



Delitos informáticos: la recomposición del crimen en la era digital

Mayo 2026

Índice

1. Presentación	2
2. Resumen.....	3
3. Delitos informáticos: impactos, convergencias y redefinición del territorio del crimen.....	4
4. Los delitos informáticos en el código Penal y modalidades asociadas	6
5. Caracterización de los delitos informáticos	10
A. Bogotá en el contexto nacional de los delitos informáticos	10
B. Cambios estructurales en el patrón delictivo en Bogotá: análisis comparado entre delitos informáticos y hurtos tradicionales	14
C. La media tarde como ventana de oportunidad delictiva	20
D. Género y delito informático.....	22
E. Perfil etario de la victimización	25
6. Disposición tecnológica de los hogares y riesgos asociados al delito informático en Bogotá	28
7. Percepción, victimización y denuncia del delito informático desde la EPV - CCB ...	30
8. Conclusiones	33
9. Recomendaciones.....	34

1. Presentación

En los últimos años, la criminalidad ha experimentado una transformación profunda que desborda los marcos tradicionales de análisis centrados exclusivamente en el territorio físico. **La expansión acelerada de las tecnologías digitales, la masificación del uso de internet, el auge de las billeteras digitales y la integración del smartphone en la vida cotidiana, han configurado un nuevo ecosistema delictivo**, en el que los delitos informáticos adquieren creciente relevancia en términos de volumen, impacto social y complejidad institucional.

Este fenómeno no constituye una simple ampliación del repertorio criminal existente, sino una redefinición estructural del territorio del crimen, en la que las fronteras físicas se diluyen y las dinámicas delictivas se anclan en entornos digitales altamente interconectados.

En este contexto, este documento ofrece una lectura integral de los delitos informáticos en Bogotá, articulando enfoques normativos, estadísticos y analíticos. Partiendo de un estado del arte que aborda los impactos sociales y económicos del delito digital, se examinan las convergencias entre criminalidad informática y delitos tradicionales, así como los cambios en las lógicas de oportunidad, riesgo y victimización. Esta aproximación permite **comprender los delitos informáticos no como fenómenos aislados, sino como parte de un proceso de recomposición del patrón delictivo que convive con descensos sostenidos en ciertos delitos como los hurtos**.

El análisis se inscribe además en el marco jurídico colombiano, examinando la forma en que el Código Penal tipifica los delitos informáticos y las principales modalidades asociadas, lo que resulta clave para entender tanto las capacidades como las limitaciones del aparato institucional frente a estas conductas. A nivel territorial, **Bogotá se analiza como un caso estratégico dentro del contexto nacional, no solo por la concentración de casos, sino por su rol como nodo central de actividad digital**, lo que la convierte en un escenario adelantado de tendencias que luego se replican en otros territorios.

El documento profundiza asimismo en dimensiones operativas y criminológicas del delito informático, como la comparación entre tasas de captura, la identificación de ventanas temporales de mayor riesgo, particularmente la media tarde, y el análisis de perfiles diferenciales de victimización por género y edad. A ello se suma el examen de la disposición tecnológica de los hogares, que permite comprender **cómo los patrones cotidianos de uso digital pueden generar ventajas estructurales para la comisión de delitos informáticos, incluso en contextos de creciente alfabetización tecnológica**.

En conjunto, este trabajo busca aportar evidencia y lectura estratégica para la formulación de acciones públicas de seguridad, resaltando que **enfrentar la criminalidad en la era digital exige nuevas capacidades, enfoques preventivos diferenciados y una comprensión ampliada del espacio del crimen**.

2. Resumen

Contexto: Los delitos informáticos presentan una tendencia de crecimiento sostenido entre 2019 y 2024, pasando de 7.208 casos en 2019 a 22.437 en 2024, lo que evidencia una expansión acelerada en el periodo pospandemia. En el año 2025 se observa una disminución del 10% con respecto al 2024, disminuyendo la incidencia en 2.266 casos

Territorialidad criminal: La revisión conceptual y empírica muestra que el delito informático ha redefinido el territorio del crimen, trasladando las dinámicas delictivas hacia espacios digitales donde la información, la interacción y la confianza adquieren un rol central.

Código Penal: El marco penal colombiano reconoce los delitos informáticos como conductas autónomas y tipificadas, aunque su investigación y judicialización enfrentan desafíos asociados a la velocidad del cambio tecnológico y a la complejidad probatoria.

Conectividad: El análisis territorial evidencia que Bogotá ocupa una posición central en la ocurrencia de delitos informáticos a nivel nacional, asociada a su alta conectividad, densidad económica y uso intensivo de tecnologías digitales.

Recomposición delictiva: La comparación entre delitos digitales y hurtos tradicionales confirma una recomposición del patrón delictivo, en la que disminuyen ciertos delitos callejeros mientras crecen modalidades menos visibles y de menor exposición operativa.

Ventanas de oportunidad: Las diferencias en la relación entre capturas y delitos registrados muestran una asimetría estructural, con probabilidades significativamente menores de judicialización en el ámbito del delito informático frente a los delitos tradicionales.

Temporalidad: La concentración de hechos en horas de la media tarde sugiere que el delito informático se articula con rutinas sociales de alta actividad digital y contextos de fatiga cognitiva, más que con esquemas horarios tradicionales.

Victimización: La victimización digital presenta una mayor incidencia en mujeres, relacionada con brechas de exposición, confianza y carga cognitiva. El perfil etario de las víctimas muestra una concentración en población joven-adulta, particularmente en edades con uso intensivo de plataformas digitales, transacciones y servicios en línea.

Percepción ciudadana del delito informático: La encuesta de la CCB muestra que el delito informático gana presencia en la experiencia de victimización, opera con baja visibilidad y enfrenta barreras de denuncia, confirmando su consolidación como componente estructural del nuevo patrón delictivo.

Riesgos cotidianos: La disposición de los hogares a realizar tareas digitales cotidianas configura un entorno de riesgo estructural, donde múltiples interacciones favorecen la operación de delitos informáticos a gran escala.

3. Delitos informáticos: impactos, convergencias y redefinición del territorio del crimen

En las últimas dos décadas, los delitos informáticos se han consolidado como uno de los fenómenos criminales de mayor impacto a nivel global, tanto por su magnitud económica como por su capacidad de afectar simultáneamente a personas, empresas y Estados.

A diferencia de los delitos tradicionales, el cibercrimen produce externalidades sistémicas que trascienden a la víctima directa, al generar presiones sobre la confianza en los sistemas financieros digitales, los servicios públicos en línea y los mecanismos de transacción y denuncia. Este impacto resulta especialmente relevante en contextos urbanos altamente digitalizados, donde la vida cotidiana, la actividad económica y la gestión pública dependen de manera creciente de infraestructuras tecnológicas, lo que amplifica los efectos sociales e institucionales del delito informático.

El crecimiento del delito informático ha ocurrido de forma paralela al desarrollo acelerado de las tecnologías digitales, las redes de comunicación y la economía de plataformas. **La masificación del uso de teléfonos inteligentes, la expansión de las redes sociales, la digitalización de los servicios financieros y la adopción de billeteras digitales han ampliado de manera significativa la superficie de exposición al delito.** Este fenómeno no responde necesariamente a un aumento proporcional en el número de delincuentes, sino a una multiplicación de oportunidades para el crimen derivada de la reducción de costos operativos, la automatización de conductas ilícitas y la posibilidad de realizar acciones criminales con un bajo de exposición para el agresor frente a otras actividades delictivas.

La expansión del entorno digital no solo incrementa las oportunidades delictivas, sino que transforma las lógicas del crimen y exige nuevas capacidades institucionales para su prevención y control.

Un rasgo central de la evolución reciente es que el delito informático no reemplaza plenamente a los delitos tradicionales, sino que los reconfigura y amplifica. Conductas como el hurto, históricamente asociadas al control territorial físico, la coacción directa y la presencialidad, se han adaptado progresivamente al entorno digital. **El uso de billeteras electrónicas, transferencias digitales, pagos instantáneos y criptoactivos ha transformado los mecanismos de exigencia, cobro y ocultamiento del beneficio económico, permitiendo que estas conductas se ejecuten con mayor alcance, anonimato y eficiencia operativa.** En este proceso, se reducen los costos logísticos y los riesgos de exposición para el victimario

Esta convergencia complejiza de manera significativa las estrategias de prevención, control y persecución penal. El entorno digital no solo habilita nuevas formas de criminalidad, sino que

optimiza y moderniza delitos preexistentes, ampliando su impacto potencial y desafiando los esquemas institucionales diseñados para actuar sobre territorios físicos claramente delimitados. En consecuencia, **comprender el delito informático exige reconocer que muchas de sus manifestaciones tienen raíces en prácticas delictivas tradicionales, ahora potenciadas por la conectividad y la deslocalización del riesgo.**

La globalización del cibercrimen introduce, además, un escenario de alta incertidumbre sobre su evolución futura y plantea tensiones profundas para los marcos clásicos de comprensión del delito. **En los entornos digitales, la relación entre autor, víctima, lugar de comisión y jurisdicción legal se vuelve cada vez más difusa.** La distancia física pierde relevancia frente a la conectividad, la arquitectura de las redes y el acceso a sistemas digitales, lo que genera una crisis de la territorialidad como categoría central para interpretar el fenómeno criminal y limita la efectividad de los mecanismos tradicionales de soberanía, control y sanción estatal.

Ante este escenario, resulta necesario replantear la forma en que se interpreta la relación entre espacio y delito. **En el ámbito digital, el control efectivo ya no se ejerce únicamente sobre espacios físicos, sino sobre plataformas, sistemas de pago, redes de datos y canales de comunicación.** Quien detenta control—formal o informal—sobre estos espacios digitales obtiene ventajas estratégicas decisivas. Desde la perspectiva institucional, estas ventajas se traducen en mayores desafíos de capacidades de prevención, detección e intervención; desde el lado criminal, en anonimato, escalabilidad del delito, deslocalización del riesgo y mayores obstáculos para la persecución penal. Así, el espacio no desaparece como variable explicativa, sino que se transforma, exigiendo nuevas categorías analíticas y enfoques de política pública.

En síntesis, el delito informático y la adaptación de delitos tradicionales al entorno digital representan no solo un incremento cuantitativo de la criminalidad, sino un cambio cualitativo en la forma de entender el delito, el territorio y la acción del Estado. Para ciudades como Bogotá, este escenario obliga a complementar los enfoques tradicionales centrados en el espacio físico con una comprensión del territorio digital como un nuevo escenario estratégico del crimen, en el que la seguridad y la justicia dependen crecientemente de capacidades tecnológicas, regulatorias y analíticas acordes con la complejidad del entorno contemporáneo.

4. Los delitos informáticos en el código Penal y modalidades asociadas

Los delitos informáticos se encuentran tipificados en 9 artículos del Código Penal colombiano (Ley 599 de 2000), enmarcados en 2 títulos:

- VII - A: de delitos contra el patrimonio cultural sumergido
- VII – Bis: de la protección de la información y de los datos

Estos 2 títulos fueron incorporados y desarrollados por la Ley 1273 de 2009, la cual creó el bien jurídico de la protección de la información y de los datos, con el fin de adecuar el ordenamiento penal a los riesgos y amenazas asociados al uso indebido de las tecnologías de la información y las comunicaciones (TIC).

A través de este marco normativo, el Estado colombiano reconoce y sanciona conductas que afectan la seguridad digital, el patrimonio económico, la privacidad de las personas y el normal funcionamiento de los sistemas y redes informáticas, en consonancia con los nuevos escenarios del delito en entornos digitales.

La tipificación de los delitos informáticos en Colombia refleja un avance hacia el reconocimiento de nuevas formas de criminalidad digital; no obstante, desde la Ley 1273 de 2009, el entorno tecnológico ha evolucionado con nuevas modalidades de smishing, vishing, malware, extorsión digital y sextorsión, cuya complejidad y sofisticación evidencian que, aunque algunas pueden encajar en los tipos vigentes, el marco normativo resulta parcialmente insuficiente frente a nuevos esquemas de engaño y conductas emergentes, lo que plantea la necesidad de su actualización.

A continuación, se presentan las principales modalidades asociadas a cada uno de los 9 delitos informáticos definidos en los artículos del 269A al 269J del Código Penal. Dichas modalidades difieren de manera sustantiva de las formas convencionales de comisión de los delitos contra el patrimonio, en la medida en que se apoyan en el uso de tecnologías digitales, la automatización de procesos, la suplantación de identidades y la explotación tanto de vulnerabilidades técnicas como de factores humanos.

i. Artículo 269A. Acceso Abusivo A Un Sistema Informático

- **Descripción general:** Ingreso no autorizado, total o parcial, a sistemas, redes o cuentas digitales.
- **Modalidades frecuentes:**
 - *Credential stuffing* (recopilan de credenciales) con bases de datos filtradas en mercados ilegales.
 - Ataques intensivos contra cuentas de correo corporativo o bancario.
 - Explotación de vulnerabilidades en páginas web institucionales o empresariales.
 - Obtención de credenciales mediante *phishing* (correos electrónicos fraudulentos), *smishing* (mensajes de texto engañosos) y *vishing* (llamadas fraudulentas),

- Uso indebido de sesiones abiertas en equipos compartidos (cafés internet, entornos laborales).

ii. Artículo 269B. Obstaculización Ilegítima De Sistema Informático o Red

- **Descripción general:** Acciones dirigidas a interrumpir, ralentizar o impedir el funcionamiento de sistemas o redes.
- **Modalidades frecuentes:**
 - Ataques de denegación de servicio (DDoS) contra portales institucionales o financieros a través de la saturación de servicios.
 - Alteración de configuraciones que bloquean servicios en entidades públicas o privadas.
 - Sabotaje de plataformas empresariales o servicios en línea.

iii. Artículo 269C. Interceptación De Datos Informáticos

- **Descripción general:** Captura no autorizada de datos durante su transmisión o procesamiento.
- **Modalidades frecuentes:**
 - *Sniffing*: interceptar, capturar y registrar los datos que viajan a través redes corporativas o públicas.
 - Ataques tipo *Man-in-the-Middle* (Intercepción entre comunicaciones) en conexiones no seguras.
 - Interceptación en redes Wi-Fi abiertas (centros comerciales, aeropuertos).
 - Captura de tráfico de credenciales o información financiera.

iv. Artículo 269D. Daño Informático

- **Descripción general:** Alteración, destrucción o inutilización de datos o sistemas.
- **Modalidades frecuentes:**
 - Eliminación o corrupción de información.
 - Alteración de bases de datos.
 - Sabotaje lógico de sistemas o aplicaciones.
 - Desconfiguración de servicios o infraestructura tecnológica.

v. Artículo 269E. Uso De Software Malicioso

- **Descripción general:** Introducción o utilización de programas diseñados para causar daño u obtener beneficios ilícitos.
- **Modalidades frecuentes:**
 - *Malware* bancario (troyanos financieros): tipo de software malicioso diseñado para infiltrarse en los dispositivos, robar credenciales de acceso a cuentas, números de tarjetas y vaciar cuentas.
 - *Spyware* (recolección encubierta de información).
 - *Ransomware* (secuestra datos digitales para extorsionar por la devolución de su control).
 - *Keyloggers* (captura de credenciales a través de software o hardware diseñada para registrar de forma secreta cada tecla que se pulsa en el teclado).

vi. Artículo 269F. Violación De Datos Personales

- **Descripción general:** Obtención, divulgación o uso indebido de información personal sin autorización.
- **Modalidades frecuentes:**
 - Filtración de bases de datos.
 - Acceso indebido por usuarios internos autorizados.
 - Recolección engañosa de datos (formularios fraudulentos).
 - Comercialización en mercados ilícitos de datos (*dark web*).

vii. Artículo 269G. Suplantación De Sitios Web Para Capturar Datos Personales

- **Descripción general:** Creación o uso de plataformas falsas para engañar a los usuarios.
- **Modalidades frecuentes:**
 - *Phishing* clásico: Correos o mensajes que redirigen a sitios falsos.
 - Clonación de páginas web oficiales o bancarias: Réplicas visuales casi idénticas.
 - Enlaces maliciosos en redes sociales o mensajería instantánea.

viii. Artículo 269I. Hurto Por Medios Informáticos Y Semejantes

- **Descripción general:** Obtención ilícita de bienes o recursos económicos mediante medios digitales.
- **Modalidades frecuentes:**
 - Fraude electrónico (transferencias no autorizadas).
 - Manipulación de plataformas de pago.
 - Uso indebido de instrumentos de pago digitales.
 - Fraudes en comercio electrónico (operaciones simuladas o engañosas).

ix. Artículo 269J. Transferencia No Consentida De Activos

- **Descripción general:** Desplazamiento de activos digitales o financieros sin autorización del titular.
- **Modalidades frecuentes:**
 - Transferencias electrónicas fraudulentas.
 - Desvío de fondos mediante suplantación de identidad digital.
 - Uso de cuentas intermediarias
 - Explotación de debilidades en procesos de autenticación.

Resulta pertinente señalar que, desde la expedición de la Ley 1273 de 2009, **el ecosistema digital ha experimentado transformaciones que han dado lugar a la aparición y consolidación de nuevas modalidades de comisión de delitos informáticos.**

Entre estas se destacan, por ejemplo, los esquemas avanzados de ingeniería social (como el smishing y el vishing), el uso de malware especializado en fraudes financieros, los ataques dirigidos a infraestructuras digitales críticas, la explotación de plataformas de comercio electrónico y sistemas de pago, así como el uso de criptoactivos y canales digitales para la dispersión y ocultamiento de recursos ilícitos.

De manera complementaria, se ha evidenciado un aumento de prácticas de extorsión apoyadas en medios digitales —incluyendo el ransomware, la extorsión mediante suplantación o acceso indebido a información sensible y las amenazas a través de canales electrónicos—, así como fenómenos asociados al uso indebido de contenidos íntimos generados en entornos digitales (comúnmente vinculados al sexting), tales como la sextorsión o la difusión no consentida de imágenes, que combinan elementos de los delitos informáticos con afectaciones a la intimidad y la libertad individual.

Si bien muchos de estos comportamientos pueden subsumirse en los tipos penales vigentes, **su creciente complejidad técnica y escala operativa evidencian la necesidad de evaluar la actualización normativa, con el fin de mejorar la precisión conceptual, fortalecer las capacidades de persecución penal y responder de manera más efectiva a las dinámicas contemporáneas del delito informático.**

5. Caracterización de los delitos informáticos

A. Bogotá en el contexto nacional de los delitos informáticos

Bogotá ocupa una posición central en la dinámica nacional de los delitos informáticos. Entre 2019 y 2026 (con corte a marzo), la capital concentra de manera consistente 1 de cada 3 de los delitos informáticos registrados en Colombia, con participaciones que oscilan entre el 29% y el 37% del total nacional. Este patrón confirma que el delito informático tiene en Bogotá uno de sus principales escenarios de manifestación, asociado a la mayor densidad poblacional, económica y digital de la ciudad.

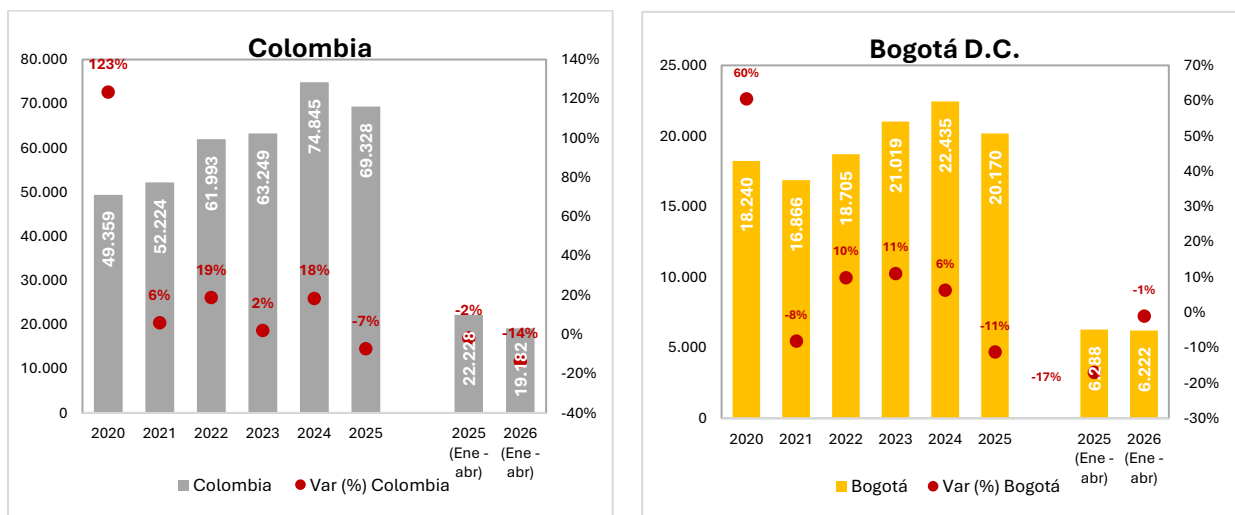
• Evolución temporal de los delitos informáticos

En términos de evolución temporal, tanto Bogotá como Colombia presentan un comportamiento similar: un crecimiento acelerado a partir de 2020, un pico nacional y distrital en el periodo 2023–2024 y una moderación posterior en 2025, con cifras parciales en 2026.

Bogotá no solo concentra una proporción significativa del delito informático nacional, sino que articula condiciones estructurales —conectividad, transaccionalidad y densidad digital— que favorecen la aparición de modalidades más complejas y aceleran la transformación del crimen en Colombia.

En Bogotá, los casos pasaron de 7.207 en 2019 a 22.435 en 2024, casi triplicándose en cinco años, mientras que a nivel nacional el incremento fue de 22.092 a 74.845 casos en el mismo periodo. Esto indica que el crecimiento del delito informático en la ciudad no es un fenómeno aislado, sino parte de una tendencia estructural de alcance nacional, aunque con una mayor intensidad relativa en la capital.

Gráfica 1. Delitos informáticos en Colombia y Bogotá D.C. años 2020 a 2025 y enero – abril de 2025 y 2026. Frecuencia y variación porcentual.



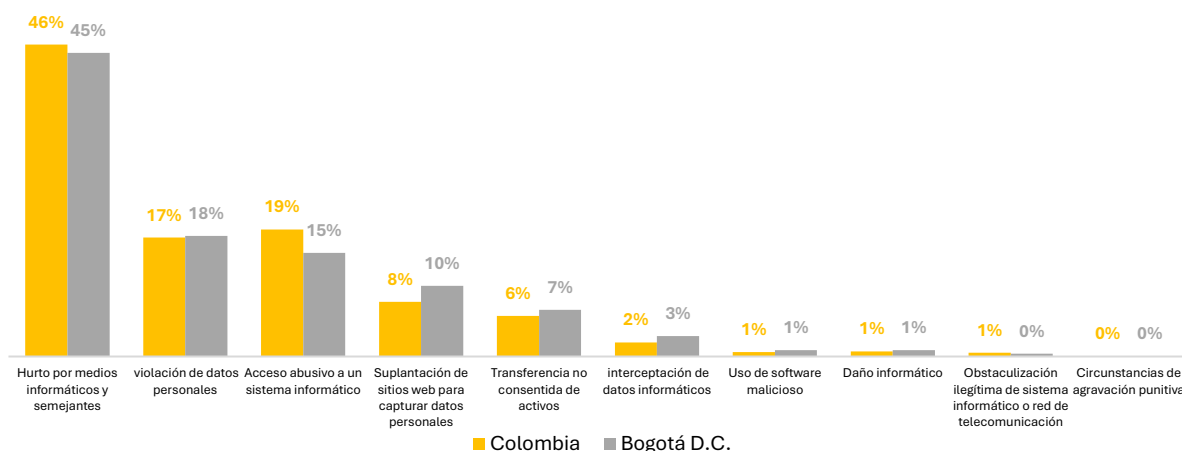
Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos extraídos de SIEDCO Plus el 2026-04-05. Sujetos a variación.

• Delitos informáticos según subtipos penales

Al analizar la composición de los delitos, se observa que el hurto por medios informáticos y semejantes (art. 269I) constituye el principal componente del fenómeno tanto en Bogotá como en Colombia.

En 2024, este delito representó más de la mitad de los casos en la ciudad (12.417 de 22.435) y cerca del 50% del total nacional. Bogotá aporta de manera estable entre el 29% y el 35% de este delito específico, lo que refleja su papel como núcleo financiero y transaccional del país, donde se concentran usuarios, plataformas digitales, comercios electrónicos y operaciones monetarias que amplían la superficie de oportunidad para este tipo de criminalidad.

Gráfica 2. Delitos informáticos Colombia y Bogotá D.C. por tipo penal. 2020 – abril



2026. Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos extraídos de SIEDCO Plus el 2026-04-05. Sujetos a variación.

Otros delitos muestran una participación de Bogotá particularmente elevada, lo que sugiere especializaciones relevantes. La interceptación de datos informáticos (art. 269C) presenta una de las participaciones más altas, con porcentajes cercanos o superiores al 40% durante todo el periodo, alcanzando hasta el 50% en algunos años.

De manera similar, el uso de software malicioso (art. 269E) registra históricamente participaciones de Bogotá superiores al promedio general, con valores que se ubican entre el 41% y el 60%. Estos comportamientos indican que la ciudad no solo concentra volumen, sino también delitos de mayor complejidad tecnológica, consistentes con su mayor nivel de conectividad y uso intensivo de sistemas digitales.

En el caso de la violación de datos personales (art. 269F) y la suplantación de sitios web para capturar datos personales (art. 269G), Bogotá mantiene participaciones relevantes y relativamente estables, cercanas a un tercio o más del total nacional.

Aunque en algunos años la participación relativa disminuye, el volumen absoluto continúa siendo alto, lo que sugiere que el menor peso porcentual responde más a la expansión del fenómeno en otras regiones del país que a una reducción estructural del problema en la ciudad.

- **Delitos informáticos en Bogotá y departamentos**

De manera transversal, el análisis comparado permite concluir que Bogotá actúa como un “amplificador” del delito informático a escala nacional: los cambios tecnológicos, sociales y económicos tienden a manifestarse primero y con mayor intensidad en la capital, para luego extenderse a otros territorios. Esta condición explica por qué, incluso cuando la participación porcentual de Bogotá se estabiliza o disminuye ligeramente, la ciudad sigue concentrando un volumen muy significativo de casos y presenta modalidades delictivas de mayor sofisticación.

En síntesis, el contexto comparado muestra que Bogotá no solo aporta una fracción sustancial del delito informático del país, sino que representa un laboratorio adelantado de las transformaciones del cibercrimen en Colombia.

Esto refuerza la necesidad de que la ciudad sea un eje prioritario para el análisis, la prevención y el fortalecimiento de capacidades institucionales frente a estos delitos, no solo por su impacto local, sino por su efecto demostrativo sobre el resto del territorio nacional.

La mayor incidencia del delito informático en territorios altamente conectados refleja un efecto estructural de la digitalización, que incrementa simultáneamente las oportunidades para la actividad delictiva.

El análisis comparado a nivel departamental confirma que el delito informático en Colombia presenta una marcada concentración territorial, estrechamente relacionada con los niveles diferenciados de uso de internet. Bogotá se destaca como el principal foco del fenómeno, al concentrar aproximadamente el 30% del total nacional de delitos informáticos, una proporción significativamente superior a su peso relativo dentro de la población del país (15%), lo que evidencia una sobrerrepresentación del fenómeno en la ciudad. Adicionalmente registra una tasa de 333 delitos por cada 100.000 habitantes, muy superior al promedio del país y al del resto de departamentos.

Si bien la ciudad no presenta una proporción de uso de internet sustancialmente distante de otros departamentos con alta conectividad —como Valle del Cauca, Antioquia o Cundinamarca—, sí exhibe una **intensidad delictiva significativamente mayor**, lo que la posiciona como un caso atípico en términos de volumen y magnitud del fenómeno dentro del contexto nacional.

Esta condición resulta coherente con su papel como principal núcleo urbano, económico y digital del país, donde convergen de manera más intensa las dinámicas de interacción en entornos digitales y, en consecuencia, los riesgos asociados.

Más allá del caso de Bogotá, el patrón departamental muestra que un número reducido de territorios concentra la mayor parte del delito informático. Antioquia (13%), Valle del Cauca (10%), Cundinamarca (7%) y Atlántico (5%) explican conjuntamente una proporción sustancial adicional del total nacional, de modo que pocos departamentos concentran cerca de dos tercios de los registros.

Estos territorios corresponden, en su mayoría, a áreas altamente urbanizadas y con mayores niveles de inserción en el ecosistema digital, lo que refuerza la hipótesis de que el delito informático no se distribuye homogéneamente, sino que se ancla selectivamente en territorios con mayor densidad poblacional, económica y tecnológica.

El gráfico evidencia una clara relación estructural: existe una correlación positiva fuerte entre el porcentaje de personas que usan internet y la tasa de delitos informáticos por cada 100.000 habitantes. A medida que aumenta el nivel de uso de internet en los departamentos, se incrementa de forma consistente la intensidad del delito informático.

No obstante, Bogotá se ubica claramente por encima de la tendencia general, lo que sugiere la presencia de factores adicionales que intensifican el fenómeno en la ciudad.

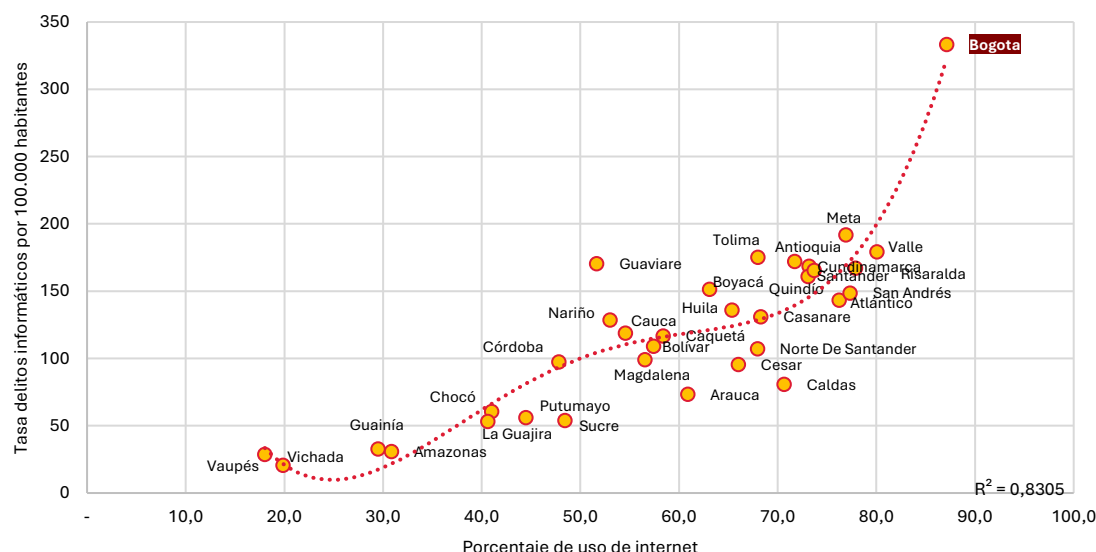
En contraste, departamentos con niveles bajos de uso de internet, como Vaupés, Vichada, Amazonas o Guainía (por debajo del 30%), presentan tasas muy reducidas; mientras que aquellos con niveles de uso superiores al 70% registran tasas significativamente más altas, concentrándose en el cuadrante superior derecho del gráfico.

Bogotá representa el extremo superior de esta relación, combina el mayor nivel de uso de internet (87,1%) con la mayor tasa de delitos informáticos del país. Otros departamentos con altos niveles de conectividad y tasas elevadas incluyen Meta, Valle del Cauca, Tolima, Antioquia, Cundinamarca y Risaralda, lo que indica que el fenómeno no es exclusivo de la capital, sino que se reproduce —aunque con distinta magnitud— en territorios que comparten una mayor integración a redes digitales, plataformas financieras, servicios en línea y transacciones electrónicas.

Este comportamiento sugiere que la mayor incidencia del delito informático no debe interpretarse únicamente como una falla de control o gestión de seguridad, sino como un efecto estructural de la digitalización territorial. Los departamentos con mayor penetración de internet concentran también mayores oportunidades delictivas, tanto para delitos nativamente digitales como para la adaptación de delitos tradicionales al entorno virtual. En contraste, territorios con menor conectividad exhiben menores tasas del delito, no necesariamente por una mayor efectividad institucional, sino por una menor exposición al espacio digital donde estas conductas se materializan.

La mayor incidencia del delito informático en territorios altamente conectados no necesariamente refleja fallas institucionales, sino un efecto estructural de la digitalización, que incrementa simultáneamente las oportunidades para la actividad delictiva.

Gráfica 3. Relación entre tasa de delitos informáticos por 100.000 habitantes y porcentaje de uso de internet en Bogotá y Departamentos de Colombia.



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos extraídos de SIEDCO Plus el 2026-04-05. Sujetos a variación.

En síntesis, la evidencia departamental y el análisis gráfico confirman que el delito informático en Colombia es un fenómeno selectivamente urbano y digital, fuertemente condicionado por los niveles de acceso y uso de internet.

Bogotá y un conjunto reducido de departamentos altamente digitalizados concentran la mayor parte del problema y presentan las tasas más elevadas, lo que tiene implicaciones directas para la política pública: las estrategias de prevención, control y fortalecimiento institucional deben priorizar estos territorios no solo por su peso estadístico, sino porque allí se anticipan y se intensifican las dinámicas del cibercrimen que, con el tiempo, tienden a extenderse al resto del país conforme avanza la digitalización.

B. Cambios estructurales en el patrón delictivo en Bogotá: análisis comparado entre delitos informáticos y hurtos tradicionales

Entre 2019 y 2026, Bogotá evidencia un **cambio estructural en la composición del delito**, caracterizado por la coexistencia de una **reducción progresiva de varias modalidades de hurto tradicional** y un **crecimiento sostenido de los delitos informáticos**, especialmente a partir de 2020. Esta dinámica no responde a una simple sustitución lineal entre delitos físicos y digitales, sino a una **reconfiguración del portafolio delictivo**, en la que las actividades criminales tienden a desplazarse hacia modalidades menos visibles, con mayor dependencia de capacidades tecnológicas y menores riesgos operativos para los delincuentes.

En este contexto, el hurto en general opera como un **delito bisagra**: se mantiene dominante en el conjunto de los delitos urbanos, pero se evidencia pérdida de prevalencia que contrasta con el crecimiento de los delitos informáticos.

La evidencia muestra que el delito en Bogotá evoluciona hacia un modelo híbrido, donde conviven la persistencia de modalidades tradicionales con la expansión acelerada del delito informático, lo que exige nuevas capacidades institucionales de prevención, control e investigación.

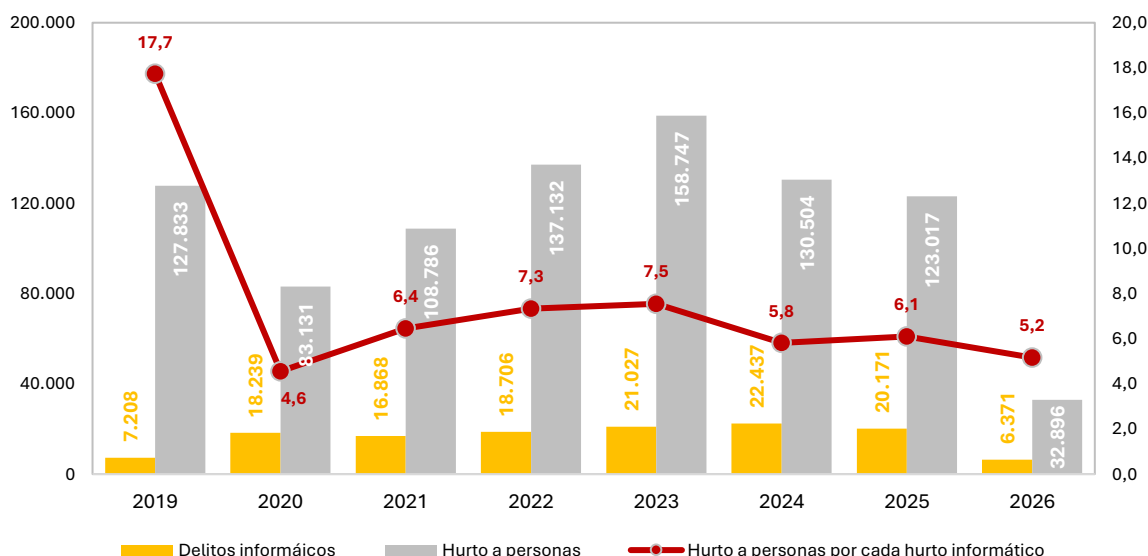
En conjunto, los datos del periodo muestran que **las reducciones en hurto no implican, por sí mismas, una reducción integral del delito**, sino que coexisten con nuevas formas de criminalidad que plantean desafíos distintos a la política pública en seguridad, prevención y control.

- **Hurto a personas: persistencia del volumen, reducción relativa frente a delitos informáticos**

El hurto a personas continúa teniendo el mayor volumen absoluto de registros en la ciudad. No obstante, su comportamiento comparado con los delitos informáticos revela una **pérdida relativa de predominancia**. Mientras que en 2019 se registraban cerca de 18 hurtos a personas por cada delito informático, esta relación cae abruptamente en 2020 y, aunque presenta oscilaciones posteriores, no retorna a los niveles prepandemia.

El fuerte crecimiento de los delitos informáticos, sumado a la mayor volatilidad del hurto a personas, evidencia que **la criminalidad urbana ya no se explica exclusivamente por la violencia o el contacto directo**, sino por esquemas que operan de forma remota y masiva.

Gráfica 4. Relación de hurto a personas vs. Delitos informáticos en Bogotá.



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

- **Hurto de celulares: pérdida de centralidad frente al delito digital**

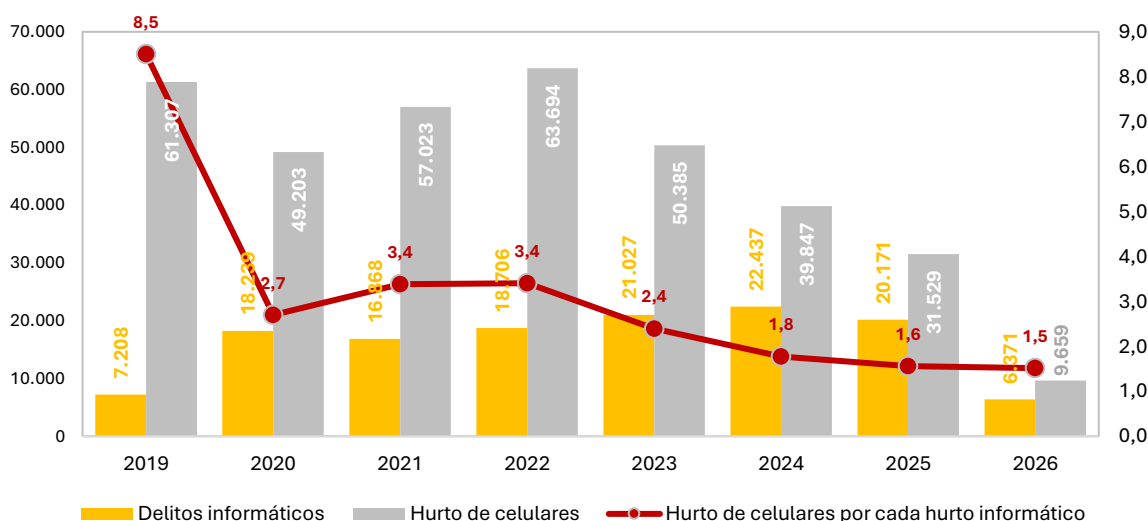
El hurto de celulares presenta un **comportamiento claramente diferenciado** frente a los delitos informáticos.

Tras alcanzar su punto más alto en 2022 (63.694 casos), inicia una disminución sostenida que se mantiene en 2023, 2024 y 2025, hasta ubicarse en 31.529 casos. Aunque la cifra de 2026 (9.659 casos) debe interpretarse como parcial, refuerza una **tendencia descendente estructural**.

En contraste, los delitos informáticos crecen aceleradamente entre 2019 y 2024, multiplicándose por más de tres en ese período.

Esta divergencia se refleja en la reducción sostenida de la relación entre ambos delitos, lo que sugiere que el celular deja de ser, progresivamente, uno de los principales activos del delito tradicional, mientras gana peso como **medio de victimización digital**, más que como objeto de hurto físico.

Gráfica 5. Relación de hurto de celulares vs. Delitos informáticos en Bogotá.



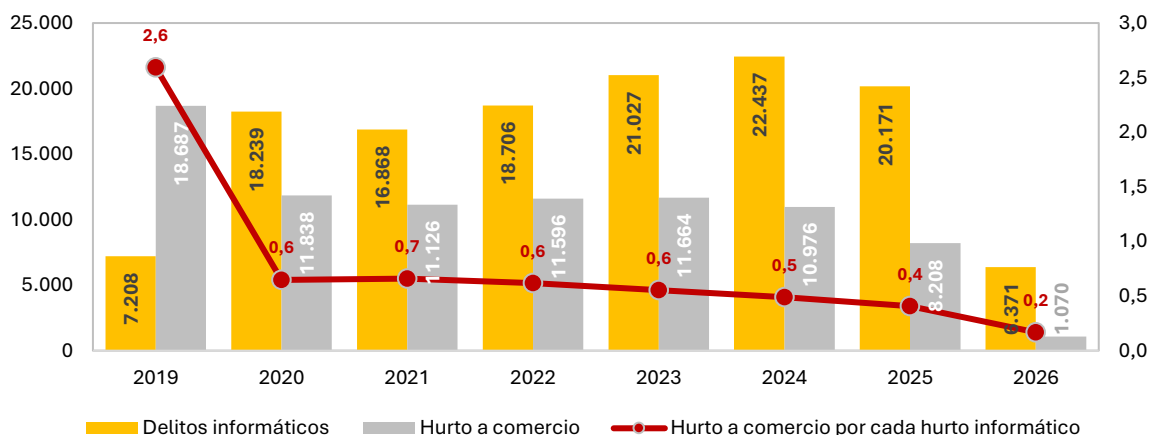
Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

- **Hurto a comercio: contracción sostenida y desplazamiento del riesgo**

El hurto a comercio muestra una **tendencia claramente decreciente** en el periodo analizado, especialmente a partir de 2019, con descensos continuos hasta 2025 y un nivel muy bajo en 2026 (dato parcial).

En paralelo, los delitos informáticos no solo crecen, sino que superan ampliamente esta modalidad desde 2020. La relación entre ambos delitos pasa de 2,6 hurtos a comercio por cada delito informático en 2019, a menos de 0,5 en 2024 y a niveles marginales en 2026. Este comportamiento sugiere un **traslado del riesgo del entorno físico del comercio al entorno digital**, donde las afectaciones se manifiestan a través de fraudes electrónicos, suplantaciones y ataques a sistemas de pago.

Gráfica 6. Relación de hurto a comercio vs. Delitos informáticos en Bogotá.



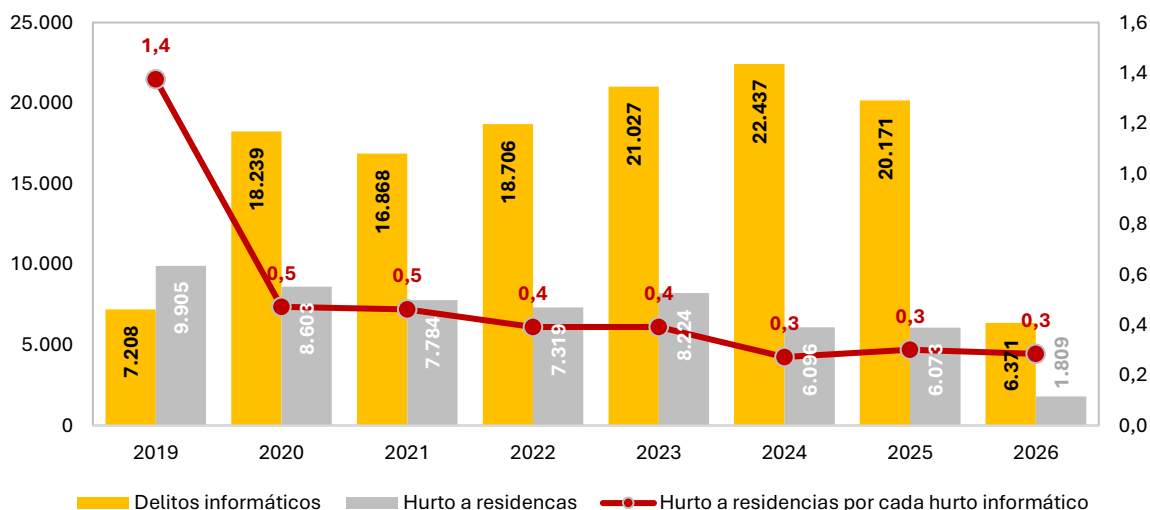
Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

- Hurto a residencias: estabilidad baja y pérdida de peso relativo**

El hurto a residencias presenta una **estabilidad relativa en niveles moderados**, con una leve tendencia descendente en el mediano plazo. Sin embargo, al contrastarlo con los delitos informáticos, se observa una reducción sostenida de su peso relativo: mientras que en 2019 se registraba más de un hurto a residencia por cada delito informático, desde 2020 esta relación se ubica de manera consistente por debajo de 0,5.

Este patrón indica que, aunque el delito contra la vivienda persiste, **ya no constituye una modalidad central dentro del ecosistema delictivo**, frente a la creciente sofisticación y escalabilidad del delito digital.

Gráfica 7. Relación de hurto a residencias vs. Delitos informáticos en Bogotá.

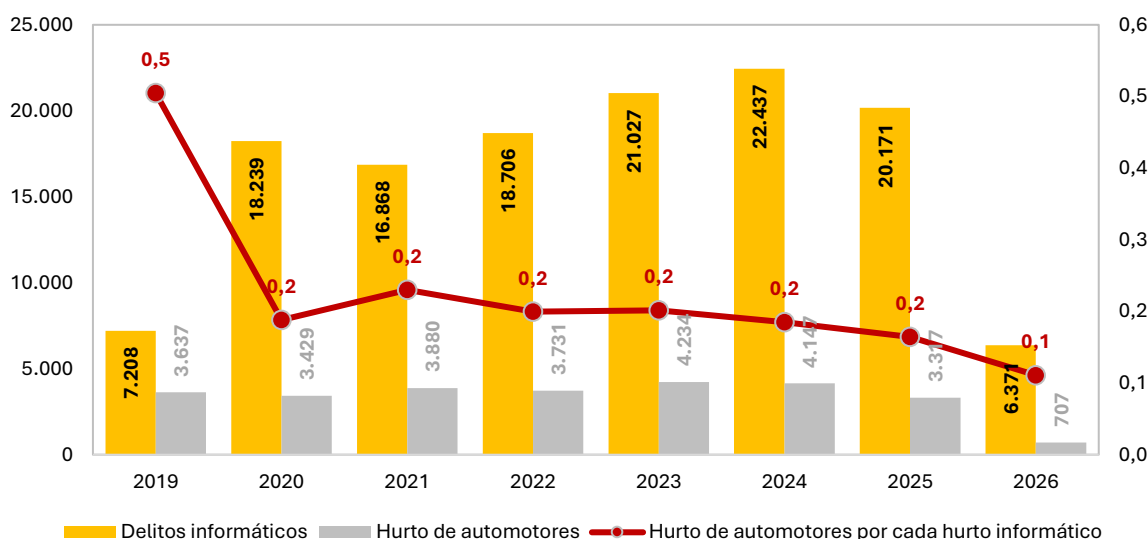


Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

- **Hurto de automotores: estabilidad contenida frente a expansión digital**

El hurto de automotores presenta una tendencia relativamente estable, con variaciones moderadas a lo largo del periodo. Sin embargo, al compararse con los delitos informáticos, muestra una clara pérdida de relevancia relativa. La relación entre ambos desciende de manera sostenida desde 2019 —cuando se registraba cerca de medio hurto por cada delito informático— hasta niveles cercanos a 0,16 en 2025 y aún más bajos en 2026. Este comportamiento sugiere que los delitos que implican mayor logística y riesgo operativo evolucionan con menor rapidez que aquellos asociados a dinámicas digitales.

Gráfica 8. Relación de hurto de automotores vs. Delitos informáticos en Bogotá.



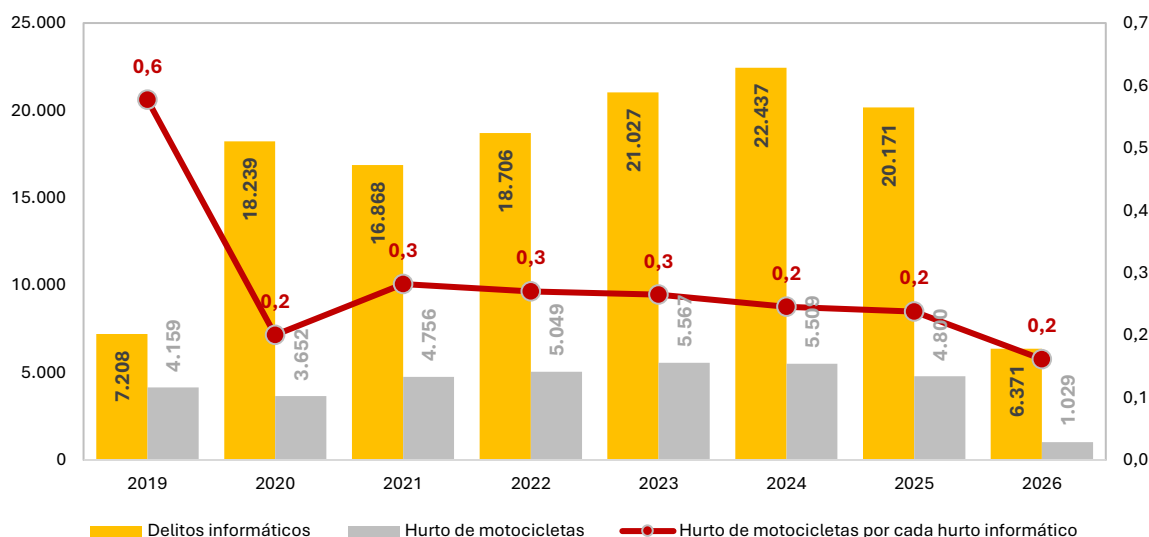
Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

- **Hurto de motocicletas: crecimiento físico controlado y subordinación relativa**

El hurto de motocicletas muestra un crecimiento moderado entre 2021 y 2023, seguido de una leve reducción posterior. Sin embargo, al contrastarlo con los delitos informáticos, se mantiene una relación consistentemente baja durante todo el periodo, inferior a 0,3 desde 2021. Esto confirma que, aunque esta modalidad conserva relevancia operativa para ciertas dinámicas criminales, **no compite en escala ni velocidad de crecimiento con el delito informático**, que concentra cada vez mayor impacto agregado sobre la ciudadanía.

En conjunto, el análisis comparado evidencia que Bogotá atraviesa una **fase de transición del patrón delictivo**, donde los avances en la reducción de varios hurtos tradicionales coexisten con un **crecimiento estructural del delito informático**. Este escenario plantea el reto de adaptar la política pública de seguridad a un entorno en el que **la disminución del delito visible no equivale a una reducción del riesgo total**, y donde la prevención, el control y la investigación requieren capacidades tecnológicas, analíticas e interinstitucionales sustancialmente distintas.

Gráfica 9. Relación de hurto de motocicletas vs. Delitos informáticos en Bogotá.



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

- Riesgo asociado a capturas por delitos informáticos y por hurto**

Esta recomposición del patrón delictivo no solo se expresa en el volumen relativo de los delitos, sino también en la **estructura del riesgo asociado a su comisión**, particularmente evidente en el caso de los delitos informáticos.

Tabla 1. Tasa de capturas por cada 10.000 delitos, según conducta delictiva en Bogotá.

Delitos	2019	2020	2021	2022	2023	2024	2025
Delitos informáticos	9,7	2,9	2,7	1,7	2,0	2,2	3,1
Hurto de automotores	29,4	39,1	29,9	31,4	41,1	47,5	93,8
Hurto a comercio	335,7	273,6	227,5	236,8	320,2	326,3	427,3
Hurto de motocicletas	14,4	18,9	15,6	17,8	19,4	18,9	28,8
Hurto a personas	90,8	97,2	66,7	49,8	47,1	52,2	53,5
Hurto a residencias	23,1	21,0	18,1	26,1	24,2	26,9	25,2

Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

El análisis de la relación entre capturas y delitos registrados muestra que, mientras las diferentes clasificaciones de hurto tradicional mantienen o incrementan sus niveles de judicialización relativa, los delitos informáticos presentan una **caída persistente en la probabilidad efectiva de captura**. En efecto, la razón de capturas por delitos informáticos descende de 9,7 en 2019 a un mínimo de 1,7 en 2022, ubicándose de manera sistemática por debajo de todos los delitos de hurto analizados durante el periodo. Aunque entre 2023 y 2025 se observa una leve recuperación del indicador, este se mantiene en niveles estructuralmente

bajos, lo que confirma que **el delito digital opera en un entorno de menor exposición al control penal.**

La transformación del patrón delictivo se acompaña de una redistribución del riesgo penal, en la que los delitos informáticos concentran menores tasas de captura, favoreciendo su expansión frente a modalidades tradicionales más expuestas.

La integración de este comportamiento con la evolución comparada del hurto refuerza la hipótesis de un desplazamiento del riesgo delictivo: a medida que se reducen los incentivos y aumentan los costos del delito callejero, producto de mejoras en control, prevención situacional y focalización operativa, emergen con mayor fuerza modalidades delictivas que combinan alta rentabilidad, escalabilidad y bajo riesgo de captura, como los delitos informáticos.

En términos estratégicos, los datos sugieren que la recomposición del perfil delictivo no responde únicamente a cambios en oportunidades de victimización, sino también a una reconfiguración racional de la actividad criminal, donde la menor probabilidad de judicialización se convierte en un factor central para el crecimiento de los delitos informáticos.

C. La media tarde como ventana de oportunidad delictiva

Tabla 2. Delitos informáticos según rango horario en Bogotá. Enero 2024 a marzo 2026.

Día/rango hora	00:00 – 02:59	03:00 – 05:59	06:00 – 08:59	09:00 – 11:59	12:00 – 15:59	15:00 – 17:59	18:00 – 20:59	21:00 – 23:59	Total
Lunes	680	742	377	713	872	1.222	1.300	975	6.881
Martes	906	813	387	741	1.044	1.549	1.445	1.078	7.963
Miércoles	979	782	373	832	1.034	1.506	1.493	1.096	8.095
Jueves	932	824	386	841	1.026	1.457	1.505	1.035	8.006
Viernes	976	827	413	727	1.007	1.387	1.461	1.148	7.946
Sábado	891	692	428	558	702	1.007	1.043	687	6.008
Domingo	683	557	336	396	421	555	604	528	4.080
Total	6.047	5.237	2.700	4.808	6.106	8.683	8.851	6.547	48.979

Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO

La ocurrencia de **delitos informáticos presenta una concentración significativa en la franja comprendida entre las 15:00 y las 21:00 horas, de lunes a viernes.** En este intervalo se registra **el 29% del total semanal de delitos**, pese a que representa únicamente **el 18% del tiempo total de la semana**, lo que evidencia una **sobrerrepresentación clara del riesgo en estas horas.**

La concentración en estos horarios se debe principalmente a 4 factores:

1. **Concentración de actividades cotidianas y multitarea.** En estos horarios se intensifican los desplazamientos urbanos, interacciones sociales y uso simultáneo de dispositivos digitales, asociado al cierre parcial de la jornada laboral, las salidas laborales o estudiantiles, uso de redes públicas y la realización de trámites personales. En ese sentido, se amplía la exposición de personas a múltiples entornos, físicos y digitales, de manera simultánea, lo que incrementa el número de objetivos potenciales y reduce la atención y control en el uso de dispositivos. En contextos urbanos altamente conectados¹, esta intensificación de actividades cotidianas genera condiciones propicias para la ocurrencia de conductas delictivas, especialmente aquellas que dependen del contacto digital y de la respuesta inmediata del usuario.
2. **Incremento del tráfico digital, asociado a los patrones de acceso a internet en la región.** Estudios regionales han identificado que **América Latina presenta un uso predominantemente móvil**, con una alta dependencia del smartphone para la realización de trámites, comunicaciones y transacciones. Según diversos análisis sobre consumo digital en la región (Comscore, DataReportal, We Are Social), estas actividades **se concentran en franjas de alta actividad cotidiana**, especialmente en los periodos de transición entre la jornada laboral y la vida personal. En estos momentos se intensifica la interacción digital en **intervalos cortos y simultáneos**, lo que incrementa el tráfico en línea y amplía de manera significativa la **superficie de ataque para fraudes informáticos, prácticas de phishing y suplantaciones**, particularmente cuando los usuarios realizan múltiples tareas y los sistemas operan con mayores niveles de carga.

El aumento de la vulnerabilidad en la media tarde está asociado al desgaste cognitivo acumulado, que favorece respuestas automáticas y disminuye la capacidad de detectar señales de fraude en entornos digitales.

3. **Deterioro de la capacidad de atención y evaluación de riesgo asociada a la acumulación de esfuerzo mental a lo largo del día.** Tras varias horas de actividad cognitiva continua, disminuyen el autocontrol, la atención sostenida y la capacidad de detectar señales de riesgo. Este desgaste mental favorece respuestas automáticas y reduce la resistencia frente a estímulos engañosos, como mensajes fraudulentos, enlaces maliciosos o solicitudes que aparentan legitimidad. En entornos digitales, donde las decisiones se toman en segundos y con información parcial, esta condición incrementa de manera significativa la vulnerabilidad de los usuarios frente a delitos informáticos.

¹ De acuerdo con la ENTIC Hogares 2024 del DANE, Bogotá presenta un patrón de alta disponibilidad y uso intensivo de dispositivos digitales en la población de 5 años y más. El 93,8 % de las personas reporta uso de teléfono celular, con una alta predominancia de smartphones (84,4 %), mientras que el uso de internet alcanza el 88,4 %. Por su parte, el 56,7 % utiliza computador —principalmente portátil (40,8 %) frente a equipos de escritorio (35,2 %)— y el uso de tabletas se mantiene en niveles más bajos (7,2 %). En conjunto, estos datos evidencian un ecosistema doméstico altamente digitalizado, caracterizado por la centralidad del teléfono inteligente como principal dispositivo de acceso y por una amplia penetración de servicios digitales en los hogares de la ciudad.

4. **Percepción de normalidad y relajación de los mecanismos de alerta.** A diferencia de otros momentos del día, en los que la atención preventiva o el control institucional son más visibles, este período tiende a presentar una dispersión de responsabilidades tanto a nivel personal como organizacional. En el ámbito digital, esta situación se traduce en una menor vigilancia activa por parte de los usuarios y una mayor dependencia de mecanismos automatizados de seguridad, cuya eficacia está condicionada al comportamiento final de la persona. Esta combinación facilita la comisión de delitos, especialmente aquellos que requieren interacción directa y una respuesta rápida del objetivo.

De manera consistente con estos patrones, **la ciberdelincuencia opera con lógicas organizativas que se ajustan a los horarios de mayor actividad de la población objetivo.**

Lejos de tratarse de acciones improvisadas, muchas redes delictivas digitales sincronizan sus operaciones con franjas de alta conectividad y respuesta inmediata, maximizando la probabilidad de éxito de estafas, campañas de phishing o intentos de fraude. La media tarde se convierte así en un momento óptimo para este tipo de conductas, al combinar altos niveles de actividad, disponibilidad del usuario y mayor vulnerabilidad cognitiva.

En contraste, la baja incidencia de delitos informáticos durante los días domingo puede explicarse por la ruptura de las rutinas sociales y digitales asociadas a los días hábiles. En este día se registra una disminución significativa de trámites, transacciones financieras, comunicaciones laborales y accesos a plataformas institucionales, que constituyen precisamente los contextos más explotados por los delitos informáticos basados en ingeniería social.

A ello se suma una menor presión temporal y cognitiva sobre las personas, lo que favorece una atención más consciente y reduce la probabilidad de respuestas impulsivas frente a mensajes engañosos.

Desde una lógica operativa, esta combinación reduce tanto la cantidad de objetivos disponibles como la efectividad de los engaños, lo que explica la menor participación relativa del domingo en el total de hechos registrados.

D. Género y delito informático

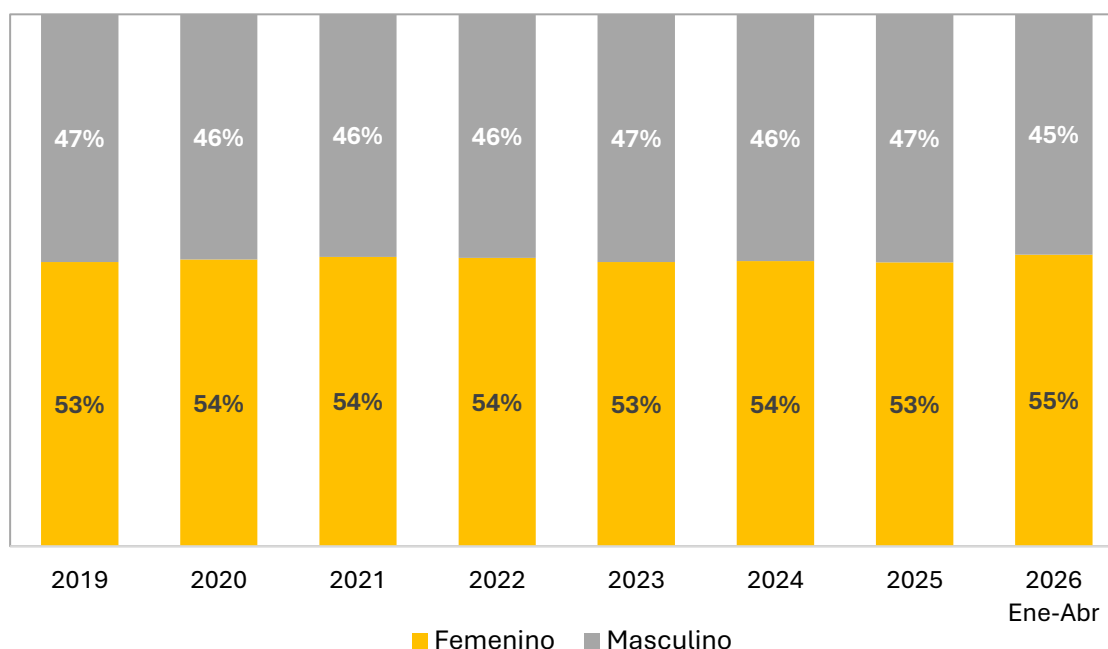
El comportamiento de los delitos informáticos según sexo de la víctima entre 2019 y 2026 muestra una **mayor afectación sistemática de mujeres frente a hombres**, tendencia que se mantiene estable a lo largo del periodo analizado.

En todos los años, las mujeres registran más casos de victimización por delitos informáticos que los hombres, con diferencias que son consistentes y estructurales. Por ejemplo, en 2024 se reportaron 11.784 víctimas femeninas frente a 10.208 masculinas, y en 2025 la relación se

mantiene con 10.511 casos femeninos frente a 9.191 masculinos. Incluso entre enero y marzo de 2026, la brecha persiste (3.420 frente a 2.820).

Esta mayor afectación puede interpretarse a la luz de los patrones diferenciados de uso del entorno digital. Diversos estudios han documentado que las **mujeres presentan mayor participación relativa en plataformas de interacción social, servicios de mensajería, comercio electrónico y trámites digitales cotidianos**, lo que amplía su exposición a interacciones mediadas por confianza, uno de los principales vectores de los delitos informáticos.

Gráfica 10. Delitos informáticos por sexo de las víctimas, 2019 – 2020 y Enero-abril de 2026



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

En este sentido, la victimización no responde a una mayor propensión individual al riesgo, sino a una posición estructural de uso intensivo y multifuncional del ecosistema digital, especialmente en contextos urbanos.

Desde el enfoque psicológico, los delitos informáticos, particularmente aquellos basados en ingeniería social, explotan mecanismos cognitivos universales como la confianza, la reciprocidad, la urgencia y la autoridad percibida. En contextos de alta carga cognitiva y multitarea (trabajo remunerado, cuidado, gestión doméstica y social), es razonable suponer una mayor vulnerabilidad situacional frente a mensajes engañosos, suplantaciones o solicitudes fraudulentas. En este marco, la sobrerrepresentación femenina puede leerse como el resultado de una mayor presión decisional acumulada en el uso cotidiano de tecnologías digitales.

Adicionalmente, el comportamiento paralelo de ambos sexos a lo largo del tiempo, incremento pronunciado entre 2020 y 2024 y moderación posterior, sugiere que las dinámicas macro del delito informático afectan de manera transversal, pero con impactos diferenciales según el posicionamiento social de los grupos. Es decir, hombres y mujeres responden a los mismos shocks estructurales (digitalización acelerada, intensificación del fraude, expansión de plataformas), pero la magnitud de la afectación varía en función de los roles sociales y patrones de interacción digital.

En conjunto, la evidencia confirma que el delito informático incorpora una dimensión de género, en la que las diferencias en uso, interacción y carga cognitiva del entorno digital configuran vulnerabilidades específicas.

Desde una perspectiva de política pública, esta evidencia refuerza la **necesidad de incorporar el enfoque de género en las estrategias de prevención del delito informático**, no desde una lógica asistencial o de vulnerabilidad pasiva, sino desde el reconocimiento de exposiciones diferenciadas al riesgo. La persistencia de la brecha a lo largo del periodo indica que las

campañas genéricas de autocuidado digital pueden resultar insuficientes si no consideran los contextos reales de uso, la carga cognitiva y los canales de victimización predominantes en cada población.

De acuerdo con la ENTIC Hogares 2024 del DANE, en Bogotá las mujeres presentan una mayor disposición relativa a participar en interacciones digitales basadas en respuesta directa, como completar cuestionarios en smartphone (35,6% entre “algo” y “muy dispuestas”), responder mensajes de texto (30,4%) y descargar aplicaciones asociadas a encuestas (30,7%). Este patrón incrementa su exposición a riesgos de delitos informáticos basados en ingeniería social, en particular a esquemas de phishing, suplantación y fraude que dependen de la interacción del usuario y de la confianza en canales digitales.

En el caso de los hombres muestran una mayor disposición relativa en conductas vinculadas a funcionalidades técnicas de los dispositivos, como la conexión vía Bluetooth en teléfonos inteligentes (46,1% entre “algo” y “muy dispuestos”) y tabletas (36,4%), así como la habilitación de permisos o modificaciones del dispositivo (37,4%). Este comportamiento incrementa la exposición a riesgos asociados a vulnerabilidades técnicas, accesos no autorizados y explotación de permisos, propios de modalidades de delito informático que operan a través de la configuración y conectividad de los dispositivos.

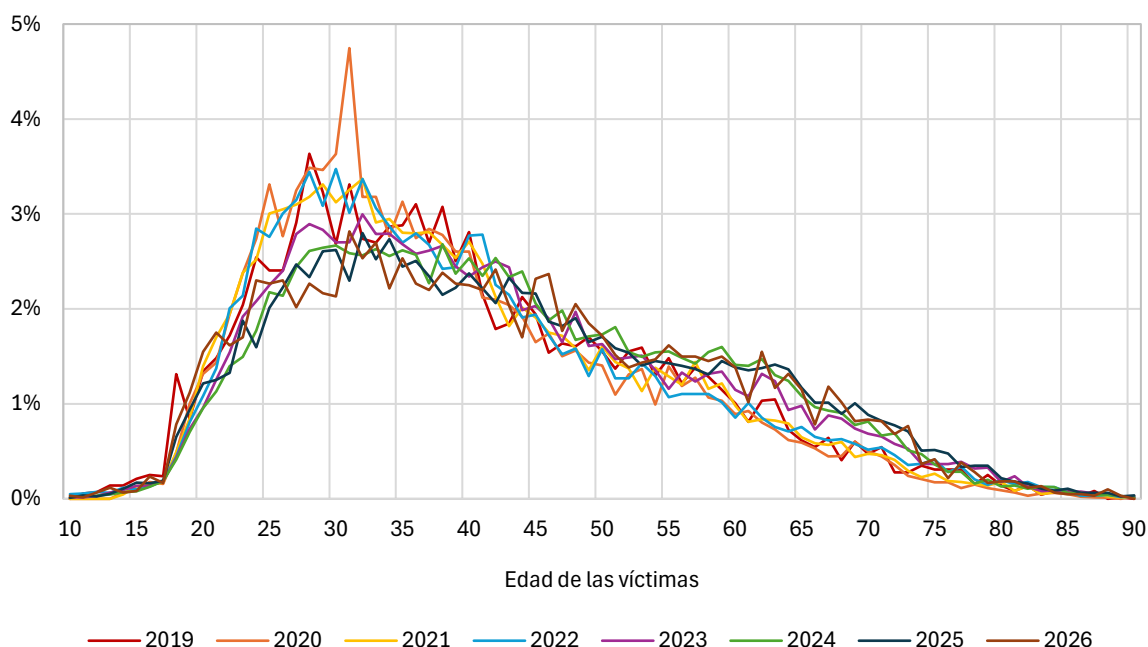
En síntesis, la mayor victimización femenina en los delitos informáticos debe entenderse como el resultado de una interacción compleja entre factores sociotécnicos y psicológicos, donde confluyen mayor presencia en entornos digitales relacionales, explotación de la confianza como mecanismo delictivo y condiciones de uso que incrementan la exposición al engaño.

E. Perfil etario de la victimización

La distribución de los delitos informáticos por edad muestra un patrón consistente y estructural a lo largo del tiempo. En todos los años analizados se observa un incremento progresivo desde la adolescencia tardía, un pico claramente definido entre los 25 y 35 años, con un máximo alrededor de los 30, y un descenso gradual a partir de los 40 años que se extiende hasta las edades más avanzadas.

La estabilidad de esta forma, independientemente del año observado, sugiere que el perfil etario del delito informático no responde a coyunturas específicas, sino a factores estructurales asociados a la inserción de las personas en la vida social y digital.

Gráfica 11. Porcentaje de delitos informáticos en Bogotá según la edad de las víctimas. Años 2019 a 2025.



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

La mayor concentración del delito informático en la adultez joven coincide con la etapa del ciclo vital en la que las personas presentan una **mayor densidad simultánea de roles y obligaciones**. Entre los 25 y los 35 años se concentran el empleo, el uso intensivo del sistema financiero, la realización de trámites digitales, el consumo en línea y la participación activa en redes sociales y plataformas tecnológicas. Esta posición central dentro de la economía y la sociedad digital amplía de manera significativa la exposición cotidiana a entornos donde se materializan los delitos informáticos, lo que explica su mayor peso relativo en este grupo etario.

Este patrón se relaciona con procesos de socialización tecnológica. **El grupo etario que concentra el mayor porcentaje de delitos informáticos corresponde a generaciones que no solo utilizan herramientas digitales, sino que estructuran su vida cotidiana a través de ellas.** En estos grupos, la conectividad permanente, la multitarea digital y la interacción constante con plataformas y servicios en línea forman parte de prácticas normalizadas.

Esta cultura digital tiende a naturalizar el riesgo, reduciendo la percepción de amenaza asociada al intercambio de información, la rapidez en la toma de decisiones o la respuesta automática a estímulos digitales, lo que incrementa la probabilidad de exposición al delito.

El descenso progresivo del porcentaje de delitos informáticos en edades mayores no implica una desaparición de la vulnerabilidad, **sino un cambio en el tipo y volumen de interacción digital.** A medida que disminuye la participación en múltiples plataformas, transacciones y entornos digitales complejos, se reduce también la probabilidad estadística de verse involucrado en un evento delictivo. En los extremos del ciclo vital —adolescencia temprana y vejez— la exposición digital suele estar más mediada, ya sea por figuras adultas, por limitaciones funcionales o por un uso más selectivo de la tecnología.

Un elemento central de la gráfica es la **ausencia de desplazamientos generacionales en el perfil delictivo.**

El pico no se traslada hacia edades más jóvenes ni mayores con el paso de los años, lo que indica que el delito informático no sigue a un grupo

La concentración del delito informático en población en edad activa digitalmente sugiere que las estrategias de prevención deben focalizarse en este grupo, incorporando enfoques sobre carga cognitiva, multitarea y toma de decisiones rápidas.

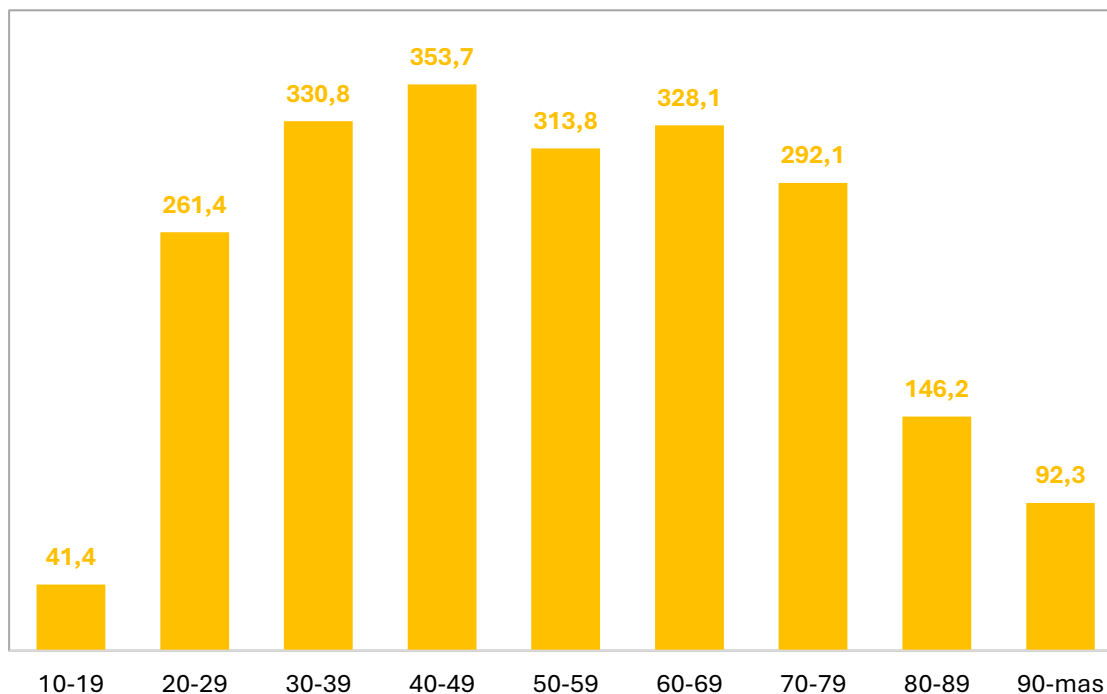
generacional específico, sino que se ancla en la etapa vital de mayor integración funcional al ecosistema digital. A medida que nuevas generaciones ingresan a la adultez productiva, reproducen patrones similares de exposición, mientras que quienes salen de esta etapa reducen su participación relativa.

En línea con lo anterior, el análisis de la tasa de delitos informáticos por grupos de edad confirma y profundiza la lectura del fenómeno en términos de intensidad. Se observa un incremento sostenido desde el grupo de 10 a 19 años (41,4 por cada 100.000 habitantes) hasta los 20 a 29 años (261,4), seguido de una consolidación en niveles altos en los rangos de 30 a 39 (330,8) y 40 a 49 años (353,7), donde se alcanza el valor máximo. Este comportamiento evidencia que no solo aumenta la participación relativa en estos grupos etarios, sino que la probabilidad de victimización es significativamente mayor en las etapas de mayor vinculación con actividades laborales, financieras y digitales.

A partir de los 50 años se observa un descenso progresivo de la tasa, aunque en niveles aún elevados en comparación con los extremos del ciclo vital, con valores de 313,8 en el grupo de 50 a 59 años y 328,1 en el de 60 a 69, seguidos de una reducción más marcada en los grupos de 70 a 79 (292,1), 80 a 89 (146,2) y 90 años y más (92,3).

Este patrón sugiere que, si bien la exposición al delito informático se extiende hacia edades medias y avanzadas, su intensidad disminuye en la medida en que se reduce la participación en entornos digitales complejos, consolidando así una curva etaria claramente definida con un pico en la adultez productiva y un descenso paulatino hacia los extremos del ciclo de vida.

Gráfica 12. Tasa por 100.000 habitantes de delitos informáticos por grupos de edad, 2025.



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos suministrados el 2026-04-15. Período de información entre el 01 de enero de 2019 y el 31 de marzo de 2026. Sujetos a variación por las denuncias que ingresan por SIEDCO y SIDENCO con posterioridad a la fecha de suministro. Fuente: SIEDCO.

6. Disposición tecnológica de los hogares y riesgos asociados al delito informático en Bogotá

Con base en los resultados de la Encuesta de Tecnologías de la Información y las Comunicaciones en Hogares (ENTIC HOGARES 2024), realizada por el Departamento Administrativo Nacional de Estadística (DANE), la población de Bogotá presenta **altos niveles de disposición a realizar tareas digitales cotidianas desde el teléfono inteligente**, lo cual resulta relevante para el análisis del **riesgo asociado a los delitos informáticos**. Entre los hallazgos que demuestran lo anterior están:

- El **72,4 %** de las personas en Bogotá manifiesta estar **dispuesta o muy dispuesta a responder encuestas desde su smartphone**, lo cual amplía la superficie de ataque para modalidades de delito basadas en **ingeniería social, phishing y suplantación de identidad**, especialmente cuando estas interacciones se presentan bajo esquemas de aparente legitimidad institucional o comercial.
- El **65,8 %** de los encuestados en Bogotá se declara **dispuesto o muy dispuesto a utilizar la cámara del teléfono** para este tipo de actividades. Desde una perspectiva de riesgo, esta disposición resulta significativa, dado que el uso de la cámara puede facilitar dinámicas de **verificación engañosa, extorsión digital o fortalecimiento de esquemas de manipulación**, en especial cuando se combina con información previamente recolectada por otros medios digitales.

En contraste, la encuesta muestra una disposición considerablemente menor frente a tareas percibidas como más sensibles, lo que **evidencia la existencia de una conciencia parcial del riesgo digital, que actúa como un factor protector frente a modalidades delictivas más intrusivas**.

- Solo el **28,9 %** de las personas manifiesta estar dispuesta o muy dispuesta a compartir su ubicación GPS.
- Apenas el **31,2 %** se muestra dispuesto a descargar aplicaciones que recolectan información de uso del dispositivo.

Sin embargo, dicha protección no resulta suficiente para neutralizar el riesgo agregado derivado de las actividades que sí cuentan con altos niveles de aceptación. En el contexto urbano de Bogotá, caracterizado por alta conectividad, uso intensivo del smartphone y recurrencia de interacciones digitales asociadas a trámites, servicios y comunicaciones cotidianas, estos patrones adquieren una relevancia estratégica.

En un contexto de alta conectividad, incluso niveles moderados de aceptación de ciertas prácticas digitales generan un volumen suficiente de interacciones para facilitar la escalabilidad del delito informático.

Integrado con el análisis previo sobre desplazamiento del riesgo y recomposición del patrón delictivo, este escenario ayuda a explicar por qué el crecimiento de los delitos informáticos coexiste con la reducción sostenida de delitos tradicionales como el hurto de celulares en Bogotá.

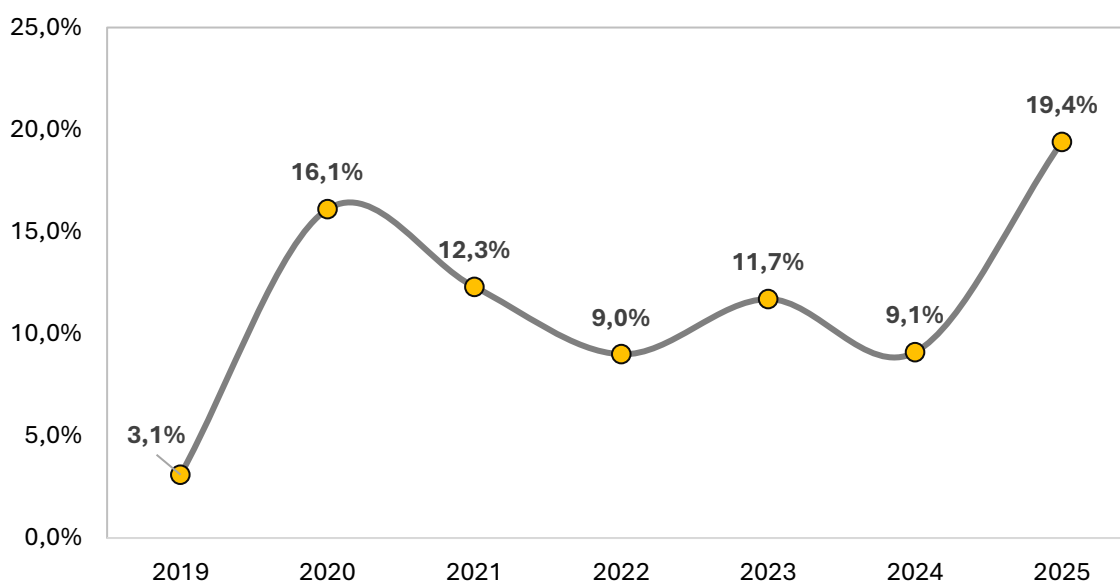
Mientras el delito callejero enfrenta mayores costos operativos y una mayor probabilidad de control, el delito informático se ve favorecido por una población mayoritariamente dispuesta a interactuar digitalmente y por entornos de bajo riesgo relativo para el ofensor, tanto en términos de exposición física como de probabilidad de captura. En consecuencia, la ENTIC Hogares 2024 confirma que la expansión del delito digital responde no solo a capacidades técnicas del delincuente, sino también a ventajas estructurales asociadas a los patrones de uso y disposición tecnológica de los hogares bogotanos.

7. Percepción, victimización y denuncia del delito informático desde la EPV - CCB

La Encuesta de Percepción y Victimización de Bogotá 2025, realizada por la Cámara de Comercio de Bogotá, aporta una lectura complementaria y estratégica al análisis de los delitos informáticos, al integrar la experiencia directa de victimización, los niveles de denuncia y la percepción ciudadana sobre el delito digital. Desde esta fuente, el **cibercrimen emerge como una modalidad que muestra una tendencia creciente y sostenida**, así como patrones diferenciados de afectación y respuesta institucional, aunque aún presenta una incidencia relativa menor frente a delitos tradicionales como el hurto a personas.

En 2025, el 19,7 % de las personas encuestadas en Bogotá manifestó haber sido víctima de un delito cibernético, consolidando al cibercrimen como una tipología relevante y en aumento dentro del conjunto de delitos experimentados por la ciudadanía. Esta proporción representa un aumento significativo frente a los registros previos del periodo 2019–2023 y confirma que la victimización digital se ha integrado al ecosistema delictivo urbano.

Gráfica 13. Porcentaje de personas que respondieron SI a la pregunta “¿Fue víctima de un delito informático?”

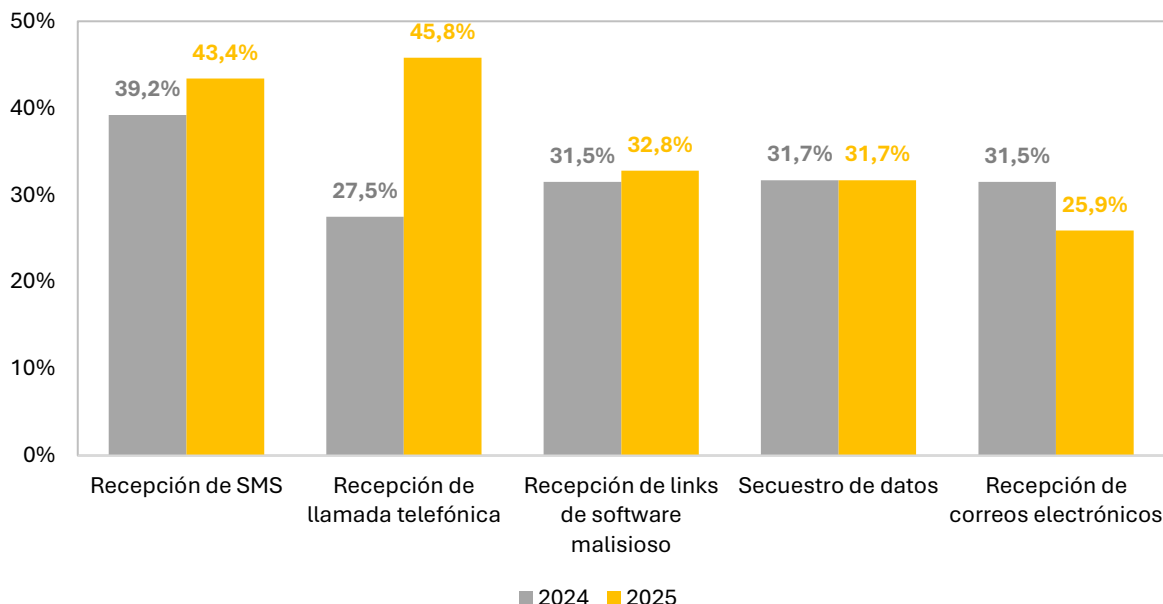


Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos consultados en la página de la Cámara de Comercio de Bogotá el 2026-04-15. Encuesta de Percepción y Victimización de la Cámara de Comercio de Bogotá EPV-CCB 2025.

Desde el punto de vista de las modalidades de comisión, la encuesta evidencia que los delitos informáticos en Bogotá se concentran mayoritariamente en estrategias de contacto virtual directo con la víctima. **En 2025, el 45,8 % de las víctimas reportó haber sido contactada mediante llamadas telefónicas, el 43,4 % a través de mensajes SMS y el 32,8 % mediante enlaces asociados a software malicioso.** Estos resultados coinciden con el análisis previo del documento, en tanto confirman que el delito informático privilegia mecanismos de bajo

costo, alta escalabilidad y escasa exposición para el agresor, apoyados en rutinas de comunicación digital socialmente legitimadas.

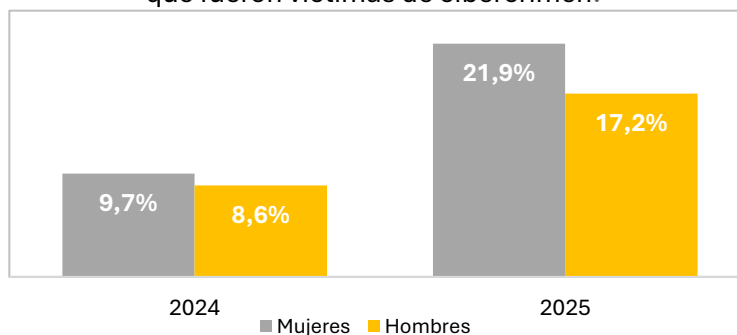
Gráfica 14. “En cuanto a los delitos cibernéticos de los que fue víctima, ¿bajo qué modalidad se cometieron?” años 2024 y 2025.



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos consultados en la página de la Cámara de Comercio de Bogotá el 2026-04-15. Encuesta de Percepción y Victimización de la Cámara de Comercio de Bogotá EPV-CCB 2025.

La encuesta también refuerza la lectura diferencial por género. **En 2025, el 21,9 % de las mujeres encuestadas manifestó haber sido víctima de cibercrimen, frente al 17,2 % de los hombres, ampliando la brecha registrada en años anteriores.** Esta diferencia no puede interpretarse como resultado de conductas individuales imprudentes, sino como expresión de mayores niveles de exposición, interacción digital y carga cognitiva en el uso cotidiano de tecnologías, en línea con el análisis desarrollado sobre victimización digital. La EPV-CCB aporta así evidencia empírica que respalda un enfoque de género en la comprensión y prevención del delito informático.

Gráfica 15. Porcentaje de hombres y mujeres que fueron víctimas de cibercrimen:



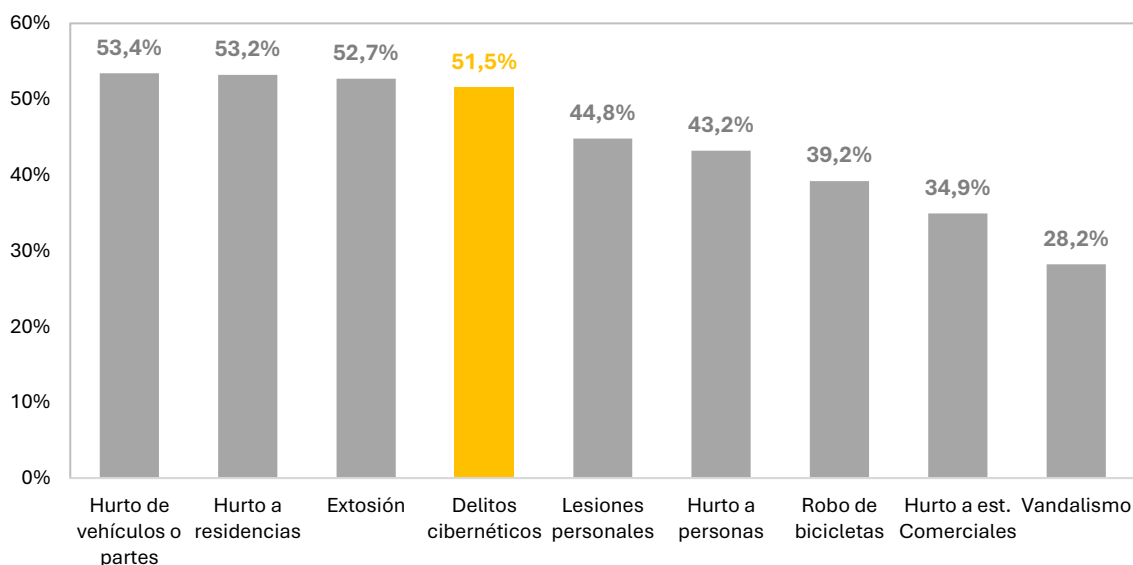
Elaborado por la OAIEE - SDSCJ. Encuesta de Percepción y Victimización de la Cámara de Comercio de Bogotá EPV-CCB 2025.

La EPV-CCB confirma que el delito informático se ha incorporado de forma creciente a la experiencia de victimización en Bogotá, con niveles relevantes de afectación, menor visibilidad relativa y patrones diferenciados de denuncia y percepción.

En términos de denuncia, la encuesta señala que los delitos cibernéticos presentan tasas inferiores a las de otros delitos tradicionales, ubicándose por debajo de modalidades como el hurto de vehículos o el hurto a residencias. Aunque para 2025 se observa una tasa

de denuncia cercana al 52 % en delitos cibernéticos, persisten barreras asociadas a la percepción dificultad del proceso y la incertidumbre sobre los resultados de la denuncia. Este hallazgo resulta consistente con el análisis de tasas de captura desarrollado en el documento, reforzando la hipótesis de que el delito informático opera en un entorno de menor riesgo penal efectivo para el ofensor.

Gráfica 14. Tasa de denuncia por delito en Bogotá año 2025.



Elaborado por la Oficina de Análisis de Información y Estudios Estratégicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia. Datos consultados en la página de la Cámara de Comercio de Bogotá el 2026-04-15. Encuesta de Percepción y Victimización de la Cámara de Comercio de Bogotá EPV-CCB 2025.

Finalmente, desde la perspectiva de la percepción, la EPV-CCB muestra que, aunque el cibercrimen no se ubica entre los delitos que más preocupación generan de manera espontánea, su presencia ha ganado visibilidad progresivamente, especialmente en un entorno donde las redes sociales y los medios digitales son una de las principales fuentes de información para la construcción de opinión sobre seguridad. Esta disociación entre niveles de victimización, percepción y denuncia refuerza la idea de que el delito informático constituye un fenómeno menos visible, pero estructuralmente relevante.

8. Conclusiones

1. **Reconfiguración estructural del delito en Bogotá:** Bogotá atraviesa una recomposición estructural del patrón delictivo, en la que los delitos informáticos crecen de manera sostenida mientras los hurtos tradicionales —en particular el hurto de celulares— pierden centralidad relativa. Esta dinámica no responde a una sustitución lineal, sino a un desplazamiento del riesgo delictivo hacia modalidades menos visibles, más escalables y de menor exposición operativa para el delincuente, aunque requiere de un nivel de conocimientos informáticos especializados.
2. **Ventaja estructural del delito informático en términos de riesgo penal:** La relación capturas-delito evidencia que los delitos informáticos operan en un entorno de baja probabilidad de judicialización, con tasas de capturas significativamente inferiores a las observadas en todas las modalidades de hurto tradicional. Esta asimetría reduce de manera sustancial el costo esperado del delito y actúa como incentivo estructural para su expansión.
3. **Bogotá como amplificador nacional del delito informático:** Bogotá concentra de manera persistente cerca de un tercio del total nacional de delitos informáticos y presenta las tasas más altas del país, asociadas a su elevada conectividad, densidad económica y centralidad digital. La ciudad actúa como un “laboratorio adelantado del cibercrimen”, anticipando dinámicas que luego se extienden a otros territorios.
4. **Disposición tecnológica como factor estructural de riesgo:** Los resultados de la ENTIC Hogares 2024 muestran que una proporción mayoritaria de la población en Bogotá está dispuesta a realizar tareas digitales de bajo umbral de alerta (encuestas, formularios, uso de cámara), lo que amplía la superficie de ataque para delitos basados en ingeniería social, pese a una resistencia parcial frente a tareas más sensibles. El riesgo no se concentra en conductas extremas, sino en la normalización de interacciones digitales cotidianas.
5. **Ventanas temporales y cognitivas que facilitan el delito:** La concentración de delitos informáticos en la media tarde y su baja incidencia los domingos confirman que el cibercrimen sigue lógicas de rutinas sociales, picos de actividad digital y fatiga cognitiva. El delito se maximiza donde convergen alta exposición, multitarea y menor capacidad de evaluación crítica.
6. **Exposiciones diferenciadas por género y edad:** La victimización informativa presenta un sesgo estructural hacia mujeres y se concentra de manera estable en la población entre 25 y 35 años, no por déficits individuales, sino por su posición central en el ecosistema digital, mayor carga cognitiva y uso intensivo de plataformas relacionales, financieras y de servicios.

9. Recomendaciones

1. Proyectar la planeación de seguridad hacia un enfoque mixto físico-digital, asegurando que los logros en reducción del delito callejero se acompañen de estrategias explícitas y medibles contra el delito informático.
2. Priorizar el fortalecimiento de capacidades investigativas digitales, trazabilidad financiera y coordinación con Fiscalía, la UIAF, Asobancaria, MinTIC y sector privado, con metas específicas de aumento en esclarecimiento y capturas asociadas a delitos informáticos.
3. Posicionar a Bogotá como territorio piloto nacional para el desarrollo de modelos predictivos, observatorios de delito digital y protocolos avanzados de prevención y respuesta, con capacidad de transferencia a otros departamentos.
4. Diseñar programas de prevención basados en escenarios reales de uso, enfocados en riesgos “invisibles” (phishing, suplantación, fraude), más que en advertencias genéricas sobre tecnologías claramente riesgosas.
5. Ajustar las estrategias preventivas y de alerta temprana a ventanas horarias críticas, fortaleciendo mensajes preventivos, monitoreo transaccional y detección de fraudes en franjas de mayor riesgo operativo.
6. Incorporar un enfoque diferencial de género y ciclo de vida en la prevención del delito informático, con campañas y herramientas adaptadas a contextos reales de uso, evitando enfoques asistencialistas o de culpabilización de la víctima.

Referencias Bibliográficas

- Americas Market Intelligence. (2025). Mapa del consumo de medios digitales en América Latina 2025. AMI.
- Baumeister, R. F., Vohs, K. D., & Tice, D. M. (2007). The strength model of self-control. *Current Directions in Psychological Science*, 16(6), 351–355. <https://doi.org/10.1111/j.1467-8721.2007.00534.x>
- Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. <https://doi.org/10.2307/2094589>
- Comscore. (2025). Tendencias digitales en América Latina: usos, hábitos y comportamientos multicanal. Comscore Latinoamérica.
- Comscore. (2025). Tendencias digitales: Definiendo el rumbo del 2025 en América Latina. Comscore Latinoamérica.
- Congreso de la República de Colombia. (2009). Ley 1273 de 2009 – Por medio de la cual se modifica el Código Penal y se crea el bien jurídico de la protección de la información y los datos.
- DataReportal. (2024). Digital 2024: Colombia. We Are Social & Meltwater.
- Departamento Administrativo Nacional de Estadística – DANE. (2024). Indicadores básicos de Tecnologías de la Información y las Comunicaciones (TIC) en Hogares. Encuesta Nacional de Calidad de Vida (ECV).
- Departamento Administrativo Nacional de Estadística – DANE. (2024). Encuesta de Tecnologías de la Información y la Comunicación en Hogares (ENTIC Hogares).
- Felson, M., & Boba, R. (2010). *Crime and everyday life* (4th ed.). SAGE Publications.
- Felson, M., & Clarke, R. V. (1998). *Opportunity makes the thief: Practical theory for crime prevention*. Home Office, Policing and Reducing Crime Unit.
- International Telecommunication Union – ITU. (2025). *Measuring digital development: Facts and figures 2025*. United Nations.
- Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC. (2024–2025). Boletines trimestrales del sector TIC y estadísticas de conectividad.
- Morales Ramírez, O. (2025). Ciberfraude: principales métodos de ataque y estrategias para su prevención. *Ciencia Latina Revista Científica Multidisciplinar*, 9(3). https://doi.org/10.37811/cl_rcm.v9i3.18122
- National Institute of Cybersecurity of Spain – INCIBE. (2026). Informe sobre tendencias y patrones de la ciberdelincuencia. Gobierno de España.
- Observatorio de Desarrollo Económico de Bogotá – SDDE. (2024). Boletín TIC No. 41.

Organisation for Economic Co-operation and Development (OECD). (2023). Bridging the digital gender divide. OECD Publishing. <https://doi.org/10.1787/ed6f5191-en>

Pessiglione, M., et al. (2018). Cognitive fatigue induces preference for immediate rewards. *Proceedings of the National Academy of Sciences*, 115(27), 708–713. <https://doi.org/10.1073/pnas.1804213115>

Policía Nacional de Colombia. (2019–2026). Sistema de Información Estadístico, Delincuencial, Contravencional y Operativo – SIEDCO. Dirección de Investigación Criminal e INTERPOL.

United Nations Office on Drugs and Crime (UNODC). (2024). Global cybercrime trends and responses. United Nations.

Vohs, K. D., Baumeister, R. F., Schmeichel, B. J., Twenge, J. M., Nelson, N. M., & Tice, D. M. (2014). Making choices impairs subsequent self-control: A limited-resource account of decision making. *Journal of Personality and Social Psychology*, 94(5), 883–898. <https://doi.org/10.1037/0022-3514.94.5.883>

World Economic Forum. (2024). Global Cybersecurity Outlook 2024. WEF.