CIBERSEGURIDAD Y CONTROL FISCAL EN COLOMBIA

RETOS Y DESAFÍOS EN LA ERA DE LA INTELIGENCIA ARTIFICIAL

CARMEN PAOLA VÉLEZ MARROQUÍN

ilae
Instituto Latinoamericano de Altos Estudios

Ciberseguridad y control fiscal en Colombia:

Retos y desafíos en la era de la inteligencia artificial

Ciberseguridad y control fiscal en Colombia:

Retos y desafíos en la era de la inteligencia artificial

Carmen Paola Vélez Marroquín

Instituto Latinoamericano de Altos Estudios –ILAE–

Publicación sometida a evaluación de pares académicos, mediante el sistema de "doble ciego", requisito para la indexación en la Web of Science de Clarivate (*Peer Review Double Blinded*).

ISBN versión digital 978-628-7661-55-4
ISBN versión impresa 978-628-7661-53-0

Cra. 18 # 39A-46, Teusaquillo, Bogotá, Colombia
pbx: (571) 601 232-3705
www.ilae.edu.co

Revisión de textos y composición / *Text revision and composition*
Harold Rodríguez Alba [harorudo10@gmail.com]

Diseño de carátula / *Cover design*
Harold Rodríguez Alba

Editado en Colombia
Published in Colombia

Contenido

ÍNDICE DE GRÁFICOS

Introducción

La amenaza cibernética se ha consolidado como uno de los riesgos más significativos del siglo XXI para los Estados, las empresas y los ciudadanos. El vertiginoso avance de las tecnologías de la información y las comunicaciones –TIC–, junto con la creciente digitalización de los procesos sociales, políticos y económicos, ha generado un escenario altamente vulnerable frente a ataques cibernéticos. Este nuevo panorama se caracteriza por la multiplicidad, sofisticación y frecuencia de los incidentes digitales que amenazan la seguridad, integridad y disponibilidad de los datos. En este contexto, la ciberseguridad se convierte en un elemento esencial para garantizar la gobernabilidad, la protección de los derechos fundamentales y la sostenibilidad de las instituciones democráticas[1].

A nivel global, el crecimiento exponencial del cibercrimen se ha manifestado en un incremento alarmante de ataques tipo *ransomware, malware, phishing*, denegación de servicios (*DDoS*) y otros mecanismos maliciosos. Informes internacionales como los de Fortinet[2] y SonicWall[3], revelan que se presentan millones de

---

1 Kaspersky. "¿Qué es la ciberseguridad?", disponible en [https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOoonPijhYIUQrnAZVNSHuCWGjW_APukiD87XLP3umEYc3XamCIBn]; Amancio Valoyes Mosquera. "Ciberseguridad en Colombia" (artículo de posgrado), Especialización en Seguridad Informática, Bogotá, Universidad Piloto de Colombia, 2019, disponible en [https://repository.unipiloto.edu.co/handle/20.500.12277/6370].

2 Fortinet. *Informe global del panorama de amenazas. Un informe semestral de FortiGuard Labs*, febrero de 2023, disponible en [https://www.fortinet.com/lat/demand/gated/threat-report-2h-2022].

3 SonicWall. *2021 SonicWall Cyber Threat Report*, 2021, disponible en [https://www.sonicwall.com/resources/white-papers/2021-sonicwall-cyber-threat-report].

ataques diarios en diferentes regiones del mundo, siendo América Latina una de las más afectadas. En esta región, Colombia ocupa el tercer lugar en número de ciberataques, registrando más de 11 millones de amenazas en 2021 y un aumento del 30% en 2022[4].

La situación nacional refleja una creciente preocupación por parte del Estado colombiano frente a la ciberseguridad. Solo entre enero y octubre de 2022 se reportaron 54.121 denuncias por delitos informáticos, una cifra que supera ampliamente los 11.223 casos registrados durante todo el 2021[5]. Estos datos evidencian la necesidad de una respuesta estructurada y sistémica por parte de las entidades públicas encargadas de la gestión y protección de los datos del Estado. En particular, las entidades responsables del control fiscal enfrentan un desafío doble: proteger sus propios sistemas de información y garantizar que los sujetos de control cuenten con mecanismos adecuados de seguridad digital.

En el ámbito de la administración pública, la ciberseguridad reviste una importancia crítica. Los sistemas de información utilizados por las entidades estatales gestionan datos sensibles sobre contratación, finanzas, salud, educación, seguridad, entre otros. La vulneración de dichos sistemas no solo compromete la operatividad institucional, sino que también pone en riesgo la privacidad de los ciudadanos, la integridad de la información pública y la confianza en las instituciones democráticas[6]. La administración electrónica, en tanto que paradigma de modernización estatal, requiere de una infraestructura tecnológica robusta, protegida y resiliente para el cumplimiento de sus funciones misionales.

---

4 Hernán Diazgranados. "Empresas: principal objetivo de ciberataques en América Latina", *Kaspersky*, 1.° de octubre de 2020, disponible en [https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/]; Centro Cibernético Policial. *Boletín estadístico de delitos informáticos*, Policía Nacional de Colombia, 2022.

5 Ídem.

6 isaca. *State of Cybersecurity 2021, Part 1: Global Update on Workforce*, isaca, 2021; Jeimy J. Cano M. "De los incidentes de seguridad en la gestión de la protección de datos personales y la Industria 4.0", en *v Congreso Internacional de Protección de Datos Personales*, Bogotá, Superintendencia de Industria y Comercio, 8 y 9 de junio de 2017.

La Contraloría General de la República –en adelante CGR–, como máximo órgano de control fiscal del Estado colombiano, no está exenta de estas amenazas. Su misionalidad depende, en gran medida, de la capacidad de recolectar, procesar, analizar y proteger grandes volúmenes de datos provenientes de entidades nacionales y territoriales. En este sentido, la incorporación de la ciberseguridad en sus procesos de auditoría, fiscalización y vigilancia resulta no solo pertinente, sino imprescindible para salvaguardar la legalidad y eficiencia en el uso de los recursos públicos[7].

La necesidad de articular la vigilancia fiscal con estrategias de ciberdefensa ha sido reconocida por el propio Estado colombiano a través de documentos de política pública como el CONPES 3701 de 2011[8], el cual establece lineamientos para una política nacional de ciberseguridad y ciberdefensa. Este documento identifica tres ejes críticos: la falta de coordinación interinstitucional, la escasa formación especializada y las debilidades normativas. Tales vacíos deben ser superados mediante un enfoque integral que combine capacidades tecnológicas, institucionales y humanas.

Frente a este panorama, la creación de la Dirección de Información, Análisis y Reacción Inmediata –en adelante DIARI– por parte de la CGR, mediante el Decreto 2037 de 2019[9], representa un paso fundamental en la transformación digital del control fiscal. Esta dependencia tiene como propósito el análisis masivo de datos, la generación de alertas tempranas y la reacción oportuna ante posibles riesgos fiscales. Desde su creación, la DIARI ha liderado el desarrollo de

---

7 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, Bogotá, CGR, 2024, disponible en [https://www.camara.gov.co/sites/default/files/2024-12/CGR-informe-de-gestion-2023-2024.pdf].

8 Departamento Nacional de Planeación. *Documento CONPES 3701 "Lineamientos de política para la ciberseguridad y la ciberdefensa"*, Bogotá, DNP, julio de 2011, disponible en [https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf].

9 Decreto 2037 de 23 de octubre de 2019, "Por el cual se desarrolla la estructura de la Contraloría General de la República, se crea la Dirección de Información, Análisis y Reacción Inmediata y otras dependencias requeridas para el funcionamiento de la Entidad", *Diario Oficial* n.° 51.130, del 7 de noviembre de 2019, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30038323].

herramientas que han permitido optimizar los tiempos de respuesta institucional ante hallazgos de presunto detrimento patrimonial.

La articulación entre tecnología, vigilancia fiscal y ciberseguridad no es solo una opción técnica, sino una obligación institucional. En un ecosistema digital caracterizado por la interconexión global, la defensa de la información se convierte en una garantía para la estabilidad fiscal y la protección de los bienes públicos. La vigilancia y control fiscal contemporáneo exige nuevos enfoques, herramientas inteligentes y capacidades humanas altamente especializadas para enfrentar los desafíos de la era digital. En este sentido, la consolidación de una estrategia de ciberdefensa fiscal requiere de la participación articulada de diferentes actores del sistema, como el MINTIC, ColCERT, la Policía Nacional, la Fiscalía General y las propias entidades auditadas.

Esta minuciosa investigación se encuentra dividida en tres partes que pretenden abordar de manera ordenada y profunda aquellos retos que supone para el Estado moderno, las instituciones y los ciudadanos en materia de ciberseguridad, atendiendo elementos fundamentales como el contexto histórico y social, acontecimientos relevantes y otros que permitan un mejor entendimiento de esta problemática. En la primera parte titulada "Tecnología y sociedad: nuevas realidades, desafíos urgentes", se plantea una reflexión crítica sobre el papel que desempeña la tecnología en la sociedad en relación al Estado y las relaciones sociales. En esta primera parte se propone una mirada interdisciplinar donde se enmarcan los principales referentes teóricos que recoge esta investigación.

La tecnología en la historia de la humanidad siempre ha marcado importantes hitos, avances que han permitido el desarrollo y progreso de los seres humanos como especie, en función de sus cambiantes aspiraciones. La aparición y desarrollo del internet y las aplicaciones digitales es una expresión de ese desarrollo que está enmarcada en lo que algunos han denominado "la sociedad del conocimiento", una sociedad donde el conocimiento es el principal activo en términos del capital y que al mismo tiempo simboliza progreso y eficiencia. De manera paralela se genera "la sociedad del desconocimiento", una marcada por la exclusión digital y la desigualdad al acceso a este

tipo de herramienta. Dentro de este apartado se explora la tensión entre estos dos escenarios y algunas de sus consecuencias.

Dentro de los apartados siguientes: "apocalípticos e integrados" y "los tecno-optimistas versus los tecno-apocalípticos", luego de un desarrollo contextual, se aborda los beneficios del desarrollo de las TIC y las innovaciones digitales en función de la eficiencia estatal y la mejora de la gobernabilidad, al mismo tiempo que se alerta de los efectos de algunas de las prácticas de control social asociada a estas como la cibervigilancia, vigilancia masiva, concentración de poder e información digital. Dentro de este capítulo se pretende, entonces, abarcar las implicaciones y los debates que genera el agenciamiento tecnológico y la ampliación de la utilización de herramientas tecnológicas con especial énfasis en su papel en el Estado.

Antes de finalizar el capítulo, se plantea una mirada a los fundamentos de CIA para proponer el concepto de ciber-resiliencia en el marco de las brechas y ataques digitales que las instituciones han sufrido en Colombia. En suma, este primer capítulo sienta las bases para comprender por qué la ciberseguridad debe ser una prioridad en el diseño y ejecución de políticas públicas de control fiscal.

La segunda parte de esta investigación titulada "Brechas institucionales en protección digital", se enfoca en las principales problemáticas que enfrentan las instituciones en Colombia en términos estructurales, normativos y operativos. En principio se exponen algunas cifras y datos que permiten reconocer la situación actual del país en términos de seguridad digital, reconocer algunas de sus principales debilidades y retos, el comportamiento del ciberdelito y algunas de las tendencias locales y globales. Además, dentro del capítulo se explora cómo las diferentes modalidades de delitos digitales han tenido incidencia en el contexto colombiano, no solo afectando a usuarios naturales, sino también a entidades estatales, perturbando el normal funcionamiento de las mismas y generando pérdidas económicas e incluso de información.

El capítulo también realiza una revisión crítica del marco normativo colombiano en materia de ciberseguridad. Se mencionan leyes fundamentales como la Ley 1273 de 2009 (delitos informáticos), la Ley 1581 de 2012 (protección de datos personales) y el

Decreto 2037 de 2019 (creación formal de la DIARI). Así mismo, se analizan políticas públicas como el CONPES 3701 de 2011 y la Estrategia Nacional de Ciberseguridad 2020–2025, las cuales buscan fortalecer la protección de infraestructuras críticas y la resiliencia digital del Estado. Sin embargo, se advierte que estas iniciativas aún presentan vacíos de implementación, debilidad en la articulación interinstitucional y una fragmentación normativa que dificulta su operatividad real.

Para la última parte de este segundo capítulo, se plantea que la protección institucional no puede depender únicamente de la tecnología, sino que debe estar acompañada de una estrategia integral que articule normatividad, talento humano, financiamiento adecuado y participación ciudadana. La interoperabilidad de sistemas entre entidades, la gobernanza de datos y la corresponsabilidad de los proveedores tecnológicos son condiciones necesarias para consolidar un modelo de control fiscal robusto en la era digital. La DIARI, como núcleo operativo del sistema, debe ser fortalecida técnica, presupuestal y normativamente para actuar con autonomía y eficacia ante escenarios de riesgo.

Dentro del tercer y último capítulo titulado "Casos emblemáticos de ciberataques a entidades públicas y sus impactos fiscales", se recopila un importante número de casos que resultan significativos e incluso emblemáticos en el marco de la seguridad digital. Su objetivo principal es evidenciar cómo los ciberataques afectan de manera directa y sistemática la gobernabilidad institucional, la administración del gasto público y la integridad del control fiscal a través del estudio de casos reales en Colombia y América Latina. Este capítulo también plantea la urgencia de consolidar capacidades institucionales de respuesta ante ciberincidentes, y resalta el papel estratégico que puede desempeñar la Dirección de Información, Análisis y Reacción Inmediata –DIARI– en el diseño de un modelo de vigilancia fiscal digital robusto y preventivo.

El capítulo recopila casos no solo del contexto colombiano, de empresas de importante preeminencia en el sector público y con relevancia para el cumplimiento de las funciones del Estado, sino también de otras entidades de países como México, donde se bus-

ca no solo comparar las experiencias y respuestas articuladas por otros organismos y entidades en otros contextos, sino también evidenciar que las dinámicas asociadas a prácticas digitales como el *hacking*, activismo digital, secuestro de información digital, ciberdelitos y otras actividades asociadas a violaciones de sistemas de seguridad son un fenómeno global que afecta a las organizaciones y Estados de manera simultánea en el contexto glo-cal. Dentro de este capítulo se examina el rol de la DIARI frente a escenarios de riesgo. Se destaca cómo esta dependencia de la Contraloría General de la República ha sido diseñada para operar como un nodo de análisis predictivo, articulando herramientas como minería de datos, *machine learning* y tableros de control territorial para generar alertas tempranas sobre posibles anomalías fiscales. Estas capacidades le permiten actuar de manera proactiva frente a eventos que podrían derivar en daño patrimonial y contribuyen a convertir la inteligencia digital en decisiones estratégicas de auditoría, fiscalización y sanción.

Atendiendo el alarmante panorama expuesto a lo largo del capítulo sobre el estado actual de la ciberseguridad en el sector público colombiano, evidenciando que los ciberataques no son eventos aislados ni meramente técnicos, sino fenómenos estructurales que pueden comprometer la sostenibilidad del Estado y la legalidad en el manejo de los recursos públicos, se sugiere la necesidad urgente de consolidar una estrategia nacional de ciber-resiliencia en el ámbito fiscal, basada en la anticipación, la prevención y la articulación efectiva entre actores técnicos, normativos y políticos. Lo anterior, se debe a que este enfoque no solo fortalece la protección institucional, sino que posiciona el control fiscal como una herramienta clave para la defensa de la soberanía digital del país.

Los resultados de investigación presentados al final de este trabajo realizan un abordaje, desde una perspectiva crítico-analítica, sobre el papel estratégico de la DIARI en la protección de los datos públicos y el fortalecimiento del control fiscal en el entorno digital. Se analiza el marco conceptual y normativo de la ciberseguridad, se exponen casos emblemáticos de vulneraciones a sistemas informáticos de entidades públicas y se proponen recomendaciones para una mayor

articulación entre tecnología y fiscalización. El objetivo es contribuir a la construcción de un modelo de vigilancia fiscal proactivo, ciber-resiliente y ajustado a las nuevas realidades del ecosistema digital.

Esta problemática planteada le da pertinencia al objetivo general de esta investigación, que es el de caracterizar el impacto de la tecnología en los sistemas de control fiscal desde un enfoque determinista débil. Este enfoque permite un mejor abordaje de las diferentes maneras en que la tecnología está afectando el control fiscal y permite desarrollar respuestas más efectivas a los desafíos que plantea este nuevo conjunto de herramientas tecnológicas.

A lo largo del proceso de investigación se analizaron datos sobre el uso de la tecnología en los sistemas de control fiscal, los beneficios y riesgos de la tecnología para los procesos de auditoría de lo público y las tendencias globales sobre el impacto de la tecnología en la vigilancia fiscal. Se analizaron las tendencias en el marco metodológico propuesto por la etnografía virtual planteada por Hine[10], haciendo una aproximación comprensiva a la fuerza de las tecnologías digitales emergentes como un fenómeno global que impacta localmente y del cual no podemos escapar.

Dentro de las conclusiones, se afirma que aunque la Contraloría General de la República ha avanzado en la implementación de herramientas tecnológicas –en especial a través de la DIARI–, persisten brechas estructurales en normatividad, talento humano, articulación interinstitucional y cultura organizacional. Se hace necesario comprender que la ciberseguridad no debe ser entendida como un tema técnico aislado, sino como un eje estratégico para la sostenibilidad del Estado, la protección del patrimonio público y la confianza ciudadana. Se propone una transición desde un modelo fiscalizador reactivo hacia uno preventivo, basado en inteligencia de datos, vigilancia anticipada y auditoría digital. Por último, se afirma que consolidar un ecosistema de ciber-resiliencia en el control fiscal no solo es un imperativo administrativo, sino también un compromiso ético y democrático con la defensa de lo público en la era digital.

---

10 Cristhine Hine. *Etnografía virtual*, Barcelona, Edit. uoc, 2004.

Capítulo primero
Tecnología y sociedad: nuevas realidades, desafíos urgentes

I. Ambivalencias: sociedad del conocimiento/sociedad del desconocimiento

Se pueden precisar diferentes autores que abordan el tema de la relación entre sociedad, conocimiento y tecnologías, los cuales logran generar aportes a través de sus estudios e investigaciones sobre la dinámica de dialéctica ambivalente[11] entre el cambio social y el cambio tecnológico[12]. Uno de los grandes líderes de este tipo de estudios es el sociólogo español Manuel Castells, quien analizó en su momento de forma casi profética el impacto social de las tecnologías de la información y la comunicación –en adelante tic– al enfrentarnos al ritmo frenético del cambio tecnológico.

La reconocida trilogía de Castells[13], aporta de manera significativa hacia la comprensión de un contexto de transformación de las

---

11 Zygmunt Bauman y Keith Tester. *La ambivalencia de la modernidad y otras conversaciones*, Barcelona, Paidós, 2011.

12 Nicholas G. Carr. *Atrapados: cómo las maquinas se apoderan de nuestras vidas*, Buenos Aires, Taurus, 2014; íd. *Superficiales: ¿qué está haciendo internet con nuestras mentes?*, Madrid, Taurus, 2017; Jeffrey D. Sachs. *Las edades de la globalización: geografía, tecnologías e instituciones*, Barcelona, Deusto, 2021; Daron Acemoglu y Simon Johnson. *Poder y progreso: nuestra lucha milenaria por la tecnología y la prosperidad*, México, D. F., Crítica, 2023; Max Fisher. *Las redes del caos: la historia secreta de cómo las redes sociales empobrecen la mente y erosionan el mundo*, Barcelona, Crítica, 2023.

13 Manuel Castells. *La era de la información: economía, sociedad y cultura, vol. 1: La sociedad red*, Madrid, Alianza, 2017

formas colectivas de pensamiento, analizando el impacto de las TIC en la economía, la sociedad y la cultura. CASTELLS[14] precisó con suficiente evidencia empírica que las TIC están transformando la forma en que vivimos, trabajamos y nos relacionamos, explicando los principales aspectos de la sociedad del conocimiento, en los cuales es factible caracterizar tres factores que la constituyen: la gestión tecnológica de los recursos económicos, la revolución del conocimiento y la necesidad imperiosa de los controles a este proceso.

CASTELLS vaticinaba cómo la tecnología puede producir cambios sociales dentro de un entorno, pero que esto depende de la fuerza de las instituciones, ya que la tecnología refleja el nivel de desarrollo de una sociedad en la medida en que logre cerrar las brechas y conseguir que todos los grupos sociales accedan a los usos de la misma. Un análisis del impacto de la era digital lo encontramos en el recorrido que realizan DAVID y FORAY:

> Se trata de una revolución importante sobre todo porque concierne fundamentalmente a las tecnologías de producción y distribución de información y conocimiento. Estas nuevas tecnologías, cuyas primeras formas surgen durante los años 50 y que estallan verdaderamente con la aparición de Internet, producen unos espantosos efectos potenciales. Permiten el acceso a distancia a la información e incluso al conocimiento. Y no solo eso, permiten la transmisión de mensajes escritos y de todo lo que se puede "digitalizar" (música, imagen), pero permiten también tener acceso a sistemas de conocimiento sobre los que se puede actuar desde lejos (experimentación a distancia), el aprendizaje a distancia en el marco de una relación dinámica entre el maestro y el alumno (tele-educación) y la posibilidad de disponer sobre la mesa de despacho de cantidades inimaginables de datos, o sea, de una especie de biblioteca universal. Cabe distinguir diversos tipos de repercusiones de las tecnologías de la información sobre la creación de conocimiento.
>
> El primero es simplemente la creación de una abundancia potencial de información, que es verdaderamente revolucionaria. Piénsese en la dificultad permanente del hombre, antes de la época moderna,

14 MANUEL CASTELLS. *Comunicación y poder*, México, D. F., Siglo XXI, 2009.

para obtener esos instrumentos del saber. GERBERT D'AURILLAC, gran intelectual del año 1000, tenía una biblioteca de 20 libros ¡lo que era mucho para la época!, con excepción de algunos lugares milagrosos donde se materializaba la vida intelectual, como la biblioteca de Alejandría, los instrumentos del saber eran raros y difíciles de encontrar. Mas si se prefiere un viaje en el tiempo menos peligroso, piénsese simplemente en el trabajo agotador que tenía que realizar un estudiante hace apenas 20 años para llegar a la "posesión del arte" de una disciplina o de un problema, así como en la dificultad casi insuperable de estar al tanto de los trabajos más recientes en la esfera estudiada. Se ha producido, pues, una lenta evolución acentuada por la invención del códice y del libro (que reemplazan a los rollos), la elaboración del papel, la transformación del libro en instrumento de saber (índices, cuadros, sistema de llamadas y de notas), el mejoramiento de la producción material de los ejemplares (desde la organización "industrial" en la sala del copista medieval hasta la invención de la imprenta), la multiplicación de las bibliotecas modernas y por último el surgimiento de redes de comunicación y de acceso cada vez más eficaces. ¿Ponen fin las nuevas tecnologías a esta evolución? Es evidente que no, puesto que todavía se han de realizar inmensos progresos, por ejemplo, en los sistemas de búsqueda de la información. Sin embargo, cabe casi decir que estas nuevas tecnologías ponen un punto final a lo que el medievalista francés G. DUBY denominaba "la búsqueda incesante de instrumentos de saber" de que se ha ocupado el hombre desde tiempos inmemoriales. El segundo tipo de repercusión está relacionado con el aumento en potencia de las interrelaciones creativas entre, por ejemplo, los creadores del producto, los proveedores y los clientes finales. La creación de objetos virtuales, modificables al infinito, a los que cada uno tiene un acceso instantáneo, facilita la labor de aprendizaje colectivo. Las nuevas posibilidades de simulación son a este respecto un elemento esencial. El tercer tipo de repercusión estriba en las posibilidades de tratamiento por medio de las nuevas tecnologías de gigantescas bases de datos, lo que constituye en sí un poderoso sistema de progreso del saber (tanto en la esfera de las ciencias de la naturaleza y humanas como en las de la gestión y las ciencias sociales). Por esa razón, la investigación impulsada por estas nuevas posibilidades se impone ineludiblemente en determinados tipos de empleo de gestión. El último tipo de repercusión combina los tres primeros. Se trata del desarrollo de sistemas descentralizados y en gran escala de recopilación de datos, de cálculo y de intercambio de

> los resultados, que caracterizan por ejemplo la manera de realizar la investigación en la actualidad en astronomía o en oceanografía[15].

En este orden de ideas, es posible entender la era de la información como una sociedad en donde los individuos dependen cada vez más de tener un acceso a la información y al conocimiento para poder generar y agregar valor a los productos, bienes y servicios. Adicional a esto, el siglo XXI se caracteriza por la desaparición de dos barreras: la del tiempo y la del espacio. A este fenómeno se le denomina globalización y ha conllevado a una creciente interconexión entre los países y las personas. Esta hiperinterconexión mediada por las TIC ha tenido un impacto significativo en la sociedad, la economía y la cultura, alterando de manera significativa el cambio de nuestra geografía mental, hoy por hoy, solo estamos a un clic de distancia[16].

Es claro que este acceso a la tecnología ha transformado muchas dinámicas sociales, generando cambios en las relaciones laborales y económicas, lo que obliga a los individuos a adaptarse a estas fuertes trasformaciones. JÁCOME[17] plantea que el término ideal es "tecnologías emergentes", ya que estas condicionan la existencia de nuevas profesiones emergentes. Para el análisis de las tecnologías en el contexto de la formación de trabajos emergentes, resultan relevante los análisis de JÁCOME, debido a que propone replantear el t**é**rmino en torno a las tecnologías y explica c**ó**mo estas permiten la aparición de nuevas profesiones.

ALDERETE y JONES[18], definen las TIC como una herramienta fundamental en la actualidad. Según estos autores, diversos sectores

---

15 PAUL A. DAVID y DOMINIQUE FORAY. "Una introducción a la economía y a la sociedad del saber", *Revista Internacional de Ciencias Sociales*, n.° 171: La sociedad del conocimiento, 2002, disponible en [https://unesdoc.unesco.org/ark:/48223/pf0000125502_spa], pp. 10 y 11.

16 PETER F. DRUCKER. *La sociedad poscapitalista*, Buenos Aires, Edit. Sudamericana, 2013.

17 ORFA DE J. JÁCOME ÁLVAREZ. "Las tecnologías emergentes en la sociedad del aprendizaje", *Revista Científica Hallazgos 21*, vol. 6, n.° 1, 2021, disponible en [https://revistas.pucese.edu.ec/hallazgos21/article/view/511], p. 105.

18 MARÍA VERÓNICA ALDERETE y CAROLA JONES. "Estrategias de TIC en empresas de Córdoba, Argentina: un modelo estructural", *SaberEs*, vol. 11, n.° 2, 2019, pp. 195 a 216, disponible en [https://saberes.unr.edu.ar/index.php/revista/article/view/203].

económicos y sociales del mercado se han visto favorecidos no solo en sus procesos internos, sino también en lo relacionado con recursos intangibles como lo son el uso de datos, la oferta de productos de excelente calidad, la flexibilidad dentro de la demanda y la innovación continua, en este sentido, las tecnologías fortalecen el desarrollo y la sostenibilidad de las empresas.

Un claro ejemplo del impacto y la necesidad de las tecnologías se evidenci**ó** durante la emergencia sanitaria declarada a mediados de 2019 por el virus del COVID-19, que gener**ó** la transformación de diversos aspectos sociales, económicos y laborales a nivel mundial. Las medidas de confinamiento y limitación a la movilidad nacieron como respuesta a la necesidad de los gobiernos de frenar la creciente ola de contagios; estas medidas si bien frenaron la expansión del virus, también debilitaron gravemente la dinámica económica global, pues ninguna nación estaba lista para afrontar la transformación de los espacios físicos a espacios de trabajo remoto mediados por tecnologías.

A causa de la crisis sanitaria por el COVID-19 numerosas empresas ya establecidas presentaron dificultades, lo que las llevó al cierre permanente o temporal dejando a una gran parte de la población en el panorama complejo del desempleo; según un informe del Banco mundial: "La pandemia dejo alrededor de 70 millones de personas en pobreza extrema en el año 2020"[19].

Por ello, las empresas y los *freelance* buscaron reinventarse a través de las nuevas tecnologías debido a que la digitalización del trabajo brindaba mayores alternativas de subsistencia durante el confinamiento, dando paso al nacimiento de nuevos trabajos y nuevas movilidades sociales. Esta situación gener**ó** una p**é**rdida masiva de empleos a raíz del cierre de múltiples empresas que no lograron adaptarse a la naciente modalidad de teletrabajo, lo que obligó a los

19 BANCO MUNDIAL. "Se frenan los avances mundiales en la reducción de la pobreza extrema", comunicado de prensa n.° 2023/011/EFI, Washington, D. C., 5 de octubre de 2022, disponible en [https://www.bancomundial.org/es/news/press-release/2022/10/05/global-progress-in-reducing-extreme-poverty-grinds-to-a-halt].

individuos a buscar alternativas para obtener ingresos desde sus hogares, utilizando el internet como herramienta principal.

Según un informe del MINTIC[20], en 2019 en Colombia solo hubo siete millones de conexiones fijas a internet, y durante los primeros nueve meses del 2020 se evidenció un crecimiento exponencial de las mismas, puesto que se sumaron 692.498 conexiones fijas nuevas de internet. Lo anterior evidencia un crecimiento significativo, demostrando la aceleración en el uso de esta herramienta durante el periodo de la pandemia, de forma simultánea debido a los cambios de las rutinas de estudio y trabajo, el internet se volvió indispensable en los hogares colombianos generando la necesidad de conectividad.

Con el auge de la globalización y la irrupción de las tecnologías digitales es factible categorizar el campo de análisis de las profesiones emergentes, aquellas que nacen a raíz de la necesidad de interconexión digital y se expanden por la influencia de los factores externos, caracterizadas por una alta incidencia dentro de las estructuras sociales. En este sentido, la apertura y el auge del mundo virtual nutrido a raíz de la pandemia por COVID-19, logró alterar las bases del mundo social y la naturaleza de las interacciones humanas, abriendo paso a lo que serían las nuevas profesiones digitalizadas de los conocidos *freelance* o trabajadores que se encargan de realizar labores de forma independiente y con contratos temporales.

En concordancia con este análisis, MENDIZÁBAL y ESCALANTE advierten que: "los trabajos tradicionales transitarán hacia nuevas formas de ser realizados"[21]. Esto no quiere decir que los trabajos serán totalmente reemplazados u automatizados sino, que pasarán por una innovación en torno al uso de plataformas digitales de ma-

---

20 REDACCIÓN SEMANA. "Acceso a internet en Colombia se aceleró durante la pandemia", *Semana*, 9 de febrero de 2021, disponible en [https://www.semana.com/economia/empresas/articulo/acceso-a-internet-en-colombia-se-acelero-durante-la-pandemia/202108/].

21 GABRIELA MENDIZÁBAL BERMÚDEZ y ANA ESTHER ESCALANTE FERRER. "El reto de la educación 4.0: competencias laborales para el trabajo emergente por la COVID-19", *RICSH Revista Iberoamericana de las Ciencias Sociales y Humanísticas*, vol. 10, n.° 19, 2021, pp. 261 a 283, disponible en [https://www.ricsh.org.mx/index.php/RICSH/article/view/242].

nera que las interacciones en torno a estos estarán mediadas y encaminadas a una industria de servicios digitales.

En el devenir de la contemporaneidad, el teletrabajo llegó para quedarse y la asunción de tecnologías en el campo laboral son imperativas e impostergables, es por esto, que las transformaciones dentro del espacio físico con relación a los procesos de adaptación al mundo digital se han dado de manera gradual y a su vez intensificadas por la ya mencionada crisis sanitaria; las actividades laborales surgidas en el contexto de la pandemia se han reconocido y han sido normalizadas por los actores sociales, pero no por la existencia de normas jurídicas que los regulen o amparen[22].

La llegada de la industria de las nuevas tecnologías o Industria 4.0, término que fue acuñado en 2011 para referirse a la implementación y uso de las nuevas tecnologías[23], se caracteriza por la interacción con el cliente dentro de la modalidad de "industrias de servicios"; si bien, en la contemporaneidad aún se guarda una relación estrecha con todo lo relacionado a los bienes materiales e industriales y la forma de comercialización de los mismos, estos han proliferado sus ventas a través de los servicios que ofrecen diversas aplicaciones digitales; cabe resaltar que este nuevo mundo se ha convertido en su mayoría en una sociedad de consumo de servicios, los mismos que son ofrecidos por la era emergente de la digitalización y el sistema de *streaming* o consumo de contenido en tiempo real.

La digitalización del trabajo permitió la continuidad de las labores dando apertura al escenario del teletrabajo, en el cual las empresas y trabajadores independientes podrían seguir teniendo reuniones y comercializando sus bienes y servicios sin necesidad del contacto físico. El uso de plataformas digitales se presentó como la solución perfecta frente al confinamiento y las demandas de subsistencia por parte de los actores sociales; como resultado, se da

---

22 Jürgen Weller. *La pandemia del COVID-19 y su efecto en las tendencias de los mercados laborales*, Santiago de Chile, Naciones Unidas, 2020, disponible en [https://repositorio.cepal.org/entities/publication/7bc229c9-c274-4208-b4a7-8581b42d68d3], p. 24.

23 Mendizábal Bermúdez y Escalante Ferrer. "El reto de la educación 4.0: competencias laborales para el trabajo emergente por la COVID-19", cit.

una proliferación en el uso de herramientas y aplicaciones digitales con el propósito de dar respuesta a las necesidades de movilidad presentada por los individuos.

De igual manera, Bueno[24] plantea el siglo xxi como la mutación del entorno físico a uno digital. Esto se debe a la variación generada por las condiciones de la pandemia, lo que llevó a muchas empresas a distribuir sus bienes a través de aplicaciones digitales, dando paso a que existiera una expansión de los mercados laborales no solo de compañías, restaurantes y demás, sino también a la creación de la necesidad de supervivencia a raíz del confinamiento, dando como respuesta a ello la nueva modalidad de comercialización por medio de plataformas de *streaming*, páginas, redes sociales, etc.

En la encuesta del dane sobre las tecnologías de la información y las comunicaciones en hogares (entic), se logra validar que existió un ascenso en el consumo de contenido en las plataformas digitales y redes sociales: "Colombia para el año 2020 aumentó el porcentaje de uso de plataformas digitales en un 82,3% y las videollamadas con un 79,9%"[25]. En el 2021 se aplica de nuevo la encuesta del dane, la cual refleja un aumento del 0,7% en comparación con el año anterior: "El uso de tecnologías y plataformas aumenta en un 83% y las videollamadas en un 85,4%"[26].

Ante la fuerza de la evidencia empírica, es factible recuperar el análisis social que realizaba en su momento Marcel Mauss, al se-

---

24 Carmen Bueno Castellanos. "Trayectorias que ilustran la confluencia entre actividades formales e informales", en Roberto Horta (coord.). *El futuro del empleo post pandemia del covid-19*, Cuadernos Orkestra, n.° 10/2022, España, Instituto Vasco de Competitividad - Fundación Deusto, 2022, disponible en [https://www.orkestra.deusto.es/images/investigacion/publicaciones/informes/cuadernos-orkestra/220085-El-futuro-del_empleo-post-pandemia-del-covid-19-COMPLETO.pdf], p. 51.

25 Departamento Administrativo Nacional de Estadística. "Encuesta de las Tecnologías de la Información y las Comunicaciones en hogares - entic Hogares 2020" (Boletín Técnico), Bogotá, dane, 14 de septiembre de 2021, disponible en [https://colombiatic.mintic.gov.co/679/articles-198835_bol_entic_hogares_2020.pdf], p. 22.

26 Departamento Administrativo Nacional de Estadística. "Encuesta de las Tecnologías de la Información y las Comunicaciones en hogares - entic Hogares 2021" (Boletín Técnico), Bogotá, dane, 28 de julio de 2022, disponible en [https://www.dane.gov.co/files/investigaciones/boletines/entic/bol_entic_hogares_2021.pdf], p. 23.

ñalar la existencia de hechos sociales totalizantes que implican un trastocamiento de las estructuras sociales, donde todas las dimensiones de la vida societal se ven alteradas, precisaba Mauss que:

> En este fenómeno social "total", como proponemos denominarlo, se expresan a la vez y de golpe todo tipo de instituciones: las religiosas, jurídicas, morales –en estas tanto las políticas como las familiares– y económicas, las cuales adoptan formas especiales de producción y consumo, o mejor, de prestación y de distribución, y a las cuales hay que añadirlos fenómenos estéticos a que estos hechos dan lugar, así como los fenómenos morfológicos que estas instituciones producen[27].

El control fiscal no escapa a este proceso. En este sentido, los sistemas de control fiscal deben adaptarse a los nuevos desafíos que plantea una sociedad donde la inteligencia artificial –en adelante IA–, se constituye en una herramienta que rápidamente se irradia a todos los campos del conocimiento conocido. Frente a la creciente complejidad de los conflictos, la expansión del ámbito digital y la necesidad de garantizar el efectivo uso de los recursos públicos a todos los ciudadanos, independiente de su condición social o económica, la IA empieza a jugar un rol preponderante.

En el ahora, nuevos debates sobre la relación entre derecho, justicia y ética saltan a la palestra pública. Se habla de transhumanismo[28], se menciona la edición genética de los seres humanos e incluso se plantea el problema del posible *hackeo* de nuestras neuronas o el almacenamiento en *hardware* de nuestra conciencia[29]. De igual manera, se habla de la irrupción de nuevos derechos: el derecho al olvido y obviamente el derecho a la desconexión.

Para afrontar estos desafíos, los sistemas de control fiscal deben mutar a la nueva realidad de la presencia de la IA en un mundo global. Esto significa explorar, categorizar y adoptar nuevas tecnologías y metodologías que permitan a los sistemas de control fiscal

---

27 Marcel Mauss. *Sociología y antropología*, Madrid, Tecnos, 1991, p. 157.

28 Antonio Diéguez. *Cuerpos inadecuados: el desafío transhumanista a la filosofía*, Barcelona, Herder, 2021.

29 Yuval Noah Harari. *Sapiens: de animales a dioses*, Barcelona, Debate, 2017.

ser más eficientes, accesibles y transparentes. Son cuatro grandes dimensiones de la vida social, las cuales se ven fuertemente trastocadas por la fuerza disruptiva de la IA:

- *Dimensión jurídica*: se refiere a las normas y principios jurídicos que rigen el control fiscal. La IA está impactando esta dimensión de diversas maneras, como el desarrollo de nuevas herramientas, algoritmos y tecnologías para la detección del detrimento a lo público.

- *Dimensión social*: tiene que ver con las relaciones y las estructuras sociales que afectan al control fiscal. La IA está impactando esta dimensión de diversas maneras, como el aumento de la desigualdad digital, la aparición de nuevas formas de discriminación y el desafío de los conceptos tradicionales de control fiscal.

- *Dimensión cultural*: implica los valores y las creencias culturales que subyacen al control fiscal. La IA está impactando esta dimensión alterando el cambio de los valores tradicionales de la ética de lo público, la aparición de nuevas formas de corrupción y el desafío del ciberdelito.

- *Dimensión antropológica*: ello presupone el estudio del pluralismo jurídico y el aumento de la demanda de justicia, la aparición de nuevas formas de participación ciudadana y el desafío de los conceptos deontológicos de justicia replanteando la relación entre el *ethos* y el ser.

En particular, Castells[30] había analizado la forma como las tecnologías digitales de punta estaban teniendo los siguientes impactos positivos en el control fiscal: facilitar el acceso a los sistemas de control social, mejorar la eficiencia de los sistemas judiciales y

30 Castells. *La era de la información: economía, sociedad y cultura, vol. 1: La sociedad red*, cit.

aumentar la transparencia y la rendición de cuentas. El sociólogo español también señala que las TIC están creando nuevos desafíos para los procesos de control fiscal. Uno de ellos tiene que ver con el enfrentamiento entre los que poseen el conocimiento y los que no: el apotegma *el conocimiento es poder* adquiere una pertinencia en el desarrollo tecnológico del ahora.

Uno de los filósofos que ha planteado esta disyuntiva entre conocer/desconocer es DANIEL INNERARITY[31], quien cuestiona fuertemente la creencia generalizada de que la tecnología por sí sola produce conocimiento. Hoy tenemos muchísima tecnología e IA que permite alcanzar el máximo desarrollo del conocimiento a los seres humanos, pero parte de esta es empleada de formas irracionales que fomentan la pseudociencia.

Lenta, seductora e inexorablemente hemos pasado de la sociedad del conocimiento a la sociedad del desconocimiento. Siempre que pensamos en tecnologías de punta, estamos pensando en infraestructuras tecnológicas, casi nunca mencionamos la importancia de lo que este filósofo español denomina *infraestructura simbólica*. Al respecto plantea que:

> Cuando se habla de progreso, de sociedades del conocimiento o de ciudades inteligentes, lo primero que viene a la cabeza es el imaginario tecnológico-digital: dispositivos tecnológicos como sensores, plataformas de gestión de servicios, el internet de las cosas, sistemas para la adquisición y almacenamiento de datos, la gestión de los transportes [...] Es decir, pensamos en términos de infraestructura material y muy poco en relación con lo que podríamos llamar infraestructura simbólica[32].

En este orden de ideas, estas dimensiones afectadas y los desafíos planteados destacan la importancia de considerar el impacto de la tecnología digital en el control fiscal desde un enfoque del determinismo débil. Es de anotar que la perspectiva determinista débil im-

---

31 DANIEL INNERARITY. *La sociedad del desconocimiento*, Barcelona, Galaxia Gutenberg, 2022.

32 Ibíd., p. 107.

plica entender que las fuerzas tecnológicas determinan los cambios sociales y culturales. El analista Jared Diamond[33] afirmaba sobre la existencia de una incidencia de la tecnología, pero esta depende de la interrelación de los grupos sociales con las herramientas y la gestión institucional de los recursos que brindan de forma *sui generis* los entornos geográficos.

La Escuela de Toronto persiste en la consigna del determinismo débil, al analizar la manera como las tecnologías emergentes influyen y determina en binomios de interacción en las formas sociales, insistiendo en entender la naturaleza tecnológica de estas configuraciones sociales. Tal como lo plantea Sachs:

> Estas interrelaciones son tecnológicas, económicas, institucionales, culturales y geopolíticas, y se producen entre sociedades de todo el mundo a través del comercio, las finanzas, las empresas, la inmigración, la cultura, los imperios y la guerra"[34].

El enfoque del determinismo débil permite comprender mejor los diferentes modos en que el alto desarrollo de la tecnología digital está afectando al control fiscal y permite desarrollar respuestas más efectivas a los desafíos que impone esta fuerte tendencia global. Asumir este debate no solo sería de gran importancia para identificar sus aspectos más importantes, sino que también nos ayudaría a generar un desarrollo de políticas y programas que aborden los desafíos planteados por las tecnologías emergentes.

Tal y como lo precisa Coeckelberg, debemos estar alertas frente a la banalidad tecnológica:

> El peligro estriba, de nuevo, en el ejercicio del poder sin conocimiento y (por lo tanto) sin responsabilidad: y lo peor es que hay terceras personas expuestas a él. Si existe algo parecido al mal absoluto, habita donde lo situó la filósofa del siglo xx Hannah Arendt: en el sinsentido del trabajo y las decisiones banales cotidianas[35].

---

33 Jared M. Diamond. *Armas, gérmenes y acero: breve historia de la humanidad en los últimos trece mil años*, Barcelona, Barcelona, Debate, 2018.

34 Sachs. *Las edades de la globalización: geografía, tecnologías e instituciones*, cit., p. 22.

35 Mark Coeckelbergh. *Ética de la inteligencia artificial*, Madrid, Cátedra, 2021, p. 148.

Frente a esta banalidad tecnológica hay una serie de posibles acciones que podrían tomarse. Una de estas sería la de educar a los responsables políticos, los operadores de justicia y el público en general sobre el impacto de las nuevas tecnologías en el control fiscal. Esto podría ayudar a promover una comprensión más amplia de los desafíos y oportunidades que plantea la tecnología para las entidades encargadas de preservar el buen uso del erario en las nuevas realidades virtuales y en el ámbito de la proliferación de algoritmos inteligentes.

En el ítem siguiente se caracteriza desde el enfoque del determinismo débil el impacto de las tecnologías de punta o visto de otra manera el enfrentamiento tradicional entre tecno-optimistas y tecno-apocalípticos.

II. Apocalípticos e integrados

El semiólogo Umberto Eco[36] mencionaba las formas de asumir la cultura de masas como un debate entre apocalípticos e integrados. Aquellos que la cuestionan y la atacan, hasta llegar a los movimientos extremos de tratar de destruirla. En la orilla opuesta los integrados, los que la asumen de una forma abierta y la aplican cotidianamente estando siempre en la vanguardia de las tendencias y cambios en la cultura de masas. Extrapolando este binarismo al análisis de tecnologías emergentes, es factible afirmar que en el mundo actual se asume el desarrollo tecnológico desde una perspectiva binaria que podemos denominar: el enfrentamiento entre los tecno-optimistas y los tecno-apocalípticos.

La visión tecno-apocalíptica pervive en nuestro imaginario colectivo y se recrea en nuestras pesadillas nocturnas, donde las máquinas, robots o tecnologías inteligentes asumen niveles de conciencia y se rebelan, dominando a los seres humanos y convirtiéndolos en sus fuentes de energía. *Terminators*, robots inteligentes o máquinas algorítmicas en códigos cifrados hacen que sea una "misión imposible" recobrar el control y el dominio sobre estas nuevas tecnologías.

---

36 Umberto Eco. *Apocalípticos e integrados*, Barcelona, De Bolsillo, 2016.

Coeckelberg realiza un brillante análisis de la forma como estos imaginarios se nutren de nuestros arraigados miedos sobrenaturales y terminan siendo proyecciones mítico-mágicas de las visiones apocalípticas integradas en las narrativas escatológicas de la religiosidad:

> Quizás estas ideas tengan tanta repercusión porque tocan preocupaciones y esperanzas profundas respecto de los humanos y las maquinas que están presentes en nuestra conciencia colectiva. Tanto si rechazamos estas ideas en concreto como si no, hay en la cultura y en la historia humanas claros vínculos con narrativas de ficción que intentan otorgar sentido a la relación entre humanos y maquinas[37].

Las ideas sobre los grandes progresos tecnológicos como los de la singularidad exponencial y el transhumanismo son factibles de rastrear en las configuraciones históricas de las diversas religiones mundiales: "... especialmente en la tradición judeocristiana y en el platonismo. En contra de lo que mucha gente piensa, la religión y la tecnología siempre han estado conectadas en la historia de la cultura occidental"[38]. Coeckelbergh retoma los análisis de Isaac Asimov, quien denominaba a este fenómeno como *el complejo de Frankenstein* para referirse al fenómeno de las visiones apocalípticas sobre los avances científicos que se salen de control.

Prácticamente toda la industria del cine contemporáneo gira en torno al famoso escrito de la poetisa y ensayista Mary Shelley[39], quien influenciada por la ciencia de su época publica *Frankenstein o el moderno Prometeo*. El relato es una obra clásica de este tipo de narrativas: un científico da vida a una monstruosa creación, pero la rechaza y esta lo persigue hasta matarlo. Es necesario recalcar que la obra de Shelley no es un ataque a la creación científica, sino a la imperiosa necesidad que tienen los hacedores de ciencia de responsabilizarse de sus creaciones; y esa es precisamente la clave del

---

37 Coeckelbergh. *Ética de la inteligencia artificial*, cit., pp. 26 y 27.
38 Ibíd., p. 30.
39 Mary Shelley. *Frankenstein o el moderno Prometeo*, México, Gran Travesía, 2023.

debate: cómo lograr crear corresponsabilidades entre instituciones, leyes y tecnologías.

A continuación, se presentan tres de los más notorios impactos negativos que están teniendo las nuevas tecnologías emergentes. Este análisis se plantea desde el determinismo débil, tratando de asumir una perspectiva realista frente a estas nuevas tecnologías:

Impacto n.° 1: El aumento de la desigualdad digital. Desde que Castells[40] planteó la nueva pirámide social como aquella que reflejaría una concentración en riqueza tecnológica, no se ha podido superar la brecha digital entre países desarrollados y países pobres a nivel global. El alto precio de los dispositivos tecnológicos, las barreras en la precaria infraestructura que soporta estas tecnologías, el analfabetismo digital, entre otros factores, hace que se tipifiquen tres tipos de brechas digitales:

- *Brechas de acceso*, que enfatizan en las diferencias de ingresos socioeconómicos (en los países y especialmente entre las personas) como un factor que obstaculiza el uso de nuevas tecnologías, dándose una relación centro-periferia que preserva las desigualdades entre los centros urbanos y los ámbitos rurales.

- *Brechas de uso*, correlacionadas con el analfabetismo digital: es innegable que en gran parte de América Latina aún viven personas que no tienen un correo electrónico.

- *Brechas en la calidad de uso*, que se refieren al uso inteligente y estratégico de las tecnologías. Muy a pesar de poseer competencias digitales, estas no les permiten a los usuarios acceder a tecnologías del aprendizaje y el conocimiento y mucho menos a tecnologías del empoderamiento y la participación[41].

---

40 Castells. *Comunicación y poder*, cit.

41 Edimer Leonardo Latorre Iglesias, Katherine Paola Castro Molina e Iván Darío Potes Comas. *Las tic, las tac y las tep: innovación educativa en la era concep-*

Como lo precisan Acemoglu y Johnson, los tecno-optimistas o tecno-apocalípticos no logran entender que:

> Las máquinas y las técnicas innovadoras no son una especie de regalo que cae solo del cielo. Pueden estar diseñadas para intensificar la automatización y la vigilancia con el objetivo de reducir los costes laborales. O, por el contrario, pueden crear nuevas tareas y empoderar a los trabajadores. En un sentido más amplio, pueden generar una desigualdad implacable o una prosperidad compartida, en función de cómo se utilicen y de la dirección que adopte la innovación. En teoría, es la sociedad la que debería tomar estas decisiones de manera colectiva. En la práctica, quienes toman las decisiones son un grupo reducido de emprendedores, ejecutivos, visionarios y, en algunos casos, lideres políticos, y sus decisiones resultan determinantes para decidir quién gana y quien pierde por la innovación tecnológica[42].

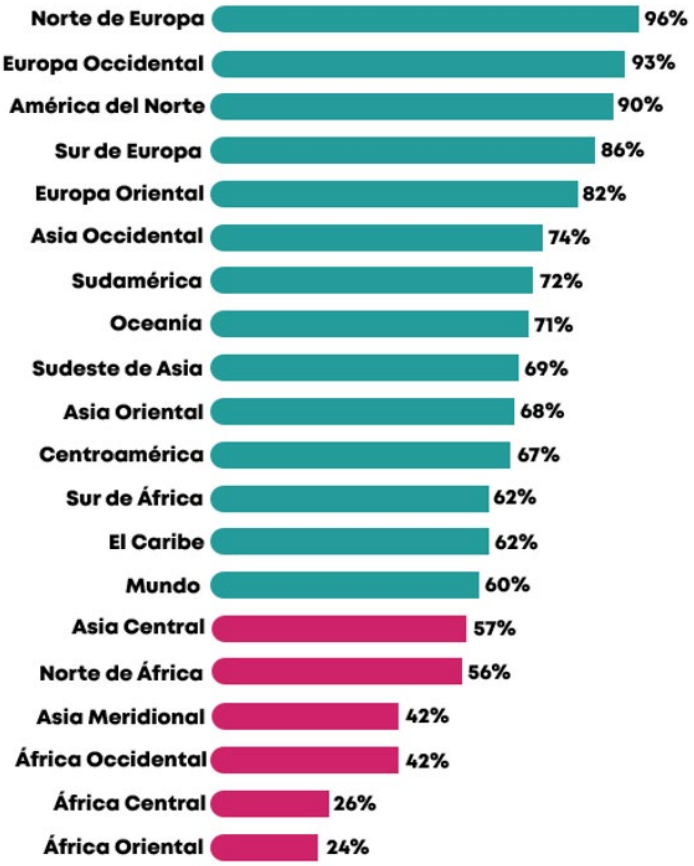
La pandemia del coronavirus hizo salir de entre los bastidores a la pobreza digital en el mundo. Fue evidente como muchas personas sufrieron de discriminación tecnológica y se constituyeron en precarizados frente al acceso a las tecnologías para realizar teletrabajo o educación remota. Personas pobres fueron radicalmente más empobrecidos al no poder tener un acceso digno a las ventajas de la digitalización. El siguiente gráfico ilustra la tasa de penetración de internet y evidencia la brecha entre países ricos y pobres.

---

tual, Bogotá, Universidad Sergio Arboleda, 2018, disponible en [https://repository.usergioarboleda.edu.co/bitstream/handle/11232/1219/TIC%20TAC%20TEP.pdf?sequence=1].

42 Acemoglu y Johnson. *Poder y progreso: nuestra lucha milenaria por la tecnología y la prosperidad*, cit., p. 33.

Gráfico 1
Tasa de penetración de Internet en enero de 2021 por regiones del mundo



Fuente: Simon Kemp. "Digital 2021: Global Overview Report", *Datareportal*, 27 de enero de 2021, disponible en [https://datareportal.com/reports/digital-2021-global-overview-report].

Según el informe del Banco Mundial sobre las tendencias digitales:

> En 2022, más del 90% de los habitantes de los países de ingreso alto estaban conectados, mientras que en los de ingreso bajo, la proporción era del 26%. Entre los países de ingreso bajo y mediano, los países de Europa y Asia central muestran mayor penetración de internet, con

> un 84%. La población conectada de Asia meridional se duplicó entre 2018 y 2020, un aumento impulsado en gran medida por India, que desde 2018 ha logrado conectar a un tercio de sus habitantes, en parte gracias a la promoción del aprendizaje sobre el uso de internet y la oferta de planes de datos más económicos. En África oriental, menos del 30% de la población usa internet[43].

Las tecnologías digitales, entre estas la IA, posiblemente termine exacerbando la desigualdad digital ya que las personas que no tienen acceso a la tecnología pueden quedar excluidas del acceso al Estado que cada día entrega una oferta apalancada en estas nuevas tecnologías e impediría a los pobres tecnológicos de disfrutar las ventajas de la economía digital. Ello hace que se deban iniciar discusiones en torno al diseño, implementación y evaluación de políticas públicas que logren garantizar el derecho al acceso digno de las tecnologías emergentes.

Impacto n.° 2: Se propician nuevas formas de discriminación. El uso del *big data* y los algoritmos centrados en IA se pueden emplear para discriminar a las personas en función de su raza, género, religión u otra característica. En este aparte, es importante incluir el problema de los sesgos de los desarrolladores o los que emplean los algoritmos para otorgar créditos, acceder a recursos económicos o programas sociales o simplemente a gozar de un derecho: "… los individuos podrían no conseguir un trabajo, no recibir un crédito, acabar en la cárcel o padecer violencia. Y no solo pueden sufrir los individuos; comunidades enteras son susceptibles de verse afectadas por decisiones sesgadas"[44].

De forma tragicómica se puede mencionar el aparte de la película *El irresistible*, protagonizada por Steve Carell quien interpreta a Gary Zimmer, un exitoso estratega electoral del partido demócrata de los Estados Unidos de América. En un esfuerzo por acercarse

---

43 Banco Mundial. "La digitalización mundial en 10 gráficos", disponible en [https://www.bancomundial.org/es/news/immersive-story/2024/03/05/global-digitalization-in-10-charts].

44 Coeckelbergh. *Ética de la inteligencia artificial*, cit., p. 109.

al votante rural de la Norteamérica profunda, este gran estratega trata de hacer que un hombre común y corriente sea alcalde de un poblado distante en Wisconsin. Hay una escena en la que expertos en *big data* analizan con un algoritmo de IA la necesidad de que el candidato regale condones en una gran hacienda, puesto que los datos indican que hay muchas mujeres solteras en la misma. La casa en mención termina siendo un convento. La IA puede hacernos concebir ideas erradas de grupos o poblaciones que pueden terminar siendo mal procesadas por los desarrolladores.

En otra arista de la realidad, es válido enunciar el ejemplo de los sesgos en el caso de los jueces del Estado de Florida que usaban el algoritmo COMPAS para dictaminar sentencias sobre libertad condicional o libertad vigilada[45]. El algoritmo permitía perfilar a los acusados con base a su historial delictivo y predecir cuáles de estos volverían a reincidir en acciones criminales. Al realizar procesos posteriores de análisis, se descubrió que el algoritmo tenía sesgos racistas.

Los falsos positivos se daban más en personas afrodescendientes, a los cuales los predictores les vaticinaban un mayor índice de reincidencia que a las personas blancas (quienes tenían una baja predicción en reincidencias). La falta de diversidad de los desarrolladores de IA y las diferencias de género (son más hombres que mujeres) de estos pueden seguir alimentando los sesgos socioculturales y revictimizar a unos grupos sociales más que a otros. Al respecto, el connotado historiador HARARI precisa que:

> La base de datos a partir de la que se adiestra a una IA es un poco como la infancia humana. Las experiencias, los traumas y los cuentos de hadas vividos durante la infancia nos acompañan toda la vida. Las IA también cuentan con experiencias de infancia. Los algoritmos incluso pueden transmitirse sus prejuicios unos a otros, como hacen los humanos. Pensemos en una sociedad futura en la que los algoritmos son ubicuos y se emplean no solo para examinar solicitudes de empleo,

---

45 MARCELA DEL PILAR ROA AVELLA, JESÚS E. SANABRIA MOYANO y KATHERIN DINAS HURTADO. Uso del algoritmo COMPAS en el proceso penal y los riesgos a los derechos humanos", *Revista Brasileira de Direito Processual Penal*, vol. 8, n.° 1, 2022, pp. 275 a 310, disponible en [https://revista.ibraspp.com.br/RBDPP/article/view/615].

> sino también para recomendar a la gente qué estudiar en la universidad. Supongamos que, debido a un prejuicio misógino preexistente, el 80 por ciento de los puestos de trabajo en el campo de la ingeniería se conceden a hombres. En esta sociedad, es probable que un algoritmo que contrata nuevos ingenieros no solo copie este sesgo preexistente, sino que además transmita el mismo prejuicio a los algoritmos de recomendación de la universidad. Una joven que entre en la universidad puede ser disuadida de estudiar ingeniería porque los datos existentes indican que es menos probable que acabe obteniendo un empleo. Lo que empezó como un mito intersubjetivo humano que afirmaba que "las mujeres no son buenas en ingeniería" puede mutar en un mito intercomputacional. Si no nos libramos del prejuicio desde el principio, los ordenadores bien pueden perpetuarlo y magnificarlo[46].

Impacto n.° 3: Desafía los conceptos tradicionales de justicia. Guy Debord en su texto ya clásico *La sociedad del espectáculo*, se percató de un cambio circunstancial e importante en el capitalismo como modo de producción y paradigma reinante. El capitalismo, sobre todo en las sociedades occidentales permeadas por la Segunda Revolución Industrial, estaba poco a poco adentrándose de lleno en una fase mucho más marcada por el consumo y la cultura de masas, en la cual, inevitablemente todo aspecto de la vida del hombre sería convertido en una mercancía predispuesta a las lógicas del libre mercado y su gran metanarrativa, el neoliberalismo.

El capitalismo neoliberal adquirió un nuevo rol performativo, el cual le hacía posible la misión de penetrar cada vez más profundo en la condición humana: "La mercancía ha conseguido colonizar toda la vida social"[47]. Si aplicamos a este proceso de mercantilización de todos los ámbitos de la existencia humana, la forma dúctil como la idea aceptada de lo justo se está trastocando, encontraríamos nuevos ajusticiamientos que movilizan a las masas con las técnicas del marketing de consumo.

Los algoritmos diseñados por IA pueden llegar a trastocar los conceptos tradicionales de justicia, ya que pueden permitir que las

---

46 Yuval Noah Harari. *Nexus: una breve historia de las redes de información desde la Edad de Piedra hasta la IA*, Barcelona, Debate, 2024, pp. 350 y 351.

47 Guy Debord. *La sociedad del espectáculo*, 2.ª ed., Valencia, Edit. Pre-Textos, 2005, p. 42.

personas tomen el control de sus propios casos o que utilicen nuevas formas de creación de conflictos o de castigos sociales llegando a irradiarse de forma tribal, sectaria y dogmática una propensión hacia el punitivismo.

En la Edad Media el linchamiento social consistía en el ajusticiamiento en formas de daño físico o en ejecuciones públicas que castigaban a la persona. Sin lugar a dudas es preferible ser condenado por un juez, tener un debido proceso e ir a prisión, que ser amarrado y desconyuntado por casi media docena de caballos, uno en cada extremidad, hasta desmembrar el cuerpo y morir en una dolorosa agonía. Se han superado ciertas prácticas punitivas tal y como lo explica Foucault[48], que hoy nadie duda en denominar de "barbáricas".

Pero el linchamiento social también podía darse en torno a las formas de rumor social como castigo reputacional. Hawthorne en su texto clásico *La letra escarlata*[49] logra crear un relato que ubica el poder del control social en grupos cerrados. El sufrimiento de su personaje principal Hester Prynne, quien es obligada a portar una letra escarlata (*guilty*) que hacía que nadie se acercara a ella y al producto de su pecado: su hija.

Sin embargo, en los últimos años, o más bien, en el último par de décadas, todo este paulatino proceso de avances en torno al castigo social se ha visto cuestionado, burlado y hasta puesto en peligro por hordas iracundas y sedientas de *justicia en mano propia* que autores como Caroline Fourest[50] catalogan como una suerte de "neo-inquisidores". Estos neo-inquisidores tecnologizados han logrado generar escenarios de retroceso en temas jurídico/punitivos y han, poco a poco, instrumentalizado las redes sociales y los algoritmos altamente sofisticados de la IA en nuevas armas para linchar y censurar a alguien de forma pública y masiva, como si de un juicio

48 Michel Foucault. *Vigilar y castigar: el nacimiento de la prisión*, México, D. F., Siglo xxi, 2018.

49 Nathaniel Hawthorne. *La letra escarlata*, Penguin Clásicos, 2015.

50 Caroline Fourest. *Generación ofendida: de la política cultural a la política del pensamiento*, Barcelona, Península, 2021.

de brujas se tratase, a través de los conocidos *escraches* y/o *funas*, lo que Byung-Chul Han[51] ha definido como *shitstorns*.

Abanderados de causas que suelen tener puntos de encuentro ideológicos como el antirracismo y el antifascismo o el feminismo y la lucha LGTBIQ+, vociferan en miles de plataformas que emplean algoritmos de IA, que sus acciones solo van encaminadas a la noble causa de proteger a la sociedad (o a ciertos grupos minoritarios) de los denominados "discursos de odio". Se perciben a sí mismos como una suerte de vigías morales, paladines de la tolerancia y la convivencia pacífica.

Estos *tribunales tecnológicos* de linchamiento y humillación, que poco tienen que envidiarles a las hogueras para quemar brujas durante la inquisición, han traído consigo situaciones contradictorias y absurdas propias del *punitivismo tecnológico*. Las nuevas formas de castigo social y de linchamiento colectivo enmarcados en el empresarismo moral, adquieren una dimensión hiperexponencial en las redes sociales.

Este fenómeno es conocido como *cancelación*. Un ejemplo de esto fue lo sucedido con la actriz estadounidense Gina Carano, quien fue cruelmente matoneada en todas las redes sociales y obviamente despedida de su papel protagónico en la serie de la plataforma Disney+ *The Mandalorian*, tras manifestar su apoyo y simpatía con el actual presidente de los Estados Unidos Donald Trump.

Estos procesos, de una magnitud global, violan características tan primordiales en los Estados sociales de derecho como la presunción de inocencia, el derecho a la legítima defensa, el debido proceso y el derecho al buen nombre. *La justicia en mano propia* hace que se agiten emociones viscerales como la rabia y el odio. Al parecer estamos en una nueva forma de guerra, tal y como lo señala Han, la información se usa como un arma:

> El sitio web de Alex Jones, conocido radical de derechas estadounidense y teórico de la conspiración, se llama InfoWars. Se trata de un destacado representante de la infocracia. Con sus burdas teorías cons-

51 Byung-Chul Han. *En el enjambre*, Barcelona, Herder, 2014.

> pirativas y con sus noticias falsas llega a un público de millones de personas que le creen[52].

Ahora bien, desde estas críticas pareciese que el determinismo débil se diluyera, como si no se tuvieran opciones que logren hacer frente a estos nuevos desafíos. Es precisamente lo que se necesita hacer, que los tecno-apocalípticos observen y analicen que toda nueva tecnología digital es una herramienta y que lo que hagamos depende del poder de las instituciones y de su capacidad de regular y controlar a las elites que dominan la tecnología, dinamizando una igualdad en el acceso a estas poderosas herramientas.

III. Los tecno-optimistas *versus* los tecno-apocalípticos

Los miedos que habitan en nuestro inconsciente colectivo tampoco permiten ver las grandes ventajas de los cambios tecnológicos. Una de las luchas más enconadas de los tecno-optimistas, es lograr que a través de las regulaciones institucionales y de las movilizaciones grupales se socialicen las tecnologías. Ya lo había predicho el sociólogo y futurólogo Alvin Toffler[53] en su texto clásico *El shock del futuro*: tecnologías y conocimientos gestionados por ciudadanos tecno-empoderados lograrían la utopía de unas tecnologías emergentes al alcance de todos.

La serie de Netflix *Black Mirror* gira en torno a las visiones apocalípticas del papel de las tecnologías de punta en la vida cotidiana. A pesar de lo distópico de esta serie y de las realidades alternativas que plantea, se deben abandonar los miedos y las emociones sin dejar de contemplar en la pantalla los desafíos futuros que agenciará la IA. Lo que se necesita desde una perspectiva tecno-optimista es ser razonable, un punto equilibrado entre la racionalidad extrema y

---

52 Byung-Chul Han. *Infocracia: la digitalización y la crisis de la democracia*, Madrid, Taurus, 2022, pp. 40 y 41.

53 Alvin Toffler. *El shock del futuro*, Barcelona, Plaza y Janes, 1981.

la emocionalidad desbordante. El connotado escritor Morgan Housel lo plantea de la siguiente manera:

> Tratar de ser más bien razonable funciona mejor que intentar ser firmemente racional [...] No eres una hoja de cálculo. Eres una persona. Una persona jodida y con emociones [...] Trata de ser solo bastante razonable. Ser razonable es más realista y tienes una mayor posibilidad de mantener esta actitud a largo plazo, que es lo que más importa…[54].

En este orden de ideas, queda claro que nuestros miedos tecnológicos no permiten ver que la IA posiblemente está ayudando a las instituciones a ser más eficientes y eficaces e impiden concentrarnos en el largo plazo. Por ejemplo, la IA está automatizando tareas administrativas, mejorando la comunicación entre los funcionarios judiciales, optimizando el tiempo de respuesta para procesos de control fiscal y reduciendo el tiempo que tarda en resolverse un caso con el manejo de algoritmos.

Tecnologías de punta permitirán reducir el tiempo en los procesos de control fiscal, logrando el acceso a la transparencia de personas que no pueden movilizarse por temas de distancias geográficas o de problemas de salud. Algoritmos de IA posibilitarán que todos los intervinientes puedan elaborar documentos de manera más rápida con los debidos controles y supervisiones. Al superarse la brecha tecnológica, también podría superarse la dinámica centro-periferia, lo que hace que puedan existir sistemas de control social sobre lo público mucho más eficaces en Estados débiles como el de la nación colombiana.

En la actualidad, la IA está permitiendo que los ciudadanos observen los procesos de control fiscal en línea y accedan a información sobre las decisiones de las entidades de control en tiempo real. Los documentos se encuentran alojados en repositorios institucionales y actualizados en modo sincrónico y asincrónico. El diseño de algoritmos potenciaría los motores de búsqueda y esto haría que se

---

54 Morgan Housel. *La psicología del dinero: 18 claves imperecederas sobre riqueza y felicidad*, México, D. F., Paidós, 2024, pp. 147 y 148.

diera una efectiva gestión de la información. La sistematización de archivos permitirá, en el largo plazo, enfrentar el problema de las demoras en dar respuestas a las denuncias de los grupos de interés y de las comunidades.

Los usos efectivos de la IA permitirían tener un control social enmarcado en el *just in time*. Obviamente, la agenda de los tecno-optimistas deberá encarar algunos desafíos para el diseño, implementación y evaluación de políticas públicas que permitan retomar el control sobre la IA en la aplicación de un control fiscal en tiempo real:

- Desarrollar políticas y programas que aborden los desafíos planteados por la IA. Estas políticas podrían centrarse en reducir la desigualdad digital, prevenir la discriminación y proteger la participación ciudadana en el contexto de la IA.

- Educar a los responsables políticos, los operadores de justicia y el público en general sobre el impacto de la IA en el control fiscal. Esto podría ayudar a promover una comprensión más amplia de los desafíos y oportunidades que plantea esta novedosa herramienta para el control de los recursos públicos.

- Generar nuevas investigaciones sobre el impacto de las tecnologías emergentes como la IA. Estas investigaciones podrían ayudar a comprender mejor los desafíos y oportunidades planteados por la IA y a desarrollar respuestas más efectivas cuyo horizonte proyectivo este en la esencia del control fiscal.

Los avances de la Comisión Europea publicado en 2019, menciona la importancia de una *IA fiable* que desde un enfoque antropocéntrico permita armonizar la IA con la esencia de lo humano. En este punto es factible proponer la noción de una ciudadanía digital, como otro concepto de estudio dentro de las investigaciones sobre el impacto de la IA. Al respecto, la evidencia empírica precisa grandes avances en los países desarrollados y un gran rezago en los países pobres como los de África y América Latina. Una de las posibles ventajas de la ciudadanía digital, sería la garantía de un conjunto de

derechos para acceder a las tecnologías emergentes y socializar las ventajas comparativas que dan estas nuevas tecnologías en especial, este logro es una de las más grandes consignas políticas de los tecno-optimistas.

Sin embargo, plantear estas consignas políticas a nivel supranacional implica asumir el debate global en términos de modelo económico, de regulación de las tecnologías y de la normatividad sobre el acceso a las mismas. El arduo camino de generar una ciudadanía digital es un proceso inacabado, es decir, siempre estará en continuo desarrollo a medida que los contextos cambian y surgen nuevos escenarios en los cuales se hace necesario cambiar, modificar y generar nueva normatividad. La implementación y asunción de estos desafíos garantizaría, siendo razonables, que la IA se utilice para promover el control fiscal y enfrentar con fuerza los delitos asociados al uso de estas nuevas tecnologías.

Las reflexiones desde el paradigma del determinismo débil sobre el impacto de tecnologías digitales en el control fiscal, evidencian que esta herramienta está teniendo un impacto significativo en la rendición de cuentas de las instituciones, tanto positivo como negativo. Por un lado, la IA está facilitando el acceso al control fiscal al incentivar la participación ciudadana, mejorando la eficiencia de los sistemas judiciales y aumentando la transparencia y la rendición de cuentas. Por otro lado, la IA también está creando nuevos desafíos como la desigualdad digital, la discriminación y el desafío de los conceptos tradicionales de control fiscal y por ende de transparencia.

Los controles institucionales podrían plantearse desde la construcción colectiva de normas y jurisprudencias que, desde una visión antropocéntrica, logren armonizar el rol de estas tecnologías en la vida social y en los desarrollos económicos. Lo que queda claro del debate entre tecno-optimistas y tecno-apocalípticos planteado a lo largo de este capítulo, es que la responsabilidad de las tecnologías y en especial la responsabilidad de las creaciones derivadas de la IA, está en nuestras manos. Y frente a esto no podemos asumir una banalidad tecnológica, por ello, es necesario cerrar este capítulo con el tema de los ciberdelitos.

IV. La ciber-resiliencia y los principios CIA

La ciberseguridad, como campo multidisciplinar, ha evolucionado con el auge de la transformación digital y el aumento de la dependencia tecnológica de las instituciones. Se entiende como el conjunto de prácticas, políticas, herramientas y procedimientos cuyo objetivo es salvaguardar la integridad, confidencialidad y disponibilidad de los sistemas de información ante amenazas internas o externas, deliberadas o accidentales[55]. Esta definición pone en evidencia que la ciberseguridad no es solo un asunto tecnológico, sino que implica una gestión integral del riesgo organizacional. En el ámbito estatal, esta función adquiere una dimensión pública ya que la información custodiada por las entidades del Estado pertenece a los ciudadanos.

Por su parte, la ciberdefensa representa el componente estratégico del Estado frente a amenazas complejas y persistentes que buscan afectar la infraestructura crítica del país. Tal como lo plantea el CONPES 3701, la ciberdefensa busca blindar los sistemas clave para la seguridad nacional –incluidos los sectores energético, financiero, salud, transporte y defensa– mediante acciones preventivas, de monitoreo y respuesta[56]. La diferencia fundamental entre ambos conceptos radica en que la ciberseguridad puede ser gestionada por actores públicos o privados, mientras que la ciberdefensa es competencia exclusiva del aparato estatal.

A su vez, la ciber-resiliencia añade una dimensión adaptativa a la gestión de la seguridad digital. Se trata de la capacidad institucional para prepararse, resistir, recuperarse y evolucionar tras la ocurrencia de un evento cibernético. Esta noción permite que las organizaciones no solo reactiven su funcionamiento luego de un ataque, sino que incorporen el aprendizaje obtenido para mejorar su postura frente a futuras amenazas[57].

---

55 Kaspersky. "¿Qué es la ciberseguridad?", cit.

56 Departamento Nacional de Planeación. *Documento CONPES 3701 "Lineamientos de política para la ciberseguridad y la ciberdefensa"*, cit.

57 Deb Bodeau y Richard Graubart. *Cyber Resiliency and NIST Special Publication*

Por último, los delitos informáticos o ciberdelitos son aquellas conductas delictivas que se cometen a través de medios informáticos o que tienen como objetivo vulnerar sistemas tecnológicos. En Colombia, la Ley 1273 de 2009[58] incorpora al Código Penal un catálogo de delitos como el acceso abusivo a un sistema informático (art. 269A), daño informático (art. 269D), uso de *software* malicioso (art. 269E) y suplantación de sitios web para capturar datos personales (art. 269G). Estos delitos representan amenazas directas al correcto funcionamiento del Estado y sus efectos se traducen en pérdidas económicas, afectación de servicios y deterioro de la confianza institucional.

En el contexto de la ciberseguridad y la vigilancia del gasto público, los principios de Confidencialidad, Integridad y Disponibilidad (CIA por sus siglas en inglés: *Confidentiality, Integrity, Availability*) se constituyen en pilares fundamentales para asegurar la calidad, trazabilidad y protección de la información empleada en los procesos de control fiscal.

Estos principios, ampliamente reconocidos en los estándares internacionales de seguridad de la información (como la norma ISO/IEC 27001[59]), son aplicables de forma transversal a todos los sistemas que soportan la gestión pública digital, y resultan esenciales para el cumplimiento efectivo de los principios misionales del control fiscal en Colombia, conforme a lo establecido en el Decreto 403 de 2020[60].

800-53 Rev.4 Controls, MITRE Technical Report MTR130531, Bedford, MA, The MITRE Corporation, 2013, disponible en [https://www.mitre.org/sites/default/files/publications/13-4047.pdf].

58 Ley 1273 de 5 de enero de 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", *Diario Oficial* n.° 47.223, del 5 de enero de 2009, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699].

59 International Organization for Standardization. *International Standard ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, 3.ª ed., ISO, 2022.

60 Decreto 403 de 16 de marzo de 2020, "Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fis-

La confidencialidad se refiere a la capacidad de garantizar que la información solo esté disponible para aquellas personas que cuenten con la debida autorización de acceso. En el ámbito del control fiscal, este principio cobra especial importancia debido a la naturaleza sensible de los datos que manejan los órganos de control, incluyendo información contable, presupuestal, contractual y de auditoría. La exposición no autorizada de dicha información puede comprometer investigaciones en curso, generar manipulación externa de hallazgos o derivar en acciones de presión sobre funcionarios públicos y contratistas[61].

La Contraloría General de la República –CGR– ha incorporado medidas técnicas y organizativas para garantizar la confidencialidad de sus operaciones digitales, incluyendo sistemas de autenticación robusta, gestión de accesos por perfiles y protocolos de clasificación de la información, conforme a la Política Operacional para la Gestión de la Información DIARI[62]. Este enfoque se articula con el principio de eficiencia del control fiscal, en tanto minimiza los riesgos de fuga o pérdida de datos en el uso de los recursos tecnológicos disponibles.

La integridad, por su parte, se relaciona con la garantía de que la información no ha sido alterada de manera indebida y que se mantiene exacta, coherente y fiable durante todo su ciclo de vida. En el control fiscal, asegurar la integridad de los datos es una condición *sine qua non* para evaluar correctamente la legalidad y eficiencia en el uso de los recursos públicos. Cualquier modificación, voluntaria o accidental, de registros presupuestales, datos de contratación o evidencias digitales, puede derivar en conclusiones erróneas, falsos positivos de detrimento fiscal o la omisión de hallazgos críticos.

---

cal", *Diario Oficial* n.° 51.258, del 16 de marzo de 2020, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=30038961].

61 ISACA. *State of Cybersecurity 2021, Part 1: Global Update on Workforce*, cit.

62 Contraloría General de la República. "Políticas operativas de seguridad de la información en la operación de los procesos Gestión de información y Análisis de información en la DIARI", código: RSC 02 PO 001, Sistema de Gestión y Control Interno –SIGECI–, 29 de junio de 2022.

La CGR ha avanzado en la implementación de mecanismos que aseguran la integridad de los datos mediante registros de auditoría digital, control de versiones, *hash* criptográficos y mecanismos de trazabilidad que permiten reconstruir el historial de cada operación digital relevante para la función de control. Esto fortalece el principio de eficacia, definido en el Decreto 403 de 2020 como la capacidad de lograr los resultados previstos en los procesos de fiscalización[63].

El tercer principio del modelo CIA, la disponibilidad, hace referencia a la posibilidad de acceder a la información y a los sistemas que la gestionan en el momento en que se requiera, sin restricciones indebidas y con tiempos de respuesta adecuados. En el marco del control fiscal, la disponibilidad es crítica para la realización de auditorías en tiempo real, el seguimiento a contratos y la generación de alertas tempranas ante posibles anomalías. La interrupción de servicios, la caída de plataformas o la indisponibilidad de bases de datos puede comprometer el accionar de la CGR, entorpecer la toma de decisiones oportunas o incluso impedir el cumplimiento de su mandato legal.

Para mitigar estos riesgos, la CGR a través de la DIARI, ha implementado políticas de respaldo continuo, sistemas redundantes y planes de continuidad del negocio que permiten garantizar la operación institucional incluso en escenarios de contingencia. Estos elementos refuerzan el principio de economía, el cual exige utilizar los recursos públicos de manera racional y sin derroche al evitar interrupciones costosas o pérdidas de información que podrían tener un impacto económico significativo.

El citado Decreto 403 de 2020 recoge y actualiza los principios orientadores del control fiscal en Colombia, entre los cuales se destacan: eficiencia, eficacia, economía, equidad, valoración de costos ambientales, transparencia, publicidad, responsabilidad y autonomía. Estos principios, al ser aplicados en un entorno digital, requieren de un marco de seguridad robusto que permita su desarrollo

63 Decreto 403 de 2020, "Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal", cit.

armónico con el uso intensivo de tecnologías de la información y la gestión de datos masivos.

- *Eficiencia*: La ciberseguridad reduce los tiempos y recursos necesarios para acceder, procesar y custodiar la información fiscal, mediante automatización, interoperabilidad segura y auditorías asistidas por tecnología.

- *Eficacia*: Se incrementa la capacidad de detectar, documentar y prevenir hechos generadores de daño fiscal, gracias a la disponibilidad y confiabilidad de la información digital.

- *Economía*: Se evitan duplicidades de esfuerzos y pérdidas económicas derivadas de ciberataques o fallos de integridad, mediante controles preventivos y políticas de respaldo eficientes.

- *Equidad*: Se garantiza un tratamiento homogéneo de los sujetos de control al aplicar criterios técnicos estandarizados en el acceso, protección y análisis de la información, sin sesgos ni privilegios indebidos.

- *Transparencia y publicidad*: La gestión segura de los datos permite que la información relevante esté disponible para la ciudadanía y otras entidades de control, sin poner en riesgo la integridad del proceso auditor.

- *Responsabilidad*: Cada funcionario vinculado a los procesos de fiscalización digital debe cumplir protocolos definidos para la gestión de la información, lo cual permite individualizar responsabilidades en caso de negligencia o fraude.

- *Valoración de los costos ambientales*: El uso racional y digitalizado de los recursos informáticos también reduce el uso de papel, transporte y otros insumos físicos, promoviendo un control fiscal sostenible y con menor huella ambiental.

- *Autonomía*: El control fiscal digital exige que la CGR cuente con sistemas propios, talento humano especializado y plataformas seguras que le permitan actuar sin depender tecnológicamente de los sujetos de control o de terceros sin capacidad técnica.

La incorporación de los principios CIA en los procesos de control fiscal ha implicado la actualización de guías, protocolos y metodologías institucionales. La CGR ha trabajado en la formulación de lineamientos que integran estos principios, tanto en las auditorías tradicionales como en los nuevos modelos de fiscalización digital, como las auditorías preventivas, de tecnología, de legalidad algorítmica y de ciber-resiliencia.

Particularmente, las metodologías lideradas por la DIARI incorporan evaluaciones del cumplimiento de estándares de seguridad por parte de los sujetos de control, análisis de riesgos asociados al ecosistema digital y recomendaciones técnicas orientadas a fortalecer la infraestructura de datos de las entidades auditadas. Esto permite que la vigilancia fiscal no solo sancione el mal uso de los recursos, sino que contribuya de forma activa a su protección mediante el fortalecimiento de la seguridad institucional.

A pesar de los avances, existen desafíos persistentes en la implementación plena del modelo CIA en el control fiscal colombiano. Muchas entidades auditadas carecen de planes de continuidad del negocio, no realizan pruebas regulares de restauración de datos y presentan debilidades en la clasificación de la información y en la gestión de incidentes de seguridad digital. Estas falencias incrementan el riesgo de daño fiscal, dificultan la trazabilidad de la información y debilitan la capacidad preventiva de la CGR.

Se recomienda, por tanto, continuar fortaleciendo la cultura de la ciberseguridad en la entidad y en los sujetos de control, actualizar los instrumentos técnicos de auditoría con énfasis en entornos digitales e intensificar la coordinación con entidades especializadas como ColCERT, la Policía Nacional y el MINTIC para garantizar una respuesta integral y articulada ante ciberincidentes.

Capítulo segundo
Brechas institucionales en protección digital

I. Ciberdelitos en el contexto colombiano

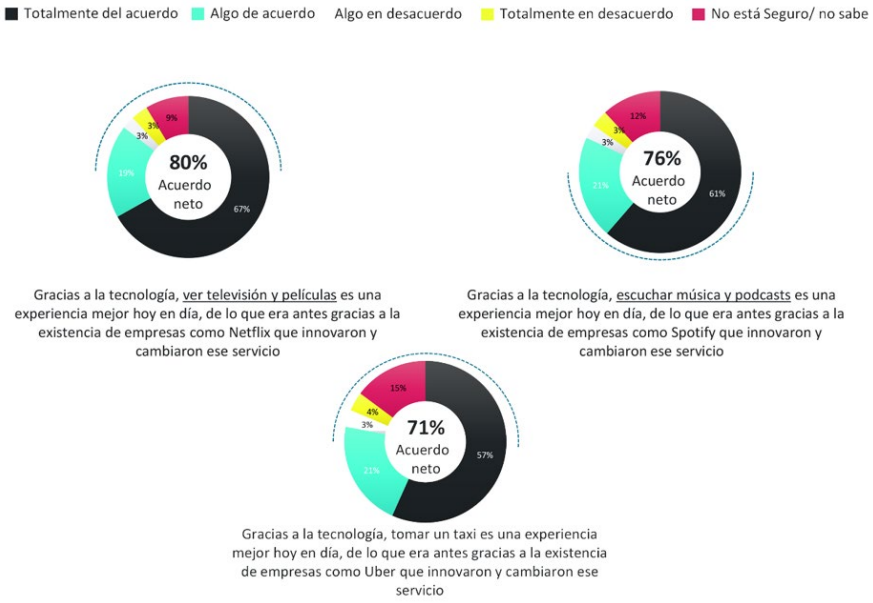
Un breve repaso de información histórica en materia de ciberdelitos en el contexto colombiano permitirá reconocer algunas de las más importantes barreras y retos en materia de ciberseguridad y ciberdefensa que enfrenta el país. Una definición plausible del ciberdelito es la nominación a un conjunto de actos ilegales, es decir, que nos referimos a un conjunto de actos que contravienen el orden legal realizados en el ciberespacio con el uso de tecnologías emergentes, dispositivos digitales y a través del empleo de las redes telemáticas. Van de lo simple a lo complejo, por ejemplo, pasando de las estafas por WhatsApp a ciberataques que colocan en jaque a Estados completos.

Es amplio el panorama, el cual se puede sintetizar a *grosso modo* en estafas y fraudes, el robo de información privada, los ciberataques para pedir dinero por el secuestro de información, el conocido como *phishing* o también entendido como robo de cuentas o de información privada, el *ransomware* que es introducir un virus para posteriormente exigir rescate para recuperar información, cuentas y datos claves, el *ciberbullyng* que es el acoso en línea, el ciberespionaje que implica ingresar a sistemas sin autorización para obtener información privilegiada, y con mucha fuerza creciente, los delitos de robo de identidad.

La firma digital GSE en alianza con la Universidad del Rosario, realizó la que denominó como la primera encuesta sobre seguridad digital en Colombia, y que se aproximó a la comprensión de las percepciones de la ciudadanía en materia de ciberseguridad en Colombia.

La encuesta fue realizada en diez ciudades principales del país, según este informe, con poblaciones desde los 18 años, incluyendo todos los estratos y sexos entre la población participante, los resultados obtenidos permiten entender la forma como las personas configuran realidades en terno a la innovación tecnológica. Al respecto la Gráfica 2 lo precisa:

Gráfico 2
Innovaciones tecnológicas que pueden mejorar la experiencia del usuario

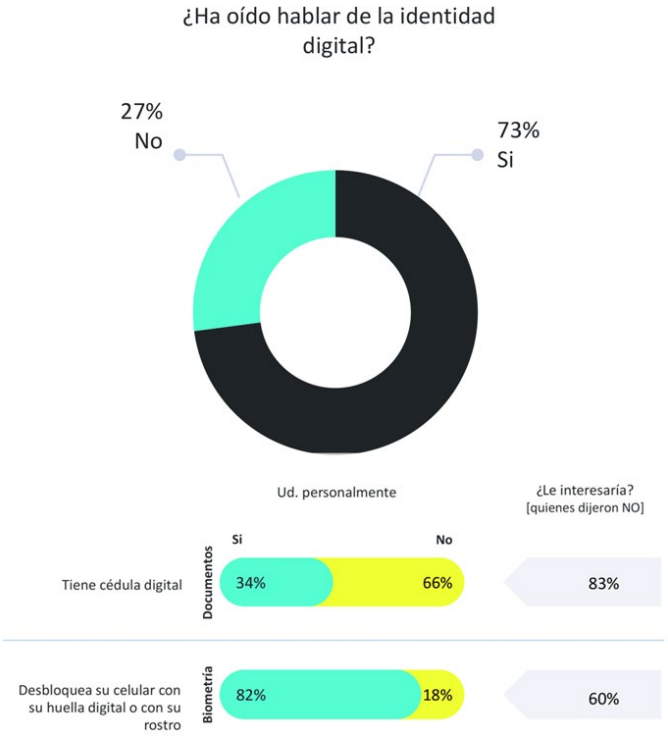


Fuente: GSE. *Primera encuesta sobre seguridad digital en Colombia*, Bogotá, 2025, disponible en [https://urosario.edu.co/sites/default/files/2025-02/estudio-seguridad-digital-infografia.pdf].

El informe deja en evidencia la gran acogida de los sistemas digitales, primordialmente los asociados a entretenimiento, en el público colombiano, donde al menos siete de cada diez personas afirman que la tecnología ha tenido un impacto positivo en su vida. Dentro del mismo informe también se rescata la percepción que

existe frente a la identidad digital, entendida como la forma en que las personas socializan y autoconfiguran realidades subjetivas en torno a su personalidad, gustos, afinidades y cultura, pero también cómo las personas moldean su identidad digital para acceder a los servicios del Estado. Acorde con la Gráfica 3:

Gráfico 3
Hay una actitud positiva hacia la identidad digital



Nota: Datos sobre percepción positiva y asociados.

Fuente: GSE. *Primera encuesta sobre seguridad digital en Colombia*, cit.

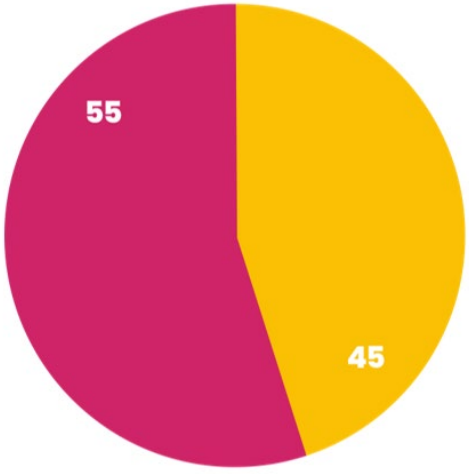
La anterior información evidencia que apenas una tercera parte de la población encuestada usa documento digital, también que el uso del documento de identificación digital aún se encuentra en proceso de expansión, pues de la población que no contaba con el

documento (más del 80%) expresó no estar interesada en el mismo, lo que sugiere la necesidad de implementar estrategias para incentivar su uso. Por otra parte, y en lo que respecta al empleo de tecnología de identificación biométrica, más del 80% de los encuestados afirmó que usa alguna de estas herramientas en su teléfono móvil. Lo anterior permite reconocer que existe una aceptación a la aplicación y uso de herramientas de identificación biométricas, pero que hasta el momento están limitadas al uso de artículos electrónicos personales.

La gráfica que sigue, permite entender la forma como las personas analizan los peligros de los ciberdelitos.

Gráfico 4
Exposición a riesgos digitales

¿Ha sufrido usted de alguna situación de riesgo asociado a su seguridad digital?



Nota: 45 de cada 100 personas mostraron que sí, siendo el robo de RRSS y suplantación de identidad las mas común (45%).

Fuente: GSE. *Primera encuesta sobre seguridad digital en Colombia*, cit.

Según información de esta misma encuesta; 45 de cada 100 colombianos afirmaron haber estado expuesto a alguna situación de riesgo en materia de seguridad digital, siendo el robo de cuentas RRSS el mayor riesgo presentado con un 39%, seguido por la suplantación de identidad con un 31%. Entre las conclusiones del informe se destaca que:

> El estudio muestra que los colombianos no dimensionan adecuadamente los riesgos que hay a nivel de seguridad digital. Los encuestados creen que el 45% de todos los colombianos han sido víctimas de algún delito contra su seguridad digital, pero en realidad el 78% ha sido víctima, sobre todo del robo de cuentas de redes sociales y de la suplantación de identidad. Las personas parecen no saber lo extendidos que están estos problemas. Conocer la magnitud del riesgo puede ser un primer paso para comenzar a trabajar en cómo atacar el problema[64].

Esto, en materia de seguridad digital, deja en evidencia una preocupación de los colombianos en torno al campo de las tecnologías emergentes, seguida de un desconocimiento en el área y que podría estar acompañada de una tendencia creciente de este fenómeno que afecta a muchos más usuarios. Así mismo, estos datos evidencian un breve panorama de la percepción de seguridad digital en el país, que busca entablar un puente entre la percepción del público en materia de seguridad digital y el panorama en el ámbito público y fiscal, sector que también enfrenta importantes retos en materia de seguridad digital y que ha comprobado la aparición de diferentes amenazas en los últimos cinco años.

Según un informe elaborado por TIcTac, el primer *think tank* de análisis y creatividad del sector TIC en Colombia, en el 2022 hubo un significativo aumento en el número de ataques a entidades del Estado en materia de ciberseguridad que dejaron en evidencia algunas de las vulnerabilidades de los sistemas, puesto que: "En el año 2021 se presentaron 41 billones de intentos de ataques cibernéticos en el mundo y siete billones en Colombia"[65].

---

64 GSE. *Primera encuesta sobre seguridad digital en Colombia*, cit., p. 11.

65 EQUIPO TICTAC. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*,

Esta cifra se encuentra asociada a la explotación de las rentas vinculadas a los delitos informáticos, los investigadores precisaron que: "Los ciber-crímenes generan cada vez más rentabilidad para los atacantes y en este sentido, si no existen herramientas para contrarrestarlos y estar protegidos, seguirá creciendo la curva de ciberataques para empresas y entidades de gobierno"[66].

Muy a pesar de los avances normativos y tecnológicos, las entidades públicas colombianas aún enfrentan importantes desafíos en materia de seguridad digital. Solo para el 2021, estos era el panorama que enfrentaban las organizaciones en materia de seguridad digital:

> De acuerdo con el último informe presentado por la Fiscalía General de la Nación, en Colombia en el año 2021 el número de ataques cibernéticos aumentó en un 30%, comparado con el año anterior. Si bien, las compañías y entidades oficiales han venido trabajando fuertemente en estrategias tendientes a robustecer las medidas de ciberseguridad, estas no han sido suficientes, ya que casos como el secuestro de información o la afectación de datos a entidades mediante *ransomware* o ataques de día cero sin filtración de datos, aún continúan presentándose y han ocasionado grandes pérdidas económicas para las organizaciones[67].

Esta situación se da en un contexto de masificación de servicios digitales, impulsados no solo por la aparición de nuevas tecnologías, sino también por fenómenos como el ya precitado confinamiento provocado por la pandemia del COVID-19, que obligó a digitalizar muchos de los procesos que se realizaban por medio de otros sistemas no digitales o que no permitían su operación mediante sistemas digitales automáticos.

Como resultado de ello, varias instituciones públicas se han volcado a la implementación de sistemas digitales complejos que comparten información sensible, personal, financiera y de diferentes índoles. Ya para el 2022, eran reconocidas algunas de las amenazas

---

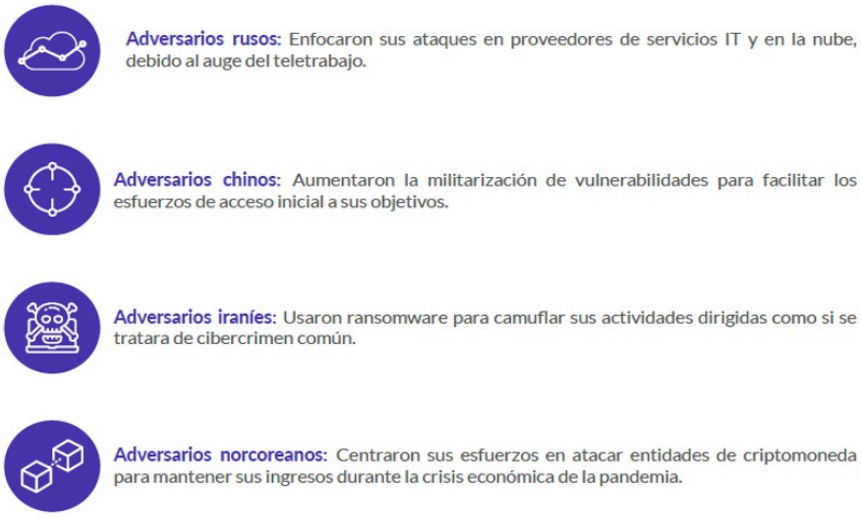
Bogotá, 2022, disponible en [https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf], p. 13.

66 Ídem.

67 Ídem.

consolidadas que las instituciones enfrentaban particularmente en el ámbito internacional. La Gráfica 5 ilustra el panorama global de grupos e individuos y sus estrategias de ataque:

Gráfico 5
Adversarios y estrategias de ataque



Fuente: Equipo TicTac. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*, cit.

Es posible apreciar que se ha consolidado un modelo de amenazas informáticas desde diferentes países que representa un tipo de especialidad específica. Se mencionan los más caracterizados debido al gran volumen de registros de acceso no autorizado y violaciones de seguridad asociadas a estos grupos en específico. Según los informes presentados por la Agencia TicTac en asociación con Crowstrike, los ataques de estos grupos son cada vez más sofisticados, lo que dificulta el trabajo del equipo de seguridad para responder a un posible ataque o violación del sistema de seguridad digital que explote un error del sistema o haya identificado una brecha para introducir y sacar datos del sistema. La gráfica que sigue precisa el tiempo de infiltración en los sistemas digitales:

Gráfico 6
Tiempo de infiltración en sistemas digitales

Fuente: Equipo TicTac. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*, cit.

Colombia no está exenta de este tipo de dinámicas y existe un número significativo de intromisiones y ataques a los sistemas informáticos que han sido previamente documentados. Desde el 2018, las entidades colombianas han sufrido de un significativo número de ataques a diferentes instituciones del Estado, siendo el sector financiero y el petrolero donde con mayor frecuencia se presentan estos ataques[68]. Y es que, aunque no fue hasta después de la pandemia que el número de ataques se incrementó, ya existía información previa de intentos por parte de actores no identificados y diferentes grupos de actores cibercriminales.

> El nivel de criticidad y características de los ataques puede variar, sin embargo, las modalidades más comunes se encuentran asociadas a la infección de *malware* con distintos alcances, sin embargo la motivación es la obtención ilícita de ganancias, bien sea por el robo de credenciales, el secuestro de información (*ransomware*), la exfiltración y fuga de información de credenciales de seguridad con fines de

68 Equipo TicTac. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*, cit.

exposición en internet y la venta de datos en la DarkNet (aunque cada vez es más frecuente la venta de datos en internet superficial)[69].

El robo de credenciales o información de identificación digital es uno de los problemas más comunes dentro de los sistemas digitales. Solo para el 2020 ya se contaba con la identificación de un grupo de ciberatacantes que por medio de un código malicioso recopilaban información de identificación que luego era vendida o intercambiada en foros dentro de la *dark web* (red oscura). Para el 2022 se revela que más de 142.000 sitios se encontraban infectados con este código, lo que supuso la infiltración de información y de datos personales más grande en la corta historia de la internet; 12 millones de credenciales de usuarios afectadas, 49.000 sitios gubernamentales a nivel mundial se encontraban dentro de la lista de sitios infectados. A continuación, algunos de los sitios gubernamentales del país expuestos[70].

Gráfico 7
Sitios gubernamentales colombianos expuestos

Fuente: Equipo TicTac. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*, cit.

69 Ibíd., p. 16.
70 Equipo TicTac. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*, cit.

El informe no solo expone algunas de las problemáticas que se han presentado en entidades estatales en materia de seguridad digital, sino también sugiere algunas prácticas que puedan facilitar la prevención e implementación de acciones que permitan la protección de información sensible para organizaciones públicas y privadas, para la protección de datos y la protección de sistemas de información frente a cualquier vulnerabilidad informática.

Gráfico 8
Habilidades necesarias para la respuesta eficiente a afectaciones de seguridad digital

Fuente: Equipo TicTac. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*, cit.

Por otra parte, existen otros retos que enfrentan las instituciones. Estas brechas se manifiestan en múltiples niveles: estratégico, organizacional, normativo, técnico y cultural. En el plano estratégico, muchas entidades no cuentan con una política institucional de ciberseguridad alineada con su misionalidad. La ausencia de marcos de referencia como el Modelo de Gestión de Seguridad de la Información o su implementación parcial, limita la capacidad de las organizaciones para identificar y gestionar riesgos asociados al entorno digital. En entidades del orden territorial, esta situación

se agrava por restricciones presupuestales y baja priorización de inversiones tecnológicas[71].

Desde la perspectiva organizacional, una de las principales brechas radica en la escasez de talento humano especializado. Aunque Colombia ha desarrollado iniciativas como el Plan Nacional de Talento Digital y la Estrategia Nacional Digital 2023-2026, la oferta formativa en ciberseguridad sigue siendo limitada frente a la demanda del sector público. La alta rotación de personal y la dependencia de contratistas externos, dificultan la consolidación de equipos técnicos estables y comprometidos con una visión de largo plazo[72].

A nivel normativo, si bien existen leyes y directrices, persiste una fragmentación regulatoria que impide su aplicabilidad homogénea. Por ejemplo, no todas las entidades están obligadas a cumplir con estándares como la norma ISO/IEC 27001. Además, los marcos de auditoría interna pocas veces incluyen la verificación de controles de ciberseguridad, lo cual representa un vacío en la gobernanza institucional.

En la misma orientación, la Estrategia Nacional Digital de Colombia 2023-2026 –END– se constituye en una hoja de ruta que articula las acciones del Gobierno nacional para avanzar hacia la transformación digital del país. Este documento establece ocho ejes estratégicos orientados a fomentar la conectividad, el uso y apropiación de los datos, el fortalecimiento de la seguridad digital, el desarrollo del talento y las habilidades digitales, la incorporación de tecnologías emergentes como la inteligencia artificial, la transformación digital del sector público, el impulso a la economía digital y la consolidación de una sociedad digital más inclusiva y sostenible.

La estrategia parte de reconocer el acceso y uso de las tecnologías digitales como un derecho y no un privilegio, y propone cerrar las brechas existentes entre zonas rurales y urbanas y entre distin-

---

71 Organización para la Cooperación y el Desarrollo Económicos. *Revisión del gobierno digital en Colombia: hacia un sector público impulsado por el ciudadano*, París, OCDE, 2018, disponible en [https://www.oecd.org/es/publications/revision-del-gobierno-digital-en-colombia_9789264292147-es.html].

72 Cano M. "De los incidentes de seguridad en la gestión de la protección de datos personales y la Industria 4.0", cit.

tos grupos poblacionales. Se fundamenta en la articulación entre entidades del Estado, el sector privado, la academia y la ciudadanía y plantea un modelo de gobernanza interinstitucional para hacer seguimiento a su implementación. La END 2023-2026 busca desencadenar el potencial de la digitalización para responder a desafíos económicos, sociales y ambientales, alineándose con los objetivos del Plan Nacional de Desarrollo 2022-2026 "Colombia, potencia mundial de la vida".

La END 2023-2026 reconoce a la *seguridad y confianza digital* como un eje fundamental para la garantía de las libertades y el desarrollo integral de las personas. Parte de la preocupación por el aumento de los ataques cibernéticos en el país, destacando el crecimiento del *malware*, los delitos informáticos y la baja preparación institucional y ciudadana frente a las amenazas digitales. En respuesta, propone fortalecer las capacidades tecnológicas del Estado, establecer un marco normativo robusto, desarrollar una cultura de hábitos seguros y crear una entidad nacional encargada de coordinar las acciones en esta materia.

La estrategia promueve el desarrollo de capacidades de *ciberresiliencia*, la creación de un *observatorio de ciberseguridad*, el fortalecimiento del COLCERT (equipo de respuesta ante incidentes del Estado) y la formación especializada de líderes públicos y privados en ciberseguridad. También resalta la importancia de establecer principios como la *seguridad digital por defecto*, la protección de infraestructuras críticas cibernéticas y el respeto por los derechos digitales de los ciudadanos. En conjunto, estos elementos constituyen un enfoque integral que sitúa la ciberseguridad como una condición habilitante para la transformación digital del país.

Como se puede observar, en lo técnico, las entidades enfrentan limitaciones en la interoperabilidad de sus sistemas. La fragmentación de plataformas, la falta de estandarización en los reportes fiscales y la escasa automatización en los flujos de información limitan la posibilidad de implementar auditorías digitales.

Durante el periodo entre junio de 2023 a mayo de 2024, la Contraloría General de la República avanzó significativamente en mate-

ria de ciberseguridad y gestión de la seguridad de la información. Implementó un Sistema de Gestión de Seguridad –SGS– y un Sistema Integral de Seguridad –GIS– como parte de su arquitectura tecnológica, los cuales fortalecen la protección frente a amenazas digitales. Además, se desarrollaron procesos de gestión de crisis, continuidad y emergencias, integrando capacidades para mitigar riesgos tecnológicos y responder a eventos críticos. La entidad también consolidó su plataforma de integración tecnológica, mejorando el gobierno de TI y elevando los estándares de ciberprotección institucional[73].

La DIARI, pese a sus avances, requiere datos de calidad y en tiempo real para que sus herramientas predictivas y de análisis puedan operar con eficacia[74]. Para lograrlo, es indispensable contar con un gobierno de datos que asegure la confidencialidad, integridad y disponibilidad de la información, pilares que sustentan las políticas operativas de seguridad implementadas por esta dirección. Dichas políticas, estructuradas conforme a estándares internacionales como la ISO/IEC 27001, incluyen la clasificación de activos de información, el uso de controles criptográficos, la gestión de incidentes, la protección frente a amenazas físicas y cibernéticas y el control riguroso del acceso físico y lógico a los sistemas. Así mismo, la DIARI promueve una cultura organizacional de seguridad y una arquitectura de defensa en profundidad, que abarca desde la gestión de usuarios hasta la continuidad del negocio y la protección en entornos de trabajo móvil y en la nube[75].

En cuanto a la dimensión cultural, muchas entidades aún no han interiorizado la ciberseguridad como una responsabilidad colectiva. El personal desconoce los riesgos asociados a malas prácticas digitales como compartir contraseñas, usar dispositivos no autorizados o conectarse a redes inseguras. La falta de capacitaciones

---

73 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

74 Contraloría General de la República. "Políticas operativas de seguridad de la información en la operación de los procesos Gestión de información y Análisis de información en la DIARI", cit.

75 Ídem.

continuas, campañas de sensibilización y simulacros de respuesta a incidentes, contribuye a mantener una postura reactiva y frágil ante las amenazas emergentes.

Superar estas brechas implica un compromiso articulado del Gobierno nacional, los órganos de control, las entidades territoriales y la sociedad civil. La consolidación de una política nacional de ciberseguridad con enfoque sectorial, el fortalecimiento del marco institucional de la DIARI, la capacitación de servidores públicos y la inversión en infraestructura tecnológica son acciones prioritarias para garantizar que la información fiscal esté protegida frente a los desafíos del siglo XXI. Ahora veamos la estructura normativa colombiana.

II. Marco normativo y político colombiano

El marco normativo y político colombiano en materia de ciberseguridad y su relación con el control fiscal, ha evolucionado gradualmente en las últimas dos décadas en respuesta a la creciente sofisticación de las amenazas digitales que afectan tanto al sector privado como a la gestión pública. El marco normativo colombiano en materia de ciberseguridad se ha construido a partir de una serie de disposiciones legales que buscan enfrentar los desafíos del entorno digital mediante la regulación del uso y protección de la información, así como la prevención de delitos informáticos.

Entre las principales normas se encuentra la Ley 1273 de 2009[76], que modificó el Código Penal para tipificar conductas delictivas relacionadas con el acceso y manipulación indebida de sistemas informáticos; la Ley 1581 de 2012[77], que establece el régimen de

76 Ley 1273 de 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", cit.

77 Ley 1581 de 17 de octubre de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", *Diario Oficial* n.° 48.587, del 18 de octubre de 2012, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507].

protección de datos personales; la Ley 1621 de 2013[78], que regula las actividades de inteligencia y contrainteligencia del Estado en el marco del respeto por los derechos fundamentales; y el Decreto 2037 de 2019[79], que formaliza la creación de la Dirección de Información, Análisis y Reacción Inmediata –DIARI– como una instancia especializada en control fiscal digital dentro de la Contraloría General de la República.

Estas normas se complementan con documentos estratégicos como el CONPES 3701 de 2011[80] y la Estrategia Nacional Digital[81], que orientan la acción institucional hacia la protección de las infraestructuras críticas del Estado, el fortalecimiento de capacidades institucionales y la coordinación intersectorial para garantizar la seguridad del ciberespacio en el ámbito público.

78 Ley 1621 de 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", *Diario Oficial* n.° 48.764, del 17 de abril de 2013, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685400].

79 Decreto 2037 de 2019, "Por el cual se desarrolla la estructura de la Contraloría General de la República, se crea la Dirección de Información, Análisis y Reacción Inmediata y otras dependencias requeridas para el funcionamiento de la Entidad", cit.

80 Departamento Nacional de Planeación. *Documento CONPES 3701 "Lineamientos de política para la ciberseguridad y la ciberdefensa"*, cit.

81 Departamento Nacional de Planeación. *Estrategia Nacional Digital de Colombia 2023 - 2026*, Bogotá, DNP, s. f., disponible en [https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/EVENTOS/END_Colombia_2023_2026.pdf].

Gráfico 9
Línea de tiempo Estrategia Nacional de Ciberseguridad

Fuente: elaboración propia.

En el mismo sentido, el marco político colombiano en materia de ciberseguridad se ha estructurado a través de políticas públicas y estrategias nacionales orientadas a fortalecer la resiliencia digital del Estado, garantizar la protección de infraestructuras críticas y promover una cultura institucional de prevención frente a riesgos cibernéticos. El referenciado Documento CONPES 3701 de 2011 marcó un hito al establecer los lineamientos de la política de ciberseguridad y ciberdefensa del país, identificando debilidades en la coordinación institucional, la formación especializada y la regulación normativa.

A esta política se suman la Estrategia Nacional Digital de Colombia 2023 - 2026, liderada por el Ministerio de Tecnologías de la Información y Comunicaciones –MINTIC–, que plantea acciones

integradas en cinco ejes estratégicos para la protección del ciberespacio colombiano; la creación y operación del Grupo de Respuesta a Emergencias Cibernéticas –ColCERT– como centro técnico para la gestión de incidentes a nivel nacional; y las acciones complementarias de entidades como la Policía Nacional, la Fiscalía General de la Nación, el Ejército y los órganos de control. Este marco político evidencia un enfoque integral y multisectorial que busca articular capacidades estatales para enfrentar los desafíos de la ciberseguridad en el ámbito del control fiscal, la protección de los recursos públicos y la gobernanza digital.

A. Ley 1273 de 2009: delitos informáticos y su impacto en la gestión pública

La Ley 1273 de 2009 representa un hito normativo en Colombia, al introducir al Código Penal un nuevo bien jurídico tutelado: la protección de la información y de los datos. Esta ley surgió como respuesta a la creciente necesidad de enfrentar penalmente conductas delictivas cometidas a través de medios electrónicos que hasta entonces no estaban suficientemente tipificadas. Con la inclusión de los artículos 269A a 269J, el legislador colombiano abordó fenómenos como el acceso abusivo a sistemas informáticos, el daño informático, el uso de *software* malicioso, el hurto por medios informáticos y la suplantación digital[82].

Desde la perspectiva del control fiscal, esta ley proporciona herramientas jurídicas para sancionar a quienes vulneren los sistemas tecnológicos de entidades públicas, en particular aquellos que manejan información financiera, contable o contractual. Además, permite judicializar a quienes interfieran en procesos de auditoría mediante alteración, sabotaje o sustracción de datos. La DIARI, en tanto instancia especializada dentro de la Contraloría General de

82 Ley 1273 de 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", cit.

la República, se apoya en esta ley para elevar alertas y establecer líneas de colaboración con la Fiscalía General de la Nación cuando detecta incidentes que podrían constituir conductas punibles.

B. CONPES 3701 de 2011: lineamientos de política para la ciberseguridad y la ciberdefensa

El Documento CONPES 3701 de 2011 traza los lineamientos generales de la política pública colombiana en materia de ciberseguridad y ciberdefensa. Elaborado por el Departamento Nacional de Planeación, este documento identificó tres grandes problemáticas estructurales: i) la falta de coordinación nacional para operaciones de ciberseguridad; ii) la limitada formación especializada en el área; y iii) la debilidad regulatoria en la protección de los datos[83].

El CONPES define responsabilidades diferenciadas entre actores como el Ministerio de Defensa, el MINTIC, la Policía Nacional y el sector privado, reconociendo que la ciberseguridad requiere un enfoque integral, multi-actor y multi-sectorial. Su adopción marcó el inicio de una estrategia nacional para mitigar riesgos en el ciberespacio y motivó la creación de iniciativas como el Grupo de Respuesta a Emergencias Cibernéticas de Colombia –ColCERT–, responsable de coordinar la gestión de incidentes a nivel nacional.

En el marco del control fiscal, este documento permite a la CGR enmarcar sus desarrollos institucionales, como la DIARI, dentro de una política estatal más amplia. La interoperabilidad de sistemas, la protección de los datos fiscales y la articulación con plataformas de vigilancia digital se derivan de las recomendaciones y principios allí contenidos.

---

83 DEPARTAMENTO NACIONAL DE PLANEACIÓN. *Documento CONPES 3701 "Lineamientos de política para la ciberseguridad y la ciberdefensa"*, cit.

C. Ley 1621 de 2013 de inteligencia y contrainteligencia: límites y garantías en la recolección de información

La Ley 1621 de 2013, conocida como la Ley de inteligencia y contrainteligencia, regula las actividades de obtención, procesamiento, análisis y difusión de información estratégica para la defensa y seguridad nacional. Aunque su objetivo principal no es el control fiscal, esta norma es relevante en tanto establece los límites legales y las garantías institucionales en el tratamiento de datos sensibles por parte del Estado[84].

Para efectos de la vigilancia fiscal, esta ley delimita el acceso a fuentes de información que pueden ser útiles en auditorías estratégicas relacionadas con seguridad nacional, compras militares o contrataciones reservadas. Así mismo, establece mecanismos de rendición de cuentas ante la Comisión Legal de Seguimiento a las Actividades de Inteligencia, lo que obliga a que cualquier cruce de información con la CGR se realice dentro de los marcos legales establecidos.

De forma complementaria, esta ley reconoce el principio de legalidad y la reserva legal en la recolección y uso de datos, lo cual impone a los órganos de control la necesidad de ajustar sus metodologías de auditoría tecnológica conforme a protocolos establecidos y con respeto por los derechos fundamentales.

D. Estrategia Nacional de Ciberseguridad 2020-2025

La Estrategia Nacional Digital de Colombia 2023-2026 –END–[85] establece un marco integral para consolidar el desarrollo digital del país, abordando la ciberseguridad como uno de los pilares fundamentales. En el eje estratégico de *seguridad y confianza digital*, la

---

84 Ley 1621 de 2013, "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", cit.

85 Departamento Nacional de Planeación. *Estrategia Nacional Digital de Colombia 2023 - 2026*, cit.

END plantea fortalecer las capacidades institucionales, normativas y tecnológicas del Estado para enfrentar el aumento de los ciberataques, en especial aquellos dirigidos a entidades públicas y ciudadanos. Reconoce la necesidad de mejorar los hábitos digitales de la población, el rezago en medidas organizativas e infraestructurales y la dispersión institucional en el liderazgo de la ciberseguridad. Entre sus acciones clave, se incluye la creación de una entidad nacional que articule y coordine la seguridad digital, el fortalecimiento del ColCERT y el establecimiento de un marco legal actualizado para responder a los riesgos digitales emergentes.

Sin embargo, la estrategia también evidencia múltiples retos críticos para Colombia en este campo. Entre ellos, se encuentran la débil infraestructura institucional para liderar y coordinar la seguridad digital, la baja adopción de estándares técnicos de protección en entidades públicas, el limitado conocimiento ciudadano sobre ciberseguridad y la falta de una legislación unificada y robusta sobre el ecosistema digital. Así mismo, se señala que Colombia se encuentra entre los países más expuestos a ciberataques en América Latina, con un incremento significativo en delitos informáticos denunciados y una creciente sofisticación del *malware* utilizado en contra de organismos estatales.

En consecuencia, la END 2023-2026 hace un llamado urgente a la formulación de políticas públicas integradas que articulen la ciberseguridad con la gobernanza digital, el control fiscal y la protección de derechos fundamentales. El documento propone crear capacidades de resiliencia cibernética, fomentar la formación de talento humano especializado y diseñar una estrategia de protección de infraestructuras críticas digitales. Estos desafíos requieren no solo voluntad política, sino también una inversión sostenida y una coordinación eficaz entre entidades del Estado, el sector privado y la sociedad civil.

Sobre el particular, se resalta la importancia del control fiscal en la protección del ecosistema digital del Estado, subrayando el papel clave de la Contraloría General de la República –CGR– y, en particular, de su Dirección de Información, Análisis y Reacción Inmediata –DIARI–. En un contexto en el que los ciberataques a entidades pú-

blicas se han incrementado en número y complejidad, el control fiscal debe incorporar capacidades tecnológicas de monitoreo y prevención, como las que ejerce la DIARI mediante el análisis masivo de datos, la generación de alertas tempranas y la evaluación de riesgos fiscales derivados de vulnerabilidades digitales.

En línea con esta necesidad, la encuesta y diagnóstico incluidos en la END revelan una débil adopción de políticas de ciberseguridad en muchas entidades públicas, lo que amplía la exposición al daño patrimonial y dificulta la trazabilidad de los recursos. Frente a este panorama, las funciones de la DIARI cobran una relevancia estratégica ya que su labor de vigilancia digital en tiempo real permite detectar desviaciones en el uso de recursos públicos, establecer correlaciones entre brechas tecnológicas y posibles riesgos de corrupción y orientar la priorización de auditorías sobre sectores más vulnerables del ecosistema estatal. Así, la DIARI se posiciona como un nodo de control fiscal preventivo y tecnológicamente adaptado al entorno digital descrito por la Estrategia.

E. Normas específicas del control fiscal digital y de vigilancia tecnológica

La evolución normativa en el ámbito del control fiscal ha llevado a la incorporación de herramientas digitales como parte integral del ejercicio auditor. La Ley 42 de 1993, aunque anterior al auge digital, estableció las bases para la vigilancia fiscal a través del principio de eficacia, eficiencia y economía, que hoy se reinterpreta bajo el prisma de la digitalización[86].

86 Ley 42 de 26 de enero de 1993, "Sobre la organización del sistema de control fiscal financiero y los organismos que lo ejercen", *Diario Oficial* n.° 40.732, del 27 de enero de 1993, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=1788293].

Más recientemente, las Leyes 1474 de 2011[87] y 2195 de 2022[88] han reforzado los mecanismos de control interno, transparencia y seguimiento a los recursos públicos, promoviendo el uso de plataformas de información que permiten una supervisión más efectiva. Estas leyes se han complementado con los planes estratégicos de la CGR, que han impulsado el desarrollo de sistemas y la incorporación de inteligencia artificial para identificar alertas tempranas.

En este contexto, la vigilancia tecnológica se convierte en una dimensión estratégica del control fiscal. La CGR ha formulado metodologías específicas para auditar los sistemas de información de los sujetos vigilados, establecer pruebas de integridad sobre bases de datos y evaluar los niveles de ciberseguridad institucional. Estas acciones no solo previenen el uso inadecuado de los recursos, sino que también fortalecen la trazabilidad, la rendición de cuentas y la protección del patrimonio público. La normatividad específica también contempla guías y procedimientos que exigen el uso de sistemas seguros, protocolos de respaldo, mecanismos de autenticación y registros de trazabilidad como parte de los controles mínimos exigibles.

La Contraloría General de la República de Colombia, y en particular su Dirección de Información, Análisis y Reacción Inmediata –DIARI–, ha avanzado en la consolidación de un modelo de gestión de la información que incorpora controles mínimos esenciales para garantizar la ciberseguridad en el ejercicio del control fiscal. Entre estos avances, se destaca la implementación de mecanismos técnicos y organizativos orientados a establecer sistemas seguros, protocolos de respaldo, mecanismos de autenticación y trazabili-

87 Ley 1474 de 12 de julio de 2011, "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública", *Diario Oficial* n.° 48.128, del 12 de julio de 2011, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=1681594].

88 Ley 2195 de 18 de enero de 2022, "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones", *Diario Oficial* n.° 51.921, del 18 de enero de 2022, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043772].

dad documental, alineados con estándares internacionales como la norma ISO/IEC 27001[89].

En materia de seguridad tecnológica, la DIARI ha adoptado políticas sólidas de respaldo de información con sistemas que permiten la generación periódica de copias de seguridad, almacenamiento en medios cifrados y prácticas de recuperación ante desastres, lo cual asegura la continuidad operativa de sus procesos críticos. Esta capacidad se complementa con mecanismos de autenticación robusta, incluyendo autenticación multifactorial, segmentación de privilegios por roles y el principio de mínimo acceso necesario.

Además, la gestión de accesos a la infraestructura tecnológica institucional contempla controles tanto físicos como lógicos, regulando el uso de dispositivos externos y el acceso remoto y aplicando monitoreo constante de los intentos de ingreso no autorizado[90].

Así mismo, la DIARI ha establecido sistemas de trazabilidad que permiten registrar en detalle quién accede a la información, desde dónde, a qué hora y con qué tipo de operación, garantizando así la posibilidad de auditorías internas y análisis forenses en caso de incidentes. Este sistema de seguimiento se articula con políticas de clasificación de la información, control de versiones, uso de medios criptográficos para proteger la integridad y confidencialidad de los datos y protocolos diferenciados para el almacenamiento, procesamiento y destrucción de archivos sensibles[91]. Tales controles no solo permiten garantizar la seguridad de la información, sino también fortalecer la cadena de custodia y la legalidad de las actuaciones de fiscalización.

En paralelo, estos elementos técnicos se complementan con un entorno organizacional que promueve la cultura de la seguridad

---

89 International Organization for Standardization. *International Standard ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, cit.

90 Contraloría General de la República. *Resultados del Sistema SAGA y control fiscal en tiempo real*, Bogotá, CGR, 2022.

91 Contraloría General de la República. "Políticas operativas de seguridad de la información en la operación de los procesos Gestión de información y Análisis de información en la DIARI", cit.

digital. La DIARI ha adoptado cláusulas de confidencialidad obligatorias para su personal, protocolos de acceso a la información con base en perfiles específicos, formación continua en buenas prácticas de ciberseguridad y evaluación periódica del cumplimiento normativo mediante auditorías internas. Todo ello se encuentra enmarcado en una política operativa institucional respaldada por la Unidad del Sistema de Administración de Tecnologías de Información –USATI–, conforme a lo estipulado en las referenciadas Leyes 1581 de 2012 sobre protección de datos personales y 1273 de 2009 sobre delitos informáticos[92].

Estos esfuerzos han generado resultados tangibles. De acuerdo con el informe de gestión 2023-2024, la DIARI lideró acciones de seguimiento fiscal por un valor de $3,9 billones de pesos con beneficios de control que superaron los $961.000 millones, lo cual demuestra que el uso de tecnologías seguras, combinadas con herramientas de análisis de datos y vigilancia en tiempo real, se traduce en impactos concretos en la protección de los recursos públicos. Este modelo de gestión digital, respaldado por prácticas sólidas de ciberseguridad, posiciona a la DIARI como un referente técnico en el fortalecimiento del control fiscal adaptado a las exigencias del entorno digital contemporáneo.

III. La Dirección de Información, Análisis y Reacción Inmediata

La Dirección de Información, Análisis y Reacción Inmediata –DIARI– fue creada mediante el Decreto 2037 de 2019, expedido por la Presidencia de la República de Colombia en ejercicio de sus funciones constitucionales. Esta dependencia se estructuró dentro del nuevo modelo organizacional de la Contraloría General de la República –CGR–, como parte de una estrategia institucional para

92 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

responder a las necesidades de vigilancia fiscal en tiempo real y fortalecer las capacidades de auditoría tecnológica[93].

Según el Decreto 2037 de 2019, la DIARI tiene como misión diseñar e implementar mecanismos para la recolección, sistematización, monitoreo y análisis de información fiscal, financiera y operativa de los sujetos de control fiscal. Su principal objetivo es detectar en tiempo real presuntos actos de corrupción, riesgos fiscales y alertas sobre el uso inadecuado de los recursos públicos. La creación de esta dirección respondió a la necesidad de una entidad con funciones permanentes de inteligencia institucional orientada al control fiscal preventivo, oportuno y eficiente[94].

La DIARI actúa como un nodo de articulación entre la tecnología, la analítica avanzada y la reacción institucional, permitiendo que los hallazgos fiscales no solo sean identificados de manera retrospectiva –como tradicionalmente ha ocurrido– sino también anticipados a través de la minería de datos y el monitoreo en línea de operaciones presupuestales, contractuales y contables en todo el país.

La DIARI se encarga de liderar procesos estratégicos relacionados con el análisis de datos, la generación de alertas, el seguimiento a operaciones fiscales, la reacción ante ciberincidentes y la coordinación con otras dependencias de la CGR. Estos procesos se articulan en un marco metodológico basado en tres componentes clave: prevención, vigilancia y respuesta.

El Decreto 2037 de 2019, mediante el cual se reestructura la Contraloría General de la República, crea la Dirección de Información, Análisis y Reacción Inmediata –DIARI– como parte del proceso de modernización institucional que buscaba adecuar la vigilancia fiscal a los retos del entorno digital y los nuevos riesgos derivados del manejo masivo de información pública. Esta dirección se con-

---

93 Decreto 2037 de 2019, "Por el cual se desarrolla la estructura de la Contraloría General de la República, se crea la Dirección de Información, Análisis y Reacción Inmediata y otras dependencias requeridas para el funcionamiento de la Entidad", cit.

94 Contraloría General de la República. *Informe de gestión 2020-2021 al Congreso y al Presidente de la República "Una Contraloría para todos"*, Bogotá, CGR, 2021, disponible en [https://www.camara.gov.co/sites/default/files/2021-08/5.1%20Informe.pdf].

cibe como una unidad especializada y de carácter transversal, encargada de liderar procesos estratégicos orientados al análisis de datos, la generación de alertas, el monitoreo del gasto público y la coordinación de respuestas institucionales ante posibles hallazgos o riesgos fiscales inminentes.

Su operación se articula bajo un enfoque metodológico basado en tres pilares complementarios: prevención, vigilancia y respuesta[95]. Desde esta perspectiva, la DIARI estructura sus funciones a través de tres unidades técnicas interrelacionadas: la Unidad de Análisis, la Unidad de Información y la Unidad de Reacción Inmediata.

La *Unidad de Análisis* tiene como principal responsabilidad transformar los datos disponibles en información fiscal útil para la toma de decisiones. Esta unidad desarrolla modelos predictivos de riesgo, define perfiles de comportamiento atípico en el uso de los recursos públicos, elabora tableros de control sectoriales y territoriales y formula alertas tempranas que orientan las auditorías programadas o la priorización de ejercicios de vigilancia y control. Su enfoque está centrado en la explotación de herramientas de analítica avanzada, inteligencia artificial y *big data*, así como en la consolidación de criterios técnicos para la clasificación del riesgo fiscal y el comportamiento presupuestal de los sujetos de control.

La *Unidad de Información*, por su parte, garantiza la confiabilidad, seguridad y trazabilidad de la información que alimenta los sistemas de análisis y reacción de la DIARI. Esta unidad lidera los procesos de interoperabilidad con otras entidades del Estado –como el DNP, el SECOP, el SIIF Nación, el SGR, entre otros– y administra las bases de datos institucionales asegurando la calidad de los registros, su actualización oportuna, su respaldo y su acceso bajo criterios de confidencialidad y control de privilegios. También tiene a su cargo el diseño e implementación de políticas de gobierno de datos, la

95 Decreto 2037 de 2019, "Por el cual se desarrolla la estructura de la Contraloría General de la República, se crea la Dirección de Información, Análisis y Reacción Inmediata y otras dependencias requeridas para el funcionamiento de la Entidad", cit.

gestión documental digital y la adopción de protocolos de ciberseguridad orientados a prevenir vulnerabilidades tecnológicas o manipulaciones indebidas de la información.

La *Unidad de Reacción Inmediata*, cuya función esencial es coordinar y ejecutar acciones institucionales de respuesta rápida frente a eventos que representen un riesgo fiscal inminente o que ameriten intervención inmediata por parte de la Contraloría General de la Republica. Esta unidad actúa sobre la base de las alertas generadas por la Unidad de Análisis o por insumos de otras direcciones, así como por denuncias ciudadanas, reportes de prensa, anomalías en los sistemas transaccionales o solicitudes urgentes de otras entidades del Estado.

Su papel es estratégico en la articulación con los equipos de auditoría, las delegadas sectoriales, las gerencias departamentales y, en los casos de mayor complejidad, con entidades como la Fiscalía General de la Nación, la Policía Nacional y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia –ColCERT–, en especial cuando los hechos analizados tienen origen en posibles ciberincidentes o uso indebido de plataformas digitales.

Estas tres unidades, al operar de forma integrada, permiten que la DIARI se convierta en un verdadero centro de inteligencia fiscal con capacidad para prevenir hechos de corrupción, reducir los tiempos de respuesta institucional y anticipar riesgos asociados a la ejecución de recursos públicos. De hecho, su modelo de trabajo ha permitido la implementación de herramientas para fortalecer la capacidad institucional en el ejercicio de un control fiscal más eficiente, selectivo y basado en evidencia.

En suma, la DIARI no solo representa una innovación organizacional, sino que materializa una nueva forma de hacer control fiscal, anclada en el uso intensivo de la información, la capacidad de respuesta y la integración interinstitucional. El citado Decreto 2037 de 2019, al asignarle esta estructura funcional, permitió a la Contraloría General de la República avanzar hacia un modelo de vigilancia fiscal proactivo, más acorde con los desafíos del siglo XXI, en los que el uso estratégico de los datos y la anticipación del riesgo son claves para proteger el patrimonio público.

A partir del análisis del citado Decreto 2037 y de la estructura operativa de la Dirección de Información, Análisis y Reacción Inmediata –DIARI–, se evidencia que la Contraloría General de la República ha consolidado una apuesta institucional coherente con los desafíos contemporáneos de la ciberseguridad aplicada al control fiscal.

La DIARI representa una innovación organizacional que trasciende el modelo tradicional de auditoría postfactual, al incorporar capacidades de análisis predictivo, monitoreo permanente de operaciones fiscales y mecanismos de reacción oportuna ante eventos que amenacen la integridad del gasto público. Aunque no reemplaza a los organismos especializados en ciberdefensa como ColCERT o la Policía Nacional, su capacidad para identificar vulnerabilidades tecnológicas en los sistemas de información de los sujetos vigilados resulta determinante.

En tales casos, la DIARI actúa como primer nodo de alerta, articulando respuestas con las áreas técnicas de la CGR, elaborando informes especializados y canalizando los hallazgos hacia instancias competentes para su investigación o judicialización[96]. Esta función de vigilancia y coordinación ante ciberincidentes fortalece el blindaje institucional del control fiscal, al integrar principios de ciberseguridad como la prevención, la resiliencia operativa y la trazabilidad digital en los procesos de fiscalización.

En este sentido, la DIARI no solo aporta al cumplimiento misional de la Contraloría, sino que también se erige como una instancia de inteligencia fiscal adaptativa, capaz de actuar frente a riesgos complejos del entorno digital. Su consolidación como nodo técnico y estratégico de vigilancia digital reafirma la necesidad de políticas públicas que articulen la seguridad digital con la transparencia fiscal y la protección efectiva del patrimonio público, en un contexto donde las amenazas informáticas son crecientemente sofisticadas y de alto impacto institucional.

---

96 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

IV. Herramientas de inteligencia fiscal y monitoreo automatizado

La Dirección de Información, Análisis y Reacción Inmediata –DIARI– de la Contraloría General de la República ha desempeñado un papel determinante en el proceso de modernización del control fiscal en Colombia, particularmente en el fortalecimiento de capacidades técnicas, analíticas y reactivas que permiten anticipar, mitigar y responder a riesgos fiscales asociados a la gestión pública.

Así lo evidencia el informe de gestión 2023-2024, en el cual se evidencia que la DIARI ha consolidado su posicionamiento institucional mediante intervenciones estratégicas que articulan herramientas tecnológicas emergentes, modelos analíticos predictivos y un sistema de monitoreo en tiempo real para proteger el patrimonio público, en especial en sectores y territorios de alta vulnerabilidad[97].

Uno de los ámbitos donde la DIARI ha mostrado mayor impacto, es en el seguimiento y control a los recursos del Sistema General de Regalías. Entre junio de 2023 y mayo de 2024, la Dirección participó activamente en la identificación de 84 alertas relacionadas con presuntos riesgos de pérdida o uso inadecuado de recursos públicos. Estas alertas se fundamentaron en análisis de patrones de ejecución presupuestal, desempeño físico-financiero de los proyectos y factores de gobernanza territorial, y fueron determinantes para incorporar cinco proyectos por más de 24.000 millones de pesos al Plan Nacional de Vigilancia y Control Fiscal 2024.

Las alertas generadas se canalizaron tanto a auditorías programadas como a mesas armónicas lideradas por la DIARI con el Departamento Nacional de Planeación –DNP– y la Procuraduría General de la Nación –PGN–, fortaleciendo así una estrategia de acción conjunta frente a potenciales focos de corrupción[98]. A través del instrumento denominado "seguimiento permanente", la DIARI llevó

97 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

98 Ídem.

a cabo 198 intervenciones estratégicas durante el período de análisis, que abarcaron un total de $7.327.216 millones de pesos.

Estos seguimientos implican una vigilancia continua a proyectos públicos con alto riesgo fiscal, utilizando herramientas de visualización, monitoreo automatizado y análisis de riesgos específicos. El valor agregado de esta metodología es que permite actuar antes de que se materialicen los hechos generadores de detrimento, facilitando la toma de decisiones correctivas, la intervención institucional oportuna y la reactivación de proyectos detenidos por ineficiencia administrativa, conflictos contractuales o disputas entre comunidades y entidades ejecutoras. Del total de proyectos intervenidos, 80 lograron cerrar el seguimiento al superar los factores de riesgo previamente alertados, lo cual demuestra la eficacia de la estrategia de acompañamiento fiscal focalizado impulsada por la Dirección.

Un ejemplo emblemático del impacto cualitativo de la DIARI, es el caso del Museo de las Víctimas en el corregimiento de Mampuján en el departamento de Bolívar. Este proyecto, vinculado a medidas de reparación colectiva dentro del marco del posconflicto, se encontraba con dificultades significativas en su ejecución física y administrativa. Gracias al seguimiento permanente de la DIARI, se logró identificar de manera temprana los obstáculos, coordinar acciones con los responsables locales y acompañar técnicamente su culminación. Como resultado, el proyecto alcanzó el 100% de avance físico y fue entregado a la comunidad beneficiaria, configurándose no solo como un logro técnico, sino también como un avance en justicia transicional y reparación simbólica[99].

Desde la dimensión cuantitativa, el informe destaca que los beneficios de control fiscal asociados a los seguimientos realizados por la DIARI ascendieron a más de $609.000 millones de pesos, lo que incluye tanto el ahorro de recursos como la protección de inversiones en riesgo. Esta cifra representa un indicador tangible de la eficacia de la vigilancia preventiva y del uso estratégico de la información para evitar el deterioro de los recursos públicos. Además,

99 Ídem.

permite demostrar que la función de la DIARI no se limita a detectar hallazgos, sino que también construye valor público a través de la gestión de la información y la articulación institucional.

Otro ámbito clave de acción de la DIARI es el desarrollo de modelos analíticos para el diagnóstico, pronóstico y prevención de riesgos fiscales. Utilizando técnicas de minería de datos, inteligencia artificial y *machine learning*, la Dirección ha diseñado algoritmos que permiten responder preguntas de negocio críticas para la Contraloría. Estas preguntas incluyen, entre otras: ¿qué tipo de proyectos presentan mayor probabilidad de incumplimiento?, ¿en qué territorios se concentran los mayores riesgos de corrupción?, ¿qué comportamientos financieros atípicos podrían alertar sobre sobrecostos o fraccionamientos contractuales? Estas herramientas se han aplicado de manera transversal en sectores como infraestructura, salud, educación y servicios públicos, y han servido como insumo para la programación de auditorías, la priorización de recursos y la formulación de líneas estratégicas de control.

En su rol como actor clave en la política de ciberseguridad institucional, la DIARI también ha asumido responsabilidades en la detección de vulnerabilidades tecnológicas de los sistemas de información de los sujetos de control. Aunque no reemplaza a las entidades especializadas como ColCERT o la Policía Nacional, cumple una función de primer nivel al identificar brechas, activar alertas internas y coordinar con las áreas técnicas de la CGR para elaborar informes que puedan ser trasladados a instancias judiciales o administrativas. Este rol se refuerza con la implementación de estándares de seguridad, respaldo de datos, control de accesos y trazabilidad de operaciones, según lo establecido en la política institucional de gestión de información[100].

Además, como parte de su contribución al ecosistema de transparencia y vigilancia ciudadana, la DIARI ha desarrollado plataformas y tableros abiertos que permiten a la ciudadanía conocer el estado de ejecución de proyectos estratégicos, consultar mapas de

100 Ídem.

alertas territoriales y participar mediante mecanismos de control social digital. Esta estrategia de apertura y rendición de cuentas ha facilitado la detección de riesgos no previstos, la recepción de denuncias y la participación activa de veedurías, lo cual amplifica la cobertura del control fiscal y promueve una cultura pública de legalidad y vigilancia.

También debe mencionarse el fortalecimiento del enfoque territorial en la acción de la DIARI, que ha priorizado intervenciones en zonas de alta conflictividad social, baja capacidad institucional o con presencia de esquemas complejos de contratación pública. Municipios con Planes de Desarrollo con Enfoque Territorial –PDET–, regiones beneficiarias del Sistema General de Regalías y departamentos con problemas históricos de corrupción, han sido objeto de acciones focalizadas que integran análisis contextual, diálogo institucional y generación de capacidades locales para la gestión eficiente de los recursos.

En esta línea, la Contraloría General de la República inauguró el 22 de abril de 2025 un moderno laboratorio forense y almacén de evidencias, una infraestructura tecnológica sin precedentes en el ecosistema del control fiscal colombiano. Este espacio, liderado por la DIARI, permitirá realizar análisis digitales avanzados, proteger la autenticidad de las evidencias y fortalecer la trazabilidad, integridad y procesamiento de pruebas recolectadas durante los procesos de auditoría. El proyecto se alinea con el desarrollo de las competencias otorgadas a la entidad por el Acto Legislativo 04 de 2019[101], en el marco del Plan Estratégico 2022-2026.

Equipado con estaciones de análisis forense de alto rendimiento, sistemas de control inteligente de acceso al almacén de evidencias, kits para recuperación de datos dañados, herramientas de monitoreo en tiempo real y plataformas para detectar manipulaciones digitales, el laboratorio marca un hito en la capacidad de la CGR para detectar anomalías, reconstruir transacciones financieras y anali-

101 Acto legislativo 04 de 18 de septiembre de 2019, "Por medio del cual se reforma el Régimen de Control Fiscal", *Diario Oficial* n.° 51.080, del 18 de septiembre de 2019, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=30038092].

zar información crítica como correos electrónicos y archivos digitales. Esta infraestructura robusta responde a las nuevas exigencias de una ciudadanía que demanda mayor transparencia, efectividad y oportunidad en la vigilancia del gasto público.

A lo largo del informe de gestión, se destaca que la DIARI no actúa de forma aislada sino en coordinación permanente con otras dependencias de la Contraloría, incluyendo las delegadas sectoriales, las gerencias departamentales y los equipos de auditoría. Esta articulación ha sido fundamental para traducir las alertas analíticas en decisiones operativas, reforzar hallazgos detectados en campo y garantizar la trazabilidad entre la identificación del riesgo, la actuación de control y la restitución oportuna de los recursos en disputa.

En conclusión, la experiencia acumulada por la DIARI durante el periodo 2023-2024 refleja un modelo de vigilancia fiscal moderno, adaptativo y centrado en la prevención, que ha demostrado capacidad de generar impactos positivos tanto en términos financieros como sociales. Su papel estratégico, sustentado en el uso intensivo de datos, la analítica predictiva, la coordinación interinstitucional y la articulación con la ciudadanía, la consolida como una de las innovaciones más relevantes en el control fiscal colombiano del siglo XXI.

Como se ha comentado, la Dirección de Información, Análisis y Reacción Inmediata –DIARI– ha comprobado ser una instancia estratégica en el fortalecimiento de la ciberseguridad institucional de la Contraloría General de la República y, por extensión, del ecosistema de control fiscal en Colombia. A través de su estructura técnica y sus capacidades analíticas, la DIARI ha logrado integrar la ciberseguridad como un componente esencial de la vigilancia fiscal, particularmente en un entorno donde los riesgos digitales representan una amenaza creciente para la integridad de los recursos públicos. Su capacidad para detectar tempranamente vulnerabilidades tecnológicas en los sistemas de información de los sujetos de control, activar protocolos internos de respuesta, coordinar con áreas técnicas y canalizar hallazgos a instancias competentes, configura un modelo operativo proactivo y adaptativo que supera la lógica tradicional de auditoría retrospectiva.

En este marco, la DIARI no solo ha consolidado procesos técnicos orientados al control de accesos, trazabilidad de operaciones y respaldo de la información institucional, sino que también ha adoptado una postura de anticipación frente a ciberincidentes, articulando su función con las entidades especializadas del Estado como ColCERT y la Policía Nacional.

Este rol ha permitido fortalecer la resiliencia del control fiscal frente a escenarios de riesgo cibernético, contribuir a la consolidación de una cultura organizacional orientada a la protección de los activos digitales y garantizar la confiabilidad de los datos como insumo central para la toma de decisiones públicas. En definitiva, la DIARI se erige como un actor clave en el diseño e implementación de una política pública de control fiscal digital con enfoque en ciberseguridad, aportando de manera decidida a la construcción de un Estado más transparente, seguro y eficaz frente a los desafíos tecnológicos del siglo XXI.

Capítulo tercero
Casos emblemáticos de ciberataques a entidades públicas y sus impactos fiscales

I. El cibercrimen en perspectiva glo-cal

Como se ha mencionado, en el contexto actual de transformación digital y creciente dependencia de los sistemas informáticos, los ciberataques se han convertido en una de las amenazas más graves para la seguridad de los Estados, las instituciones públicas y en general de gran parte de la ciudadanía. A nivel global, el aumento en la frecuencia, sofisticación y alcance de estos ataques ha generado una creciente preocupación en gobiernos, organismos internacionales y expertos en ciberseguridad.

De tal modo, las tecnologías digitales, aunque han permitido mejorar la eficiencia administrativa y facilitar el acceso a servicios públicos, también han expuesto a las instituciones a nuevos riesgos asociados al uso de tecnologías vulnerables y redes interconectadas. En tanto esta problemática no se limita a sectores privados o empresas tecnológicas, sino que afecta con especial intensidad a las entidades públicas, responsables de gestionar datos sensibles y prestar servicios esenciales a millones de personas en cada uno de los Estados.

En la actualidad los ciberataques no solo buscan causar daños financieros o robar información, sino generar caos institucional, desacreditar gobiernos o interferir en procesos democráticos. De tal manera que organismos como las agencias de salud, los ministerios de justicia, las fuerzas militares o las autoridades tributarias han sido blanco de ciberataques, muchos de los cuales han logrado paralizar

temporalmente servicios, filtrar datos personales, alterar el funcionamiento de sectores estratégicos e incluso exigir "pagos" a los Estados para que la información sea liberada o no sea revelada públicamente.

Casos como el ataque a la Agencia de Asistencia Legal del Reino Unido en 2025, considerado uno de los incidentes más graves recientemente presentados, cuando sufrió un ciberataque masivo poniendo en riesgo la información privada de más de 2,1 millones de personas, revelando datos como antecedentes penales, información bancaria, números de seguro social y archivos de casos judiciales vigentes, entre otros. Es de mencionar, que la violación no solo afectó gravemente la privacidad de las personas, sino que generó demoras en los procesos judiciales y en los pagos a los abogados de la defensa pública. Así mismo, aumentó el peligro y las alertas por posibles extorsiones, dado que los atacantes podrían utilizar estos datos confidenciales para chantajear a las víctimas[102].

Otro de los casos más relevantes en cuanto a consecuencias, fue el ciberataque al Servicio de Salud de Irlanda (HSE, por sus siglas en inglés) en mayo de 2021. Este fue identificado como un ataque de tipo *ransomware* ejecutado por un grupo conocido como Conti, quienes exigieron un rescate de 20 millones de dólares para la liberación de los sistemas. De tal modo que el sistema hospitalario irlandés se paralizó casi por completo, se suspendieron cirugías, se bloquearon registros médicos digitales y se cancelaron consultas médicas en todo el país; el ataque fue de tal magnitud que algunos hospitales debieron funcionar con sistemas manuales y recurrir al uso de papel, lo que afectó seriamente la calidad del servicio. Cabe mencionar que el gobierno se negó a pagar el "rescate", pero el proceso de recuperación fue lento y costoso para el Estado irlandés[103].

---

102 Rajeev Syal. "Legal aid hack: data from hundreds of thousands of people accessed, says MoJ", *The Guardian*, 19 de mayo de 2025, disponible en [https://www.theguardian.com/law/2025/may/19/significant-amount-of-personal-data-accessed-in-legal-aid-agency-data-breach-says-moj].

103 Rafa de Miguel. "Un ciberataque obliga a Irlanda a cerrar el sistema informático de la sanidad pública", *El País*, Londres, 14 de mayo de 2021, disponible en [https://elpais.com/internacional/2021-05-14/un-ataque-cibernetico-en-irlanda-obliga-a-cerrar-el-sistema-informatico-de-la-sanidad-publica.html].

Por su parte, en mayo de 2025 se reportó un ciberataque significativo que afectó directamente a las comunicaciones oficiales del Gobierno de los Estados Unidos, tras la vulneración de TeleMessage, una plataforma de mensajería cifrada utilizada por diversos funcionarios públicos para intercambiar información de manera segura[104]. Esta herramienta tecnológica era empleada por entidades clave como la Agencia Federal para el Manejo de Emergencias –FEMA–, el Servicio Secreto, funcionarios diplomáticos y otros empleados gubernamentales que requieren mantener canales protegidos frente a amenazas externas.

El incidente fue atribuido a un actor cibernético no identificado que logró acceder de forma no autorizada a los servidores de la aplicación y extraer información asociada con más de 60 empleados públicos. Aunque las autoridades señalaron que no se había comprometido información estrictamente clasificada, la filtración incluyó datos sensibles como historiales de mensajes internos, identidades de usuarios, correos electrónicos gubernamentales, números telefónicos y redes de contacto, lo que generó preocupación inmediata sobre los posibles riesgos para la seguridad nacional[105].

Este ataque dejó en evidencia la fragilidad estructural de algunos sistemas de comunicación digital utilizados por instituciones del Estado norteamericano, y puso de manifiesto que incluso plataformas con estándares avanzados de cifrado pueden presentar vulnerabilidades. De tal suerte que la exposición de datos relacionados con patrones de comunicación, contactos oficiales y posibles operaciones en curso, podría tener consecuencias graves al permitir que actores hostiles identifiquen relaciones estratégicas, detecten rutas de decisión y diseñen ataques más elaborados a partir de la información obtenida.

---

104 A. J. Vicens y Raphael Satter. "Exclusive: Hacker who breached communications app used by Trump aide stole data from across US government", *Reuters*, 21 de mayo de 2025, disponible en [https://www.reuters.com/world/us/hacker-who-breached-communications-app-used-by-trump-aide-stole-data-across-us-2025-05-21].

105 Ídem.

Así mismo, la posibilidad de utilizar los datos filtrados para suplantar identidades, interferir en operaciones delicadas o ejecutar campañas de desinformación constituyó una amenaza directa para la estabilidad de los procesos internos del gobierno. De acuerdo con NBC News[106], las autoridades estadounidenses reaccionaron de manera inmediata restringiendo el uso de la plataforma TeleMessage, iniciando una investigación oficial a cargo del FBI y de la Agencia de Seguridad de Infraestructura y Ciberseguridad –CISA–, promoviendo la revisión urgente de los sistemas de protección en otras herramientas tecnológicas utilizadas por dependencias públicas.

Es de mencionar que este incidente también tuvo un impacto en la percepción internacional sobre la seguridad cibernética del Gobierno estadounidense, dado que la exposición mediática del ataque generó preocupación entre aliados y socios estratégicos, al tiempo que reavivó el debate sobre la necesidad de mejorar los marcos normativos y presupuestales destinados a la protección de infraestructuras digitales críticas.

Como respuesta, el Congreso comenzó a considerar una iniciativa para fortalecer la ciberdefensa del Estado mediante un aumento significativo del presupuesto y la adopción de regulaciones más exigentes para la contratación de servicios tecnológicos[107]. En últimas, el caso TeleMessage no solo representó una violación concreta a la privacidad y confidencialidad de las comunicaciones estatales, sino que puso en evidencia la urgencia de reformular las estrategias de ciberseguridad, en un contexto global cada vez más hostil, donde las amenazas digitales son empleadas como instrumentos de presión política, espionaje y desestabilización institucional.

Por otro lado, no puede ignorarse el componente geopolítico que comienza a visibilizarse en los ciberataques registrados en países europeos, como es el caso de España, que en lo corrido del 2025

---

106 Kevin Collier y Ben Goggin. "Messaging app seen in use by Mike Waltz suspends service after hackers claim breach", *NBC News*, 5 de mayo de 2025, disponible en [https://www.nbcnews.com/tech/security/telemessage-suspends-services-hackers-say-breached-app-rcna204925].

107 Ídem.

ha registrado un drástico aumento de ciberataques contra entidades públicas. El Centro de Ciberseguridad Industrial de Gipuzkoa –ZIUR–, señaló que estos ataques están vinculados a una campaña de "hacktivismo" prorruso, en represalia por el apoyo del Gobierno español a Ucrania; de modo que han atacado a instituciones gubernamentales, aeropuertos, sistemas de transporte y compañías eléctricas. No obstante, aunque muchos de estos ataques no lograron interrumpir la prestación de los servicios, sí demostraron la capacidad de estos grupos para comprometer temporalmente páginas oficiales, sistemas de correo electrónico y datos internos[108].

Frente a este panorama, es urgente que a nivel global se desarrollen mecanismos más robustos de prevención, respuesta y cooperación internacional en materia de ciberseguridad. Los ciberataques a entidades públicas no solo representan una amenaza técnica, sino que se han transformado en un fenómeno multidimensional que compromete la gobernabilidad, los derechos fundamentales, la privacidad de los ciudadanos y la soberanía digital de los Estados. Reconocer esta realidad es el primer paso para promover una agenda pública más decidida, que garantice la ciber-resiliencia institucional y la protección efectiva de los sistemas informáticos frente a amenazas cada vez más complejas y organizadas.

II. Casos emblemáticos de ciberataques a entidades e instituciones en Latinoamérica

El panorama se vuelve aún más crítico cuando se observa la situación en América Latina, una región que ha experimentado un notable aumento en los ciberataques durante los últimos años. De acuerdo con el informe de Check Point Software[109] correspondiente

---

108 Redacción Radio San Sebastián. "ZIUR alerta del 'drástico aumento' de ciberataques contra entidades españolas", *Sociedad Española de Radiodifusión*, 15 de mayo de 2025, disponible en [https://cadenaser.com/euskadi/2025/05/15/ziur-alerta-del-drastico-aumento-de-ciberataques-contra-entidades-espanolas-radio-san-sebastian/].

109 Maxi Fanelli. "Informe global de ciberataques del primer trimestre de 2025 de Check Point Software", *ITSitio*, 23 de abril de 2025, disponible en [https://www.

al primer trimestre de 2025, América Latina fue la región con mayor incremento porcentual en ciberataques a nivel mundial, con un aumento del 108% en comparación con el año anterior.

Esta cifra pone en evidencia la urgente necesidad de fortalecer las capacidades de defensa cibernética en los países latinoamericanos, cuyas instituciones públicas suelen estar menos preparadas tecnológicamente y con presupuestos limitados para enfrentar este tipo de amenazas. La mayoría de los ataques se han dirigido contra infraestructuras críticas, ministerios, organismos de salud, sistemas judiciales y oficinas tributarias, afectando no solo el funcionamiento de los servicios, sino también la confianza de la ciudadanía en sus instituciones.

La región enfrenta, además, particularidades estructurales que agravan esta situación: falta de políticas públicas sólidas en materia de ciberseguridad, escasa coordinación entre organismos estatales, baja inversión en tecnologías de protección y limitada formación del talento humano en temas digitales. A esto se suma la creciente actividad de grupos de *ransomware* que, en busca de ganancias económicas, explotan vulnerabilidades de sistemas obsoletos o mal protegidos. Un ejemplo claro fue el caso de Costa Rica, donde en 2022 el grupo "Hive" ejecutó un ataque coordinado que paralizó temporalmente las finanzas del Estado y los servicios de salud, obligando al Gobierno de ese país a declarar un estado de emergencia nacional, medida inédita para un ciberataque en esta región del mundo.

A. Ciberataque a la Secretaría de la Defensa Nacional de México

El ataque informático a la Secretaría de la Defensa Nacional –SEDENA– ha sido catalogado como un hecho sin precedentes, al tratarse de una institución clave en la protección de la soberanía y la seguridad del país, el grupo de *hackers* conocido como "Guacamaya"

itsitio.com/seguridad/informe-global-de-ciberataques-del-primer-trimestre-de-2025-de-check-point-software/].

logró filtrar aproximadamente seis terabytes de datos almacenados en los servidores de esta entidad, lo que representa una cantidad estimada entre 24 y 40 millones de documentos, incluyendo miles de correos electrónicos, desde 2016 hasta septiembre del año en que ocurrió la filtración[110].

Esta fuga de información es de tal magnitud que duplica lo revelado en los *Pandora Papers*, que en 2021 expuso operaciones financieras internacionales con un total de 2,9 terabytes, equivalentes a 11,9 millones de documentos. También supera ampliamente los *Panama Papers* de 2016, que involucraron 2,6 terabytes[111]. Por esta razón, se considera uno de los ataques cibernéticos más graves en la historia reciente por la cantidad de datos comprometidos. Los especialistas señalan que los responsables del ataque aprovecharon una vulnerabilidad del servidor Microsoft Exchange, la cual había sido identificada desde la primera mitad de 2021. Sin embargo, el Gobierno mexicano no corrigió el fallo debido a la falta de presupuesto para adquirir actualizaciones ni recursos técnicos suficientes[112].

Al final, expertos en análisis forense digital afirman que los *hackers* probablemente necesitaron al menos tres días para copiar toda la información, lo que sugiere una falta de vigilancia adecuada y una reacción tardía por parte del equipo encargado de los sistemas informáticos de SEDENA.

B. Ciberataque en Argentina: portal Mi Argentina y otros sitios oficiales

Varios servicios digitales del Gobierno argentino, como el portal Mi Argentina, la aplicación SUBE y otros sitios oficiales dejaron de funcionar producto de un ataque cibernético, lo que impidió a los

110 COPARMEX. "Grave y preocupante el hackeo a la SADENA", 2023, disponible en [https://coparmex.org.mx/downloads/ENVIOS/SC_030_Newsletter.pdf].

111 Ídem.

112 FORBES STAFF. "Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque", *Forbes México*, 30 de septiembre de 2022, disponible en [https://forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/].

ciudadanos acceder a información o realizar trámites en línea. El Gobierno explicó que este incidente se debió a la falta de inversión en infraestructura crítica, una situación que, según afirmaron, pudo haberse evitado.

Y es que no se trata de un hecho aislado, dado que se suma a una serie de incidentes previos que han comprometido la ciberseguridad del Estado argentino, independiente del gobierno de turno. Uno de los más destacados ocurrió en 2017, cuando el Ministerio de Seguridad, bajo la dirección de Patricia Bullrich, fue blanco de un ataque que se inició con un correo de *phishing* dirigido a la propia ministra. A partir de esa vulnerabilidad, los delincuentes lograron acceder a distintas dependencias del Estado y filtrar documentos sensibles vinculados a la Dirección General de Inteligencia Criminal[113].

En 2019, tras las elecciones primarias, se produjo un nuevo ataque, esta vez mediante correos falsos enviados a diversas comisarías. En esa ocasión, los atacantes accedieron a escuchas telefónicas, archivos confidenciales de altos mandos policiales y hasta nombres de agentes implicados en investigaciones de narcotráfico, este caso se conoció como "LaGorraLeaks", y en enero de 2024 se detuvo al presunto responsable.

Durante la pandemia, en 2020, la Dirección Nacional de Migraciones también fue atacada mediante un *ransomware* que paralizó su sistema de ingresos y egresos, los criminales exigieron millones de dólares a cambio de no divulgar la información robada. Al año siguiente, el Registro Nacional de las Personas –RENAPER– fue blanco de otra filtración, en la que al menos 60.000 datos personales fueron comprometidos.

En 2024, la Agencia Nacional de Seguridad Vial –ANSV– detectó una posible filtración masiva luego de que un usuario en la red social X (antes Twitter) informara sobre la oferta de venta de 1,2 te-

113 Sebastián Davidovsky. "Cómo fue el ciberataque al sitio Argentina.gob.ar, el último de una larga serie de ataques a organismos estatales", *La Nación*, 26 de diciembre de 2024, disponible en [https://www.lanacion.com.ar/tecnologia/como-fue-el-ciberataque-al-sitio-de-mi-argentina-el-ultimo-de-una-larga-serie-de-ataques-a-nid26122024].

rabytes de datos en un canal de Telegram. Entre los datos comprometidos figuraban licencias de conducir de figuras públicas como el presidente de la Nación, ministros y otros funcionarios[114].

C. Ciberataque al Ministerio de Hacienda en Costa Rica

La Contraloría General de Costa Rica identificó serias inconsistencias en el manejo de los pagos salariales por parte del Ministerio de Hacienda, como consecuencia del ciberataque que afectó a la entidad entre abril y junio de 2022. Durante ese periodo se presentaron errores que incluyeron tanto pagos en exceso como omisiones en el pago de sueldos, lo cual quedó en evidencia tras una auditoría financiera sobre la ejecución presupuestaria de ese año. Con posterioridad, el área de fiscalización de la Contraloría explicó que el Ministerio todavía no ha podido recuperar todos los fondos que se desembolsaron de forma indebida ni completar los pagos que quedaron pendientes a varios trabajadores[115].

El informe señaló que el monto total pagado sin justificación se acercó a los 15 millones de dólares y que la deuda por sueldos no cancelados supera los 6,2 millones. Además, al finalizar el 2022, el Ministerio aún no había logrado identificar con claridad a qué tipo de impuesto correspondían aproximadamente 529 millones de dólares recaudados durante los meses en que se produjo el ataque, lo cual también generó preocupación institucional.

El ministro de Hacienda Nogui Acosta, se refirió al tema mediante un video en el que señaló que el informe pone de manifiesto el efecto real que tuvo el ciberataque sobre el funcionamiento del ministerio, ya que en su momento se tomó la decisión de recurrir a planillas anteriores para poder pagar salarios, lo que provocó distorsiones en los pagos procesados a través de la tesorería nacional.

---

114 Ídem.

115 Djenane Villanueva. "Ataques cibernéticos repercuten en las finanzas de la Hacienda Pública en Costa Rica, según órgano fiscalizador", *cnn en Español*, 20 de julio de 2023, disponible en [https://cnnespanol.cnn.com/2023/07/20/ataques-ciberneticos-finanzas-hacienda-publica-costa-rica-orix].

A pesar de estas dificultades, Acosta afirmó que las consecuencias fueron relativamente controladas dadas las circunstancias que enfrentaba el país en ese momento y aseguró que ya se está avanzando en los procesos para recuperar los recursos desembolsados de manera errónea[116].

En respuesta a la gravedad de la situación, en mayo de 2022 el Gobierno costarricense declaró el estado de emergencia nacional para todo el sector público, dado que los ataques cibernéticos habían comprometido de manera grave la estructura operativa de los sistemas de información estatales. La agencia calificadora Moody's también se pronunció sobre el tema, advirtiendo que este incidente evidenciaba serias debilidades institucionales y de ciberseguridad que obligaban al gobierno a aumentar sus inversiones en estas áreas críticas para garantizar la continuidad del servicio público[117].

Al menos 27 instituciones del Estado resultaron afectadas, de las cuales nueve registraron daños importantes en sus sistemas. Entre las entidades comprometidas se encuentran, además del Ministerio de Hacienda, la Caja Costarricense de Seguro Social, el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, el Instituto Meteorológico Nacional y la empresa estatal Radiográfica Costarricense, lo que demuestra la amplitud del impacto y la necesidad de fortalecer la protección digital del aparato público en Costa Rica[118].

D. Ciberataque a IFC Networks

El Gobierno nacional colombiano informó sobre el ataque cibernético dirigido a la empresa IFX Networks, un proveedor de servicios tecnológicos y de telecomunicaciones. El ciberataque afectó el funcionamiento de las páginas web de varias instituciones, entre ellas la Superintendencia de Industria y Comercio, la Superintendencia

116 Ídem.

117 Villanueva. "Ataques cibernéticos repercuten en las finanzas de la Hacienda Pública en Costa Rica, según órgano fiscalizador", cit.

118 Atahualpa Amerise. "'Estamos en guerra': 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia", *BBC News Mundo*, 20 de mayo de 2022, disponible en [https://www.bbc.com/mundo/noticias-america-latina-61516874].

de Salud, el Ministerio de Salud y Protección Social y el Consejo Superior de la Judicatura, estas plataformas presentaron fallas como mensajes de error, interrupciones en el servicio o problemas técnicos que impidieron el acceso de los usuarios desde el 12 de septiembre de 2023[119].

El equipo asesor de Transformación Digital aclaró que el incidente tuvo como blanco directo a IFX Networks, no a las entidades estatales. Sin embargo, debido a que muchas de estas instituciones dependen de los servicios tecnológicos de dicha empresa, sus plataformas se vieron afectadas de manera indirecta. El ataque fue ejecutado mediante un *ransomware*, una modalidad de cibercrimen que consiste en bloquear el acceso a sistemas o información a cambio de un rescate, y logró impactar a unas 762 compañías en América Latina[120]. Aunque no se identificaron filtraciones de datos personales o institucionales, el incidente ha generado preocupación por la interrupción de servicios y la posibilidad de que se presenten nuevos ataques.

En un comunicado oficial, el Gobierno señaló que, según los primeros análisis realizados por IFX Networks, no se comprometió la integridad de la información en ninguna de sus plataformas. No obstante, se encuentran en el proceso de determinar cuántos activos de información podrían haber sido alcanzados en el territorio colombiano[121]. De acuerdo con datos suministrados por la firma de ciberseguridad Fortinet, Colombia enfrentó más de 5.000 millones de intentos de ciberataques solo en el primer semestre del año, ubicán-

---

119 Ministerio de Tecnologías de la Información y las Comunicaciones. "Gobierno nacional atiende ataque cibernético que afecta a varias entidades e instala PMU CIBER", 13 de septiembre de 2023, disponible en [https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/278831:Gobierno-Nacional-atiende-ataque-cibernetico-que-afecta-a-varias-entidades-e-instala-PMU-CIBER].

120 Ídem.

121 Kiara K. Rochel Galeano. "Ciberataque a proveedor de servicios de Entidades Públicas", Asociación Nacional de Comercio Exterior –analdex–, 2023, disponible en [https://analdex.org/2023/09/18/ciberataque-a-proveedor-de-servicios-de-entidades-publicas/].

dose como el cuarto país más afectado por estas amenazas en América Latina, superado únicamente por Brasil, México y Venezuela[122].

E. Ciberataque a la Fiscalía General de la Nación de Colombia

En 2022, la Fiscalía General de la Nación fue blanco de un ciberataque ejecutado por el colectivo activista "Guacamaya". Según información revelada por los medios de comunicación, los atacantes lograron sustraer más de cinco terabytes comprimidos de información, lo que equivaldría a más de diez terabytes reales, comparables a la carga de unos mil camiones llenos de documentos impresos.

Dentro del material comprometido se encontrarían expedientes confidenciales gestionados por la Fiscalía desde 2018 hasta 2022. Estos archivos abarcarían investigaciones relacionadas con casos de corrupción, narcotráfico y organizaciones armadas ilegales, entre otros temas delicados. También se presume que entre los datos extraídos se encuentran registros sobre personas que han colaborado como fuentes humanas en los procesos judiciales durante los últimos años[123].

El 6 de noviembre, el diario *El Espectador* publicó detalles sobre la información obtenida por los *hackers*[124]. Según el medio, el acceso no autorizado se habría dado a través del servidor de correos electrónicos institucionales de la Fiscalía. Frente a las primeras revelaciones en los medios, el 19 de octubre la entidad emitió un comunicado oficial anunciando la apertura de una investigación interna con el objetivo de esclarecer los hechos.

En ese mismo pronunciamiento, la Fiscalía explicó que, a través de su contratista Colombia Telecomunicaciones S. A., se implemen-

---

122 Ídem.

123 Jenny Angarita. "Fiscalía sigue investigando hackeo de información clave judicial", *W Radio*, 4 de noviembre de 2022, disponible en [https://www.wradio.com.co/2022/11/04/fiscalia-sigue-investigando-hackeo-de-informacion-clave-judicial/].

124 Redacción Judicial. "Hackeo a la Fiscalía: detalles inéditos de una filtración sin precedentes", *El Espectador*, 6 de noviembre de 2022, disponible en [https://www.elespectador.com/judicial/los-archivos-secretos-del-hackeo-a-la-fiscalia].

taron medidas para revisar y mitigar posibles riesgos derivados del ataque. Además, se inició un proceso administrativo para determinar si este proveedor de servicios tecnológicos pudo haber tenido alguna responsabilidad en la vulnerabilidad de los sistemas.

El Espectador informó que logró acceder a más de 38.000 carpetas filtradas, las cuales contenían correos electrónicos de funcionarios como fiscales, asistentes, policías judiciales y miembros del CTI. También se encontraron documentos altamente sensibles como información de testigos protegidos, órdenes de seguimiento y detalles sobre colaboraciones internacionales de la Fiscalía.

Sobre "Guacamaya", se sabe que es un colectivo de *hackers* que busca exponer información confidencial de instituciones gubernamentales o privadas que, a su juicio, han cometido abusos de poder que perjudican a comunidades vulnerables o al medio ambiente. Este grupo no solo ha operado en Colombia, sino que también ha atacado instituciones en otros países latinoamericanos como México, Chile y Guatemala, según reveló la misma investigación periodística[125].

F. Ciberataque a Empresas Públicas de Medellín: infraestructura crítica comprometida

Uno de los eventos más representativos de vulnerabilidad institucional en Colombia fue el ciberataque a Empresas Públicas de Medellín –EPM–, ocurrido el 13 de diciembre de 2022. Según los comunicados de la entidad y los reportes periodísticos, EPM fue víctima de un ataque de tipo *ransomware*, en el que sus archivos fueron encriptados y se les exigió un rescate para su liberación. El grupo delincuencial utilizó la variante de *ransomware* denominada "BlackCat" o "ALPHV", una de las más sofisticadas identificadas por expertos en ciberseguridad[126].

---

125 INFOBAE. "Hackers tendrían 'secuestrada' información de la Fiscalía de Colombia: más de 10 teras de datos habrían sido hurtados", *Infobae*, 11 de noviembre de 2022, disponible en [https://www.infobae.com/america/colombia/2022/11/11/hackers-tendrian-secuestrada-informacion-de-la-fiscalia-de-colombia-mas-de-10-teras-de-datos-habrian-sido-hurtados].

126 DAVID ALEJANDRO MERCADO. "Medellín: Este es el grupo que se adjudicó el ataque

El impacto fiscal de este incidente fue considerable. Según la información suministrada por la misma empresa, cerca del 25% de su infraestructura digital se vio comprometida, lo que afectó la disponibilidad de sus servicios internos, el procesamiento de pagos, el sistema de atención a usuarios y la integridad de datos financieros y contractuales. Se calcula que los daños asociados al ciberataque podrían superar los cinco millones de dólares, sin considerar los costos de reputación, pérdida de confianza y esfuerzos en recuperación[127].

Según datos del Centro Cibernético de la Policía Nacional, hasta octubre de 2022 se habían reportado 54.121 casos relacionados con delitos informáticos, lo que representa un incremento de 11.223 denuncias en comparación con el 2021, es decir, un aumento del 30%, de acuerdo con la Cámara Colombiana de Informática y Telecomunicaciones.

Por su parte, la firma Fortinet en su informe más reciente, señaló que durante el primer semestre del 2022 se presentaron 137.000 intentos de ciberataques en América Latina, lo que equivale a un aumento del 50% frente al mismo periodo del año anterior, cuando se registraron 91.000[128]. En cuanto a las acciones que planea desarrollar EPM, la entidad contempla realizar un análisis para identificar la causa raíz del incidente, así como una investigación forense. También se evaluará el impacto del ataque, se revisarán las políticas internas del grupo y se emitirá una comunicación oficial al respecto.

Por último, se debe indicar que la afectación de una empresa de servicios públicos con la magnitud y relevancia de EPM refleja la necesidad de que entidades con infraestructura crítica adopten es-

cibernético a EPM", *El Tiempo*, 27 de diciembre de 2022, disponible en [https://www.eltiempo.com/colombia/medellin/blackcat-el-grupo-que-se-adjudico-el-ataque-cibernetico-a-epm-729363].

127 Allison Gutiérrez Núñez. "EPM y Afinia, entre las compañías que han sido víctimas de ciberataques", *La República*, 17 de diciembre de 2022, disponible en [https://www.larepublica.co/empresas/epm-y-afinia-entre-las-companias-que-han-sido-victimas-de-ciberataques-en-el-ano-3510742].

128 Lilian Mariño Espinosa. "Ataque cibernético que EPM sufrió esta semana se dio desde la Central de Ituango", *La República*, 16 de diciembre de 2022, disponible en [https://www.larepublica.co/empresas/ataque-cibernetico-que-epm-sufrio-esta-semana-se-dio-desde-la-central-de-ituango-3510139].

quemas robustos de ciber-resiliencia, implementen auditorías continuas sobre sus sistemas de TI y desarrollen capacidades internas para la detección, contención y mitigación de amenazas digitales.

G. Sanitas y el Grupo Keralty: compromiso de datos de salud y proveedores

En noviembre de 2022, el Grupo Keralty, matriz en Colombia de las EPS Sanitas y Colsanitas, confirmó haber sido víctima de un ataque cibernético masivo perpetrado por el grupo criminal "RansomHouse". El ataque comprometió información confidencial de pacientes, proveedores, contratos y registros financieros. RansomHouse filtró parte de esta información a través de canales en la red oscura, incluyendo plataformas como Telegram[129].

Los impactos fiscales de este ataque no se limitaron a la interrupción temporal de los servicios de atención médica, sino que también implicaron riesgos de detrimento patrimonial por el potencial uso indebido de los recursos públicos destinados al sistema de salud. Así mismo, la exposición de datos sensibles abre la puerta a fraudes, suplantaciones, extorsión y reclamos legales por violación de habeas data. La CGR, en conjunto con la Superintendencia Nacional de Salud, inició un proceso de seguimiento fiscal y técnico para determinar el alcance de los daños y la posible responsabilidad administrativa de la entidad.

Posteriormente, mediante un comunicado de prensa, la Superintendencia Nacional de Salud –Supersalud– informó que, transcurridos 45 días desde que se reportó el ciberataque que afectó las plataformas de Sanitas, aún persisten obstáculos que impiden el funcionamiento normal de los servicios. El ente señaló que ha mantenido un seguimiento constante para garantizar el acceso efectivo

129 Laura Lesmes. "Keralty, la nueva víctima de los ataques de 'ransomware'", *El Tiempo*, 4 de diciembre de 2022, disponible en [https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175].

a los servicios de salud y que ha recibido respuesta por parte de la EPS ante los requerimientos realizados.

El comunicado advierte que las plataformas aún no logran una interoperabilidad adecuada, lo cual se traduce en retrasos, reprocesos y afectaciones en la gestión del riesgo en salud y finanzas, funciones que son de responsabilidad directa del asegurador. En cuanto a la seguridad de los datos personales, la Supersalud indicó que, según las investigaciones adelantadas por Sanitas, se confirmó la afectación de la información personal de 241.589 usuarios. Ante esta situación, la entidad exigió que Sanitas notifique de forma oportuna, clara y completa a cada uno de los usuarios comprometidos[130].

Por otro lado, la EPS informó que hasta el momento no se ha detectado ninguna vulneración a la confidencialidad ni a la integridad de las historias clínicas. No obstante, este caso demuestra cómo los ciberataques a instituciones que manejan recursos del Sistema General de Participaciones pueden tener consecuencias fiscales directas, comprometiendo la eficiencia del gasto y generando afectaciones al servicio público esencial.

H. Ciberincidentes en entidades territoriales colombianas: fragilidad estructural y afectación presupuestal

Además de los casos de grandes entidades, se han documentado múltiples ciberincidentes en alcaldías, gobernaciones, hospitales y universidades públicas. Según información revelada por la DIJIN y el Centro Cibernético de la Policía Nacional, solo en 2022 se registraron más de 15.000 denuncias asociadas a ciberataques contra páginas web y sistemas de información del sector público territorial[131].

Los efectos fiscales de estos ataques incluyen: pérdida de registros contables, interrupción en la ejecución presupuestal, atraso en la contratación, dificultad para hacer pagos, pérdida de trazabilidad

---

130 UNIDAD DE SALUD. "EPS Sanitas: ciberataque vulneró datos de 241.589 usuarios, según Supersalud", *El Tiempo*, 26 de enero de 2023, disponible en [https://www.eltiempo.com/salud/eps-sanitas-ciberataque-vulnero-datos-de-241-589-usuarios-736961].

131 CENTRO CIBERNÉTICO POLICIAL. *Boletín estadístico de delitos informáticos*, cit.

en procesos licitatorios y manipulación de bases de datos de beneficiarios de programas sociales. En algunos municipios se han tenido que destinar recursos extraordinarios para la recuperación de sistemas, compra de nuevos equipos y contratación de personal técnico, lo que afecta los planes de inversión previamente aprobados.

Entidades como la Contraloría General de la República, han advertido que las debilidades en seguridad informática están asociadas a la falta de manuales de protección de datos, ausencia de análisis de riesgos, carencia de políticas de respaldo y actualización irregular de *software* institucional. Estas deficiencias constituyen riesgos fiscales latentes que ameritan intervención preventiva.

III. Rol potencial de la DIARI en escenarios de riesgo y prevención de daño fiscal

En el actual contexto de transformación digital de la administración pública y frente a la creciente sofisticación de las amenazas cibernéticas, el rol de la Dirección de Información, Análisis y Reacción Inmediata –DIARI– de la Contraloría General de la República –CGR–, se ha redefinido como un componente estratégico no solo para el control fiscal sino también para la protección del ecosistema digital del Estado colombiano. Esta dirección no solo se ha especializado en el monitoreo de información fiscal en tiempo real, sino que se ha consolidado como una unidad clave para la prevención de riesgos sistémicos que pueden derivar en daño fiscal, pérdida de recursos públicos o debilitamiento institucional por vulnerabilidades tecnológicas.

Como se ha mencionado en el capítulo anterior, la DIARI ha sido diseñada para operar como un nodo de análisis predictivo, capaz de anticipar escenarios de riesgo a través de la integración de tecnologías como inteligencia artificial, minería de datos y *machine learning*. Estas capacidades le permiten generar alertas tempranas sobre comportamientos atípicos en la ejecución presupuestal, patrones inusuales de contratación, modificaciones contractuales injustificadas o retrasos en proyectos críticos, factores que han sido identificados históricamente como antecedentes de detrimento patrimonial. Esta facultad analítica, apoyada en el uso de tableros de control fiscal te-

rritorial y plataformas como el Sistema Analítico del Gasto Público –SAGA–, permite a la Contraloría actuar de manera proactiva, en lugar de reactiva, en la defensa de los recursos públicos[132].

A nivel operativo, la DIARI articula sus acciones en tres grandes funciones interdependientes: la prevención, a través de la identificación de patrones de riesgo; la vigilancia, mediante el monitoreo continuo de operaciones y bases de datos; y la respuesta, mediante la articulación con otras instancias de la CGR y entidades del Estado como la Fiscalía General de la Nación, el MINTIC, la Policía Nacional y el Grupo ColCERT. Esta última dimensión adquiere una importancia particular en escenarios de ciberincidentes, en los que la DIARI no actúa como cuerpo de reacción técnica directa –función propia de las entidades de ciberdefensa–, pero sí como primer detector de anomalías en los sistemas digitales de los sujetos de control[133].

Desde el punto de vista institucional, uno de los principales aportes de la DIARI ha sido la implementación de una arquitectura de datos basada en principios de seguridad digital, que garantiza la integridad, disponibilidad y confidencialidad de la información bajo auditoría. El establecimiento de políticas de respaldo, autenticación robusta, trazabilidad documental y control de accesos, conforme a estándares internacionales como ISO/IEC 27001, ha permitido a la entidad blindar su operación ante intentos de sabotaje digital, acceso no autorizado o alteración de registros que son fundamentales para los procesos de responsabilidad fiscal[134].

En escenarios de riesgo, la DIARI cuenta con la capacidad para activar protocolos de respuesta inmediata ante la identificación de posibles ataques cibernéticos, fugas de información o comportamientos que comprometan la estabilidad de los sistemas institucionales. Esta actuación incluye el cierre temporal de accesos, el aislamiento de sistemas comprometidos, la emisión de informes de

---

132 Contraloría General de la República. *Resultados del Sistema SAGA y control fiscal en tiempo real*, cit.

133 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

134 Ídem.

vulnerabilidad y la coordinación con unidades judiciales o técnicas para determinar la materialidad del riesgo. Así, la DIARI funciona como una plataforma intermedia entre la tecnología y la decisión fiscal, permitiendo convertir la inteligencia de datos en decisiones oportunas que previenen la materialización del daño[135].

Además, la DIARI ha contribuido a la construcción de una cultura organizacional de seguridad de la información en la CGR a través de la formación continua de sus funcionarios, la elaboración de protocolos específicos para el manejo de la información sensible y la implementación de auditorías internas periódicas que garantizan el cumplimiento de los requisitos normativos en ciberseguridad. Esta labor pedagógica ha permitido que la prevención del daño fiscal ya no se limite a la acción sancionatoria, sino que se posicione como una política institucional que involucra a todos los actores del sistema de control[136].

A futuro, el potencial de la DIARI puede expandirse aún más mediante la incorporación de herramientas como simuladores de ciberataques (*red teaming*), *blockchain* para trazabilidad de auditorías, autenticación biométrica y visualización de datos basada en georreferenciación y aprendizaje automático. Estas herramientas permitirían mejorar la capacidad predictiva de la entidad, reducir los tiempos de reacción y aumentar la precisión en la identificación de puntos críticos en el gasto público.

En síntesis, el rol de la DIARI en escenarios de riesgo y prevención del daño fiscal no solo se enmarca en una lógica de control tecnológico, sino que responde a una concepción estratégica del control fiscal adaptado al ecosistema digital. Su acción articula tecnología, normatividad y capacidad analítica para blindar el gasto público frente a amenazas externas e internas, consolidando así un modelo de vigilancia inteligente que sitúa a Colombia en la vanguardia regional del control fiscal con enfoque de ciberseguridad.

---

135 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

136 ISACA. *State of Cybersecurity 2021, Part 1: Global Update on Workforce*, cit.

IV. Retos y oportunidades de la Contraloría General en el ecosistema digital

La irrupción del ecosistema digital en la administración pública ha transformado de forma radical las condiciones bajo las cuales se ejerce el control fiscal. La Contraloría General de la República –CGR–, como organismo superior de control en Colombia, se enfrenta al desafío de adaptarse a un entorno caracterizado por la complejidad tecnológica, la velocidad del intercambio de datos y la sofisticación creciente de los riesgos asociados a la gestión de la información pública. En este escenario, los retos institucionales de la CGR no son meramente técnicos, sino también estratégicos y estructurales, ya que involucran el rediseño de su modelo de operación, la transformación de su cultura organizacional, la reconfiguración de sus alianzas interinstitucionales y la reconceptualización de su función misional a la luz de la gobernanza digital.

Este apartado analiza cuatro dimensiones clave: el fortalecimiento institucional y técnico de la Dirección de Información, Análisis y Reacción Inmediata –DIARI–; la coordinación interinstitucional con actores como la Policía Nacional, la Fiscalía General de la Nación, el MINTIC y el ColCERT; la evaluación de las capacidades en *big data* y ciberinteligencia de la entidad; y la necesidad crítica de contar con talento humano especializado y un marco de interoperabilidad normativa adecuado. Estas dimensiones, abordadas de manera articulada, no solo representan desafíos operativos, sino también oportunidades para consolidar un modelo de control fiscal innovador, resiliente y acorde con los estándares internacionales en materia de ciberseguridad.

La Dirección de Información, Análisis y Reacción Inmediata –DIARI– es el corazón del sistema de control fiscal digital de la CGR. Su consolidación como unidad técnica especializada ha permitido integrar herramientas de vigilancia en tiempo real, analítica, predictiva, monitoreo territorial y reacción estratégica ante eventos de riesgo. Sin embargo, su fortalecimiento institucional requiere acciones adicionales en varios frentes.

En primer lugar, se hace necesario dotar a la DIARI de una infraestructura tecnológica de alta disponibilidad, capaz de procesar y almacenar grandes volúmenes de datos en múltiples formatos, con esquemas de redundancia, continuidad operativa y cumplimiento de los estándares ISO/IEC 27001 y NIST[137].

En segundo lugar, se debe garantizar una asignación presupuestal sostenida que permita mantener actualizadas las plataformas analíticas, licencias de *software*, servicios de ciberseguridad gestionada y recursos para la investigación aplicada. En tercer lugar, es urgente avanzar en la institucionalización de la DIARI como eje transversal de las demás dependencias, promoviendo la gobernanza de datos y la integración sistemática de la vigilancia digital en los procesos misionales de la CGR. El desarrollo de modelos de riesgo, algoritmos de priorización de auditorías y tableros de control dinámicos debe extenderse hacia las delegadas sectoriales y gerencias departamentales, fomentando una cultura organizacional orientada al uso inteligente de los datos.

El control fiscal en entornos digitales no puede ser concebido como una función aislada. Las amenazas cibernéticas, el fraude digital y las vulnerabilidades en los sistemas de información públicos demandan respuestas articuladas entre diferentes instituciones del Estado. En este sentido, la CGR enfrenta el reto de fortalecer sus canales de coordinación con organismos como la Policía Nacional (especialmente su Centro Cibernético), la Fiscalía General de la Nación, el Ministerio de Tecnologías de la Información y las Comunicaciones –MINTIC– y el Grupo de Respuesta a Emergencias Cibernéticas de Colombia –ColCERT–.

Cada uno de estos actores cumple funciones complementarias en la cadena de prevención, detección, investigación y sanción de eventos relacionados con la ciberseguridad del Estado. Por ejemplo, mientras que la DIARI puede detectar patrones anómalos en el uso de recursos públicos y emitir alertas sobre riesgos sistémicos, es la Fiscalía la que debe investigar penalmente los delitos informá-

137 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

ticos, y la Policía Nacional quien debe actuar como cuerpo técnico judicial. Por su parte, el MINTIC y ColCERT lideran las políticas y protocolos técnicos ante incidentes de seguridad digital. La CGR debe integrarse a estos ecosistemas mediante acuerdos de intercambio de información, interoperabilidad técnica, protocolos de respuesta y comités conjuntos de análisis de riesgo[138].

Una de las transformaciones más profundas del control fiscal es el tránsito desde el análisis documental tradicional hacia modelos de análisis de datos masivos (*big data*). Este cambio no es solo cuantitativo, sino cualitativo, ya que implica nuevos marcos analíticos, infraestructura computacional, herramientas especializadas y una redefinición de las competencias del auditor. La DIARI ha avanzado en la construcción de modelos predictivos, generación de alertas tempranas y visualización de información territorial. No obstante, se requiere una evaluación exhaustiva de las capacidades actuales de la entidad en términos de captura, integración, análisis y visualización de grandes volúmenes de datos heterogéneos y en tiempo real.

La ciberinteligencia, entendida como el uso sistemático de tecnologías de la información para anticipar, prevenir y neutralizar amenazas a los recursos públicos, debe convertirse en un eje transversal del control fiscal. Para ello, se requiere consolidar una arquitectura institucional basada en lagos de datos, sistemas de almacenamiento distribuidos, técnicas de minería de procesos y analítica visual dinámica. La CGR debe definir métricas claras para evaluar su madurez analítica, capacidad de integración de fuentes externas (como SECOP, SIIF Nación, RUV, etc.) y niveles de automatización en la toma de decisiones[139].

El avance tecnológico solo es sostenible si va acompañado de una estrategia de gestión del conocimiento y formación continua del talento humano. La CGR debe incorporar perfiles profesionales especializados en ciencia de datos, ciberseguridad, arquitectura de sistemas, inteligencia artificial, visualización de datos y derecho digital. Estos perfiles deben integrarse de manera articulada a los

138 Ídem.

139 ISACA. *State of Cybersecurity 2021, Part 1: Global Update on Workforce*, cit.

equipos de auditoría, análisis, tecnología y gestión estratégica. A su vez, es necesario que los servidores públicos de la Contraloría cuenten con programas permanentes de actualización en competencias digitales, ética del dato y metodologías ágiles.

En paralelo, la interoperabilidad normativa constituye otro de los desafíos centrales. El marco jurídico actual sobre ciberseguridad, protección de datos, delitos informáticos y contratación digital presenta vacíos, duplicidades y desarticulaciones que pueden limitar el accionar efectivo de la CGR. Se requiere una revisión y armonización normativa que facilite el acceso, tratamiento y uso legítimo de la información, respetando los principios de legalidad, proporcionalidad y necesidad. Así mismo, la CGR debe participar de forma activa en los procesos de formulación de políticas públicas de gobernanza digital, inteligencia fiscal y protección de infraestructuras críticas del Estado[140].

La transición hacia un modelo de control fiscal digital en Colombia plantea retos estructurales que requieren una respuesta estratégica y sostenida por parte de la Contraloría General de la República –CGR–. En este marco, el papel de la Dirección de Información, Análisis y Reacción Inmediata –DIARI– ha sido fundamental para diseñar e implementar mecanismos de vigilancia en tiempo real, gestión inteligente de datos y anticipación de riesgos fiscales.

Sin embargo, el entorno digital actual exige una expansión de estas capacidades en varias dimensiones. Este apartado presenta una serie de propuestas concretas para fortalecer el control fiscal digital en cuatro ejes estratégicos: la articulación entre el control fiscal, la gestión de riesgos y la ciberseguridad; la creación de líneas de auditoría con enfoque en ciber-resiliencia; el establecimiento de políticas internas de seguridad de la información y blindaje institucional; y la promoción de auditorías preventivas y de tecnologías de la información –TI– como mecanismos eficaces de prevención de la corrupción. Estas propuestas se sustentan en experiencias institu-

140 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

cionales recientes, estándares internacionales y lecciones extraídas de las mejores prácticas comparadas.

El ecosistema digital en el que se desarrolla la administración pública está expuesto a múltiples riesgos que comprometen la integridad de los datos, la continuidad de los servicios y la confianza en las instituciones. En este contexto, el control fiscal debe integrarse a modelos de gestión de riesgos operacionales y de seguridad digital, superando su enfoque tradicional centrado en la verificación documental. La articulación entre control fiscal, gestión de riesgos y ciberseguridad, requiere repensar el proceso auditor desde la fase de planeación hasta la emisión del informe, incorporando variables de exposición digital, vulnerabilidades tecnológicas y amenazas a la infraestructura crítica[141].

Uno de los principales avances en esta materia ha sido la incorporación de modelos analíticos dentro de la DIARI para identificar patrones de comportamiento anómalo en la ejecución del gasto público. Estos modelos permiten generar alertas sobre desviaciones significativas en las líneas presupuestales, sobrecostos no justificados o retrasos en la ejecución física de proyectos, muchos de los cuales se relacionan con fallas en los sistemas de información, pérdida de trazabilidad o acceso no autorizado a plataformas transaccionales. En estos casos, la articulación con unidades de riesgo institucional y con los órganos especializados en ciberdefensa, como el ColCERT o el Centro Cibernético Policial, permite activar una respuesta oportuna que combina el análisis fiscal con la investigación de posibles ataques o negligencias tecnológicas.

Se propone, por tanto, institucionalizar una metodología conjunta entre las áreas de auditoría, tecnología y análisis de riesgos de la CGR que integre el mapeo de riesgos cibernéticos dentro de los instrumentos de control fiscal. Esta metodología debe contemplar criterios de priorización de auditorías en función del nivel de exposición tecnológica de las entidades, su infraestructura crítica, el historial de incidentes de seguridad digital y la sensibilidad de la infor-

141 Ídem.

mación que manejan. La sistematización de estos criterios permitirá construir mapas de riesgo fiscal digital a nivel territorial, sectorial y por tipo de entidad, los cuales deben actualizarse de forma continua con base en nuevas fuentes de datos y eventos emergentes[142].

La ciber-resiliencia se ha posicionado como un eje fundamental de las estrategias de seguridad digital a nivel mundial. En el ámbito del control fiscal, su adopción representa una oportunidad para evaluar no solo los procesos financieros, sino también la capacidad institucional para garantizar la continuidad de la operación ante eventos disruptivos. Esto incluye ataques cibernéticos, fallas tecnológicas, desastres naturales o cualquier evento que pueda comprometer los sistemas de información.

Una línea de auditoría con enfoque en ciber-resiliencia debe incluir una evaluación integral de las capacidades institucionales de recuperación, tanto tecnológicas como organizativas. Debe revisar la existencia de planes de continuidad del negocio, la calidad de los respaldos de información, la redundancia de sistemas, los protocolos de respuesta ante incidentes, la periodicidad de simulacros y pruebas de restauración, así como los mecanismos de reporte y aprendizaje post-incidente. Estas auditorías permitirán no solo verificar el cumplimiento normativo, sino también identificar cuellos de botella, recursos insuficientes o procesos críticos sin medidas de mitigación.

La experiencia internacional demuestra que las auditorías de ciber-resiliencia deben combinar enfoques técnicos y funcionales. Por ejemplo, la Oficina del Auditor General de Canadá ha implementado revisiones que cruzan la infraestructura tecnológica con los procesos misionales de cada entidad, evaluando su grado de dependencia digital y su nivel de preparación ante eventos de ciberseguridad. En Colombia, esta experiencia podría replicarse con ajustes contextuales, y bajo el liderazgo de la DIARI, que ya cuenta con capacidades en análisis de sistemas críticos, modelación de riesgos y trabajo interinstitucional.

---

142 ISACA. *State of Cybersecurity 2021, Part 1: Global Update on Workforce*, cit.

La creación de esta línea de auditoría implicaría también la capacitación de un equipo especializado dentro de la CGR, la actualización de los manuales de auditoría y la definición de indicadores de madurez digital aplicables a los sujetos de control. Estos indicadores podrían incluir el porcentaje de activos digitales clasificados y protegidos, la cobertura de planes de respaldo, el tiempo promedio de respuesta a incidentes y la existencia de roles definidos para la gestión de la ciber-resiliencia. Esta información debe ser reportada por las entidades auditadas como parte de sus obligaciones de transparencia tecnológica.

Las políticas internas de seguridad de la información constituyen el marco normativo y operativo que permite a una organización proteger sus activos digitales, prevenir accesos no autorizados, garantizar la integridad de los datos y asegurar la disponibilidad de los sistemas. En el caso de la CGR, el fortalecimiento de estas políticas no solo tiene efectos sobre la protección de su propia información, sino que también define las condiciones bajo las cuales se ejecutan las auditorías digitales, se accede a plataformas externas y se resguarda la evidencia recolectada.

En la actualidad, la DIARI ha implementado una política operacional de gestión de la información basada en la norma ISO/IEC 27001[143], que incluye medidas de clasificación de información, control de accesos, trazabilidad documental, uso de criptografía, destrucción segura de información y protección contra *malware*[144]. Estas medidas han sido certificadas y se actualizan de forma regular, lo que sitúa a la CGR como una de las pocas entidades del Estado con un sistema de gestión de la seguridad de la información formalmente establecido.

Sin embargo, este esfuerzo debe ampliarse al conjunto de la entidad. Se recomienda elaborar una política institucional unificada de

---

143 International Organization for Standardization. *International Standard ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, cit.

144 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

seguridad de la información que sea de obligatorio cumplimiento para todas las dependencias, incluyendo unidades territoriales, delegadas sectoriales y áreas administrativas. Esta política debe contar con una unidad de seguimiento, un sistema de reportes y un modelo de indicadores para evaluar su implementación. Así mismo, debe contemplar un componente formativo que promueva la cultura de la ciberseguridad mediante campañas de sensibilización, capacitación a funcionarios, simulacros y espacios de intercambio de experiencias.

El blindaje institucional también requiere revisar y fortalecer los acuerdos de confidencialidad con proveedores tecnológicos, las cláusulas de protección de datos en los contratos y las condiciones de acceso remoto a los sistemas. En este sentido, la interoperabilidad debe ir acompañada de medidas de seguridad equivalentes entre las entidades que comparten información. La adopción de sistemas de autenticación robusta, la implementación de *firewalls* de nueva generación y el uso de tecnologías como *blockchain* para la trazabilidad de los procesos, son mecanismos que deben considerarse como parte de una estrategia integral de protección institucional.

El informe de gestión 2023-2024 de la Contraloría General de la República presenta avances sustanciales en materia de ciberseguridad, en especial mediante el fortalecimiento de la Dirección de Información, Análisis y Reacción Inmediata –DIARI–, unidad clave para la implementación de estrategias de vigilancia digital en el contexto del control fiscal. Entre los logros más destacados, se encuentra el desarrollo y consolidación del Sistema de Gestión de Seguridad de la Información –SGSI– y la Gestión Integral de Seguridad –GIS–, enmarcados dentro del Programa de Transformación Digital de la CGR, con apoyo del Banco Interamericano de Desarrollo –BID–.

Este programa permitió mejorar la infraestructura tecnológica y los sistemas de integración de información, así como establecer protocolos de respuesta ante crisis, continuidad operativa y ciberincidentes, con una orientación clara hacia la protección de los activos digitales institucionales. En términos de protocolos y controles técnicos, la CGR ha implementado mecanismos de respaldo, autenticación y trazabilidad a través del Sistema Integral de Infor-

mación de la Gestión Pública –SIIGEP– y de herramientas como el Sistema General de Advertencia Público –SIGAP–.

Este último fue clave para emitir diez advertencias entre junio de 2023 y mayo de 2024 sobre riesgos inminentes en entidades como la Agencia Nacional de Infraestructura –ANI–, el Instituto Colombiano de Bienestar Familiar –ICBF– o el Ministerio del Interior. Además, se destaca la articulación interinstitucional con ColCERT, la Policía Nacional y la Fiscalía en temas de ciberseguridad. Si bien la DIARI no reemplaza a estas entidades en funciones de ciberdefensa, sí coordina acciones técnicas y de respuesta temprana cuando se detectan vulnerabilidades en los sistemas de información de los sujetos vigilados. Esta función se sustenta en protocolos de alerta y en la generación de informes técnicos que son canalizados a las dependencias de TI de la CGR y, cuando es pertinente, a autoridades externas.

En conclusión, la Contraloría General de la República ha transitado hacia un modelo de vigilancia fiscal digital más robusto, en el que la ciberseguridad se consolida como un eje transversal. La implementación de modelos analíticos, sistemas de monitoreo automatizado y esquemas de inteligencia institucional han permitido prevenir el daño fiscal y mejorar la eficiencia del control. Aun así, el informe reconoce que persisten desafíos en interoperabilidad normativa, gestión del talento especializado y consolidación de una cultura organizacional enfocada en la ciber-resiliencia.

Las auditorías preventivas y las auditorías de tecnologías de la información –TI– son herramientas fundamentales para anticipar riesgos, identificar focos de vulnerabilidad y evitar que las irregularidades se traduzcan en daño fiscal. En el marco del control fiscal digital, estas auditorías permiten evaluar en tiempo real los comportamientos atípicos, verificar la calidad de los datos con los que se toman decisiones públicas y revisar la funcionalidad y seguridad de los sistemas que soportan la gestión institucional.

En el caso de la DIARI, estas auditorías han sido utilizadas con éxito en el seguimiento permanente a proyectos financiados con recursos del Sistema General de Regalías, en la verificación de la trazabilidad de la contratación pública y en el análisis de patrones de ejecución presupuestal. El uso de alertas automatizadas, tableros analíticos y

algoritmos de detección de fraude ha permitido a la CGR intervenir antes de que se materialice el detrimento patrimonial, redirigir auditorías y coordinar acciones con otras entidades del Estado[145].

Se propone ampliar la cobertura de estas auditorías mediante una política de auditoría preventiva digital que incluya criterios de selección con enfoque territorial, diferencial y temático. Esta política debe establecer mecanismos de priorización con base en mapas de riesgo digital, definir protocolos de revisión de sistemas críticos y estandarizar formatos de reporte que faciliten la toma de decisiones. Además, debe promover la participación ciudadana mediante la incorporación de mecanismos de control social digital, plataformas de denuncias y alianzas con veedurías comunitarias para validar la información recolectada.

También se recomienda fortalecer las auditorías de TI como una función autónoma dentro del modelo de control fiscal, dotando a la CGR de equipos especializados, herramientas propias y capacidad para evaluar desde el diseño los sistemas que soportan los procesos administrativos del Estado. Estas auditorías deben incluir pruebas de integridad de datos, validación de algoritmos, verificación de accesos y evaluación de plataformas interoperables. Solo así se podrá garantizar que la digitalización de la gestión pública se traduzca en mayor transparencia, eficiencia y legalidad.

145 Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, cit.

Conclusiones

El análisis detallado del ecosistema de ciberseguridad en Colombia, las capacidades institucionales de la Contraloría General de la República –CGR– y los avances alcanzados por la Dirección de Información, Análisis y Reacción Inmediata –DIARI–, permiten establecer una conclusión integral que reconoce tanto los logros como los desafíos estructurales de la vigilancia fiscal digital.

La CGR ha emprendido una transformación relevante hacia un modelo de control adaptado al entorno digital, mediante el uso de herramientas tecnológicas, análisis de datos masivos, seguimiento permanente y coordinación con organismos especializados en ciberdefensa. No obstante, el nuevo entorno global y nacional de amenazas cibernéticas plantea desafíos transversales que requieren una actualización urgente y continua de sus guías, metodologías y estándares de auditoría para garantizar que la vigilancia del gasto público no solo sea legal, sino también oportuna, eficiente, eficaz y económica.

La DIARI ha logrado consolidarse como una de las unidades más innovadoras dentro de la estructura de la CGR. Su papel ha trascendido el análisis de información técnica para convertirse en un núcleo operativo de inteligencia fiscal institucional. El despliegue de múltiples herramientas y los seguimientos permanentes ha permitido mejorar la trazabilidad de la ejecución del gasto y prevenir riesgos de daño fiscal. La incorporación de modelos analíticos predictivos, algoritmos de detección de comportamientos atípicos y sistemas de alertas tempranas ha sido fundamental para anticipar desviaciones y apoyar decisiones correctivas en tiempo real[146].

---

146 Ídem.

A pesar de estos logros, persisten retos importantes relacionados con su consolidación normativa, su autonomía operativa y su inserción sistémica en todos los procesos misionales de la CGR. La DIARI requiere fortalecer su capacidad para coordinar acciones tanto internas como externas, actuar en sinergia con ColCERT, la Policía Nacional, el MINTIC y la Fiscalía General de la Nación, y liderar procesos de actualización tecnológica sostenida, incluyendo capacidades en *blockchain*, inteligencia artificial explicable y visualización territorial avanzada.

Además, es imprescindible que la DIARI se convierta en el articulador de una cultura institucional orientada a la ciber-resiliencia, que promueva la formación continua de los servidores públicos en seguridad digital, la adopción de estándares de interoperabilidad segura y la integración de criterios de riesgo digital en los planes de vigilancia y control fiscal. En este marco, debe liderar la creación de metodologías propias para auditorías en entornos digitales y definir guías específicas para la intervención sobre sistemas críticos del Estado.

La ciberseguridad ya no puede ser vista como un asunto exclusivo del área de tecnologías de la información. En el contexto del control fiscal, debe ser reconocida como una dimensión transversal que condiciona la calidad del gasto, la transparencia institucional, la trazabilidad de los procesos y la confianza de la ciudadanía. La CGR debe participar activamente en la formulación de políticas públicas integradas de seguridad digital, con un enfoque orientado a la protección de infraestructuras críticas, la interoperabilidad normativa, la capacitación especializada y la actualización continua de las guías de auditoría[147].

Uno de los principales retos institucionales es adaptar los procedimientos, guías y metodologías de auditoría a las condiciones del entorno digital. Las auditorías convencionales, centradas en expedientes físicos y visitas presenciales, son insuficientes para intervenir sobre plataformas tecnológicas, algoritmos de contratación automatizada, sistemas interoperables o infraestructuras digitales

147 ISACA. *State of Cybersecurity 2021, Part 1: Global Update on Workforce*, cit.

que operan con base en inteligencia artificial. Por tanto, se requiere rediseñar los enfoques de auditoría para incorporar elementos como análisis forense digital, revisión de *logs*, simulaciones de ciberataques, validación de algoritmos de decisión y trazabilidad de datos en tiempo real.

De igual forma, la aplicación de los principios constitucionales del control fiscal –eficiencia, eficacia, economía, equidad y valoración de costos ambientales– debe ser reinterpretada a la luz de la transformación digital. La eficiencia ya no solo implica hacer más con menos, sino hacerlo con mejor capacidad de anticipación; la eficacia se traduce en prevenir, no solo sancionar; la economía exige priorizar intervenciones sobre sectores de alto riesgo digital y la equidad demanda garantizar que todos los ciudadanos –sin importar su ubicación o nivel de conectividad– tengan acceso a sistemas públicos protegidos contra amenazas digitales.

En este contexto, la CGR debe liderar un cambio metodológico que permita que la auditoría digital sea no solo una herramienta técnica, sino también una política pública orientada al fortalecimiento de la democracia. Esto implica elaborar un nuevo Plan Nacional de Vigilancia Fiscal Digital, formular normas técnicas específicas sobre auditorías en entornos de datos masivos, generar espacios de formación interinstitucional y establecer mecanismos de participación ciudadana para la vigilancia digital colaborativa.

La ciberseguridad ha dejado de ser un componente accesorio para convertirse en un eje estructural del control fiscal moderno. La CGR, con la DIARI como núcleo técnico, ha logrado avances significativos en este campo, pero su proyección futura dependerá de su capacidad para liderar una transformación profunda de sus modelos de auditoría, sus capacidades tecnológicas, su cultura institucional y su articulación con las políticas públicas nacionales de seguridad digital. Solo mediante este proceso será posible garantizar un control fiscal que esté a la altura de los desafíos tecnológicos del siglo XXI.

Referencias

Acemoglu, Daron y Simon Johnson. *Poder y progreso: nuestra lucha milenaria por la tecnología y la prosperidad*, México, D. F., Crítica, 2023.

Acto legislativo 04 de 18 de septiembre de 2019, "Por medio del cual se reforma el Régimen de Control Fiscal", *Diario Oficial* n.° 51.080, del 18 de septiembre de 2019, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=30038092].

Alderete, María Verónica y Carola Jones. "Estrategias de tic en empresas de Córdoba, Argentina: un modelo estructural", *SaberEs*, vol. 11, n.° 2, 2019, pp. 195 a 216, disponible en [https://saberes.unr.edu.ar/index.php/revista/article/view/203].

Amerise, Atahualpa. "'Estamos en guerra': 5 claves para entender el ciberataque que tiene a Costa Rica en estado de emergencia", *bbc News Mundo*, 20 de mayo de 2022, disponible en [https://www.bbc.com/mundo/noticias-america-latina-61516874].

Angarita, Jenny. "Fiscalía sigue investigando hackeo de información clave judicial", *W Radio*, 4 de noviembre de 2022, disponible en [https://www.wradio.com.co/2022/11/04/fiscalia-sigue-investigando-hackeo-de-informacion-clave-judicial/].

Banco Mundial. "La digitalización mundial en 10 gráficos", disponible en [https://www.bancomundial.org/es/news/immersive-story/2024/03/05/global-digitalization-in-10-charts].

Banco Mundial. "Se frenan los avances mundiales en la reducción de la pobreza extrema", comunicado de prensa n.° 2023/011/efi, Washington, D. C., 5 de octubre de 2022, disponible en [https://www.bancomundial.org/es/news/press-release/2022/10/05/global-progress-in-reducing-extreme-poverty-grinds-to-a-halt].

Bauman, Zygmunt y Keith Tester. *La ambivalencia de la modernidad y otras conversaciones*, Barcelona, Paidós, 2011.

Bodeau, Deb y Richard Graubart. *Cyber Resiliency and nist Special Publication 800-53 Rev.4 Controls*, mitre Technical Report mtr130531, Bedford, MA, The mitre Corporation, 2013, disponible en [https://www.mitre.org/sites/default/files/publications/13-4047.pdf].

Bueno Castellanos, Carmen. "Trayectorias que ilustran la confluencia entre actividades formales e informales", en Roberto Horta (coord.). *El futuro del empleo post pandemia del covid-19*, Cuadernos Orkestra, n.° 10/2022, España, Instituto Vasco de Competitividad - Fundación Deusto, 2022, pp. 47 a 61, disponible en [https://www.orkestra.deusto.es/images/investigacion/publicaciones/informes/cuadernos-orkestra/220085-El-futuro-del_empleo-post-pandemia-del-covid-19-COMPLETO.pdf].

Cano M., Jeimy J. "De los incidentes de seguridad en la gestión de la protección de datos personales y la Industria 4.0", en *v Congreso Internacional de Protección de Datos Personales*, Bogotá, Superintendencia de Industria y Comercio, 8 y 9 de junio de 2017.

Carr, Nicholas G. *Atrapados: cómo las maquinas se apoderan de nuestras vidas*, Buenos Aires, Taurus, 2014.

Carr, Nicholas G. *Superficiales: ¿qué está haciendo internet con nuestras mentes?*, Madrid, Taurus, 2017.

Castells, Manuel. *Comunicación y poder*, México, D. F., Siglo xxi, 2009.

Castells, Manuel. *La era de la información: economía, sociedad y cultura, vol. 1: La sociedad red*, Madrid, Alianza, 2017.

Centro Cibernético Policial. *Boletín estadístico de delitos informáticos*, Policía Nacional de Colombia, 2022.

Coeckelbergh, Mark. *Ética de la inteligencia artificial*, Madrid, Cátedra, 2021.

Coeckelbergh, Mark. *La filosofía política de la inteligencia artificial: una introducción*, Madrid, Cátedra, 2023.

Collier, Kevin y Ben Goggin. "Messaging app seen in use by Mike Waltz suspends service after hackers claim breach", *nbc News*, 5 de mayo de 2025, disponible en [https://www.nbcnews.com/tech/security/telemessage-suspends-services-hackers-say-breached-app-rcna204925].

Contraloría General de la República. *Informe de gestión 2020-2021 al Congreso y al Presidente de la República "Una Contraloría para todos"*, Bogotá, cgr, 2021, disponible en [https://www.camara.gov.co/sites/default/files/2021-08/5.1%20Informe.pdf].

Contraloría General de la República. *Informe especial sobre recursos covid-19*, Bogotá, cgr, 2021.

Contraloría General de la República. *Plan Estratégico Institucional 2022-2026*, Bogotá, cgr, 2022.

Contraloría General de la República. *Resultados del Sistema saga y control fiscal en tiempo real*, Bogotá, cgr, 2022.

Contraloría General de la República. "Políticas operativas de seguridad de la información en la operación de los procesos Gestión de información y Análisis de información en la diari", código: rsc 02 PO 001, Sistema de Gestión y Control Interno –sigeci–, 29 de junio de 2022.

Contraloría General de la República. *Informe de gestión 2023-2024 al Congreso y al Presidente de la República "Una Contraloría con independencia para el cambio"*, Bogotá, cgr, 2024, disponible en [https://www.camara.gov.co/sites/default/files/2024-12/CGR-informe-de-gestion-2023-2024.pdf].

Coparmex. "Grave y preocupante el hackeo a la sadena", 2023, disponible en [https://coparmex.org.mx/downloads/ENVIOS/SC_030_Newsletter.pdf].

David, Paul A. y Dominique Foray. "Una introducción a la economía y a la sociedad del saber", *Revista Internacional de Ciencias Sociales*, n.° 171: La sociedad del conocimiento, 2002, disponible en [https://unesdoc.unesco.org/ark:/48223/pf0000125502_spa].

Davidovsky, Sebastián. "Cómo fue el ciberataque al sitio Argentina.gob.ar, el último de una larga serie de ataques a organismos estatales", *La Nación*, 26 de diciembre de 2024, disponible en [https://www.lanacion.com.ar/tecnologia/como-fue-el-ciberataque-al-sitio-de-mi-argentina-el-ultimo-de-una-larga-serie-de-ataques-a-nid26122024].

DE MIGUEL, RAFA. "Un ciberataque obliga a Irlanda a cerrar el sistema informático de la sanidad pública", *El País*, Londres, 14 de mayo de 2021, disponible en [https://elpais.com/internacional/2021-05-14/un-ataque-cibernetico-en-irlanda-obliga-a-cerrar-el-sistema-informatico-de-la-sanidad-publica.html].

DEBORD, GUY. *La sociedad del espectáculo*, 2.ª ed., Valencia, Edit. Pre-Textos, 2005.

Decreto 2037 de 23 de octubre de 2019, "Por el cual se desarrolla la estructura de la Contraloría General de la República, se crea la Dirección de Información, Análisis y Reacción Inmediata y otras dependencias requeridas para el funcionamiento de la Entidad", *Diario Oficial* n.° 51.130, del 7 de noviembre de 2019, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30038323].

Decreto 403 de 16 de marzo de 2020, "Por el cual se dictan normas para la correcta implementación del Acto Legislativo 04 de 2019 y el fortalecimiento del control fiscal", *Diario Oficial* n.° 51.258, del 16 de marzo de 2020, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=30038961].

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA. "Encuesta de las Tecnologías de la Información y las Comunicaciones en hogares - ENTIC Hogares 2020" (Boletín Técnico), Bogotá, DANE, 14 de septiembre de 2021, disponible en [https://colombiatic.mintic.gov.co/679/articles-198835_bol_entic_hogares_2020.pdf].

DEPARTAMENTO ADMINISTRATIVO NACIONAL DE ESTADÍSTICA. "Encuesta de las Tecnologías de la Información y las Comunicaciones en hogares - ENTIC Hogares 2021" (Boletín Técnico), Bogotá, DANE, 28 de julio de 2022, disponible en [https://www.dane.gov.co/files/investigaciones/boletines/entic/bol_entic_hogares_2021.pdf].

DEPARTAMENTO NACIONAL DE PLANEACIÓN. *Documento CONPES 3701 "Lineamientos de política para la ciberseguridad y la ciberdefensa"*, Bogotá, DNP, julio de 2011, disponible en [https://colaboracion.dnp.gov.co/CDT/Conpes/Económicos/3701.pdf].

Departamento Nacional de Planeación. *Estrategia Nacional Digital de Colombia 2023 - 2026*, Bogotá, dnp, s. f., disponible en [https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/EVENTOS/END_Colombia_2023_2026.pdf].

Diamond, Jared M. *Armas, gérmenes y acero: breve historia de la humanidad en los últimos trece mil años*, Barcelona, Barcelona, Debate, 2018.

Diazgranados, Hernán. "Empresas: principal objetivo de ciberataques en América Latina", *Kaspersky*, 1.° de octubre de 2020, disponible en [https://latam.kaspersky.com/blog/empresas-principal-objetivo-de-ciberataques-en-america-latina/20209/].

Diéguez, Antonio. *Cuerpos inadecuados: el desafío transhumanista a la filosofía*, Barcelona, Herder, 2021.

Drucker, Peter F. *La sociedad poscapitalista*, Buenos Aires, Edit. Sudamericana, 2013.

Eco, Umberto. *Apocalípticos e integrados*, Barcelona, De Bolsillo, 2016.

Equipo TicTac. *Estudio trimestral de ciberseguridad: ataques a entidades de gobierno*, Bogotá, 2022, disponible en [https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf].

esg innova Group. "Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad", 1.° de febrero de 2018, disponible en [https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/].

Fanelli, Maxi. "Informe global de ciberataques del primer trimestre de 2025 de Check Point Software", *ITSitio*, 23 de abril de 2025, disponible en [https://www.itsitio.com/seguridad/informe-global-de-ciberataques-del-primer-trimestre-de-2025-de-check-point-software/].

Fisher, Max. *Las redes del caos: la historia secreta de cómo las redes sociales empobrecen la mente y erosionan el mundo*, Barcelona, Crítica, 2023.

Forbes Staff. "Hackeo masivo a Sedena evidencia vulnerabilidad de ciberseguridad; así fue el ataque", *Forbes México*, 30 de septiembre de 2022, disponible en [https://forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/].

Fortinet. *Informe global del panorama de amenazas. Un informe semestral de FortiGuard Labs*, febrero de 2023, disponible en [https://www.fortinet.com/lat/demand/gated/threat-report-2h-2022].

Foucault, Michel. *Vigilar y castigar: el nacimiento de la prisión*, México, D. F., Siglo xxi, 2018.

Fourest, Caroline. *Generación ofendida: de la política cultural a la política del pensamiento*, Barcelona, Península, 2021.

gse. *Primera encuesta sobre seguridad digital en Colombia*, Bogotá, 2025, disponible en [https://urosario.edu.co/sites/default/files/2025-02/estudio-seguridad-digital-infografia.pdf].

Gutiérrez Núñez, Allison. "epm y Afinia, entre las compañías que han sido víctimas de ciberataques", *La República*, 17 de diciembre de 2022, disponible en [https://www.larepublica.co/empresas/epm-y-afinia-entre-las-companias-que-han-sido-victimas-de-ciberataques-en-el-ano-3510742].

Han, Byung-Chul. *En el enjambre*, Barcelona, Herder, 2014.

Han, Byung-Chul. *Infocracia: la digitalización y la crisis de la democracia*, Madrid, Taurus, 2022.

Harari, Yuval Noah. *Sapiens: de animales a dioses*, Barcelona, Debate, 2017.

Harari, Yuval Noah. *Nexus: una breve historia de las redes de información desde la Edad de Piedra hasta la IA*, Barcelona, Debate, 2024.

Hawthorne, Nathaniel. *La letra escarlata*, Penguin Clásicos, 2015.

Hine, Cristhine. *Etnografía virtual*, Barcelona, Edit. uoc, 2004.

Housel, Morgan. *La psicología del dinero: 18 claves imperecederas sobre riqueza y felicidad*, México, D. F., Paidós, 2024.

Infobae. "Hackers tendrían 'secuestrada' información de la Fiscalía de Colombia: más de 10 teras de datos habrían sido hurtados", *Infobae*, 11 de noviembre de 2022, disponible en [https://www.infobae.com/america/colombia/2022/11/11/hackers-tendrian-secuestrada-informacion-de-la-fiscalia-de-colombia-mas-de-10-teras-de-datos-habrian-sido-hurtados].

Innerarity, Daniel. *La sociedad del desconocimiento*, Barcelona, Galaxia Gutenberg, 2022.

International Organization for Standardization. *International Standard iso/iec 27001:2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements*, 3.ª ed., iso, 2022.

isaca. *State of Cybersecurity 2021, Part 1: Global Update on Workforce*, isaca, 2021.

Jácome Álvarez, Orfa de J. "Las tecnologías emergentes en la sociedad del aprendizaje", *Revista Científica Hallazgos 21*, vol. 6, n.° 1, 2021, pp. 101 a 110, disponible en [https://revistas.pucese.edu.ec/hallazgos21/article/view/511].

Kaspersky. "¿Qué es la ciberseguridad?", disponible en [https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security?srsltid=AfmBOoonPijhYIUQrnAZVNSHuCWGjW_APukiD87XLP3umEYc3XamCIBn].

Kemp, Simon. "Digital 2021: Global Overview Report", *Datareportal*, 27 de enero de 2021, disponible en [https://datareportal.com/reports/digital-2021-global-overview-report].

Latorre Iglesias, Edimer Leonardo; Katherine Paola Castro Molina e Iván Darío Potes Comas. *Las tic, las tac y las tep: innovación educativa en la era conceptual*, Bogotá, Universidad Sergio Arboleda, 2018, disponible en [https://repository.usergioarboleda.edu.co/bitstream/handle/11232/1219/TIC%20TAC%20TEP.pdf?sequence=1].

Lesmes, Laura. "Keralty, la nueva víctima de los ataques de 'ransomware'", *El Tiempo*, 4 de diciembre de 2022, disponible en [https://www.eltiempo.com/tecnosfera/novedades-tecnologia/keralty-detalles-del-ataque-de-ransomware-a-eps-sanitas-723175].

Ley 42 de 26 de enero de 1993, "Sobre la organización del sistema de control fiscal financiero y los organismos que lo ejercen", *Diario Oficial* n.° 40.732, del 27 de enero de 1993, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=1788293].

Ley 1273 de 5 de enero de 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", *Diario Oficial* n.° 47.223, del 5 de enero de 2009, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1676699].

Ley 1474 de 12 de julio de 2011, "Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública", *Diario Oficial* n.° 48.128, del 12 de julio de 2011, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=1681594].

Ley 1581 de 17 de octubre de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", *Diario Oficial* n.° 48.587, del 18 de octubre de 2012, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507].

Ley 1621 de 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones", *Diario Oficial* n.° 48.764, del 17 de abril de 2013, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1685400].

Ley 2195 de 18 de enero de 2022, "Por medio de la cual se adoptan medidas en materia de transparencia, prevención y lucha contra la corrupción y se dictan otras disposiciones", *Diario Oficial* n.° 51.921, del 18 de enero de 2022, disponible en [https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043772].

MacLuhan, Marshall y Quentin Fiore. *El medio es el masaje: un inventario de efectos*, Barcelona, Paidós, 1969.

Mariño Espinosa, Lilian. "Ataque cibernético que epm sufrió esta semana se dio desde la Central de Ituango", *La República*, 16 de diciembre de 2022, disponible en [https://www.larepublica.co/empresas/ataque-cibernetico-que-epm-sufrio-esta-semana-se-dio-desde-la-central-de-ituango-3510139].

Mauss, Marcel. *Sociología y antropología*, Madrid, Tecnos, 1991.

Mendizábal Bermúdez, Gabriela y Ana Esther Escalante Ferrer. "El reto de la educación 4.0: competencias laborales para el trabajo emergente por la covid-19", *ricsh Revista Iberoamericana de las Ciencias Sociales y Humanísticas*, vol. 10, n.° 19, 2021, pp. 261 a 283, disponible en [https://www.ricsh.org.mx/index.php/RICSH/article/view/242].

Mercado, David Alejandro. "Medellín: Este es el grupo que se adjudicó el ataque cibernético a epm", *El Tiempo*, 27 de diciembre de 2022, disponible en [https://www.eltiempo.com/colombia/medellin/blackcat-el-grupo-que-se-adjudico-el-ataque-cibernetico-a-epm-729363].

Ministerio de Tecnologías de la Información y las Comunicaciones. "Gobierno nacional atiende ataque cibernético que afecta a varias entidades e instala pmu ciber", 13 de septiembre de 2023, disponible en [https://www.mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/278831:Gobierno-Nacional-atiende-ataque-cibernetico-que-afecta-a-varias-entidades-e-instala-PMU-CIBER].

Organización para la Cooperación y el Desarrollo Económicos. *Revisión del gobierno digital en Colombia: hacia un sector público impulsado por el ciudadano*, París, ocde, 2018, disponible en [https://www.oecd.org/es/publications/revision-del-gobierno-digital-en-colombia_9789264292147-es.html].

Redacción Judicial. "Hackeo a la Fiscalía: detalles inéditos de una filtración sin precedentes", *El Espectador*, 6 de noviembre de 2022, disponible en [https://www.elespectador.com/judicial/los-archivos-secretos-del-hackeo-a-la-fiscalia].

Redacción Radio San Sebastián. "ziur alerta del 'drástico aumento' de ciberataques contra entidades españolas", *Sociedad Española de Radiodifusión*, 15 de mayo de 2025, disponible en [https://cadenaser.com/euskadi/2025/05/15/ziur-alerta-del-drastico-aumento-de-ciberataques-contra-entidades-espanolas-radio-san-sebastian/].

Redacción Semana. "Acceso a internet en Colombia se aceleró durante la pandemia", *Semana*, 9 de febrero de 2021, disponible en [https://www.semana.com/economia/empresas/articulo/acceso-a-internet-en-colombia-se-acelero-durante-la-pandemia/202108/].

Roa Avella, Marcela del Pilar; Jesús E. Sanabria Moyano y Katherin Dinas Hurtado. Uso del algoritmo compas en el proceso penal y los riesgos a los derechos humanos", *Revista Brasileira de Direito Processual Penal*, vol. 8, n.° 1, 2022, pp. 275 a 310, disponible en [https://revista.ibraspp.com.br/RBDPP/article/view/615].

Rochel Galeano, Kiara K. "Ciberataque a proveedor de servicios de Entidades Públicas", Asociación Nacional de Comercio Exterior –analdex–, 2023, disponible en [https://analdex.org/2023/09/18/ciberataque-a-proveedor-de-servicios-de-entidades-publicas/].

Sachs, Jeffrey D. *Las edades de la globalización: geografía, tecnologías e instituciones*, Barcelona, Deusto, 2021.

Shelley, Mary. *Frankenstein o el moderno Prometeo*, México, Gran Travesía, 2023.

SonicWall. *2021 SonicWall Cyber Threat Report*, 2021, disponible en [https://www.sonicwall.com/resources/white-papers/2021-sonicwall-cyber-threat-report].

Syal, Rajeev. "Legal aid hack: data from hundreds of thousands of people accessed, says MoJ", *The Guardian*, 19 de mayo de 2025, disponible en [https://www.theguardian.com/law/2025/may/19/significant-amount-of-personal-data-accessed-in-legal-aid-agency-data-breach-says-moj].

Toffler, Alvin. *El shock del futuro*, Barcelona, Plaza y Janes, 1981.

Unidad de Salud. "eps Sanitas: ciberataque vulneró datos de 241.589 usuarios, según Supersalud", *El Tiempo*, 26 de enero de 2023, disponible en [https://www.eltiempo.com/salud/eps-sanitas-ciberataque-vulnero-datos-de-241-589-usuarios-736961].

Valoyes Mosquera, Amancio. "Ciberseguridad en Colombia" (artículo de posgrado), Especialización en Seguridad Informática, Bogotá, Universidad Piloto de Colombia, 2019, disponible en [https://repository.unipiloto.edu.co/handle/20.500.12277/6370].

Vicens, A. J. y Raphael Satter. "Exclusive: Hacker who breached communications app used by Trump aide stole data from across US government", *Reuters*, 21 de mayo de 2025, disponible en [https://www.reuters.com/world/us/hacker-who-breached-communications-app-used-by-trump-aide-stole-data-across-us-2025-05-21].

Villanueva, Djenane. "Ataques cibernéticos repercuten en las finanzas de la Hacienda Pública en Costa Rica, según órgano fiscalizador", *cnn en Español*, 20 de julio de 2023, disponible en [https://cnnespanol.cnn.com/2023/07/20/ataques-ciberneticos-finanzas-hacienda-publica-costa-rica-orix].

Weller, Jürgen. *La pandemia del covid-19 y su efecto en las tendencias de los mercados laborales*, Santiago de Chile, Naciones Unidas, 2020, disponible en [https://repositorio.cepal.org/entities/publication/7bc229c9-c274-4208-b4a7-8581b42d68d3].

La autora

Abogada, con Especialización y Maestría en Derechos de Autor y Propiedad Intelectual de la Universidad Carlos III de Madrid, España. Maestría en Innovación y *Legal Tech* de la Universidad Sergio Arboleda. Más de 20 años en el sector público y privado en el área de propiedad intelectual, telecomunicaciones y jurídica a nivel directivo, gerenciando proyectos de impacto nacional e internacional con excelentes habilidades de liderazgo, dirección de equipos de trabajo y toma de decisiones estratégicas, orientada a resultados, con alta capacidad de análisis, recursiva, con excelentes relaciones interpersonales y públicas. Se desempeña actualmente como Contralora Delegada Intersectorial de la Contraloría General de la República.

E-mail [pao_velez@hotmail.com]

ORCID [https://orcid.org/0009-0007-7143-9415]

Editado por el Instituto Latinoamericano de Altos Estudios –ILAE–,
en junio de 2025

Se compuso en caracteres Cambria de 12 y 9 ptos.

Bogotá, Colombia