblemas visibles, cuyas motivaciones políticas gradualmente se hibridaron para transitar después hacia otras de corte pecuniario. Una de las consecuencias de dicha mutación fue, precisamente, el agotamiento, la resistencia y la insuficiencia del lenguaje y las representaciones disponibles para perfilar con precisión a los nuevos actores violentos emergentes ajenos al escenario de la guerra (Orellana, 2022a, 2022b; Orellana y Santacruz Giralt, 2022).

El cibercriminal parece encarnar en la actualidad la figura del "extraño" definitivo, el extraño por antonomasia. Según Lee (2007, p. 6), "*the shadowy stranger"*, el extraño sombrío, remite a la figura difusa del otro-criminal en cierto tiempo y espacio caracterizado por un accionar inesperado e impredecible al elegir a sus víctimas. Ante la carencia de una corporeización precisa, el extraño en la sombra constituye el fermento de temores racionales e irracionales, de estereotipos y el objeto de asignación azarosa de peligrosidad. De esta manera los temores colectivos atizados, en el barrio, las noticias o en el habla cotidiana, dialécticamente, construyen en la calle, pero también la red, tanto a un individuo amedrentador como a un individuo amedrentado.

Utilizando la reflexión de Rundell (2014, pp. 14-16), se puede afirmar que el ciberespacio constituye la nueva "ciudad" en la que se aglomeran extraños y, con ello, nuevos imaginarios y "economías emocionales", particularmente las relativas a la ansiedad y el miedo. El ciberespacio es el nuevo lugar no-familiar. Un lugar, un ámbito, una esfera ambigua que ofrece libertad y temores, configurado con pasadizos, callejones oscuros y vínculos impersonales en el que las oportunidades, legales e ilegales, se multiplican. Un lugar lleno de "extraños contingentes" que viven un eterno presente fugaz y que, como las figuras del extranjero o el extraño de Simmel (2014), constituyen formas ambiguas, próximas y lejanas, abstractas y concretas, a la vez.

La figura del extraño como actor criminal parece exhibir todo su potencial amenazante e impredecible especialmente en la experiencia amplificada de temor al delito de las mujeres ante la posibilidad adicional de daño físico o sexual (Hirtenlehner y Farrall, 2014; Scott, 2003; Wilcox *et al.*, 2006). Cabe suponer que el cibercriminal, en cuanto extraño por excelencia, cuenta con la capacidad –imaginada o real– de intensificar o enmascarar miedos potenciales a distintas formas de menoscabo, lo cual sería más cierto en el caso de personas vulnerables (Bocij y McFarlane, 2003; Grinshteyn *et al.*, 2021).

El carácter representacional borroso del ciberdelincuente puede llevar a pensar que es imposible trazar un perfil definido que lo caracterice. Ocurre, no obstante, que la necesidad de un perfil preciso es una aspiración criminológica o penal cuando, desde un punto de vista sociológico y psicosocial, como del que parte este trabajo, lo relevante es la construcción social y la existencia objetiva de tales creencias, la atribución de rasgos o preconcepciones, así como las fuentes y posibles consecuencias de dichos procesos. La relevancia social de una amenaza para una sociedad dada radica en la creencia de su mera existencia, con independencia de que esta constituya o no una realidad objetiva.

Considerando las reflexiones previas y situados en una sociedad en el que proliferan "muchos otros", parias y extraños amenazantes, el objetivo general de este trabajo es explorar las características que una muestra de personas adultas salvadoreñas atribuye a un cibercriminal.

## 2. Método

### 2.1. Participantes

La muestra participante fue obtenida a partir de un muestreo no probabilístico propositivo, es decir, atendiendo a procesos oportunistas de selección, pero con base en características precisas de interés (Clark-Carter, 2002), en este caso, salvadoreños y salvadoreñas con 18 años o más que residían en el país durante el desarrollo de la investigación. La muestra final estuvo compuesta por 315 personas cuyo promedio de edad no supera los 30 años ($M$ = 27.5, $DE$ = 10.2). Casi 6 de cada 10 participantes (58%) se identificó como del sexo femenino mientras el restante 42% como del sexo masculino. La gran mayoría de los participantes dijeron dedicarse principalmente a estudiar (42%) o estudiar y trabajar (31%), 24% solo trabaja y el restante 3% señaló otra situación ocupacional (oficios del hogar, jubilación, desempleo, etc.).

### 2.2. Instrumento

Se desarrolló una investigación transversal con una encuesta en línea (Stockemer, 2019). Como datos de identificación en el cuestionario elaborado se incluyeron los datos sociodemográficos apuntados (sexo, edad y ocupación) pero también opiniones sobre victimización y percepciones sobre el posible agravamiento del delito común y del cibercrimen. En concreto se incluyeron cuatro preguntas con enunciados similares: dos sobre victimización por delito convencional y dos referidas a victimización por ciberdelito: "¿Ha sido usted víctima de alguna forma de ciberdelito/algún hecho delincuencial en los últimos doce meses?" y "¿conoce usted a algún familiar o amigo que haya sido víctima de algún ciberdelito/algún hecho delincuencial en los últimos doce meses? En ambos casos las opciones de respuesta fueron dicotómicas (1 = Sí, 0 = No). Asimismo, se incluyeron dos preguntas sobre percepción de agravamiento, una sobre delito común y otra sobre cibercrimen, cuyos enunciados rezaban así: "en su opinión, ¿el problema de la delincuencia común en el país ha aumentado o ha disminuido en el último año?" y "en su opinión, ¿el problema de la ciberdelincuencia en el país ha aumentado o ha disminuido en el último año?". Para ambas preguntas existían tres opciones de respuesta, 3 = "Ha aumentado", 2 = "Sigue igual" y 1 = "Ha disminuido".

Asimismo, para explorar las características atribuidas al cibercriminal se construyó un diferencial semántico (Osgood, 1952; Stockemer, 2019). Esta es una variante de escala de medición propia de investigación por encuestas conformada por preguntas cerradas con dos alternativas bipolares sobre –en este caso– posibles características del cibercriminal. Quien responde debía puntuar tales características en una escala de 1-5 puntos según el significado o peso atribuido a cada opción de respuesta. El valor escogido ofrece información connotativa o actitudinal antes que sumativa y persigue capturar representaciones, no así una asignación de puntaje particular. Por ejemplo, si 80% de la muestra elige la opción Hombre = 1 y 20% la opción Mujer = 5, esto indicaría que el cibercriminal es mayoritariamente representado como un hombre y no que ocho de cada 10 personas de la muestra asignan un bajo puntaje al ítem.

El diferencial semántico empleado estuvo compuesto por 11 díadas cuyo extremo izquierdo siempre mostraba el valor de 1 y su extremo derecho el valor de 5. Las alternativas bipolares presentadas fueron las siguientes: 1) Hombre/Mujer, 2) Heterosexual/LGBTI, 3) Joven/Adulto, 4) De clase baja/De clase alta, 5) Pertenece a pandillas/No pertenece a pandillas, 6) Opera en grupo/Opera solo, 7) También es delincuente común/Solo es ciberdelincuente, 8) Tiene baja escolaridad/Tiene alta escolaridad, 9) Es una persona común y corriente/Es una persona sofisticada, 10)

Persigue fines principalmente económicos/Persigue fines principalmente políticos, 11) Pertenece al mundo del crimen común/Pertenece al mundo del crimen organizado.

Para explorar algunas características métricas del diferencial semántico construido se realizó un Análisis Factorial Exploratorio (AFE). Como se aprecia en la tabla 1, los ítems del diferencial semántico se aglutinan en 3 factores[4] bastante equilibrados al explicar cada uno alrededor de un tercio del 50.2% de la varianza total de los resultados. El primer factor aglutina cuatro pares de adjetivos, los referidos a escolaridad, clase social, tipo de criminalidad y refinamiento personal, por lo que fue denominado como "sofisticación delictiva". El segundo factor incluyó otros cuatro pares de adjetivos, los referidos al género, la orientación sexual, los fines que se persiguen y la edad, lo que condujo a etiquetar este factor como "demografía cibercriminal". Finalmente, el tercer factor mostró los restantes pares de grupalidad-individualidad, pertenencia a pandillas y modalidad de operación por lo que fue denominado como "diversificación criminal".

**Tabla 1**
*Ítems y matriz factorial de los adjetivos opuestos que componen el diferencial semántico*

| Pares de adjetivos | F1 | F2 | F3 |
|---|---|---|---|
| Baja escolaridad/Alta escolaridad | .728 | | |
| De clase baja/De clase alta | .629 | | |
| Crimen común/Crimen organizado | .611 | | |
| Persona común y corriente/Persona sofisticada | .586 | | |
| Hombre/Mujer | | .774 | |
| Heterosexual/LGBTI | | .756 | |
| Fines principalmente económicos/Fines Políticos | | .425 | |
| Joven/Adulto | | .404 | |
| También delincuente común/Solo es Ciberdelincuente | | | .781 |
| Pandillas/No pandillas | | | .663 |
| Opera en grupo/Opera solo | | | .511 |
| Autovalor | 2.668 | 1.594 | 1.258 |
| Porcentaje de varianza explicada posterior a la rotación | 18.446 | 16.845 | 14.893 |
| Porcentaje de varianza acumulada posterior a la rotación | 18.446 | 35.291 | 50.184 |

*Nota*. Elaboración propia. El AFE recurrió a una rotación Varimax y su ejecución comprobó el cumplimiento de los supuestos para llevar a cabo el análisis (KMO = .699; P. esfericidad de Bartlett: p < .001).

El análisis factorial permite exponer la estructura subyacente de un constructo. Los tres factores identificados –sofisticación criminal, demografía cibercriminal y diversificación delictiva– sugieren que el diferencial semántico construido retrata la figura de un perpetrador, el cibercriminal, por supuesto, pero resaltando el carácter innovador de este criminal.

## 2.3. Procedimiento

Los datos que se exponen en este artículo fueron tomados de una encuesta en línea titulada "Inseguridad ciudadana y cibercrimen" que fue administrada entre mayo y julio de 2022. El proceso

4 La solución inicial del AFE extrajo cuatro factores, pero dos ítems mostraron cargas cruzadas muy similares entre factores distintos (lo que se presta a interpretaciones ambiguas) mientras aparecían factores desbalanceados, uno conformado por solo dos ítems y otro por cinco ítems. En búsqueda de una estructura factorial más equilibrada, cohesionada y legible, y atendiendo a los resultados iniciales del análisis, se decidió replicar el AFE solicitando específicamente tres factores.

de recolección de datos inició distribuyendo por correo electrónico las instrucciones y el enlace de la encuesta a contactos de los investigadores. Al inicio de las instrucciones del cuestionario se incluyó una pregunta de consentimiento informado que exponía los fines de la investigación y las características de la tarea por realizar. Asimismo, las instrucciones especificaban la participación de los destinatarios del correo siempre y cuando cumplieran con los criterios de inclusión establecidos (personas salvadoreñas de 18 años o más) y se solicitaba el reenvío del cuestionario a otras personas (p. ej., bola de nieve). Además, en las consignas se hicieron explícitos aspectos éticos importantes como el anonimato, el uso exclusivo de los datos con fines académicos y la libertad de abandonar la encuesta en cualquier momento. Al final solo un participante declinó participar en la pregunta de consentimiento. Además de las preguntas expuestas en el apartado de instrumentos, los pares de adjetivos del diferencial semántico se vieron precedidos de la pregunta única "¿Cómo describiría a un ciberdelincuente?" El cuestionario fue construido con la herramienta *Google Forms* y los análisis fueron llevados a cabo con el programa SPSS v. 25. Para el desarrollo de esta investigación no se contó con ninguna tecnología asistida por inteligencia artificial (IA).

## 3. Resultados

Los resultados se dividen en dos partes. Primero se exponen las proporciones de victimización directa y el conocimiento de la victimización de otros (victimización vicaria) por delincuencia común y cibercrimen reportada por los participantes, así como la percepción de evolución de ambos tipos de criminalidad. En segundo lugar, se expone la proporción de personas que se inclina por cada par de adjetivos consignados en el diferencial semántico, lo que permitirá identificar el perfil general que se dibuja del cibercriminal a partir de la opinión mayoritaria de la muestra.

### 3.1. Victimización directa, victimización vicaria y percepción de cambio de la criminalidad

Respecto a la victimización por delincuencia común y ciberdelincuencia reportada por los participantes en el estudio, los resultados evidencian que el porcentaje de victimización por cibercriminalidad es apenas superior (20%) al que se reporta de victimización por delincuencia convencional (16%), y que 51% y 65% dijo, respectivamente, conocer a un familiar o amigo que fue víctima de algún cibercrimen o de delincuencia común.

Sobre la percepción de agravamiento de la criminalidad, se encontró que una tercera parte de la muestra afirmó que la delincuencia ha aumentado, así como que la ciberdelincuencia ha disminuido o se ha mantenido invariable, mientras que el 67% y el 64% de los participantes expresaron, de manera respectiva, que la delincuencia ha decrecido o se ha mantenido igual pero que la cibercriminalidad ha aumentado en el último año.

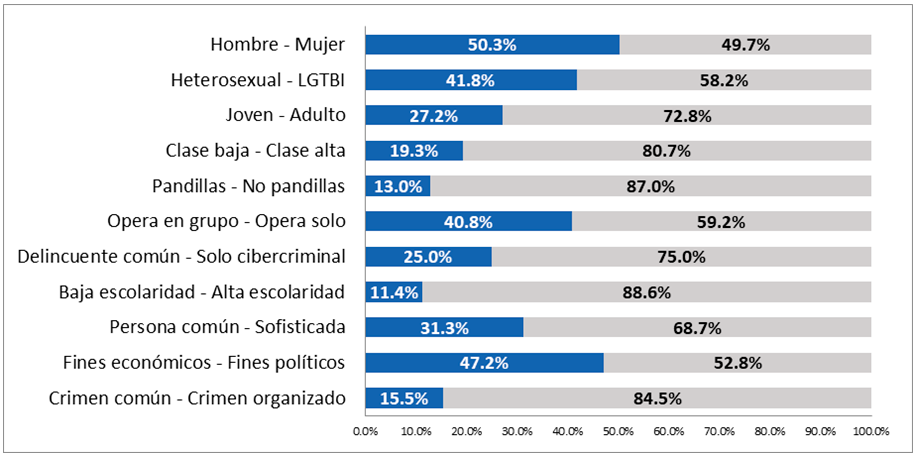
En suma, según la experiencia de los participantes, la victimización directa por delincuencia y ciberdelincuencia es parecida; la victimización vicaria es alta en ambos casos, especialmente la delincuencia común, pero, no obstante, esta última no habría cambiado o habría disminuido en el último año, en contraste con la cibercriminalidad, cuya percepción mayoritaria es que manifiesta una tendencia alcista.

### 3.2. El perfil atribuido al cibercriminal

Para determinar el rasgo dominante seleccionado de cada díada presentada en la encuesta, cada ítem fue dividido en dos a partir de su punto medio. Es decir, de los cinco puntos de la escala de respuesta, los puntajes menores o iguales a 2.5 fueron adjudicados al polo izquierdo de cada ítem del diferencial semántico y los valores superiores a 2.5, al polo derecho. La distribución porcentual, y con ello, la atribución tendencial de rasgos al cibercriminal se puede apreciar en la figura 1.

**Figura 1**

*Proporciones de respuesta distribuidos en los polos de cada par de adjetivos del diferencial semántico*




*Nota*. Elaboración propia

La distribución de las respuestas, atendiendo a los datos de la gráfica 1, evidencian que, para los participantes en el estudio, el cibercriminal tendría un perfil tendencialmente caracterizado por alejarse de la heterosexualidad, situarse en la adultez, pertenecer a la clase alta, no pertenecer a pandillas, operar en soledad, solo dedicarse a la ciberdelincuencia, tener alta escolaridad, ser una persona sofisticada y vincularse al mundo del crimen organizado. Menos definitivas son las atribuciones de género y de los fines perseguidos, pues las respuestas se aglutinan cerca del punto medio y, respectivamente, apenas en favor de que el cibercriminal sería un hombre cuyos fines perseguidos son primordialmente políticos.

## 4. Discusión

Mientras se escriben estas líneas, las redes sociales ebullen con la filtración de una base de datos del Instituto Salvadoreño del Seguro Social con datos personales de algo más de 974 mil personas salvadoreñas, llevada a cabo por un grupo de hackers –CiberinteligenciaSV–, en principio, para exponer los sueldos desconocidos de funcionario de gobierno y sus colaboradores (Bernal, 2024c). El cibercrimen constituye ya una realidad innegable, en constante crecimiento, diversificación y complejización en El Salvador (Alvarado, 2022; Bernal, 2024a, 2024b).

Con el establecimiento de una caracterización general del cibercriminal por parte de la muestra participante, se accede a una aproximación objetivizada de la figura del perpetrador que refuerza la existencia de esta forma de criminalidad en la vida cotidiana de personas salvadoreñas comunes. De esta manera, además de dar cumplimiento al objetivo general trazado para la investigación, este trabajo se suma a otros recientes que vienen mostrando indicios de esta criminalidad y sus consecuencias en el país y en el ámbito regional (Orellana y Carrillo, 2023; Vargas y Vargas, 2023).

Los resultados obtenidos muestran la existencia de victimización directa y vicaria por cibercrimen, así como la percepción de aumento de éste. La manifestación específica de cibercrímenes, en cuanto que efecto concreto, ofrece una confirmación de la existencia de un contexto cibercriminógeno. Este se habría visto propiciado por factores exógenos globales como la digitalización acelerada de las sociedades (agudizadas por la pandemia). Pero también endógenos, como la existencia de inseguridad ciudadana objetiva y subjetiva, brechas digitales, la implementación gubernamental de medidas que se cristalizan o instigan acciones ilegales en

la red (como espionaje, estafas, hackeos) o la represión intensa contra el crimen en las calles que, presumiblemente, coadyuva a la mutación hacia estrategias criminales intramuros, como las que facilita internet (FESPAD, 2021; Miró Llinares, 2021; UNODC, 2013).

De hecho, los tres factores en que se aglutinan los ítems del diferencial semántico –sofisticación criminal, demografía cibercriminal y diversificación delictiva–, además de la connotación general de innovación que parecen ofrecer sobre el cibercriminal, más de fondo, recogen en conjunto la tensión entre cambio y estabilidad de la figura de este en contraposición a otros más familiares y con características muy definidas en el contexto salvadoreño, como ha ocurrido, típicamente, con los miembros de pandillas en las últimas décadas. La investigación, por tanto, al encontrar que el cibercriminal es caracterizado con rasgos muy divergentes y hasta opuestos a los del miembro de pandilla promedio, constata la existencia de indicios de que, en el imaginario de parte de la sociedad salvadoreña, el cibercriminal es una nueva figura criminal, un nuevo perpetrador, un nuevo extraño para la galería de parias que ha conocido el país a lo largo de su historia.

Algunas características predominantes asignadas al cibercriminal por los participantes en el estudio son coincidentes con la que recogen otros trabajos (Cámara Arroyo, 2020; López Gutiérrez *et al.*, 2022), como que se trata de hombres, situados en la adultez joven, que manifiestan atributos de sofisticación o alto nivel educativo. No obstante, como un correlato del contexto precario que constituye el país, aquí no necesariamente se cumple que el ciberdelincuente sea hombre o que tenga conocimientos especializados, todo lo contrario (por ejemplo, mujeres que cometen estafas en Facebook; Ayala, 2024; Marroquín, 2023). Otras características predominantes atribuidas –pertenecer al crimen organizado, no pertenecer a pandillas, dedicación exclusiva a la cibercriminalidad–, estarían reflejando, presumiblemente, imaginarios sociales sobre el cibercriminal como fruto entreverado de experiencias reales y vicarias, suposiciones, así como caracterizaciones de las que ahora abundan en películas y las redes sociales.

Aunque no se puede descartar el peso de factores como los productos culturales como series o películas en la elaboración de un retrato imaginado y hasta fantasioso del cibercriminal, sería un error ignorar las pistas del sentido social que dicha construcción encierra. Situados en la peculiar sociedad salvadoreña, el cibercriminal imaginado cobra sentido considerando la violencia pandilleril de décadas y, ahora, el clima de incertidumbre –extrañeza– signada por exabruptos cibercriminógenos varios, como estafas, espionaje, manipulación, hackeos masivos y hasta atisbos de violencia política a través de las redes (ANDRYSAS, 2024; Bernal, 2024b, Gavarrete, 2022; Kinosian, 2022). El vacío de conocimiento igualmente se llena con una representación. Como nos recuerdan Vargas y Vargas, en el istmo centroamericano y el Caribe se carece de "perfiles de las víctimas y agresores de ciberdelitos y violencia digital, para el análisis del fenómeno criminal" (Vargas y Vargas, 2023, p. 71).

Por ejemplo, como ha sido apuntado, primero, para los participantes en la investigación, el cibercriminal no es un miembro de pandillas: un cambio en el perpetrador lleva a seguir la intuición social implícita de la existencia de condiciones criminógenas novedosas o que al menos coexisten con las que propician el crimen convencional[5]. En segundo lugar, se cree –de manera más titubeante– que este perpetrador se escora hacia los fines políticos (pero no menos hacia fines económicos), ser un hombre (pero podría ser mujer), operar en soledad (pero podría hacerlo en grupo) y, llamativamente, ser una persona LGBTI (lo que tampoco descarta que sea heterosexual)[6]. Aunque las respuestas obtenidas se ven marcadas por idiosincrasias de la muestra participante, como una confirmación del carácter difuso e inasible que la ciberinseguridad ciudadana conlleva, pero en coherencia con el contexto salvadoreño actual –opaco, "bajo reserva", enfrentado en las

5 En el estudio de Orellana y Carrillo (2023) se comprueba que el principal predictor estadístico del miedo al cibercrimen es el miedo al delito. La existencia de condiciones criminales convencionales constituye un caldo de cultivo para la cibercriminalidad (UNDOC, 2013).

6 Se han considerado como características ambiguas aquellas díadas que en el diferencial semántico se situaron en proporciones cercanas a 50/50 o a 40/60 por ciento.

redes, autoritario, con hackers como protagonistas–, muchos rasgos atribuidos al cibercriminal lo confirman como una figura ambigua, como un extraño contingente al que las redes –esa urbe-caja negra anónima y etérea– amplifican su capacidad antisocial, incluyendo formas de acoso que fácilmente se alinean con las que caracterizan a la extrema derecha (Bocij y McFarlane, 2003; Simmel, 2014).

### 4.1. Limitaciones y recomendaciones

Esta investigación contó con un muestreo no probabilístico por lo que sus resultados no son extrapolables a la opinión general de las personas salvadoreñas mayores de edad. El diferencial semántico construido constituyó una parte de un cuestionario mayor. Por ello, su extensión fue limitada y apenas realizó un esfuerzo exploratorio para captar las representaciones sobre la figura del cibercriminal. Otras investigaciones pueden cimentarse mejor resolviendo algunos de estos problemas u orientando de manera diferente la investigación. Así, aunque lo ideal sería contar con muestreos amplios y probabilísticos, más relevante y viable puede ser identificar las representaciones de ciertos grupos sociales con afán de profundización o comparación: jóvenes, víctimas de cibercrímenes específicos o expertos (por ejemplo, especialistas en ciberseguridad, políticos, periodistas).

Asimismo, en este estudio se han indagado características de un cibercriminal único o general cuando otra posibilidad es explorar representaciones de cibercriminales específicos (tales como hacktivistas, acosadores o estafadores) considerando la enorme variedad que existe de estos (ver Cámara Arroyo, 2020). Por último, considerando que el miedo que despierta el crimen se encuentra siempre situado (Orellana, 2022a), es posible sugerir otras diadas para añadir a un hipotético diferencial semántico más amplio, consistente con la realidad salvadoreña actual: salvadoreño/extranjero, vive en el país/vive fuera del país, solo vive en El Salvador/entra y sale de El Salvador, es alguien conocido/es alguien desconocido, es pro-gobierno/es anti-gobierno, es de izquierda/es de derecha, el ciberdelincuente es una aplicación de IA o un bot/es una persona real[7].

## 5. Conclusión

El cibercrimen constituye una realidad global y su presencia en El Salvador no es la excepción. La dependencia de la digitalización de la existencia social, intensificada por eventos como la pandemia, han arrojado a las sociedades contemporáneas al ciberespacio. Así se abren un sinnúmero de posibilidades sinérgicas virtuosas (esto es, comunicación, comercio), pero también amenazas y peligros como la cibercriminalidad cuyas múltiples caras y omnipresencia contribuyen a sobrepasar los recursos instalados tanto de gobiernos como de las personas comunes.

La investigación constata victimización directa, indirecta o vicaria y, sobre todo, la representación de un cibercriminal con características extrañas, ambiguas o claramente disímiles a las de un pandillero: un extraño en la sombra. En otras palabras, existe prevalencia objetiva de esta forma de criminalidad, pero también una percepción social de que el responsable de esta responde a unas características muy peculiares, acorde con su "hábitat": el ciberespacio como nuevo lugar de lo no familiar, de producción de extrañeza contingente y, con ello, de amplificación de distintas formas de inseguridad y miedos sociales.

El conocimiento académico sobre la experiencia social y personal del cibercrimen aún es escaso, particularmente en países de la región centroamericana. Menos aún se conoce –dentro y fuera de la región– sobre la figura del perpetrador. Su imagen parece nutrirse de la esporádica

7 Esta diada hace explícita una posibilidad adicional respecto al cibercriminal cuyas implicaciones no se ha discutido en el artículo: que el perpetrador no sea una persona real, sino un tipo de tecnología (un robot, una aplicación o IA), aunque existan individuos concretos detrás de su creación o funcionamiento.

casuística real (esto es, noticias, casos judicializados), pero también de la resonancia social de los casos de hackeo, el sentido común y la imaginería mediática. Los resultados ofrecen un atisbo de posibles adaptaciones criminógenas, mismas que, como ha sido documentado, se han visto dinamizadas por acciones gubernamentales.

En conjunto, los hallazgos y el escenario descritos refuerzan la idea de que cabe esperar más cibercrimen y sus consecuencias (es decir, afectación de gobiernos, empresas, victimización personal, miedo al cibercrimen). Y si esto es así, se requerirá mucha imaginación investigativa para aproximarse mejor al cibercriminal, a este nuevo extraño tan concreto como imaginado.

## Referencias

Alvarado, M. (2022, 28 de noviembre). US$12 millones fueron hurtados de Chivo Wallet en El Salvador. *NO FICCIÓN*. https://www.no-ficcion.com/project/us12millones-hurto-chivo-wallet

Asociación Nacional de Regidoras, Síndicas y Alcaldesas Salvadoreñas. (2024). *Informe de resultados. Observación de violencia a mujeres políticamente activas en las elecciones internas en 2023.* ANDRYSAS. https://andrysas.org.sv/wp-content/uploads/2024/02/Informe_Violencia_politica.pdf

Ayala, F. (2024, 28 de junio). Capturan a cuatro mujeres acusadas de estafar por medio de Facebook en diferentes lugares de El Salvador. *La Prensa Gráfica*. https://www.laprensagrafica.com/elsalvador/Capturan-a-cuatro-mujeres-acusadas-de-estafar-por-medio-de-Facebook-en-diferentes-lugares-de-El-Salvador-20240628-0034.html

Bernal, D. (2022, 1 de octubre). Extraen información de FAES y PNC mediante hackeo informático. *La Prensa Gráfica*. https://www.laprensagrafica.com/elsalvador/Extraen-informacion-de-FAES-y-PNC-mediante-hackeo-informatico-20220930-0077.html

Bernal, D. (2024a, 12 de abril). Hubo 9,790 delitos informáticos en El Salvador hasta 2021; pero desde 2022 no se comparten cifras oficiales. *La Prensa Gráfica*. https://www.laprensagrafica.com/elsalvador/Hubo-9790-delitos-informaticos-en-El-Salvador-hasta-2021-pero-desde-2022-no-se-comparten-cifras-oficiales-20240412-0096.html

Bernal, D. (2024b, 7 de abril). Hackers han realizado al menos cuatro grandes filtraciones de datos de salvadoreños en lo que va de abril. *La Prensa Gráfica*. https://www.laprensagrafica.com/elsalvador/Hackers-han-realizado-al-menos-cuatro-grandes-filtraciones-de-datos-de-salvadorenos-en-lo-que-va-de-abril-20240407-0049.html

Bernal, D. (2024c, 5 de septiembre). Filtran datos de 974 mil salvadoreños que cotizan al ISSS: sus nombres, salarios, direcciones, DUI y más. *La Prensa Gráfica*. https://www.laprensagrafica.com/elsalvador/Filtran-datos-de-974-mil-salvadorenos-que-cotizan-al-ISSS-20240905-0052.html

Bocij, P. y McFarlane, L. (2003). Cyberstalking: The Technology of Hate. *The Police Journal: Theory, Practice and Principles, 76*(3), 204-221. https://doi.org/10.1350/pojo.76.3.204.19442

Brenan, M. (2018, 9 de noviembre). *Cybercrimes Remain Most Worrisome to Americans.* GALLUP. https://news.gallup.com/poll/244676/cybercrimes-remain-worrisome-americans.aspx

Carbajal, J. (2022, 25 de marzo). Detenidos esta madrugada habrían hurtado $16 mil 500 a seis víctimas a través de medios electrónicos. *La Prensa Gráfica*. https://www.laprensagrafica.com/elsalvador/Detenidos-esta-madrugada-habrian-hurtado--16-mil-500-a-seis-victimas-a-traves-de-medios-electronicos--20220325-0005.html

Cámara Arroyo, S. (2020). La cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*, (60), 470-512. https://portalcientifico.uned.es/documentos/61d68a62b32d1a43ae-9f2c64

Clark-Carter, D. (2002). *Investigación cuantitativa en Psicología. Del diseño experimental al reporte de investigación.* Oxford University Press.

Cristosal. (2024). *El silencio no es opción. Investigación sobre las prácticas de tortura, muerte y justicia fallida en el régimen de excepción.* Cristosal. https://cristosal.org/ES/el-silencio-no-es-opcion-informe-completo/

Departamento de Economía de la Universidad Centroamericana José Simeón Cañas. (2022). *Análisis socioeconómico de El Salvador: crisis, pandemia y elementos para pensar el desarrollo.* Universidad Centroamericana José Simeón Cañas.

Diazgranados, H. (2021, 31 de agosto). *Ciberataques en América Latina crecen un 24% durante los primeros ocho meses de 2021.* Kaspersky Daily. https://latam.kaspersky.com/blog/ciberataques-en-america-latina-crecen-un-24-durante-los-primeros-ocho-meses-de-2021/22718/

López Gutiérrez, J., Sánchez Jiménez, F., Herrera Sánchez, D., Martínez Moreno, F., Rubio García, M., Gil Pérez, M. V., Santiago Orozco, A. M. y Gómez Martín, M. A. (2022). *Informe sobre la cibercriminalidad en España 2021*. Ministerio del Interior. https://www.interior.gob.es/opencms/pdf/archivos-y-documentacion/documentacion-y-publicaciones/publicaciones-descargables/publicaciones-periodicas/informe-sobre-la-cibercriminalidad-en-Espana/Informe_cibercriminalidad_Espana_2021_126200212.pdf

Fundación de Estudios para la Aplicación del Derecho. (2021). *Desaparición de personas en El Salvador. La desaparición de personas y el contexto de violencia actual en El Salvador. Una aproximación inicial.* FESPAD. https://www.fespad.org.sv/investigacion-desaparicion-de-personas-en-el-salvador

Gavarrete, J. (2022, 17 de marzo). CIDH exige a El Salvador investigar espionaje contra periodistas y activistas. *El Faro*. https://elfaro.net/es/202203/el_salvador/26074/CIDH-exige-a-El-Salvador-investigar-espionaje-contra-periodistas-y-activistas.htm

Grinshteyn, E. G., Whaley, R. y Couture, M. C. (2021). Fear of Bullying and Its Effects on Mental Health among College Students: An Emerging Public Health Issue. *Journal of School Violence*, *20*(4), 536-551. https://doi.org/10.1080/15388220.2021.1979018

Henson, B., Reyns, B. W. y Fisher, B. S. (2016). Cybercrime Victimization. En C. A. Cuevas y C. M. Rennison (Eds.), *The Wiley Handbook on the Psychology of Violence* (pp. 553-570). Wiley-Blackwell. https://doi.org/10.1002/9781118303092.ch28

Hirtenlehner, H. y Farrall, S. (2014, 2 de agosto). Is the 'Shadow of Sexual Assault' Responsible for Women's Higher Fear of Burglary? *The British Journal of Criminology, 54*(6), 1167-1185. https://doi.org/10.1093/bjc/azu054

Instituto Universitario de Opinión Pública. (2022). La población salvadoreña opina sobre la situación económica familiar, la implementación del bitcoin y el Régimen de Excepción. *Boletín de prensa, 36*(4),. https://uca.edu.sv/iudop/wp-content/uploads/Boletin-de-Regimen-de-Excepcion.pdf

International Crisis Group. (2020, 13 de noviembre). *Violencia a prueba de virus: crimen y COVID-19 en México y el Triángulo Norte. Informe sobre América Latina N°83.* International Crisis Group. https://www.crisisgroup.org/sites/default/files/083-virus-proof-violence-spanish.pdf

International Crisis Group. (2022, 5 de octubre). *Un remedio para la fiebre carcelaria en El Salvador. Informe sobre América Latina N°96.* International Crisis Group. https://www.crisisgroup.org/sites/default/files/2022-10/096-a-remedy-for-el-salvadors-prison-fever-spanish.pdf

Kinosian, S. (2022, 29 de noviembre). *Trolls, propaganda and fear stoke Bukele's media machine in El Salvador.* Reuters. https://www.reuters.com/investigates/special-report/el-salvador-politics-media/

Lee, M. (2007). *Inventing Fear of Crime: Criminology and the politics of anxiety*. Willan Publishing.

Mahadevan, P. (2020). *Cybercrime. Threats during the COVID-19 Pandemic.* Global Initiative Against Transnational Organized Crime. https://globalinitiative.net/wp-content/uploads/2020/04/Cybercrime-Threats-during-the-Covid-19-pandemic.pdf

Marroquín, M. (2023, 31 de enero). Capturan a mujer que estafaba a través del sistema de ahorro "cuchubal" en redes sociales. *La Prensa Gráfica.* https://www.laprensagrafica.com/elsalvador/Capturan-a-mujer-que-estafaba-a-traves-del-sistema-de-ahorrocuchubal-en-redes-sociales-20230131-0027.html

Martel Trigueros, R. (2006). Las maras salvadoreñas: nuevas formas de espanto y control social. *ECA: Estudios Centroamericanos, 61*(696), 957-979. https://doi.org/10.51378/eca.v61i696.3585

Miró Llinares, F. (2021). Crimen, cibercrimen y COVID-19: desplazamiento (acelerado) de oportunidades y adaptación situacional de ciberdelitos. *IDP: revista d'Internet, dret i política,* (32), 1-17. https://doi.org/10.7238/idp.v0i32.373815

Morales-Arjona, I., Pastor-Moreno, G., Ruiz-Pérez, I., Sordo, L. y Henares-Montiel, J. (2022, 14 de noviembre). Characterization of Cyberbullying Victimization and Perpetration Before and During the COVID-19 Pandemic in Spain. *Cyberpsychology, Behavior, and Social Networking*, *25*(11), 733-743. https://doi.org/10.1089/cyber.2022.0041

Nord, M., Lundstedt, M., Altman, D., Angiolillo, F., Borella, C., Fernandes, T., Gastaldi, L., Good God, A., Natsika, N. y Lindberg, S. I. (2024). *Democracy Report 2024: Democracy Winning and Losing at the Ballot*. V-Dem Institute. https://v-dem.net/documents/43/v-dem_dr2024_lowres.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito. (2013). *Estudio exhaustivo sobre el delito cibernético.* Naciones Unidas. https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime_Study_Spanish.pdf

Oficina de las Naciones Unidas contra la Droga y el Delito. (2022). *Compendio de ciberdelincuencia organizada.* Naciones Unidas. https://www.unodc.org/documents/organized-crime/tools_and_publications/21-05345_S_eBook.pdf

Orellana, C. I. (2022a). El concepto de inseguridad ciudadana como hecho social subjetivo. *ECA: Estudios Centroamericanos, 77*(768), 33–56. https://doi.org/10.51378/eca.v77i768.6663

Orellana, C. I. (2022b). Tiempo de carroña: La dificultad representacional de la violencia en la posguerra salvadoreña (1990-2002). En C. I. Orellana y S. A. Herrera Mena (Eds.), *Una hidra de mil palabras. Análisis semántico del concepto de violencia en la revista* Estudios Centroamericanos (ECA). *El Salvador, 1946-2000*. (pp. 143-192). UCA Editores.

Orellana, C. I. y Santacruz Giralt, M. (2022). Epílogo-La laboriosa institución de lenguajes para nombrar las violencias salvadoreñas. En C. I. Orellana y S. A. Herrera Mena (Eds.), *Una hidra de mil palabras. Análisis semántico del concepto de violencia en la revista* Estudios Centroamericanos (ECA). *El Salvador, 1946-2000* (pp. 195-209). UCA Editores.

Orellana, C. I. y Carrillo, A. (2023). *El miedo al cibercrimen: explorando una faceta novedosa de la inseguridad ciudadana*. FLACSO Costa Rica. https://www.researchgate.net/publication/376352945_El_miedo_al_cibercrimen_explorando_una_faceta_novedosa_de_la_inseguridad_ciudadana_Fear_of_Cybercrime_Exploring_a_new_facet_of_Citizen_Insecurity

ONU Mujeres. (2021). *Midiendo la pandemia de sombra: La violencia contra las mujeres durante el COVID-19.* UN WOMEN. https://data.unwomen.org/sites/default/files/documents/Publications/Measuring-shadow-pandemic-SP.pdf

Osgood, C. E. (1952). The nature and measurement of meaning. *Psychological Bulletin*, *49*(3), 197-237. https://doi.org/10.1037/h0055737

Romo-Tobón, R. J., Vázquez-Sánchez, V., Rojas-Solís, J. L. y Alvídrez, S. (2020). Cyberbullying y Ciberviolencia de pareja en alumnado de una universidad privada mexicana. *Propósitos y Representaciones, 8*(2), e303. http://dx.doi.org/10.20511/pyr2020.v8n2.303

Rundell, J. (2014). Imagining cities, others: Strangers, contingency and fear. *Thesis Eleven, 121*(1), 9-22. https://doi.org/10.1177/0725513614528783

Scott, H. (2003). Stranger Danger: Explaining Women's Fear of Crime. *Western Criminology Review, 4*(3), 203-214. https://www.westerncriminology.org/documents/WCR/v04n3/article_pdfs/scott.pdf

Simmel, G. (2014). *Sociología: estudios sobre las formas de socialización.* Fondo de Cultura Económica.

Stockemer, D. (2019). *Quantitative Methods for the Social Sciences. A Practical Introduction with Examples in SPSS and Stata*. Springer International Publishing. https://doi.org/10.1007/978-3-319-99118-4

United Nations Development Programme. (2024). *Human Development Report 2023/2024. Breaking the gridlock. Reimagining cooperation in a polarized world.* Human Development Reports UNDP. https://hdr.undp.org/system/files/documents/global-report-document/hdr2023-24reporten.pdf

Vargas, P. y Vargas, K. (2023). *Ciberdelito en Centroamérica y el Caribe*. FLACSO Costa Rica.

Wilcox, P., Jordan, C. E. y Pritchard, A. J. (2006). Fear of Acquaintance Versus Stranger Rape as a "Master Status": Towards Refinement of the "Shadow of Sexual Assault". *Violence and Victims, 21*(3), 355-370. https://doi.org/10.1891/vivi.21.3.355

World Economic Forum. (2022, 11 de enero). *The Global Risks Report 2022* (17ª. ed.). World Economic Forum. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf