El miedo al cibercrimen:
explorando una faceta novedosa de la inseguridad ciudadana

Personas autoras

Carlos Iván Orellana

Adilio Carrillo

conose
RED DE CONOCIMIENTO SOBRE SEGURIDAD CIUDADANA

infoSEGURA

USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

PNUD

El miedo al cibercrimen:

explorando una faceta novedosa de la inseguridad ciudadana

conose

RED DE CONOCIMIENTO SOBRE **SEGURIDAD CIUDADANA**

Red de Conocimiento sobre Seguridad Ciudadana (CONOSE)

El miedo al cibercrimen:
explorando una faceta novedosa de la inseguridad ciudadana

Comité Coordinador:
FLACSO Costa Rica: Ilka Treminio Sánchez
Fundación Dr. Guillermo Manuel Ungo: Manuel Delgado
Universidad Centroamericana José Simeón Cañas: Mario Zetino

Secretaría Técnica: Carlos Guillermo Ramos González y Karla Salazar Sánchez

Autores:
Carlos Iván Orellana
Adilio Carrillo

Revisión filológica: Karen Iliana Martínez Flores

Diseño y diagramación: Pamela Abrego

Esta publicación ha sido posible gracias al apoyo brindado por el pueblo de los Estados Unidos por medio de la *Agencia de los Estados Unidos para el Desarrollo Internacional* (USAID, por sus siglas en inglés), y a la asistencia técnica del Centro Regional para América Latina y el Caribe del *Programa de las Naciones Unidas para el Desarrollo* (PNUD LAC). Las opiniones y los puntos de vista que se presentan en este documento son exclusiva responsabilidad de sus autores y autoras, y no reflejan necesariamente los de USAID, del Gobierno de los Estados Unidos, del PNUD o de los países miembros de las Naciones Unidas.

El miedo al cibercrimen:
explorando una faceta novedosa de la inseguridad ciudadana

364.09
O-66m Orellana Calderón, Carlos Iván
El Miedo al cibercrimen : explorando una faceta novedosa de la inseguridad ciudadana [recurso electrónico] / Carlos Iván Orellana Calderón. – primera edición – San José, Costa Rica, FLACSO, 2023.
E-book ; pdf : 810 Kb.
ISBN 978-9977-68-353-9

1.DELITOS INFORMÁTICOS. 2. CRIMINOLOGÍA. 3. INSEGURIDAD. CIUDADANA. 4. VÍCTIMAS. 5. COMUNICACIÓN ELECTRÓNICA. 6. MODELO INFORMÁTICO. I.Título.

Este estudio se llevó a cabo en el marco del programa de investigación de la Red de Conocimiento sobre Seguridad Ciudadana (CONOSE).

Editorial FLACSO Costa Rica, 2023

La Red CONOSE surgió en el año 2015, a partir del Foro Regional “Gestión de conocimiento en seguridad ciudadana: una mirada desde la sociedad civil”, como una respuesta a la necesidad de articular una serie de instituciones que abordan el tema de seguridad ciudadana. Su objetivo es promover espacios de reflexión y colaboración para la generación de evidencia rigurosa en materia de violencia y criminalidad, con el fin último de orientar la toma de decisiones de políticas públicas que abordan dichas problemáticas.

Corolario de lo anterior, una de las líneas de trabajo fundamentales de la Red es el apoyo a la investigación académica para fortalecer los abordajes metodológicos, analíticos y prácticos en materia de violencia y seguridad ciudadana, sobre la base de información actualizada, contextualizada y con los más altos estándares de calidad.

El cibercrimen es un nuevo reto para las políticas de seguridad ciudadana y el presente artículo busca dar luces sobre victimización, victimización vicaria, percepciones y el nivel de miedo al cibercrimen y abonar así a un mejor entendimiento de este fenómeno y sus posibles abordajes a futuro.

Contenido

Introducción

Los cibercrímenes han aumentado en los últimos años gracias a la convergencia de distintas circunstancias. Entre estas, la creciente dependencia digital de la sociedad, las medidas de confinamiento –aplicadas por igual sobre posibles víctimas y perpetradores– provocadas por la pandemia y, en general, al "trasvase operacional que existe entre el mundo físico y el ciberespacio" (Arroyo Guardeño et al., 2020, pp. 9-10; Stickle y Felson, 2020; World Economic Forum, 2022). Miró Llinares (2021) precisa que la Covid-19 habría acelerado un proceso de digitalización de la vida cotidiana que ya estaba en marcha y que, en estas circunstancias, aunque no se pueden descartar vínculos entre el crimen no cibernético y el cibercrimen[1], los ciberdelincuentes habrían recurrido a adaptaciones diversas –tipológicas, de objetivos, técnicas y de ciberlugar–, debido a las condiciones de permanencia prolongada en línea.

Según Diazgranados (2021), con base en el informe "Panorama de Amenazas en América Latina 2021" de Kaspersky, los ciberataques en Latinoamérica durante el 2021 crecieron un 24 % en comparación con el 2020. Estos afectan tanto a personas como a empresas, y se calcula que acaece un ataque de *malware* o software malicioso cada 35 segundos. Las condiciones de conexión remota (e.g., trabajar desde casa), la piratería –uso de programas copiados, sin controles o registro– y la masiva utilización (y dependencia) de teléfonos móviles inteligentes incrementan la amenaza de llegar a ser víctima de un ataque por medios electrónicos. Se considera que las ciberamenazas en la actualidad sobrepasan las habilidades de las sociedades contemporáneas para prevenirlas o responder a ellas adecuadamente (World Economic Forum, 2022).

1 En la nomenclatura al uso, términos como los siguientes se utilizan de manera intercambiable: crimen, delito, delito común, delito convencional, delito no cibernético, delito fuera de línea o delitos *off-line*. Asimismo, por su parte, en cuanto al ámbito ciber, suelen usarse como sinónimos términos como ciberdelito, cibercrimen, delitos electrónicos, delitos informáticos, delitos en línea o delitos *on-line*. En este trabajo se intentará evitar la variabilidad terminológica para ganar claridad expositiva y se empleará, principalmente, el termino *delito* para referirse a las formas de inseguridad objetiva o subjetiva que acaecen en el mundo físico o concreto (e.g. miedo al delito, hurto de pertenencias), y el término *cibercrimen* para aludir a formas de inseguridad objetiva o subjetiva que acaecen en el mundo virtual o mediado por artefactos electrónicos (e.g. miedo al cibercrimen, hurto de datos personales).

La investigación reciente de Vargas y Vargas (2023), confirma que el cibercrimen ya es una realidad en los países de Centroamérica y del Caribe. Asimismo, ofrece ciertos indicios de algunas peculiaridades que adopta esta modalidad de criminalidad en la región: constituye, especialmente, un fenómeno urbano; afecta a personas que atraviesan la adultez joven (18-40 años); mayoritariamente se concreta en ciberacoso, *malware* y el hackeo de redes o correo electrónico; acarrea consecuencias psicológicas y materiales perniciosas; y estos delitos están teniendo lugar en un escenario social de carencia de una "cultura de denuncia" (p. 60) ante su manifestación.

Así pues, El Salvador no constituye una excepción respecto al fenómeno del cibercrimen, sus manifestaciones y sus efectos. Durante 2021 se habrían producido 2.1 millones de ataques a empresas centroamericanas[2] y, de estos, 206,000 ataques cibernéticos se habrían dirigido contra empresas salvadoreñas. Adicionalmente, los delitos informáticos contra las personas, especialmente el hurto de dinero y de identidad, se habrían multiplicado por siete. Estos hechos, presumiblemente, habrían encontrado una circunstancia favorable con la implementación de la "Chivo Wallet"[3], la billetera gubernamental para gestionar bitcoins (Alfaro, 2022; Jordán, 2022). Los casos de espionaje a activistas y a periodistas por parte del gobierno (Gavarrete, 2022) también han constituido casos sonados que verifican tanto la incidencia como la variabilidad fenomenológica del cibercrimen en la sociedad salvadoreña. Actualmente, incluso la Aso-

2 Cada vez es más frecuente encontrar en los periódicos nacionales noticias que consignan los resultados de informes de empresas de ciberseguridad que reportan cifras altísimas de ataques informáticos. Por ejemplo, recientemente, con base en datos de la empresa Fortinet, se reportó el suceso de 24 millones de "intentos" de ataques cibernéticos en El Salvador durante el primer trimestre de 2023 (360,000 millones en toda Latinoamérica según el mismo informe; ver Molina, 2023). El carácter inconmensurable de las cifras de ciberataques disponibles permite resaltar tres aspectos propios de la fenomenología de la cibercriminalidad: primero, cabe presumir que tales cifras de incidencias se explican, en buena medida, por que corresponden a repetidos conatos o intentos de sistemas persistentes y autónomos de amenaza (e.g., códigos maliciosos). En segundo lugar, las cifras se disparan porque, a diferencia del crimen convencional, el cibercrimen permite trazabilidad y se registran y reportan tanto los intentos exitosos como los fallidos cuya totalidad es contabilizada como una incidencia. El crimen convencional suele traducirse en estadísticas de hechos consumados y no en recuentos de intentos de cometimiento, lo que, de llevarse a cabo, seguro también inflarían las estadísticas de estos. En tercer lugar, las cifras seguirán subiendo, ya que se coincide en que la afectación a empresas y personas se mantiene al alza, en un escenario en el que tampoco los gobiernos se libran de convertirse en blancos de ciberataques, como lo demostró el hackeo de sitios del ejército y de la policía en varios países latinoamericanos a manos de un grupo de *hacktivistas* autodenominado "Guacamaya" (Bernal, 2022).

3 Los dispositivos de gestión de criptomonedas se conocen como *wallets* (billeteras). Debido a que en El Salvador se implementó el bitcoin como moneda de curso legal en septiembre de 2021, esta medida fue acompañada del lanzamiento de una *wallet* gubernamental denominada "Chivo Wallet". La palabra "Chivo" es un salvadoreñismo polisémico de carácter exclamativo, propio del habla popular, que indica aprobación, acuerdo o disfrute (replica un sentido semántico equivalente al de vocablos como "chido" en México, "chévere" en algunos países de Sudamérica o "guay" en España).

ciación Bancaria Salvadoreña (ABANSA) constata el incremento de fraudes cibernéticos que afectan a usuarios comunes (Machuca, 2023).

Como país en vías de desarrollo cabe presuponer que su vulnerabilidad al cibercrimen es alta, debido al uso masivo de telefonía móvil, de criptomonedas (en particular bitcoin), de redes sociales y acceso creciente a internet, especialmente por ocio o consumo, y debido a la persistencia de inequidades digitales propias de países con economías de bajo crecimiento (Dirección General de Estadística y Censos [DIGESTYC], 2021; Instituto Universitario de Opinión Pública [IUDOP], 2022; Kemp, 2022; World Economic Forum, 2022). Todo esto, en interacción con condiciones de educación tecnológica deficiente, persistentes brechas socioeconómicas y digitales, así como de presencia de crimen organizado y desorganizado que, con la pandemia, cabe presumir que habrían encontrado nuevas oportunidades de acción y expansión (Mahadevan, 2020; Oficina de Naciones Unidas contra la Droga y el Delito [UNODC], 2013).

Por otra parte, la existencia de legislación dispersa[4] para el combate de delitos cibernéticos en el país que acompaña a una incipiente política de ciberseguridad nacional (Secretaría de Innovación de la Presidencia, 2021), confirmaría el reconocimiento oficial del fenómeno. En conjunto, todo lo anterior demuestra tanto la novedad como el desconocimiento que aún prevalece en este país centroamericano sobre esta forma de inseguridad ciudadana (Orellana, 2022), en tanto que la sociedad está habituada a expresiones y al estudio del crimen común o convencional, lo que incluye, entre otros, la violencia de género (Centro de Estudios de Opinión Pública [CEOP], 2022; Delgado et al., 2021).

Con base en las reflexiones previas, y considerando que la investigación descansa en el empleo de una encuesta en línea, los objetivos de la presente investigación son cinco: primero, describir la victimización, la victimización vicaria (conocimiento de la victimización de otros) y la percepción de agravamiento de la inseguridad (delito y cibercrimen) por parte de los participantes en el estudio; segundo, establecer el nivel de miedo al cibercrimen en la muestra participante; en tercer lugar, determinar la relación de este miedo con variables sociodemográficas, recursos financieros electrónicos y el miedo al delito; cuarto, explorar la existencia de temores a cibercrímenes específicos según el género; por último, en quinto lugar, elaborar un modelo predictor del miedo al cibercrimen con las variables consideradas.

4 Ley Especial contra los Delitos Informáticos y Conexos, Código Penal y Código Procesal Penal. Algo más de la situación jurídica del país -y de la región centroamericana y del Caribe- sobre el tema se comenta en Vargas y Vargas (2023).

1. **Cibercrimen: conceptos básicos, vulnerabilidad y factores asociados**

Las ciberamenazas, conceptualmente, suelen referirse a vulneraciones de sistemas informáticos, pero su alcance connotativo puede incluir el llamado cibercrimen, ciberdelito o delitos cibernéticos. La ciberseguridad, por su lado, constituiría el reverso defensivo de la ciberamenazas; esto es, dispositivos, estrategias y protocolos de protección contra ataques en línea. Aquí también se incluiría la protección personal ante el embate de problemas informáticos impersonales cotidianos (e.g., virus), pero también ante el acecho calculado del cibercrimen en sus distintas manifestaciones. Según el Foro Económico Mundial (World Economic Forum, 2022, p. 48) la "falla de la ciberseguridad" constituye uno de los principales riesgos a nivel mundial que se vio agravado por la pandemia.

Significa que la cibercriminalidad puede afectar a gobiernos, organizaciones y empresas, pero acá interesa explorar una consecuencia específica en ciudadanos comunes: el miedo a la posibilidad de convertirse en víctima personal de un cibercrimen (Henson et al., 2016), situación que, no obstante, presupone que toda experiencia personal de inseguridad se encuentra socialmente mediada, responde a un contexto de sentido y nunca se vive de manera aislada de los otros (Orellana, 2022). Así, el cibercrimen será comprendido, de manera amplia, como aquellas acciones delictivas capaces de atentar contra la integridad personal física, psicológica o moral (e.g., amenazas, reputación, odio) o contra el patrimonio material o informático del individuo (e.g., dinero, información, identidad), que ocurren en o a través del ciberespacio o debido a la gestión de medios electrónicos[5].

Globalmente, la victimización individual por delitos cibernéticos ya sobrepasa a la producida por delitos comunes. En países en vías de desarrollo, como cabría esperar en el caso de El Salvador, la vulnerabilidad a la victimización por cibercrimen está vinculada con la presencia de actores fuera de la ley capaces de operar en y fuera de línea (e.g., crimen organizado). También con la elevada incidencia de delitos convencionales y con variables contextuales como

5 Aunque definiciones como esta parecen de sentido común, en realidad existen múltiples concepciones, disensos, matices, clasificaciones y tipologías variables sobre el cibercrimen (e.g., Brands y Van Doorn, 2021; Brar y Kumar, 2018; Ibrahim, 2016; Payne, 2020; UNODC, 2013). De igual manera, cabe pensar que este tipo de criminalidad exacerba el temor de victimización de ciertos individuos en cuanto que personas jurídicas, lo que puede añadir capas de complejidad a la comprensión y estudio del fenómeno.

ciertas condiciones socioeconómicas (i.e., mayor o menor poder adquisitivo) o sociodemográficas (i.e., edad, género, nivel educativo) (UNODC, 2013, 2022). La consideración de la vulnerabilidad o la mayor o menor probabilidad de ocurrencia y victimización por cibercrimen, atendiendo a ciertos contextos y condiciones particulares, permite realizar dos precisiones sobre el miedo al cibercrimen.

En primer lugar, la alta incidencia de cibercrímenes y su creciente repercusión social a través de noticias, estudios o anécdotas personales, hace esperar un incremento en el miedo asociado a su ocurrencia. Esta es una cuestión nada menor, si se considera que el cibercrimen tiene la capacidad de "producir niveles de miedo, pavor o preocupación", es decir, emociones capaces de competir con las que producen en las víctimas los más graves delitos personales tradicionales (Henson et al., 2016, p. 556). Por ejemplo, según la comprehensiva revisión de Marín-Cortés y Linne (2020), las víctimas de ciberacoso (*cyberbullying*) con frecuencia experimentan miedo y otras emociones de carácter persecutorio o con el potencial de derivar en aislamiento, como la ansiedad, la angustia o la desconfianza. Cabe establecer un hecho cuya obviedad cede ante la realidad que confirma: la proliferación del cibercrimen constata la vulnerabilidad de las personas a sufrir este tipo de delitos mientras que tal incidencia delictual constituye, a su vez, un factor de vulnerabilidad para la emergencia del miedo a la cibercriminalidad con sus consecuencias aparejadas.

NortonLifeLock (2021), a partir de una encuesta administrada en 10 países, encontró que el 58 % de participantes concordaba mucho o algo con que temían "como nunca" llegar a ser víctimas de un cibercrimen; y que entre las emociones que experimentaron quienes sufrieron un acceso no autorizado a sus cuentas o dispositivos se reportó enojo (52 %), estrés (46 %), vulnerabilidad (41 %), sentido de violación y miedo (34 %). Según datos de la encuesta Gallup, en Estados Unidos, el miedo a ser víctima de cibercrímenes, en concreto, robo de información personal y financiera y robo de identidad, ya ocupa la principal preocupación ciudadana en la última década, por encima de crímenes no cibernéticos (Brenan, 2018). Vargas y Vargas (2023) encuentran que, entre otros, el impacto psicosocial del cibercrimen en países de Centroamérica y el Caribe, destacan los daños emocionales (e.g., ansiedad, miedo, preocupación), la inseguridad y el menoscabo a la reputación personal. La percepción de riesgos *online* nunca es inocua, pues puede conducir al incremento del miedo al cibercrimen y a tomar acciones de evitación, como limitar actividades de entretenimiento o la realización de compras en línea (Brands y Van Doorn, 2022).

La segunda precisión que cabe exponer está referida a los factores y el contexto posibilitadores del cibercrimen. Para aproximarse a la victimización por cibercrimen, se suele recurrir como marco explicativo a la Teoría de Actividades Rutinarias (en inglés, *Routine Activity Theory* (RAT)), (Henson, 2020; Morillo Puente y Ríos Hernández, 2022; Rodríguez et al., 2017). Según esta perspectiva, la victimización en línea puede ocurrir debido a la interdependencia de tres factores: un delincuente motivado (*motivated offender*), la carencia de defensas apropiadas (*lack of capable guardianship*) y la idoneidad del blanco u objetivo (*target suitability*). En consonancia con la RAT, aquí se parte de comprender que el miedo al cibercrimen acaece en un contexto objetivo de tendencias ascendentes de este tipo de criminalidad (victimización, noticias, conocimien-

to de casos, etc.). Pero, además, que tal expresión emocional de temor emerge también gracias a la lectura escenificada, idiosincrática, sesgada y situada en un contexto singular de riesgo y vulnerabilidad –el salvadoreño, en este caso–, que la persona realiza a partir de los mayores o menores recursos (educativos, tecnológicos¬, etc.) de los que dispone (Beck, 2008; Orellana, 2022; Santacruz Giralt, 2022; Virtanen, 2017).

El miedo al cibercrimen adquiere contornos más claros a partir de la identificación de factores que modulan su manifestación[6]. Según la revisión sistemática de Brands y Van Doorn (2022), hay factores asociados al miedo al delito como el género (específicamente, ser mujer), la percepción de riesgo o la experiencia concreta de victimización, que, igualmente, constituyen correlatos usuales del miedo al cibercrimen. Otros factores como la edad, la educación, así como el uso de recursos financieros específicos (tarjetas de crédito o banca en línea), ofrecen evidencia variable de su vínculo con el miedo al cibercrimen por su naturaleza cambiante o su dependencia de la muestra participante (Abdulai, 2020; Brands y Van Wilsem, 2021; Rodríguez et al., 2017; UNODC, 2013). Contar con menos confianza técnica, bajas habilidades computacionales, un estatus socioeconómico más precario, así como experimentar más miedo al delito en general, también se asocian con el miedo al cibercrimen (Guedes et al., 2022; Virtanen, 2017). Estas reflexiones, además, ponen de manifiesto que tanto perpetradores como víctimas, tienden a pertenecer a categorías o grupos sociales en virtud de cuyas características específicas se modula la capacidad de operación de los primeros y la posible vulnerabilidad de las segundas (Nurse y Bada, 2019).

La existencia de variables que incrementan la vulnerabilidad al miedo al cibercrimen, como la falta de competencia técnica o el empleo de ciertos productos financieros, pone de manifiesto una característica paradójica del cibercrimen, respecto al delito común, que podría enunciarse de la siguiente forma: la inclusión incrementa la vulnerabilidad al cibercrimen. Es de sobra sabido, como lo prueban las investigaciones sobre violencia y crimen convencionales, relativas a pandillas (e.g., los volúmenes de maras y pandillas en Centroamérica), que la exclusión orilla –en este caso– a jóvenes a incurrir en y a sufrir actos delictivos, así como a ejercer violencia. En el caso del cibercrimen, es verdad que formas de exclusión, como la brecha digital, puede conllevar, a la postre, a una baja competencia y educación digital, pero la inclusión –e.g., reducción de la

6 A manera de nota precautoria, hay que decir que las tendencias de la cibercriminalidad que se reportan en este trabajo a partir de las distintas fuentes consignadas corresponden a lecturas generales de dichas tendencias. Esto es así porque los estudios sobre inseguridad, cibervictimización o miedo al cibercrimen presentan múltiples variaciones entre sí: en cuanto a la definición de conceptos, a la operacionalización de variables (cibercrimen general o ciberdelitos muy específicos, como robo de identidad o fraudes referidos al uso de cierto producto financiero como tarjetas de crédito, etc.), a la mayor o menor representatividad muestral, los contextos cambiantes o la sofisticación general del diseño de la investigación (e.g., datos de correlaciones o de modelos predictivos). No obstante, el carácter acumulativo y tendencial de la evidencia permiten confiar en las variables o patrones generales que se reportan.

brecha digital– expone al cibercrimen por la mera presencia incrementada en el ciberespacio, con el consiguiente cambio de rutinas cotidianas y el añadido de ciertas características personales de riesgo (i.e., mayor exposición, imprudencia al navegar en la red) de quien antes permanecía fuera de línea (Herrero et al., 2021; Velásquez et al., 2021; Virtanen, 2017; Wijayanto y Prabowo, 2020). La aproximación a la vulnerabilidad, a formas peculiares de criminalidad, en este caso, requiere problematizaciones teóricas y metodológicas constantes desde el momento en que dicha condición tiene lugar en contextos de precariedades y violencias múltiples que hacen de la vulnerabilidad una condición inherente e inescapable del ciudadano contemporáneo (Santacruz Giralt, 2022).

La problematización del binomio exclusión-inclusión de cara a la vulnerabilidad al cibercrimen se complejiza al considerar la difuminación de los límites entre el mundo real y el mundo digital. A propósito del papel del miedo al delito, y en consonancia con el "trasvase operacional" entre el mundo digital y el real antes apuntado (Arroyo Guardeño et al., 2020), Cross y Lee (2022), citando el trabajo de Powell et al. (2018), establecen que las divisiones entre mundos *offline* y *online* ya resultan obsoletas. Así lo demostrarían los casos de "fraude romántico" –estrategia que conlleva fingir tener una relación sentimental con la víctima–, ya que en estos se solapan y potencian victimizaciones y miedos tanto físicos como virtuales. Otros estudios –del mismo volumen de la revista *Victims & Offenders*, en la que aparece el trabajo de Cross y Lee– comprueban cómo este mismo principio de traslape y potenciación mutua se produce también entre la violencia feminicida y la violencia de pareja, facilitada por la tecnología (McLachlan y Harris, 2022), y la victimización por ciberacoso y la victimización sexual cara a cara (Choi et al., 2022).

La digitalización obligatoria y acelerada provocada por la pandemia no solo colapsó súbitamente el mundo real con el virtual, sino que, además, entreveró las posibilidades de victimización y miedo al delito y al cibercrimen. Esta circunstancia magnificó, en particular, el riesgo de las mujeres para sufrir violencia doméstica y sexual, expresiones graves de victimización que resultan temidas y experimentadas distintivamente en mayor proporción por ellas que por los hombres (Jauregui y Vozmediano, 2021; Lee, 2007). Así, la crisis sanitaria incrementó la violencia generalizada contra las mujeres (ONU Mujeres, 2021), incluyendo la exacerbación de amenazas virtuales, como el ciberacoso sexual y el fraude en distintas formas. Cabe pensar que el confinamiento durante la pandemia configuró un contexto de sobrexposición en línea al interior de ámbitos riesgosos como el hogar (mientras se teletrabajaba o estudiaba, a la vez que se proveían cuidados a terceros y se mantenían contactos afectivos a distancia). Paradójicamente, también cabía esperar que se produjera una (auto) limitación del uso de internet por temor, con la consiguiente ampliación de la brecha digital de género preexistente a la pandemia (Leone y Caballero, 2021; Vera Morales, 2021). El género constituye un operador analítico que deja poco margen a las dudas sobre la superposición fenomenológica que se produce entre diversas inseguridades, en planos objetivos y subjetivos, analógicos y virtuales.

En última instancia, la transposición que se produce entre el miedo al delito y el miedo al cibercrimen, como lo demuestran los casos de ciberacoso en todas sus formas, evidencian el diferencial y el abuso de poder que las nuevas

tecnologías permiten y amplifican (Hirigoyen, 2010). El cibercrimen acecha, como lo hace en la vida real el delito común, principalmente a individuos vulnerables, a quien se aparta de las normas convencionales, a quien está sometido a ellas en desventaja o porque su sufrimiento resulta normalizado o socialmente minimizado (i.e., mujeres, *outsiders*, personas con carencias de recursos técnicos o financieros, pertenecientes a minorías). Asimismo, la capacidad de acción amplificada del cibercrimen y su miedo concomitante, se alimentan de las dinámicas favorables que la virtualidad concede al perpetrador, como el anonimato o la posibilidad de afectar a muchos de forma simultánea (Bocij y McFarlane, 2003; Grinshteyn et al., 2021; Jauregui y Vozmediano, 2021).

2. Metodología

2.1. Diseño de la investigación y participantes

El diseño de investigación implementado corresponde a un diseño por encuestas (Stockemer, 2019), específicamente, un sondeo en línea de tipo transversal (aplicación en un período específico), encaminado a explorar actitudes generales (valores, creencias, preferencias).

El muestreo empleado puede ser definido como no probabilístico propositivo (Clark-Carter, 2002). Es decir, que el procedimiento de selección muestral no responde a procesos aleatorios, pero sí al establecimiento de características de inclusión específicas: personas salvadoreñas mayores de 18 años que residieran en el país al momento del estudio. La muestra participante consta de 315 personas con un promedio de edad de 27.5 años (*DE* = 10.2). El 58 % de la muestra se identificó como del sexo femenino y el 42 % restante como del sexo masculino. En cuanto a su ocupación principal, 42 % de los participantes declararon ser estudiantes, casi una tercera parte (31 %) dijo estudiar y trabajar, 24 % dijo que solo trabajaba y un minoritario 3 % seleccionó otras condiciones ocupacionales (e.g., jubilación, oficios del hogar, desempleo).

2.2. Instrumento

La encuesta utilizada fue diseñada para este estudio. Además de recabar algunos datos sociodemográficos (sexo, edad y ocupación), esta también registró opiniones sobre el posible agravamiento y la victimización por delito común y por cibercrimen a través de cuatro preguntas (que se exponen más adelante en los resultados). Asimismo, se incluyeron tres escalas específicas: a) escala de empleo de recursos financieros electrónicos; b) escala de miedo al delito; y c) escala de miedo al cibercrimen. La encuesta incluyó al final un espacio opcional abierto para conocer opiniones sobre el fenómeno o comentarios de las personas participantes.

Escala de empleo de recursos financieros electrónicos

Esta escala mide la posible utilización de nueve recursos financieros electrónicos: cuenta de ahorro, tarjeta de crédito, tarjeta de débito, cajeros automáticos, plataformas de banca en línea, *wallet* del gobierno para gestionar bitcoin (la llamada “Chivo Wallet”), uso de otras *wallets*, la recepción y el envío de remesas. La escala, por tanto, explora la posesión o utilización de servicios o herramientas en línea y electrónicas asociadas al manejo de dinero, cuestión

que, en principio, incrementa el riesgo de exposición a victimización, tanto por delincuencia común como por ciberdelincuencia.

La estructura de respuesta de la escala es dicotómica (Sí = 1, No = 0) y, en promedio, las personas participantes expresaron utilizar cerca de cuatro recursos electrónicos en su vida cotidiana (M = 3.7, DE = 1.9). Los recursos de uso minoritario por parte de la muestra (con un 26 % o menos de menciones) fueron la tarjeta de crédito, las *wallets* y la gestión de remesas. Un análisis factorial exploratorio (AFE) encontró cuatro factores a la base de esta escala, cuya estructura y consistencia interna, sin embargo, resultaba mejorable[7]. A partir de los resultados de este primer AFE realizado, se decidió aglutinar los ítems de remesas (recepción y envío) y se eliminó el ítem de uso de la "Chivo Wallet". De esta forma, la consistencia interna de la escala alcanzó un índice Alfa de Cronbach satisfactorio de .75. Asimismo, un nuevo análisis factorial exploratorio (AFE; KMO = .829 y prueba de esfericidad de Bartlett con valor de p = .001), recurriendo a un método de componentes principales y rotación Varimax, ahora encontró una estructura factorial más parsimoniosa de solo dos factores que explicaban el 64 % de la varianza de los resultados. El primer factor da cuenta del 47 % de la varianza e incluye los recursos de uso más generalizado, incluyendo la tarjeta de crédito[8], por lo que fue denominado como "recursos financieros comunes". Mientras que el segundo factor incluye el uso de otras *wallets* y la gestión de remesas, es decir, recursos financieros de uso más infrecuente por parte de la muestra participante. Este factor fue denominado como "criptomonedas-remesas" y alcanzó a explicar el restante 17 % de la varianza.

Escala de miedo al delito

La escala de miedo al delito fue tomada de Orellana (2022) y explora el temor a ser víctima de ocho delitos específicos, relativamente comunes en el contexto salvadoreño: homicidio, agresión física, violación sexual, secuestro, robo a mano armada, robo sin agresión (hurto), extorsión/ "renta" y soborno por parte de alguna autoridad o funcionario público ("mordida", en el argot salva-

7 AFE: KMO = .801 y prueba de esfericidad de Bartlett con valor de p = .001. Empleando un método de componentes principales y rotación Varimax, se encontraron cuatro factores en la escala que alcanzaron a explicar el 77 % de la varianza. El primer factor aglutinó el uso de recursos electrónicos financieros más comunes: cuenta de ahorro, tarjeta de débito, cajeros y banca en línea (37 %), el segundo factor se compone de las dos *wallets* para criptomonedas (15 %), el tercer factor reúne el uso de tarjeta de crédito y la recepción de remesas (13 %). Finalmente, el envío de remesas figuró como ítem único en el último factor (12 %). Por su parte, el análisis de consistencia interna mostró que esta escala quedaba apenas por debajo del límite ideal que establecen las convenciones (α = .69).

8 El uso de tarjeta de crédito, de hecho, muestra cargas cruzadas en ambos factores inferiores a .40 (pero más alta en el primero factor que en el segundo: .386 vs .363), lo que resulta consistente con la idea de que se trata de un recurso familiar o conocido por los participantes, pero no necesariamente de uso generalizado. Según Kemp (2022), menos del 6 % de salvadoreños con 15 años o más cuenta con una tarjeta de crédito.

doreño). Se agregó un ítem sobre el delito de desaparición de personas dada la incidencia que el mismo tiene en la realidad salvadoreña actual.

La escala cuenta con una estructura de respuesta tipo Likert de cuatro puntos (3 = mucho, 2 = algo, 1 = poco y 0 = nada; puntaje máximo posible 27 y mínimo de 0) y su consistencia interna fue muy alta (α = .93). Un análisis factorial exploratorio (AFE; KMO = .92 y prueba de esfericidad de Bartlett con valor de p = .001), encontró una estructura unifactorial que explicó el 70 % de la varianza de los resultados. Es decir, la escala mide un único factor: el miedo al delito.

Escala de miedo al cibercrimen

Esta escala se creó para los propósitos de este estudio y replica la lógica y las opciones de respuesta de la escala de miedo al delito recién expuesta. Es decir, a través de una escala Likert de cuatro puntos (puntaje máximo posible 36 y mínimo de 0), explora el temor a ser víctima de 12 cibercrímenes posibles: robo/hurto de datos personales, robo/hurto de dinero en línea, estafa en línea, suplantación de identidad, hackeo de cuenta de correo electrónico o de sitio web personal, extorsión con información o imágenes personales, espionaje por parte del gobierno, espionaje por parte de otros, clonación de tarjeta de crédito/débito, ciberacoso sexual, ciberacoso personal (*bullying*) y ciberacoso laboral (*mobbing*)[9].

Las características métricas de la escala indicaron una alta consistencia interna (α = .93), mientras que su estructura factorial[10] se constituyó de dos factores con una varianza explicada y distribución de ítems bastante simétrica: el primer factor explicó el 35 % de la varianza y fue denominado como "invasión a la intimidad", por reunir los seis ítems vinculados a ciberdelitos que refieren a prácticas de acoso (sexual, personal y laboral), extorsión con información o imágenes personales y espionaje (gubernamental y de otras personas). Siguien-

9 Parte del reto actual en el abordaje científico del cibercrimen se encuentra en la labor de búsqueda de consensos, la atención al habla académica y cotidiana, y en el intento de traducción del inglés al español de términos complejos para describir e investigar cibercrímenes específicos. Por ejemplo, solo en la propuesta de taxonomía de cibercrímenes de Brar y Kumar (2018), se identifican -en inglés- cuatro categorías generales que, a su vez, se desglosan en 12 subcategorías en total (e.g., Ciberviolencia = ciberguerra, ciberterrorismo, ciber acoso y cibervenganza). Asimismo, en el estudio de Vargas y Vargas (2023), sobre el ciberdelito en Centroamérica y el Caribe, se destaca la principalidad de 11 ciberdelitos para cuya denominación ha sido necesario colocar el término directamente en inglés (e.g., *malaware*) o en español y en inglés (e.g., *grooming* o ciberengaño pederasta). Precisamente, en atención a posibles dificultades de comprensión, en el caso de la presente investigación, igualmente se decidió emplear dos términos con su respectiva traducción, ciberacoso personal (*bullying*) y ciberacoso laboral (*mobbing*), con el fin de reducir la probabilidad de desconocimiento por parte de las personas participantes en el estudio. La potabilización de una terminología predominantemente en inglés, amplia, que tiende a multiplicarse, además de ser redundante y cacofónica (debido al prefijo ciber), constituye un desafío actual para la comprensión y el estudio del cibercrimen en países de habla hispana.

10 AFE: KMO = .91, prueba de esfericidad de Bartlett con valor de p = .001, método de componentes principales y rotación Varimax.

do la taxonomía de Brar y Kumar (2018, p. 5), el segundo factor fue denominado "ciberfraude", por aglutinar el resto de los ítems que, precisamente, atañen a delitos relacionados con la obtención de ganancias por medio de engaños como son la estafa, el robo (de datos, de dinero o el hackeo de información), suplantación de identidad y clonación de tarjetas. Este factor complementa el 34 % de la varianza total de los resultados (69 %).

2.3. **Procedimiento**

Se elaboró una encuesta en línea identificada como "Inseguridad ciudadana y Cibercrimen". Las instrucciones generales y el vínculo de la encuesta fueron distribuidos por correo electrónico, entre contactos de los investigadores, con el fin de propiciar una dinámica de "bola de nieve". El avance del llenado condujo a mantener abierta la posibilidad de participar en el estudio durante dos meses, desde el 3 de mayo al 5 de julio de 2022. Las instrucciones solicitaban la participación de la persona receptora del correo, atendiendo a los criterios de inclusión establecidos, pero también anticipaba resguardos éticos importantes, tales como el anonimato, el uso estricto de los datos con fines académicos y la entera libertad de suspender el llenado del cuestionario en cualquier momento. Asimismo, antes de iniciar el cuestionario, se incluyó una pregunta cerrada de consentimiento informado (i.e., compresión del propósito del estudio). Al final solo un participante fue descartado debido a que optó por no participar más allá del consentimiento informado.

Sobre la pregunta abierta incluida al final del cuestionario, se encontró que 80 % de la muestra optó por no contestarla, el 15 % contestó cuestiones generales (e.g., expresó que no tenía nada que agregar, agradeció participar, etc.) y solo 5 % de las respuestas contenían algún comentario específico referido al cibercrimen[11]. En los apartados siguientes se consignan respuestas destacables de esta pregunta general. El cuestionario fue construido con Google Forms y los análisis fueron realizados con el programa SPSS v. 25.

11 A propósito del uso académico estricto de la información, es menester comentar que, debido a la situación política que experimenta el país, la que, entre otras cosas, vuelve sensible la indagación de aspectos problemáticos de la realidad nacional, también se aclaró en las instrucciones a los participantes que no tendrían que responder preguntas de tipo político. No obstante, en la pregunta abierta incluida en el cuestionario, un participante expresó que había notado la encuesta "muy política", "como en contra del GOES [gobierno de El Salvador]". Esta respuesta se explicaría por los sesgos políticos de la persona entrevistada, frente a una encuesta que explora un problema relevante en el país, antes que por el interés o el carácter político del instrumento creado.

3. **Resultados**

3.1. **La relación del miedo al cibercrimen con variables sociodemográficas y de percepción de inseguridad**

Los resultados muestran que la proporción de victimización por cibercrimen reportada por la muestra es apenas más alta (20 %) que la victimización por delincuencia común (16 %). Sobre el conocimiento de la victimización de otras personas (victimización vicaria), uno de cada dos participantes (51 %) dijo conocer a alguien allegado que había sido víctima de la ciberdelincuencia en el último año, pero esta proporción aumenta a 65 % en el caso de víctimas de delincuencia común. No obstante, solo el 33 % de la muestra opina que la delincuencia ha aumentado en el último año en contraste con dos terceras partes que sostuvieron que esta, en realidad, ha disminuido o se ha mantenido igual (67 %). Lo contrario aparece respecto a la ciberdelincuencia: dos terceras partes de la muestra sostuvieron que ha aumentado en el último año (64 %), contra el 36 % que opinó que ha disminuido o se ha mantenido invariable. A propósito, en la pregunta abierta, se encuentran declaraciones como las siguientes: “el cibercrimen ha aumentado”, “se está volviendo más común”, “no he sido victimizado, pero lo han intentado”, “perdí $50 dólares por ingresar en una página e ingresar el código de mi tarjeta”, “no fui victimizado en el último año, pero sí en el anterior” y “el aumento de estafas de dinero electrónicas han aumentado luego de la pandemia”.

En la tabla 1 se presentan los niveles de miedo al delito, miedo al cibercrimen y de empleo de recursos financieros electrónicos en función de las variables sociodemográficas y de percepción de inseguridad recién revisadas (victimización, victimización vicaria y opinión sobre el agravamiento de los fenómenos).

Tabla 1. Medias y desviaciones de las escalas de miedo al cibercrimen, miedo al delito y uso de recursos financieros, según variables sociodemográficas e indicadores de inseguridad

		Miedo al cibercrimen	Miedo al delito	Recursos financieros
Variables		**M(DE)**	**M(DE)**	**M(DE)**
TODOS/AS		**27.9 (8.3)**	**20.8 (6.8)**	**3.7 (1.9)**
Sexo	Masculino	25.9 (8.9)	18.9 (7.3)	4.2 (1.8)
	Femenino	29.3 (7.4)***	22.2 (6.0)***	3.3 (2.0)***
Edad	25 años o menos	29.0 (7.7)	22.6 (5.3)	3.0 (2.1)
	Más de 25 años	26.4 (8.7) **	18.3 (7.7)***	4.6 (1.3)***
Ocupación+	Solo trabaja	25.9 (8.6)	17.7 (7.9)	4.7 (1.2)
	Estudia y trabaja	28.7 (7.9) *	21.9 (6.0) *	3.4 (2.0) *
Victimización por delincuencia	Sí	29.5 (6.5)	22.6 (5.2)	3.7 (2.0)
	No	27.6 (8.5)	20.5 (7.0) *	3.7 (1.9)
Conoce víctimas de delincuencia	Sí	29.0 (7.3)	21.9 (5.9)	3.6 (1.9)
	No	25.8 (9.5) **	18.8 (7.8)***	3.8 (2.0)

		Miedo al cibercrimen	Miedo al delito	Recursos financieros
Variables		**M(DE)**	**M(DE)**	**M(DE)**
TODOS/AS		**27.9 (8.3)**	**20.8 (6.8)**	**3.7 (1.9)**
Situación del delito	Ha aumentado	29.9 (6.7)	21.9 (6.2)	3.5 (1.9)
	Ha disminuido o sigue igual	26.9 (8.7) **	20.3 (7.0) *	3.7 (2.0)
Victimización por ciberdelincuencia	Sí	29.7 (7.5)	21.5 (6.9)	4.1 (1.8)
	No	27.4 (8.4)	20.6 (6.8)	3.6 (2.0)
Conoce víctimas de ciberdelincuencia	Sí	29.4 (6.9)	21.2 (6.4)	3.9 (1.9)
	No	26.4 (9.2) **	20.4 (7.2)	3.4 (2.0) *
Situación del ciberdelito	Ha aumentado	28.9 (7.5)	21.0 (6.6)	3.9 (1.9)
	Ha disminuido o sigue igual	26.2 (9.2) **	20.6 (7.0)	3.3 (2.0) *

Nota: M = Media, DE = Desviación Estándar. Todos los análisis corresponden a pruebas t student de muestras independientes. + La categoría de ocupación "otros" (jubilados, desempleados, etc.) no ha sido considerada en los análisis por constituir un número marginal de la muestra. $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$.

Fuente: elaboración propia.

Como se aprecia en la tabla 1 el nivel de miedo al cibercrimen es alto, pues alcanza un promedio de casi 28 puntos, cuando el puntaje máximo de la escala es de 36. Algo similar ocurre con el miedo al delito (puntaje máximo de escala de 27 puntos) y, como se estableció anteriormente, las personas participantes reportaron utilizar un promedio cercano a los cuatro recursos financieros electrónicos.

Tanto el miedo al delito como al cibercrimen y el empleo de recursos financieros se encuentran mediados por algunas de las variables consideradas. Según los datos de la tabla 1, manifiestan estadísticamente más miedo al cibercrimen y al delito, en comparación con sus contrapartes: las mujeres, personas con menos de 25 años, quienes estudian y trabajan, quienes conocen a víctimas de delincuencia y quienes creen que el crimen común ha aumentado. Adicionalmente, experimentan niveles estadísticamente más altos de miedo al delito quienes han sido victimizados, así como de miedo al cibercrimen quienes conocen víctimas de ciberdelincuencia y que creen que el cibercrimen ha aumentado. Por último, el uso de recursos financieros electrónicos resultó estadísticamente mayor en hombres, entre quienes superan los 25 años, que trabajan, que conocen de casos de victimización por ciberdelincuencia y que consideran que este problema ha aumentado.

3.2. **Género y miedo al cibercrimen**

En la tabla 1 quedó establecido que las mujeres experimentan estadísticamente mayores niveles generales de miedo al cibercrimen y de miedo al delito[12]. En términos específicos, en lo que al miedo al delito se refiere, con excepción del temor al robo sin violencia (hurto) y la solicitud de soborno por una autoridad, el temor hacia los restantes siete delitos[13] consultados es estadísticamente mayor entre las mujeres que entre los hombres, destacando la máxima diferencia de medias en el miedo al delito de violación sexual (M = 1.68, DE = 1.2 para hombres y M = 2.63, DE = .80 para mujeres, $p < .001$). Por su parte, dicho miedo a la violación sexual presenta una correlación promedio de .68 con el acoso sexual en línea, el *ciberbullying* y el *cibermobbing*, y

12 Al contrastar las variables de inseguridad consideradas y el género, se encontró asociación entre ser mujer y la percepción de agravamiento de la delincuencia ($\chi 2$ [1, 315] = 8.765, p = .002) y de conocimiento de la victimización por delincuencia de otros ($\chi 2$ [1, 315] = 3.993, p = .030).

13 Como fue mencionado en el apartado de instrumento, por primera vez en el país se preguntó por el miedo a la desaparición. El 82 % de participantes manifestó mucho o algo de temor de llegar a ser desaparecido, 13 % dijo sentir algo de miedo y solo 5 % sostuvo que no temía nada sufrir una desaparición.

de .51 con el miedo a la extorsión de imágenes o información personal, mientras que las correlaciones promedio decaen a .38 con los restantes temores a los 8 cibercrímenes considerados[14].

Asimismo, y con significación estadística, las mujeres participantes en el estudio manifestaron mayor temor que los hombres al robo de datos personales (p = .02), a la extorsión con información o a través de imágenes personales (p = .003), al espionaje por parte de otros (p = .002) y a las tres formas de acoso consideradas (p =.001): sexual, personal (*bullying*) y laboral (*mobbing*). En otras palabras, con excepción del miedo al espionaje por parte del gobierno (p = .10), las mujeres presentan un miedo significativamente más alto que los hombres respecto al resto de delitos que conforman el primer factor identificado de la escala de miedo al cibercrimen y respecto al factor en su totalidad, que fue denominado invasión a la intimidad (M = 14.1, DE = 4.5 para mujeres y M = 11.2, DE = 5.5 para hombres, p < .001). Sobre esto, un comentario recogido en la pregunta abierta del cuestionario exponía que en el país "se experimentan graves crímenes a través de redes sociales (Reddit, Telegram, WhatsApp, Twitter, grupos de Facebook) donde contenido explícito no consentido de mujeres es intercambiado y filtrado". No se encontraron diferencias entre hombres y mujeres respecto al miedo a los distintos delitos aglutinados en el factor ciberfraude, ni respecto al factor como un todo (p = .26).

3.3. **Correlatos y predictores estadísticos del miedo al cibercrimen**

En la tabla 2 se aprecian las correlaciones entre las escalas y subescalas de los constructos principales. Existe una correlación significativa fuerte y positiva entre el miedo al delito y el miedo al cibercrimen (r = .79, p < .001). En cambio, no existe correlación entre el miedo al cibercrimen y el uso de recursos financieros (r = -.05, p = .38), mientras que la relación entre estos últimos y el miedo al delito es inversa (r = -.20, p < .001). Es decir, el miedo al delito incrementa en la medida en que se utilizan menos recursos financieros electrónicos.

Por otro lado, existen relaciones fuertes y positivas entre los dos factores del miedo al cibercrimen (invasión a la intimidad y ciberfraude), y entre estos y el miedo al delito, aunque la relación es más fuerte con el factor invasión a la intimidad (r = .81, p < .001). De manera interesante, los dos factores de la escala de recursos financieros –recursos financieros comunes y criptomonedas-remesas– no correlacionan entre sí. Luego, el factor criptomonedas-remesas no se relaciona con el miedo al delito ni con el miedo al cibercrimen o sus factores, pero el factor recursos financieros comunes sí correlaciona de forma inversa con la invasión a la intimidad (r = -.20, p < .001) y con el miedo al delito (r = -.23, p < .001).

14 p < .001, en todos los casos.

Tabla 2. Correlaciones entre escalas y subescalas principales

		(1)	(1.1)	(1.2)	(2)	(3)	(3.1)	(3.2)
(1)	Miedo al cibercrimen	-						
(1.1)	*Invasión a la intimidad*	.93 ***	-					
(1.2)	*Ciberfraude*	.88 **	.66 ***	-				
(2)	Miedo al delito	.79 ***	.81 ***	.60 ***	-			
(3)	Recursos-e	-.05	-.17 **	.12 *	-.20 ***	-		
(3.1)	*Rec. financieros comunes*	-.07	-.20 ***	.11	-.23 ***	.92 ***	-	
(3.2)	*Criptomonedas-remesas*	.07	.05	.09	.06	.40 ***	.08	-

Nota: $^{*}p < .05$, $^{**}p < .01$, $^{***}p < .001$
Fuente: elaboración propia.

Finalmente, se llevaron a cabo tres análisis de regresión lineal múltiple en los que las variables dependientes las constituyeron el miedo al cibercrimen y sus factores (invasión a la privacidad y ciberfraude). Las variables independientes en los modelos, surgen de las variables sociodemográficas y del resto de las mediciones asociadas a percepciones de inseguridad y el empleo de recursos electrónicos.

La tabla 3 muestra que los distintos modelos obtenidos explican, en promedio, casi el 60 % de la varianza del miedo al cibercrimen y sus dimensiones (59 % promedio de R^2 ajustada). Destacan el miedo al delito como el factor de mayor peso en los tres modelos (β promedio de .758), y la percepción de aumento del cibercrimen como variables predictoras comunes al miedo al cibercrimen y a sus dos dimensiones. Asimismo, el uso de recursos financieros comunes (banca en línea, cajeros, tarjeta de débito, etc.) aparece igualmente en los modelos de miedo al cibercrimen y su dimensión de ciberfraude. Ser mujer constituye un predictor significativo específico del factor invasión a la intimidad (β = -.081, p = .016), así como tener 25 años o más lo es del miedo al ciberfraude (β = -.107, p = .031).

Tabla 3. Regresión lineal múltiple para el miedo al cibercrimen y sus factores

	Cibercrimen	Ciberfraude	Invasión a la intimidad
Miedo al delito	.982 ***	.393 ***	.594 ***
	-.042	-.026	-.025
	.808	.679	.788
Cibercrimen ha aumentado	2.148 ***	.867 *	1.136 ***
	-.58	-.348	-.344
	.126	.107	.107
Recursos financieros comunes	.446 **	.438 ***	
	-.162	-.107	
	.096	.199	
Sexo (mujer)			-.839 *
			-.346
			-.081
Edad (25 años o más)		-.846 *	
		-.391	
		-.107	
N	315	315	315
R^2 Ajustado	.65	.44	.67

Nota: Se aplicó el método por pasos sucesivos (*Stepwise*). En cada celda se presentan tres cifras en vertical, en este orden: el coeficiente del modelo y su significación estadística, la desviación estándar en paréntesis y β. $^{*}p < .05$; $^{**}p < .01$; $^{***}p < .001$.

Fuente: elaboración propia.

4. **Discusión**

El avance imparable, rápido y global de la ciberseguridad y las ciberamenazas (UNODC, 2013, 2022; World Economic Forum, 2022) va concediendo notoriedad al miedo al cibercrimen entre la ciudadanía común. Tal inseguridad no solo remite a la preocupación por que un sistema informático de una empresa pueda llegar a sufrir perjuicios sino, además, conlleva el temor personal por el menoscabo de la integridad material o personal producida por medios electrónicos. No obstante, los estudios sobre miedo al cibercrimen aún son escasos (Brands y Van Doorn, 2022), lo que, como es de esperarse, suele ser más cierto en países en vías de desarrollo como El Salvador.

En este país, a su reconocida situación de inseguridad ciudadana, es menester ya sumar la experiencia del cibercrimen a distintos niveles (Jordán, 2022; UNODC, 2022; Vargas y Vargas, 2023), lo que incluye el miedo personal a llegar a ser víctima de estos. De esta manera, se constata el cumplimiento de los objetivos de investigación, al comprobar que las personas participantes han experimentado victimización y miedo al cibercrimen, así como que dicho temor se encuentra asociado con distintas variables relevantes, entre las que destacan el miedo al delito, el género y el empleo de herramientas financieras electrónicas.

Según los resultados obtenidos, una quinta parte de la muestra manifestó haber sido víctima de cibercrímenes, la mitad conoce a familiares o amigos que igualmente los han sufrido y algo más de seis de cada diez participantes consideró que el cibercrimen ha aumentado durante el año previo. También perciben más miedo al cibercrimen quienes conocen a víctimas de este y quienes consideran que su incidencia ha incrementado en el último año. La experiencia personal o vicaria, la resonancia social, así como la percepción de agravamiento del fenómeno, constituyen indicios inequívocos de la sobreexposición que existe en la actualidad al mundo virtual y, con ello, de la vulnerabilidad igualmente aumentada de victimización directa o del temor a sufrir el embate de este tipo de criminalidad (Henson et al., 2016; NortonLifeLock, 2021). Aunque la victimización constituye una variable que usualmente se encuentra asociada con la experiencia de miedo al crimen convencional y al cibercrimen (Adbulai, 2020; Lee, 2007; Virtanen, 2017), en este estudio el promedio de miedo al cibercrimen de quienes reportaron haber sido víctimas de cibercrimen fue más alto, pero no estadísticamente significativo (por muy poco, $p = .055$), lo que encontraría una explicación en el tamaño y composición particular de la muestra.

El vínculo entre contexto posibilitador, victimización y miedo al cibercrimen es coherente con el marco general de las teorías asociadas a las actividades rutinarias. Sucede que los estilos de vida y las actividades preponderantes actuales de las víctimas potenciales y las de los perpetradores, quizás, como nunca,

tienden a traslaparse entre sí gracias a la mayor o menor vulnerabilidad de las primeras y de las capacidades de adaptación de los segundos, en el marco de digitalización generalizada de la vida cotidiana de todas las personas (Henson, 2020; Herrero et al., 2021; Miró Llinares, 2021). Varios comentarios compartidos en la pregunta abierta del cuestionario mencionaron aspectos a medio camino entre los desafíos del contexto y las condiciones de vulnerabilidad asociadas a la manifestación de la cibercriminalidad, como la "falta de educación [de las personas o usuarios]", "poco interés sobre el tema", "poca denuncia [por parte de personas usuarias]", "cada vez [hay] más necesidad de hacer transacciones en línea" y que, por tanto, no queda otra alternativa que ser "cauteloso".

Este marco de referencia ayuda a explicar el miedo al cibercrimen que manifiestan ciertos segmentos de la muestra. Por ejemplo, el temor de quienes tienen menos de 25 años y estudian y trabajan por ser, presumiblemente, quienes tienen menos estatus económico o poder adquisitivo, al tiempo que tienden a conectarse con frecuencia por ocio y entretenimiento sin, necesariamente, tomar precauciones o contar con conocimientos suficientes sobre seguridad en la red (Kemp, 2022; UNODC, 2013; Vargas y Vargas, 2023; Virtanen, 2017). Por otro lado, también el miedo de quienes utilizan más recursos financieros en línea –hombres mayores de 25 años que trabajan– en cuanto que esta condición propendería a conocer víctimas de cibercrimen con recursos similares, así como considerar que el mismo ha aumentado.

De igual manera, manejar recursos financieros en línea –sobre todo comunes, como una tarjeta de débito– incrementa el miedo al ciberfraude, pero el empleo de estos recursos se asocia, a su vez, con un menor miedo al delito convencional y al miedo a cibercrímenes asociados a comportamientos de acoso, al espionaje o la exposición de imágenes personales. Este resultado encontraría su explicación en que el uso de recursos financieros es más alto en hombres mayores que trabajan. Estos, conforme aumenta su edad, tienden a alejarse de la demografía usual de la victimización por delincuencia común[15] y de la posibilidad de experimentar miedo por sufrir formas de ciberacoso. Cabe suponer que la experiencia de miedo y victimización por cibercrimen responde a procesos grupales dinámicos (Nurse y Bada, 2019), en los que víctimas y perpetradores interactúan entre sí –a veces inadvertidamente– hasta propiciar situaciones de mayor o menor vulnerabilidad (afinidad, exposición, acecho, etc.). Esto explica que, en la práctica, la incidencia del estatus socioeconómico sobre la victimización o el miedo al cibercrimen, como el de otras variables so-

15 La victimización por delitos comunes en El Salvador suele ser más alta en hombres que no superan los 30 años. Esto se corrobora en la actualidad, cuando mientras escribimos estas líneas, se encuentra vigente un régimen de excepción que, a base de medidas represivas y vulneración de derechos humanos, ha disminuido drásticamente el cometimiento de homicidios. No obstante, según el IUDOP (2022), son los hombres entre 18 y 25 años los que han experimentado más victimización durante el régimen de excepción aludido, pero ahora a manos de elementos policiales y militares.

ciodemográficas, arroje resultados mixtos según los énfasis particulares de cada investigación. Las variables que se emplean en las investigaciones corresponden a medidas aproximadas o construidas (e.g., estatus socioeconómico = ingreso o nivel de estudios), que se modulan entre sí (e.g., edad o género en relación con el poder adquisitivo) o que se analizan en función de ciertos tipos específicos de cibervictimización (e.g., Brands y Van Doorn, 2022; Brands y Van Wilsem, 2021; Guedes et al., 2022).

Si a la presencia del cibercrimen se suma un ambiente con altos niveles de crimen común, como es el caso de El Salvador, entonces cabe suponer la configuración de un ecosistema de inseguridad ciudadana generalizado, dado su potencial criminógeno (favorable al cometimiento y refuerzo mutuo de crímenes en línea y fuera de línea) y amedrentador (propicio para la producción de temor a llegar a ser víctima de ambas formas de criminalidad). En este marco de discusión cobra aún más sentido que la muestra participante manifieste altos niveles de miedo al cibercrimen y al delito convencional, y que ambos tipos de miedo se encuentren altamente correlacionados. Asimismo, que el miedo al delito sea el principal predictor del miedo al cibercrimen o que la percepción de empeoramiento del cibercrimen constituya un predictor común en los tres modelos de regresión obtenidos (ver tabla 3). No en vano un participante del estudio afirmó que “el crimen en un país tercermundista siempre estará presente”.

El miedo al cibercrimen se encuentra vinculado con variables usualmente asociadas al miedo al delito (Brands y Van Doorn, 2022). De hecho, ambos temores, además, modulan su intensidad -en los análisis bivariados- de acuerdo con variables similares como ser mujer, contar con menos de 25 años, estudiar y trabajar, tener conocimiento de víctimas de delincuencia y percibir que el crimen ha aumentado. Estos resultados son consistentes con varias fuentes (Bocij y McFarlane, 2003; Choi et al., 2022; Cross y Lee, 2022; Stickle y Felson, 2020; McLachlan y Harris, 2022) que sugieren o ratifican el desdibujamiento, o trasvase contemporáneo, entre el mundo criminal *online* y *offline*, y el potencial de los crímenes contemporáneos para encontrar formas de ejercicio gracias a y en cualquiera de los dos ámbitos. Asimismo, este trabajo coincide con el estudio de Guedes et al. (2022), en el que el miedo al cibercrimen –en este caso, específicamente el miedo al robo de identidad en línea– encuentra al miedo al delito como su predictor estadístico principal.

La presencia del uso de recursos financieros comunes en el modelo predictor general del miedo al cibercrimen, como en el modelo del factor de miedo al ciberfraude, remite a la modulación del temor debido al uso más frecuente de tales herramientas financieras. La edad –ser más joven–, por tanto, contrarresta tal posibilidad y, por ello, el miedo a esta forma de cibercrimen. Por otro lado, es conocido que las mujeres manifiestan mayor miedo al delito en general, en particular a los que atañen a expresiones diversas de violencia sexual (Jauregui y Vozmediano, 2021; Lee, 2007). Esta investigación ratifica tales resultados, pero además encuentra que dicho temor correlaciona especialmente con las distintas formas de ciberacoso consideradas y con la extorsión por medio de imágenes o de información personal. De hecho, el género constituye un predictor distintivo que se ve asociado específicamente al miedo a los cibercrímenes aglutinados en el factor denominado como invasión a la intimidad (ver tabla 3).

La investigación de Choi et al. (2022) encontró traslapes entre victimización sexual física y en línea, y un predictor común de estos crímenes en lo que denominaron "desorden escolar", es decir, la presencia de delincuentes, crímenes y lugares riesgosos en la institución. Significa que la posibilidad de convertirse en víctima o de experimentar miedo a cibercrímenes es especialmente elevada entre las mujeres, pero, además, que tal conciencia personal de vulnerabilidad y la exposición a potenciales daños no puede desligarse de aspectos contextuales que la posibilitan (i.e., confinamiento doméstico, brechas digitales) y/o la sancionan (i.e., roles y mandatos tradicionales, desbalance de poder) (Delgado et al., 2021; Hirigoyen 2010; Jauregui y Vozmediano, 2021). Esta discusión es especialmente relevante en un país como El Salvador, en el que la vulnerabilidad constituye una "condición ontológica compartida" (Santacruz Giralt, 2022, p. 120), donde fenómenos como los altos niveles de violencia física y sexual hacia la mujer, la impunidad y la reinvención constante de la criminalidad, se superponen en una sociedad cuya lúdica y galopante conectividad parece seguir una trayectoria inversa a su nivel de preparación, destreza y alfabetización digital colectiva ante el cibercrimen que ya mora, acecha y crece en su interior.

4.1. **Limitaciones y recomendaciones de la investigación**

La limitación principal de la investigación se encuentra en su muestra, ya que la misma no es de corte probabilístico, cuestión que impide que los resultados obtenidos puedan generalizarse a la totalidad de la población salvadoreña. No obstante, dicha condición apunta a vías de mejora para futuras investigaciones sobre el tema. Aunque una muestra representativa constituye una aspiración ideal para explorar distintas facetas de la inseguridad en muestras heterogéneas, los antecedentes bibliográficos y empíricos empleados en este trabajo respaldan y sugieren el estudio focalizado del cibercrimen, su victimización o sus miedos aparejados, con ciertas categorías o grupos específicos (Nurse y Bada, 2019), en los que se superpongan características demográficas (e.g. género) o la experiencia particular de procesos sociológicos o grupales de interés (e.g., violencia, discriminación, relación entre jóvenes y nuevas tecnologías). Así lo probaría el temor particular a cibercrímenes asociados a la invasión de la intimidad en mujeres o el mayor temor al ciberfraude, según el manejo de recursos financieros. Un participante en la investigación atinadamente sugería, dado que en este estudio participaron personas con 18 años o más, que sería relevante "conocer el punto de vista de menores de edad respecto al *sexting* y el conocimiento sobre el riesgo de soborno con material explicito (ya sea sexual o no) y sus peligros consecuentes". Asimismo, el estudio de la inseguridad ciudadana en El Salvador se desarrolla fundamentalmente a través de instrumentos estandarizados, por lo que tirar de la metodología cualitativa para atender los discursos y narrativas de la ciberinseguridad igual es una aspiración investigativa relevante.

Atendiendo al trabajo de Brands y Van Doorn (2022), igualmente convendría profundizar en el impacto que el cibercrimen tiene en hábitos y comportamientos sociales específicos. En buena medida, es en estos donde el carácter

subjetivo de la inseguridad cobra objetividad o donde la actitud se cristaliza en actos concretos (Guillén Lasierra, 2020; Orellana, 2022). Podrían ser de interés aquellos repertorios comportamentales colectivos que atañen a ocio, cuidado, consumo, pero también en lo relativo a estrategias precautorias, tanto en línea como fuera de línea, o en una combinación de ambas, dado el impulso que los dos ámbitos conceden a la victimización en la actualidad. Como complemento, el estudio del miedo al cibercrimen sugiere que no se puede perder de vista la comprensión del agente amedrentador, del cibercriminal, especialmente si este constituye una hibridación criminógena que, como cabe hipotetizar en el caso de países como El Salvador, posiblemente nutre su accionar de una sociedad precaria, impune, trasnacional y con conectividad creciente, a la que hace tiempo asola la inseguridad (UNODC, 2013, 2020).

Finalmente, en lo que al instrumento se refiere, siempre es recomendable el refinamiento de escalas de miedo y de victimización de cibercrímenes siguiendo clasificaciones comprehensivas disponibles (e.g., Brar y Kumar 2018) o en atención a la incidencia y evolución concreta del cibercrimen en la sociedad salvadoreña. En este esfuerzo no es ocioso enfatizar que el miedo al delito y el miedo al cibercrimen debe constituir siempre un análisis debidamente contextualizado, dadas las formas idiosincráticas que cada sociedad experimenta, padece o se resguarda de estos temores cotidianos (Ibrahim, 2016; Orellana, 2022).

5. Conclusiones

Dos grandes conclusiones generales pueden ser entresacadas a propósito de un fenómeno social sobre el que apenas se comienza a abrir brecha de conocimiento en el país:

La necesidad de considerar la cibercriminalidad como un problema de actualidad y de sofisticar constantemente la comprensión de la inseguridad ciudadana

Esta investigación abre brecha en el conocimiento del miedo al cibercrimen en personas salvadoreñas, pero también cabría pensar que los resultados y las reflexiones encuentran aplicabilidad, al menos, en países con contextos similares, como los del istmo centroamericano y otros países latinoamericanos en vías de desarrollo. Los resultados obtenidos demuestran que el cibercrimen y el temor que despierta esta faceta de la inseguridad ciudadana son una realidad presente en El Salvador.

El miedo al cibercrimen constituye una emoción que cobra sentido en contextos y grupos específicos, como lo demuestra el miedo al ciberfraude, sobresaliente en quienes gestionan recursos financieros en línea, y el miedo a la invasión a la intimidad en mujeres. Las personas participantes corroboran haber sido victimizadas, conocen acerca de experiencias de victimización de otras personas allegadas, perciben el agravamiento del fenómeno, así como experimentan miedo al cibercrimen. Las noticias que, día sí y día también, aparecen en los medios de comunicación, advirtiendo sobre la incidencia o el riesgo del cibercrimen, constatan la presencia cotidiana del cibercrimen en el país (Alfaro, 2022; Machuca, 2023).

Las manifestaciones, las características y la novedad de la cibercriminalidad muestran de forma diáfana que el estudio tradicional de la inseguridad ciudadana (i.e., encuesta de victimización e inseguridad exclusivamente enfocadas en el mundo *offline*) requiere atender al traslape, refuerzo y, por tanto, a la manifestación peculiar y combinada que en la actualidad exhiben el delito convencional y el cibercrimen, así como a sus temores aparejados. Estos, lamentablemente, han llegado para quedarse, de la mano de la inevitable digitalización creciente de las sociedades contemporáneas. En esta investigación se recogen trabajos que muestran la difuminación y refuerzo mutuo entre realidades criminógenas en línea y fuera de línea. También el papel crucial que juega el delito convencional para instigar el cibercrimen y, en consecuencia, el efecto recíproco que ocurre entre los miedos a ambas formas de criminalidad, fenómeno advertido ya hace una década atrás por la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC, 2013).

Orellana (2022) identifica cinco distorsiones o fallas epistemológicas en la conceptualización de la inseguridad ciudadana (tecnocratismo, ineficacia categorial, solipsismo securitario, animismo delictivo y ceguera heteronormativa). La discusión sobre el miedo al cibercrimen conduce a añadir una sexta distorsión conceptual: la *falacia de la desconexión*. Es decir, la pretensión de que la persona ciudadana se encuentra o vive desconectada, ajena a la digitalización contemporánea de la existencia y, por ende, que su temor a la violencia, a la delincuencia o las posibilidades de llegar a ser victimizada solo ocurren en el mundo "analógico", fuera de línea. Se trataría de una noción anacrónica en cuanto que responde a una concepción de la inseguridad ciudadana propia de un mundo pre-digital. Entre otras consecuencias, dicha falacia se verificaría en la omisión en los análisis de aspectos relevantes como: la conexión permanente de las personas (a redes sociales, telefonía, etc.), la reproducción de cotidianeidad en o gracias a medios digitales (educación, trabajo, comercio, cuidados) o que, en el caso de las encuestas al uso, aún se pregunte exclusivamente por la seguridad en el barrio, si las medidas de precaución que se toman son tangibles (e.g.: evitar lugares o contratar seguridad privada) o si se teme exclusivamente a posibles victimarios de carne y hueso.

Hace tiempo resulta cuestionable el carácter objetivo puro de la seguridad (i.e., responde a construcciones, intereses, etc.), como urgente resulta la necesidad de objetivar la seguridad subjetiva a través de sus manifestaciones e implicaciones concretas (Guillén Lasierra, 2020). De la misma manera, ya se vuelve menester romper con la dicotomía *online-offline* para acercarse a la criminalidad. Los indicios se encuentran ahí, como demuestran antecedentes, noticias y los mismos resultados de este estudio. En una encuesta representativa de personas salvadoreñas de 18 años o más, llevada a cabo por la extinta DIGESTYC (2018), se encontró que eran los cajeros automáticos de la vía pública los lugares en los que la gran mayoría de la población –7 de cada 10 personas, especialmente mujeres– se sentía más insegura. El cajero automático constituye un escenario cotidiano en el que el mundo en línea y fuera de línea se yuxtaponen. Si esta pregunta no hubiera sido incluida en la encuesta, se habría "descubierto" que son los buses y sus respectivas paradas los lugares de la vía pública que –nuevamente y como hace ratos sabemos– habrían "destacado" –otra vez– como los que más despiertan inseguridad en la población. El escudriñamiento apropiado de los entresijos de realidades complejas y escurridizas, como el cibercrimen, dependen de agudizar la observación de la realidad, actualizar las herramientas teóricas y de adecuar los dispositivos metodológicos y técnicos disponibles.

Las manifestaciones del miedo al cibercrimen ofrecen indicios para la formulación de políticas públicas

El crimen y la violencia convencionales, sus riesgos y consecuencias, no afectan de manera uniforme a la sociedad. Lo mismo cabe afirmar del cibercrimen y la ciberviolencia. Como lo demuestra este estudio, al menos cuatro constataciones sobre el miedo al cibercrimen pueden sugerir pistas para la formulación de políticas públicas en favor de los ciudadanos comunes.

a. El miedo al cibercrimen es más probable en la medida en que se teme por el delito convencional: significa que el diseño e implementación de polí-

ticas enfocadas en la contención de la delincuencia común conlleva una exigencia adicional hasta ahora no contemplada, ya que en la medida en que sus manifestaciones prosperan así lo hacen sus posibles mutaciones, mismas que pueden propender hacia la configuración objetiva y la experiencia de un medio social más peligroso, lo que incluye el mundo *on-line*. Quien teme al crimen, teme al cibercrimen. Contener el delito es, en alguna media, contener el ciberdelito. Lo inverso también sería cierto.

b. Los jóvenes temen más al cibercrimen en general, aunque temen menos a ciertos cibercrímenes específicos como el ciberfraude: que los jóvenes experimenten menos temor al ciberfraude, se encuentra asociado a que utilizan menos recursos financieros. Pero el cibercrimen no afecta solo atendiendo al poder adquisitivo ni solo genera menoscabos económicos. En general, cabe presumir que los jóvenes son quienes más tiempo permanecen conectados, de forma más intensa y a través de múltiples plataformas, sin que estos patrones de comportamiento conlleven necesariamente altos conocimientos de seguridad o la necesaria toma de precauciones ante las múltiples amenazas que ahora se ciernen en el ciberespacio. La digitalización de la sociedad requiere del Estado procurar la alfabetización temprana y permanente de la sociedad en materia digital y sobre los riesgos potenciales que se ciernen sobre ciertos grupos vulnerables (i.e., niños y niñas, adolescentes), debido a la gestión persistente de la cotidianeidad a través de dispositivos electrónicos.

c. El poder adquisitivo alimenta el miedo al ciberfraude: los resultados obtenidos hacen patente la relevancia de la educación financiera digital y que esta atañe tanto al conocimiento del manejo del dinero en sí como al de las herramientas electrónicas de mediación que ahora se requieren para su administración. Asimismo, delitos en línea como el ciberfraude subrayan la importancia del refinamiento constante de los mecanismos de control y seguridad de las entidades bancarias, así como de la necesidad de la sofisticación permanente de los sistemas de seguridad y justicia en materia de cibercrimen.

d. Las mujeres temen más por cibercrímenes referidos a la invasión a la intimidad: rémoras culturales como el machismo, la misoginia y el acoso encuentran un caldo de cultivo en el anonimato y masificación de la red. Quiere decir que la protección especial de niñas, adolescentes y mujeres, quienes tradicionalmente temen y sufren en el mundo concreto formas de victimización como las apuntadas, amerita una atención especial. Son ellas quienes igualmente más acusan las brechas digitales –de acceso, uso y formación y, por tanto, presumiblemente también de competencia y confianza– que amplifican su riesgo de victimización por medios informáticos. En este cometido, es menester considerar las "asimetrías digitales" que, paradójicamente, parecieran cerrar las brechas digitales aludidas (e.g., mayor participación en la realización de gestiones bancarias, llamadas por internet) pero que, no obstante, podrían conducir al incremento de la carga de cuidados y, con ello, a la sobreexposición riesgosa a distintas formas de victimización en línea (Velásquez et al., 2021, p. 30; Vera Morales, 2021;

ONU Mujeres, 2021). No debe perderse de vista que existe evidencia que muestra que, en El Salvador, así como en distintos países de la región, el ciberacoso figura como uno de los cibercrímenes más frecuentes (Vargas y Vargas, 2023). El conocimiento progresivo sobre la manifestación y los temores aparejados al cibercrimen aún está por revelar las formas en que estos acechan interseccionalmente en El Salvador, es decir, a partir de la superposición e interacción compleja y dinámica de distintos contextos y facetas de las personas (e.g., género, edad, extracción social, competencias digitales) que las vuelven más o menos vulnerables al embate de esta forma de inseguridad ciudadana.

6. **Referencias**

Abdulai, M. A. (2020). Examining the Effect of Victimization Experience on Fear of Cybercrime: University Students' Experience of Credit/Debit Card Fraud. *International Journal of Cyber Criminology, 14*(1), 157–174. https://doi.org/10.5281/zenodo.3749468

Alfaro, K. (2022, 16 de septiembre). El Salvador enfrentó 206,000 ataques cibernéticos en 2021. *La Prensa Gráfica* https://www.laprensagrafica.com/economia/El-Salvador-enfrento-206000-ataques-ciberneticos-en-2021-20220915-0058.html

Arroyo Guardeño, D., Gayoso Martínez, V. y Hernández Encinas, L. (2020). *Ciberseguridad*. CSIC y Los Libros de La Catarata.

Beck, U. (2008). *La sociedad del riesgo mundial. En busca de la seguridad perdida.* Paidós Ibérica.

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

Brands, J. y Van Doorn, J. (2022). The measurement, intensity and determinants of fear of cybercrime: A systematic review. *Computers in Human Behavior*, 127, 107082. https://doi.org/10.1016/j.chb.2021.107082

Brands, J. y Van Wilsem, J. (2021). Connected and fearful? Exploring fear of online financial crime, Internet behaviour and their relationship. *European Journal of Criminology,* 18(2), 213–234. https://doi.org/10.1177/1477370819839619

Brar, H. S. y Kumar, G. (2018). Cybercrimes: A proposed taxonomy and challenges. *Journal of Computer Networks and Communications*, 1798659, 1-11. https://doi.org/10.1155/2018/1798659

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

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

Centro de Estudios de Opinión Pública [CEOP]. (2022). *Evaluación de la gestión gubernamental y temas de actualidad del 2022.* Boletín temático-septiembre https://www.fundaungo.org.sv/products/evaluacion-de-la-gestion-gubernamental-y-temas-de-actualidad-del-2022/770

Choi J., Dulisse, B. y Han, S. (2022). Assessing the Overlap between Cyberstalking Victimization and Face-to-face Sexual Victimization among South Korean Middle and High School Students, *Victims & Offenders*, 17(5), 660-678. https://doi.org/10.1080/15564886.2022.2029785

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

Cross, C. y Lee, M. (2022). Exploring Fear of Crime for Those Targeted by Romance Fraud, *Victims & Offenders,* 17(5), 735-755. https://doi.org/10.1080/15564886.2021.2018080

Delgado, M., Portillo, V. y Quintanilla, A. (2021). *El contínuum de la violencia sexual contra las mujeres en El Salvador: identificación de los factores que la determinan y sus impactos en las mujeres jóvenes de 15 a 29 años.* FUNDAUNGO. https://bit.ly/3CxXWc6

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/

Dirección General de Estadística y Censos [DIGESTYC]. (2018). *Encuesta de Victimización y Percepción de Inseguridad / Encuesta de Cultura de Paz.* https://infosegura.org/2019/04/10/encuesta-de-victimizacion-y-percepcion-de-inseguridad-encuesta-de-cultura-de-paz/

Dirección General de Estadística y Censos [DIGESTYC]. (2021). *Encuesta de Hogares de Propósitos Múltiples.* https://www.bcr.gob.sv/documental/Inicio/vista/PUBLICACION_EHPM_2021.pdf

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. (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

Guillén Lasierra, F. (2020). La falacia de la seguridad objetiva y sus consecuencias. *International e-Journal of Criminal Sciences, 15,* 1-28. https://ojs.ehu.eus/index.php/inecs/article/view/21484

Guedes, I., Martins, M. y Cardoso, C. F. (2022). Exploring the determinants of victimization and fear of online identity theft: an empirical study. *Security Journal.* https://doi.org/10.1057/s41284-022-00350-5

Hirigoyen, M. (2010). *El acoso moral: El maltrato psicológico en la vida cotidiana* (16a Reimp.). Paidós.

Henson, B. (2020). Routine Activities. En J. H. Thomas y A. M. Bossler. (Eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 469-489). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3

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

Herrero, J., Torres, A., Vivas, P., Hidalgo, A., Rodríguez, F.J., y Urueña, A. (2021). Smartphone Addiction and Cybercrime Victimization in the Context of Lifestyles Routine Activities and Self-Control Theories: The User's Dual Vulnerability Model of Cybercrime Victimization. *Int. J. Environ. Res. Public Health*, 18, 3763. https://doi.org/10.3390/ijerph18073763

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44-57. http://dx.doi.org/10.1016/j.ijlcj.2016.07.002

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

Jauregui, C. y Vozmediano, L. (2021). Miedo al delito experimentado por las mujeres: relevancia de una perspectiva centrada en el contexto. *International e-Journal of Criminal Sciences*, *16*, 1-23. https://ojs.ehu.eus/index.php/inecs/article/view/23420

Jordán, L. (2022, 2 de marzo). Delitos informáticos incrementaron hasta siete veces en el último año en El Salvador. *La Prensa Gráfica*. https://www.laprensagrafica.com/elsalvador/Delitos-informaticos-incrementaron-hasta-siete-veces-en-el-ultimo-ano-en-El-Salvador-20220301-0086.html

Kemp, S. (2022). *Digital 2022: El Salvador report*. https://datareportal.com/reports/digital-2022-el-salvador

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

Leone, M. S. y Caballero, S. (2021). Estudios feministas de seguridad y ética del cuidado: la seguridad en Latinoamérica a raíz de la pandemia. *URVIO, Revista Latinoamericana de Estudios de Seguridad, 31*, 43-61. https://doi.org/10.17141/urvio.31.2021.4989

Machuca, E. (2023, 30 de mayo). Abansa advierte sobre fraudes cibernéticos. *La Prensa Gráfica*. https://www.laprensagrafica.com/economia/Abansa-advierte-sobre-fraudes-ciberneticos-20230529-0072.html

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

Marín-Cortés, A. y Linne, J. (2020). Una revisión sobre emociones asociadas al ciberacoso en jóvenes adultos. *Psicoperspectivas, 19*(3), 1-16. https://dx.doi.org/10.5027/psicoperspectivas-vol19-issue3-fulltext-1824

McLachlan, F. y Harris, H. (2022). Intimate Risks: Examining Online and Offline Abuse, Homicide Flags, and Femicide, *Victims & Offenders*, *17*(5), 623-646. https://doi.org/10.1080/15564886.2022.2036658

Molina, K. (2023, 22 de julio). El Salvador ha recibido 24 millones de intentos de ciberataque. *La Prensa Gráfica*. https://www.laprensagrafica.com/economia/El-Salvador-ha-recibido-24-millones-de-intentos-de-ciberataque-20230721-0081.html

Morillo Puente, S., y Ríos Hernández, I. N. (2022). Cyber victimization within the Routine Activity Theory Framework in the Digital Age. *Revista de Psicología, 40*(1), 265-291. http://dx.doi.org/10.18800/psico.202201.009

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

NortonLifeLock. (2021). *2021 Norton Cyber Safety Insights Report: Global Results.* https://bit.ly/3xWjT1M

Nurse, J. R. C. y Bada, M. (2019). The Group Element of Cybercrime: Types, Dynamics, and Criminal Operations. En A. Attrill-Smith, C. Fullwood, M. Keep y D. J. Kuss. (Eds.). *The Oxford Handbook of Cyberpsychology* (pp. 691-716). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780198812746.013.36

Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC). (2013). E*studio exhaustivo sobre el delito cibernético.* https://bit.ly/2KTTBUu

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

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

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

Payne, B. L. (2020). Defining Cybercrime. En J. Holt Thomas y A. M. Bossler. (Eds.). *The Palgrave Handbook of International Cybercrime and Cyberdeviance* (pp. 3-26). Palgrave Macmillan. https://doi.org/10.1007/978-3-319-78440-3

Rodríguez, J., Oduber, J. y Mora, E. (2017). Actividades Rutinarias y Cibervictimización en Venezuela. URVIO. *Revista Latinoamericana De Estudios De Seguridad, 20*, 63-79. https://doi.org/10.17141/urvio.20.2017.2583

Santacruz Giralt, M. (2022). Investigar sobre vulnerabilidad y sufrimiento en un espacio-tiempo singular. Comentario sobre la investigación "COVID-19 y violencia estructural". *ECA: Estudios Centroamericanos*, *77*(770), 89–101. https://doi.org/10.51378/eca.v77i770.7598

Secretaría de Innovación de la Presidencia (2021). *Política de ciberseguridad de El Salvador.* https://bit.ly/3ViEEyX

Stickle, B. y Felson, M. (2020). Crime Rates in a Pandemic: The Largest Criminological Experiment in History. *American Journal of Criminal Justice, 45,* 525-536. https://doi.org/10.1007/s12103-020-09546-0

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

Vargas, P. y Vargas, K. (2023). *Ciberdelito en Centroamérica y el Caribe.* Red CONOSE https://redconose.org/2023/08/09/el-ciberdelito-en-centroamerica-y-el-caribe/

Velásquez, A., Cisneros, G., y Gil, L. (2021). *Inclusión digital y desigualdad social en El Salvador. Una aproximación a las brechas por ingresos, género, área geográfica y edad en el acceso, el uso y la apropiación del internet, como una de las tecnologías digitales básicas en la era de la cuarta revolución tecnológica.* Laboratorio de Investigación para el Desarrollo Internacional.

Vera Morales, K. N. (2021). *La ciberseguridad de las mujeres durante la pandemia del COVID-19: experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital. Organización de los Estados Americanos (OEA).* https://www.oas.org/es/sms/cicte/docs/Ciberseguridad-de-las-mujeres-durante-COVID-19.pdf

Virtanen, S. M. (2017). Fear of cybercrime in Europe: Examining the effects of victimization and vulnerabilities. *Psychiatry, Psychology and Law, 24*(3), 323-338. https://doi.org/10.1080/13218719.2017.1315785

Wijayanto, H., y Prabowo, I. A. (2020). Cybersecurity Vulnerability Behavior Scale in College During the Covid-19 Pandemic. *Jurnal Sisfokom (Sistem Informasi dan Komputer)*, *9*(3), 395-399. https://doi.org/10.32736/sisfokom.v9i3.1021

World Economic Forum. (2022). *The Global Risks Report 2022* (17th Ed.) https://www.weforum.org/reports/global-risks-report-2022

7. **Sobre los autores**

Carlos Iván Orellana. Salvadoreño.

Doctor en Ciencias Sociales por la Facultad Latinoamericana de Ciencias Sociales (FLACSO-Centroamérica). Investigador social y profesor de la Universidad Don Bosco (UDB) de El Salvador. Codirector de los programas de Doctorado y Maestría en Ciencias Sociales en cotitulación con la Universidad Centroamericana José Simeón Cañas UCA y la UDB. Editor de la Revista de Ciencias Sociales y Humanidades de la UDB, Teoría y Praxis. ORCID: https://orcid.org/0000-0002-4936-867X. Correo electrónico: ivan.orellana@udb.edu.sv

Adilio Carrillo. Salvadoreño.

Abogado, Maestro en Ciencia Política y con estudios en Seguridad y Desarrollo Nacional por el Colegio de Altos Estudios Estratégicos de la Fuerza Armada de El Salvador (FAES). Fue Director Regional de la Coalición Centroamericana para la Prevención de la Violencia Juvenil (CCPVJ). Se desempeñó como analista del Instituto Universitario de Opinión Pública (IUDOP) de la UCA de El Salvador. Actualmente es profesor e investigador del Departamento de Sociología y Ciencias Políticas de la UCA. ORCID: https://orcid.org/0000-0002-1956-1137. Correo electrónico: acarrillo@uca.edu.sv

El miedo al cibercrimen: explorando una faceta novedosa de la inseguridad ciudadana

Personas autoras: Carlos Iván Orellana y Adilio Carrillo

Considerando que la investigación descansa en el empleo de una encuesta en línea, los objetivos de la presente investigación son cinco: primero, describir la victimización, la victimización vicaria (conocimiento de la victimización de otros) y la percepción de agravamiento de la inseguridad (delito y cibercrimen) por parte de los participantes en el estudio; segundo, establecer el nivel de miedo al cibercrimen en la muestra participante; en tercer lugar, determinar la relación de este miedo con variables sociodemográficas, recursos financieros electrónicos y el miedo al delito; cuarto, explorar la existencia de temores a cibercrímenes específicos según el género; por último, en quinto lugar, elaborar un modelo predictor del miedo al cibercrimen con las variables consideradas.

conose
RED DE CONOCIMIENTO SOBRE SEGURIDAD CIUDADANA

infoSEGURA

USAID
DEL PUEBLO DE LOS ESTADOS UNIDOS DE AMÉRICA

PNUD

ISBN: 978-9977-68-353-9