Rev. Crim. / Volumen 64 - Número 3 - Septiembre-Diciembre 2022 - pp. 95-116 - ISSN 1794-3108 https://doi.org/10.47741/17943108.368

Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos?

Cybercrime in Colombia: how efficient has the Computer Crime Law been?

Cibercrime na Colômbia: qual tem sido a eficácia da Lei de Crimes Informáticos?

Fecha de recepción: 2022/01/26 I Fecha de evaluación: 2022/03/16 I Fecha de aprobación: 2022/07/30

Jaime Andrés Rincón Arteaga
Máster of Business Administration
Director de Gestión Operativa y de Seguridad
Asociación Bancaria y de Entidades Financieras de Colombia – Asobancaria
Bogotá, Colombia
jrincon@asobancaria.com

Santiago Armando Castiblanco Hernández
Profesional en Finanzas
Profesional Junior de la Dirección de Gestión Operativa y de Seguridad
Asociación Bancaria y de Entidades Financieras de Colombia – Asobancaria
Bogotá, Colombia
scastiblanco@asobancaria.com

Andrés Quijano Díaz
Máster of Business Administration
Profesional Senior de la Dirección de Gestión Operativa y de Seguridad
Asociación Bancaria y de Entidades Financieras de Colombia – Asobancaria
Bogotá, Colombia
andres.quijano@uexternado.edu.co

Juan David Urquijo Vanegas
Magister (c) en Economía Aplicada
Profesional Junior de la Dirección de Gestión Operativa y de Seguridad
Asociación Bancaria y de Entidades Financieras de Colombia – Asobancaria
Bogotá, Colombia
jurquijo@asobancaria.com

Yuliana Katherine Pregonero León
Profesional en Negocios Internacionales
Profesional Junior de la Dirección de Gestión Operativa y de Seguridad
Asociación Bancaria y de Entidades Financieras de Colombia – Asobancaria
Bogotá, Colombia
ypregonero@asobancaria.com

Para citar este artículo / To reference this article / Para citar este artigo: Rincón, J., Quijano, A., Castiblanco, S., Urquijo, J., & Pregonero, Y. (2022). Ciberdelincuencia en Colombia: ¿qué tan eficiente ha sido la Ley de Delitos Informáticos? *Revista Criminalidad, 64*(3), 95-116. https://doi.org/10.47741/17943108.368

Resumen

Este documento está centrado en determinar qué variables afectan los incentivos que tienen los delincuentes al cometer sus ciberdelitos, e identificar si la legislación actual está diseñada teniendo en cuenta la tipificación de las conductas y las herramientas de los entes encargados de capturar los criminales. Se busca entender los principales factores que incentivan la ciberdelincuencia en el país, teniendo en cuenta el contexto de la ciberdelincuencia para el 2019 en Colombia, y con ello, el comportamiento de los delincuentes informáticos en la prepandemia. Con la Ley 1273 de 2019, encargada de tipificar los delitos informáticos en Colombia, se revisarán los datos reportados de delitos informáticos y se compararán con los casos e indicadores de delitos de hurto calificado, con el fin de determinar la relación de estos dos delitos, que son relevantes para las entidades y han sido interiorizados por las entidades policivas en su estudio y lucha anticriminal desde hace mucho tiempo. Una vez definida teóricamente la eficiencia de las entidades apoderadas en la lucha contra los delitos informáticos, se propone una función de beneficios económicos de la ciberdelincuencia adaptada para el caso colombiano, determinando las variables que mejor explican esta función. Al final de este ejercicio académico, mediante un análisis de sensibilidad, se señala qué aspectos de política pública se deben considerar como prioritarios, teniendo en cuenta los incentivos económicos para los ciberdelincuentes y la efectividad de la Ley 1273 de 2009.

Palabras clave

Delitos informáticos, criminalidad mediante computadoras, políticas públicas, seguridad informática (fuente: Tesauro Criminológico - Instituto Interregional de las Naciones Unidas para la Investigación sobre la Delincuencia y la Justicia - UNICRI). Hurto calificado, función de beneficios, ciberdelincuencia (fuente: autores).

Abstract

This paper is focused on determining which variables affect the incentives that criminals have when committing cybercrime, and identify whether the current legislation is designed taking into account the criminalization of behaviors and the tools of the entities in charge of catching criminals. It seeks to understand the main factors that encourage cybercrime in the country, taking into account the context of cybercrime for 2019 in Colombia, and with it, the behavior of cybercriminals in the pre-pandemic. With Law 1273 of 2019, in charge of criminalizing computer crimes in Colombia, the reported data of computer crimes will be reviewed and compared with the cases and indicators of qualified theft crimes, in order to determine the relationship of these two crimes, which are relevant for the entities and have been internalized by the police entities in their study and anti-crime fight for a long time. Once the efficiency of the entities empowered in the fight against cybercrime has been theoretically defined, a function of economic benefits of cybercrime adapted to the Colombian case is proposed, determining the variables that best explain this function. At the end of this academic exercise, through a sensitivity analysis, it is pointed out which aspects of public policy should be considered as a priority, taking into account the economic incentives for cybercriminals and the effectiveness of Law 1273 of 2009.

Key words

Computer crime, computer related crime, public policy, computer security (source: criminological thesaurus - United Nations Interregional Crime and Justice Research Institute- UNICRI). Qualified theft, benefit function, cybercrime (source: authors).

Resumo

Este documento está focado em determinar quais variáveis afetam os incentivos que os criminosos têm quando cometem crimes cibernéticos, e identificar se a legislação atual é elaborada levando em conta a classificação dos comportamentos e as ferramentas das entidades encarregadas de capturar os criminosos. Ela procura compreender os principais fatores que incentivam o cibercrime no país, levando em conta o contexto do cibercrime para 2019 na Colômbia, e com ele, o comportamento dos cibercriminosos na pré-pandemia. Com a Lei 1273 de 2019, encarregada de criminalizar os crimes cibernéticos na Colômbia, os dados comunicados de crimes cibernéticos serão revistos e comparados com os casos e indicadores de crimes de roubo, a fim de determinar a relação entre esses dois crimes, que são relevantes para as entidades e foram internalizados por entidades policiais em seu estudo e combate aos crimes por um longo tempo. Uma vez definida teoricamente a eficiência das entidades habilitadas na luta contra o crime cibernético, propõe-se uma função dos benefícios econômicos do crime cibernético adaptada ao caso colombiano, determinando as variáveis que melhor explicam esta função. Ao final deste exercício acadêmico, por meio de uma análise de sensibilidade, indica-se quais aspectos das políticas públicas devem ser considerados prioritários, levando em conta os incentivos econômicos para os cibercriminosos e a eficácia da Lei 1273 de 2009.

Palavras-chave

Crimes informáticos, crimes informáticos, políticas públicas, segurança informática (fonte: Thesaurus Criminológico - Instituto Inter-regional de Pesquisa em Crime e Justiça das Nações Unidas - UNICRI). Roubo qualificado, função de benefício, cibercrime (fonte: autores).

Introducción

La ciberdelincuencia es uno de los principales retos de la economía en la actualidad. Para la primera mitad del 2020, se originaron alrededor de 73 millones de ciberataques solo en Latinoamérica, mientras que a nivel global el costo de una filtración de datos se estima en 3.86 millones de dólares. Además, el 37% de ejecutivos y directores generales consideran el área de ciberseguridad como una de las más importantes para liderar el crecimiento en sus compañías, con un porcentaje que incrementa en 67% para aquellos que forman parte del sector financiero.

En el sector financiero, al manejar fondos e información privada de millones de personas, es uno de los principales objetivos de estos criminales. Con base en esto, es necesario que las entidades financieras, usuarios y agencias estatales apliquen e implementen mecanismos para combatir estos delitos.

Uno de los principales retos al enfrentar la ciberdelincuencia es la naturaleza del crimen (uso

de herramientas tecnológicas que se renuevan constantemente); existe desconocimiento en la rama judicial y policíal del marco legal que tipifica estos crímenes. De esta manera, no todos los fiscales y jueces tienen el conocimiento o la formación adecuada sobre ciberdelincuencia, a pesar de que el Código Penal colombiano (Congreso de Colombia, 2009), tipifique los delitos informáticos en en el país.

En este estudio se asume que esta falta de eficiencia por parte de la justicia puede actuar en favor de la función de beneficio percibida por el criminal, aclarando que esto dependerá de la concavidad de la función de utilidad, además del grado de aversión al riesgo que el delincuente puede tener.

Las posibles ganancias que pueden llegar a tener los ciberdelincuentes están condicionadas a la cantidad de ataques que perpetúan; a la cantidad de usuarios a los que pueden llegar a afectar; los fondos que manejan estos usuarios en sus productos financieros, y por supuesto, al costo percibido dada la condena que tendrían en caso de ser atrapados. Esta última, se utiliza como *proxy* para medir la percepción de la eficacia del sistema judicial, usando la probabilidad de ser capturado por las entidades judiciales o policiales al cometer estos crímenes, junto con el castigo que recibirían en caso de ser capturados.

A raíz de la pandemia de COVID-19, se comprobó —aún más— la importancia de las tecnologías de la información en un mundo globalizado; a su vez, puso de manifiesto el papel fundamental que juegan los ambientes ciberseguros, en los que los usuarios puedan utilizar los servicios financieros sin temor a ser atacados. Tema de particular relevancia, si se tiene en cuenta el aumento de noticias sobre ataques y estafas que buscan engañar a las personas para que entreguen sus datos personales, a cambio de recibir ayudas o descuentos en el marco de la crisis económica provocada por la pandemia.

Teniendo en cuenta el desarrollo tecnológico y, del mismo modo, el aumento de ciberdelincuencia en Colombia, ¿de qué manera el país puede hacer más eficiente los procesos judiciales sobre los actos delictivos en tecnología?

Con este estudio, se busca estimar la tasa de efectividad de la Ley 1273 de 2009 (Congreso de Colombia, 2009) (ley que no ha tenido ninguna modificación durante los más de diez años que ha estado en vigor), así como un posible rango de ganancias percibidas por los ciberdelincuentes y hacer una aproximación de qué dependen sus variaciones.

De esta manera, se podrán aportar datos que permitan, por medio de los resultados, proponer sugerencias o medidas sobre cómo hacer más eficientes los actuales mecanismos y tácticas de disuasión, con los que cuenta el país para combatir a este tipo de delitos. Por ello, se establecen diversos *objetivos* centrados en identificar los principales factores que incentivan la ciberdelincuencia con la evaluación de la eficacia de la Ley 1273 en Colombia; estos dos últimos objetivos se centran en resolver las incógnitas en el contexto de la ciberdelincuencia y la prepandemia del 2019 en Colombia.

Hipótesis

La tasa de efectividad de la Ley 1273 de 2009 —entendida como la relación entre el número de capturas efectuadas por delitos informáticos y la cantidad de denuncias por estos delitos— es menor a la tasa de efectividad de delitos similares. Para demostrarlo, se compararán las denuncias y capturas relacionadas con delitos informáticos con las realizadas por hurto agravado.

Además, esta tasa no está correlacionada con factores como población, inclusión financiera y el índice de desarrollo humano (IDH), dado un análisis regional; por tanto, deben ser otros factores difíciles de medir (como la solidez interinstitucional) los que se correlacionan con la eficiencia de la gestión institucional para combatir el ciberdelito.

A partir de la percepción de una baja tasa de capturas por estos delitos, el ciberdelincuente llega a considerar el costo del delito alrededor de 0, por lo que ser ciberdelincuente sería rentable, y las ganancias por realizar ataques de *phishing/smishing* a clientes del sistema bancario colombiano pueden, en la mayoría de los casos, ser mayores a 0.

Revisión de literatura

Para llevar a cabo este estudio, se revisaron diferentes publicaciones relacionadas con los delitos informáticos, y se encontraron ejes temáticos que sirven como fuente para su desarrollo. Entre los diversos temas considerados, se encuentran enfoques económicos del comportamiento del ciberdelincuente, el marco legal penal existente en Colombia en materia de delitos informáticos, la efectividad de los ataques de *phishing*, promedios de ciberataques en diferentes países e industrias, y los costos del cibercrimen.

El estudio "*Phishing: An economic analysis of cybercrime perpetrators*", es uno de los principales insumos de este estudio, al realizar un

análisis económico del comportamiento de los ciberdelincuentes y su percepción de las posibles ganancias y contramedidas al efectuar estas actividades (Konradt et al., 2016).

En esta publicación, los autores proponen una función de beneficios para un ciberdelincuente que ejecuta ataques de *phishing*. Al tomar esta función de beneficios y utilizar datos del cibercrimen en Colombia, se espera tener una mayor perspectiva cuantificable del efecto del marco legal vigente en la toma de decisiones del ciberdelincuente colombiano.

De esta forma, es difícil calcular cuántos ciberataques y medir cuántas cuentas terminaron afectadas, por lo cual es una limitación en esta investigación. Sin embargo, se analiza la naturaleza del delito, por el subregistro y porque no todos los ataques acaban estafando a los usuarios, y no todos los usuarios defraudados denuncian ante una entidad judicial o policial. Según el *Internet Crime Report*, en los últimos cinco años, Estados Unidos ha recibido, en promedio, 340.000 denuncias por año; estas denuncias abordan una amplia gama de estafas en internet que afectan a las víctimas durante todo el año (Internet Crime Complaint Center (IC3); 2019).

Respecto a los ciberataques, de acuerdo con el artículo Países de América Latina y el Caribe más atacados por ataques de *phishing* en 2020", el 20.61% de los usuarios de Kaspersky en Colombia fueron atacados con *phishing* en el 2019. A partir de la información del Banco Mundial y según el Censo Nacional de Población y Vivienda del 2018, se estima que estos ataques representan alrededor de 6.618.311 personas[1] en Colombia (Statista, 2019).

Otro aporte tenido en cuenta es el estudio de "Estado de la ciberseguridad en el sistema financiero colombiano". Indica que, mediante encuestas anónimas a entidades financieras y a usuarios financieros de Colombia, brinda información sobre eventos o incidentes de seguridad de la información del sistema financiero colombiano. Además, uno de los hallazgos es el porcentaje de usuarios financieros que luego de sufrir un incidente de seguridad informan a las autoridades que han sido afectados, el cual es solo del 26% para el 2019 (OEA, 2020).

Al comparar el número de cuentas atacadas entre la información pública de la Fiscalía General de la Nación sobre el número de denuncias y el porcentaje de denuncias calculado en el estudio de la Organización de los Estados Americanos (OEA) con el de incidentes de seguridad estimado a partir de la información del DANE (2020), Banco Mundial y Statista, es posible hallar una razón de cuán exitoso puede ser un ataque de *phishing*.

Una de las principales variables para considerar en el estudio, son las ganancias que pueden obtener los ciberdelincuentes al defraudar una cuenta. Si bien se encontraron diferentes rangos de ganancias, según el objeto de estudio, se observa que en cualquier caso las ganancias de estas actividades son altamente rentables. En el informe "Understanding the cost of cybercrime", se encuentra que mientras los vendedores que ofrecen datos de tarjetas de crédito y débito pueden ganar entre £ 4,000 y £ 16,000 al precio mínimo, los compradores de estos datos financieros robados pueden ganar entre £ 6.1 millones y £ 25.2 millones, dependiendo de cuántas de las cuentas estuvieran activas si se compraron en lotes de 50 grupos de datos de cuentas (Home Office, 2018).

El estudio "Measuring the cost of cybercrime" se centra en el análisis de datos para el Reino Unido; indica que los diferentes costos que genera el cibercrimen en la sociedad y en las empresas, los costos de defensa o de prevención pueden compararse con las pérdidas reales. Sin embargo, aquellos costos indirectos (pérdidas y costos de oportunidad impuestos a la sociedad por el hecho de que se lleve a cabo un determinado ciberdelito independientemente de que tenga éxito o no) en los que incurren las empresas por temor al fraude, tanto para consumidores como para comerciantes, son varias veces superiores (Anderson, 2012).

En el caso colombiano, el informe "Costos del cibercrimen en Colombia 2016-2017", del Centro Cibernético Policial, encontró que para el 2017, las ganancias asociadas a las estafas mediante compras *on-line* oscilan entre $30.000 y $300.000, y las asociadas al *phishing* (suplantación de páginas bancarias o de gobierno) oscilan entre $200.000 y $50.000.000, dependiendo de la cantidad de dinero que las víctimas tengan en sus cuentas bancarias o el monto de su tarjeta de crédito (Policía Nacional de Colombia, 2017).

Asimismo, una mayor aproximación a la función de costos y beneficios de los ciberdelincuentes, implica también observar costos asociados como el tiempo dedicado a realizar el fraude y el precio de adquirir las herramientas cibernéticas. Si bien estas variables escapan al objeto de este estudio, publicaciones como "Russian Underground 2.0", que es un estudio del mercado negro o clandestino en el que interactúan cibercriminales rusos, presenta el comportamiento

1 El cálculo se hace a partir de proyecciones del DANE, que calculan para el 2019 una población de 49.395.678 de personas, junto con los datos del Banco Mundial que estiman que 65,01% de la población total colombiana tiene acceso a internet, lo que equivale a 32.112.131. Este segmento de la población podría ser afectado por un ataque de *phishing*, por lo que se calcula el 20,61% a esta. (Censo Nacional de Población y Vivienda 2018, s. f.)

de los precios de algunos servicios ofrecidos en este mercado a través de los años (Goncharov, 2015).

Finalmente, el principal insumo para este estudio son las cifras relacionadas con denuncias y capturas de la Ley 1273 de 2009, que modifica el Código Penal y tipifica los delitos informáticos en Colombia. Esta ley constituye el primer objeto de estudio de esta investigación (en cuanto a su eficiencia). La ley adiciona al Código Penal el título VII BIS, "De la protección de la información y de los datos, y agrega los artículos 269A a 269J, que mencionan las penas de prisión y las multas en salarios legales mensuales vigentes de quienes cometan este tipo de delitos.

En vista de lo anterior, existe un punto de partida para hacer una aproximación al nivel de eficiencia de la Ley 1273 de 2009 y cuantificar las ganancias promedio de un ciberdelincuente en Colombia en un año, así como tratar de determinar los factores que explican estos dos objetivos.

Metodología

La información base la suministra la Dirección de Política y Estrategias de la Fiscalía General de la Nación, obtenida del Sistema Penal Oral y Acusatorio (SPOA), que indica el número de denuncias y capturas por delitos informáticos, al igual que las denuncias y capturas por hurto agravado, mensual y departamental del período 2010-2020. A partir de ello, se calcula un indicador de captura por denuncia *Cd,* que es la razón del número de capturas por denuncias por departamento para determinado año. A continuación, el indicador *Cd*:

Cd = Número de capturas / Número de denuncias

Este indicador se calcula para los delitos de hurto agravado y hurto por medio informático en los 32 departamentos y el Distrito Capital para el 2019.

Así entonces, se compara el indicador *Cd* entre un agregado de los delitos informáticos tipificados en la Ley 1273 de 2009 y el hurto calificado, con el fin de identificar si la aplicación de esta ley es tan efectiva a la de un delito de hurto. Se elige el delito de hurto calificado por tratarse de delitos similares (ambos involucran robo, al igual que el delito de hurto calificado es un delito "consolidado", es decir, la policía está acostumbrada a atender denuncias de este tipo). Cabe mencionar que las diferencias en la *efectividad* pueden deberse a diferentes factores: como la preparación o capacitación en el manejo de pruebas que tienen las fuerzas policiales frente a un tipo de delitos, en comparación al otro para poder realizar capturas; el número de policías asignados para atender cada tipo de denuncias; qué tan fácil (o difícil) puede ser identificar a los ciberdelincuentes en comparación con los ladrones comunes; entre otros factores.

Siguiendo este análisis, se desea cuantificar la ganancia esperada de los ciberdelincuentes colombianos que buscan defraudar a clientes del sistema bancario colombiano mediante el *phishing*.

Para ello, se aplicará la función de ganancias esperadas por el ciberdelincuente, presentada por Konradt, que considera la posible ganancia de un ataque menos el posible costo del ataque:

$$Beneficios = \frac{L * S_1 * S_2 * Pk}{g} - F * Pc(K), \text{ con } Pc(K) = 1 - \frac{1}{(1+B)^{\wedge}K}$$

Las variables se interpretan así:

L = ganancia esperada por un ataque perpetuado. Se calcula a partir de la información recolectada por Asobancaria, de acuerdo con el "Informe mensual de fraude" elaborado con la información suministrada por sus agremiados sobre el reclamo por fraude promedio.

$s1$ = tasa de éxito de obtener la información. Calculada a partir de un indicador: número de usuarios afectados por un ataque, obtenido a partir de la información de la OEA de su documento del 2020: "Estado de la ciberseguridad en el Sistema Financiero Colombiano", divido entre la cantidad de ataques en Colombia en el 2019, utilizando como *proxy* la variable k.

$s2$ = tasa de éxito de vender la información. A diferencia del estudio de Konradt et al. (2016), se toma como L la ganancia obtenida por los ciberdelincuentes del ataque perpetuado, y no la ganancia esperada de vender la información obtenida, por lo que se asume $s2 = 1$.

k = número de cuentas atacadas. Calculado a partir del porcentaje de colombianos que recibió ataques en el 2019, según el informe "Cybersecurity in Latin America" de Statista.

g = miembros de la banda delincuencial. Por principio de parsimonia, se asume que $g = 1$. Sin embargo, como se quiere saber la ganancia promedio de un ciberdelincuente, se reemplazará el valor de g por n.

n = número de capturas que se efectuaron en ese año.

F = multa por cometer estos delitos. Se revisó el Código Penal y se toman en cuenta las multas en salarios mínimos legales vigentes y los años de privación de libertad, y se consideran, asimismo, las

rebajas de 3/5 partes que pueden darse en este tipo de delitos, correspondiendo así a seis años de cárcel. Para medir el costo de oportunidad de estos seis años de cárcel, se toma el salario promedio colombiano para el 2019, según las cifras de la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2021).

Pc(*k*) = probabilidad de ser capturado. Se utilizará el indicador *Cd*. En Konradt et al. (2016) se presenta como una función dependiente de un parámetro *b* aleatorio y *k,* número de cuentas atacadas. Para calcular con mayor precisión *b,* se ha decidido emplear el número de cuentas atacadas ya estimado e igualar de la siguiente forma *Pc*(*k*) = *Cd*.

Así, la ecuación queda de la siguiente forma:

$$Beneficios = (L * s1 * k)] n - F * Cd$$

Finalmente, se evalúa la posibilidad de que a partir de un ataque de un cibercriminal las ganancias sean mayores a 0, y se analiza el efecto (y su magnitud) que aumenta en las variables *k* (*número de cuentas atacadas*), *s*1 (*tasa de éxito en la obtención de información*) y *F* (*multa por la comisión de estos delitos*), en la función de beneficios del ciberdelincuente.

Análisis de información preliminar

Con base en la información suministrada por la Dirección de Política y Estrategias de la Fiscalía General de la Nación, obtenida del Sistema Penal Oral y Acusatorio (SPOA), para el 2019 se recibieron 23.917 denuncias de los delitos tipificados en la Ley 1273 de 2009 en materia de los delitos informáticos. De estos últimos, 13.242 denuncias corresponden a hurto por medio informático (55.37%), seguidas por acceso abusivo a un sistema informático con 3.492 denuncias (14.6%) y violación de datos personales con 3.178 denuncias (13.29%) (Corporación Excelencia en la Justicia, 2019)

De igual manera, para el mismo año, se presentaron 1361 detenciones para los delitos tipificados en esta ley. Que corresponden a 541 capturas a hurto por medio informático (31.94%), 454 capturas (26.8%) de acceso abusivo a un sistema informático, y violación de datos personales con 366 capturas (21.61%). En cambio, para este mismo año, 2019, en cuanto al delito de hurto calificado, se tuvieron 115.074 denuncias, con 26.276 capturas.

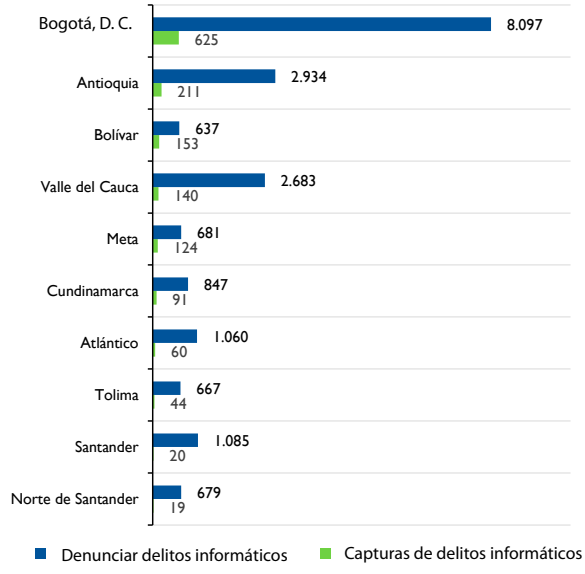
Al observar esta información a nivel departamental, se encuentra que Bogotá es la entidad territorial con mayor número de denuncias por delitos informáticos, con 8.097, seguida de Antioquia con 2.934 denuncias y Valle del Cauca con 2.683. Asimismo, Bogotá es la entidad territorial con mayor número de capturas por delitos informáticos, con 625, seguida de Antioquia con 211 capturas y Bolívar con 153.

Para el delito de hurto calificado, Valle del Cauca es el primer departamento con 29.479 denuncias, seguido de Antioquia con 16.409 y Bogotá con 13.052 denuncias; mientras que, por capturas de este delito, Bogotá tuvo 7.858, seguida de Antioquia con 3.336 capturas y Valle del Cauca con 2.055.

Como se observa en la figura 1, los principales entes territoriales donde ocurren los delitos informáticos son los centros urbanos importantes del país, en los que se concentran las actividades económicas y servicios financieros.

Figura 1.

Top 10 de denuncias y capturas por delitos informáticos a nivel departamental.



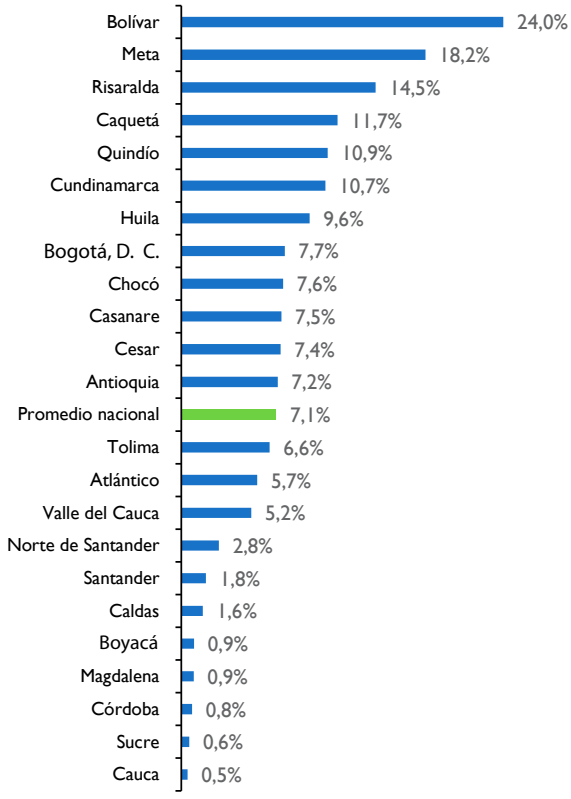
Fuente: datos aportados por la Fiscalía General de la Nación.

Indicador captura por denuncia (*Cd*) o probabilidad de ser capturado

A continuación, se presentan los resultados del indicador de captura por denuncia (*Cd*), que es la relación de número de capturas por denuncias por departamento para determinado año.

Al calcular el indicador de captura por denuncia (*Cd*), en primer lugar, se encuentra que son diez los departamentos que no tuvieron capturas por delitos informáticos en el 2019: Amazonas, Arauca, Archipiélago de San Andrés, Providencia y Santa Catalina, Guainía, Guaviare, La Guajira, Nariño, Putumayo, Vaupés y Vichada, por lo que el indicador de captura para estos departamentos es de 0. En estos departamentos se presentaron 710 denuncias, por lo que teniendo en cuenta que representa un valor bajo con respecto al total de denuncias por delitos informáticos para el 2019 (8.8%), se decidió excluirlos del estudio, pues el objetivo es centrarnos en comparar las entidades territoriales con un indicador *Cd* superior a 0.

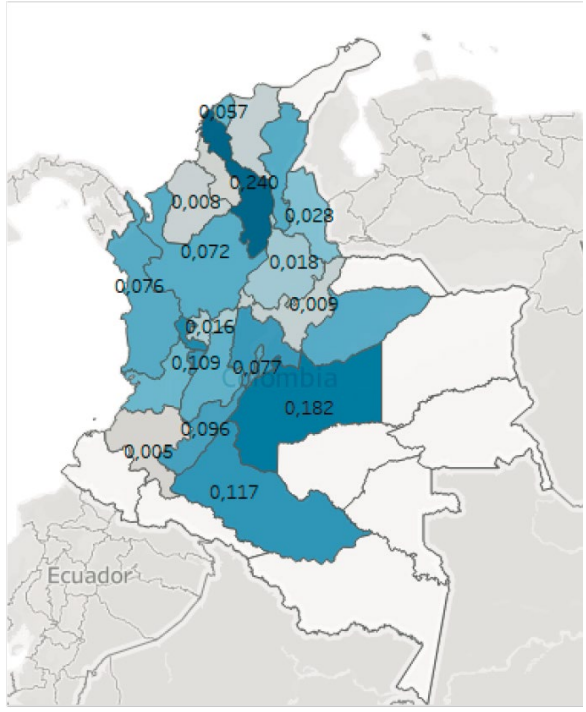
Figura 2.
Indicador Cd por departamento.



Fuente: datos aportados por la Fiscalía General de la Nación.

Como se observa en las figuras 2 y 3, los departamentos con mayor indicador de captura por denuncia son Bolívar con 24%, Meta con 18,2% y Risaralda con 14.5%. Estos indicadores al leerlos como porcentaje se interpretan como de cada 100 denuncias por delitos informáticos, se realizan *x* capturas".

Figura 3.
Mapa territorial de Colombia (por indicador Cd).



Fuente: datos aportados por la Fiscalía General de la Nación.

Asimismo, estos indicadores se interpretan como la probabilidad de ser capturado por la policía al cometer un delito informático; así, la probabilidad de ser capturado en Bolívar por cometer un delito informático es del 24%, mientras en Risaralda es del 14%.

En términos agregados, el indicador de captura nacional es de 7.1%, mientras que para hurto calificado es de 22.8%, como se verá más adelante. Ante estos resultados, se decidió analizar las variables: nivel de inclusión financiera y población estimada en los diferentes departamentos, y determinar si estas influyen en la dispersión del indicador en el ámbito nacional.

Al existir una mayor población con productos financieros, es posible que el número de denuncias por delitos informáticos sea mayor, lo que implica más trabajo para las fuerzas policiales. Sin embargo, también puede existir el efecto de que, con una mayor inclusión financiera, las fuerzas policiales pueden tener un mayor conocimiento de los delitos informáticos.

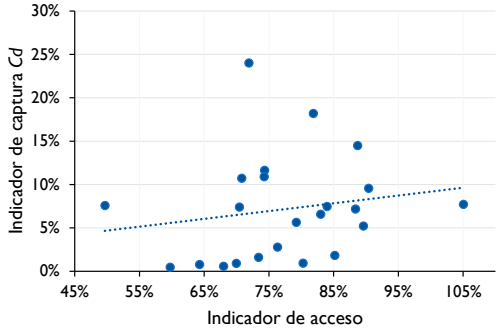
Teniendo en cuenta lo anterior, a partir del Informe de Inclusión Financiera de Personas Naturales para diciembre 2019 de la Banca de las Oportunidades, (2020) la población estimada según el DANE y el índice de desarrollo humano (IDH) por

entidad territorial, se analiza el comportamiento de las variables de población e indicador de acceso[2] por departamento y el coeficiente de correlación con los delitos informáticos (véase tabla 1).

Tabla 1.
Matriz de correlación.

	Índice captura delitos informáticos	Índice captura hurto calificado
Índice captura delitos informáticos	100%	
Índice captura hurto	9.90% (0.533)	100%
Índice de desarrollo humano	15.87% (0.4695)	25.47% (0.2408)
Indicador de acceso	17.49% (0.4247)	25.09% (0.2408)
Población	−1.54% (0.9443)	20.73% (0.3425)

Figura 4.
Indicador de delitos informáticos y el indicador de acceso.



El coeficiente de correlación entre el índice de captura por delitos informáticos y el indicador de acceso es de 17.49%; el coeficiente de correlación entre este índice de captura y el índice de desarrollo humano (IDH) es de 15.87%; mientras que el coeficiente de correlación entre el índice de captura y la población estimada es de −1.54% (véanse figuras 4, 5 y 6).

A partir de estos resultados, se observa que el acceso a servicios financieros en las entidades territoriales y el índice de desarrollo humano no tienen una relación estadísticamente significativa a un nivel de confianza de 95%.

Figura 5.
Indicador de delitos informáticos y el índice de desarrollo humano.

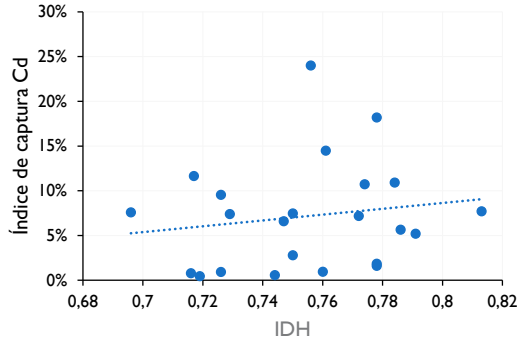
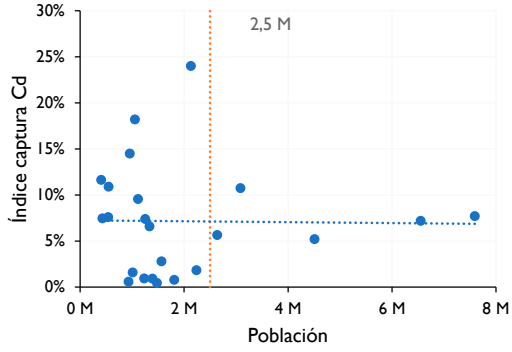


Figura 6.
Indicador de delitos informáticos y población estimada.



También se debe mencionar que, en promedio, la correlación entre el índice de captura por hurto calificado y los factores propuestos, es mayor, en términos generales, a los ligados al índice de captura por delitos informáticos. Esto claramente se puede obviar, puesto que tampoco representan una correlación significativa.

De esta forma, sugiere que entre departamentos existen factores difíciles de medir, que determinan la eficiencia de la captura de delitos informáticos. Por ejemplo, los factores de cohesión institucional de las entidades encargadas de las capturas; pues no cuentan con herramientas precisas para llevar a cabo su labor, debido a su capacidad de rastreo o de alcance.

Al observar la figura 6, se identifica un grupo de datos, aquellos que se encuentran con una población menor a 2.500.000 habitantes[3]. Si bien el coeficiente de correlación entre el índice de captura

2 Indicador de acceso: porcentaje de adultos con productos financieros sobre el total de la población adulta. En el Anexo 1 se presentan los indicadores de acceso por departamento.

3 La población estimada para cada una de las entidades territoriales se presenta en el Anexo del documento.

Cd y la población es cercano a 0, los análisis a nivel departamental también se realizaron a partir de este subgrupo, ya que se supone que los miembros que lo integran tienen un desempeño similar frente al índice de captura por delitos informáticos.

Tabla 2.

Matriz de correlación con departamentos con menos de 2.5 millones de habitantes

	Índice captura delitos informáticos	Índice captura hurto calificado
Índice captura delitos informáticos	100%	
Índice captura hurto	8.32% (0.7426)	100%
Índice de desarrollo humano	21.24% (0.3974)	9.53% (0.7068)
Indicador de acceso	25.4% (0.3091)	12.55% (0.6198)
Población	−9.64% (0.7036)	−18.06% (0.4734)

De acuerdo con lo anterior, el subgrupo poblacional con menos de 2.500.000 habitantes no presenta un comportamiento diferente en sus correlaciones con respecto a lo observado previamente en el análisis sin la diferenciación propuesta de corte en 2.500.000 habitantes. De hecho, para este subgrupo, la correlación entre el índice de captura por delitos informáticos y la población es de −9.64%; entre el índice de captura por delitos informáticos y el índice de desarrollo humano es de 21.24%; mientras que entre el índice de captura por delitos informáticos y el indicador de acceso es de 25.4% (véase tabla 2).

Asimismo, a partir de estos resultados, se observa que, para este subgrupo, el acceso a servicios financieros en las entidades territoriales y el índice de desarrollo humano, no tienen una relación estadísticamente significativa a un nivel de confianza de 95%.

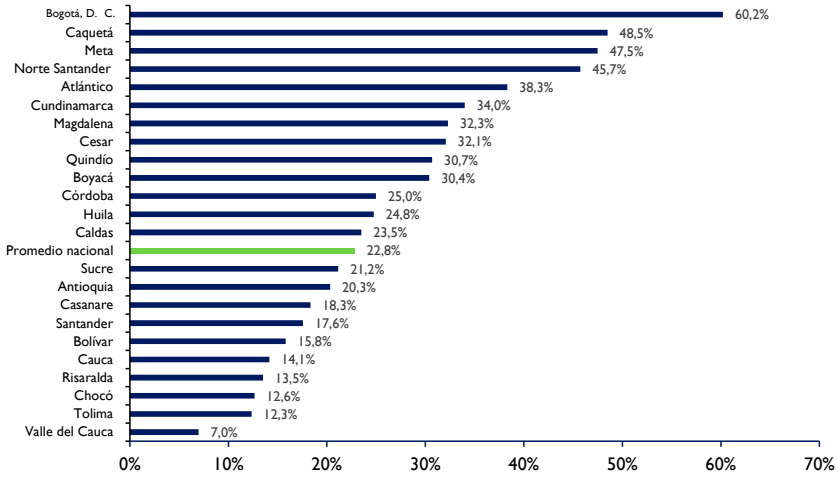
Para finalizar, se realizó el ejercicio de proponer una regresión lineal simple, tomando como variable dependiente el índice de captura por delitos informáticos y los demás factores propuestos como variables independientes; también para el índice de captura por hurto calificado como variable dependiente. Como resultado, se encontró que ninguna de las variables tiene un coeficiente significativo, lo que afirma la hipótesis de que son otras variables las que pueden estar explicando estos índices.

Resultados: comparación entre índices de captura de delito informático e índices de captura de hurto calificado

A continuación, se presenta el índice de captura de hurto calificado para el 2019 (SPOA, 2019) para las 23 entidades territoriales que se consideran en el estudio (véase figura 7). Como en el índice de captura de delitos informáticos, este también se interpreta como "de cada 100 denuncias por hurto calificado, se realizan por capturas". De igual manera, se calcula el coeficiente de correlación entre el índice de hurto calificado y el indicador de acceso a servicios financieros (25.47%), entre la población estimada (20.73%) y el índice de desarrollo humano (25.47%).

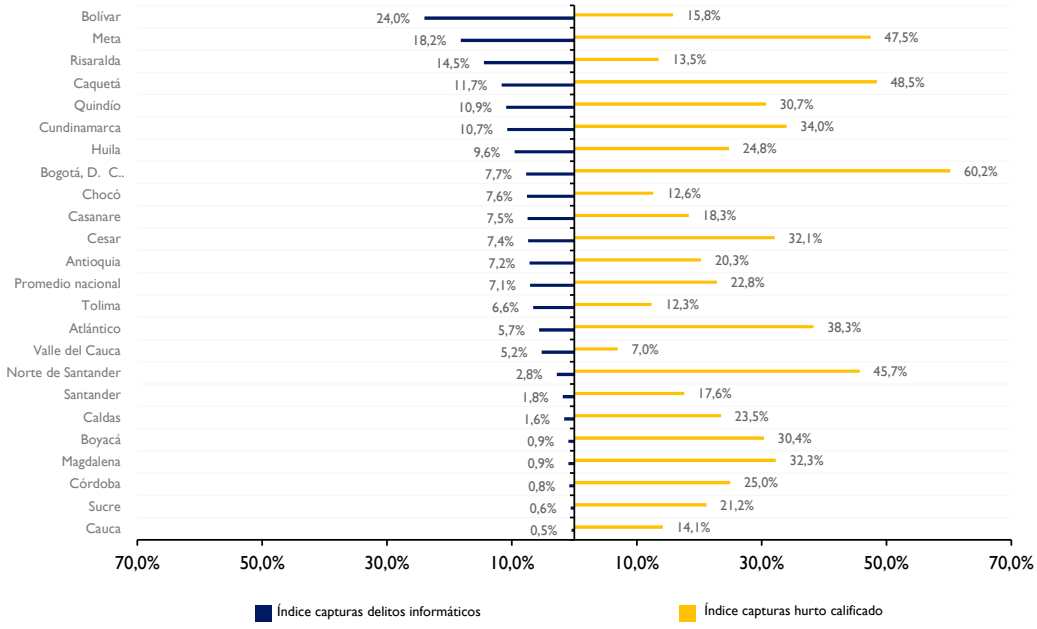
Figura 7.

Indicador de captura por hurto calificado por departamento.



Fuente: datos aportados por la Fiscalía General de la Nación.

Figura 8.
Comparación entre índices de captura a nivel de entidad territorial.



Fuente: datos aportados por la Fiscalía General de la Nación

A partir de esta información, se comparan los índices de captura de hurto calificado y el índice de captura para delitos informáticos *Cd* (véase figura 8).

En los anexos de este documento, se relacionan las capturas y denuncias con el indicador de captura por departamento y el acceso de la denuncia que relacionan el cumplimiento entre la denuncia y el delito por territorio.

Se observa que, para la mayoría de las entidades territoriales, el indicador de captura por hurto calificado es mayor que el de delito informático, siendo las únicas excepciones Bolívar y Risaralda; lo que sustenta la hipótesis de que la ejecución de la Ley de Delitos Informáticos, de 2009 ha sido menos eficiente, al menos en la mayoría de los departamentos, si se compara con el delito de hurto calificado.

Además, cuando se analiza el indicador de captura para hurto por medio informático (el delito informático del que más se recibieron denuncias), se encuentra que para todas las entidades territoriales la diferencia es negativa, por lo que el índice de captura por hurto por medio informático es menor al de hurto calificado[4].

Por otra parte, llama la atención el poco número de denuncias por delitos relacionados con el hurto por medios informáticos. Si se tiene en cuenta que, para efectuar un hurto por medio informático, es habitual que se realicen accesos abusivos, *software* malicioso o uso no autorizado de información personal (como se indicó en la figura 1), lo que podría indicar una cierta falta de conocimiento de los entes policiales al atender las denuncias que reciben.

Continuando con la comparación de estos índices, al analizar las correlaciones de variables como el indicador de acceso, la población y el índice de desarrollo humano, se encuentra que estas variables no presentan correlaciones significativas a un nivel de confianza del 95%. Por tanto, se podría afirmar que estas variables no tienen relación con la capacidad o eficiencia de las fuerzas policiales de las entidades territoriales, para realizar capturas en delitos tipificados en la Ley 1273 de 2009 o delitos de hurto calificado, indicando que son otros aspectos y no los que suelen asociarse a un mayor desarrollo (mayor población, desarrollo humano o inclusión financiera) que hacen que las fuerzas policiales sean más eficaces.

4 Los indicadores para los otros delitos tipificados en la Ley 1273 de 2009 se presentan en el Anexo 1.

En el caso de los departamentos de Bolívar y Risaralda, se observa que el indicador para el "acceso abusivo a un sistema informático es mayor al indicador para hurto calificado[5], y es el principal delito que permite que *Cd* sea mayor al indicador de hurto calificado. Sería de interés observar y conocer los procedimientos que realizan en estos departamentos frente a este tipo de delitos, para así identificar buenas prácticas que se puedan compartir con las otras entidades territoriales.

A continuación, se calculan los indicadores de captura para delitos informáticos y de hurto calificado para tres grupos identificados en la figura 6, los que se encuentran por encima de la tendencia y con una población menor de 2.500.000 habitantes; los que están por debajo de la tendencia y con una población menor de 2.500.000 habitantes, y los principales centros poblacionales que superen los 2.500.000 habitantes (véase figura 9).

De estos grupos, los principales centros urbanos son Antioquia, Atlántico, Bogotá, D. C., Cundinamarca y Valle del Cauca; los departamentos con bajo *Cd*: Boyacá, Caldas, Cauca, Córdoba, Magdalena, Norte de Santander, Santander, Sucre y Tolima, y los que presentan alto *Cd*: Bolívar, Caquetá, Casanare, Cesar, Chocó, Huila, Meta, Quindío y Risaralda.

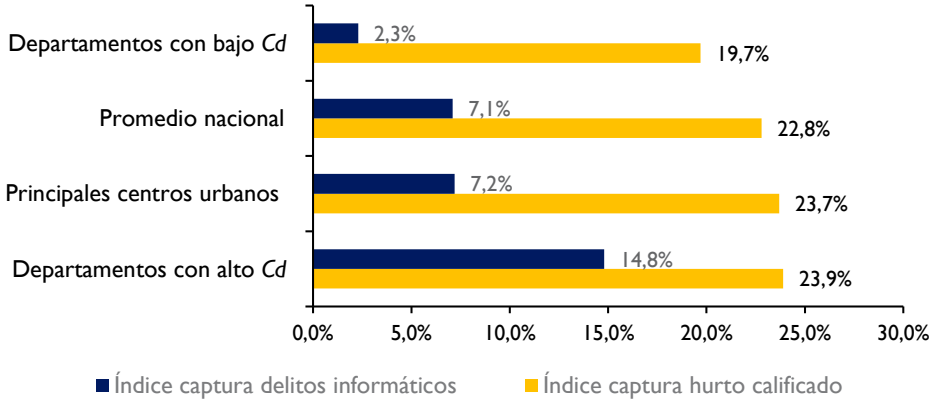
De la información de la figura 9, es posible observar que los departamentos con alto índice de captura en delitos informáticos, son los que tienen mayor índice de captura en hurto calificado; lo que sustenta la idea de que la eficiencia en la captura de delitos informáticos no está relacionada con los indicadores de población, desarrollo humano o acceso a servicios financieros, sino con la formación que reciben las fuerzas policiales de estos territorios y que pueden estar asociadas en la misma formación en delitos como el hurto calificado.

También se debe mencionar que la correlación entre el índice de captura por delitos informáticos y el índice de captura por hurto calificado, no supera ni siquiera el 10% para los grupos poblacionales de menos de 2.5 millones de habitantes, así como tampoco para grupos de más de 2.5 millones de habitantes.

Finalmente, se muestra el valor de los indicadores de captura de delitos informáticos *Cd* y hurto calificado en los últimos diez años, con el fin de conocer su comportamiento (véanse figuras 10 y 11).

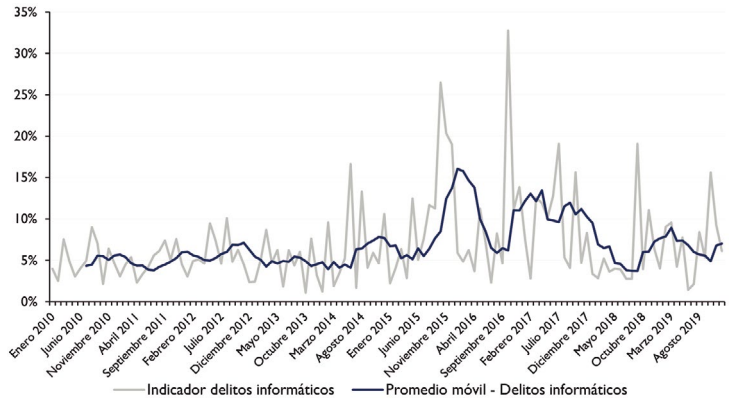
5 Para el departamento de Risaralda, el indicador para transferencia no consentida de activos también es mayor al indicador de hurto calificado.

Figura 9.
Comparación entre índices de captura entre grupos.



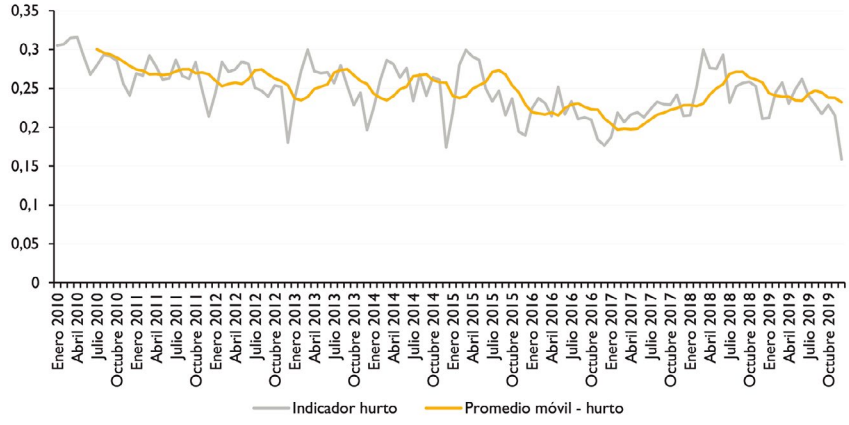
Fuente: datos aportados por la Fiscalía General de la Nación.

Figura 10.
Comportamiento histórico del indicador de delitos informáticos Cd.



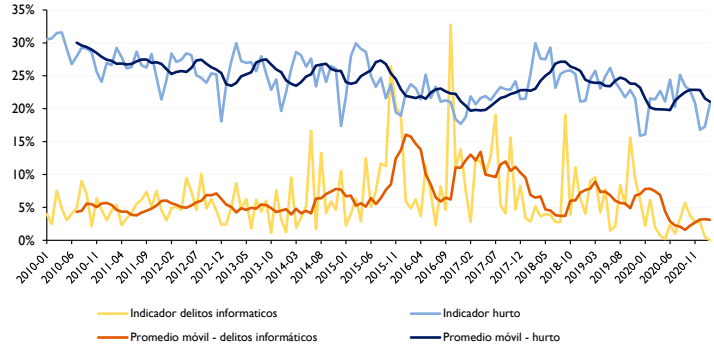
Fuente: datos aportados por la Fiscalía General de la Nación.

Figura 11.
Comportamiento histórico del indicador de hurto calificado.



Fuente: datos aportados por la Fiscalía General de la Nación.

Figura 12.
Comportamiento histórico del indicador de hurto calificado y delitos informáticos.



Fuente: datos aportados por la Fiscalía General de la Nación.

La Figura 12 muestra que el indicador de delitos informáticos *Cd* ha sido menor en los últimos años en comparación con el de hurto calificado.

Teniendo en cuenta los resultados de esta primera fase del estudio, se puede afirmar y concluir que la eficiencia de la aplicación de la Ley 1273 de 2009, que tipifica los delitos informáticos, ha sido baja en comparación con un delito similar como lo es el hurto calificado. Asimismo, si se tiene en cuenta que el indicador analiza la relación de capturas por denuncias, ya baja de por sí, se esperaría que la relación de sentencias por denuncias sea igual o menor (no todas las capturas necesariamente conllevan sentencias).

Por consiguiente, se observa que las variables inclusión financiera, población o desarrollo humano no tienen relación con que una región o un departamento sea más eficiente enfrentando a estos delitos, lo que sugiere que son mecanismos directamente asociados con la formación de la Policía Nacional en determinadas entidades territoriales, que les permite ser más eficientes que otras. Estos mecanismos pueden ser capacitaciones en temas como identificación de evidencia digital, extracción y uso de información electrónica involucrada en casos de fraude digital, conocimiento del marco jurídico y legal para el adecuado manejo de estos casos, entre otros.

A continuación, se procede con la segunda hipótesis del estudio, que establece que, dado que la tasa de captura (eficiencia) en los delitos informáticos en Colombia es baja, el ciberdelincuente percibe que las ganancias de un ciberataque a los usuarios financieros son mayor o al menos igual a 0 pesos.

Como se mencionó, la ecuación que se va a utilizar está definida como:

$$Beneficios = (L * s1 * k)| n - F * Cd$$

Análisis de la función de beneficios del ciberdelincuente (ganancias)

$$Beneficios = (L * s1 * k)| n - F * Cd$$

Las ganancias de la ciberdelincuencia vienen dadas por la parte izquierda de la ecuación, compuesta de *L*, *s*1, *s*2, *k* y *n*. Como se mencionó anteriormente, se asume *s*2 y *n* iguales a 1.

Para calcular *k* (número de cuentas atacadas), se usaron los datos obtenidos del informe "Cybersecurity in Latin America" de Statista (2019), estimando así 6.618.311 personas (y cuentas) atacadas en el 2019 en Colombia.

En el caso de *s*1 (tasa de éxito en la obtención de información), se divide el número de personas que fueron objeto de fraude en el 2019, de acuerdo con la información de la Organización de los Estados Americanos (OEA, 2020), que se estiman en 91.989, entre el número de cuentas atacadas (es decir *k*), lo que da como resultado 0.0139 o 1.39%.

Para estimar *L*, a partir de los datos recolectados por Asobancaria y sus entidades agremiadas, se estima que para el 2019 la reclamación por fraude promedio por persona fue de $825.050.

Finalmente, se obtiene que las ganancias promedio para el 2019 de la ciberdelincuencia en Colombia (*L***s*1**k*) fueron de $75.895.568.279. Teniendo en cuenta que el objeto del estudio es estimar la ganancia promedio de un ciberdelincuente, estas ganancias totales se dividen por *n* (un *proxy*, que puede ser imperfecto en el corto plazo, del número total de ciberdelincuentes)[6], que es el número de capturas en el 2019 (1.694), dando así $44.802.579; ganancia anual promedio del ciberdelincuente.

Ganancias totales

Con base en los resultados anteriores, se estima que los beneficios o "ganancias netas" del ciberdelincuente son de $37.215.330 promedio anual, lo que permite afirmar nuestra hipótesis de que los ciberdelincuentes perciben que las ganancias de esta actividad son mayores a 0. A partir de este resultado, se efectúan los análisis de sensibilidad de las variables *k*, *s*1 y *F*, para determinar cómo se pueden reducir las ganancias esperadas y de esta manera reducir la ciberdelincuencia en Colombia.

Análisis de la función de beneficios del ciberdelincuente: costos

A partir de un promedio simple de los años que podría pasar en la cárcel un delincuente por cometer crímenes tipificados en la Ley 1273 de 2009, y teniendo en cuenta las rebajas de condena, se calcula un costo de oportunidad que equivale al salario promedio colombiano para el 2019, de acuerdo con las cifras de la Organización para la Cooperación y el Desarrollo Económicos (OECD, por sus siglas en inglés, 2021)[7].

6 Un *proxy* puede ser imperfecto en el corto plazo, del total de ciberdelincuentes.

7 Esta estimación se hace con base en el Código Penal que tipifica de 6 a 14 años de cárcel para las personas que cometan el delito de hurto por medios informáticos (el delito más denunciado de la Ley 1273 de 2009), tomando como valor promedio diez años. A estos diez años se les aplica el beneficio

Este costo de oportunidad corresponde a *F* y se estima en $107.121.744.

Pc (k) corresponde a la probabilidad de ser capturado, por lo que se tomará el valor hallado de *Cd* a nivel nacional, que corresponde a 0.071 o 7.1%.

Con estos datos, se estima que el costo esperado asociado con cometer ciberdelitos en Colombia $-F * Cd -$ es de $7.587.249.

Análisis de sensibilidad

Análisis de sensibilidad: número de cuentas atacadas k

Se realiza un análisis de sensibilidad con la variable *k*, con el fin de determinar el número de cuentas afectadas para que los ciberdelincuentes perciban 0 pesos como ganancias netas. Se obtiene como resultado que para que las ganancias netas sean iguales a 0, es necesario que *k* se reduzca a 1.120.801 cuentas, es decir, una disminución del 83.07% (su valor actual es de 6.618.311). Reducir el número de cuentas atacadas a estos niveles es una tarea complicada, considerando que cada vez más personas acceden a los servicios financieros y que los ciberdelincuentes acceden a nuevos programas maliciosos, que son cada vez más eficientes para llegar a mayor cantidad de usuarios para estafarlos. Teniendo esto presente, se procede al análisis de la variable *s*1.

Análisis de sensibilidad: tasa de éxito de los ataques s1

Para que los ciberdelincuentes perciban ganancias netas de 0, es necesario que *s*1 disminuya a un valor de 0.235%, lo que equivale a una disminución del 83.07% o a 1.155 puntos porcentuales (su valor actual es de 1.39%).

La diferencia del análisis con cuentas afectadas, la reducción de la tasa de éxito es más fácil, ya que esta se puede disminuir con políticas públicas, ya sea con mayor protección o cautela de los usuarios, no entregando su información personal en correos sospechosos, no abriendo enlaces maliciosos, entre otros. Además, estrategias propuestas por la Asobancaria, como el bloqueo preventivo de los URL maliciosos para evitar que los usuarios financieros accedan a estos, se transforman en una excelente herramienta para disminuir la tasa de éxito de los ciberataques.

Los bancos, constantemente realizan actividades de concientización y educación financiera, y en el caso colombiano, actores como la Policía Nacional, Incocrédito y Asobancaria hacen constantes esfuerzos para concientizar a los usuarios financieros sobre la importancia de cuidar datos sensibles como contraseñas y claves de sus productos.

Análisis de sensibilidad: multa por cometer estos delitos F

Para que los ciberdelincuentes obtengan una ganancia neta de 0, *F* debe aumentar a $632.552.114, lo que implica un aumento del 490,50%, que equivale a 523.430.370 más del valor actual. Para lograr este incremento, es necesario aumentar a más de 35 años la condena que figura en el Código Penal para los delincuentes que cometen el delito de hurto por medios informáticos, o reducir los beneficios de penas para este tipo de delitos.

Las reformas a las leyes y al Código Penal colombiano implican esfuerzos en el poder legislativo, por lo que a mediano y corto plazo la modificación de estas normas es poco viable. De igual manera, incrementar las penas que cumplirían los delincuentes implica aumentos en los costos del Estado para una mayor población carcelaria. Finalmente, es aún más importante considerar que los cambios al sistema penitenciario, no solo deben contemplarse en términos económicos, sino también desde aspectos de las ciencias sociales como las teorías punitivas, la reinserción social, entre otros.

Análisis de sensibilidad: probabilidad de ser capturado Pc(k) = *Cd*

Para que los ciberdelincuentes obtengan ganancias netas de 0, *Pc*(*k*) = *Cd* debe aumentar al 41.82%, lo que representa un aumento de 490.50% o 34.74 puntos porcentuales (actualmente es de 7.08%). Este aumento implica un mayor número de capturas, por lo que es deseable y necesario un mayor nivel de formación en capacidades judiciales o de investigación para tratar estos delitos entre los miembros de la Policía Nacional.

de rebaja de la condena de 3/5 partes, correspondiendo así a seis años de privación de la libertad. Según la OECD (2021), la relación salario mínimo/salario medio es de 0,59. Aplicando esta razón al salario mínimo del 2019, se obtuvo que el salario mensual promedio en Colombia para el 2019 fue de $1.487802.

Tabla 3.

Análisis de sensibilidad tasa de éxito de ataques s1 y probabilidad de ser capturado Cd

			Probabilidad de ser capturado por delito informático - Cd						Probabilidad de ser capturado por hurto calificado
			Porcentaje de cambio						
			Valor inicial	98%	196%	294%	392%	490%	
			7.10%	14%	21%	28%	35%	42%	22.80%
Tasa de éxito del delincuente para obtener información - s1	Porcentaje de cambio	Valor inicial	1.39%	$37.215.330	$29.772.264	$22.329.198	$14.886.132	$7.443.066	$0	$20.342.397
		-17%	1.16%	$29.772.264	$22.329.198	$14.886.132	$7.443.066	$0		$12.899.331
		-33%	0.93%	$22.329.198	$14.886.132	$7.443.066	$0			$5.456.266
		-50%	0.70%	$14.886.132	$7.443.066	$0				
		-66%	0.47%	$7.443.067	$0					
		-83%	0.24%	$0						

Teniendo en cuenta que los cambios en la tasa de éxito *s*1 y la probabilidad de ser capturado, *Pc*(*k*) son los de mayor interés, a continuación, se realiza un análisis bivariado con estas dos variables.

Análisis bivariado

Se realiza un análisis de tipo bivariado en una tabla de decisión con dos variables que se pueden mover a través de políticas públicas. Así, se presentan los aumentos en cada variable para mostrar el resultado de las ganancias del ciberdelincuente, si todas las demás variables se mantienen constantes. En la tabla 3 se presenta la información del análisis.

Se observa que los aumentos en la probabilidad de ser capturado junto a la disminución en la tasa de éxito de los ataques pueden llevar incluso a generar "ganancias negativas" para el ciberdelincuente, algo deseable. Asimismo, aun con un aumento del 100% en la probabilidad de ser capturado, a la tasa actual de éxito de los ataques (1.39%), todavía quedan más de la mitad de las ganancias esperadas, mientras que una reducción cercana al 50% en la tasa de éxito sí implica una reducción de más del 50% en las ganancias esperadas.

Por tanto, se destaca la importancia y el efecto de las políticas que generan una reducción en la tasa de éxito de los ciberataques, con el fin de disuadir a los ciberdelincuentes de realizar ataques.

Conclusiones

Esta investigación ha permitido identificar que la eficiencia de la Ley 1273 de 2009 sobre delitos informáticos, ha sido baja en comparación con los delitos también consolidados, como el hurto calificado. Existen solo dos departamentos con una tasa mayor de capturas por delitos informáticos en comparación con la de hurto calificado. Asimismo, se encuentra que la ganancia neta esperada de los ciberdelincuentes es mayor a 0 y, por tanto, estos tienen incentivos para seguir cometiendo estos crímenes.

Asimismo, se puede estimar que las variables como población, indicador de acceso o desarrollo humano, no tienen relación con un departamento específico, en especial, que enfrente con más efectividad estos delitos; lo que sugiere que existen otros mecanismos o variables que se correlacionan con estos índices. Por ejemplo, variables difíciles de medir como la formación de la Policía Nacional y la Fiscalía en determinadas seccionales, capacitaciones en temas de identificación de pruebas digitales, extracción y uso de información electrónica involucrada en casos de fraude digital, conocimiento del marco jurídico y legal adecuado para el manejo de estos casos, entre otros.

De igual manera, se destaca que la falta de correlación regional entre el indicador de hurto calificado y el indicador de delitos informáticos sugiere que las diferencias regionales entre estos, no se explican por diferencias en las capacidades de la

policía. Es decir, no existe una relación positiva directa entre la capacidad institucional de la policía en delitos de hurto calificado y los delitos informáticos. A su vez, las dinámicas de fortaleza institucional se reflejan en que, si bien ambos son delitos, existen diferencias cuando se trata de capacitar a los policías para que cumplan su valiosa labor.

Al analizar las variables (k = número de cuentas atacadas y F = multa por cometer estos delitos) de la ecuación de beneficios del ciberdelincuente, se denota que estas son difíciles de modificar por la política pública. La tendencia de k es aumentar a medida que existan más personas bancarizadas y la tendencia de F depende de la política criminal de Colombia; por lo cual, el reto es integrar estas dos variables en la agenda nacional para mejorar la capacidad operativa de los entes de control y policivos. Por ello, se encuentra que las variables más factibles de modificar mediante propuestas de política pública son $s1$ (tasa de éxito en la obtención de información) y transversalmente, la probabilidad de ser capturado por delitos informáticos Cd. Al combinarse, se requerirían cambios factibles para que las ganancias del ciberdelincuente en un año sean cercanas a 0, de acuerdo con nuestro análisis, manteniendo todo lo demás constante (Principio de Pareto).

Estos resultados nos sugieren buscar diferentes estrategias, como diseñar un indicador que mida la efectividad del delito, y se propone realizar una mesa de seguimiento entre entidades de investigación y la Asobancaria, donde se determine el avance del indicador con variables como el desarrollo formativo, herramientas de investigación, entre otras. Se pueden crear indicadores por regionales y departamentos que en conjunto determinen planes de acción con la Policía y Fiscalía para incrementar el nivel de captura del delito respecto a las denuncias, asegurando el cumplimiento de la Ley 1273 de 2009.

Se recomienda mejorar el trabajo conjunto en comunicación y capacidad institucional articulada para el gremio financiero, entidades gubernamentales y las entidades responsables de las capturas por estos delitos (Policía Nacional, jueces, Fiscalía, bancos, Colcert, CSIRT, entes territoriales). También, hacer más campañas orientadas al usuario, que se centren en la concientización y de educación financiera, con el objetivo de reducir los actos de cibercrimen, entre otros. Esta última recomendación se puede desarrollar a través de mensajes de textos o herramientas contra la ciberdelincuencia, con el objetivo de detectar mensajes maliciosos y bloquear las URL de riesgo cibernético para el usuario final, afectando los modos de operación de las bandas, correlacionando qué monitores IPS generan estos mensajes maliciosos y que afectan las estructuras de ganancias de los ciberdelincuentes.

Referencias

Anderson, R., Barton, Ch., Böhme, R., Clayton, R., Eeten, M., Levi, M., Moore, T., & Savage, S. (2012). *Measuring the cost of cybercrime*. https://cseweb.ucsd.edu/~savage/papers/WEIS2012.pdf

Banca de las Oportunidades. (2020). *Personas con productos financieros*. https://bancadelasoportunidades.gov.co/index.php/es/personas-empresas

Censo Nacional de Población y Vivienda 2018. (s.f.). https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/censo-nacional-de-poblacion-y-vivienda-2018

Centro Cibernético Policial. (2017). *Costos del cibercrimen en Colombia 2016-2017*. https://caivirtual.policia.gov.co/sites/default/files/costos_del_cibercrimen_2017.pdf

Congreso De Colombia (5 enero de 2009). *Ley 1273, Protección de la información y de los datos. Código Penal Colombiano*. https://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

Council, H. O. (2018). *Undertanding the cost of cibercrim*e. https://bit.ly/2IDou1k

Datos abiertos de la. (s. f.). Fiscalía General de la Nación. Recuperado 11 de octubre de 2022, de https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

Díaz, M. R. O., & Rangel, P. E. S. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: Un análisis para Colombia*. *Revista Criminalidad, 62*(2), 199–217. https://revistacriminalidad.policia.gov.co:8000/index.php/revcriminalidad/article/view/168

Departamento Administrativo Nacional de Estadística, DANE. (2020). *Censo Nacional de Población y Vivienda -CNPV- 2018*. https://www.dane.gov.co/index.php/estadisticas-por-tema/demografia-y-poblacion/proyecciones-de-poblacion

Fiscalía General de la Nación (s.f.). (2022, 11 de octubre), de https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

Global Data Lab. (s.f.). *Human development indices 5.0* https://hdr.undp.org/data-center/human-development-index#/indicies/HDI.

Goncharov, M. (2015). *The Russian underground 2.0*. https://okapitech.co.uk/2016/04/27/the-russian-underground/

Home Office. (2018, 18 enero). Understanding the costs of cyber crime. GOV.UK. https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime

Internet Crime Complaint Center (IC3) | Annual Reports. (s. f.). (2022, 11 de octubre). https://www.ic3.gov/Home/AnnualReports

Konradt, C., Schilling, A., & Wemers, B. (2016). Phishing: An economy analysis of cybercrime perpetrators. *Computers & Security*, *58*, 39-46. https://doi.org/10.1016/j.cose.2015.12.001

Mundial, B. (2021). *Individual using the internet-Colombia*. https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=CO

Organización de los Estados Americanos, OEA. (2020). *Estado de la ciberseguridad en el sistema financiero colombiano.* https://www.asobancaria.com/wp-content/uploads/2020/10/20201014-ASOBANCARIA-2020_compressed.pdf

Organization for Economic Co-Operation and Development. (OCDE, 2021). *Minimum relative to average wages of full-time workers.* https://stats.oecd.org/Index.aspx?DataSetCode=MIN2AVE

Reportes anuales. (s. f.). *Reporte de Inclusión Financiera 2021* https://www.bancadelasoportunidades.gov.co/index.php/es/publicaciones/reportes-anuales

Ross, A., Barton, C., Bohme, R., Clayton, R., Levi, M., Moore, T., & Stefan, S. (2012). Measuring the cost of cybercrime. https://cseweb.ucsd.edu/~savage/papers/WEIS2012.pdf

Senado de la Republica. (2000). *Código Penal colombiano* - Ley 599 de 2000. https://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20130808_01.pdf

Corporación Excelencia en la Justicia. (2019). *Informe de estadísticas del Sistema Penal Oral Acusatorio (SPOA)*. https://cej.org.co/wp-content/uploads/2021/02/Balance-Sist.-Penal-Acusatorio-2019-1.pdf

Statista. (2019). *Países de América Latina y el Caribe más atacados por ataques de phishing en 2020*. https://www.statista.com/statistics/997956/phishing-attack-user-share-latin-america-country/

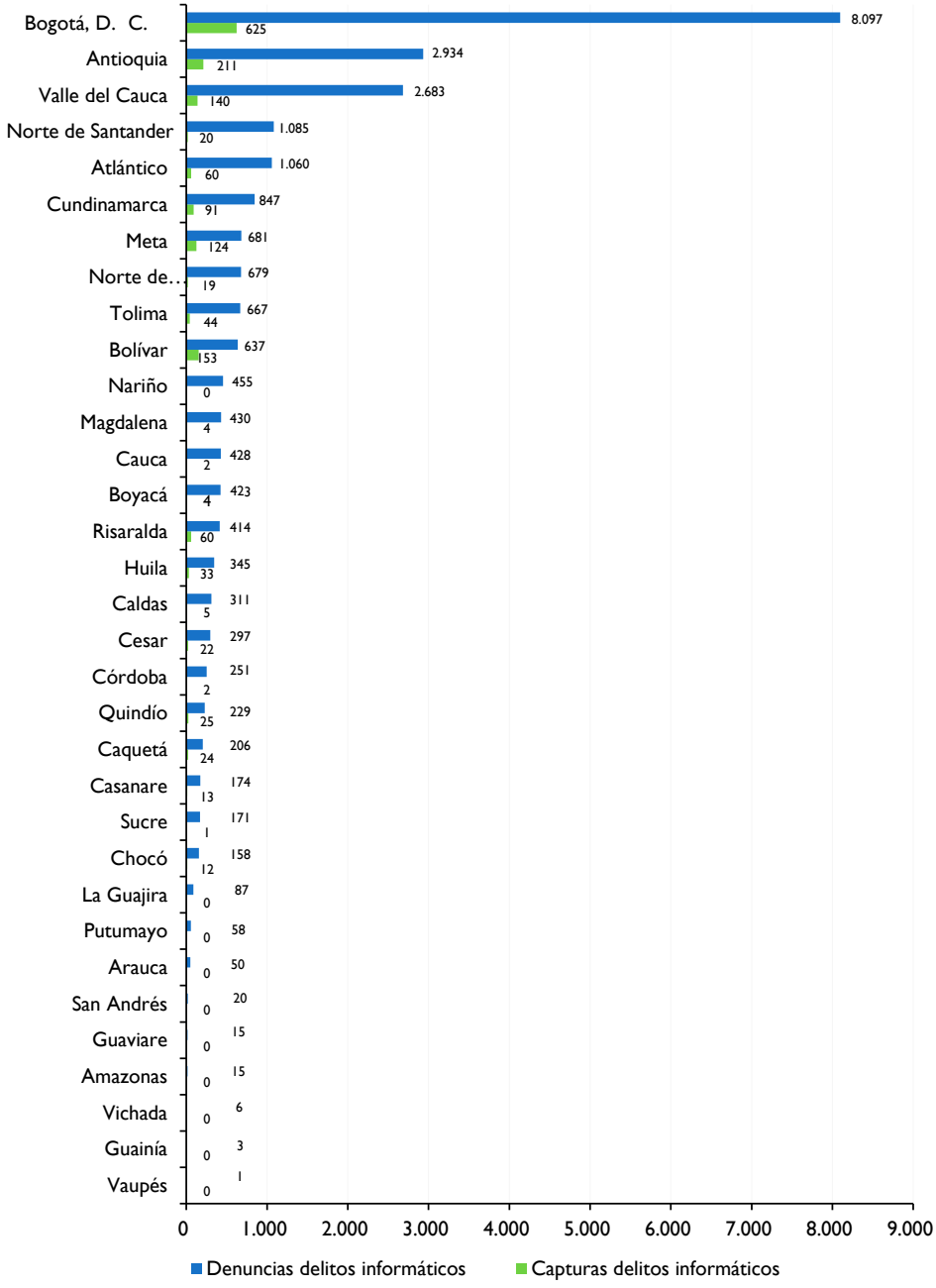
Yonge, J. D. (2022). EY. *The pandemic hastened the arrival of trends already on the leadership agenda. CEOs must seize this opportunity to transform or be left behind*. https://www.ey.com/en_us/ceo/the-ceo-imperative-how-has-adversity-become-a-springboard-to-growth

Anexos

Anexo 1

Figura 13.

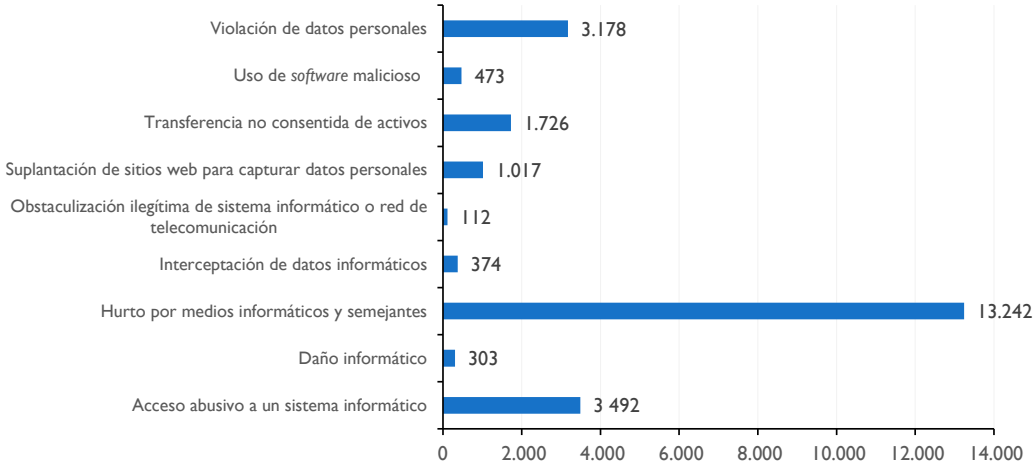
Denuncias y capturas por delitos informáticos a nivel departamental.



Fuente: datos aportados por la Fiscalía General de la Nación.

Figura 14.

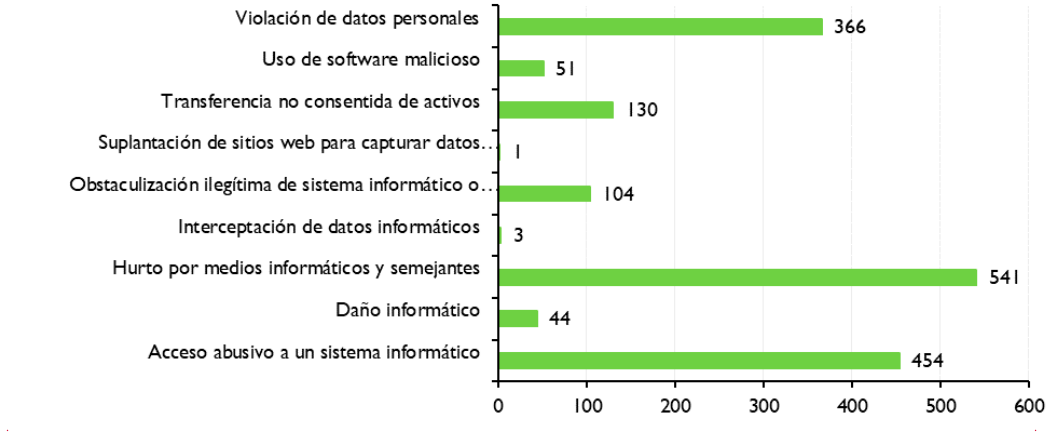
Denuncias de delitos informáticos en el 2019.



Fuente: datos aportados por la Fiscalía General de la Nación.

Figura 15.

Capturas de delitos informáticos en el 2019.



Fuente: datos aportados por la Fiscalía General de la Nación.

Anexo 2

Para diciembre de 2019, hay once departamentos (incluyendo Bogotá) con un indicador de acceso mayor a 80%, por lo cual ocho de cada diez adultos (o más) en estos departamentos cuentan con productos financieros, diez departamentos con un indicador de acceso entre 70% y 79,9%, seis departamentos con un indicador entre 60% y 69,9%, dos departamentos con indicadores entre 50% y 59,9% y cuatro departamentos con indicadores menores a 50% (Vaupés, Vichada, Guainía y Chocó) (véase tabla 4).

Tabla 4.
Indicador de acceso por departamento.

Departamento	Indicador de acceso	Departamento	Indicador de acceso
Amazonas	0.60	Guaviare	0.79
Antioquia	0.884	Huila	0.904
Arauca	0.83	La Guajira	0.54
Archipiélago de San Andrés, Providencia y Santa Catalina	0.78	Magdalena	0.699
Atlántico	0.792	Meta	0.819
Bogotá, D. C.	1,051	Nariño	0.65
Bolívar	0.719	Norte de Santander	0.763
Boyacá	0.803	Putumayo	0.68
Caldas	0.734	Quindío	0.743
Caquetá	0.743	Risaralda	0.887
Casanare	0.840	Santander	0.852
Cauca	0.597	Sucre	0.680
Cesar	0.704	Tolima	0.830
Chocó	0.497	Valle del Cauca	0.896
Córdoba	0.643	Vaupés	0.29
Cundimamarca	0.708	Vichada	0.32
Guanía	0.40	Total general	0.82

Tabla 5.
Población estimada por entidad territorial para el 2019.

Departamento	Población	Departamento	Población
Bogotá, D. C.	7.592.871	Caldas	1.088.344
Antioquia	6.550.206	Risaralda	952.511
Valle del Cauca	4.506.768	Sucre	928.984
Cundinamarca	3.085.522	La Guajira	927.506
Atlántico	2.638.151	Quindío	547.855
Santander	2.237.587	Chocó	539.933
Bolívar	2.130.512	Casanare	428.563
Córdoba	1.808.439	Caquetá	406.142
Nariño	1.628.981	Putumayo	353.759
Norte de Santander	1.565.362	Arauca	280.109
Cauca	1.478.407	Vichada	110.599
Magdalena	1.388.862	Guaviare	84.716
Tolima	1.335.313	Amazonas	77.753
Cesar	1.252.398	Archipiélago de San Andrés, Providencia y Santa Catalina	62.482
Boyacá	1.230.910	Guainía	49.473
Huila	1.111.844	Vaupés	42.721
Meta	1.052.152		

Tabla 6.

Indicador de captura por denuncia, hurto calificado y delitos de la Ley 1273 de 2009.

Entidades territoriales	Hurto calificado	Acceso abusivo a un sistema informático	Daño informático	Hurto por medios informáticos y semejantes	Interceptación de datos informáticos	Obstaculización ilegítima de sistema informático o red de telecomunicación	Suplantación de sitios web para capturar datos personales	Transferencia no consentida de activos	Uso de *software* malicioso	Violación de datos personales
Amazonas	0,600									
Antioquia	0,203	0,096		0,049		0,364		0,238		0,127
Arauca	0,235									
Archipiélago de San Andrés, Providencia y Santa Catalina	0,195									
Atlántico	0,383	0,005	1,375	0,049		3,000	0,019	0,110		0,008
Bogotá, D. C.	0,602	0,163	0,104	0,054	0,005	1,087		0,084	0,004	0,092
Bolívar	0,158	0,703		0,047						1,327
Boyacá	0,304	0,018		0,008						0,020
Caldas	0,235			0,014					0,250	0,030
Caquetá	0,485	0,188		0,126				0,500		0,077
Casanare	0,183	0,129		0,008						0,571
Cauca	0,141	0,015								0,014
Cesar	0,321	0,046		0,048				0,278		0,500
Chocó	0,126	0,462	2.00							
Córdoba	0,250			0,006				0,125		
Cundinamarca	0,340	0,381	0,063	0,005	0,019	2,154				
Guainía	0,571									
Guaviare	0,216									
Huila	0,248	0,156	0,750	0,100				0,018		0,128
La Guajira	0,400									
Magdalena	0,323			0,019						
Meta	0,475	0,033	0,500	0,038				0,250	4,800	0,547
Nariño	0,223									
Norte de Santander	0,457		0,167	0,056				0,012		
Putumayo	0,441									
Quindío	0,307			0,123						0,227
Risaralda	0,135	0,270		0,079				0,273		0,429
Santander	0,176			0,021						0,028

Tabla 6.

Indicador de captura por denuncia, hurto calificado y delitos de la Ley 1273 de 2009. (Continuación)

Entidades territoriales	Hurto calificado	Acceso abusivo a un sistema informático	Daño informático	Hurto por medios informáticos y semejantes	Interceptación de datos informáticos	Obstaculización ilegítima de sistema informático o red de telecomunicación	Suplantación de sitios web para capturar datos personales	Transferencia no consentida de activos	Uso de *software* malicioso	Violación de datos personales
Sucre	0,212			0,008						
Tolima	0,123	0,058	0,333	0,038		3,000				0,096
Valle del Cauca	0,070	0,125		0,026	0,038	0,143			0,040	0,160
Vaupés	0,333									
Vichada	0,297									
Total general	0,228	0,130	0,145	0,041	0,008	0,929	0,001	0,075	0,108	0,115