La brecha digital: Un blanco fácil para la cibercriminalidad

ANDERSON LEMOS VARGAS

Universidad Santiago de Cali

Facultad de derecho

Diplomado Abogados 2.0 Marketing de redes y gestión de datos.

JEFFREY ARCOS TROYANO

Santiago de Cali - Colombia

OCTUBRE DE 2024

Resumen

La brecha digital es un fenómeno que ha cobrado relevancia en los últimos años debido al acelerado avance de las tecnologías de la información y la comunicación (TIC). Esta brecha no solo crea desigualdades económicas y sociales, sino que tiene implicaciones graves en términos de ciberseguridad por lo que expone a la población a riesgos en sus diferentes modalidades *(malware, phishing, vishing y smishing),* que son utilizadas por los ciberdelincuentes para aprovechar esa falta de conocimiento de las personas sobre el mundo digital. *Este artículo tiene como objetivo analizar cómo la brecha digital se convierte en un blanco fácil para los* ciberdelincuentes, por lo que se pretende identificar como la falta de educación digital expone a las personas a riesgos que ni siquiera conocen. En un mundo donde las transacciones digitales, el uso de redes sociales y el acceso a la información son esenciales para el día a día, quienes no cuentan con las habilidades necesarias para proteger sus datos se convierten en objetivos vulnerables para la cibercriminalidad.

Palabras clave

ciberdelincuente, cibercriminalidad, brecha digital, educación digital, ciberseguridad, TIC, *malware, phishing, vishing, smishing*.

Abstract

The digital divide is a phenomenon that has gained relevance in recent years due to the accelerated advancement of information and communication technologies (ICT). This gap not only creates economic and social inequalities, but also has serious implications in terms of cybersecurity, exposing the population to risks in its different modalities *(malware, phishing, vishing and smishing)*, which are used by cybercriminals to take advantage of people's lack of knowledge about the digital world. This article aims to analyze how the digital divide becomes an easy target for cybercriminals, so it aims to identify how the lack of digital education exposes people to risks that they do not even know about. In a world where digital transactions, the use of social networks and access to information are essential for everyday life, those who do not have the necessary skills to protect their data become vulnerable targets for cybercrime.

Keywords

cybercriminal, cybercrime, digital divide, digital education, cybersecurity, ICT, malware, phishing, vishing, smishing.

1. Introducción

En el mundo cada vez se evidencia el avance de las tecnologías de la información y la comunicación (TIC), estamos presenciando la era de la revolución digital, en la que esta cambiado cada aspecto de la manera en la que vivimos, por lo cual el humano debe evolucionar, adaptarse y adquirir las habilidades necesarias para el uso correcto de estas herramientas digitales. Sin embargo, este desarrollo no es eficaz al enfrentarse con barreras socioeconómicas y educacionales, creando así una brecha digital que disminuyo y tuvo avances forzosos, en razón a la pandemia del COVID-19. En el contexto colombiano este acontecimiento también logro cerrar un poco esta brecha, logro digitalizar aspectos relevantes como el teletrabajo, la digitalización de expedientes y procesos en la administración de justicia, la educación virtual y la realización de muchas otras tareas que son posibles gracias a las herramientas digitales que nos ofrecen. En cuanto a la brecha existente, Colombia afronta todavía muchos problemas de conectividad, de desigualdad y de un aspecto que considero el más importante para la evolución digital en el país, como lo es la falta de educación digital, la cual también podemos llamar brecha cognitiva.

La falta de educación digital ha contribuido considerablemente a riesgos en la sociedad, este es un problema proveniente desde los diferentes niveles de educación, siendo la educación superior, la que más se acerca a una constante evolución digital, pero poco privilegiada, es por esto que las personas que no cuentan con esa formación digital, son más propensas a caer en engaños, fraudes y ataques cibernéticos, generando así un camino fácil para todo tipo de delito informático.

Este avance forzado hacia la digitalización también ha venido acompañado de un aumento en las conductas cibercriminales, cada día se genera una dependencia de las herramientas digitales, de las cuales los ciberdelincuentes han aprovechado las brechas para crear vulnerabilidades en la sociedad. Dentro de las modalidades empleadas encontramos, los malware, el phishing, el vishing, el smishing y como estas existas muchas más.

En este contexto de transformación digital, donde la alfabetización digital juega un papel determinante, la implementación de herramientas tecnológicas y enfoques educativos no solo busca cerrar la brecha digital, sino también preparar a la sociedad para los desafíos del siglo XXI "Hoy, la región enfrenta un doble desafío. De una parte, superar rezagos endémicos en materia de deserción escolar, bajos logros educativos y segregación en dichos logros por estratos socioeconómicos y por corte rural-urbano. Por otro lado, mejorar la calidad y pertinencia del sistema educacional a fin de que éste cumpla un papel estratégico en el tránsito de las sociedades nacionales hacia un orden global, competitivo y altamente interconectado, centrado en el paradigma de la sociedad del conocimiento." (Hopenhayn; 2003, p.8)

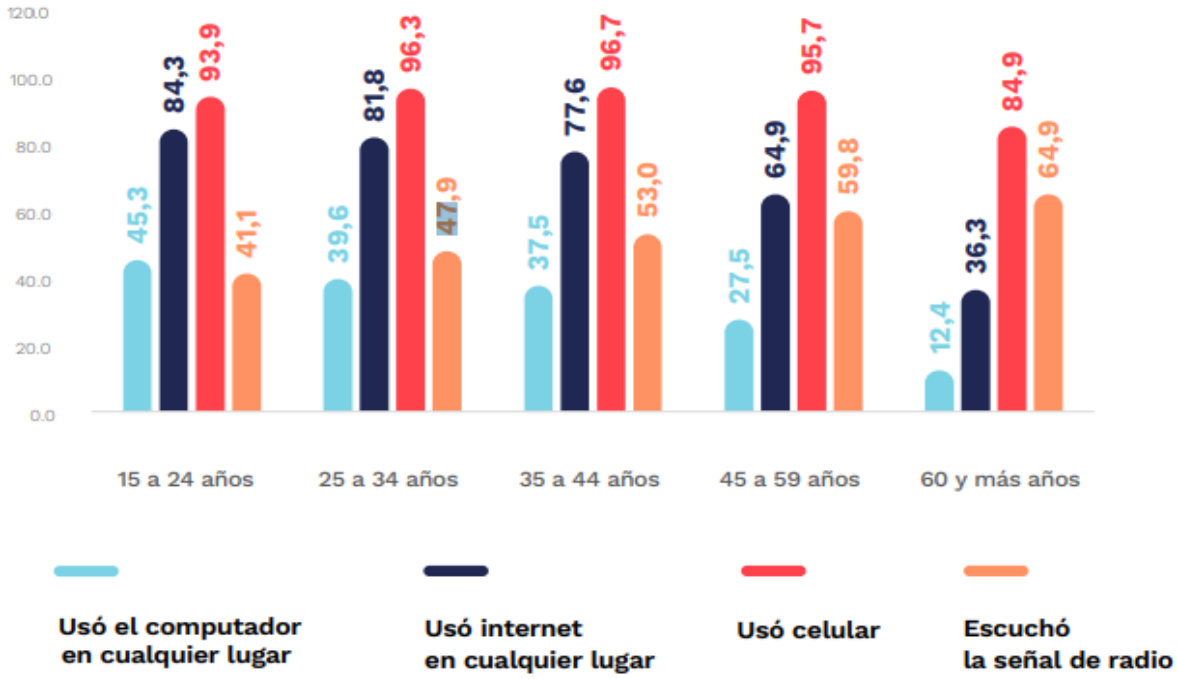
2. Contexto actual de brecha digital y ciberdelincuencia

El termino brecha digital no tiene un origen exacto según Van Dijk (como se citó en Gómez Navarro et al. 2018) "inicialmente, la brecha digital se refería a la desigualdad entre aquellos que tenían o no tenían acceso físico a las TIC", pero en la actualidad el termino abarca una amplia variedad de aspectos que van desde la desigualdad hasta diferencias culturales, y educativas. Un ejemplo de esta variedad de aspectos de brecha digital, son frente a la población de 60 y más años, según Sunkel y Ullmann (2019) sustentan que "los datos indican que las personas mayores no son participantes activos en las sociedades digitales en las que viven y que existen un enorme espacio para ampliar el uso de internet entre estas personas en la región"

En las encuestas nacionales de calidad de vida del DANE, se puede evidenciar una notoria diferencia entre las personas que usaron las TIC según su grupo de edad, donde se puede demostrar como las personas de 60 y más años utilizan mucho menos estas herramientas digitales que otros grupos etarios, por lo que se genera una brecha digital en razón de la edad.

Figura 1

Porcentaje de personas que usó TIC, según grupo de edad. Total, nacional. 2020



Fuente: DANE, Encuesta Nacional de Calidad de Vida-E

De manera más amplia podemos evidenciar como la brecha digital es causada por diferentes factores que varían por las razones socioeconómicas, culturales y educativas. El DANE (2021) nos señala las principales razones por las que no usan las herramientas digitales según los grupos de edad.

Tabla 1

Porcentaje de personas que no usan internet, según razón principal por la que usa internet. Total, nacional. 2020

Razón principal para no usar internet	Grupo de edad				
	15 a 24 años	25 a 34 años	35 a 44 años	45 a 59 años	60 y más años
No sabe usarlo	7,4	12,5	22,2	38,4	60,5
No lo considera necesario	21,7	26,4	28,8	30,7	26,8
Es muy costoso	51,7	46,8	38,7	25,1	9,9
No hay cobertura del servicio en la zona	14,6	11,3	8,1	4,6	1,7
Otra	3,1	2,4	1,6	0,7	0,9
No le tienen permitido usar internet	1	0,4	0,1	0,2	0,2
Por razones de seguridad o privacidad	0,4	0,3	0,5	0,3	0,1

Fuente: DANE, Encuesta Nacional de Calidad de Vida-E

Así como se puede observar, gran parte de la población en general no usa el internet en razón a la falta de alfabetización digital, y por qué hago tanto hincapié en este aspecto, porque este es el camino más fácil para la consecución de delitos informáticos. A la hora de la verdad toda persona que tenga acceso a Internet puede ser víctima de un ciberdelito, pero el cibercriminal siempre está pendiente de las vulnerabilidades que le permitan acceder a algún sistema de información. Cáceres García (2022) plantea que las actividades realizadas en el entorno digital forman una reputación que es semejante a la reputación de nuestra vida cotidiana, se construye a partir de nuestras acciones e interacciones, y que esta identidad digital deja huellas que pueden ser predecibles, facilitando así el trabajo de los ciberdelincuentes, quienes buscan apropiarse de identidades para realizar fraudes, acceder a información privilegiada de manera ilegal o acoso cibernético. (p. 7)

El contexto actual en Colombia muestra que la brecha digital va más allá del simple acceso a la tecnología, involucrando también aspectos culturales educativos y de edad. Esta realidad hace que ciertos grupos, como los adultos mayores, sean mas vulnerables a la hora de acceder a internet. Cerrar esta brecha requiere una intervención estructural con programas para el acceso a las TIC, para adquirir las habilidades necesarias para usarlas de forma segura. En ese sentido es fundamental promover una educación digital adaptada a las diversas necesidades de la población.

3. Una mirada al contexto mundial en cuanto al Cibercrimen

El cibercrimen es un asunto de carácter mundial, esta problemática afecta tanto a naciones desarrolladas como en vía de desarrollo, los ataques cibernéticos han aumentado de forma exponencial, afectando a individuos, empresas en inclusive gobiernos. Según el informe de Defensa Digital de Microsoft (2023) citado por Ficarazzi Giovanna, (2023), más de 120 países han enfrentado ciberataques que han comprometido desde sistemas gubernamentales, hasta a entidades privadas.

Es coherente hablar de que hay naciones que están menos preparadas frente a estos ataques, siendo de igual modo la brecha digital uno de sus principales factores países como Ucrania, Israel, Corea del Sur y Taiwán han sido blanco de crecientes amenazas cibernéticas, el caso de Ucrania se debe principalmente por su conflicto actual con Rusia, según Ficarazzi

Giovanna, (2023) “Los ataques cibernéticos dirigidos a Ucrania han variado desde intrusiones destructivas hasta operaciones de espionaje y desinformación”.

Modalidades como el phishing y los malware siguen siendo las formas más comunes de ciberdelincuencia a nivel mundial. “En Estados Unidos, el phishing y el pharming fueron los tipos de ciberdelincuencia más denunciados en 2022, con más de 300.000 víctimas reportadas” (SEON 2023).

En conclusión, este es un problema que afecta a todas las naciones, países como Estados Unidos están más capacitados para actuar frente a estos delitos, lo que ayuda a mitigar un poco el riesgo, por esa razón las naciones más vulnerables deben adoptar e implementar este tipo de medidas.

4. Modalidades recurrentes del ciberdelincuente que afectan a la población más vulnerable

Dentro de las modalidades más utilizadas por los cibercriminales frente a este tipo de víctimas se encuentran el phishing, el vishing y el smishing y el malware. siendo estas las modalidades delictivas más utilizadas, donde la principal característica es que se realiza a través del engaño, aprovechándose de la falta de verificación de autenticidad de enlaces, publicidades, archivos, aplicaciones e inclusive de llamadas telefónicas de fuentes desconocidas o suplantaciones.

El phishing, considerado por Miro Linares (2012) como “La modalidad estrella dentro de este subtipo de conductas de ciberfraude” (p. 72) está relacionada análogamente con la estafa, esta técnica delictiva es la más común debido a su capacidad para engañar a las víctimas y obtener así información sensible. Castillo Rubiano (2021), afirma que “implica el uso de diversas técnicas para obtener información confidencial, como (usuarios, contraseñas, números de identificación, información financiera, etc.). De esta manera, los ciberdelincuentes suelen enviar correos electrónicos que aparentan ser de fuentes confiable, como entidades bancarias, y contienen enlaces o archivos que redirigen a las víctimas a sitios web clandestinos, donde se obtiene información valiosa, que es utilizada de manera fraudulenta, con consecuencias significativas” (p. 21)

El vishing y el smishing, Son una variante del phishing, ambas comparten semejanzas en su enfoque de estafa, cada una tiene un modus operandi característico, por ende, son unas de las modalidades más comunes dentro del actuar delictivo. García Sánchez (2021) como se citó en (BBVA, 2015), "el vishing, implica el uso de llamadas telefónicas y mensajes de texto que aparentan ser de entidades legitimas como bancos, para engañar a las víctimas y obtener su información personal. Los estafadore envían menajes alarmantes sobre supuestas compras no autorizadas, incluyendo enlaces o números telefónicos falsos y cuando las victimas responden, los delincuentes aprovechan para obtener sus datos privados". Por otro lado, el smishing utiliza el servicio de mensajes de texto para engañar a los usuarios, quienes en promedio envían y reciben numerosos mensajes en el día, aumentando así la probabilidad de ser víctimas de este tipo de fraude.

El malware, es una de las amenazas más comunes que enfrenta la sociedad a la hora de navegar en internet. Este término abarca una amplia gama de programas, diseñados con intenciones malignas, que pueden causar grandes daños en los sistemas operativos de cualquier equipo tecnológico. Para Londoño y Ramírez (2023), "el malware o software malicioso, se refiere a la creación de un programa, una aplicación o un código, que, al ser incorporado en cualquier dispositivo inteligente, (teléfono celular, computadora portátil o de mesa, tableta, cámara de seguridad inalámbrica, localizador, entre muchos más dispositivos), busca atacar, infectar, espiar, encriptar, destruir o secuestrar información." esta amenaza se origina comúnmente descargar cualquier tipo de archivo de fuentes desconocidas.

Este tipo de modalidades son las más recurrentes por los ciberdelincuentes y continúan perpetuándose en el tiempo, en razón a la cantidad de vulnerabilidades encontradas para desarrollar su actividad criminal. En Colombia vivimos en un fenómeno donde las personas que conocen de estas formas delictivas o que ya han sido víctimas de estas, hacen caso omiso ello y no se cercioran mínimamente para corroborar la autenticidad de las fuentes informáticas utilizadas en el diario vivir. Así mismo se demuestra como la cibercriminalidad, evoluciona constantemente para explotar las vulnerabilidades de la población menos concientizada

5. **¿Es suficiente el marco normativo colombiano para combatir la cibercriminalidad en un entorno de constante evolución digital?**

En Colombia, la normatividad frente a los delitos informáticos ha dado pasos significativos para combatir a estas estructuras delincuenciales, no obstante, la velocidad a la que evoluciona el mundo digital presupone un desafío continuo. La ley 1273 de 2009 representa un avance fundamental para la regulación y protección de la información y los datos de la población, tipificando delitos como el acceso abusivo a sistemas de información, el uso de software malicioso y la violación de datos personales. Según Ojeda Pérez et al. (2010) Esta normativa "crea un nuevo bien jurídico tutelado a partir del concepto de la protección de la información y de los datos, con el cual se preserva integralmente a los sistemas que utilicen las tecnologías de la información y las comunicaciones". Esto demuestra un esfuerzo claro por parte del legislador por adaptar la legislación a las realidades de la era digital.

Sin embargo, aunque la ley 1273 ha permitido delimitar ciertos delitos, no es suficiente frente a la velocidad con la que surgen nuevas figuras del cibercrimen. Las modalidades delictivas, como el malware y sus variantes o como las avanzadas técnicas de phishing, no solo son un desafío para la infraestructura tecnológica, sino que también ponen a prueba la capacidad del sistema legal para responder de manera eficaz.

En este sentido, la evolución del cibercrimen plantea una necesidad inminente de actualización normativa. No basta con tener leyes que definan los delitos actuales si estas no contemplan la capacidad de adaptarse a los cambios tecnológicos. La colaboración internacional también juega un rol crucial, y la adhesión de Colombia al convenio de Budapest es un paso importante para hacerle frente a los delitos informáticos a través de la cooperación internacional. Sin embargo, la implementación efectiva de políticas derivadas de acuerdos internacionales depende de que las instituciones locales cuenten con las herramientas jurídicas y tecnológicas necesarias, de lo contrario, cualquier esfuerzo quedara rezagado frente a la innovación delictiva.

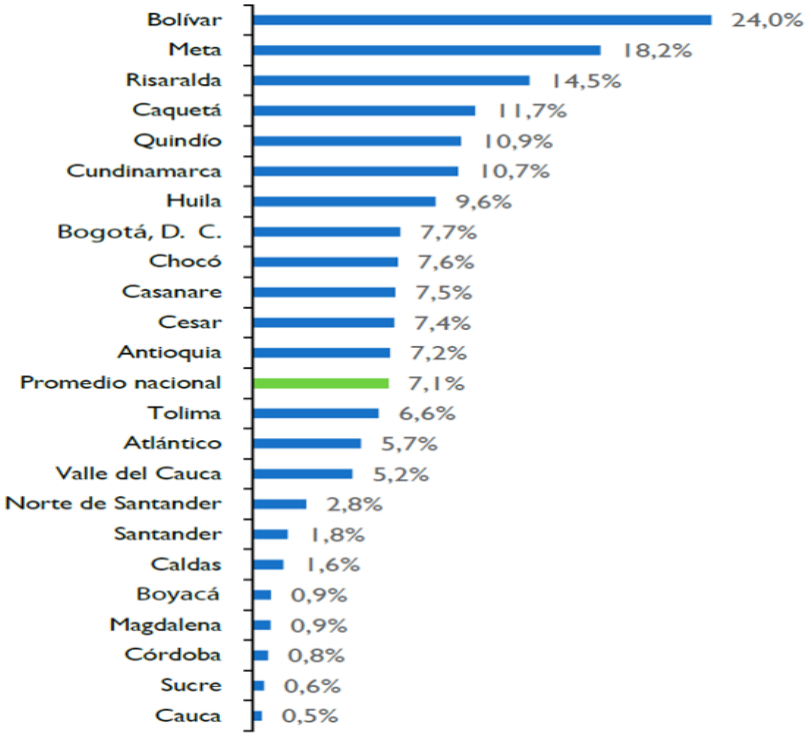
6. **¿Hasta qué punto la estructura del sistema penal colombiano es eficaz para investigar y procesar delitos informáticos?**

El sistema penal colombiano, afronta grandes desafíos en la lucha contra los delitos cibernéticos, especialmente en lo que respecta a su intervención eficaz, si bien existe una

estructura normativa e institucional para actuar frente a la cibercriminalidad, la realidad demuestra que los resultados han sido escasos, principalmente en la capacidad de investigación y captura de los responsables. Un claro ejemplo de esto se refleja en el indicador de captura por denuncia (Cd) que se presenta en el análisis de Rincón Arteaga et al. (2023).

Figura 2

Indicador Cd por departamento (2019)



Fuente: datos aportados por la fiscalía general de la Nación.

Este indicador, pone en evidencia que, en muchos departamentos del país, la probabilidad de que un ciberdelincuente sea capturado sigue siendo baja, a nivel nacional, “el indicador de capturas por denuncia de delitos informáticos fue de solo un 7.1% en comparación con otros delitos como el hurto calificado, que presenta un indicador de 22.8%” (Rincón Arteaga et al. 2023). Estos datos son preocupantes ya que demuestra que el sistema judicial aun no logra dar una respuesta proporcionalmente efectiva.

Queda demostrado la insuficiente infraestructura tecnológica y de recursos disponibles para la investigación de estos delitos que posee el país. Obando, resalta que “las fuerzas policiales están haciendo esfuerzos para bloquear actividades ilegales, como las 11.163 paginas

relacionadas con pornografía infantil y juegos de azar ilegales que se bloquearon en 2022" Pero los ciberdelincuentes siempre van un paso adelante, la existencia de la norma pasa a un segundo plano cuando no se activan los mecanismos para hacerla valer. Según Obando, (2023), "La mera existencia de estas penas no garantiza una búsqueda exitosa". La falta de especialización y conocimientos en las fuerzas de seguridad en el sistema judicial contribuye a la impunidad, es fundamental que el país invierta en la estructura tecnológica del sistema y en la capacitación continua de sus agentes de policía, fiscales y jueces en los temas de ciberdelincuencia y nuevas tecnologías.

En conclusión, la estructura del sistema penal colombiano aun presenta muchas deficiencias en su capacidad para investigar y procesar delitos cibernéticos. Aunque existen avances en la legislación y en la creación de instituciones especializadas, la falta de recursos, tecnologia, y la limitada cooperación internacional siguen siendo barreras significativas. En un entorno digital que evoluciona constantemente, es imprescindible que las estrategias jurídicas y las politicas de seguridad informática se adapten pronto para poder ofrecer una respuesta eficaz y contundente ante este tipo de criminalidad.

7. Políticas y programas para combatir la brecha digital

Gran parte de la responsabilidad de la brecha digital actual es la poca implementación de programas en pro del acceso a las herramientas digitales, las políticas establecidas por los diferentes mandatarios no han cumplido en totalidad con expectativas de los colombianos. Programas como la implementación de puntos vive digital, impulsadas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), eran una gran medida para la alfabetización digital de muchos y la reducción de la brecha digital, este programa tenía como objetivo "promover la conectividad y acceso a las tecnologías, especialmente en las áreas más vulnerables del país" (MinTIC 2017). son políticas que en el momento no poseen el mismo auge, promoción y sostenibilidad por parte de algunas entidades territoriales.

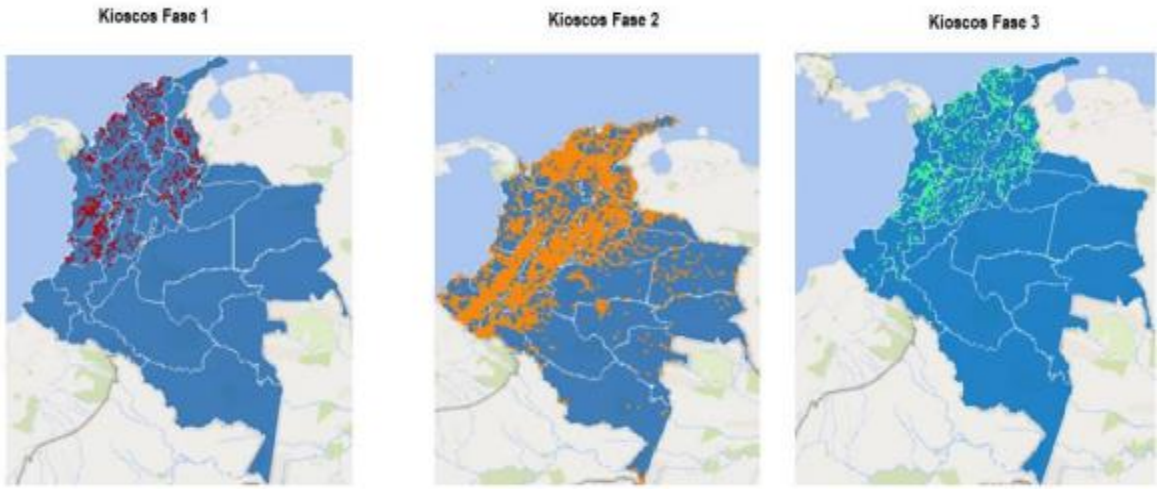
En el gobierno actual, han impulsado iniciativas como los centros de acceso comunitario a internet en zonas rurales, que forman parte de los Programas de Desarrollo con Enfoque Territorial (PDET). Estas políticas son implementadas para reducir la brecha digital en zonas vulnerables, permitiendo la conectividad de la comunidad que habita en estas zonas. El MinTIC indica que busca "que el acceso a internet se conciba como un derecho y no como un privilegio".

Otro programa destacado actualmente es el Proyecto Nacional de Acceso Universal a Tecnologías de la Información y las Comunicaciones impulsado por el CONPES 4001 de 2020. Este busca “ofrecer y generar soluciones en el acceso a internet sostenible en áreas rurales, este proyecto pretende llegar a un universo de 1.000 centros poblados en 378 municipios.

Actualmente es necesario seguir implementando este tipo de proyecto y así llegar a todos los hogares en Colombia. Por su parte el Departamento Nacional de Planeación (DNP) adelanto un análisis del programa de Kioscos vive digital (KVD) desde 2010 con los kiocos los cuales se distribuyeron hasta la actualidad en 3 fases.

Mapa 1

Alcance geográfico de la iniciativa KVD (2012-2019)



Fuente: Dirección de Infraestructura - Ministerio de Tecnologías de la Información y las Comunicaciones, 2019.

Este análisis, detallado por el CONPES, indica que “para el año 2018, de acuerdo con la disponibilidad de recursos del hoy FUTIC, se adelantaron nuevas adiciones presupuestales para soportar la operación de 6.879 kioscos, repartidos en 8952 municipios, beneficiando principalmente a sedes educativas”.

Se demuestra que las políticas y programas implementados para combatir la brecha digital han contribuido sustancialmente, pero estas políticas deben ser acompañadas y

actualizadas en pro de mejorar, y de esa forma no se quede como en un proyecto realizado por el gobierno de turno. Resulta imperioso sostener este tipo de programas e iniciativas como los punto vive digital, El acceso a la tecnología debe ser una prioridad y no solo políticas que perecerán en el tiempo.

8. Recomendaciones

Al Ministerio de las TIC y gobierno nacional recomiendo

- Avanzar en la implementación de más programas enfocados en la alfabetización digital, donde se incluya una debida capacitación sobre ciberseguridad, adaptado a la situación de la población más vulnerable a estos riesgos.

- Actualización del sistema educativo colombiano frente a al uso de herramientas digitales.

- Aumentar la cobertura y acceso a internet en el territorio nacional, principalmente en las zonas rurales y marginas para garantizar un acceso total en el país.

- Capacitar y actulizar toda la estructura del sistema judicial frente a los delitos cibernéticos para garantizar un uso de internet seguro.

- Promover conjuntamente con entidades públicas o privadas que manipulan una gran parte de datos sensibles de la población, al uso de tecnologías seguras y accesibles, implementando campañas de educación digital dirigidas a los usuarios brindando información de cómo proteger sus datos personales y como reconocer amenazas cibernéticas.

9. Conclusiones.

La brecha digital no solo refleja desigualdades económicas y sociales, en ella se evidencian la vulnerabilidad de la sociedad con acceso a internet, el mundo digital sigue avanzando sin medida, y nosotros como sociedad debemos prepararnos y adaptarnos a este

cambio. Los riesgos existentes en el internet no deben impedirnos poder utilizar todas estas herramientas digitales, la mejor forma de asumir estos riesgos es afrontándolos y capacitándonos cada vez más, la educación digital es crucial para reducir la vulnerabilidad de la población, como sociedad siempre vamos a estar expuestos a cualquier tipo de ataque cibernético, pero debemos reducir sustancialmente estos casos y que cada vez sea un poco más complicado para estos actores delictivos cumplir con su objetivo.

A pesar de los avances legislativos y los esfuerzos de cooperación internacional como la adhesión al convenio de Budapest, la efectividad del sistema penal colombiano en la investigación y procesamiento de delitos informáticos aún debe afrontar muchos desafíos. El gobierno colombiano debe aumentar el presupuesto a la estructura del sistema judicial. También existen nuevos desafíos legislativos frente a nuevas tecnologías emergentes, como la regulación de la inteligencia artificial.

Finalmente, la lucha contra los delitos informáticos deben ser una prioridad en la agenda nacional, esta es una problemática que afecta a todas las naciones, solo que hay unas mejor preparadas que otras, solo a través de esfuerzos combinados podremos disminuir la brecha y construir una sociedad más segura en el entorno digital.

Referencias

- Alzate J, González M, Aristizábal M y Pareja L. (2021) Personas mayores en Colombia: Hacia la inclusión y la participación. https://www.dane.gov.co/files/investigaciones/notas-estadisticas/oct-2022-nota-estadistica-personas-mayores-en-colombia.pdf

- Castillo Rubiano (2021) PHISHING: DÍA DE PESCA. https://bdigital.uexternado.edu.co/server/api/core/bitstreams/e8eac144-41c1-4efe-a7a8-85d8f4f93097/content

- CONPES 4001 (2020) Declaración de importancia estratégica del proyecto nacional acceso universal a las tecnologías de la información y las comunicaciones en zonas rurales o apartadas. https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4001.pdf

- Garcia Sánchez (2021) Delitos contra el patrimonio económico, el phishing en Colombia aproximadamente criminológica . https://repositorio.unal.edu.co/bitstream/handle/unal/82270/1032430963.2021..pdf?sequence=4&isAllowed=y

- Ficarazzi Giovanna (2023) Ciberseguridad en el mundo: los países más vulnerables y las tendencias de ataques. https://cuadernosdeseguridad.com/2023/10/ciberseguridad-en-el-mundo/

- Gómez N, Alvarado L, Martínez D y León C. (2018) La brecha digital: una revisión conceptual y aportaciones metodológicas para su estudio en México. https://www.redalyc.org/journal/4576/457654930005/html/

- Hopenhayn Martin (2023) Educación, comunicación y cultura en la sociedad de la información: una perspectiva latinoamericana. https://repositorio.cepal.org/server/api/core/bitstreams/3c829a3e-fb18-46d1-ae5a-5611189946aa/content

- Ley 1273 (2009) Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=34492

- Londoño R y Ramírez O (2023) Usó de sofware malicioso en Colombia: problemáticas emergentes y nuevas tendencias https://repository.unilibre.edu.co/bitstream/handle/10901/27118/02%20-%20Artículo%20de%20Reflexión.pdf?sequence=2&isAllowed=y

- MinTIC (2017) Informe de acciones de política para el cierre de la brecha digital. https://www.mintic.gov.co/portal/historico/articles-62254_Documento_de_Cierre.pdf

- Miro Llinares (2012) El cibercrimen: fenomenología y criminologia de la delincuencia en el ciberespacio. https://dialnet.unirioja.es/servlet/libro?codigo=756351

- Obando J. (2024). Ciberseguridad en Colombia: panorama completo de su estado en 2023 https://linktic.com/blog/panorama-completo-de-la-ciberseguridad-en-colombia/

- Ojeda P, Arias F, Rincón R y Daza M. (2010) Delitos informáticos y entorno jurídico vigente en Colombia https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176/2416

- Rincón A, Castiblanco H, Quijano D, Urquijo V y Pregonero L. (2022). Ciberdelincuencia en Colombia: ¿Qué tan eficiente ha sido la Ley de Delitos Informáticos? https://www.asobancaria.com/wp-content/uploads/2022/03/1318_BE.pdf

- Rosas Prado (2022) EL CIBERCRIMEN EN COLOMBIA Y SU EVOLUCIÓN EN LOS ÚLTIMOS DOS AÑOS (2020 – 2021). https://repository.unimilitar.edu.co/items/7f343af5-3f55-442f-9360-1a2915a71993

- Seon (2023) Informe global sobre ciberdelincuencia: ¿Qué países corren mayor riesgo? https://seon.io/es/recursos/informe-global-sobre-ciberdelincuencia-que-paises-corren-mayor-riesgo/

- Sunkel G y Ullmann H (2019) Las personas mayores de América Latina en la era digital: superación de la brecha digital. https://repositorio.cepal.org/server/api/core/bitstreams/80368184-dd91-4a12-a5b4-b3d23e870e45/content