DIGIntegridad

La transformación digital de la lucha contra la corrupción

CAF BANCO DE DESARROLLO DE AMÉRICA LATINA

Título: DIGIntegridad: La transformación digital de la lucha contra la corrupción

Depósito Legal: DC2022000457

SBN: 978-980-422-263-4

Editor: CAF

Responsables de la edición: Camilo Cetina y Carlos Santiso, Gerencia de Infraestructura Física y Transformación Digital.
Gerente de Infraestructura Física y Transformación Digital, Antonio Silveira

Elaborado bajo la dirección de Carlos Santiso, anteriormente responsable de la Dirección de Innovación Digital del Estado y Claudia Flores, directora (E) de Transformación Digital.

La coordinación, edición y elaboración de los capítulos estuvo a cargo de Camilo Cetina, ejecutivo principal y líder en integridad pública de la Dirección de Transformación Digital en CAF. Con el apoyo de: Paula Cruz Manrique como asistente de investigación y Maffert Lizcano, pasante CAF.

Coordinación de la publicación: Nathalie Gerbasi, directora (E) de Capacitación.

Las ideas y planteamientos contenidos en la presente edición son de exclusiva responsabilidad de sus autores y no comprometen la posición oficial de CAF.

Diseño gráfico: Gastón Cleiman

Fotografía de portada: 12 Best Social Media Stocks To Buy Now, Almario, 2021.
Otras fotografías de la publicación: pexels.com y unsplash.com

Esta y otras publicaciones sobre Transformación Digital en: scioteca.caf.com

RECONOCIMIENTOS

Este informe ha sido elaborado bajo la guía y supervisión de Carlos Santiso, anteriormente responsable de la Dirección Innovación Digital del Estado y Claudia Flores, directora (E) de la Dirección Transformación Digital, adscrita a la Gerencia de Infraestructura Física y Transformación Digital de CAF –banco de desarrollo de América Latina. La coordinación, consolidación y redacción del reporte estuvo a cargo de Camilo Cetina, ejecutivo principal y líder de la agenda de integridad pública de CAF.

El presente informe se basa en un conjunto de estudios realizados específicamente para este proyecto. CAF agradece a las personas mencionadas a continuación la riqueza de sus reflexiones y análisis, así como los comentarios y precisiones aportados a la redacción de cada capítulo.

Capítulo 1: elaborado por Camilo Cetina, con la asistencia de Paula Cruz Manrique.

Capítulo 2: **sección 2.1**, elaborada por Gustavo Fajardo y Jorge Gallego.
sección 2.2, elaborada por Camilo Cetina, con los insumos de Ana María Niño Ardila.
sección 2.3, elaborada por Gustavo Fajardo, Jorge Gallego y Camilo Cetina.

Capítulos 3, 4 y 6: elaborados por Camilo Cetina, con la asistencia de Paula Cruz Manrique. La sección 3.2.3 está basada en el trabajo de Cetina, Garay Salamanca, Salcedo-Albarán y Vanegas (2021).

Capítulo 5: elaborado por Camilo Cetina, con los insumos de Erick Rincón Cárdenas y la asistencia de Paula Cruz Manrique.

También, agradecemos al siguiente equipo de especialistas de CAF por su valiosa revisión y comentarios para mejorar el documento: Pablo Sanguinetti, anteriormente Vicepresidente de Conocimiento; Andrés Zamora y Martha Eloína Hernández, de la Dirección de Comunicación Estratégica; María Isabel Mejía, Nathalie Gerbasi y Enrique Zapata, de la Dirección de Transformación Digital; Anabella Abadi, de la Dirección de Evaluación de Impacto y Aprendizaje de Políticas, y Gustavo Fajardo, de la Dirección de Investigaciones Socioeconómicas. La coordinación de la publicación estuvo a cargo de Nathalie Gerbasi, con el apoyo de Lorena López y Maffert Lizcano, de la Dirección de Transformación Digital.

ÍNDICE

INTRODUCCIÓN

Los escándalos de corrupción sin precedentes en América Latina, conocidos en la última década, sugieren que la región se enfrenta a un fenómeno de macrocooptación institucional (Garay, Salcedo-Albarán y Macías, 2018; Garay y Salcedo-Albarán, 2021). Esto quiere decir que existe una coordinación entre agentes de los sectores privado y público para controlar la provisión de bienes y servicios del Estado, así como sus instituciones y normas. La lucha contra la corrupción y la impunidad de sus redes criminales es parte fundamental de la agenda de desarrollo, que busca acabar con la pobreza, reducir las extremas desigualdades y, en el contexto pospandemia, facilitar la reactivación económica.

La corrupción –entendida como el abuso de un poder encomendado para beneficio privado– le podría estar costando al planeta, según varias estimaciones, entre el 2 % y el 5 % del Producto Interno Bruto (PIB) mundial (CAF, 2019; ONU, 2018), con efectos adversos tanto en el funcionamiento de la democracia como en la economía de mercado. El Foro Económico Mundial (FEM, 2019) estima un costo al mundo en desarrollo de USD 1,26 billones al año, monto equivalente a 7,5 veces la ayuda anual al desarrollo, de acuerdo con los datos de la OCDE (2019d). Transparencia Internacional (2021) documentó incluso el posible efecto que tiene la corrupción sobre el deterioro de las democracias y la violación de derechos humanos.

De modo paralelo, el mundo es testigo de la aceleración digital de las economías, los Gobiernos y las sociedades. La digitalización comporta efectos positivos a la economía: Naciones Unidas estima que el sector de las Tecnologías de Información y Comunicaciones (TIC) emplea a un 2 % de la población mundial, representa un capital suscrito (solo en plataformas) que supera los USD 7 billones, y puede contribuir con un 15 % del PIB mundial (UNCTAD, 2019). Sin embargo, la revolución digital, aparejada a la globalización de la economía, también les cede espacio a las redes de corrupción para crecer en tamaño y capacidad de daño, puesto que, al usar el ciberespacio, operan sin territorialidad alguna y limitan las capacidades jurisdiccionales para su detección y sanción por parte de los Gobiernos (Shelley, 1998).

De hecho, Transparencia Internacional (2021) ha acuñado el concepto de **«formas modernas de corrupción»**, en el cual vincula dos tipos de fenómenos: (i) los que tienen una naturaleza transnacional, y (ii) aquellos que requieren del uso de tecnología para adquirir, mover o disponer ilícitamente de los activos obtenidos tras la comisión de los delitos. Casos famosos como Lava Jato, Odebrecht, Panamá Papers y FIFA-Gate, entre otros, son ejemplos de estas formas modernas de corrupción. El avance de la digitalización de las economías y las telecomunicaciones aumenta todavía más el potencial para que las redes de corrupción operen a escala global, identifiquen nuevos mecanismos

de cooperación y acumulen enormes ganancias obtenidas a través de operaciones transnacionales. Esto, simultáneamente, aumenta su capacidad para reorganizarse y ocultarse entre cantidades incontables de datos, en medio de las plataformas tecnológicas que movilizan dinero alrededor del mundo.

Sorprendentemente, la literatura que vincula la revolución digital con el control de la corrupción aún es incipiente (Haafst, 2017). Sin embargo, desde la década pasada, los Gobiernos y otros actores del ecosistema digital han comenzado a **documentar experiencias** sobre el potencial y el impacto de la digitalización para promover la transparencia, abrir los datos gubernamentales al escrutinio público, automatizar los procesos burocráticos, restringir la discreción de los funcionarios y limitar la interacción de los ciudadanos con los funcionarios públicos para acceder a servicios esenciales.

En ese sentido, este informe busca contribuir al estado del arte que vincula los conceptos de digitalización e integridad, y propone una estructura de política pública basada en la adopción de innovaciones digitales para la prevención, detección e investigación de fenómenos de corrupción. La irrupción de la tecnología en el espacio de la integridad tiene, por lo menos, tres grandes mecanismos de acción:

1. A través de la expansión del acceso a la información y la apertura de datos, los ciudadanos tienen mayor información sobre sus derechos en la interacción con sus Gobiernos[1].

2. El avance del gobierno digital permite la simplificación de los procesos administrativos, y la racionalización de la política regulatoria y las infraestructuras de datos abiertos. Al reducir la burocracia, la digitalización de los trámites reduce la discreción y, por lo tanto, las oportunidades de soborno.

3. El uso de técnicas de análisis de datos como dispositivos anticorrupción por parte de los actores de la integridad dentro y fuera del Gobierno permite adoptar un enfoque proactivo y predictivo para la gestión de riesgos de corrupción sistémica (Cetina, 2020; Santiso, 2021).

El potencial que ofrece la digitalización en materia de integridad pública es reconocido en varios escenarios internacionales que buscan influir en esta agenda alrededor del mundo. En 2018, el Foro Económico Mundial lanzó la iniciativa **Tech4integrity**, que sirve como un mercado global de innovaciones tecnológicas para la integridad. En 2019, el **Foro Global Anticorrupción e Integridad de la OCDE** (Organización para la Cooperación y el Desarrollo Económicos) estuvo dedicado a examinar el potencial de las tecnologías digitales como blockchain (cadena de bloques), inteligencia artificial y datos abier-

[1] Este no es un problema menor: por ejemplo, en 2019, solo el pequeño soborno le costó a la economía mexicana USD 650 millones, según la agencia de estadísticas (Santiso, 2021).

tos para un amplio rango de temas que van desde la prevención del soborno hasta la protección de los denunciantes; la OCDE acuñó así el término «Dig-integrity». En 2020, el Banco Mundial, a través de la iniciativa **T4I**, siguió promoviendo la expansión de tecnologías digitales dentro de los Gobiernos que quieren adoptar mejores políticas de integridad y lucha contra la corrupción. Finalmente, en 2021, se desarrolló la **Sesión Especial** de la Asamblea General de la ONU contra la Corrupción, donde se **respaldó de modo explícito el uso de tecnologías digitales** para facilitar el acceso a la información, promover la rendición de cuentas y prevenir riesgos que van desde el conflicto de interés hasta el lavado de activos.

A pesar de la notable conciencia que surge alrededor del mundo sobre el nexo entre aceleración digital y políticas de integridad pública, **aún no existe una guía integral para que los Gobiernos adopten mecanismos de lucha contra la corrupción con un enfoque de innovación digital. El presente informe busca llenar ese vacío**, de modo que las autoridades públicas y otros actores del ecosistema de integridad puedan identificar el modo que más se ajuste a las necesidades para formular e implementar exitosamente una agenda anticorrupción tipo DIGIntegridad o T4I (Santiso, 2020), mediante la combinación de seis componentes esenciales, como se detalla a continuación:

- Los conceptos de transparencia activa y datos abiertos como habilitadores para que cualquier forma de desarrollo digital opere con éxito en el ecosistema de integridad y lucha contra la corrupción. El capítulo 1 aborda el derecho de acceso a la información pública y los conjuntos de datos que componen dicha información, así como condiciones técnicas e institucionales para que los Gobiernos incorporen componentes digitales en las políticas de integridad pública.

- El gobierno digital y la transformación digital del Estado. El capítulo 2 reconoce que la digitalización de los servicios que el Gobierno ofrece a la ciudadanía precede a la de procesos más sofisticados, como investigación y sanción de la corrupción. En particular, esta sección muestra cómo los mayores niveles de digitalización de los Gobiernos se correlacionan con menores riesgos de corrupción. Igualmente, documenta, cuantitativa y cualitativamente, el desarrollo de dicha relación en los aspectos específicos del gobierno digital que afectan el gasto público y la confianza ciudadana.

- Desarrollo de las principales técnicas de reutilización de los datos para la lucha contra la corrupción. El capítulo 3 considera que la articulación de políticas de gobierno digital con las de transparencia y datos abiertos genera un ecosistema que reutiliza los datos y aplica con éxito la ciencia de datos y la inteligencia artificial en la prevención e investigación de fenómenos de corrupción. Dicho ecosistema ha mostrado resultados desde varios actores: sociedad civil, organismos de control, agencias de compra pública y sector privado, los cuales se documentan en esta sección.

- Usos de tecnologías disruptivas como el blockchain en materia de integridad. A pesar de la controversia alrededor de dicha innovación tecnológica, el capítulo 4 documenta usos del *blockchain* que, en calidad de prueba de concepto, muestran un potencial para reducir riesgos de corrupción en procesos específicos y especialmente vulnerables, como la contratación pública, las entregas condicionadas de efectivo y el abastecimiento de las vacunas contra el coronavirus. De nuevo, hay un orden que precede a esta tecnología: la aplicación de ciencia de datos permite a los Gobiernos desarrollar infraestructuras digitales (capítulo 3), lo cual posibilita la inversión en gran poder de cómputo. Este último es una condición –casi que una infraestructura– para el adecuado funcionamiento de la tecnología *blockchain*.

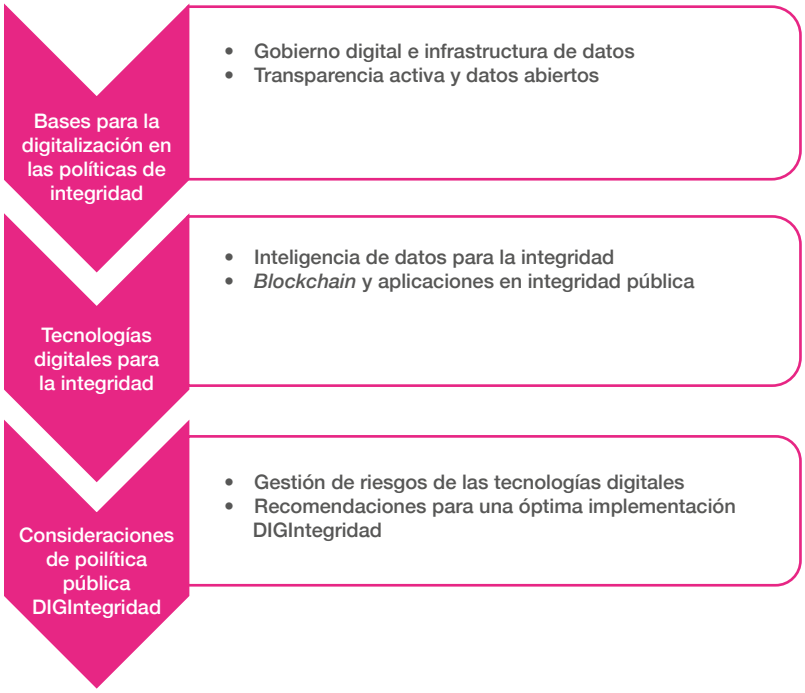
- Gestión de riesgos tecnológicos. El capítulo 5 reconoce que, aunque la adopción de tecnologías digitales contribuye a reducir riesgos de corrupción, en sí mismas, no están exentas de usos indebidos. Así como existe una tecnología para la integridad, debe garantizarse la integridad en el uso de la tecnología. Este capítulo analiza algunos aspectos de gestión de riesgo tecnológico que deben tener en cuenta los Gobiernos. En especial, dichas vulnerabilidades se alimentan de algunos de los vacíos legales e institucionales que rodean la adopción de tecnologías digitales, como el uso indebido de datos personales, la suplantación de la identidad digital o la sofisticación de las redes criminales para el lavado de dinero a través, por ejemplo, del uso de criptoactivos.

- Recomendaciones de política pública para asegurar una óptima formulación e implementación de una agenda de innovaciones tecnológicas al servicio de la integridad pública. Dichas sugerencias, recopiladas en el capítulo 6 del presente informe, exigen, por un lado, desarrollar ciertos ajustes institucionales para fortalecer la integridad en las políticas públicas, y, por otro, generar los recursos necesarios para la innovación digital en las autoridades públicas que hacen parte del ecosistema de integridad.

La figura 1, que presenta la estructura del informe, es también un esquema general para formular una política pública de integridad apalancada en tecnologías digitales, con un supuesto importante: la digitalización en la lucha contra la corrupción no comienza ni termina con el simple desarrollo de plataformas tecnológicas para investigar o detectar conductas indebidas en la gestión pública.

A pesar de la notable conciencia que surge alrededor del mundo sobre el nexo entre aceleración digital y políticas de integridad pública, aún no existe una guía integral para que los Gobiernos adopten mecanismos de lucha contra la corrupción con un enfoque de innovación digital. El presente informe busca llenar ese vacío.

Figura 1 Estructura del informe y propuesta de política de digitalización para la integridad



Fuente: Elaboración propia.

A este respecto, la exitosa incorporación de elementos de digitalización en la lucha contra la corrupción exige la puesta en marcha de varias iniciativas de política pública, así:

- **Fortalecimiento y garantía de acceso a la información pública a través de datos abiertos, y funcionamiento de servicios digitales para los ciudadanos**. Solo de este modo pueden los Gobiernos desarrollar infraestructuras de datos, que son la materia prima para que las tecnologías funcionen y generen resultados.

- Una vez los Gobiernos cuentan con esas **infraestructuras de datos** e implementan estándares de **transparencia activa**, se abre la ventana de oportunidad para poner en marcha las tecnologías digitales contra la corrupción a través de la reutilización de estos datos. El informe ilustra el uso de **la inteligencia de datos contra la corrupción**, puesto que sus propiedades en materia predictiva ayudan no solo a prevenir dichos fenómenos, sino a hacer más expeditas las investigaciones judiciales en la materia.

- Para adoptar estas tecnologías, los Gobiernos deben invertir en **infraestructura digital con poder de cómputo**. Las infraestructuras de datos y de computación bien consolidadas ofrecen la oportunidad a los Gobiernos de explorar el *blockchain* como un modo de proteger algunos procesos de la gestión pública de la captura por parte de intereses indebidos.

- De modo complementario, pero no menos importante, el informe considera que la política de integridad basada en tecnologías digitales necesita un componente que adopte estándares de transparencia e integridad dentro de la digitalización misma. Por ello, se plantean algunas consideraciones sobre **la gestión de riesgos** que conlleva la adopción de dichas tecnologías.

- Finalmente, una adecuada gestión de la política de integridad exige, adicionalmente, la modernización de los **arreglos legales e institucionales** para que la lucha contra la corrupción sea más preventiva y restaurativa cuando fracase la prevención, y para que el entorno digital facilite la innovación y modernización en esa tarea.

La integridad pública implica la adopción de un enfoque integral que no solo incluya el desarrollo de plataformas tecnológicas, sino la puesta en marcha de condiciones que vayan desde la consolidación de una agenda de datos abiertos y conjuntos de datos de calidad, hasta la inversión en infraestructura de cómputo, de datos y de aseguramiento frente al riesgo de las nuevas tecnologías. Este informe brinda herramientas para la implementación de agendas digitales anticorrupción alineadas con las necesidades, restricciones y contexto de cada país.

1.

Condiciones habilitantes

«¡Datos, datos, datos!», exclamaba con impaciencia. «¡No puedo hacer ladrillos sin arcilla!».

Sir Arthur Conan Doyle, El misterio de Copper Beeches, en Las aventuras de Sherlock Holmes

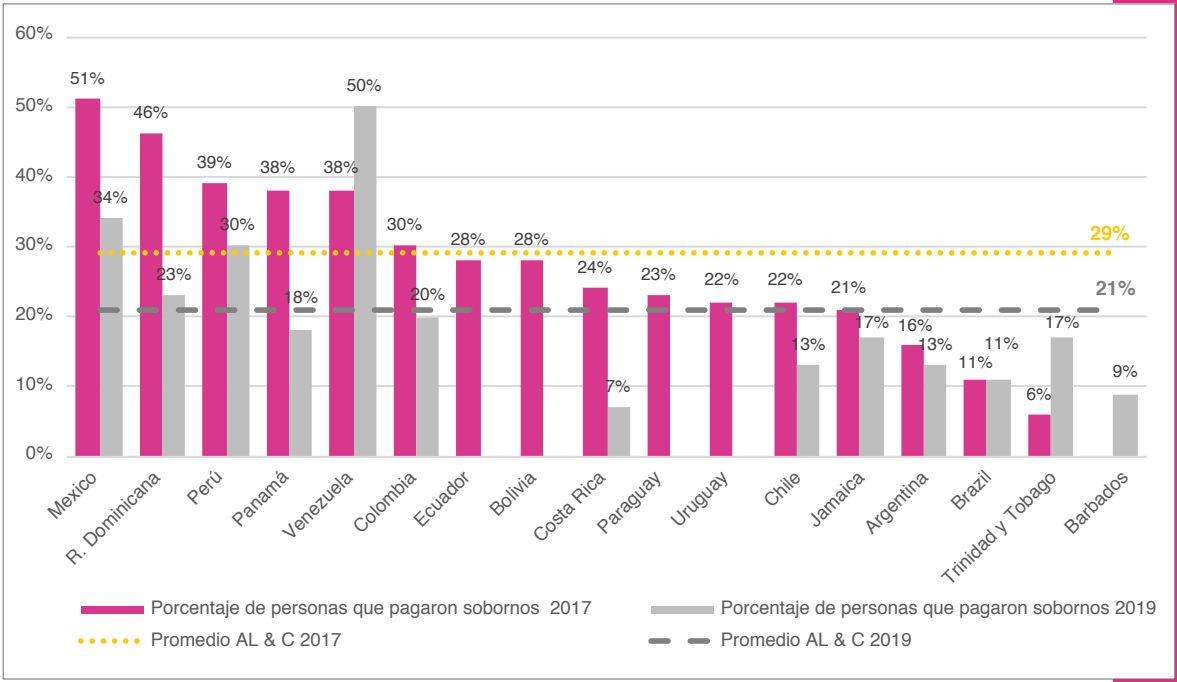
Condiciones habilitantes

La corrupción implica el abuso de un poder encomendado con el fin de apropiarse indebidamente de beneficios privados. Este fenómeno se manifiesta en conductas variadas, como el apoderamiento ilícito de recursos públicos, el pago de sobornos, el conflicto de interés dentro de las actuaciones de los Gobiernos, y, en ocasiones, se vincula con otros delitos, como el lavado de activos o el contrabando. El fenómeno de la corrupción preocupa de modo especial a los Gobiernos, puesto que, al depredar bienes públicos, impide el crecimiento, contribuye a la desigualdad y obstaculiza la innovación (FEM, 2017).

A pesar de la persistencia del fenómeno, América Latina ha mostrado que es posible mitigar los riesgos de corrupción. De acuerdo con el Barómetro Global de Corrupción 2017, entre los ciudadanos encuestados en América Latina y el Caribe, en promedio, el 29 % reportó haber pagado un soborno para acceder a servicios públicos básicos[2] como educación, salud y obtención de documentos de identidad (Transparencia Internacional, 2017). Este promedio regional disminuyó al 21 % en los resultados de la medición 2019 (Transparencia Internacional, 2019). En México, por ejemplo, **uno de cada dos encuestados** (51 %) en 2017 informó haber pagado un soborno para acceder a los servicios públicos básicos mencionados (Transparencia Internacional, 2017). En 2019, esta proporción se redujo al 34 %.

[2] La pregunta realizada a los encuestados fue: ¿Cuán a menudo ha tenido que pagar un soborno, dar un regalo o hacer un favor a: un docente o funcionario escolar; un trabajador de la salud o un miembro del personal de una clínica u hospital; un funcionario gubernamental para obtener un documento; un funcionario gubernamental para recibir servicios públicos; un policía; o un juez o funcionario judicial; o no lo ha hecho nunca? Los encuestados que tuvieron ocasión de efectuar alguna gestión en relación con un servicio de los descritos en los 12 meses anteriores, excluidas las respuestas faltantes.

Figura 1.1. Porcentaje de personas que han pagado por sobornos en América Latina y el Caribe 2017 y 2019



Fuente: Transparencia Internacional, resultados del Barómetro Global de Corrupción 2017 y 2019.

¿Cómo desarrollar una agenda que reduzca de modo sostenido y transversal los fenómenos de corrupción? En México, la aceleración de la transformación digital del Estado a través, entre otros, de la creación en 2015 de un portal único de trámites del Gobierno federal contribuyó a reducir los sobornos en los procedimientos públicos federales. La plataforma **www.gob.mx** hace parte de la Estrategia Digital Nacional que comenzó en 2014, y representa un replanteamiento de la relación entre los ciudadanos y el Gobierno. Ofrece a los primeros la posibilidad de realizar en línea los trámites más solicitados de la Administración Pública Federal, como los relacionados con identidad, educación, trabajo, impuestos y contribuciones, atención médica, registros de marca, licencias de comunicaciones y transporte, programas sociales y registro de turismo, entre otros. En una sola plataforma, de fácil acceso y con un diseño simple e intuitivo, se centralizó la información de más de 5 000 sitios del Gobierno federal.

Mediante la digitalización y simplificación de los trámites con la automatización de los procesos administrativos, los Gobiernos pueden limitar la discrecionalidad de las autoridades públicas y reducir así las interac-

ciones que dan lugar a conductas de corrupción (Santiso, 2021). El Foro Económico Mundial (FEM) reconoce las tecnologías digitales como un aliado importante en materia de transparencia e integridad, y como una herramienta fundamental en la lucha contra la corrupción (Santiso, 2020). Las nuevas tecnologías disruptivas de la denominada Cuarta Revolución Industrial (4IR), como *blockchain* e inteligencia artificial, generan innovaciones con un potencial significativo para que las empresas y los Gobiernos reduzcan riesgos de corrupción.

Sin embargo, las tecnologías digitales, per se, no garantizan más integridad ni mejor gestión de las administraciones públicas. Se requieren ciertas condiciones y habilitadores para que los Gobiernos puedan aprovechar las oportunidades que ofrece la transformación digital para fortalecer la integridad pública. Las políticas de transparencia activa, el acceso a datos abiertos y la reutilización de los mismos en el marco de políticas claras de gobierno digital representan el insumo mínimo para desarrollar políticas públicas que faciliten el desarrollo de sistemas preventivos de corrupción basados en inteligencia de datos (Cetina, 2020a).

Este capítulo presenta un conjunto de habilitadores para el despliegue efectivo de las nuevas tecnologías dirigidas a la prevención, detección e investigación de la corrupción

En ese sentido, la agenda de digitalización debe ir de la mano de políticas de transparencia activa en los Gobiernos, de modo que se generen las condiciones para que la tecnología pueda usarse en la lucha contra la corrupción. **Este capítulo presenta un conjunto de habilitadores para el despliegue efectivo de las nuevas tecnologías dirigidas a la prevención, detección e investigación de la corrupción, así:**

1. **Se aborda la política de gobierno digital**, en particular, la digitalización de los trámites y registros públicos, y la automatización de procesos administrativos como la contratación pública.

2. **Se examinan la transparencia activa y los datos abiertos.** La digitalización de servicios gubernamentales y registros públicos implica la generación de una cantidad considerable de conjuntos de datos, e, igualmente, requiere que los ciudadanos puedan acceder a la información relacionada con los servicios y procesos digitalizados.

3. Por último, **se identifican los conjuntos de datos con un uso reconocido en materia de integridad**, así como algunas aplicaciones a través de las cuales la reutilización de los datos habilita iniciativas de rendición de cuentas y de control social, contribuyendo a prevenir riesgos de corrupción y mejorar la gestión pública.

1.1. Digitalización de servicios gubernamentales e integridad pública

En América Latina, la interacción de los ciudadanos con sus Gobiernos, al menos antes de la crisis COVID-19, requería normalmente desplazarse a una sede gubernamental, hacer filas, esperar horas para radicar un documento físico, solicitar información sobre algún tema, e interactuar con un servidor público. En algunos casos, y como lo muestran los barómetros de Transparencia Internacional, también significaba exponerse a la solicitud indebida de pagos para agilizar dichos trámites. Este escenario contrastaba con la digitalización progresiva de la vida ciudadana, que implicaba el uso de redes sociales para revelar preferencias en el consumo, de las plataformas electrónicas para pagar bienes o servicios y recibir salarios, o la adopción masiva de servicios como el correo electrónico y la mensajería instantánea para trabajar.

Con la aceleración digital de los últimos años, también se avanzó en la simplificación de interacciones entre ciudadanía e instituciones. De acuerdo con el Banco Interamericano de Desarrollo – BID (2018), antes de la pandemia, un ciudadano latinoamericano tardaba, regularmente, 5,4 horas en completar un trámite, con diferencias notables entre países. Sin embargo, los servicios digitales han contribuido a la aceleración de los trámites (74 % más ágiles en promedio), hacen más eficientes los procedimientos públicos (los trámites digitales cuestan entre 2,35 % y el 5 % menos que uno presencial para los Gobiernos) y son una estrategia aceptada por los ciudadanos para mejorar la gestión pública (Roseth, Reyes y Santiso, 2018, p. 76). Estos esfuerzos también contribuyen a la agenda de integridad, puesto que la complejidad de los trámites abre ventanas de corrupción y solicitudes indebidas a los ciudadanos.

La experiencia internacional confirma los beneficios de la digitalización para fortalecer la integridad de las políticas públicas. En el caso de **Estonia**, por ejemplo, se impulsó la transformación digital de la administración pública a partir de 1994, con la promoción de los *Principios de la Política de Información de Estonia (*e-Estonia, 2021). Desde 2017, el 99 % de los trámites y servicios se pueden realizar en línea[3]. La apropiación de los servicios digitales por parte de los estonianos es alta. En 2014, se realizaron 80 millones de transacciones digitales en un país de tan solo 1,3 millones de habitantes (Goede, 2019). Para acceder a los e-servicios, los ciudadanos cuentan con un documento de **identidad digital** que emplea tecnología *blockchain* para generar un identificador único. e-Estonia

[3] Los matrimonios, divorcios y transacciones inmobiliarias son los únicos tramites que requieren ser realizados físicamente (Goede, 2019, p. 218).

permite que operaciones como identificación y firma digital, votaciones populares, registro de vehículos, declaración de impuestos y atención médica, entre otras, se realicen completamente en línea (Naciones Unidas, 2020).

Adicionalmente, e-Estonia presenta beneficios económicos importantes: ahorra 844 años de trabajo por cada año de operaciones de intercambio de información a través de **X-Road**[4]. En dicha plataforma, cada agencia del Estado administra sus propios datos, y es posible que las entidades autorizadas accedan a las bases de datos de otras oficinas gubernamentales. Así, los ciudadanos deben suministrar sus datos una única vez para realizar cualquier tipo de trámite ante diferentes autoridades públicas y privadas (e-Estonia, 2021). Además, los macrodatos generados en el curso de las transacciones son utilizados por la Oficina Nacional de Estadística para la toma de decisiones públicas[5]. Esta política también incide en los niveles de transparencia, puesto que los ciudadanos pueden acceder a datos abiertos, estandarizados y estructurados (Asamblea de Cooperación de Estonia, **2020**).

Transformar los sistemas analógicos basados en papel y utilizados tradicionalmente para interactuar con los ciudadanos

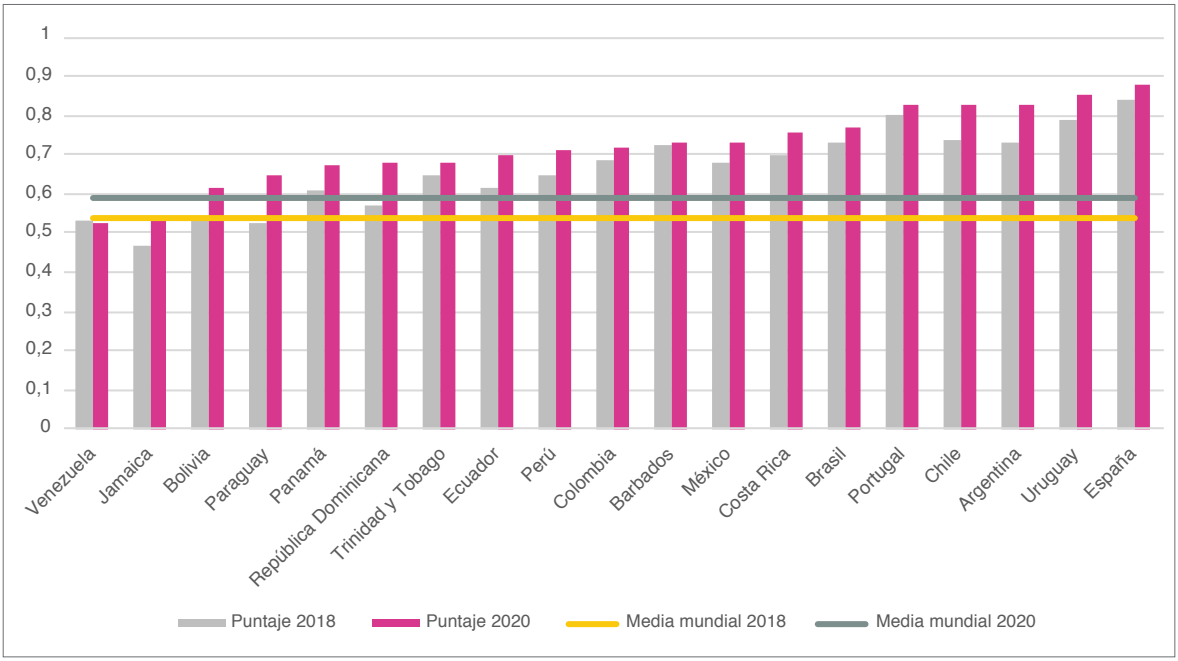
El propósito de la digitalización del Gobierno es usar las tecnologías digitales como un elemento integrado de las estrategias de modernización administrativa para crear valor público (OCDE, 2014; BID, 2016). Esto implica transformar los sistemas analógicos basados en papel y utilizados tradicionalmente para interactuar con los ciudadanos, de modo que los servicios públicos funcionen mejor, sean más ágiles, se desplieguen de manera más inteligente y se centren en las necesidades de los ciudadanos (Santiso, 2019). Se estima, por ejemplo, que **Dinamarca** ahorra EUR 296 millones anualmente desde que se inició la digitalización del Gobierno en 1996, reduciendo en un 30 % el tiempo de procesamiento de los trámites y aumentando sus niveles de transparencia en 96 % (Digital Denmark, 2021). Este país cuenta con el portal *online* **borger.dk**, en el cual, gracias a la articulación de las agencias públicas nacionales, regionales y municipales, se encuentra casi la totalidad de los servicios que ofrece el sector público danés (Naciones Unidas, 2020; Digital Denmark, 2021).

Ahora bien, **la digitalización no se reduce a la implementación de plataformas tecnológicas para realizar los trámites públicos**. También incluye adelantos en la conectividad digital y las habilidades digitales de los ciudadanos. Los avances en materia de digitalización en los Gobiernos se miden a través del Índice de Desarrollo del Gobierno Electrónico (IDGE), liderado por Dinamarca, Corea y Estonia. Está compuesto por tres dimensiones: prestación de servicios digitales, conectividad de telecomunicaciones y capacidad digital humana. Vale la pena resaltar que, en 2020, 17 de los 19 países miembros de la CAF se situaron por encima del promedio mundial calculado a partir de

[4] Software de intercambio de datos que garantiza la accesibilidad, la integridad y la confidencialidad de los datos generados y requeridos para las prestaciones de los servicios digitales públicos y privados.
[5] Por ejemplo, los datos catastrales, las transacciones inmobiliarias, las solicitudes de permisos de construcción y los relacionados con la utilización del transporte público son macrodatos que el Gobierno de Estonia usa para adopción de decisiones transparentes y basadas en evidencia (Asamblea de Cooperación de Estonia, 2020).

las calificaciones de 193 países miembros de la ONU incluidos en la medición IDGE (0,5988)[6] (ver figura 1.2). La variación en el índice, de 2018 a 2020, fue impulsada principalmente por un aumento en el subíndice de conectividad (TII por sus siglas en inglés, *Telecommunication Infrastructure Index*) que mostró avances en infraestructura de telecomunicaciones en todos los países CAF objeto de medición. También se evidenció un incremento en el subíndice de capacidad digital humana (HCI por sus siglas en inglés, *Human Capital Index*) en casi la totalidad de los países CAF, descontando a Perú y Ecuador.

Figura 1.2. Resultados IDGE para los países miembros de CAF en 2018 y 2020



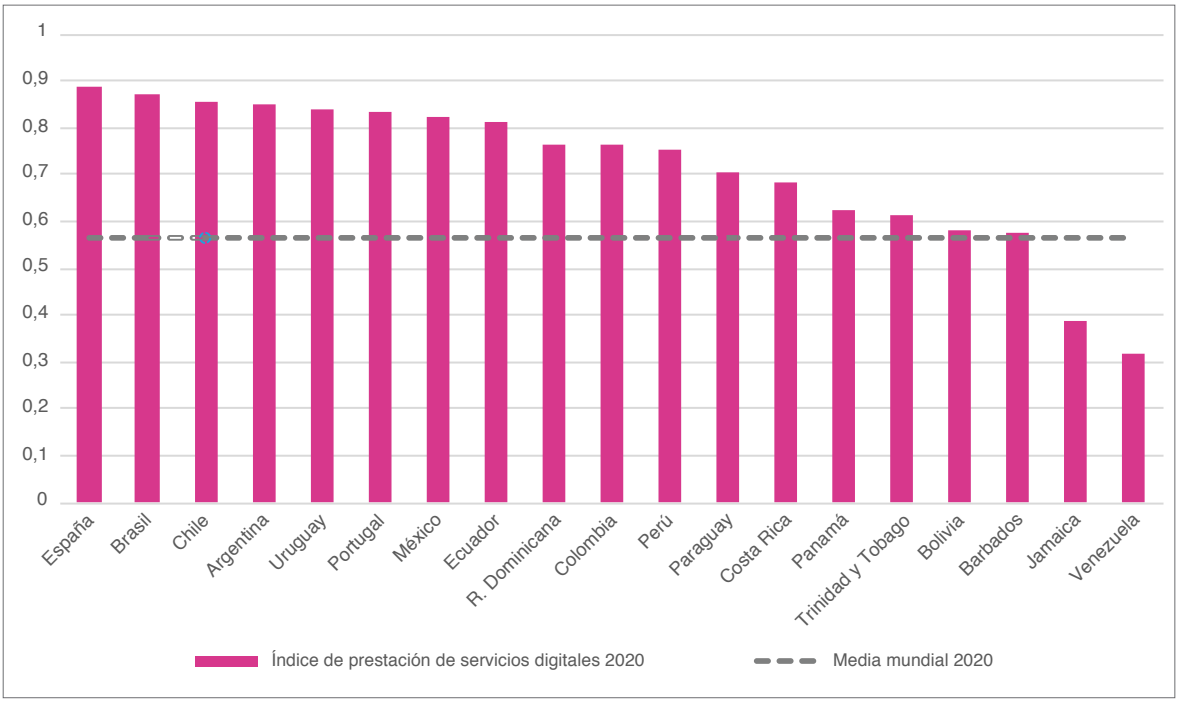
Fuente: ONU (2020). La escala IDGE va de 0 a 1, Dinamarca (0,9758), Corea (0,9560) y Estonia (0,9473) fueron los países líderes en 2020. La medición asigna, a cada país miembro, un puntaje en una escala de 0 a 1, en la que 1 representa el máximo nivel de desarrollo del gobierno digital (Naciones Unidas, 2020). La media mundial se refiere al promedio de la calificación de los 193 países incluidos en la medición para los años 2018 y 2020.

El desarrollo de los servicios en línea ofrecidos a los ciudadanos se mide con el subíndice de prestación de servicios digitales, *Online Services Index* (OSI), el cual hace parte del IDGE. Aquí, los países miembros de CAF muestran un comportamiento similar al observado con este índice. Los factores determinantes de la calificación incluyen la funcionalidad de los portales, la disponibilidad de la información, la rapidez de las plataformas, el diseño intui-

[6] Jamaica y Venezuela, con puntajes respectivamente de 0,5391 y 0,5268, fueron los dos países miembros de CAF que se situaron por debajo de la media mundial de IDGE en la medición 2020. Llama la atención que, a nivel mundial, los puntajes de Dinamarca (0,9758), Corea (0,9560) y Estonia (0,9473) se acercan mucho al máximo de 1.

tivo y la posibilidad de ejecutar trámites en línea (ONU, 2020). En 2020, 17 de los 19 países miembros de CAF se situaron por encima del promedio mundial (0,5262)[7] del OSI. El líder en la medición fue Estonia, con una puntuación de 0,994, país donde el 99 % de los trámites y servicios se pueden realizar en línea (figura 1.3).

Figura 1.3. Resultados OSI para los países miembros de CAF 2020

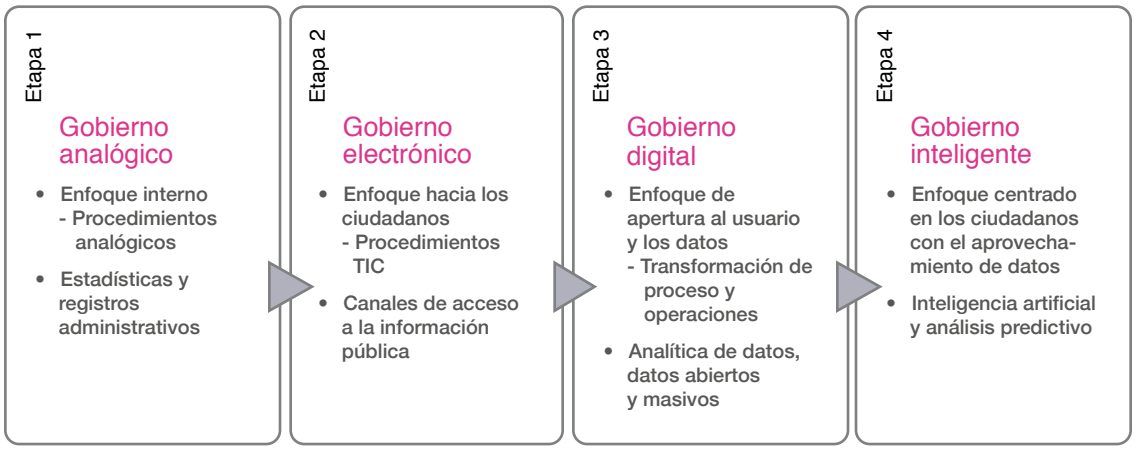


Fuente: ONU (2020). La escala OSI va de 0 a 1; Estonia (0,994) fue el país líder en 2020. La media mundial corresponde al promedio de la puntuación de los 193 países incluidos en la medición OSI de 2020.

La transformación digital de los Gobiernos también implica el aprovechamiento de los datos para mejorar las políticas públicas y la calidad de los servicios (figura 1.4). Existen cuatro capacidades claves para alcanzar un Gobierno inteligente, es decir, guiado por el uso y reúso de los datos con fines predictivos: (i) los servicios digitales a los ciudadanos; (ii) los procesos administrativos internos; (iii) las decisiones de la administración soportadas en datos, y (iv) los datos mismos, de fácil acceso y reúso, para habilitar la innovación digital en servicios públicos (Santiso y Ortiz, 2020, p. 25).

[7] Jamaica y Venezuela, con puntajes de 0,3882 y 0,3176, respectivamente, fueron los únicos países miembros de CAF que se situaron por debajo de la media mundial de OSI en su edición 2020.

Figura 1.4. Elementos y etapas de la transformación digital de las administraciones



Fuente: Santiso y Ortiz (2020).

La digitalización del Estado, además de entregar mejores servicios a los ciudadanos y ahorrar recursos públicos, hace posible la centralización de datos que contienen información sobre los procesos llevados a cabo por las administraciones públicas. Estos datos e información, cuando son de público acceso, tienen el potencial de fomentar mayores niveles de transparencia e integridad del Estado.

Sin embargo, la digitalización en sí misma no necesariamente implica ni genera mayores niveles de transparencia, integridad y valor público. La tecnología encuentra límites si el ordenamiento jurídico e institucional no consagra el derecho de acceso a la información pública ni genera disposiciones sobre la apertura de datos (Volosin, 2015). Por ello, para que realmente se aprovechen los sistemas digitales en materia de integridad, corresponde a los Gobiernos implementar estrategias e iniciativas que permitan el acceso a la información pública y el uso y reúso de los datos (OCDE, 2021).

Una iniciativa que articula las innovaciones digitales, los datos y la transparencia dentro de los Gobiernos para potenciar sus efectos en las políticas públicas es la **Alianza para el Gobierno Abierto** (**OGP,** por sus siglas en inglés), que empezó en 2011 con la Declaración de Gobierno Abierto. Los países miembros de OGP, a través de planes de acción bianuales, desarrollan iniciativas para: 1) aumentar la disponibilidad de información sobre las actividades gubernamentales; 2) apoyar la participación ciudadana; 3) aplicar los más altos estándares de integridad profesional, y 4) aumentar el acceso de nuevas tecnologías para la apertura de datos y rendición de cuentas. A la fecha, la mayoría de los países miembros de CAF adhirieron a OGP (OGP, 2021).

Figura 1.5. Políticas habilitadoras para fortalecer el desarrollo, la confianza y el valor público

Fuente: Elaboración propia.

1.2 Del acceso a la información a la transparencia activa con datos abiertos

En las últimas dos décadas, la transparencia activa y los datos abiertos se han convertido en aliados clave para la lucha contra la corrupción en la era digital. Los datos masivos, estandarizados y abiertos han facilitado el despliegue de alternativas de análisis de información imposibles de implementar a partir de documentos físicos. Dichos análisis solo son posibles si se adoptan prácticas de transparencia y acceso a la información pública, las cuales, al igual que el gobierno digital, requieren de un proceso de maduración en las instituciones y regulaciones gubernamentales, como se propone en la figura 1.6.

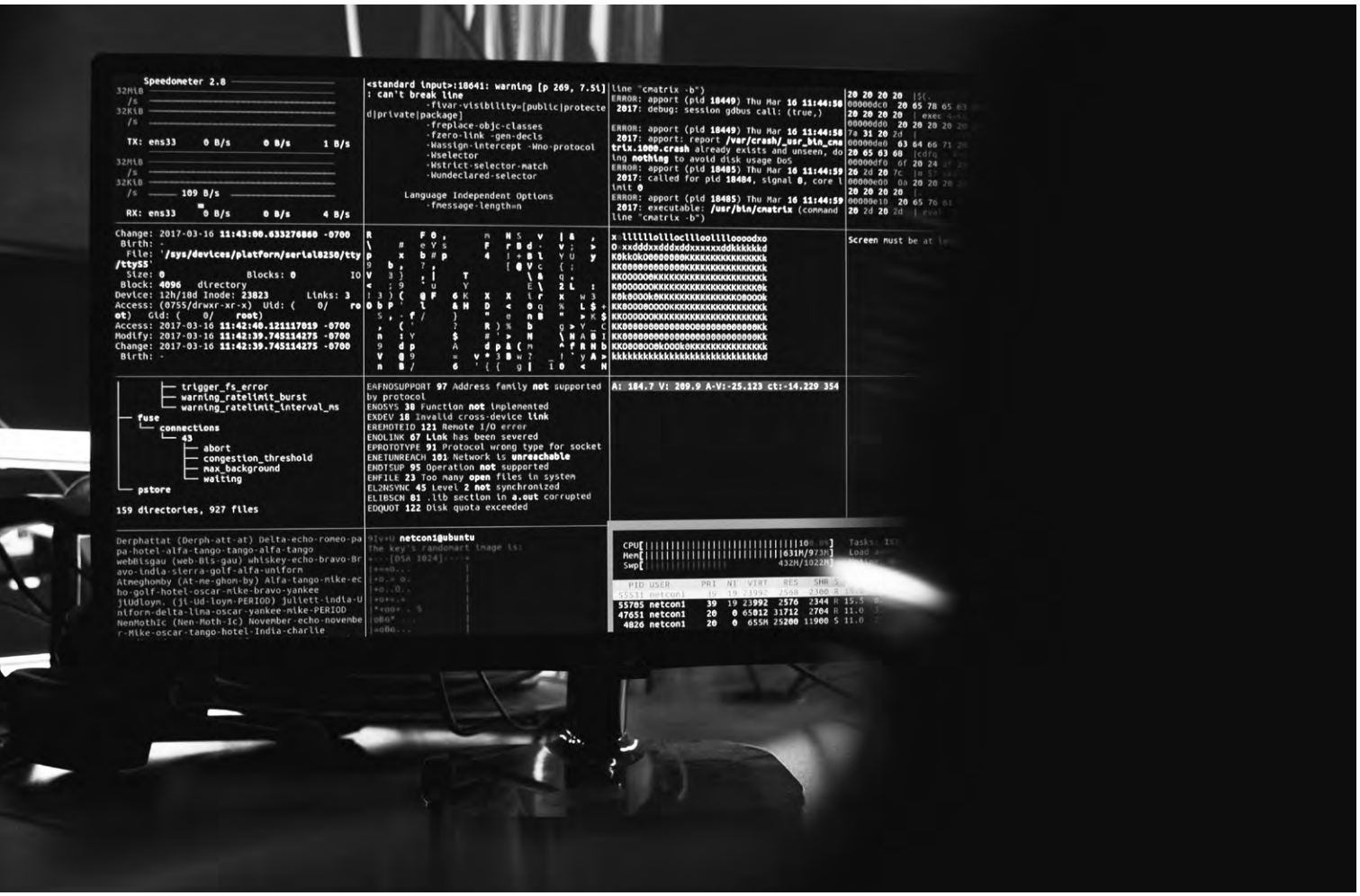
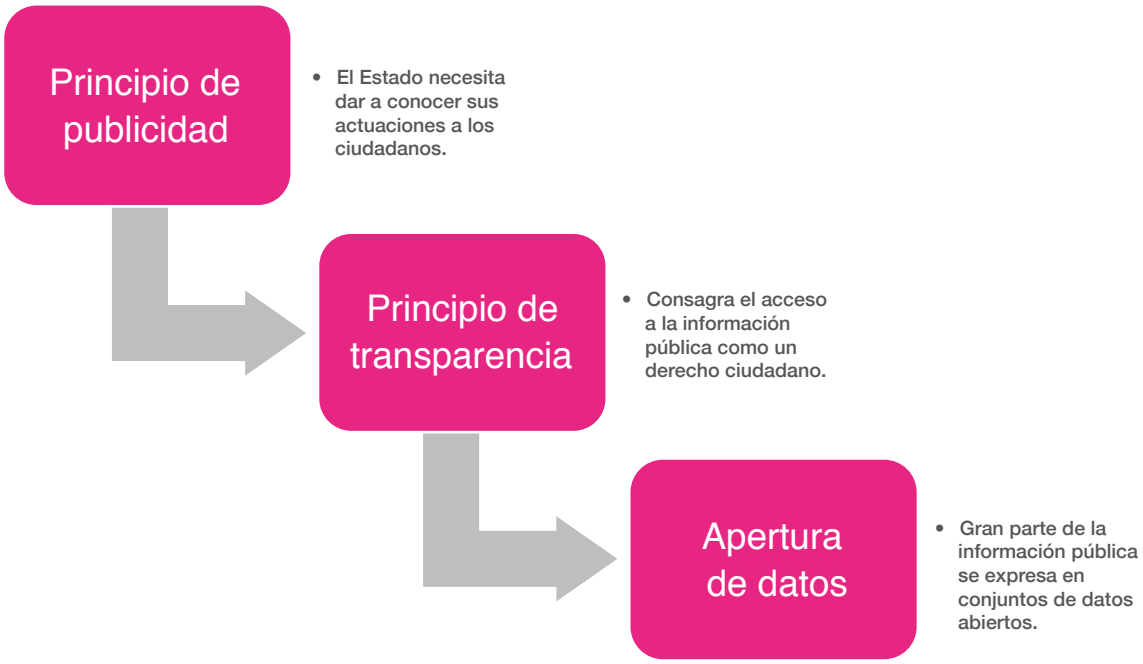


Figura 1.6. Evolución en el acceso a la información pública



Fuente: Elaboración propia.

1.2.1 Del principio de publicidad a los estándares de transparencia

El principio de publicidad[8] implica que las actuaciones del Estado deben ser públicas. Es decir, los ciudadanos deben conocer las acciones, decisiones y políticas del Gobierno, y, del mismo modo, las razones que motivan estas actuaciones. En tal sentido, se deben evitar «zonas de sombra», donde prosperen la ilegalidad o las conductas que socaven el interés general (Romeu y Rodriguez, 2013). Aplicar el principio de publicidad también facilita el desarrollo de las políticas públicas, puesto que su formulación e implementación exigen la interacción entre diferentes actores: los ciudadanos, la sociedad civil, el sector privado, los servidores públicos (Ejecutivo, Legislativo y Judicial), los organismos independientes y las autoridades fiscalizadoras. Así, dar a conocer las actuaciones del Estado en el ciclo de políticas públicas es un mínimo fundamental para que estas puedan hacerse cumplir.

[8] En algunos países de la región, como Venezuela, el principio de publicidad se denomina «principio de responsabilidad pública».

Sin embargo, el concepto de transparencia es más ambicioso que el de publicidad de las actuaciones de los entes públicos. Bajo el principio de transparencia, se habilita el ejercicio de varios derechos fundamentales (como el debido proceso, de defensa, de acceso a información pública y la participación ciudadana), de modo que se permite el control sobre decisiones de las autoridades. El conocimiento público y los canales de atención e interacción relacionados con las actuaciones de las agencias gubernamentales permiten que los ciudadanos deliberen y reclamen sus derechos.

El acceso libre y directo a los datos sobre las actuaciones del Gobierno, así como a herramientas de visualización que posibiliten una comprensión mucha más rápida e intuitiva de la información, aumenta la transparencia de los procesos y permite fortalecer la integridad pública.

Y así como la transparencia va más allá de la simple publicidad, existen también niveles de acceso a la información pública. Por ello, hay que distinguir dos tipos de transparencia gubernamental:

- La **pasiva** se refiere a los casos en los que un interesado entrega información como consecuencia de solicitud o requerimiento a una entidad pública (De la Fuente, 2014). En este escenario, las solicitudes verbales y escritas en ejercicio del derecho de petición juegan un papel fundamental. Las peticiones son solicitudes elevadas ante las agencias públicas y privadas con el fin de conocer hechos, solicitar documentos, o reclamar la prestación o mejora de un servicio. Las entidades públicas deben concederles el trámite correspondiente y responderlas de manera completa y sustentada dentro de los términos legales.

- Por su parte, la **activa** va más allá de la simple respuesta a solicitudes de información: corresponde a la obligación de las agencias del Gobierno de publicar de manera sistemática, periódica y oportuna, sin que medie requerimiento alguno, la totalidad de la información y los datos que no estén específicamente sometidos a reservas legales o constitucionales. En tal sentido, cualquier persona, sin importar su calidad (ciudadano, extranjero, persona natural o jurídica, mayor o menor de edad) y sin necesidad de acreditar un interés o condición particular, tiene el derecho a acceder a la información y a los datos públicos. El acceso libre y directo a los datos sobre las actuaciones del Gobierno, así como a herramientas de visualización que posibiliten una comprensión mucha más rápida e intuitiva de la información, aumenta la transparencia de los procesos y permite fortalecer la integridad pública.

La regulación en materia de acceso a la información pública en la región tiene varias décadas y, gracias al principio de transparencia activa, los Gobiernos han ido evolucionando hacia la apertura de datos (De la Fuente, 2014; ILDA, 2021). De los países miembros de CAF, 18 cuentan con normativa que garantiza el acceso a la información pública (ver tabla 1.1). Sin embargo, algunas de estas normas fueron expedidas hace más de una década y no han sido actualizadas. Por lo anterior, muchas no se guían por el principio de transparencia activa. En consecuencia, la información solo se obtiene a través de peticiones o requerimientos a las autoridades públicas.

Igualmente, se evidencia un rezago en materia de acceso a la información en un mundo de datos masivos, como se puede inferir de la discrepancia entre la adopción de leyes de transparencia y la escasa aceptación de estándares internacionales como la Carta Internacional de Datos Abiertos (ODC por sus siglas en inglés, *Open Data Charter*).

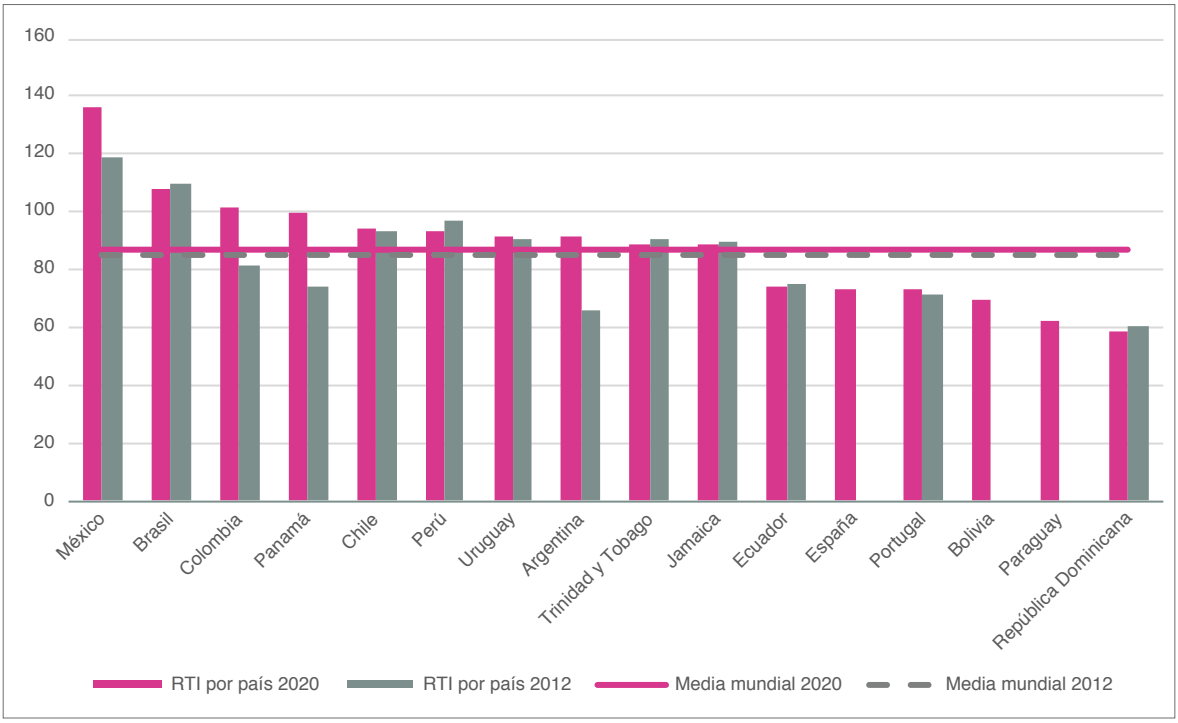
Tabla 1.1. Marcos normativos sobre acceso a la información pública en los países miembros de CAF

País	Normas más recientes/N.°	Año	Política de datos abiertos	Adoptante Open Data Charter
Costa Rica	Constitución Política (Artículos 27, 30) - Decreto Ejecutivo 40 199	1949/2017	✓	✓
Portugal	Ley de Acceso a los Documentos de la Administración/ 65 – Ley de Acceso a la Información Administrativa y Ambiental y Reutilización de Documentos Administrativos/26	1993/2016	✓	✗
Trinidad y Tobago	Ley de Libertad de Información/26	1999	-	✗
México	Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental	2002	✓	✓
Perú	Ley de Transparencia y Acceso a la Información Pública/27 806	2002	✓	✗
Jamaica	Ley de Libertad de Información/21	2002	-	✗
República Dominicana	Ley General de Libre Acceso a la Información Pública/200-04 – Decreto 486-12	2004/2012	✓	✗
Ecuador	Ley Orgánica de Transparencia y Acceso a la Información Pública/24 – Constitución	2004/2008	✓	✗
Bolivia	Decreto Supremo sobre Acceso a la Información/28 168	2005	✗	✗
Uruguay	Derecho de Acceso a la Información Pública/18 381	2008	✓	✓
Chile	Ley de Transparencia de la Función Pública y de Acceso a la Información/20 285	2008	✓	✓
Brasil	Ley de Acceso a la Información/12 527	2011	✓	✗
Venezuela	Ley Orgánica de la Administración Pública (Artículos 9 y 13)	2011	✗	✗
Panamá	Ley que crea la Autoridad Nacional de Transparencia y Acceso a la información/33	2013	✗	✓
España	Ley de Transparencia, Acceso a la Información Pública y Buen Gobierno/19	2013	✓	✗
Colombia	Ley de Transparencia y Derecho de Acceso a la Información Pública/1 712	2014	✓	✓
Paraguay	Ley de Libre Acceso Ciudadano a la Información Pública y Transparencia Gubernamental/5 282	2014	✓	✓
Argentina	Ley de Acceso a la Información Pública/27 275	2016	✓	✓

Fuente: Elaboración propia a partir de De la Fuente (2014), CEPAL (s. f.), ODC (2021).

El acceso a los datos abiertos representa, además de un derecho de los ciudadanos, un instrumento para monitorear y ejercer control sobre posibles casos de corrupción. Mediciones como el **RTI**[9] (ver figura 1.7) mostraron mejoras en la calidad de las normas *de jure* de acceso a la información. Sin embargo, se requiere perfeccionar y agilizar los procedimientos de solicitud de información y la imposición de sanciones para los servidores que deliberadamente socaven el ejercicio efectivo de este derecho.

Figura 1.7. **Índice de acceso a la información (RTI) para los países miembros de CAF 2012 y 2020**



Fuente: RTI 2019 y 2012. La escala RTI va de 0 a 160. Una calificación cercana a 160 muestra mayor fortaleza de los marcos legales. La media mundial corresponde al promedio de la puntuación de los 128 países incluidos en la medición RTI en 2019, y 93 países incluidos en 2012.

La transparencia activa es un instrumento indispensable en la agenda de integridad pública (Zapata, Scrollini y Fumega, 2020). Sin que medie una

[9] Índice Global de Derecho a la información RTI *(Right to Information Rating)*, propuesto por el Centro por el Derecho y la Democracia y el equipo Access Info. Mide la fortaleza del marco legal para el derecho de acceso a la información en poder de las autoridades públicas, teniendo en cuenta 61 indicadores discretos organizados en 7 categorías principales: derecho de acceso, alcance, procedimiento de solicitud, excepciones y rechazos, apelaciones, sanciones y protecciones, y medidas promocionales (RTI, 2021).

petición verbal o escrita y un trámite burocrático, cualquier individuo puede acceder a datos completos y actualizados sobre las actuaciones estatales en un formato que habilite su reúso para efectos analíticos. Por ejemplo, antes de la existencia de las plataformas de *e-procurement* o abastecimiento en línea, conocer los datos relativos a la contratación pública implicaba superar una serie de barreras: presentar una petición de información, someterse a los procedimientos internos, y esperar para recibir datos no estandarizados u obsoletos. Con la evolución de plataformas digitales que contienen datos abiertos en tiempo real (que incluso permiten crear visualizaciones intuitivas, como en el caso de **Paraguay**), el conocimiento, la participación y el control sobre las actuaciones públicas es más estricto e informado.

1.2.2. De la transparencia activa a los datos abiertos

Los datos abiertos no solo son transparentes y accesibles, sino que se pueden reusar para efectos analíticos a través de herramientas automatizadas. La organización **Open Knowledge Foundation** (OKF) define los datos abiertos como aquellos que las personas pueden usar, reusar y redistribuir libremente, sin restricciones legales, tecnológicas o económicas. Por su parte, la **OCDE** los define como los datos que están disponibles y son accesibles y reutilizables (esto es, leíbles por máquina) sin que medien barreras impuestas por parte de los Gobiernos. En 2015, se comenzó a tomar mayor conciencia sobre la importancia de presentar la información pública en formato de datos abiertos para facilitar y potenciar su reúso. Así, la Asamblea Nacional de las Naciones Unidas promulgó la **Carta Internacional de Datos Abiertos** (*Open Data Charter* en inglés), fijando principios fundamentales para apoyar la transparencia, innovación y rendición de cuentas en la gobernanza de los datos públicos. La Carta destaca la importancia de los datos en la transformación de los Gobiernos hacia mayores transparencia, eficiencia y efectividad en la gestión pública. Los principios para la publicación establecidos en la ODC se describen en la tabla 1.2.

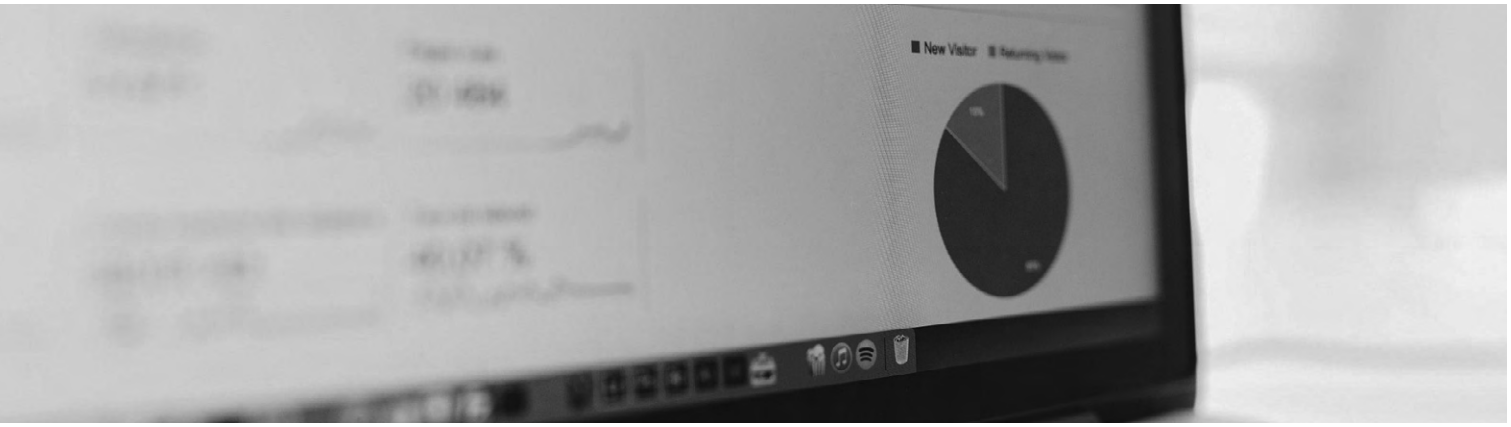


Tabla 1.2. Principios para la apertura de datos gubernamentales

Principio		Contenido
Apertura por defecto		La regla general consiste en que todos los datos gubernamentales deben estar públicamente disponibles, salvo cuando exista una explicita razón legal debidamente justificada. Además, el acceso a los datos no debe comprometer la privacidad de quien los consulta. Por ejemplo, los Gobiernos deben mantener disponibles los datos sobre la contratación de insumos médicos durante la pandemia. Sin embargo, las normas expresa y excepcionalmente pueden disponer que alguna información esté sometida a reserva. Esto ocurre, por ejemplo, con los secretos industriales (componentes químicos de las vacunas), u otros relacionados con la «seguridad nacional y defensa nacional» (informes de inteligencia militar).
Oportuna y completa		Los datos deben ser publicados de manera oportuna, completa y sin ser alterados. Asimismo, deben actualizarse periódicamente. Lo anterior implica que, por ejemplo, los datos de un proceso de selección de un contratista deben hacerse públicos de manera oportuna, completa y en su versión sin alteraciones, no después de que el proceso de contratación ha llegado a su fin.
Accesible y utilizable		No deben existir barreras administrativas, económicas ni tecnológicas para ingresar. Los portales deben facilitar la experiencia del consultante, permitir la entrada sin registro como usuarios, proveer formatos de acceso y descarga que maximicen la usabilidad y estar completamente libres de cargos monetarios.
Comparable e interoperable		Los datos deben ser estandarizados para permitir comparaciones e integraciones con otros conjuntos de datos y sistemas. En tal sentido, los datos que, por ejemplo, una agencia nacional de compras públicas tiene disponibles en su portal web deben cumplir con estándares que permitan a cualquier interesado compararlos con otras fuentes como, por ejemplo, las páginas web de los órganos de control.
Para mejorar la gobernanza y participación ciudadana		Los datos deben permitir que los ciudadanos, el sector privado, la sociedad civil y otras agencias gubernamentales conozcan del desempeño del sector público. La transparencia y rendición de cuentas mejoran la provisión de servicios públicos, posibilitan el control de los agentes estatales y el imperio de la ley.
Para el desarrollo inclusivo y la innovación		El acceso a los datos genera espacios para la innovación. Además, ofrece mayores beneficios económicos y sociales para toda la sociedad.

Fuente: ODC, 2015.

La apertura de datos permite la trazabilidad en las actuaciones e interacciones de los Gobiernos para identificar irregularidades, divulgarlas, corregirlas, prevenirlas y/o sancionarlas. Para que esto sea posible, los Gobiernos deben superar tres limitaciones generales que dificultan el aprovechamiento de los conjuntos de datos (Cetina, 2020a; ILDA, 2021; ODC, 2018):

- **Disponibilidad:** los datos deben existir y producirse de modo que se puedan utilizar, reutilizar y distribuir sin restricciones.

- **Integridad:** los datos deben capturar información que refleje la realidad con exactitud, completitud, homogeneidad y coherencia con la intención de los creadores. Por ello, los países deben diseñar sistemas de información que no solo sirvan para registrar hechos y datos, sino para asegurar la exactitud de la información y la uniformidad con que esta se digitaliza.

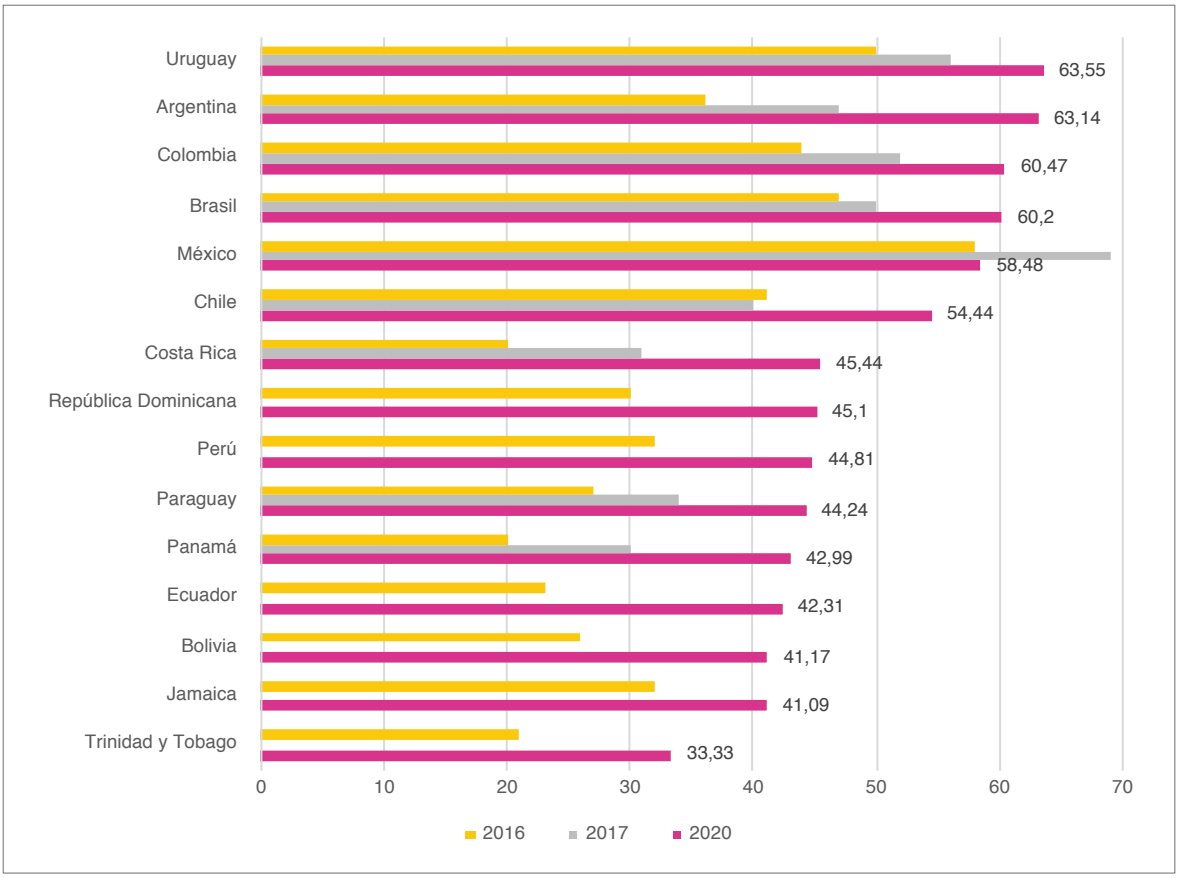
- **Estructura:** las bases de datos deben contar con una estructura interna predefinida (organización y formatos) que facilite la interoperabilidad entre diversos sistemas. Cuando los datos no están estructurados, se generan dificultades para la utilización, reutilización y distribución (por ejemplo, correos electrónicos, textos en redes sociales, audios, videos, archivos planos de texto y formatos PDF).

De acuerdo con el Barómetro Regional de Datos Abiertos para América Latina y el Caribe 2020 (ILDA, 2021), que mide la preparación[10], implementación[11] e impacto de los datos abiertos[12], la región mostró un crecimiento marginal comparado con los resultados de 2016, alcanzando una calificación promedio de 40,38 en una escala de 0 a 100. Esto refleja una desaceleración de la

[10] Se refiere a la disposición de los Gobiernos, ciudadanos y empresarios para asegurar la apertura de los datos.
[11] Corresponde al grado en que los Gobiernos publican conjuntos de datos clave de forma accesible, oportuna y abierta.
[12] Identifica hasta qué punto hay evidencia de que la publicación de datos abiertos del Gobierno ha tenido impacto positivo en una variedad de sectores del país.

agenda, en particular en los ámbitos de preparación e impacto. Los avances en materia de implementación son desiguales, y en lo que atañe al impacto, los países observados no presentaron mayores avances (Zapata, Scrollini y Fumega, 2020).

Figura 1.8. Resultados del Barómetro Regional de Datos Abiertos para América Latina y el Caribe para los países miembros de CAF 2016, 2017 y 2020



Fuente: Zapata, Scrollini y Fumega (2020). La escala va de 0 a 100, una calificación de 100 muestra mayores niveles de preparación, implementación y apertura. Reino Unido es el país líder con un puntaje de 76.

Con el fin de avanzar en materia de datos abiertos, ILDA (2021) recomienda a los Gobiernos de la región:

i) invertir de manera constante y sostenida en equipos que guíen e implementen políticas de datos abiertos en todos los niveles gubernamentales;

ii) implementar una visión holística en materia de datos, que incluya aspectos regulatorios de protección de privacidad, usos para el bien común e inclusión de sujetos vulnerables;

iii) aumentar los esfuerzos por incluir al sector privado y la sociedad civil en el ecosistema de apertura de datos;

iv) generar mejores y mayores usos de los datos para producir beneficios a los diversos grupos de la sociedad, y

v) promover el apoyo político a la agenda de datos abiertos.

En general, la adopción de estándares de transparencia activa y de gobierno digital centrados en los ciudadanos precede a la agenda de datos abiertos, de modo que estos ganen un propósito y capturen la información relevante. En este proceso, se van configurando los conjuntos de datos más importantes para la agenda de integridad y la lucha contra la corrupción a través de su publicación y reutilización, como se ilustra en la siguiente sección.

Recuadro 1.1. Portal de información abierta sobre contrataciones públicas de Ecuador

A finales de 2021, gracias a la cooperación entre CAF, *Open Contracting Partnership* y el apoyo del Ministerio de Telecomunicaciones de Ecuador (MINTEL) se lanzó la **Plataforma de Información Abierta de Contratación Pública**. Esta iniciativa se construyó en cumplimiento de los compromisos de gobierno abierto por parte del Servicio Nacional de Contratación Pública (SERCOP). El SERCOP es la entidad rectora del Sistema Nacional de Contratación Pública (SNCP), responsable de desarrollar y administrar el Sistema Oficial de Contratación Pública del Ecuador (SOCE) y de establecer las políticas y condiciones de la contratación pública a nivel nacional
Con la implementación de esta herramienta, se espera mejorar la divulgación, uso y calidad de los datos de contratación pública por parte de los diferentes actores del Sistema Nacional de Contratación Pública (SNCP). Al cierre del año 2021, la plataforma ha registrado al menos 127 163 procedimientos de contratación, los cuales representan un monto total adjudicado que asciende a USD 3,6 mil millones. El portal también permite navegar de acuerdo con características como tipo de contrato, sector asociado, entidades, empresas y monto de los mismos.

Fuente: Elaboración propia.
Fuente: CAF (2021).

1.3. El rol de los datos abiertos en las políticas de integridad

1.3.1. Conjuntos de datos para luchar contra la corrupción

El acceso a la información pública, vinculado a la digitalización y la aceleración de la cuarta revolución industrial, permitió a los Gobiernos organizar su información en datos con una estructura más definida para facilitar su reutilización, y con un propósito más específico. El reconocimiento del acceso a la información pública como un derecho abrió la puerta para que los ciudadanos pudieran exigir información sobre las decisiones y acciones de las instituciones públicas.

Los conjuntos de datos específicos de utilidad en integridad pública varían según las conductas investigadas y la naturaleza del organismo interesado en prevenir, detectar e investigar fenómenos de corrupción. De hecho, dentro del ecosistema de datos que usan los Gobiernos, hay esfuerzos para identificar, hacer accesibles y reutilizar información clave para combatir la corrupción como la Guía de Apertura de Datos del ODC[13].

Este reporte destaca seis conjuntos de datos con gran capacidad para levantar alertas tempranas sobre riesgos de corrupción y vulnerabilidades en los sistemas de integridad, es decir, relaciones, comunicaciones, locaciones y patrones detrás de ciertas decisiones públicas y transacciones gubernamentales, de acuerdo con los usos que se mostrarán en los capítulos 2 y 3.

1. **Datos de contratación y compra pública:** hoy en día, es posible acceder a información proveniente de las diferentes fases de los procesos de contratación que hacen los Gobiernos, desde el momento en que identifican una necesidad de abastecimiento hasta la entrega final de los bienes y servicios. Condiciones de suministro, precios y cantidades de compra, naturaleza y nombre de los proponentes, empresas o individuos ganadores de contratos, adendas, renegociaciones, sanciones y registros de cumplimiento, e informes de ejecución, entre otros, son los principales aspectos de captura de información en estos procesos estatales. En América Latina, los portales de las agencias de contratación y compra pública de **Buenos Aires**, **Chile**, **Colombia**, **Uruguay** y **Paraguay** han implementado el Estándar de Datos de Contratación Abierta (**OCDS** por sus siglas en inglés, *Open Contracting Data Standard*), que registra y permite consultar en datos abiertos las variables más importantes en las fases precontractual, contractual y poscontractual de cada proceso. Sin embargo, resulta relevante mencionar que existen límites a los deberes de publicidad de la información pública establecidos en la leyes de cada país como, por ejemplo, los relacionados con los secretos industriales y comerciales, seguridad nacional y defensa nacional. Estas limitaciones deben evaluarse caso a caso sin que los Gobiernos puedan alegar de manera genérica que existe información secreta sin mayor detalle, abusando de estas clasificaciones (CIDH, 2020).

2. **Declaraciones de activos e intereses[14]:** aunque no existe un estándar internacional en esta materia, de modo general, se trata de documentos suscritos por los funcionarios públicos, que señalan la existencia de intereses privados que podrían entrar en conflicto con el interés general que

[13] Ver https://opendatacharter.net/themes_and_topics/anti-corruption/
[14] Declarar activos e intereses constituye un mismo acto y requiere un mismo formato, puesto que la propiedad sobre ciertos activos puede generar conflicto de interés. Piénsese en la participación accionaria que un funcionario tiene sobre una compañía que contrata con el Estado, o en la propiedad sobre un inmueble cuyo valor puede verse afectado por una intervención pública, como la construcción de vías o la autorización de licencias de uso de suelo

La Contraloría General del Perú tiene un esquema en el cual el público puede descargar las declaraciones de los funcionarios sin necesidad de hacer solicitud.

se deriva del ejercicio de cargos públicos (CAF, 2019). En la mayoría de los países de la región, los funcionarios públicos[15] deben declarar ante la autoridad que regula y supervisa la función pública información relacionada con la naturaleza de sus bienes, deudas, cuentas de ahorro, títulos valores, y membresía a juntas directivas, asambleas o concejos en entidades de derecho privado, entre otros. Estas declaraciones deben establecerse, por lo general, cada año, constituyendo las primeras líneas de posibles conflictos de interés[16] que existen en el ejercicio de cargos públicos. En Francia, por ejemplo, la Autoridad de Transparencia e Información Pública recolecta y publica las declaraciones de bienes, rentas y conflictos de interés a través de su portal **www.hatvp.fr**. En México, la plataforma **Declaranet** permite consultar los bienes y rentas declarados por los funcionarios públicos en formato .csv[17]. En otros países, como Paraguay[18], se puede acceder a esta información, siempre y cuando sea por medio de una solicitud hecha a la Contraloría. La Contraloría General del Perú tiene un esquema en el cual el público puede descargar las declaraciones de los funcionarios sin necesidad de hacer solicitud, una a la vez.

3. **Datos en materia tributaria[19]:** las autoridades tributarias, por su naturaleza, tienen un acceso privilegiado a la información sobre el domicilio y movimientos de los contribuyentes. Adicionalmente, necesitan capturar datos estructurados para administrar su propia información de recaudo. Por ejemplo, en Argentina, el Sistema de Identificación Nacional Tributario y Social (**SINTyS**) integra y relaciona en la nube datos de individuos y empresas en tiempo real, para reducir la evasión y controlar la informalidad. Por su parte, el Servicio de Impuestos Internos (**SII**) de Chile captura tal nivel de información sobre los contribuyentes, que genera declaraciones prediligenciadas, con información obtenida de bancos y los propios contribuyentes en sus transacciones económicas[20].

4. **Registros de empresas:** el registro formal de las personas jurídicas, en particular de las empresas o firmas, es un paso necesario en su proceso de constitución y reconocimiento ante el Estado y terceras partes en el mercado. La información subyacente a los diferentes tipos de socieda-

[15] Generalmente, quienes deben diligenciar esta información son funcionarios de nivel directivo y con responsabilidad directa en la toma de decisiones de las autoridades o empresas públicas, así como otros con funciones de asesoría para los tomadores de decisiones.
[16] Este tipo de datos podría no estar completamente disponible para consulta pública, puesto que contiene campos de información personal (direcciones, números de cuenta), por lo que se considera reservada ante las leyes de acceso a la información o protegida por las leyes de acceso a datos personales. No obstante, son de gran utilidad en actuaciones administrativas o judiciales.
[17] Ver http://servidorespublicos.gob.mx/registro/consulta.jsf
[18] Es interesante este caso porque se puede hacer el rastreo público de la solicitud de información y de la respuesta generada por las entidades públicas. En el portal https://informacionpublica.paraguay.gov.py/ se puede consultar con el parámetro de búsqueda «declaración» las solicitudes y respuestas al respecto de declaraciones de bienes de funcionarios de ese país.
[19] Ver nota de pie de página número 15.
[20] Seco y Muñoz. (2018). Panorama del uso de las tecnologías y soluciones digitales innovadoras en la política y la gestión fiscal. Documento de trabajo, Washington, D.C.: IDB. Disponible en: https://publications.iadb.org/publications/spanish/document/Panorama-del-uso-de-las-tecnolog%C3%ADas-y-soluciones-digitales-innovadoras-en-la-pol%C3%ADtica-y-la- gesti%C3%B3n-fiscal.pdf

des y vehículos corporativos, como patrimonio, accionistas, miembros de órganos directivos, representación legal y beneficiarios finales, al igual que las relaciones entre matrices y subsidiarias, generalmente es administrada y centralizada por entidades encargadas de dar fe pública de dichos registros. Por ejemplo, el Registro Único Empresarial y Social (**RUES**), en Colombia, concentra información de todas las cámaras de comercio y permite la posibilidad de consulta abierta de la ciudadanía en tanto tenga el número de identificación tributaria de la compañía que busca indagar.

5. **Sanciones a personas naturales y jurídicas:** las autoridades judiciales tienen la facultad de condenar prácticas relacionadas con corrupción, como el soborno o la celebración indebida de contratos, y generar registros sobre dichas actuaciones. Por su parte, algunas autoridades administrativas pueden castigar conductas como la colusión o cartelización, las cuales son especialmente importantes en la contratación pública. Los datos sobre la penalización de la corrupción o lavado de activos resultan fundamentales para identificar algunos patrones (cuáles conductas son las más repetidas, promedios de las condenas o multas, lugares de comisión de delitos, etc.), y para entender mejor la naturaleza del fenómeno. Igualmente, dichos registros son necesarios para hacer cumplir prohibiciones o restricciones sobre los sancionados para hacer transacciones con el Estado o con particulares.

6. **Datos de inteligencia financiera[21]:** actualmente, 17 países de América Latina hacen parte del Grupo de Acción Financiera de Latinoamérica (**GAFILAT**), versión regional del Grupo de Acción Financiera (GAFI), mandatado para prevenir y combatir el lavado de activos. GAFILAT ha generado recomendaciones para la consolidación de las Unidades de Inteligencia Financiera (UIF), así como de la cooperación judicial regional para la investigación y sanción de crímenes de lavado. Medidas de manejo de información como el Reporte de Operaciones Financieras Sospechosas o la distinción de Personas Políticamente Expuestas[22] ayudan a consolidar información que permite hacer seguimiento a operaciones transnacionales, entender sus patrones e identificar riesgos que, en muchos casos, están asociados a fenómenos de corrupción.

Estos conjuntos de datos son un insumo importante para identificar prácticas indebidas y riesgos de corrupción, a partir de tres tipos de análisis: descriptivo, preventivo o prescriptivo (Cetina, Fonseca y Zuleta, 2021). Con las innovaciones digitales, se busca superar los roles reactivos y adoptar otros más proactivos (es decir, de prevención motivada por la capacidad de predicción) en la lucha contra la corrupción. En un rol reactivo, los

[21] Esta información también tiene restricciones de acceso al público. Puede ser clasificada o reservada, por lo que caen en las excepciones al principio de publicidad existentes en las leyes de acceso a la información.
[22] Véase Grupo de Acción Financiera de Latinoamérica https://www.gafilat.org/index.php/es/gafilat/preguntas-frecuentes

sujetos interesados –empresas, el Gobierno y la sociedad civil– se concentran en la detección, divulgación y sanción de hechos una vez se ha materializado la conducta corrupta y los perjuicios derivados de esta. En el rol proactivo, las acciones indebidas se identifican de manera temprana, y se pueden prevenir fenómenos de corrupción sin esperar a que se haya lesionado el patrimonio estatal y afectado los intereses públicos.

Tabla 1.3. Propósito del uso de los datos

Descriptivo	Preventivo	Prescriptivo
Análisis de asociación de agrupación para identificar comportamientos, problemas y oportunidades	Modelos estadísticos y regresiones para detectar patrones, hacer proyecciones e identificar riesgos	Técnicas de simulación y optimización para evaluar alternativas de decisión
Gráficas, histogramas, tortas y visualizaciones interactivas para entender qué ocurrió en el pasado	Analítica de datos estructurados para entender qué es probable que ocurra	Analítica de datos estructurados para entender qué debe hacerse
Descripciones o diagnósticos sobre el gasto, categorías de bienes, obras y servicios, medios de selección, etc.	Pronósticos para apoyar la eficiencia del gasto y potenciales riesgos de corrupción	Prescripción de soluciones para la optimización de recursos, mejoras operativas y anticipación de dificultades en los procesos

Fuente: Cetina, Fonseca y Zuleta (2021).

1.3.2. Contribuciones específicas de los datos abiertos en el combate a la corrupción

Se pueden destacar algunas formas en las que la digitalización y los datos abiertos han sido empleados para lograr mayores niveles de integridad, habilitando especialmente iniciativas de rendición de cuentas y control social.

En materia de **rendición de cuentas**, por ejemplo, **CoST** (*Construction Sector Transparency Initiative*) permite a los ciudadanos interactuar con entidades del Gobierno y del sector privado para acceder a información sobre las inversiones en infraestructura pública, mediante la publicación de datos claves relacionados con lo que ocurre en cada una de las etapas del proyecto. En un ambiente web, CoST se encarga de georreferenciar la información de los proyectos de infraestructura, publicar datos abiertos sobre los diferentes proyectos, los contratos que los componen, los recursos invertidos y los beneficiarios potenciales. En América Latina, esta iniciativa está siendo adoptada en países como Argentina, Colombia, Ecuador y Panamá.

Recuadro 1.2.

Plataformas CoST para Jalisco (México) y Bogotá (Colombia)

En 2020, CAF apoyó el desarrollo de las plataformas **CosT para el estado de Jalisco**, en México, y la ciudad de Bogotá, en Colombia.
La plataforma CoST hace pública la información de proyectos de infraestructura claves para el desarrollo de estas entidades territoriales, siguiendo los lineamientos del Manual de Contrataciones Abiertas para el Estándar de Datos sobre Infraestructura (**OC4IDS**).
En el caso de Jalisco, se publican datos sobre 37 proyectos, que incluyen renovación urbana, alcantarillado y carreteras, entre otros, con un presupuesto asignado de más de USD 500 millones.
En Bogotá, se busca garantizar transparencia y rendición de cuentas en proyectos valorados en USD 7,3 billones, como la construcción de la primera línea de metro de la ciudad, hospitales, tratamiento de aguas residuales y malla vial (Iniciativa de Transparencia en Infraestructura, 2021).

Fuente: CAF (2021).

Otro ámbito en donde los datos abiertos, su consulta y uso tienen una aplicación práctica en materia de integridad es el ejercicio del *control social*, especialmente a partir de iniciativas impulsadas desde las *startups Civic Tech* y *GovTech.* Las tecnologías digitales basadas en datos buscan reinventar las prácticas del sector público, aportar nuevas capacidades e incrementar los

niveles de confianza de los ciudadanos y las empresas en las agencias del Estado. Las empresas GovTech son una apuesta por la solución de problemas públicos a través del desarrollo de innovaciones digitales que reutilizan datos (Santiso y Ortiz de Artiñano, 2020).

Por ejemplo, Datasketch, una GovTech colombiana que provee soluciones para el uso, visualización y descarga de información sobre el fortalecimiento de la gestión pública, mediante el uso intensivo de datos y nuevas tecnologías digitales (Cruz, 2020), desarrolló la plataforma **Monitor Ciudadano de la Corrupción**. En 2018, con el apoyo del Programa de las Naciones Unidas para el Desarrollo (PNUD), el Ministerio de Tecnologías de la Información y Comunicaciones (MinTIC), y la organización Somos Más, se desarrolló la plataforma Elecciones y Contratos, con el objetivo de facilitar el análisis de la relación entre los datos de financiación de campañas electorales y de contratación pública. En 2019, se lanzó la fase 3 del Monitor Ciudadano, que permite consultar datos abiertos y públicos sobre corrupción en Colombia. Con sustento en los casos de corrupción reportados por la prensa, se realizan la sistematización, categorización, validación y publicación de datos en cuatro secciones: información general (tipo de corrupción, departamento,

sector y entidad), características (año, tipo de investigación), consecuencias (afectación a grupos poblacionales y monto de dinero comprometido) y actores. Hasta 2020, la plataforma logró identificar y sistematizar 967 casos de corrupción, concentrados en los sectores de defensa y seguridad (20,79 %), judicial (11,17 %), educación (9,31 %), vivienda (8,07 %), salud (6,93 %), transporte (6,41 %) y electoral (5,89 %), entre otros, por un valor aproximado de COP 92,77 billones (Transparencia por Colombia y Monitor Ciudadano de la Corrupción, 2021). En un estudio reciente para calcular el costo-beneficio de la plataforma Monitor Ciudadano, CAF concluyó que por cada dólar invertido en este desarrollo digital se reciben 37 de retorno (Cruz, 2020).

Las tecnologías digitales basadas en datos buscan reinventar las prácticas del sector público, aportar nuevas capacidades e incrementar los niveles de confianza de los ciudadanos y las empresas en las agencias del Estado.

En Argentina, la *startup* GovTech Munidigital, fundada en 2015, facilita el control ciudadano sobre las actuaciones de los gobiernos locales (10 provincias y 50 municipios) y provee soluciones digitales para algunos de los miembros de la Red Argentina de Municipios frente al Cambio Climático (RAMCC). Además de gestionar intervenciones de arbolado público, el software MuniArbol contiene los datos sobre las especies arbóreas, imágenes, edad, estado y geoposicionamiento, entre otros. La *app* detecta irregularidades, faltantes y riesgos en la provisión de vegetación en las localidades (RAMCC, 2020). En otro esfuerzo colaborativo de reutilización de datos abiertos, la municipalidad de Villa Carlos Paz, que cuenta aproximadamente con 62 mil habitantes, empleó MuniSocial en el marco de la pandemia como herramienta para ordenar, priorizar y geolocalizar las ayudas sociales. La base de datos creada a partir de MuniSocial contiene detalles de las familias que reciben las ayudas, que pueden ser gubernamentales, provinciales o municipales, con datos de individuos concretos y requisitos específicos validados. Este aplicativo permitió que las ayudas llegaran a las personas más necesitadas y crear un mapa de zonas vulnerables (Santiso, 2020; González, s. f.).

1.4. Reflexiones finales: consolidando una agenda de datos para la integridad

La transformación digital de los Gobiernos y los datos abiertos cobraron una importancia sin precedentes para el mundo durante la crisis sanitaria y económica provocada por el COVID-19[23]. La aceleración digital también representa una oportunidad para la lucha contra la corrupción, siempre que se apoye en políticas públicas que garanticen la transparencia activa y la apertura de datos con el potencial de generar alertas sobre riesgos de corrupción.

La proliferación y reutilización de datos permite que las nuevas tecnologías hagan parte de la agenda de integridad pública. Sin embargo, **para que dicha transformación digital tenga éxito en materia anticorrupción, se requiere un ajuste tanto institucional como tecnológico en los Gobiernos, en torno a los siguientes cuatro ejes:**

1. **Es necesario adoptar reformas y prácticas que garanticen la transparencia activa en las autoridades gubernamentales**, publicando toda aquella información que no esté específicamente sometida a reservas legales o constitucionales, sin que medien peticiones, trámites administrativos o judiciales.

2. **La transparencia activa debe articularse y coordinarse con agendas de gobierno digital, para poder adoptar políticas de datos abiertos exitosas.** A medida que se digitalizan los procesos dentro de los Gobiernos y los trámites ciudadanos, deben desarrollarse mecanismos para que los datos producidos se abran al público, como sucede con las compras públicas. Esto puede extenderse a otros asuntos, como el otorgamiento de licencias, la digitalización de declaraciones de conflicto de interés y los registros de empresas con sus beneficiarios finales, entre otros. Esa apertura de datos debe asegurar estándares de calidad, estructura y reusabilidad de los datos puestos a disposición general en cada materia regulada por las leyes de acceso a la información pública.

[23] Grandes conjuntos de datos, debidamente compartidos y reutilizados, ayudaron a tener certeza sobre las circunstancias de la aparición del virus entre los humanos: el mercado ilegal de especies exóticas en la ciudad de Wuhan, China. Aún más asombroso resulta saber que fenómenos de corrupción asociados a crimen organizado habilitaron la aparición del virus, puesto que fue en medio del comercio ilegal y sacrificio de especies que el COVID-19 logró pasar de animales a humanos, dando origen a la pandemia y abriendo una nueva era para el planeta. En una especie de espiral, dicha crisis aceleró la trasformación digital de las economías y de los Gobiernos, lo cual les otorga un rol más fundamental a los datos como activo para la gestión de los Estados y el funcionamiento de los mercados.

3. **Una vez la política de datos abiertos asegura una infraestructura de datos robusta (calidad, integridad y reusabilidad), la reutilización de estos permite comprender y prevenir fenómenos complejos como la corrupción.** Adicionalmente, la transparencia en cuanto a las acciones gubernamentales y los resultados de gestión genera más confianza ciudadana. El acceso de bajo costo a datos críticos crea una base para desarrollar aplicaciones y plataformas que respondan a las necesidades de los ciudadanos, mejora la gestión de los Estados al evaluarla con análisis y cruces de grandes conjuntos de datos, y facilita la rendición de cuentas de los Gobiernos.

4. **Con una agenda de datos abiertos consolidada, los Gobiernos pueden avanzar en la adopción de estándares internacionalmente reconocidos en áreas de especial interés para la integridad pública,** como son la contratación, la tributación, el gasto público, la infraestructura y la función pública, entre otros. La aplicación de estándares y prácticas internacionales para la producción, publicación y reutilización de los datos son una alternativa costo-efectiva para contar con información útil en programas e iniciativas anticorrupción. Por ejemplo, el Programa Interamericano de Datos Abiertos (PIDA) contra la corrupción, adoptado por la Cumbre de las Américas en 2018, contiene un conjunto de recomendaciones para apalancar 30 conjuntos de datos que pueden ser usados en la lucha contra la corrupción.

Los Gobiernos de la región están experimentando procesos de transformación digital que correctamente orientados pueden generan desarrollo, confianza, integridad y valor público (Santiso, 2020). La crisis del COVID-19 aceleró ese proceso y puso en el centro de la agenda de Gobierno la necesidad de seguir avanzando en la transformación digital y en fomentar políticas de integridad. Nuevos desarrollos en tecnologías de información y comunicaciones, acompañados de una política de datos abiertos, contribuyeron en el frente de batalla contra el coronavirus, y también tienen el potencial de ayudar en la lucha contra la corrupción.

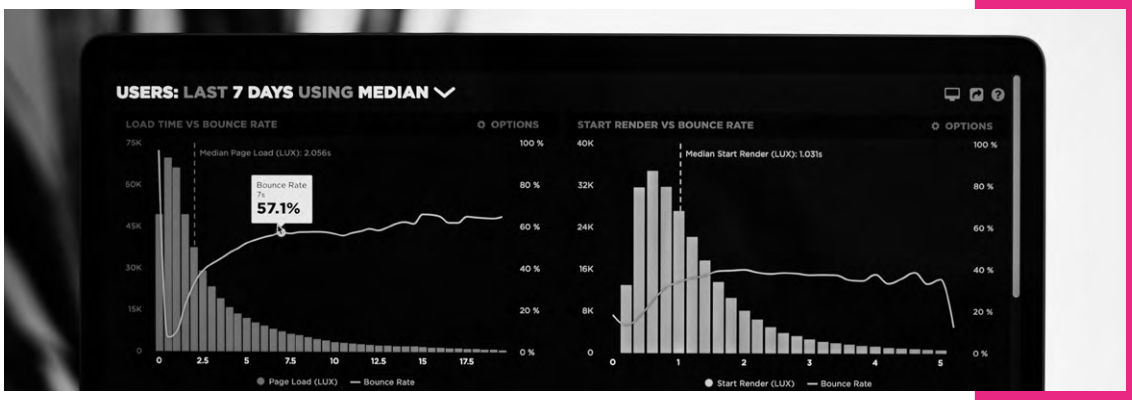
2.

Aproximación a la evidencia sobre los vínculos entre digitalización e integridad

—[…] Es un error capital teorizar antes de tener datos. Sin darse cuenta, uno empieza a deformar los hechos para que se ajusten a las teorías, en lugar de ajustar las teorías a los hechos".

Sir Arthur Conan Doyle, Escándalo en Bohemia, en Las aventuras de Sherlock Holmes

Aproximación a la evidencia sobre los vínculos entre digitalización e integridad



En la última década del siglo XX, **el gobierno electrónico empezó a ganar tracción dada la necesidad de implementar soluciones tecnológicas para modernizar la gestión pública**, mejorar la prestación de servicios gubernamentales a los ciudadanos y empoderar a la empresa privada y la sociedad civil a través de más transparencia y acceso a la información (OCDE, 2003; Banco Mundial, 2015). **De forma independiente y paralela, la lucha contra la corrupción comenzó a exigir mecanismos de coordinación entre los países:** en 1996, con la Convención Interamericana; en 1997, con la Convención Anticohecho de la OCDE; en 2003, con la Convención de Naciones Unidas contra la Corrupción. En cada uno de estos instrumentos, se empezó a fomentar la transparencia activa y a reconocer el papel que las tecnologías y los datos tienen en la adopción y seguimiento sobre las medidas para prevenir la corrupción (ver capítulo 1).

La relación entre las políticas de transparencia y las de gobierno electrónico comenzó a hacerse evidente en el sector de la hacienda pública a principios del siglo XXI. Primero, las bases de datos de los Gobiernos debían ordenarse a la hora de presentar las cuentas públicas y acceder al crédito internacional. El impulso de los organismos internacionales de crédito para que los Gobiernos adoptaran estándares en el ordenamiento y estructura de los datos sobre las finanzas públicas fue determinante. Ello abrió ventanas para diseñar medidas de control del gasto, detectar ineficiencias y mejorar la inversión. El gobierno electrónico fue ganando espacio de la mano de las TIC en el área de las finanzas públicas, especialmente respecto al manejo de la previsión social y los planes sociales (que se multiplicaron a partir del año 2000), y en las transferencias fiscales a los niveles subnacionales.

Así, se alinearon, de un modo casi casual, dos tendencias internacionales en ecosistemas diferentes: la de las convenciones internacionales que comenzaron a promover entre los Gobiernos la adopción de medidas de transparencia e integridad pública, y la del Gobierno, que encontraba en las TIC un medio para ordenar y revelar información concerniente a su gestión fiscal y sus resultados.

Las agendas de integración de la tecnología y de transparencia en las políticas públicas comenzaron a entrelazarse con mayor claridad en 2009. Ese año, un memo de la presidencia de los Estados Unidos acuñó el concepto de **gobierno abierto**, el cual promovía una iniciativa de gestión gubernamental basada en la transparencia, la colaboración, la participación y la innovación digital. Este punto de inflexión llevaría a la constitución de la Alianza para el Gobierno Abierto. Así, **la agenda de transparencia empezó a sincronizarse con el paso de gobiernos analógicos a digitales, haciendo de la tecnología una herramienta determinante para la concepción de** gobierno abierto, en donde la información y la comunicación permean la gestión de los órganos públicos y facilitan la interacción con los ciudadanos.

Hacia la segunda década del siglo XXI, la aceleración de la producción de datos y su procesamiento masivo para la toma de decisiones, predicciones y corrección de modalidades del gasto público permitió a los Gobiernos **implementar repositorios de datos públicos para mejorar el monitoreo de la gestión pública** (BID, 2016). Esta evolución implicó ir más allá de la simple introducción de las tecnologías digitales en la gestión pública; hubo que incorporarlas para una verdadera modernización del sector público, que ejecutara procesos y suministrara servicios centrados en el ciudadano (Santiso y Ortiz, 2020).

Aunque, de modo gradual, los procesos de digitalización y lucha contra la corrupción se interrelacionan en la gestión pública, la literatura no ha documentado con la misma abundancia la dinámica detrás de ese vínculo.

Aunque, de modo gradual, los procesos de digitalización y lucha contra la corrupción se interrelacionan en la gestión pública, la literatura no ha documentado con la misma abundancia la dinámica detrás de ese vínculo. Un grupo de hallazgos se restringe a vincular fenómenos específicos de digitalización con la prevalencia o reducción de la corrupción. Por ejemplo, Andersen, Bentzen, Dalgaard y Selaya (2010) sostienen que internet es una poderosa tecnología anticorrupción y también un importante impulsor del crecimiento económico. Haafst (2017) muestra evidencia, sugiriendo que no es internet o la digitalización lo que influye en la corrupción, sino los procedimientos burocráticos que subyacen a la digitalización. Bologna (2014) aborda el concepto de alfabetización digital y sugiere que existe una correlación negativa entre la alfabetización digital y la corrupción. Finalmente, Bailard (2009) apoya esa idea mediante el uso del teléfono móvil, y afirma que la descentralización de la información disminuye las oportunidades de corrupción.

El trabajo seminal de Choi (2014) abordó de modo más integral el concepto de *e-Government* y encontró efectos positivos en la reducción de la corrupción. El autor empleó los resultados del Índice de Desarrollo de Gobierno Electrónico (IDGE) y los subíndices de infraestructura de telecomunicaciones, partici-

pación ciudadana en línea y servicios ciudadanos en línea, para concluir que dichas dimensiones tienen una influencia estadísticamente significativa sobre la corrupción. En particular, sugiere que el Gobierno facilita el acceso a la información, abre espacios de rendición de cuentas y empodera a los ciudadanos para interactuar con él.

Sin embargo, la aceleración digital que en los últimos 10 años ha afectado el modo en que las instituciones públicas suministran servicios, así como la escala en la reutilización de grandes conjuntos de datos, sugieren que la relación entre gobierno digital e integridad ofrece más propiedades que deben ser consideradas para la formulación e implementación de políticas de integridad. Este capítulo busca documentar algunas propiedades del gobierno digital, como sigue:

- **En la primera parte, se hace un análisis de la evidencia estadística que explora tanto la relación entre gobierno digital e integridad como los efectos probados que tiene aquel en la reducción de los fenómenos de corrupción** dentro de sectores especialmente sensibles a las finanzas públicas (*i. e.*, gasto e inversión pública, fiscalización interna, compras públicas y aduanas).

- **En la segunda parte, se describen algunas experiencias de América Latina, en donde la expansión de políticas y servicios de gobierno digital mostraron dividendos en materia de integridad.** Este segmento analiza, desde un punto de vista cualitativo, experiencias específicas de algunos países en tres frentes de operación: trámites, compras públicas y participación ciudadana.

- **Al final, se reflexiona sobre la evidencia presentada y las lecciones que esta ofrece en materia de digitalización e integridad pública.** En general, podemos observar que aún es necesario aunar esfuerzos entre academia, sector público y sociedad civil para identificar las estrategias más efectivas de digitalización en la lucha contra la corrupción. Esto implica adoptar prácticas de reutilización de los datos en las iniciativas de digitalización de los Gobiernos, para propósitos de evaluación de política pública como parte integrante del ciclo de política de gobierno digital.

2.1. Análisis cuantitativo: revisión estadística sobre la relación entre transformación digital y prevención de la corrupción

La tecnología ocupa un espacio importante en las discusiones de política pública, como una herramienta esencial en materia anticorrupción. Ese espacio es cada vez mayor, a medida que aparecen nuevas aplicaciones y soluciones digitales con potencial en este campo. Sin embargo, hay relativamente poca evidencia causal del impacto de herramientas tecnológicas específicas. Ese déficit de evidencia no es único de las iniciativas de carácter tecnológico: hay poco conocimiento sobre el impacto de políticas anticorrupción de cualquier índole porque la corrupción es un fenómeno difícil de estudiar cuantitativamente.

En los últimos años, han comenzado a aparecer estudios de calidad sobre estos temas. El objetivo de este capítulo es documentar la efectividad de distintas herramientas tecnológicas en el control de la corrupción. Además, se hará un esfuerzo por entender las razones que explican que algunas intervenciones prosperen y otras no. Esto último es crucial para hacer un análisis prospectivo de las herramientas de punta que empiezan a ser aplicadas en algunos contextos pero que, por su novedad, aún no han podido ser evaluadas. En esta revisión, se valorará la rigurosidad metodológica de los estudios considerados, dando mayor peso y prioridad a aquellos que logran mostrar relaciones causales de manera creíble.

2.1.1. Correlación entre corrupción y digitalización

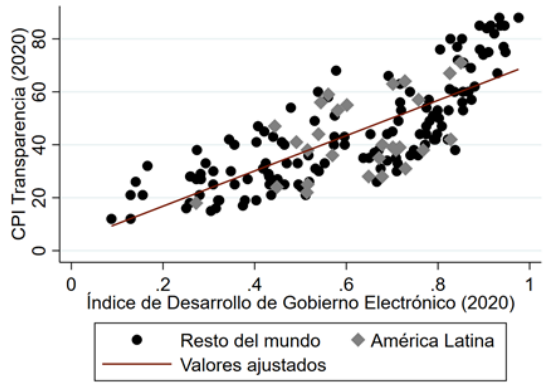
Antes de iniciar los análisis de causalidad, es importante subrayar que existe una clara correlación entre la digitalización del Estado y el control de la corrupción, de acuerdo con múltiples indicadores agregados (Gallego, 2021). Por ejemplo, países con mayores valores en el IDGE de Naciones Unidas también muestran mejores resultados en el Índice de Percepción de la Corrupción (IPC) de Transparencia Internacional, como muestra la figura 2.1 (números mayores en el IPC señalan menor percepción de corrupción en el país).

Esa correlación es robusta a la utilización de medidas alternativas de digitalización o corrupción. Por ejemplo, en el panel B de la figura 2.1, se sustituye el IDGE con el Índice de Adopción Digital del Banco Mundial. En los paneles C y D, se sustituye el IPC, respectivamente, con la medida de control de la corrupción de los Indicadores de Gobernanza Mundial del Banco Mundial y una medida de autorreporte de pago de sobornos de Transparencia Internacional. En todos los casos, se mantiene la misma relación[24].

[24] En el panel D, el signo de la correlación es negativo porque el indicador de corrupción usado allí toma valores mayores cuando la corrupción es alta, al contrario que en los indicadores de los otros paneles.

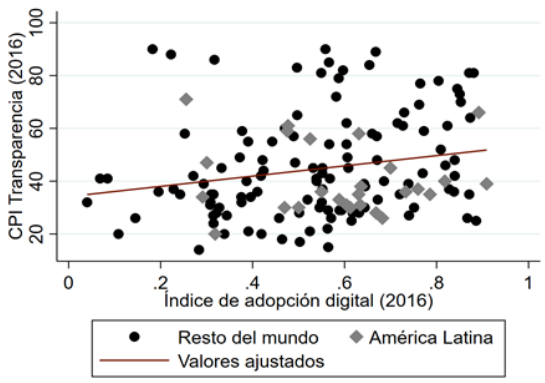
Figura 2.1: Correlación entre digitalización y corrupción en países de América Latina

Panel A. Gobierno electrónico y transparencia



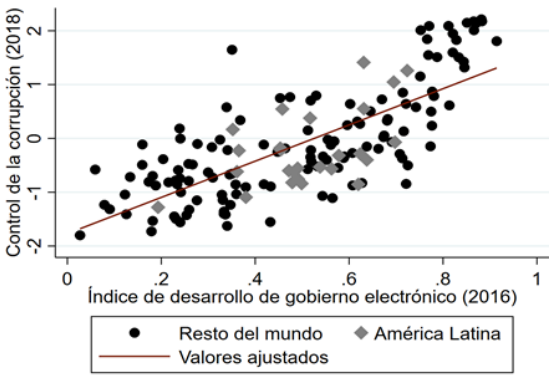
Nota: Se reporta el Índice de Desarrollo de Gobierno Electrónico de las Naciones Unidas (eje horizontal), en el que valores más altos muestran mayor desarrollo electrónico, y el Índice de Percepción de la Corrupción de Transparencia Internacional (eje vertical), en el que valores mayores señalan menor percepción de corrupción. La línea continua representa la correlación entre las variables. La muestra la componen 28 países de América Latina.

Panel B. Adopción digital y transparencia



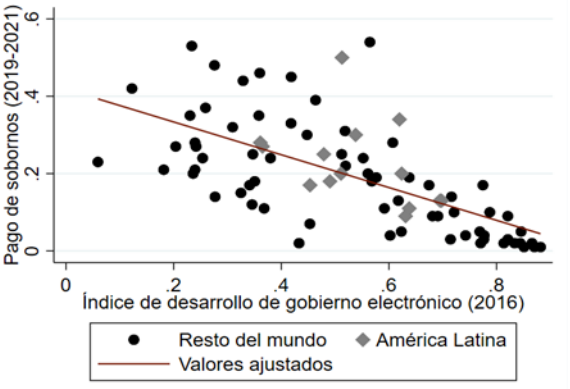
Nota: Se reporta el Índice de Desarrollo de Gobierno Electrónico de las Naciones Unidas (eje horizontal), en el que valores más altos marcan un mayor desarrollo electrónico, y el indicador de Pago de Sobornos del Barómetro Global de Corrupción de Transparencia Internacional (eje vertical), que señala el porcentaje de usuarios de servicios públicos que reportan haber pagado un soborno por recibir esos servicios. La línea continua representa la correlación entre las variables. La muestra la componen 14 países de América Latina.

Panel C: Gobierno electrónico y control sobornos



Nota: Se reporta el Barómetro de Datos Abiertos de CAF (eje horizontal), en el que valores más altos denotan mayor desarrollo de datos abiertos, y el Índice de Percepción de la Corrupción de Transparencia Internacional (eje vertical), en el que valores mayores evidencian menor percepción de corrupción. La línea continua representa la correlación entre las variables. La muestra la componen 23 países de América Latina.

Panel D: Gobierno electrónico y pago de



Nota: Se reporta el Barómetro de Datos Abiertos de CAF (eje horizontal), en el que valores más altos muestran mayor desarrollo de datos abiertos, y el indicador de Pago de Sobornos del Barómetro Global de Corrupción de Transparencia Internacional (eje vertical), que señala el porcentaje de usuarios de servicios públicos que reportan haber pagado un soborno por recibir esos servicios. La línea continua representa la correlación entre las variables. La muestra la componen 23 países de América Latina.

Fuente: Gallego (2021).

Al restringir la muestra a países de América Latina, el patrón general se sostiene. El IDGE se asocia a menor percepción de corrupción (según el IPC de Transparencia Internacional) y a menor reporte de pago de sobornos (de nuevo, de acuerdo con la medida recogida por TI), como se puede apreciar en los paneles A y B de la figura 2.2.

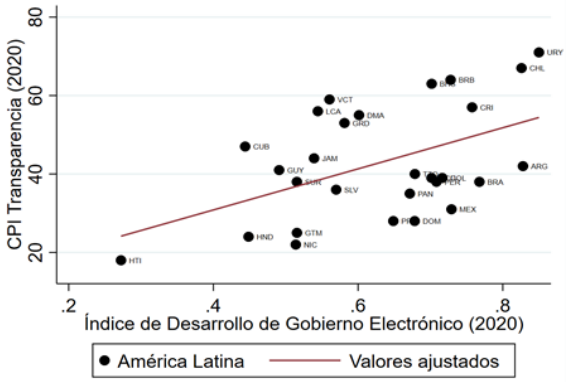
Sin embargo, la correlación se debilita o desaparece cuando se usa el Barómetro de Datos Abiertos como medida de digitalización del Estado (figura 2.2, paneles C y D). Al observar el conjunto de los países de América Latina, este indicador no tiene una asociación clara con el nivel de corrupción.

El Barómetro de Datos Abiertos se enfoca específicamente en medir el grado de apertura de datos, mientras que el IDGE captura de manera más integral el uso de soluciones y herramientas digitales en la gestión pública. Por tanto, una posible interpretación de las correlaciones vistas hasta ahora es que la apertura de datos, por sí sola, no es suficiente para reducir la corrupción, y que hace falta una utilización más profunda de la tecnología en la gestión de los Estados para generar cambios[25].

[25] En esa dirección, algunos estudios sugieren que, en las estrategias de gobierno digital, el elemento transaccional (es decir, la capacidad de obtener servicios y completar transacciones con el Estado) es el más importante para mover las percepciones de transparencia que tienen los ciudadanos. Lizardo (2018) encuentra que el acceso electrónico a trámites y la calidad de la infraestructura de telecomunicaciones son los componentes de gobierno electrónico que se correlacionan más con las percepciones de corrupción, mientras que Valle-Cruz, Sandoval y Gil-García (2016) observan que la calidad y completitud de las páginas web y de los canales digitales de comunicación de los órganos del Gobierno se asocian a mejores opiniones sobre su transparencia por parte de la población en municipios mexicanos. Aunque estos resultados son sugerentes, es importante destacar que no hacen referencia a intervenciones específicas, y tampoco analizan efectos sobre los niveles reales de corrupción.

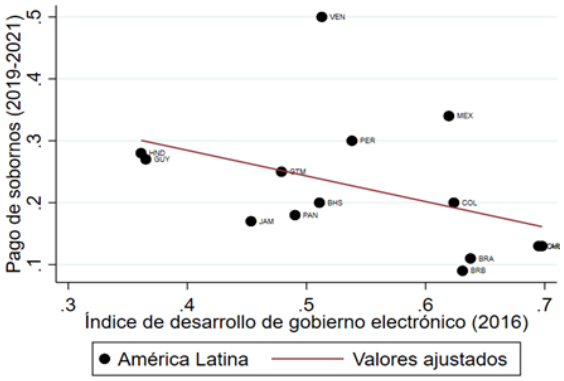
Figura 2.2: Correlación entre digitalización y corrupción

Panel A. Gobierno electrónico y transparencia en AL



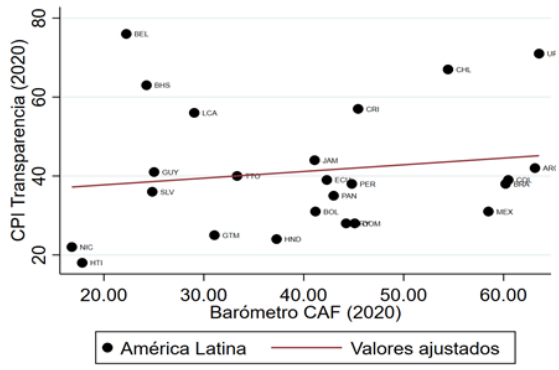
Nota: Se reporta el Índice de Desarrollo de Gobierno Electrónico de las Naciones Unidas (eje horizontal), en el que valores más altos muestran mayor desarrollo electrónico, y el Índice de Percepción de la Corrupción de Transparencia Internacional (eje vertical), en el que valores mayores señalan menor percepción de corrupción. La línea continua representa la correlación entre las variables. La muestra la componen 28 países de América Latina.

Panel B. Adopción digital y sobornos en AL



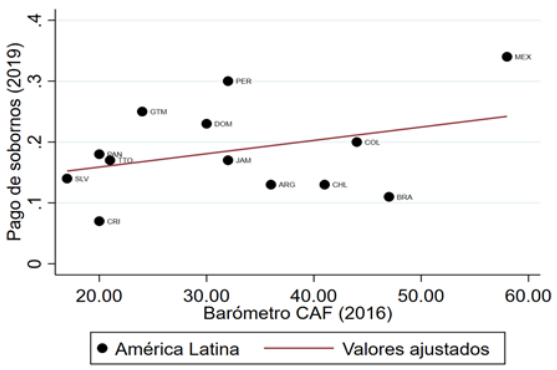
Nota: Se reporta el Índice de Desarrollo de Gobierno Electrónico de las Naciones Unidas (eje horizontal), en el que valores más altos marcan un mayor desarrollo electrónico, y el indicador de Pago de Sobornos del Barómetro Global de Corrupción de Transparencia Internacional (eje vertical), que señala el porcentaje de usuarios de servicios públicos que reportan haber pagado un soborno por recibir esos servicios. La línea continua representa la correlación entre las variables. La muestra la componen 14 países de América Latina.

Panel C. Datos abiertos y transparencia en AL



Nota: Se reporta el Barómetro de Datos Abiertos de CAF (eje horizontal), en el que valores más altos denotan mayor desarrollo de datos abiertos, y el Índice de Percepción de la Corrupción de Transparencia Internacional (eje vertical), en el que valores mayores evidencian menor percepción de corrupción. La línea continua representa la correlación entre las variables. La muestra la componen 23 países de América Latina.

Panel D. Datos abiertos y sobornos en AL



Nota: Se reporta el Barómetro de Datos Abiertos de CAF (eje horizontal), en el que valores más altos muestran mayor desarrollo de datos abiertos, y el indicador de Pago de Sobornos del Barómetro Global de Corrupción de Transparencia Internacional (eje vertical), que señala el porcentaje de usuarios de servicios públicos que reportan haber pagado un soborno por recibir esos servicios. La línea continua representa la correlación entre las variables. La muestra la componen 23 países de América Latina.

Fuente: Gallego (2021).

Aunque las correlaciones observadas muestran patrones interesantes, son insuficientes como evidencia concluyente sobre el impacto de las herramientas digitales en la corrupción. Para responder a esa pregunta, el resto de este capítulo analiza estudios que estiman efectos causales de intervenciones específicas en distintos contextos. Ordenaremos la discusión clasificando las intervenciones según las tareas del Estado que afectan principalmente el comportamiento del gasto público, como lo son el monitoreo de gasto e inversión, fiscalización interna, gestión de las compras públicas, control y seguimiento de transferencias, y la gestión aduanera.

2.1.2. Inversión y gasto público

La generación y difusión de información es uno de los principales mecanismos a través de los cuales la digitalización del Estado puede ayudar a disminuir la corrupción. Como principio general, si los gastos e inversiones llevados a cabo por las entidades públicas dejan un rastro digital, se incrementa la información disponible para que la ciudadanía y los órganos de control los monitoreen. Esta idea es consistente con evidencia proveniente de iniciativas recientes en América Latina.

Inversión

En la región, en años recientes, las plataformas de divulgación de información relacionada con los proyectos de inversión pública se han vuelto particularmente populares. La plataforma **MapaInversiones, desarrollada con el apoyo del Banco Interamericano de Desarrollo (BID)**, se sustenta en la experiencia **MapaRegalías** en Colombia, que, desde 2012 y a través de georreferenciación, permite conocer el avance de los proyectos de inversión pública financiados con regalías. En Costa Rica, desde 2018, se viene utilizando una plataforma llamada **MapaInversiones**, un portal web que permite a los ciudadanos acceder a información georreferenciada, verificar el progreso y hacer consultas sobre diferentes proyectos de inversión pública.

Rossi, Vásquez y Cruz (2020) evaluaron el impacto de MapaInversiones en Costa Rica, usando un universo de 649 proyectos de inversión pública, administrados y ejecutados por 57 organismos de diversos sectores. Los proyectos variaron en tamaño (desde la compra de mobiliario escolar hasta la construcción de sistemas de abastecimiento de agua) y alcanzaron un monto total de USD 13 000 millones, aproximadamente. Sobre ese universo de proyectos, se hizo un experimento aleatorio controlado (RCT, por sus siglas en inglés): 460 proyectos elegidos al azar fueron publicados en abril de 2018, y los 189 restantes, un año más tarde.

Los resultados del experimento sugieren efectos que aparecen muy pronto. En el corto plazo (tres meses después de la publicación en el portal), los proyectos publicados presentaron un mayor grado de avance físico (13,5 %) y financiero (127,4 %) que los no publicados. En el mediano plazo (a un año de la publicación) los impactos se atenuaron: las diferencias en avance financiero se redujeron a un todavía alto 57,4 %, y las diferencias en avance físico desaparecieron. Estos resultados sugieren que la implementación de la herramienta digital tuvo efectos positivos en la gestión de los proyectos, sobre todo en el corto plazo. Sin embargo, los autores no discuten por qué el efecto es mayor en el avance financiero que en el físico.

La plataforma tiene funcionalidades que facilitan compartir la información a través de redes sociales o correos electrónicos.

Otros dos resultados interesantes surgen del estudio. Primero, investigando los mecanismos detrás del impacto observado, los autores señalan que el monitoreo ciudadano de los proyectos se incrementó gracias a la implementación de la plataforma. En particular, muestran que la probabilidad de que un proyecto reciba comentarios u observaciones aumenta siete puntos porcentuales cuando se publica en la plataforma. En segundo lugar, encuentran que los efectos se dan casi exclusivamente en los proyectos más chicos, lo que es consistente con la idea de que el monitoreo ciudadano puede ser más relevante ante proyectos relativamente sencillos y de menor escala.

Un caso similar es el de la introducción de **MapaRegalías** en Colombia. Esta plataforma, lanzada en agosto de 2014 por el Departamento Nacional de Planeación (DNP), presenta información georreferenciada y datos sobre las regalías provenientes del sector extractivo y los proyectos financiados con las mismas[26]. En el ambiente web de MapaRegalías, los usuarios pueden encontrar perfiles de proyecto que incluyen información sobre el monto ejecutado, las fuentes de financiamiento, el organismo ejecutor, los contratistas y auditores, y una galería de fotos para observar el nivel de avance de las construcciones. También se pueden ver datos a nivel de departamento o municipalidad, incluyendo el monto de las regalías recibidas por la jurisdicción, los proyectos en que se invierten esos recursos y la producción de hidrocarburos y minerales en la jurisdicción. La plataforma tiene funcionalidades que facilitan compartir la información a través de redes sociales o correos electrónicos.

La estrategia de implementación de MapaRegalías no permite emplear una metodología rigurosa para medir con claridad sus impactos causales sobre la gestión de los proyectos. Sin embargo, Lauletta, Rossi, Cruz y Arisi (2019) aportan algunos datos descriptivos sobre el ritmo de avance de los proyectos

[26] El desarrollo de esta plataforma siguió a una reforma más integral sobre el mecanismo de distribución de recursos provenientes de las actividades extractivas, que se materializó con la creación del Sistema General de Regalías (SGR). El cambio más importante del SGR fue la modificación en la regla de repartición de los recursos, pues las regalías ya no irían en su mayoría a las regiones productoras, sino que se crearían fondos a los cuales podrían acceder, con previa solicitud, municipios productores y no productores. Además, los mecanismos de monitoreo, vigilancia y rendición de cuentas también fueron ampliamente modificados. Gallego, Maldonado y Trujillo (2020) muestran que esta reforma tuvo efectos positivos en el bienestar de los hogares colombianos, al incrementar el impacto de las regalías sobre la incidencia de la pobreza multidimensional en el país.

La generación y difusión de información es uno de los principales mecanismos a través de los cuales la digitalización del Estado puede ayudar a disminuir la corrupción.

antes y después de la puesta en marcha de la página. A partir de una muestra de 321 proyectos, los autores encuentran que el nivel de avance físico de las obras aumentó siete puntos porcentuales en promedio tras la introducción de MapaRegalías. En cuanto al grado de utilización de la página, los autores señalan que en 2016 (último año observado en el estudio) tuvo 74 742 visitas, con una tendencia ligeramente creciente desde su lanzamiento[27]. Si bien los datos permiten establecer una mejora en la gestión del gasto y no necesariamente sobre la reducción de corrupción, los efectos medidos son generalmente ligados y difíciles de distinguir.

Gasto público

Una experiencia que hace uso de la telefonía móvil es la intervención en el Programa de Alimentación Escolar (PAE) en Colombia. A través del PAE, el Ministerio de Educación transfiere fondos del Gobierno central para financiar comidas en las escuelas públicas. Su implementación, que implica la contratación y supervisión de proveedores, es responsabilidad de los gobiernos subnacionales (departamentos, principalmente, y algunos municipios certificados). Tras algunas denuncias públicas sobre la calidad de los alimentos, el Gobierno decidió hacer una intervención para mejorar el cumplimiento de las condiciones contractuales por parte de los proveedores. La intervención tuvo dos componentes: i) la realización de auditorías informales continuas sobre la calidad de la comida, y ii) el envío semanal de mensajes de texto a los padres con información sobre las comidas que sus hijos deberían recibir (de acuerdo con las obligaciones contractuales de los proveedores).

Keefer y Roseth (2021) encontraron que la intervención tuvo efectos positivos en el cumplimiento de los operadores con el menú exigido contractualmente. En cuanto a los mecanismos, es imposible separar claramente el papel de las auditorías y el de la campaña de información a los padres. Sin embargo, los autores encuentran pistas de que la campaña de información tuvo algún efecto. En particular, observan que los mensajes de texto aumentaron (en aproximadamente 50 %) la participación de los padres en comités y reuniones de monitoreo del PAE.

El conjunto de casos descritos muestra que el uso de herramientas digitales para fomentar el control ciudadano contra la corrupción tiene evidencia mixta. Esto es consistente con una literatura más amplia sobre la efectividad del monitoreo por parte de la ciudadanía para prevenir y castigar la corrupción, y que ha encontrado resultados que varían mucho entre experiencias (se pueden contrastar, por ejemplo, los trabajos de Bjorkman y Svensson, 2009, y Olken, 2007). Esta aparente inconsistencia refleja que la efectividad de

[27] Además de facilitar el monitoreo ciudadano, MapaRegalías puede facilitar el control oficial dentro del Estado. Por mandato legislativo, las agencias ejecutoras tienen la obligación de subir a la plataforma (gestionada por el DNP) la información sobre los proyectos dentro de un calendario estipulado, con sanciones establecidas en caso de incumplimiento. Estas responsabilidades bien definidas pueden facilitar la tarea de control del DNP.

este tipo de iniciativas depende de muchas variables contextuales, referidas tanto a los detalles de la intervención específica que se considera como al tipo de corrupción que se quiere combatir y al funcionamiento del entramado institucional general.

En el caso de las políticas de transparencia y apertura de datos, su valor para generar cambios depende de que la información que se difunda cumpla con ciertos estándares y de su utilización por parte de los órganos de control y la ciudadanía. Así, la utilización de los datos por parte de los interesados refuerza el proceso de rendición de cuentas.

La Alianza para el Gobierno Abierto propone algunos estándares en esta materia, que apuntan a que el control del gasto a través de las herramientas digitales sea más efectivo. Lamentablemente, no hay estudios empíricos que evalúen los impactos de la adopción de este tipo de estándares sobre la corrupción. En cambio, sí hay evidencia descriptiva sobre las dificultades para su adopción. Por ejemplo, Sheffer, Pizzigatti y Soares (2014) analizan los portales de transparencia de los municipios brasileños, y concluyen que dicha implementación no ha cumplido a cabalidad con los estándares y requerimientos técnicos de gobierno abierto comúnmente aceptados. Los requerimientos en los que se presenta más incumplimiento son aquellos relacionados con la estructura y el formato de los datos, la facilidad para buscarlos y acceder a ellos, y la posibilidad de automatizar los procesos de extracción, procesamiento y análisis (*machine readability*).

De manera similar, Cardona, Cortés y Wong (2015) encuentran –a través de encuestas a funcionarios y ciudadanos– que el grado de transparencia en municipalidades panameñas es bajo, a pesar de la implementación de programas gubernamentales para promover la apertura de datos fiscales. Por ejemplo, 48 % de los gobiernos municipales reconoció que los ciudadanos no tienen vías de acceso a información sobre el manejo presupuestal. Además, cuando sí pueden consultar, por lo general, es por canales diferentes a los digitales.

Estos estudios ponen de manifiesto que, aunque en la región hay interés en abrir datos y crear una cultura de la transparencia potenciada por la digitalización, en la práctica, aún existen importantes barreras a la información. Una consecuencia directa de esto es que se dificulta el adecuado ejercicio del monitoreo ciudadano. Adicionalmente, esta distancia entre las políticas formales de transparencia y la implementación efectiva de las mismas ayuda a explicar la escasez de evidencia creíble sobre este tipo de herramientas.

2.1.3. Fiscalización interna

En la sección anterior, nos enfocamos en las herramientas para auspiciar el monitoreo ciudadano. Por supuesto, la **tecnología también puede usarse para potenciar las capacidades de los órganos de control del Estado.** En particular, los modelos de aprendizaje automático (*machine learning*) pueden aportar mucho a las tareas de fiscalización de cuentas y transacciones. La idea general es la siguiente: si se tienen una base de datos amplia (con muchas variables y observaciones) de algún tipo de transacción oficial (por ejemplo, compras públicas de insumos) e información sobre cuáles de esas transacciones presentaron irregularidades, se puede entrenar un modelo computacional que descubra los patrones en las variables observadas que se asocian a la incidencia de irregularidades. Con ese modelo, las transacciones subsiguientes pueden ser evaluadas para estimar el riesgo de irregularidades en la misma. Mientras más datos se usen para alimentar el modelo, mejores las predicciones que generará.

Estas son herramientas relativamente nuevas y, en consecuencia, hay poca evidencia sobre su funcionamiento. El principal obstáculo a su implementación es la necesidad de datos suficientemente ricos y sistemáticos para poder entrenar modelos funcionales. Sin datos, estas soluciones no se pueden aplicar. Pero una vez superado ese alto costo de entrada, estos modelos pueden ser una manera relativamente económica de evaluar riesgos en la gestión pública, y asignar de manera más eficiente los recursos humanos de fiscalización e investigación.

Las aplicaciones específicas se pueden dar en distintas áreas. Como se sugirió anteriormente, el control de las compras y contrataciones públicas es una de las tareas en donde se ha visto potencial para estos modelos. Gallego, Rivero y Martínez (2021) discuten la utilidad de estos enfoques, entrenando un modelo a partir de datos de dos millones de contratos de compras públicas en Colombia para predecir casos de irregularidades, incumplimiento de contratos e ineficiencias de implementación. Ash, Galletta y Giommoni (2020) exploran otra aplicación: la detección de corrupción a partir de presupuestos gubernamentales. Para eso, desarrollan un modelo usando presupuestos detallados de los municipios brasileños, que entrenan con datos sobre irregularidades provenientes de auditorías oficiales. Los autores argumentan que la capacidad predictiva del modelo es alta y que usar esas predicciones para definir dónde auditar llevaría a un aumento en la tasa de detección de irregularidades respecto al *statu quo* (en el que las auditorías se hacen de manera aleatoria). Finalmente, otros autores han desarrollado modelos para la predicción de fraude tributario, a partir de datos de declaraciones y contribuyentes (De Roux, Pérez, Moreno, Villamil y Figueroa, 2018; Solon, Rigitano, Carvalho y Souza, 2016; Castellón y Velásquez, 2013).

A pesar de que no existe evidencia clara sobre la efectividad de las herramientas de aprendizaje automático, parecen una vía muy promisoria para mejorar los procesos de control interno, especialmente porque son un instrumento flexible que se puede incorporar progresivamente dentro de los protocolos tradicionales de trabajo, sin generar rupturas muy costosas.

2.1.4. Compras públicas

La adquisición de bienes y servicios es una tarea cotidiana en los órganos públicos y, dados los recursos que se manejan y los espacios de discrecionalidad que existen, el riesgo de corrupción en este campo es una fuente de preocupación constante. En realidad, no hay estimaciones claras sobre la incidencia o magnitud de la corrupción en compras públicas, pero sí buena evidencia sobre algunos factores que aumentan el riesgo de irregularidades en los procesos licitatorios.

El factor de riesgo más señalado en la literatura tiene que ver con las modalidades de licitación y contratación: los procesos cerrados y discrecionales presentan más irregularidades que los procesos abiertos. Hay varios ejemplos de esto. Corredor (2018) muestra que, en el contexto del PAE en Colombia, la contratación directa de proveedores facilita la provisión de alimentos de menor calidad y mayor costo. Brugués, Brugués y Giambra (2018) encuentran que, en Ecuador, las empresas privadas que poseen conexiones con funcionarios públicos evidencian una probabilidad mayor a

las no conectadas de obtener contratos con el Estado, pero solo en los casos en que los funcionarios tengan discreción para la asignación del contrato. Zamboni y Litschig (2018) muestran que, para Brasil, las modalidades de alta discrecionalidad (que incluyen las compras directas, los concursos por invitación y los concursos entre proveedores previamente registrados) restringen la competencia y duplican la probabilidad de cometer irregularidades respecto a las modalidades de baja discrecionalidad (subastas que no condicionan la participación de competidores).

Sin embargo, los procesos más abiertos y transparentes son tradicionalmente más costosos en términos de tiempo y atención para las organizaciones y los funcionarios encargados. Las legislaciones en materia de compras públicas reconocen esta disyuntiva, y tratan de encontrar un equilibrio entre la agilidad y el control de los procesos.

En este contexto, **las herramientas tecnológicas emergen como una innovación potencialmente transformadora, y se pueden incorporar con distintos grados de profundidad en los sistemas de compras públicas**. A un nivel superficial, es posible usar páginas web para anunciar los procesos de adquisición con antelación y difundir la información a interesados. También, emplear plataformas electrónicas para registrar las transacciones una vez que se han realizado, lo que podría facilitar su monitoreo interno (por órganos públicos) y externo (por ciudadanos, medios, etc.). Finalmente, en un estadio más avanzado de digitalización, varias administraciones públicas han empezado a usar plataformas transaccionales para sus procesos de adquisición, que sirven para gestionar la totalidad de los procesos (convocatorias, comunicaciones con los licitantes, decisiones, e incluso desembolsos), aunque también es común que se implementen soluciones más parciales.

La promesa de estas herramientas radica en que, comparadas con los métodos tradicionales, disminuyen el costo de realizar procesos abiertos y equitativos porque permiten una mayor difusión de información a los interesados y dificultan la colusión entre funcionarios y empresas específicas. Además, el registro sistemático de las acciones realizadas aumenta la probabilidad de detección de irregularidades. Si ese registro es bueno y suficientemente extendido, se abre la posibilidad adicional de usar esos datos para detectar patrones en las transacciones estatales y crear sistemas de alarma a partir de modelos de aprendizaje automático, como se expuso en la sección anterior.

La mejor evidencia sobre el impacto de la digitalización de las compras públicas viene de Lewis-Faupel, Neggers, Olken y Pande (2016), quienes estudiaron datos de la India e Indonesia, dos países con altos niveles de corrupción. Para Indonesia, la herramienta que se evaluó es un sistema semielectrónico de compras, que permite a las empresas hacer en línea tareas como la manifestación de interés, la descarga de información y pliegos téc-

La promesa de estas herramientas radica en que, comparadas con los métodos tradicionales, disminuyen el costo de realizar procesos abiertos y equitativos porque permiten una mayor difusión de información a los interesados y dificultan la colusión entre funcionarios y empresas específicas.

nicos, el envío de materiales de precalificación, y la formulación de preguntas y quejas, pero que excluye el envío final de la oferta, el cual debe llevarse a cabo por medios tradicionales. El sistema que se reemplazó era uno en que todas las fases de la licitación se adelantaban por vías tradicionales, y posteriormente a la resolución del proceso se publicaba en Internet la información del contrato y de cada oferta. En el caso de India, se evaluaron sistemas de compra electrónica introducidos por nueve estados (provincias) a partir de 2000, que sustituyeron los procesos manuales tradicionales.

Los contratos incluidos en el estudio fueron principalmente de obras de construcción, específicamente carreteras en el caso de India. Sin embargo, en Indonesia también se examinaron contratos de consultoría. Las obras, generalmente, se asignaban a la oferta más barata, condicionado esto por el cumplimiento de requisitos administrativos y técnicos, mientras que las consultorías se solían adjudicar usando fórmulas que combinaban el precio y un puntaje técnico entre los oferentes precalificados.

Los resultados arrojaron efectos en algunos indicadores, y no en otros. Algunas variables que no se vieron afectadas por los sistemas de compra electrónica fueron: el número de ofertas recibidas, los precios de los contratos ganadores, el costo final de las obras (incluyendo sobreprecios o adendas) y la duración de los proyectos hasta la finalización de las obras. Por otra parte, sí hubo efectos en algunas dimensiones importantes: aumentó la probabilidad de que la oferta ganadora fuera de una localidad distinta al lugar de la obra (especialmente pronunciado para los contratos de consultoría) y también la de que ganaran firmas preexistentes (de nuevo, especialmente para las consultorías).

Quizás el efecto más significativo haya sido que la calidad de las obras aumentó. Esto se pudo observar en el caso de India, dado que allí existe un esquema de monitoreo central que audita la calidad de un conjunto aleatorio de carreteras. El sistema electrónico de compras se asocia a un incremento de entre 10 y 20 puntos porcentuales en las notas de calidad de las obras ya completadas. Los autores hallaron que la razón detrás de las mejoras era que las compras electrónicas permitían seleccionar mejores prestadores.

Si bien Lewis-Faupel *et al.* (2016) no pudieron observar variables directamente asociadas con la reducción de la corrupción, las estimaciones sí mostraron que esas plataformas aumentaban la eficiencia en las contrataciones: el sistema tradicional (manual) llevaba a contratos de igual precio, pero de menor calidad. En tal sentido, puede **al menos afirmarse que la digitalización del sistema de contratación reduce los riesgos de corrupción existentes en los procesos tradicionales basados en papel, los cuales facilitan los espacios para la colusión entre funcionarios y proveedores**.

Para América Latina, el único estudio en esta materia se ha realizado sobre la plataforma **COMPR.AR** de Argentina (De Michele y Pierri, 2020). Algunos indi-

cadores descriptivos parecen señalar resultados positivos en cuanto a precios pagados y duración de los procesos. Lamentablemente, no es posible obtener estimaciones claras de impacto causal de la plataforma, por limitaciones de datos y detalles de la implementación del programa. Este es un tema en el que sería muy valioso producir evidencia para la región.

2.1.5. Transferencias sociales

Una forma de corrupción que genera preocupación en muchos contextos es la desviación de fondos públicos destinados a programas sociales. Es común que esos recursos atraviesen varias instancias burocráticas, donde aparecen riesgos de filtraciones. En respuesta a esto, un uso importante de las aplicaciones tecnológicas es aumentar la trazabilidad de los fondos en su camino a los beneficiarios legítimos. Con ese mismo objetivo, las soluciones específicas pueden tomar formas muy variadas. Los Gobiernos regionales de la India se han convertido en un lugar de ensayo y aprendizaje en esta materia; a continuación, compartimos tres experiencias relevantes, provenientes de ese país, cuyos efectos han sido documentados en estudios muy rigurosos.

El primer caso trata de la introducción de tarjetas de identificación biométrica para la autenticación de los desembolsos en el Esquema de Garantía de Empleo Rural (NREGS por sus siglas en inglés; un enorme programa social que garantiza 100 días de empleo pagado a cada hogar rural)[28] en la India. El proyecto, que tuvo lugar en el estado de Andhra Pradesh, generó dos reformas simultáneas. En primer lugar, cambió la tecnología con que las personas demuestran su identidad a la hora de recibir pagos, sustituyendo el uso de documentos de identidad tradicionales por tarjetas inteligentes que contienen información biométrica (las diez huellas digitales). Esas tarjetas se crearon en campañas de registro voluntario e iban vinculadas a nuevas cuentas bancarias. El segundo cambio consistió en sustituir la organización encargada de gestionar los pagos. Tradicionalmente, se encargaban de esto funcionarios públicos (del servicio postal o de agencias locales de desarrollo), pero la intervención los sustituyó con bancos contratados por el Gobierno regional para manejar la última milla de la gestión.

En el *statu quo* (antes de la reforma), el Gobierno estatal transfería electrónicamente los recursos, atravesando varios niveles subnacionales, hasta que el dinero en efectivo llegaba a las unidades más locales (generalmente, a través de oficinas postales). Allí, los beneficiarios retiraban el pago, directamente o por persona interpuesta, con documentos de identidad tradicionales. Bajo el

[28] Además de los desembolsos del NREGS, la misma reforma se aplicó a los pagos del sistema de pensiones de la seguridad social (SSP, por sus siglas en inglés). Aunque nos enfocamos en discutir el caso del NREGS, los efectos de la reforma fueron muy similares para el SSP.

Un uso importante de las aplicaciones tecnológicas es aumentar la trazabilidad de los fondos en su camino a los beneficiarios legítimos.

nuevo sistema, el Gobierno estatal transfiere fondos electrónicos a los bancos, y estos a empresas subcontratadas para la gestión de los desembolsos. Los beneficiarios retiran el pago usando la tarjeta de identificación biométrica.

Muralidharan, Niehaus y Sukhtankar (2016) analizaron los efectos de la reforma y encontraron resultados positivos en las tres dimensiones que evaluaron: logística de pagos, acceso de los beneficiarios y prevención de corrupción. En cuanto a logística, se observaron reducciones de hasta 20 % en el tiempo dedicado por las personas para recibir sus pagos. En lo relativo al acceso, hubo un aumento de 17 % en cantidad de hogares que trabajaron y cobraron bajo el programa de empleo NREGS. De manera muy significativa, se evidenció que la intervención disminuyó el desvío de fondos: mientras los beneficios recibidos por los hogares aumentaron en 24 %, el monto de los fondos transferidos por el Gobierno no cambió. Es decir, la intervención logró que un porcentaje mayor del dinero terminara efectivamente en las manos de los beneficiarios, en lugar de filtrarse en el camino. Los autores estiman que la reducción en fondos desviados fue ligeramente superior al 40 %.

Un ejercicio adicional de los autores intenta desentrañar qué aspectos de la intervención produjeron los cambios observados. Sus resultados sugieren que el cambio tecnológico (es decir, el uso de la tarjeta con información biométrica para autenticar la identidad) es responsable de las ganancias en acceso y de la reducción en la desviación de fondos; mientras que el cambio organizacional (el uso de bancos para hacer la gestión de los pagos) fue la causa de las mejoras en la logística y la velocidad de los pagos.

La segunda intervención ocurrida en India también tiene que ver con el programa NREGS, pero en otro estado, Bahir. En este caso, la reforma consistió en un mecanismo para que las transferencias del Gobierno estatal a los niveles subnacionales se realizaran «en tiempo real», en lugar de hacerse por adelantado. En el esquema tradicional, las unidades más locales de Gobierno (encargadas de los desembolsos a los beneficiarios finales) debían escalar solicitudes de transferencias adicionales cuando se quedaba sin fondos asociados al programa. Esas solicitudes solo iban acompañadas de un «certificado de utilización» de los fondos, sin información sobre quiénes eran los beneficiarios empleados o cuánto se les pagaba. Las solicitudes subían varios niveles de Gobierno hasta alcanzar el estatal, que hacía la transferencia. Los gobiernos locales, eventualmente, debían reportar la información sobre los beneficiarios y pagos específicos, pero esto típicamente ocurría meses después de la operación. Tras la reforma, las transferencias solo se llevaban a cabo después de que las unidades locales de Gobierno cargaban directamente la información sobre los beneficiarios y pagos realizados, lo que debían hacer de manera continua a través de una plataforma digital.

Este programa implementó tres cambios simultáneos. Por un lado, las transferencias pasaron de ser avances de dinero para cubrir desembolsos futuros, a

transferencias (casi) en tiempo real contra el trabajo realizado por los beneficiarios bajo el NREGS. Segundo, se eliminaron los intermediarios que canalizaban las solicitudes entre las unidades locales y el Gobierno regional. Tercero, se creó un costo para los agentes más locales de Gobierno, porque tenían que registrar de manera continua la información sobre los beneficiarios en el sistema (algo que, en el contexto rural del programa, podía ser significativo).

Banerjee, Duflo, Imbert, Matthew y Pande (2020) mostraron los resultados. En primer lugar, hallaron que la reforma redujo los gastos del NREGS en 24 %. Usando datos de una encuesta independiente a hogares, observaron que la intervención no afectó el número de beneficiarios, los pagos recibidos ni los proyectos construidos, lo que indica que **la reducción en los gastos fue producto de una menor filtración de recursos, y que no hubo caída en los beneficios de las personas**. El único aspecto negativo fue un aumento en las demoras para recibir los pagos por parte de los beneficiarios. Los autores también encontraron evidencia de que el programa redujo el número de «hogares fantasma» a los que se acreditaban pagos. Los autores atribuyen la reducción en la corrupción a la mayor facilidad para monitorear los desembolsos del programa, gracias al registro continuo de beneficiarios y transacciones.

La tercera experiencia es la vinculación del sistema de identificación biométrica con el Sistema de Distribución Pública (PDS, por sus siglas en inglés) en India, programa que permite a los beneficiarios comprar cantidades fijas de alimentos básicos a precios muy subsidiados en tiendas gubernamentales específicas. La iniciativa tuvo dos etapas: la primera fue la introducción de puntos de venta electrónicos en las tiendas, que permitían exigir a los beneficiarios usar su tarjeta biométrica cada vez que hacían una compra dentro del PDS. En la segunda (llamada «reconciliación»), el Gobierno comenzó a ajustar (hacia abajo) la cantidad de alimentos que distribuía a cada tienda, usando la información de las transacciones electrónicas para calcular el nivel de inventario que debía tener la tienda. Esta etapa debía reducir las filtraciones de recursos (en este caso, de alimentos).

Muralidharan *et al.* (2020) presentaron varios resultados interesantes sobre esta experiencia. En primer lugar, calcularon las filtraciones antes de la implementación del programa en 20 % del valor de los alimentos distribuidos. Adicionalmente, observaron una muy baja incidencia de beneficiarios ficticios (en contra de lo que se creía), por lo que las filtraciones ocurrían casi totalmente en el margen intensivo (reportando falsamente entregas de alimentos a beneficiarios reales). La introducción de los puntos de venta electrónicos (sin la reconciliación) cambió poco las cosas: no afectó el gasto del Gobierno en alimentos del PDS, ni las desviaciones de recursos. Aunque los beneficios recibidos por las personas no cambiaron en promedio, sí hubo algunos efectos distributivos relevantes. En particular, la probabilidad de que un beneficiario real no recibiera alimentos en absoluto en un mes dado aumentó 2,4 puntos porcentuales. Ese efecto estuvo concentrado en

Una lección importante es que las intervenciones para cambiar la manera en que se hace la entrega de programas sociales y transferencias a la población deberían incluir dispositivos para evaluar, en tiempo real, los efectos sobre el acceso y la experiencia de los beneficiarios.

los hogares donde al menos un miembro no pudo autenticar su identificación electrónica, y fue regresivo debido a que ese problema era más común en hogares más pobres. Otro efecto relevante de la primera etapa del programa fue un aumento en los costos de transacción de los beneficiarios, por dos razones: i) se incrementó el porcentaje de viajes infructuosos a las tiendas (posiblemente asociado a fallas en los puntos de venta electrónicos), y ii) aumentó el costo de oportunidad del tiempo destinado a comprar los alimentos porque la identificación electrónica requería la presencia del beneficiario, mientras que, en el esquema anterior, los hogares tenían flexibilidad para mandar a otros miembros a la tienda. Los autores calculan en 17 % el aumento en los costos de transacción de los beneficiarios.

La segunda etapa de la iniciativa (reconciliación) sí tuvo impactos sobre el gasto del Gobierno en el PDS y sobre las filtraciones. La reducción en el gasto en alimentos para el PDS estuvo entre el 20 % y el 35 %. La mayoría de esa reducción (de 66 % a 75 %) se debió, efectivamente, a una caída en los desvíos de alimentos, pero una parte no despreciable (entre un cuarto y un tercio) se originó en una disminución de los alimentos recibidos por beneficiarios reales. Varios factores de implementación pueden explicar la caída en los beneficios recibidos por los hogares. Por ejemplo, es posible que el Gobierno haya logrado ajustar las entregas de comida a las tiendas (de acuerdo con cálculos muy precisos sobre los inventarios), pero no evitar la desviación en los inventarios supuestamente acumulados, creando escasez de productos en estas.

En general, los efectos de la iniciativa aparecen mezclados, y vale la pena sintetizarlos separando las dos etapas del programa: i) el uso de la identificación biométrica, por sí solo, no generó beneficios y, en cambio, dio lugar a la exclusión de un número modesto pero relevante de beneficiarios, además de un aumento en los costos de transacción para los hogares, y ii) el protocolo de reconciliación logró una caída significativa en el desvío de recursos, aunque también provocó una disminución en los beneficios recibidos por beneficiarios legítimos.

Las experiencias analizadas muestran que la tecnología puede tener efectos importantes en la gestión de programas y transferencias sociales, que dependerán de las decisiones políticas sobre qué se debe enfatizar y en los detalles de la implementación. El objetivo de las intervenciones era reducir los recursos perdidos por corrupción en los distintos programas, y se alcanzó, pero con diferencias importantes en cuanto a los efectos colaterales. Por ejemplo, la introducción de tarjetas biométricas para el cobro del NREGS se hizo subrayando el acceso de los beneficiarios como prioridad, y se obtuvieron mejoras también en esa dimensión, si bien no hubo efectos globales en la carga fiscal del programa. En cambio, la intervención en el PDS logró bajar el costo del programa, pero descuidó los aspectos del acceso y acabó disminuyendo la cobertura del programa entre beneficiarios legítimos. Una lección importante es que las intervenciones para cambiar la manera en

que se hace la entrega de programas sociales y transferencias a la población deberían incluir dispositivos para evaluar, en tiempo real, los efectos sobre el acceso y la experiencia de los beneficiarios. **En esto, distintas tecnologías también pueden ser útiles**, de acuerdo con la penetración que tengan entre la población. Un ejemplo, documentado en la literatura, es el uso de llamadas telefónicas a muestras representativas de beneficiarios para asegurar que reciben las ayudas de manera adecuada (Muralidharan, Niehaus, Sukhtankar y Weaver, 2021).

2.1.6. Gestión aduanera

Una forma relativamente básica, y potencialmente poderosa, de digitalización del Estado es la computarización de trámites aduaneros. El Programa Siglo XXI, llevado adelante en Colombia a través de la Dirección de Impuestos y Aduanas Nacionales (DIAN), es un ejemplo de este tipo de iniciativas. El programa se implementó secuencialmente en las diferentes aduanas del país entre 2000 y 2005, y su eje central fue la digitalización de trámites para permitir a los usuarios hacer las declaraciones de sus importaciones de manera electrónica.

A partir de su diseño, incluyó varios elementos que apuntaban a reducir las oportunidades de corrupción, y que iban más allá de la sola digitalización de las declaraciones. Se redujo la discreción de los agentes para determinar cuándo hacer una inspección de la carga o los documentos de un usuario, transfiriendo esa decisión al propio sistema, según los criterios objetivos basados en el perfil de riesgo del caso y en inconsistencias en las declaraciones. Además, se aumentó la trazabilidad y la transparencia de las decisiones tomadas por cada agente aduanero en el proceso, para reducir el riesgo de que los inspectores dieran su conformidad a declaraciones fraudulentas. Esto también permitiría evitar los subreportes de cantidades y valores de mercancías que pasaban por aduanas. Además de reducir la corrupción, se esperaba que el programa aumentara la eficiencia con que se gestionaban estos trámites, reduciendo los tiempos, los errores en los procesos y la incertidumbre de los usuarios.

Laajaj, Eslava y Kinda (2020) evaluaron los efectos del programa en varias dimensiones, con resultados generalmente positivos. En primer lugar, los autores hallaron una reducción sustancial en la corrupción. La reforma redujo la incertidumbre respecto a la duración de las transacciones aduaneras, lo que se asocia a una menor discreción de los agentes para acelerar o retrasar procesos, y también cayó el número de casos judiciales de la Procuraduría General de la Nación por corrupción en las aduanas. Asimismo, la gestión mejoró más allá de la reducción en prácticas corruptas: por ejemplo, hubo

una disminución en las discrepancias entre los impuestos adeudados y los pagados. Los autores señalaron que estas diferencias ocurren porque las empresas explotan deficiencias de comunicación entre bancos y aduanas para pagar menos de lo que les corresponde. Igualmente, la digitalización perfeccionó esa comunicación y la capacidad para verificar los pagos antes de liberar las mercancías. En cuanto a la agilidad de los trámites, el número de días necesarios para procesar el ingreso de las mercancías se redujo en 8 %, y la recaudación por esta vía aumentó tras la reforma. De manera significativa, todo esto redundó en una mejora de la productividad de las empresas importadoras, que elevaron en 7 % su valor agregado y en 6 % su empleo.

Los efectos positivos del programa se debieron a que la intervención tecnológica estuvo bien integrada, con un cambio en los procesos y el uso de la información para la toma de decisiones en el manejo de los trámites. Esto fue lo que permitió reducir el uso indebido de la discrecionalidad de los agentes, y redirigir esfuerzos para agilizar los procesos y hacer frente al contrabando y otras formas de fraude.

Deben resaltarse dos conclusiones importantes de este estudio. Primero, los efectos positivos del programa se debieron a que la intervención tecnológica estuvo bien integrada, con un cambio en los procesos y el uso de la información para la toma de decisiones en el manejo de los trámites. Esto fue lo que permitió reducir el uso indebido de la discrecionalidad de los agentes, y redirigir esfuerzos para agilizar los procesos y hacer frente al contrabando y otras formas de fraude. Segundo, los autores calculan que los beneficios generados en términos de recaudación y crecimiento fueron varias veces mayores que los costos de la computarización (estimados en USD 9 millones). Esto sugiere que la inversión generó retornos importantes.

Actualmente, empiezan a aparecer tecnologías más modernas, con posibles aplicaciones en este campo. En particular, la inteligencia artificial es una herramienta que —como en la gestión de compras públicas— tiene el potencial de contribuir a optimizar recursos en la lucha contra el fraude y la corrupción en materia aduanera. En Brasil, por ejemplo, el proyecto HARPIA surge de la colaboración entre universidades y la Secretaría de Ingresos Federales, con el objetivo de detectar diversas formas de fraude aduanero a través de la inteligencia artificial (Digiampetri, Trevisan, Meira, Jambiero, Ferreira y Kondo, 2008)[29]. En particular, HARPIA utiliza modelos de datos atípicos (*outliers*) para identificar operaciones aduaneras sospechosas. Del mismo modo, incluye un sistema de información de productos y exportadores foráneos, que busca ayudar a los importadores en el registro y clasificación de sus productos y proveedores. Por su parte, también con datos brasileños, Paula, Ladeira, Carvalho y Marzagao (2017) (2017) entrenan modelos de aprendizaje profundo (*deep learning*) no supervisado para detectar exportadores con alto riesgo de cometer fraude y lavado de dinero. Preliminarmente, el modelo muestra un poder predictivo potencialmente alto.

Por ahora, no existe evidencia causal sobre los efectos del uso de estas herramientas basadas en la inteligencia artificial. Es de esperar que, como ilustra el estudio analizado sobre la computarización de trámites en Colombia, estas técnicas podrán ser efectivas solo en la medida en que se integren bien con los procesos de gestión y toma de decisiones de los órganos competen-

[29] HARPIA proviene de las siglas para Análisis de Riesgo e Inteligencia Artificial Aplicada en portugués.

tes. Un posible beneficio es que ayuden a perfeccionar los cálculos de riesgo de las operaciones aduaneras y a detectar mejor los casos de riesgo, redundando así en un uso más eficiente de los recursos de fiscalización.

La revisión de la literatura muestra que la evidencia estadística sobre los efectos de la digitalización del Estado sobre la corrupción es aún escasa. Hay varias razones para esto, desde la relativa novedad de algunas de las soluciones digitales en consideración hasta la dificultad inherente a estudiar la corrupción empíricamente. Una consecuencia es que resulta muy valioso que las intervenciones digitales desplegadas por los Estados se acompañen de estudios rigurosos que permitan documentar sus resultados y evaluar su impacto.

Alternativamente, es posible explorar de modo más cualitativo cómo algunas iniciativas de gobierno digital han generado resultados en materia de integridad, a partir del análisis de experiencias específicas de los países, sus condiciones de funcionamiento y sus objetivos de política pública. Esto se abordará en la siguiente sección, que examina algunos casos en América Latina.

2.2. Análisis cualitativo: experiencias de transformación digital para la prevención de corrupción en América Latina

La aceleración digital que viene experimentando el mundo en las dos últimas décadas, en especial tras la crisis sanitaria COVID-19, está cambiando el modo en que los Gobiernos suministran servicios, no solo por la necesaria reducción de canales presenciales para interactuar, sino por la rapidez y eficiencia que las tecnologías permiten en los procesos de gestión pública. Por otra parte, tanto ciudadanos como empresas —cada vez más conectados e informados— tienen expectativas crecientes sobre la calidad y la conveniencia de los servicios públicos, y exigen una toma de decisiones más inclusiva y transparente.

Como se ha visto anteriormente, las tecnologías digitales pueden mejorar la divulgación de información, su acceso cuando proviene del sector público y una mayor participación ciudadana (ver capítulo 1 y sección 2.1). Al implementar un uso más estratégico de los datos y la información del sector público, las tecnologías digitales pueden beneficiar la formulación de políticas y el diseño de servicios, y mejorar la participación, la rendición de cuentas y la transparencia en todos los niveles del Gobierno.

Los Gobiernos han puesto cada vez más servicios en línea. Sin embargo, a menudo, esto no ha cambiado significativamente las estructuras y los procesos de back office (OCDE, 2016). Las nuevas tecnologías digitales (por ejemplo, plataformas de redes sociales y teléfonos móviles e inteligentes) y los actuales enfoques para el uso de la tecnología (entre otros, datos gubernamentales abiertos y *big data*) ofrecen formas más colaborativas de trabajar dentro y entre las administraciones, así como mejores mecanismos de interacción con el público. Esto puede ayudar a los Gobiernos a ser no solo más eficientes y eficaces, sino también más abiertos, transparentes y responsables ante sus electores.

Esta nueva etapa de madurez de las tecnologías digitales y su creciente uso por parte de los Gobiernos está marcando un cambio de paradigma del gobierno electrónico al digital. De acuerdo con la Recomendación de la OCDE del Consejo sobre Estrategias de Gobierno Digital de 2014, este se

define como:

> el uso de tecnologías digitales, como parte integral de las estrategias de modernización de los gobiernos, para crear valor público. Se basa en un ecosistema de gobierno digital compuesto por actores gubernamentales, organizaciones no gubernamentales, empresas, asociaciones de ciudadanos e individuos que apoya la producción y el acceso a datos, servicios y contenido a través de interacciones con el gobierno (OCDE, 2014a).

El principal resultado de este cambio es que el gobierno digital ya no se trata solo de poner los servicios en línea y lograr la eficiencia operativa. Los Gobiernos comienzan a adoptar una concepción completamente nueva de las TIC como mecanismo para fortalecer la gobernanza pública, haciéndolos más abiertos, efectivos y eficientes; al tiempo, integran las preferencias de los ciudadanos en el diseño y la prestación de servicios públicos. El gobierno digital consiste en nuevas formas de ofrecer valor público y hacer que los servicios y procedimientos gubernamentales sean digitales por diseño.

En la última década, los países de América Latina han avanzado en la implementación de estrategias de transformación digital, y lo han hecho a distintas velocidades. La mayor parte de los países de la región cuentan con agendas digitales y políticas de transformación digital del sector público, que generaron transformaciones tecnológicas importantes y adaptaron sus instrumentos legales para abrirles paso a la gobernanza digital y a un Gobierno cada vez más abierto[30]. **El interés de los Gobiernos de América Latina para avanzar en la digitalización se materializa en diferentes instrumentos que planifican e incluso decretan metas en materia de gobierno digital**, como sigue:

- México publicó recientemente su **Estrategia Digital Nacional 2021-2024**, basada en dos ejes principales: (i) la transformación de la Administración Pública Federal mediante el uso de las TIC para mejorar y transparentar los servicios gubernamentales que se otorgan a la ciudadanía, y (ii) el aumento de la cobertura de internet a todo el país para combatir las brechas digitales existentes en el país.

- Colombia, por su parte, definió la **política de Gobierno Digital** mediante el **Decreto 1008 de 2018**, buscando que las entidades públicas sean más eficientes para atender las necesidades y problemáticas de los ciudadanos, y que estos sean los protagonistas en los procesos de cambio a través del uso y apropiación de las tecnologías digitales.

[30] OCDE. Gobierno Abierto. Contexto mundial y el camino a seguir (2016). La OCDE define el gobierno abierto como «una cultura de gobernanza basada en políticas públicas y prácticas innovadoras y sostenibles, que se basan a su vez en unos principios de transparencia, rendición de cuentas y participación que promueven la democracia y el crecimiento inclusivo». https://www.oecd.org/gov/Open-Government-Highlights-ESP.pdf

- Perú ejecuta su **Agenda Digital**, respaldada por el **Decreto Legislativo 1412** de 2018, cuyo objetivo es alcanzar una transformación digital que le permita constituirse en un país transparente, competitivo e innovador, y que pueda hacer viable la mejora social. Sus principales estrategias están relacionadas con inclusión digital, accesibilidad y participación ciudadana activa.

- Chile trabaja por una **Transformación Digital del Estado**, con tres pilares fundamentales: (i) un Estado Moderno; (ii) un Estado Innovador, y (iii) un Estado Sustentable y Eficiente. Para este fin, fue promulgada la **Ley de Transformación Digital del Estado**, en noviembre de 2019, y se definieron otros documentos que constituyen la hoja de ruta para la modernización del Estado.

- Argentina promulgó la **Agenda Digital 2030** mediante el **Decreto 996 de 2018**, con el objetivo de coordinar las iniciativas gubernamentales para el aprovechamiento de las tecnologías digitales, a fin de desarrollar un Gobierno eficiente y eficaz, orientado al ciudadano, con valores de apertura y transparencia.

- Brasil presentó la **Estrategia de Gobierno Digital 2020-2022**, mediante el **Decreto 10.332 de 2020**, que involucra al país entero. Con este plan, pretende orientarse hacia un Gobierno totalmente digital, en el que los datos y la tecnología respalden políticas y servicios públicos de mejor calidad. También, alienta a los estados y municipios a expandir la oferta de servicios digitales y acabar definitivamente con el uso del papel.

De la mano de la **implementación de las tecnologías digitales**, hay una intención clara en América Latina para aplicar las tendencias del gobierno digital en sistemas y procesos administrativos internos, como las compras públicas electrónicas, los portales de datos abiertos y los trámites digitales. Algunos de estos espacios de digitalización tienen un potencial en materia de integridad pública.

La digitalización de los servicios de Gobierno contribuye a la reducción de riesgos de corrupción a través de, por lo menos, tres mecanismos:

- Primero, las tecnologías digitales limitan la discrecionalidad de los servidores públicos mediante la automatización y uso de herramientas digitales que hacen más eficiente la prestación de asistencias y servicios públicos, reduciendo el contacto entre agentes del Gobierno y los usuarios.

- Segundo, la digitalización del Gobierno contribuye a aumentar la transparencia y el control. Al garantizar el acceso a la información, aún más si es en formato de datos abiertos, se aumenta la transparencia y la rendición de cuentas, facilitando así el control sobre las actuaciones administrativas

por parte de los órganos de auditoría y los ciudadanos. En otras palabras, el crecimiento exponencial de los datos disponibles para consulta, intercambio y análisis actúa como propulsor de integridad en la gestión pública.

- Tercero, la digitalización ofrece nuevas herramientas para el control social y el empoderamiento ciudadano. Se faculta a los ciudadanos para reclamar un buen desempeño de los Gobiernos y para hacer parte de las propuestas para la solución de problemas públicos. Por ejemplo, a través de plataformas y aplicaciones móviles interactivas, es posible medir la experiencia de los usuarios de los programas públicos. De esta forma, es posible garantizar una mejora en la calidad de la prestación de los servicios e implementar políticas públicas basadas en las necesidades de los usuarios finales.

Las políticas en América Latina en materia de gobierno digital son bien amplias si se examinan las regulaciones y hojas de ruta adoptadas por los países. Pero es posible destacar al menos tres ámbitos de gobierno digital que han generado dividendos en materia de integridad: trámites ciudadanos, compras públicas y fomento del control social.

2.2.1. Digitalización de los trámites para la integridad pública

Relevancia

Si se tiene en cuenta que **uno de cada cinco ciudadanos latinoamericanos pagaron un soborno para acceder a un servicio** (Transparencia Internacional, 2019), **es claro que los trámites abren un mercado considerable para el abuso** de los funcionarios públicos sobre millones de usuarios. El trabajo seminal de Roseth *et al.* (2018) define el **trámite como un conjunto de requisitos, pasos o acciones a través de los cuales los usuarios piden o entregan información a una entidad pública, sea para obtener un derecho o para cumplir con una obligación**. El rango de los derechos y obligaciones que dan lugar a los trámites es bien amplio: desde lo más básico y común, como conseguir una identidad, hasta lo más idiosincrático, como una interdicción judicial. En cada país de América Latina se registran entre 1 000 y 5 000 trámites dentro del portafolio de servicios de los Gobiernos; cada ciudadano, en promedio, hace unos cinco trámites al año, y el 89 % —al menos antes de la pandemia— se hacen de manera presencial (Roseth *et al.*, 2018).

Con la profundización en el uso de las tecnologías digitales, se cierran espacios de corrupción y abuso en los trámites ciudadanos, puesto que digitalizarlos los vuelve impersonales y uniformes para todos los usuarios, gracias a algoritmos programados. Dicha programación cierra ventanas de discrecionalidad en los funcionarios que procesan solicitudes ciudadanas y los hace más responsables ante otras autoridades, puesto que sus actuaciones son fácilmente rastreables gracias a los datos que se producen a lo largo de los procedimientos administrativos y que quedan para consulta (OCDE, 2003).

Casos de uso

La simplificación y digitalización de los trámites relacionados con los sistemas de identificación son elementos esenciales para el desarrollo de los países y para la lucha contra la corrupción (Banco Mundial, 2019). Los trámites presenciales para la obtención de identificaciones son lentos y vulnerables a la corrupción, y terminan excluyendo a la gente con menos recursos (Roseth *et al.*, **2018**). En un caso emblemático documentado por el BID (Roseth *et al.*, **2018, p. 18),** una ciudadana de la tercera edad de Bolivia tardó 11 meses en renovar su identificación, tuvo que someterse a varios desplazamientos y terminó accediendo a pagar el soborno que le solicitó un policía a cambio de agilizar las gestiones.

Simplificar y digitalizar el trámite para obtener una identidad implica democratizar el acceso a otros derechos y crear sistemas más igualitarios.

El Banco Mundial (2021) estimó que, en América Latina, en 2018, aproximadamente 34 millones de personas (5 % de la población de la región) no contaban con identificación básica. En su mayoría, estas hacen parte de los grupos más pobres y vulnerables. En consecuencia, la institución propuso la iniciativa de identificación para el desarrollo (ID4D, por sus siglas en inglés) y una guía orientada a crear sistemas de información (SDI) inclusivos y seguros. Simplificar y digitalizar el trámite para obtener una identidad implica democratizar el acceso a otros derechos y crear sistemas más igualitarios. Esta iniciativa ha inspirado la digitalización y simplificación del trámite para obtener una identificación en algunos Gobiernos de América Latina.

La implementación de servicios digitales fácilmente accesibles mediante procedimientos de identificación y autenticación digital tiene la potencialidad de reducir los riesgos de corrupción al limitar las interacciones humanas, y reducir los tiempos de procesamiento y los espacios para la adopción de decisiones discrecionales de los oficiales públicos (Roseth *et al.*, 2018). Algunos ejemplos de experiencias de la región en la materia se abordan a continuación.

Por ejemplo, **Perú** adelanta un proceso de modernización digital en el servicio público y simplificación de procedimientos, a través de la implementación del documento de identificación electrónico (DNIe) o la solicitud vía trámite digital del DNI o del pasaporte. Sin embargo, el gran desafío en el país es incentivar el uso de documentos electrónicos, como el DNI, o de usar trámites digita-

les; puesto que los documentos nacionales de identidad son necesarios para todos los ciudadanos, es importante que tengan acceso a internet o infraestructura digital, lo cual **es un reto para el caso peruano, donde solo un 40 %** de los hogares pueden conectarse a internet.

El estado de **Nuevo León**, en México, introdujo la autenticación digital y dio paso a los servicios digitales. En mayo de 2020, presentó la plataforma **Acceso N.L.**, en la cual es posible adelantar los trámites para acceder a una identidad y otros, como el pago de impuestos. El portal es muy nuevo y aún no existen análisis o evaluaciones disponibles sobre su funcionamiento, capacidad de procesamiento y acogida entre la ciudadanía. Sin embargo, vale la pena tener esta experiencia presente porque se trata de un gobierno subnacional, con un desempeño destacado en materia de infraestructura digital y gobierno abierto en México (PDE, 2021).

Otro gobierno subnacional que documenta una experiencia positiva en materia de simplificación de trámites y digitalización es la municipalidad de **Córdoba**, en Argentina, que dispuso un canal de trámites digitales a través de su plataforma Ciudadano Digital. No solo se digitaliza el trámite para la obtención de la identidad, sino que el número de ciudadanos que ya tienen identidad digital llegó a los 727 608, de una población total de 1,4 millones (López-Azumendi, Facchina y Zapata, 2021). Córdoba expandió la digitalización a otros trámites como: (i) registros catastrales para cambios en la titularidad de un inmueble y reclamos sobre la valuación de inmuebles; (ii) permisos de uso de suelo y ejecución de obras privadas, y (iii) solicitudes de habilitación de negocios. El proceso de simplificación y digitalización en las reparticiones de la municipalidad, que costó alrededor de USD 1,5 millones —a precios corrientes—, generó ahorros de eficiencias por unos USD 3,7 millones (López Azumendi *et al.*, 2021).

La agilización y digitalización de trámites no solo representa mayor bienestar para los ciudadanos, sino que el Gobierno se beneficia de dicha simplificación por medio de ahorros en tiempo y dinero. Brasil es un ejemplo de optimización de recursos públicos a través de un proceso de digitalización de servicios y trámites en el sitio del Gobierno federal, **Gov.br.** Durante la pandemia, alcanzó la cifra de **3 000 servicios digitalizados** (aproximadamente 70 % de los 4 300 servicios que ofrece) y espera digitalizar y rediseñar el 100 % de los trámites, hasta 2022. Esta modernización permite a la ciudadanía realizar y monitorear el avance de las solicitudes realizadas, brindando flexibilidad y seguridad a los usuarios. Entre los servicios, se encuentran la Asistencia de Emergencia y la **Prueba de Vida Digital del Instituto Nacional de Seguridad Social** (INSS). Con estas iniciativas, el Gobierno afirma que ahorra, aproximadamente, **USD 350 millones** al año, de los cuales, unas tres cuartas partes representan ahorros para los usuarios.

En esta misma línea ha actuado la **Agencia Digital de Innovación Pública** (ADIP) de la **Ciudad de México (CDMX)**, que avanza en el diseño de un sistema de ventanilla digital única para atender a la ciudadanía y disminuir los costos de interacción y aquellos asociados con microcorrupción. Según **Claudia Sheinbaum**, jefa del Gobierno de Ciudad de México desde 2018, la digitalización de las funciones gubernamentales encuentra su razón en la erradicación de la corrupción, la mejora de la relación Gobierno-ciudadanía y el desarrollo económico sostenible e inclusivo.

A pesar de las ventajas en la digitalización de los trámites, esta modalidad tiene un uso muy bajo en la región[31]. De acuerdo con el estudio de Roseth *et al.* (2018) y CAF (2021), pocos trámites se pueden completar en línea en la región, aunque, con la pandemia, la proporción de uso de internet entre los ciudadanos superó el 30 % en América Latina para, al menos, acceder a servicios públicos (Roseth, Reyes y Yee Amézaga, 2021). Las bajas tasas de uso digital obedecen a varias razones, que van desde la carencia de precondiciones básicas para digitalizar, las brechas de infraestructura digital en los países con grandes disparidades regionales, y las preferencias ciudadanas que, o encuentran difícil navegar por las plataformas digitales de Gobiernos o, simplemente, tienen más confianza en los canales presenciales.

Desafíos pendientes

Si bien las iniciativas acá señaladas no tienen como objetivo principal y explícito abordar los desafíos de la corrupción, se esperan muchos beneficios de integridad pública asociados con el gobierno electrónico (Santiso 2021; Banco Mundial **2016**; Dupuy y Serrat **2014**; Zinnbauer **2012**), como los siguientes:

- Los trámites digitalizados, cuando van de la mano de un adecuado acceso a la información para los ciudadanos, permite a estos últimos ejercer con mayor facilidad sus derechos y acceder a servicios de Gobiernos sin que la corrupción interfiera.

- Al limitar la discreción de los burócratas y automatizar procesos específicos para reducir las interacciones entre los funcionarios y los ciudadanos, se reducen oportunidades de obtener sobornos. Sin embargo, la simplificación debe acompañar estos procesos de digitalización, pues, si el trámite sigue siendo engorroso, se puede, por ejemplo, abrir una oportunidad para intermediarios que a menudo crean un mercado para el soborno.

- Los trámites digitalizados también aumentan la transparencia de las transacciones con los funcionarios públicos, ya que los hacen auditables, lo

[31] Según cifras de Roseth et al. (2018), el uso de canales digitales no superaba el 18 % para varios tipos de trámites en el continente.

cual disuade los comportamientos como solicitudes indebidas o demoras injustificadas.

- En algunos casos, las administraciones pueden recibir comentarios y evaluaciones por parte de los usuarios del servicio para realizar un seguimiento regular de la satisfacción e identificar problemas relacionados con corrupción, por ejemplo.

El potencial que está desplegando la digitalización de los trámites no se aplica con la misma celeridad en el ecosistema de integridad y en los procedimientos propios de las autoridades públicas encargadas de prevenir, investigar y sancionar la corrupción. Identificamos, por lo menos, dos oportunidades de mejora:

- Los canales de denuncia de hechos de corrupción: América Latina tiene un récord pobre para organizar, simplificar y procesar de modo expedito y efectivo las denuncias por hechos de corrupción (CAF, 2019). A nivel mundial, las plataformas digitales de denuncia que permitan hacer un seguimiento a todo el proceso de investigación y sanción en cada uno de los hechos reportados son prácticamente inexistentes, puesto que, en realidad, apenas sirven de repositorios para hacer públicos los hechos denunciados, pero no para agilizar la restitución de los derechos vulnerados a los ciudadanos (U4, **2016**). La denuncia no ha tenido el mismo tratamiento que los demás trámites citados a lo largo de esta sección, lo cual puede deberse a que su procesamiento implica la concurrencia de varias autoridades de las diferentes ramas del poder público.

- Los procedimientos para investigar y sancionar hechos de corrupción: en América Latina, concurren tanto autoridades judiciales como administrativas en la investigación, detección y sanción de los casos de corrupción. En países como Argentina, Brasil, Colombia, Chile y Perú, aparte de la rama judicial, los hechos de corrupción pueden ser conocidos por organismos de control o por el Ministerio Público. Sin embargo, los arreglos institucionales implican que cada autoridad lleve sus procesos por sí misma, creando silos en sus actuaciones, e incluso sistemas de información diferentes que dificultan la coordinación y son susceptibles de duplicar esfuerzos en las investigaciones. Esto, sumado a la complejidad en las regulaciones para procesar penal, disciplinaria o administrativamente los casos de corrupción, limita considerablemente el espacio que puede ofrecer la digitalización en estos procesos de Gobierno. La digitalización de los sistemas de información donde reposan las sanciones por corrupción, la implementación de expedientes digitales, el establecimiento o mejoramiento de las páginas de consultas de procedimientos y procesos relativos a la investigación y sanción de actos de corrupción, entre otros, podrían facilitar esfuerzos conjuntos de los órganos administrativos y judi-

ciales. Adicionalmente, harían más eficientes los trámites que persiguen la sanción de conductas corruptas.

Para cumplir con estas expectativas, los Gobiernos deben simplificar, agilizar y hacer más accesibles los procesos y servicios relacionados con investigación, detección y sanción de la corrupción. Las transformaciones digitales y las estrategias de simplificación administrativa podrían aplicarse a los procedimientos propios del ecosistema de investigación y sanción de la corrupción. Dichas simplificación y coordinación son necesarias para que las soluciones tecnológicas funcionen y para mejorar la eficiencia y efectividad de las autoridades judiciales o administrativas, ampliando así su capacidad de disuasión.

2.2.2. Digitalización en la compra pública

Relevancia

Parte importante del gasto público se asigna a la compra de bienes y servicios, y a la ejecución de obras públicas, para la operación y funcionamiento de las instituciones públicas. Todo esto requiere que los Estados organicen un sistema de compra y contratación, lo cual comprende decisiones sobre gastos e inversiones. Esto implica definir los procesos y procedimientos para el abastecimiento del Estado, la elección del método de selección del proveedor o contratista, la definición y los criterios de tal elección, y la forma de gestionar el contrato, incluyendo, entre otros, pagos y administración de riesgos (OEA, 2020). A través de la contratación y compra públicas, se invierte aproximadamente el 30 % anual del presupuesto nacional de los países de América Latina y el Caribe.

A finales del siglo XX, se desarrollaron los sistemas de *e-procurement*[32], es decir, compra o abastecimiento en línea. El *e-procurement* es el uso combinado de información y tecnología de las comunicaciones por medios electrónicos, para gestionar compras y suministros. Este concepto hace referencia a la integración de tecnologías digitales en el reemplazo o rediseño de procesos (que se administran ya no en papel sino en archivos electrónicos) para el abastecimiento de bienes, obras y servicios (OCDE, 2015).

[32] Los mecanismos de compra pública sufrieron una transformación importante a finales del siglo XX, inspirada en el sector privado. En la década de 1980, las firmas empezaron a utilizar herramientas digitales que transmitían mensajes estandarizados de computador a computador, para mejorar la eficiencia en los procesos de abastecimiento al emitir direcciones de envío, identificación y cantidad de productos, mejorando tiempos y minimizando errores frente al envío por correo y las llamadas telefónicas. En los años 90, el desarrollo de las TIC permitió que los sistemas de ERP (siglas en inglés de enterprise resource planning) facilitaran los flujos de los procesos de compra, los catálogos y las órdenes de compra.

El objetivo principal de los Gobiernos al adoptar el *e-procurement* estaba asociado a gestionar el conocimiento del sistema de compra para apoyar las decisiones de los compradores públicos.

Es a principios del siglo XXI que el uso del *e-procurement* se extiende a la compra y contratación públicas para facilitar la administración de grandes volúmenes de actividades de gasto reguladas por las complejas leyes de la compra pública. Estas reformas buscaron la automatización de los procesos de abastecimiento para racionalizarlos y agilizarlos, así como para reducir sus costos y el tiempo que requieren. También, se buscaba incrementar la competencia y concurrencia de proveedores. El *e-procurement* se inscribía así como parte de la expansión de los servicios de *e-government*.

El objetivo principal de los Gobiernos al adoptar el *e-procurement* estaba asociado a gestionar el conocimiento del sistema de compra para apoyar las decisiones de los compradores públicos. Al manejar la información a partir de archivos electrónicos y usar los medios digitales para el abastecimiento, era posible reutilizar los datos para entender mejor la demanda de bienes, obras y servicios de las entidades estatales; conocer mejor el mercado y las opciones para satisfacer las necesidades públicas; diseñar mejor la estrategia de compra, y organizar la ejecución del contrato para garantizar su eficacia (Cetina, Fonseca y Zuleta, 2021).

La implementación del *e-procurement* ayuda a la integridad de los procesos de compra pública a través de los siguientes mecanismos (OCDE, 2015):

- Libre acceso a la información relativa a la contratación pública, a través de un portal en internet, para todas las partes interesadas (proveedores nacionales y extranjeros, sociedad civil, organismos de control), como:
  - los marcos institucionales, leyes y regulaciones relevantes;
  - los procesos concretos de contratación pública para convocatoria (por ejemplo, información sobre la previsión de contratos públicos, términos de referencia para el mercado, las convocatorias o los anuncios de adjudicaciones), y
  - el funcionamiento del sistema de contratación pública (por ejemplo, comparativos de precios o de condiciones de abastecimiento, resultados de seguimiento y otros aspectos que muestren al público los resultados del sistema).

- **Mayor transparencia en la asignación de los recursos públicos**, desde el principio del proceso presupuestal y a lo largo de todo el ciclo de la contratación pública. Esto permite que sociedad civil, sector privado y otras partes interesadas conozcan las prioridades de las autoridades y el gasto que ellas realizan.

- **Cuando los portales de compra pública son transaccionales, se cierran aún más las ventanas de corrupción.** Por ejemplo, al permitir que los proponentes pujen en línea para obtener un contrato, se reduce la posibilidad de colusión. Al adjudicar los contratos en línea y evaluar a los proponentes, también disminuyen las oportunidades de que haya acuerdos indebidos para adjudicar contratos a cambio de sobornos.

- La permanente exposición de los datos y la información sobre proveedores y contratos suscritos facilita la actuación de las autoridades o de los ciudadanos para ejercer control posterior sobre las actuaciones de los funcionarios públicos.

Casos de uso

En **Colombia**, solo entre 2018 y 2021, el Estado generó ahorros del orden de COP 946 280 millones en la Tienda Virtual del Estado Colombiano (TVEC), según **declaraciones** de la Agencia Nacional de Contratación Pública Colombia Compra Eficiente (CCE). Sin embargo, a pesar del esfuerzo de digitalización de las compras públicas y la puesta a disposición de la información contractual en formatos abiertos, aún es insuficiente el avance en términos de prevención de corrupción. Los casos más importantes de detección de conductas anticompetitivas y de corrupción provienen de denuncias hechas con

posterioridad a la adjudicación de contratos[33]. También se han documentado fenómenos de «contratistas multipropósito» (Enciso y Romero, 2020), que aprovecharon la emergencia sanitaria del COVID-19 para cambiar o ampliar los objetos sociales de los proveedores del Estado con el fin de obtener contratos de modo directo.

La crisis del coronavirus expuso riesgos y escándalos de corrupción en las compras de emergencia. No obstante, varios países, entre los que se destacan **Colombia**, **Chile**, Paraguay y **Perú**, y la **Ciudad de México**, se han propuesto liberar información relativa a la contratación por emergencia, en plataformas de datos abiertos, lo que facilita el control fiscal y la participación ciudadana. Así mismo, algunos de estos países han implementado *dashboards* en los que es posible ver información sobre compras por emergencia en tiempo real, por ejemplo, en **Brasil** y **Chile**.

En 2020, todos los países, de la región y del mundo, orientaban la mayoría de sus recursos hacia la compra pública de suministros hospitalarios y medicamentos para hacer frente a la crisis sanitaria. Varios Estados de la región sobresalen por la publicación de datos en formatos abiertos y la consecuente transparencia de sus contrataciones. **Chile**, por su parte, tiene a disposición pública la **plataforma de datos abiertos de ChileCompra**, en donde publica la información de las compras públicas adelantadas en el portal transaccional **MercadoPublico**. Con esta iniciativa, **el Gobierno chileno garantiza la interoperabilidad de sus datos entre varias entidades[34], fomentando el desarrollo de nuevas aplicaciones e informes basados en datos y facilitando su análisis, monitoreo y fiscalización**. Durante 2020, Chile logró ahorros que ascienden a los **USD 21 millones**, comparado con el presupuesto inicial, en la adquisición de mascarillas, guantes y alcohol gel necesarios para hacer frente a la crisis sanitaria, apenas uno de los diversos sectores que generaron ahorros ese año.

Ciudad de México ha trabajado en la transformación digital en varios ejes, encaminados a la promoción de integridad, haciendo un uso más eficiente de las tecnologías a través de la implementación de la plataforma Tianguis Digital (ver capítulo 3, recuadro 3.1), con el apoyo de CAF. El uso de tecnologías en los sistemas de compra pública, según **información dispuesta en la plataforma**, logra (i) bajar los costos asociados a la burocracia y bienes y servicios adquiridos; (ii) reducir las barreras de participación, al aumentar la competencia y la divulgación de procesos de contratación públicos; (iii) agilizar los procesos, y (iv) disminuir los espacios de discrecionalidad de los procesos de compra pública. Adicionalmente, los datos allí recolecta-

[33] A modo de ejemplo, cabe referenciar la Resolución 12156 de 2019 de la Superintendencia de Industria y Comercio, mediante la cual fueron sancionadas tres personas jurídicas y dos naturales por haber coludido en procesos de Acuerdos Marco de Precios, adelantados por CCE para la provisión de insumos de oficina.
[34] Chile. DatosAbiertos - ChileCompra. Los datos están orientados a un modelo de colaboración interinstitucional, con el objetivo de potenciar no solo el valor de la información de las compras públicas, sino también ofrecer una mayor cantidad de datos en formatos definidos, y complementarlos con los existentes sobre el Estado. https://datosabiertos.chilecompra.cl/Home/SobreDatosAbiertos

dos aseguran la interoperabilidad entre dependencias para evitar la duplicación de labores y facilitar la gestión pública. La captura de datos en tiempo real también permite evidenciar oportunamente banderas rojas de corrupción, para que los Gobiernos actúen eficazmente y corrijan las falencias de forma preventiva. Es interesante destacar que esta plataforma se está desarrollando como herramienta *open source* o de código abierto[35].

Desafíos pendientes

A pesar de los considerables avances en la digitalización de los procesos de contratación y compra pública, aún quedan espacios de mejora para que estas plataformas digitales aseguren aún más integridad en los procesos de contratación, entre los que se incluyen:

- **Ampliación de la cobertura de los datos abiertos a todo el ciclo de la compra gubernamental.** Los usuarios pueden interactuar con los sistemas de compra pública puesto que la información de los contratos se publica en documentos digitalizados, pero solo partes de los datos están estructurados, y únicamente en algunas etapas del proceso contractual. Por consiguiente, la trazabilidad de las transacciones es limitada. Algunos países como Chile, Colombia y Paraguay han avanzado a la implementación de **estándares de datos de contrataciones abiertas**, si bien este no es el caso general para América Latina.

- **Mayor impulso a la implementación de sistemas transaccionales de compra pública.** La «transaccionalidad» implica que los procesos de registro de proveedores, la selección de los contratistas, la adjudicación de los contratos y la firma de los mismos deben hacerse por medios digitales; es decir, que los usuarios del sistema interactúen e intercambien información en tiempo real. La información registrada permite trazabilidad de las transacciones, con datos del usuario, fecha y actividad en la plataforma. Sin embargo, las plataformas existentes son transaccionales solo para algunos procesos.

- **Mejor interconexión de los sistemas de compra pública para generar reportes compatibles con otros sistemas de información de Gobierno, en especial, de hacienda pública y del ecosistema de integridad**.

    - La centralización de los procesos de abastecimiento del Estado por parte de las agencias de compra pública en América Latina genera

[35] El código abierto es un modelo de desarrollo de software basado en la colaboración abierta, y sus beneficios trascienden las cuestiones éticas o de gratuidad. Estos modelos ayudan a abaratar los costos de creación e implementación de softwares y amplían la participación de agentes interesados (en estos casos, entidades públicas, ciudadanos, órganos de control, organismos multilaterales, etc.). Adicionalmente, el código presenta ventajas en términos de actualización y adaptación a los contextos específicos; por ejemplo, si se promulgara una ley que obligara a modificar algún procedimiento de la plataforma, el código abierto permitiría hacer una actualización inmediata, sin depender de proveedores de software externos para evaluar la solicitud de actualización.

incentivos para que cada una de estas administre la información de acuerdo con estándares ajustados a las leyes y regulaciones en la materia, aunque no necesariamente se produce para ser compatible también con otros sistemas de información. En particular, la trazabilidad del gasto, la evaluación del desempeño fiscal y la transparencia en el proceso presupuestal de los Gobiernos serían más precisas si los sistemas de información de todas las fuentes del gasto (recursos humanos, deuda pública, inversión, compras) fueran compatibles en tiempo real (FMI, 2019).

- Adicionalmente, debe existir compatibilidad de los sistemas de información de compra pública con otros del ecosistema de integridad. Las autoridades y organismos de investigación y control de la corrupción conservan datos sobre las personas naturales o jurídicas sancionadas por conductas indebidas en el marco de la adjudicación y ejecución de los contratos públicos, **pero no necesariamente mantienen una conexión o verificación en tiempo real sobre las actuaciones de los sancionados en el ecosistema de contratación pública. Esto genera riesgos, puesto que los sancionados penal o administrativamente podrían arroparse en vehículos corporativos para seguir contratando** con el Estado, como **recientemente ocurrió con un contrato del Ministerio TIC de Colombia** por valor de USD 260 millones.

2.2.3. Rol de las Civic Tech en la lucha contra la corrupción

Relevancia

La relación entre los ciudadanos y sus Gobiernos puede enmarcarse dentro del «problema de principal-agente» (Varian, 1992), en donde los primeros encargan a los segundos de la administración y gestión de los bienes y servicios públicos esenciales para la sociedad. En dicha relación, existen asimetrías de información, dado que no todas las acciones del agente (en este caso, el Gobierno) pueden ser observadas por el principal (en este caso, los ciudadanos). La aplicación de estándares de transparencia activa reduce estas asimetrías. Sin embargo, la puesta a disposición de datos abiertos e información pública no resuelve completamente el problema de «principal-agente».

Por lo tanto, es necesario activar otros mecanismos de participación ciudadana, para dar voz a más sectores interesados en los procesos de formulación e implementación de programas y políticas específicos.

Así, el control sobre el «agente» no es solo función de la información revelada, sino también de la capacidad del «principal» (los ciudadanos) para ejercer una acción colectiva que ajuste, cuando sea necesario, las acciones del «agente» (Persson, Rothstein y Teorell, 2013). La **Alianza para el Gobierno Abierto** sostiene que la participación ciudadana es natural al desarrollo de políticas públicas, puesto que aquellos que son afectados por decisiones del Gobierno tienen derecho a hacer parte del proceso de toma de la misma, que reconozca y comunique las necesidades e intereses de todos los participantes.

Las organizaciones de la sociedad civil (OSC) y los Gobiernos están experimentando con plataformas digitales para alentar y proyectar la voz de los ciudadanos, con el objetivo de mejorar la prestación de servicios públicos e incidir en políticas públicas (Peixoto y Fox, 2016). Las herramientas tecnológicas, en particular los celulares inteligentes, sirven para canalizar y organizar la participación ciudadana en los procesos de Gobierno, en una tendencia llamada **Civic Tech. Esta se define como «cualquier tecnología usada por los ciudadanos para empoderarlos o ayudar al Gobierno a ser más accesible, eficiente y efectivo»** (Peixoto y Sifry, 2017).

Los **Gobiernos, cuando articulan sus políticas de digitalización con sus iniciativas de rendición de cuentas, también activan mecanismos Civic Tech o tecnología cívica.** Un ejemplo reseñado por la OCDE es Urna de Cristal de Colombia, administrada por su Ministerio TIC. Esta iniciativa busca brindar al mayor número de ciudadanos la posibilidad de interactuar con el Gobierno, conocer las actualizaciones de los proyectos y participar haciendo preguntas y ofreciendo propuestas al respecto. Urna de Cristal se ha usado para temas macro y de incidencia nacional, como consultar e informar a los ciudadanos sobre el **Plan Decenal de Justicia**, hasta asuntos de lucha contra la corrupción local en el programa la alimentación escolar (Keefer y Roseth, 2021).

Las nuevas tecnologías digitales tienen el potencial de habilitar y organizar el control ciudadano sobre las actuaciones de los funcionarios públicos en la implementación de programas y políticas o en el suministro de bienes o servicios públicos.

Las nuevas tecnologías digitales tienen el potencial de habilitar y organizar el control ciudadano sobre las actuaciones de los funcionarios públicos en la implementación de programas y políticas o en el suministro de bienes o servicios públicos. Aún no existe evidencia sistemática sobre la efectividad de estas innovaciones digitales para reducir la corrupción, debido, en parte, a que el éxito de estas plataformas se mide por la acogida entre los ciudadanos, pero no por la respuesta institucional frente a la participación ciudadana que convoca el Civic Tech (Peixoto y Fox, 2016). Esta sección describe algunas experiencias recientes de plataformas de tecnología cívica y gobierno digital que vienen implementándose en América Latina para habilitar la participación ciudadana.

Casos de uso

Las innovaciones de tecnología cívica y aplicativos ciudadanos se aplican cada vez más intensamente en materia de transparencia fiscal y presupuestos participativos. La transparencia en el presupuesto público es un aspecto fundamental en las políticas de integridad, puesto que el objetivo de los corruptos es, justamente, depredar las finanzas públicas. La transparencia presupuestal no solo implica divulgar toda la información relevante de manera oportuna y sistemática, sino que exige ciertos estándares de claridad, confiabilidad, accesibilidad y usabilidad de los datos e informes públicos sobre las finanzas públicas. Iniciativas multilaterales como la Iniciativa Global para la Transparencia Fiscal (GIFT, por sus siglas en inglés) han impulsado un estándar de datos para implementar la apertura presupuestaria en los países.

Sin embargo, la transparencia presupuestal puede ser más ambiciosa si incorpora a los ciudadanos activamente desde el momento en que los Gobiernos definen los presupuestos y asignan recursos para inversiones públicas. Los presupuestos participativos en el nivel local, que consisten en convocar a la ciudadanía para que haga parte de la deliberación y decisión en la asignación del presupuesto de su ciudad, son una forma más ambiciosa de transparencia presupuestal, que va más allá de los datos abiertos.

La habilitación de las tecnologías digitales para involucrar a los ciudadanos en la definición del presupuesto público fue posible en la última década en **Brasil**. Peixoto y Sifry (2017) muestran cómo la inclusión del voto remoto y mediado por herramientas digitales para definir y asignar el presupuesto a nivel estatal en Rio Grande do Sul impactaba las tasas de participación, la inclusión y la forma en que los ciudadanos se involucran durante todo el proceso en línea. Los autores no solo muestran que la participación subió más de un 12 % (frente a la línea de base que era la participación presencial), sino que el perfil de los ciudadanos que participaron en la iniciativa era en promedio más joven y más educado (aunque no necesariamente más participativo). Sin embargo, aún falta evidencia estadística que muestre el impacto que tendría el presupuesto participativo basado en plataformas digitales en la reducción de la corrupción.

Una combinación de tecnologías cívicas disruptivas fue implementada en **Perú**, donde el Ministerio de Economía y Finanzas desarrolló el **Sistema de Seguimiento de Inversiones**, una herramienta que vincula la información del Banco de Inversiones con la del Sistema Integrado de Administración Financiera (SIAF-RP), el Sistema Electrónico de Contrataciones del Estado (SEACE) y otros aplicativos informáticos que permiten el seguimiento de la inversión[36]. Esta plataforma fue clave en el **Operativo Virtual** que se implementó desde la sociedad civil durante la emergencia sanitaria para hacerle seguimiento al programa «Arranca Perú»[37]. La interoperabilidad entre datos de diferentes entidades públicas permite hacer un control del gasto público más afinado que el que puede derivarse de la revisión independiente de datos del SEACE. Por ejemplo, el sistema está en capacidad de recoger datos de todas las dependencias comprometidas con este programa de reactivación económica. No obstante, se evidenció la necesidad de mejorar la accesibilidad a las bases de datos y herramientas de registro, así como de incentivar un mejor uso de las mismas por parte de las autoridades competentes.

Las nuevas tecnologías están mejorando la interacción entre las personas y las autoridades presupuestarias. Por ejemplo, **Paraguay** introdujo una aplicación móvil llamada **PresupuestApp** en octubre de 2019, que no solo sirve para realizar consultas sobre presupuestos y gastos aprobados de cualquier institución pública, sino que también les permite a los ciudadanos reportar o denunciar irregularidades ante el Ministerio de Hacienda. Experiencias como las de Brasil y Paraguay muestran que las TIC ofrecen un potencial considerable en materia de acción colectiva para que los ciudadanos participen en las acciones y decisiones de sus Gobiernos. En particular, la ciu-

[36] Perú. Ministerio de Economía y Finanzas. https://www.mef.gob.pe/es/?option=com_content&language=es-ES&Itemid=100828&view=article&catid=767&id=5903&lang=es-ES

[37] Arranca Perú es un programa que busca reactivar la economía del país en medio de la emergencia sanitaria por el coronavirus (COVID-19). Involucra una serie de inversiones en el país que se aplicarán a sectores como los de transporte, vivienda y agricultura, entre otros, a fin de generar trabajos y mitigar el desempleo producto de la pandemia. Solo el sector de transporte recibirá cerca de PEN 3 800 millones para el mantenimiento de la red vial nacional y vecinal; ver Decreto de Urgencia 070-2020 que establece el plan de mantenimiento de vías como parte del programa: https://cdn.www.gob.pe/uploads/document/file/863907/DU070_2020.pdf

dadanía puede ser un actor más activo gracias a las TIC en las políticas de integridad presupuestal.

Las nuevas tecnologías cívicas también contribuyen a mejorar los mecanismos de denuncia ciudadana. Los países con buen desempeño en los índices de transparencia cuentan con leyes de protección de denunciantes de actos de corrupción (OCDE, 2016), reconociendo la importancia de incentivar a los ciudadanos para que denuncien los delitos asociados a corrupción. Adicionalmente a las leyes, las tecnologías digitales también pueden ser un recurso para incentivar y canalizar la denuncia ciudadana.

En Ciudad de México, la Agencia Digital de Innovación Pública (**ADIP**), a través del **Centro de Contacto Ciudadano**, ha aunado esfuerzos con las alcaldías locales de la ciudad para fortalecer los canales de reportes y quejas de la ciudadanía y garantizar que las peticiones ciudadanas sean atendidas eficazmente. Se busca ampliar el centro de contacto para una mayor participación ciudadana por medio de la innovación y la apertura.

A nivel federal, México adoptó la **Plataforma Digital Nacional**, construida de manera colaborativa con los ciudadanos y los Sistemas Locales Anticorrupción, y administrada por la Secretaría Ejecutiva del Sistema Nacional Anticorrupción. La plataforma utiliza el intercambio de datos del Gobierno para detectar fenómenos de corrupción como el conflicto de interés, la colusión y la celebración indebida de contratos a nivel nacional. De igual manera, no solo permite a la ciudadanía identificar fácilmente los conjuntos de datos que se ajustan a sus intereses en materia de reutilización y consulta para ejercer control social, sino que evalúa la calidad y estructura de los datos, de modo que, si no cuenta con los estándares necesarios, las entidades responsables de la información corrijan los informes y conjuntos de datos para reportar a la plataforma y, así, se garantice que la ciudadanía reutilice la información y ejerza control social.

Desafíos pendientes

El enfoque expuesto a lo largo de esta sección muestra cómo el gobierno digital puede usar el potencial de los datos y las tecnologías digitales para estimular la participación ciudadana y el control social como formas de acción colectiva en la lucha contra la corrupción. Sin embargo, existe un gran desafío en el seguimiento y evaluación de las plataformas digitales que habilitan el entorno Civic Tech como componente de las políticas de integridad pública.

Gran parte de **las investigaciones sobre plataformas de participación digitales se centra principalmente en la captación ciudadana y no en la respuesta institucional.** La revisión de experiencias se ha concentrado en aspectos como descargas, número de usuarios e interacciones (por ejemplo,

Gigler y Bailur, 2014). No obstante, no existe evidencia clara de que el ciclo de interacción entre el Gobierno y el ciudadano realmente se cierre, es decir, no se conoce si estas plataformas fomentan que el Estado responda a las denuncias ciudadanas, corrija comportamientos o solucione problemas. En consecuencia, es necesario que se también se mida el nivel de respuesta institucional[38].

Usando el marco del problema entre el «principal» y el «agente», se muestra que los ciudadanos (*i. e.*, el principal) tienen más información acerca de las acciones del Gobierno y, en algunos casos, colaboran en dichas acciones, pero no hay evidencia sobre cómo esa participación habilitada por medios tecnológicos se traduce en cambios o respuestas concretas en el comportamiento e integridad de los Gobiernos (*i. e.*, el agente). En la práctica, la literatura existente pareciera implicar que la aceptación de las plataformas necesariamente conduce a respuestas institucionales positivas. Esto podría inducir un alto grado de optimismo tanto en la literatura científica como en la práctica de política pública, sobre el rol de las tecnologías en la participación ciudadana (Peixoto y Fox, 2016).

Sumado a lo anterior, **la literatura tampoco ha identificado qué tan disuasorio es el espacio de participación y control ciudadanos sobre los agentes corruptos** (CAF, 2019; Ryvkin, Serra y Tremewan, 2017). Aunque Ryvkin *et al.* (2017) sugieren que la posibilidad de geolocalización sobre hechos de corrupción denunciados en plataformas de participación ciudadana podrían tener un efecto disuasorio, la literatura aún necesita identificar las variables que podrían hacer del entorno Civic Tech una herramienta de integridad efectiva. En este sentido, las políticas de gobierno digital que ponen en marcha plataformas que habilitan el entorno Civic Tech podrían fortalecer su desarrollo e implementación mediante algunas mejoras en su diseño, como:

- **Perfeccionar la recopilación y el uso de datos acerca de los ciudadanos que hacen uso de las plataformas de participación, tanto en línea como en persona.** Estos datos deben hacerse más abiertos, junto con los resultados, de modo que los mismos Gobiernos, las OSC y la academia puedan reutilizarlos para identificar variables de interés y espacios de mejora en los mecanismos de participación y control ciudadanos.

- **En el diseño de las políticas de participación ciudadana, control social y rendición de cuentas, incluir mecanismos de medición y seguimiento sobre la respuesta institucional a las peticiones, quejas y denuncias ciudadanas.** Dicho seguimiento debería incluir no solo aspectos objetivos, como las solicitudes efectivamente procesadas y cerradas, sino una valoración subjetiva de parte de los usuarios y las OSC acerca de la calidad de la respuesta institucional que recibieron.

[38] Esto también es consistente con lo señalado en las Lecciones y desafíos del capítulo 2, sección 2.2.1., sobre queja y denuncia ciudadanas.

- Respecto a la detección y denuncia de casos de corrupción a través de las plataformas Civic Tech, **los Gobiernos deben llevar registros y rendir cuentas sobre su procesamiento en datos abiertos, hasta el cierre final**. Esto plantea un reto, puesto que exige un ambiente colaborativo entre las diferentes ramas del poder público para que compartan datos sobre la investigación, judicialización y sanción de los casos denunciados, cuando haya mérito para ello.

- **Finalmente, las plataformas de participación ciudadana deben superar los retos que imponen las disparidades sociales y regionales en los países de América Latina, para aumentar e incentivar la participación ciudadana y el control social.** Esto implica aumentar la conectividad y cobertura de la infraestructura de comunicaciones, que aún no llega ni al 60 % de la población en promedio (Agudelo, 2021). Igualmente, estas plataformas deben ser diseñadas con un enfoque diferencial y facilitar la interacción ciudadana. En general, reducir la brecha digital es una medida necesaria para habilitar el ecosistema Civic Tech.

2.3. Reflexiones finales y recomendaciones

La revisión de la literatura y de las experiencias de política pública en materia de digitalización de los Gobiernos y la correspondiente reducción de riesgos de corrupción son indicios de que **las tecnologías digitales se están ganando un lugar como componente fundamental en las políticas de integridad pública, aunque persisten algunos retos en torno a la medición de su impacto para reducir la corrupción.** En ese sentido, es importante que los nuevos programas y políticas que vinculan integridad e innovación digital cuenten con mecanismos para reutilizar los datos, aplicando diseños experimentales o semiexperimentales que evalúen el efecto de la digitalización en la reducción de la corrupción.

De todos modos, sí hay estudios de calidad sobre algunas experiencias relevantes que dejan lecciones de interés. En este capítulo, la discusión logró distinguir ciertas funciones del Estado sujetas a digitalización, como:

- difusión de información para el control ciudadano
- transparencia y auditoría sobre el gasto público
- compras y contrataciones públicas
- control de transferencias sociales
- gestión aduanera
- trámites ciudadanos
- participación y denuncia ciudadanas

Para cada una de esas tareas, se pueden desarrollar soluciones digitales muy diversas. Aunque los efectos de cada intervención dependen en buena medida de sus especificidades de diseño e implementación, el compendio de experiencias analizadas en este reporte revela patrones importantes sobre el impacto que se puede esperar.

Las herramientas pensadas para fomentar el control ciudadano muestran resultados muy variados entre contextos. Esto revela, al menos, dos aspectos. Primero, que los detalles de implementación tienen consecuencias

de primer orden para el impacto de este tipo de herramientas. Segundo, que algunas formas de corrupción son más susceptibles de ser contenidas por el control ciudadano que otras. La transparencia puede ser especialmente útil ante formas de corrupción de baja escala y muy cercanas a la ciudadanía, en las que una pieza de información es suficiente para inferir irregularidades (por ejemplo, saber cuántos recursos maneja una escuela para hacer ciertas compras o proyectos puede ser suficiente para que la comunidad afectada detecte estas anomalías). Ante formas de corrupción complejas o que ocurren lejos de la última milla de provisión de servicios, puede ser muy difícil para la ciudadanía descubrir algo, incluso si tiene acceso a piezas de información. Esto no implica que el valor de las herramientas digitales para la difusión de información sea cuestionable: la transparencia es un principio de Gobierno fundamental, aun cuando no tenga efectos inmediatos contra la corrupción. Por otra parte, si se quiere que estas herramientas ejerzan un impacto concreto en la prevención de corrupción, es necesario evaluarlas constantemente y hacer los ajustes pertinentes.

Sobre los efectos de adoptar estándares de datos abiertos en la gestión pública, es muy poco lo que se sabe. Por ahora, están muy documentadas importantes deficiencias en la implementación de esos estándares, que generan grandes brechas entre las políticas formales y la transparencia real. Una de las consecuencias de esa diferencia entre lo formal y lo real es que se complica estudiar empíricamente este tipo de iniciativas.

En relación con las tareas de fiscalización dentro del propio Estado, las soluciones basadas en aprendizaje automático (*machine learning*) parecen promisorias.

En relación con las tareas de fiscalización dentro del propio Estado, las soluciones basadas en aprendizaje automático (*machine learning*) parecen promisorias. Aunque no hay análisis disponibles de impacto, distintos estudios han entrenado modelos usando datos reales (de compras públicas, presupuestos municipales o declaraciones tributarias) que muestran buen desempeño predictivo y que, aparentemente, podrían usarse para dirigir mejor los recursos de auditoría y control que tiene el Estado. Una ventaja de estas herramientas es su flexibilidad para integrarse de manera progresiva a los métodos tradicionales de trabajo.

Las plataformas electrónicas de compra y contratación han mostrado tener impacto en algunas variables de desempeño de las contrataciones (asociadas a la diversidad y calidad de los proveedores seleccionados) y no en otras (asociadas a los costos y duración de los proyectos). La literatura es aún muy limitada para ser concluyente, y no hay ningún estudio riguroso para América Latina. Un aspecto alentador es que los estudios existentes provienen de contextos de bajas capacidades institucionales (India e Indonesia) y, aun así, se ven algunos efectos positivos. Las plataformas de contratación electrónica parecen muy valiosas y, es de esperar que sus virtudes se potencien a medida que su uso se sistematice, porque esto permitiría tener registros cada vez más ricos y completos de las transacciones hechas por el Estado, lo que abre posibilidades de usos adicionales con esos datos.

En cuanto al control de **transferencias y programas sociales, las herramientas digitales en esta materia resultaron muy poderosas para reducir las pérdidas de recursos.** Sin embargo, también crean riesgos, especialmente asociados a la exclusión de beneficiarios legítimos de los programas en cuestión. Los efectos globales de cada intervención dependen mucho de las prioridades de política que se definen y de detalles de implementación. Una recomendación general es que iniciativas de este tipo se acompañen con mecanismos que permitan verificar que el acceso de los beneficiarios legítimos no se vea perjudicado.

En el campo de la **gestión aduanera**, se repasó una experiencia de computarización de trámites, en la que **se hallaron indicios de reducción en la incidencia de prácticas corruptas.** La misma mostró efectos muy positivos sobre la agilidad de los procesos, que repercutieron en la productividad y el empleo de las empresas importadoras.

Las experiencias repasadas también ilustran los mecanismos a través de los cuales la digitalización puede impactar sobre la corrupción. El mecanismo más claro es la reducción de la discrecionalidad de agentes del Estado para tomar ciertas decisiones y registrar transacciones. Por ejemplo, tareas como registrar a los beneficiarios de un programa social o decidir qué cargamentos fiscalizar en una aduana pueden tener mucha discrecionalidad y opacidad en ciertos contextos. La automatización de esos procesos es generalmente valiosa, especialmente cuando es fácil establecer criterios claros y algorítmicos para las decisiones que hay que tomar (es decir, cuando la discrecionalidad no tiene un valor intrínseco de gestión).

Un segundo mecanismo, potencialmente poderoso aunque con poca evidencia de respaldo por ahora, es la mejora de la inteligencia interna del Estado gracias a la generación y uso de datos. La digitalización abre la posibilidad de aprender mejor sobre la propia gestión, y esto tiene aplicaciones valiosas contra la corrupción. La mejor ilustración de eso son los modelos de aprendizaje automático para hacer un control más eficiente de las transacciones y operaciones del Estado.

La transparencia es un tercer mecanismo a través del cual la digitalización puede repercutir en los niveles de corrupción. Como se discutió previamente, este canal puede ser más efectivo contra algunas formas de corrupción que contra otras. Más aún, la capacidad de impacto de las iniciativas de transparencia depende de que también existan canales de reclamo y rendición de cuentas (electorales, administrativos, judiciales) a través de los cuales convertir la información en acción.

La tecnología avanza rápido, y constantemente aparecen nuevas herramientas con potenciales aplicaciones en la gestión pública. Los Gobiernos de América Latina comienzan a reconocer estas tendencias y adoptar políticas de

gobierno digital a partir de componentes que sugieren un potencial en materia de integridad pública en los campos de los trámites, el acceso a la información y las compras públicas, ente otros. Dada la velocidad de las cosas, es difícil anticipar con claridad los impactos de estas soluciones. Aun así, **las experiencias acumuladas dejan razones para ser optimistas respecto al papel de la digitalización en la prevención de la corrupción, a la vez que alertan sobre la enorme importancia de hacer evaluaciones rigurosas de las herramientas que se implementen**, tanto para maximizar su impacto como para evitar efectos colaterales indeseados.

3.

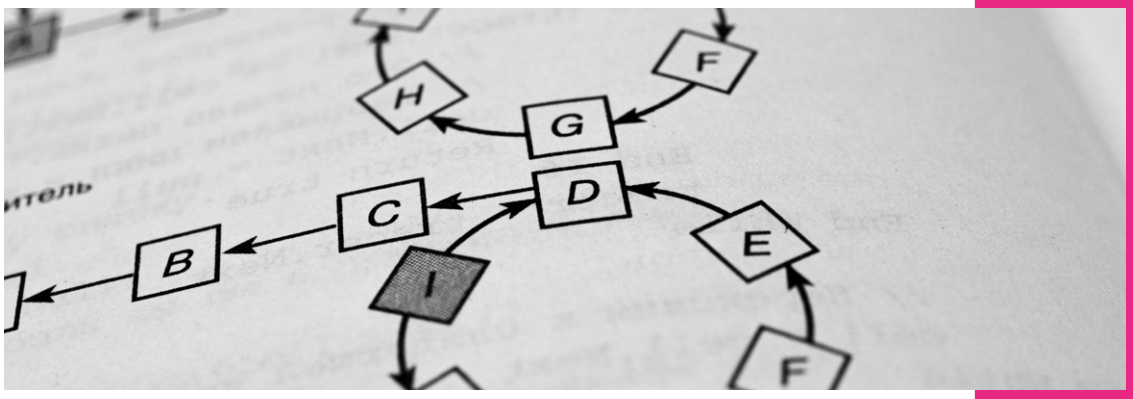
Inteligencia de datos

“

—Lo he comprobado con mucho cuidado —manifestó el ordenador—, y ésa es exactamente la respuesta. Para ser franco con ustedes, creo que el problema consiste en que nunca han sabido realmente cuál es la pregunta”.

Douglas Adams, Guía del autoestopista galáctico

Inteligencia de datos



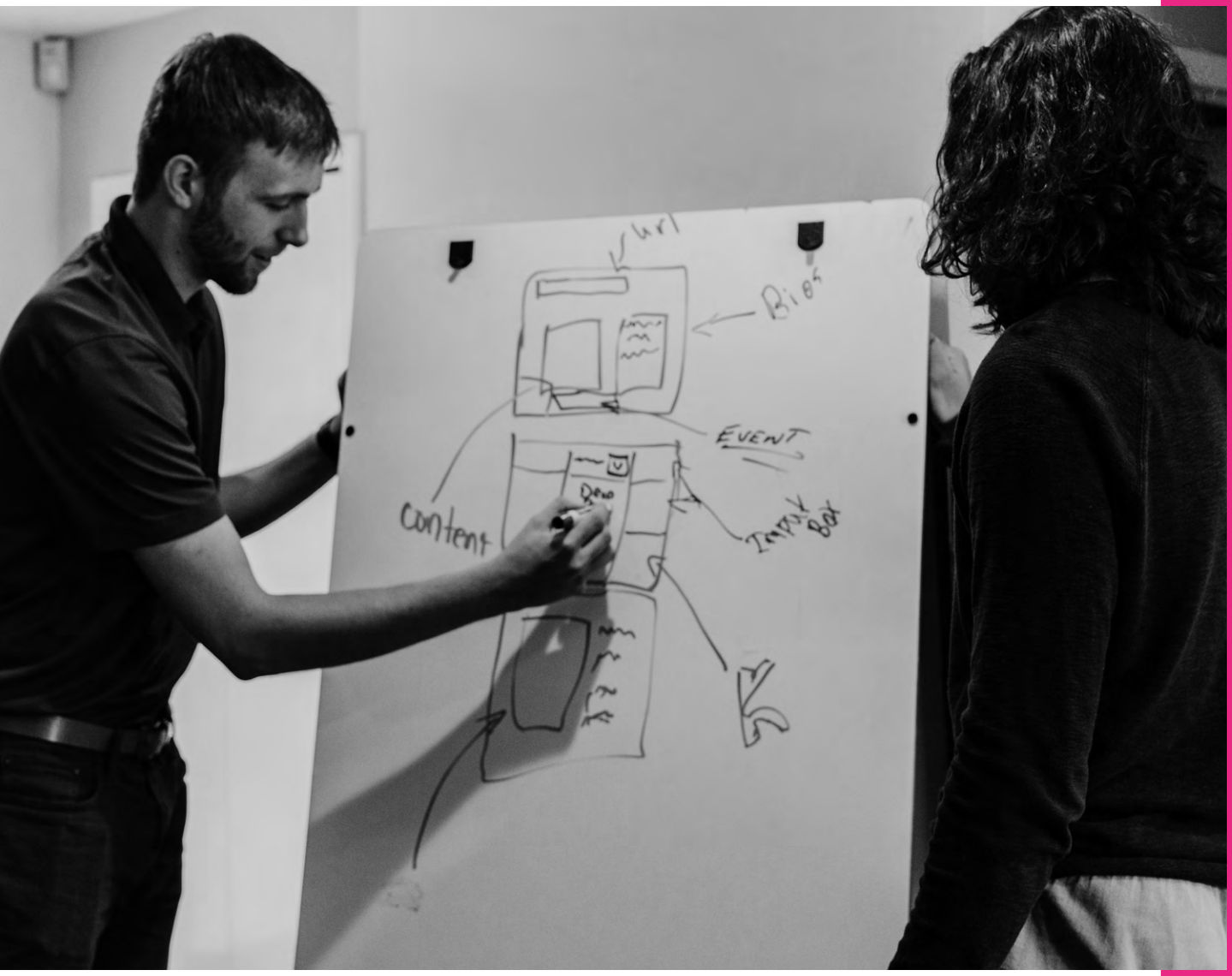
El primer experimento documentado en América Latina para aplicar técnicas computacionales en la toma de decisiones de Gobierno a partir de la captura descentralizada de datos ocurrió en Chile, en 1970. El proyecto Synco o **Cybersyn** fue una iniciativa impulsada por el entonces presidente Salvador Allende y desarrollada por el consultor británico Stafford Beer. Cybersyn requería una computadora central conectada a máquinas télex en las fábricas, para que desde allí se ingresaran datos sobre el proceso productivo, que luego serían analizados **centralizadamente**. La consolidación de la información se hacía en una oficina hexagonal, de 10 metros de diámetro, con capacidad para siete sillas giratorias y pantallas en las paredes. Las mesas y el papel estaban prohibidos para los analistas.

Cybersyn prometía recabar datos en tiempo real, diseñar programas estadísticos, **construir simulaciones computarizadas** de la economía chilena y comunicarse con las fábricas al localizar problemas que afectaran su rendimiento, aplicando un sistema de alertas tempranas. El golpe de Estado de 1973 terminaría con Cybersyn. Aunque la herramienta estaba pensada para la planificación centralizada de la producción reemplazando a las instituciones del mercado (lo cual fracasó), su tecnología abrió el camino a lo que hoy conocemos como **«inteligencia de datos»**.

50 años después, la idea seminal de Cybersyn no puede ser más relevante para enfrentar los fenómenos de corrupción en la región. Tras la aceleración digital de los últimos años (ver capítulo 2), tanto Gobiernos como entidades multilaterales están notando el potencial de herramientas que automáticamente capturan información proveniente de procesos y registros regidos por principios de transparencia activa y datos abiertos (por ejemplo, la

contratación pública, la gestión del gasto público, el nombramiento de funcionarios públicos y la rendición de cuentas de entidades públicas, entre otros). A diferencia del orden imperante en tiempos de Stafford Beer, la tecnología para procesar la abundancia de datos cuenta con un creciente poder de cómputo.

Los nuevos desarrollos en las tecnologías digitales, acompañados de un estándar adecuado de datos abiertos, podrían cambiar políticas y lograr herramientas anticorrupción más efectivas. Como se ha mostrado en los capítulos 1 y 2 de este informe, los Gobiernos que cuentan con elementos habilitadores como la digitalización de los servicios gubernamentales, políticas de transparencia activa y una agenda de datos abiertos pueden aprovechar las oportunidades que ofrece la transformación digital para fortalecer la integridad pública.



3.1. DIGIntegridad: definición e ilustración

Las experiencias internacionales evidencian los beneficios del uso de tecnologías que combinan los análisis predictivos y los macrodatos para fortalecer la transparencia y el enfoque preventivo en la lucha contra la corrupción. Por ejemplo, el Banco Mundial desarrolló un Sistema Automatizado, en prueba de concepto, para detectar potenciales fraudes en los procesos de contratación de los proyectos por él financiados (Grace, Rai, Redmiles y Ghani, 2016). La iniciativa consistió en un modelo de aprendizaje automático (o *machine learning*) para determinar la probabilidad de ocurrencia de fraude a partir de las denuncias o reportes sobre los procesos de contratación. El modelo empleó un método de potenciación de gradiente[39] y se entrenó con los datos de las investigaciones anteriores, en las que se encontraron denuncias tanto fundamentadas como infundadas. Adicionalmente, se puso a prueba el algoritmo, comparando los casos en los que el sistema predijo corrupción frente a las irregularidades realmente observadas. La plataforma alcanzó una tasa de éxito del 70 % en detección de casos de fraude, corrupción y colusión (Grace, *et al.*, 2016).

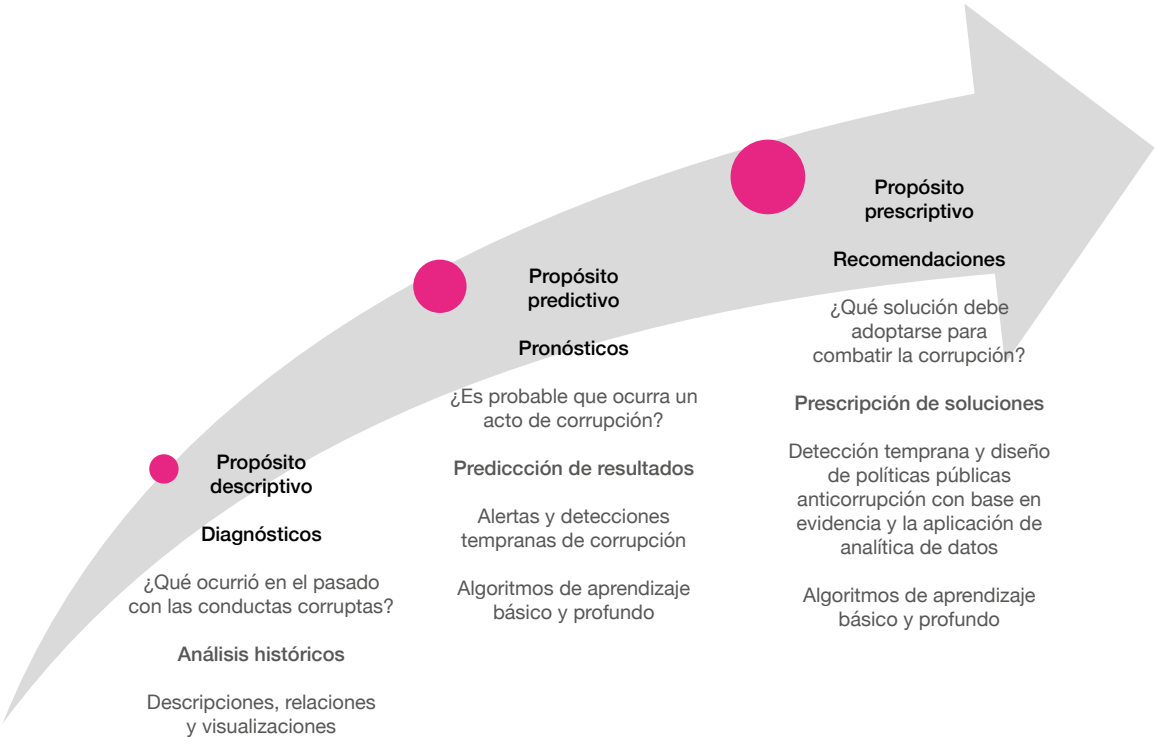
Varios Gobiernos están adoptando un enfoque disruptivo en sus esquemas de mitigación de riesgos de corrupción, que consiste en el uso de tecnologías digitales y procesamiento de datos para prevenir, detectar e investigar hechos de corrupción.

Los datos abiertos y las infraestructuras de datos abren la posibilidad de tomar grandes conjuntos y reutilizarlos para prevenir fenómenos de corrupción. Esto se puede hacer mediante la combinación de análisis predictivos con la aplicación de poder de cómputo para el procesamiento de macrodatos o *big data*.

Varios Gobiernos están adoptando un enfoque disruptivo en sus esquemas de mitigación de riesgos de corrupción, que consiste en el uso de tecnologías digitales y procesamiento de datos para prevenir, detectar e investigar hechos de corrupción. Estas innovaciones pueden hacer un uso inteligente de datos a partir de modelos descriptivos y predictivos (aunque la literatura distingue cuatro grandes usos: diagnóstico, descriptivo, predictivo y prescriptivo)[40]. Igualmente, representan un avance incremental en la lucha contra la corrupción, por cuanto permiten análisis cada vez más sofisticados en la identificación temprana y oportuna de los riesgos de corrupción. Las conclusiones que provienen del análisis de esta información también sirven para ajustar las políticas de integridad pública con base en evidencia (ver figura 3.1). Sin embargo, **para efectos de este informe, las experiencias internacionales existentes se agruparán en dos categorías: modelos descriptivos y predictivos.**

[39] El modelo se produce a partir de prototipos de predicción débiles, como regresiones, modelos logit y probit, y discontinuidades, entre otros. Luego, de forma secuencial y escalonada, se combinan para generar un modelo predictivo más general (Rudin, 2012).
[40] Ver: https://www.oracle.com/business-analytics/data-analytics/

Figura 3.1. Evolución del propósito del uso de datos como estrategia anticorrupción



Fuente: Elaboración propia.

Las iniciativas digitales para la integridad, o DIGIntegridad, sustentadas en el análisis de datos, emplean, en diferentes formas y grados, dos herramientas fundamentales: la analítica predictiva y los macrodatos (ver figura 3.2). Por un lado, la **analítica predictiva** (AP) permite estimar u otorgar un valor numérico o puntuación de probabilidad a la ocurrencia de un fenómeno o conducta particular de corrupción. Para determinar esa probabilidad, se realizan análisis estadísticos, consultas y algoritmos automáticos de aprendizaje a conjuntos de datos nuevos e históricos, creando así modelos predictivos (OCDE, 2019; Waller y Fawcett, 2013). De otra parte, los **macrodatos**[41] (o *big data*) corresponden a grandes volúmenes y variedad de datos, que se procesan a gran velocidad para obtener información sobre decisiones estratégicas frente a fenómenos analizados (Ortega, 2019). El analista de macrodatos rastrea patrones específicos en el conjunto de datos por medio de algoritmos[42] que le permiten identificar y valorar ciertas piezas considera-

[41] Un conjunto de datos que mida más de mil terabytes puede, al momento de hacer esta publicación, considerarse big data.
[42] Un algoritmo es un procedimiento computacional (conjunto de pasos finitos) que toma un valor o conjunto de valores como entrada, y produce un valor o conjunto de valores como salida (Cormen et al., 2001). Permite analizar enormes cantidades de datos y seleccionar una opción entre una infinidad de posibles decisiones.

das de importancia para el análisis individual de auditoría o de determinación de riesgos de corrupción.

Figura 3.2. Mecanismo de la analítica predictiva

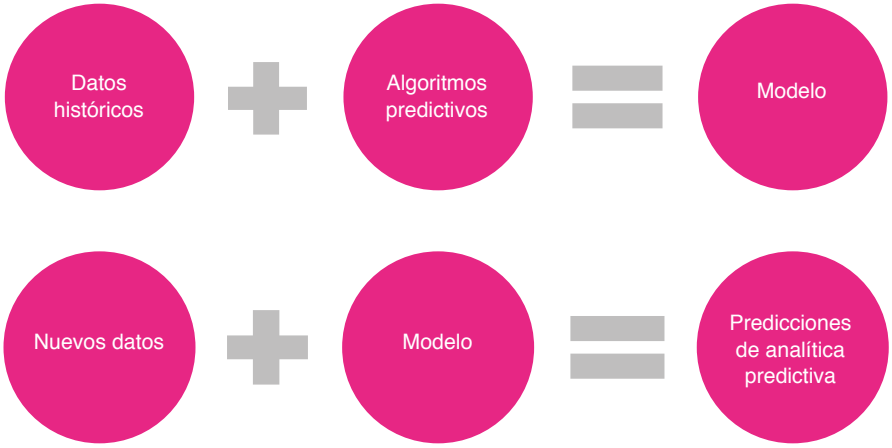


Figura 2.1. Fuente: Cetina (2020a).

La inteligencia artificial (IA) emerge como una herramienta para generar predicciones de analítica a partir del procesamiento de grandes conjuntos de datos, aunque su aplicación más común es la automatización de procesos. Existen varias definiciones, pero todas ellas tienen al menos dos elementos en común: implican el desarrollo de sistemas informáticos capaces de realizar tareas que normalmente requieren inteligencia humana[43], y exigen una gran cantidad de datos para entrenar a dichos sistemas en el desarrollo de las tareas que se le asignan a la IA. Las computadoras capaces de jugar al ajedrez o al go forman parte del campo de la IA, al igual que las plataformas de respuestas automatizadas o de reconocimiento facial.

Las técnicas de analítica predictiva (AP) de datos pueden sustentarse en aprendizajes automáticos básicos y profundos. La AP de aprendizaje automático básico *(basic machine learning*) requiere de un trabajo de identificación de los riesgos específicos[44] o comportamientos atípicos en cada una de las etapas del procedimiento en el que se busca alcanzar un mayor nivel de transparencia. Una vez que los riesgos de corrupción son explícitamente determinados por expertos y los modelos son programados para detectarlos, los algoritmos evidencian la presencia de estos dentro de los datos analiza-

[43] Como, por ejemplo, percepción visual, reconocimiento de voz, toma de decisiones, traducción entre idiomas y detección de patrones, entre otras.
[44] Por ejemplo, en el sector de adquisiciones públicas, existen listados de señales de alerta en cada una de las etapas de la cadena de compras (Volosin, 2015). Las sucesivas adiciones a los contratos, largos plazos entre la adjudicación del contrato y el inicio de su ejecución, o cambios súbitos en los objetos sociales de las sociedades contratistas, son algunos ejemplos de riesgo en la contratación pública (Cetina, 2020a).

dos, generando señales de alerta. Adicionalmente, mediante algoritmos de aprendizaje automático profundo (*deep machine learning*) es posible analizar los datos estructurados y no estructurados. Sin que previamente se definan alertas o predictores de corrupción, el software identifica patrones que provienen de datos históricos de casos de corrupción pasados, generando modelos aplicables a nuevos datos[45] (CAF, 2021). Así, es posible detectar o predecir posibles casos de corrupción. Los algoritmos de aprendizaje profundo abren nuevas posibilidades para la toma de decisiones basada en datos (Strusani y Houngbonon, 2019).

Este capítulo muestra las tecnologías sustentadas en ciencia de datos que pueden implementar los Gobiernos en materia de integridad pública y control de la corrupción. A partir de la clasificación y evolución del propósito del uso de datos (ver figura 3.1), se presentan casos prácticos en los que las innovaciones digitales usan ciencia de datos como parte de una estrategia anticorrupción.

- **Primero, se analizan las tecnologías que permiten desarrollar estudios descriptivos o diagnósticos.** Estas innovaciones están orientadas a detectar casos de corrupción y a fortalecer la integridad pública mediante la reutilización de los datos abiertos, la generación de relaciones y construcción de visualizaciones que ayudan a identificar y comprender mejor los riesgos de corrupción dentro de las actuaciones públicas. Asimismo, estas herramientas permiten el seguimiento y la vigilancia del gasto público por parte de autoridades de control y sociedad civil.

- **Segundo, se abordan las tecnologías que realizan análisis predictivos.** Estos métodos permiten anticipar cambios en el entorno antes de su ocurrencia. Para ello, asignan, con altos niveles de precisión, una puntuación de probabilidad de que los actos de corrupción ocurran. Estas tecnologías emplean algoritmos de aprendizaje básico y profundo (ver figura 3.5).

[45] Los algoritmos de aprendizaje se crean automáticamente a partir de datos y, cuanto más rico es el conjunto, mejor funcionan (Strusani y Houngbonon, 2019), de modo que la plataforma programada puede hacer una predicción o tomar una decisión como resultado.

3.2. Analítica descriptiva

Los desarrollos DIGIntegridad con propósitos descriptivos generalmente reutilizan conjuntos de datos abiertos para identificar anomalías que puedan estar asociadas a riesgos de corrupción (Cetina *et al.*, 2021). El acceso libre y directo a la información sobre las actuaciones del Gobierno, que es posible gracias a las políticas de transparencia activa y datos abiertos, combinado con el uso de herramientas digitales para procesar los conjuntos de datos, permite una comprensión integral de la gestión pública y de los fenómenos de corrupción que se generan en su entorno.

Una de las aplicaciones más efectivas de la tecnología y la analítica descriptiva de datos es la visualización que, aunque por sí misma no genera información nueva, transforma la estructura de representación de los datos. Dado que los seres humanos cuentan con una mayor facilidad de entender información en representaciones gráficas que en estructuras más complejas (Few, 2014), las herramientas visuales permiten procesar una gran cantidad de datos y presentarlos de una manera clara y sencilla. **El aporte de la visualización está en su capacidad de simplificar la representación sin perder información, no en los datos que la alimentan** (Chae y Olson, 2013).

3.2.1. Analítica visual para inteligencia financiera

Mediante visualizaciones de macrodatos, es posible detectar relaciones, patrones y anomalías entre los datos. Estos hallazgos orientan y alertan a los analistas sobre casos que merecen un seguimiento e investigaciones particulares. Las visualizaciones permiten identificar características difíciles de detectar con la simple observación manual de bases de datos. Las herramientas que se basan en el uso de técnicas matemáticas para traducir datos multidimensionales, como frecuencias, momentos, relaciones o vínculos, hacia figuras más bien intuitivas, como redes, nodos, nubes, mapas de calor y esquemas jerárquicos (*treemapping*), son muy útiles para detectar relaciones ocultas, demostrar la existencia de redes complejas y rastrear movimientos de flujos de dinero.

La Organización de las Naciones Unidas (ONU) desarrolló una plataforma de detección de redes de lavado de activos (goAML) y otra de intercambio de

información de inteligencia financiera (goINTEL)[46]. Ambas se basan en una idea relativamente sencilla: para procesar grandes volúmenes de información, las autoridades pueden recurrir a la visualización analítica de macrodatos. A nivel mundial, más de 49 países han adoptado goAML para la detección de redes de lavado de activos y financiamiento del terrorismo.

Generalmente, las entidades que suministran servicios financieros, y otras, como las intermediarias del sector inmobiliario, reportan a las autoridades de inteligencia financiera una serie de operaciones que consideran sospechosas (ROS)[47]. Los ROS son un insumo fundamental en las tareas de inteligencia financiera, que buscan prevenir e impedir la utilización del sistema financiero para la comisión de los delitos de lavado de activos o el pago de sobornos. Las Unidades de Inteligencia Financiera (UIF) de los Gobiernos procesan una cantidad considerable de información a partir de los ROS. El detalle de las transacciones allí consignadas genera un volumen de datos que no resulta analizable a partir de métodos tabulares[48]. Por ejemplo, consultar el portal del Financial Crimes Enforcement Network (FinCEN) acerca de la actividad de lavado de activos con uso de tarjeta débito en los Estados Unidos arroja más de 37 000 resultados[49].

Figura 3.3. Red de transacciones criminales visualizadas a partir de datos tabulares

Fuente: https://neo4j.com/blog/detect-investigate-financial-crime-patterns-linkurious/

[46] Esto hace parte de un ambicioso paquete llamado goPortfolio, que contiene modelos y plataformas tecnológicas para luchar contra el crimen organizado. De acuerdo con la ONU, actualmente, unos 125 países usan al menos uno de los aplicativos contenidos en goPortfolio. Ver: https://unite.un.org/goportfolio/
[47] Un ROS (Reporte de Operaciones Sospechosas) se hace sobre transacciones que, por su monto y otras características, no se ajustan a prácticas normales del negocio, de una industria o de un sector determinado, y no están razonablemente justificadas. Estos reportes hacen parte de un Sistema de Administración de Riesgos en Lavado de Activos y Financiación del Terrorismo (Sarlaft).
[48] Es decir, a partir del examen de funciones y valores en arreglos simples de filas y columnas, para luego seleccionar celdas de datos de interés.
[49] Nótese que nos referimos a solo un posible delito, en un año, en un país, a través de un medio de pago, y, de todos modos, se obtiene un volumen de información considerable. Ver: https://www.fincen.gov/reports/sar-stats.

La plataforma goAML comparte técnicas aplicadas en América Latina por las UIF de Gobiernos como Chile, Colombia y Perú, que han expuesto sus experiencias en los últimos años. El esquema trabaja en las siguientes cuatro fases:

5. **Recolección de datos:** se mapean las transacciones de fondos. De allí, el sistema sugiere transacciones inusuales que el analista también debe seleccionar. Es posible, por ejemplo, que un mismo grupo de personas (naturales o jurídicas) usen una misma cuenta bancaria, una misma dirección de domicilio, dispongan de uno o pocos proveedores (que pueden ser ficticios) y muevan en esa red gran cantidad de dinero.

6. **Análisis de datos:** posteriormente, las transacciones son filtradas de nuevo para determinar transacciones sospechosas y, luego, cruzadas con información concerniente a transferencias internacionales, reportes transfronterizos de intercambio de activos financieros y otros reportes adicionales, que los analistas aplican a la plataforma para filtrar de nuevo las transacciones y seleccionar aquellas que deben ser investigadas.

7. **Diseminación de información:** en este caso, las operaciones seleccionadas se reportan a los organismos de investigación que tienen facultades de policía judicial, así como a autoridades administrativas que se dedican a la vigilancia y regulación de actividades económicas. Allí, la información es valorada de nuevo.

8. **Desarrollo de interfaz:** si los organismos de policía judicial o investigación deciden abrir un caso, entonces, se crea una interfaz para que los movimientos de personas o corporaciones objeto de investigación sean detectados en tiempo real para las unidades de inteligencia, de investigación y judicialización, de modo que ratifiquen (o descarten) la existencia de una red de movimientos ilícitos de dinero.

3.2.2. Plataformas de visualización de las inversiones públicas

Las plataformas de visualización de inversiones públicas permiten que todos los interesados (ciudadanos, sector privado, organizaciones de la sociedad civil y otras agencias estatales) monitoreen en tiempo real dónde y cómo se invierten los recursos públicos. Los datos sobre las inversiones públicas son recolectados, refinados, automatizados, analizados y georreferenciados, con el fin de ponerlos en conocimiento público. Las visualizaciones de la información están disponibles en una plataforma *online*, cuyo diseño unificado e intuitivo facilita su consulta (ver figura 3.4). Al acceder a las

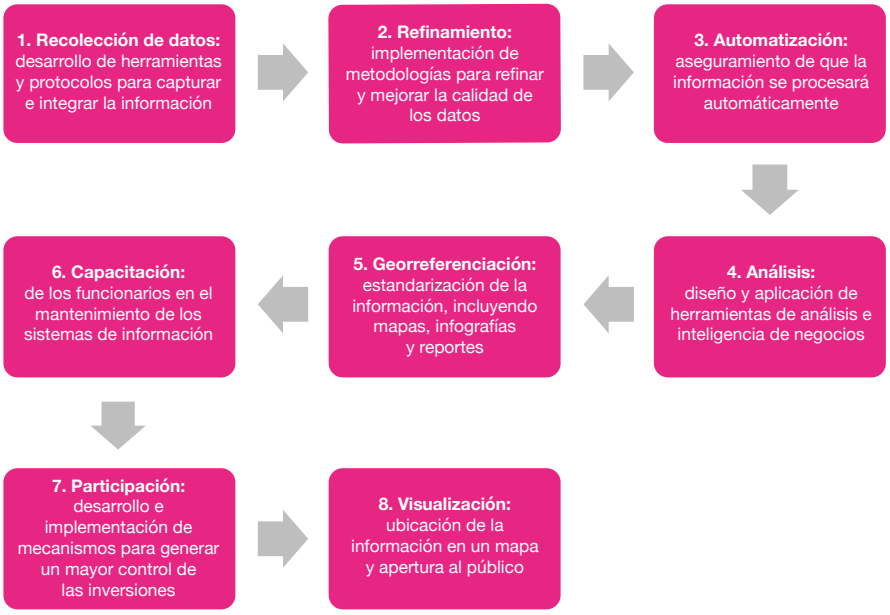
plataformas, los interesados pueden conocer, por ejemplo, cuál es el número de proyectos de inversión pública aprobados en una región específica, cuántos de ellos corresponden a una determinada vigencia fiscal, el avance del proyecto, su monto, y quiénes son los contratistas e interventores. De esta forma, la visualización facilita el seguimiento y la vigilancia del gasto público por parte de todos los sujetos interesados.

Los Gobiernos de la región están desplegando plataformas de monitoreo georreferenciado y automatizado de seguimiento de las inversiones públicas para mejorar su transparencia y eficiencia, como la plataforma **MapaInversiones, desarrollada con el apoyo del Banco Interamericano de Desarrollo (BID)**. La iniciativa se sustentó en la experiencia **MapaRegalías** en Colombia, la cual, desde 2012, permite conocer el avance de los proyectos de inversión pública financiados con regalías. De acuerdo con estimaciones del BID, el módulo MapaRegalías (ver sección 2.1) mostró un aumento promedio de aproximadamente el 8 % en la eficiencia de la ejecución física de los proyectos (Lauletta *et al.*, 2019).

MapaInversiones busca que, mediante plataformas digitales, los usuarios accedan a información georreferenciada y datos sobre los avances de proyectos públicos en locaciones específicas (ver sección 2.1). Estas plataformas ponen a disposición del público información inmediata y abierta (ver figura 3.4), relacionada con las inversiones públicas de sectores específicos, como, por ejemplo, inversiones en infraestructura, en servicios públicos domiciliarios y en salud, entre otros. Los usuarios pueden participar enviando sus comentarios y aportes, y cargando fotos para verificar avances de proyectos específicos (Foro Económico Mundial, 2021). Con el fin de hacer el gasto más transparente, eficiente y efectivo, se pone en conocimiento público dónde y cómo invierten las instituciones gubernamentales los fondos públicos. Actualmente, **Argentina**, **Colombia**, **Costa Rica**, **Jamaica**, **Paraguay**, **Perú** y **República Dominicana** cuentan con plataformas MapaInversiones que permiten conocer cómo se invierten los recursos públicos.

Figura 3.4.

Procesamiento de datos en la iniciativa MapaInversiones BID



Fuente: BID, s. f.

En el marco del COVID-19, se crearon módulos especiales para dar seguimiento y brindar transparencia a los recursos destinados para atender la emergencia sanitaria y social (BID, s. f.). Paraguay fue el primer país que implementó el **Módulo COVID-19**, seguido por Argentina, Costa Rica y República Dominicana. La construcción de estos módulos demuestra que los datos y las nuevas tecnologías habilitan controles y mecanismos de transparencia en las compras públicas para la atención de emergencias, por medio de la digitalización de procesos que maximizan la exposición de las actuaciones de los Gobiernos y permiten rastrear el uso de los recursos en tiempo real (Cetina, 2020b).

Los órganos de control también han puesto en marcha portales de visualización de obras públicas. En Perú, la plataforma **InfObras** fue creada en 2012 por la Contraloría General de la República del Perú, con el apoyo de la Cooperación Alemana al Desarrollo – GIZ, con el fin de fortalecer la transparencia en la ejecución de obras nacionales. En el **Infomapa**, puede hacerse el seguimiento a obras por localización, tipo de ejecución, monto de inversión, e inicio y estado de la obra, entre otros. A la fecha, se han registrado 106 265 obras por valor de USD 71 millones. Por su parte, en Chile, la Contraloría General de la República creó la plataforma **GEOCGR** en 2014. La plataforma digital busca fortalecer la transparencia y fomentar la participación de la sociedad civil. En el portal se encuentra disponible información georreferenciada sobre antecedentes de licitaciones, apertura de propuestas, adjudicación, desarrollo de la obra, montos y plazos (Chile Compra, 2014).

Los portales de visualización y seguimiento de obras no solo existen a nivel nacional, sino que también han sido desarrollados por gobiernos subnacionales. En Buenos Aires, desde 2017, la Plataforma **BA Obras** permite conocer a todos los interesados los avances de las obras públicas que se están construyendo. El portal usa georreferenciación y permite conocer todos los detalles del desarrollo de los proyectos por etapas, comunas y presupuesto. Cada proyecto cuenta con la información específica sobre la agencia gubernamental responsable, el avance, los datos de la empresa contratista, los montos de contrato y el proceso de contratación. La página tiene **software de código abierto** para que cualquier municipalidad pueda replicar el sitio web, y **datos abiertos** para que los interesados los utilicen de acuerdo con su interés.

3.2.3. Analítica de redes en la lucha contra el crimen organizado

El análisis de redes es un conjunto de técnicas integradas para representar las relaciones entre actores y determinar el alcance y naturaleza de las estructuras sociales que surgen de la recurrencia de estas relaciones. El supuesto básico es que las mejores explicaciones de los fenómenos sociales se obtienen mediante el análisis de las relaciones entre entidades (Chiesi, 2001). Esta técnica se realiza mediante la recopilación de datos relacionales organizados en forma de matriz. Si los actores se representan como nodos y sus relaciones como líneas entre pares de nodos, el concepto de red social pasa de ser una metáfora a una herramienta analítica operativa, que utiliza el lenguaje matemático de la teoría de grafos y del álgebra matricial y relacional.

Las técnicas que subyacen al análisis de redes permiten a los investigadores especificar indicadores y controlar hipótesis de trabajo, a través de la definición y medición de conceptos generales tradicionales, como estructura social y cohesión. En materia de lucha contra la corrupción, por ejemplo, el caso de los **Panamá Papers**, requirió de técnicas de **análisis de redes** para exponer la dimensión de los flujos ilícitos que se movilizaban entre miles de actores.

La Procuraduría General de la Nación (PGN) de Colombia, con el apoyo de CAF, desarrolló un protocolo conformado por algoritmos para la analítica de redes de los casos de corrupción investigados por la Procuraduría[50]. Como punto de partida para el desarrollo de la analítica de redes criminales en el contexto de la Procuraduría General de la Nación (ARCPGN), los datos del

[50] En Colombia, la Procuraduría General de la Nación (PGN) tiene dentro de sus competencias vigilar la conducta de los servidores públicos y de los particulares que ejercen funciones públicas o manejan recursos gubernamentales.

Sistema de Información Misional (SIM) que recopila la información de todos los procesos disciplinarios adelantados por la PGN, se complementó[51] con la información existente en los expedientes físicos de carácter público. Para el efecto, se digitalizaron dichos expedientes con algoritmos OCR (*Optical Character Recognition*), de manera que fueran potencialmente analizables con algoritmos NER (*Named-Entity Recognition*) ajustados, a fin de extraer las entidades básicas necesarias para estructurar interacciones.

La digitalización de los expedientes por OCR y NER permitió consolidar una Base de Datos de Interacciones (BdI), que sirvió para modelar redes identificando nodos y formas de interacción comunes. Estos modelos permiten extraer información de estructuras de macrocorrupción y cooptación institucional (Garay Salamanca, Salcedo-Albarán y Macías, 2018), informando acerca de:

- Frecuencias estadísticas de personas naturales y jurídicas que se repiten en distintos casos.
- Niveles de influencia de determinadas personas naturales y jurídicas.
- Nodos y agentes que concentran niveles de centralidad directa o capacidad de intervención.
- Patrones de formas de interacción y articulación de macrorredes.
- Cantidad de redes y casos en los que aparece un mismo nodo/agente, entre otros niveles de análisis.

El Análisis de Redes Criminales puede ayudar a identificar estructuras ilícitas de cooptación institucional, que no operan a partir de sobornos esporádicos sino de procedimientos sistemáticos durante períodos extensos, pero que son susceptibles de pasar desapercibidas frente a los organismos de investigación, judicialización y control[52]. En Colombia, la herramienta ARCPGN ha permitido elaborar modelos de redes ilícitas de elevada complejidad y diversidad, en las que miles de nodos y agentes establecen miles de interacciones. Estas redes, en algunos casos, pueden denominarse «macro» porque superan por el doble de magnitud el tamaño de una red social que puede aprehender y analizar directamente la mente humana (Salcedo-Albarán y Garay-Salamanca, 2016)[53]. En particular, una red de macrocorrupción y cooptación institucional es aquella establecida para ejecutar esquemas de

[51] La CAF encontró que la información consignada en algunos campos del SIM presenta limitaciones de cantidad y de calidad. Los datos no estaban estructurados y la forma de descripción de los casos variaba en nivel de explicación.
[52] Sin embargo, el análisis, en sí mismo, no tiene el objetivo de servir como soporte o aporte a investigaciones en curso; más bien, es una herramienta de apoyo para identificar las hipótesis y los cursos de las investigaciones.
[53] En general, la complejidad de una red en la que participan más de 300 nodos/agentes hace imposible, en términos prácticos, memorizar, asociar y, por tanto, entender las características de los agentes que participan en dicha red y sus interacciones.

El Análisis de Redes Criminales puede ayudar a identificar estructuras ilícitas de cooptación institucional, que no operan a partir de sobornos esporádicos sino de procedimientos sistemáticos durante períodos extensos, pero que son susceptibles de pasar desapercibidas frente a los organismos de investigación, judicialización y control.

corrupción, y cuyo tamaño cumple las características de complejidad de una macrorred criminal (Garay Salamanca, Salcedo-Albarán y Macías, 2018d).

Con el ARCPGN, se analizaron tres casos sobre redes de corrupción en Colombia que han tenido trascendencia nacional y cuya operación bien podría haber pasado desapercibida:

- El **«cartel de la salud»**, que operaba en el departamento de Córdoba, desviando recursos destinados a atender tratamientos médicos. Este mecanismo operaba a través de la creación de pacientes ficticios y de la complicidad de las entidades aseguradoras y las que prestan los servicios de salud a los ciudadanos. En este caso, la información de tres expedientes fue consolidada en una BdI unificada que permitió modelar una red conformada por 287 nodos/agentes relacionados mediante 621 interacciones. Esto contrasta con la visualización de la información del sistema de la PGN, donde solo se reportaron 21 nodos/agentes y nueve interacciones. Esto implica que el segundo modelo informa más acerca de la complejidad del fenómeno analizado.
- El **Programa de Alimentación Escolar** (PAE), que es el complemento alimentario que reciben los niños en las escuelas y colegios públicos en Colombia. Con la complicidad de entidades contratantes e interventores, se cobraron precios exorbitantes por los alimentos y se subestandarizaron las raciones alimentarias (Keefer y Roseth, 2021). Tras consolidar la información de tres expedientes acerca de deficiencias en la implementación del PAE en los departamentos de Guajira, Caquetá y Putumayo, el resultado fue un modelo de red conformada por 323 nodos/agentes, que establecieron 555 interacciones.
- El caso Odebrecht, particularmente, las irregularidades ocurridas en el contrato de concesión de la Ruta del Sol II. La firma Odebrecht pagaba sobornos y financiaba campañas políticas a cambio de la adjudicación de contratos de obra pública (Garay Salamanca, Salcedo-Albarán y Macías, 2018d). Tras analizar con el ARCPGN un fallo disciplinario, complementado con sentencias judiciales y administrativas, la PGN destapó un modelo de red de 162 nodos/agentes con 266 interacciones.

Los análisis de redes, que facilitan la identificación de relaciones ilícitas, mostraron que algunas personas jurídicas se constituyen con el único propósito de contratar fraudulentamente e incurrir en actuaciones sancionadas penal o administrativamente, mientras que otros vehículos corporativos se establecen para cometer actos aparentemente legales pero funcionales a objetivos ilícitos en el contexto de una estructura de macrocorrupción y cooptación institucional. Igualmente, se detectaron personas naturales que se contratan a sí mismas por medio de dos personas jurídicas diferentes, para capturar recursos de los contratos con el Estado.

A través de la minería de datos, pueden descubrirse patrones o relaciones, en especial al cruzar varias fuentes de datos como transacciones electrónicas, registros bancarios, reportes de los empleadores, registros de compra de vehículos y publicaciones realizadas en redes sociales, entre otras..

3.2.4. Publicidad de las compras públicas para la emergencia sanitaria

Con el fin de garantizar apertura y publicidad necesarias en las compras públicas (ver capítulo 2), aun en el marco de circunstancias excepcionales como la emergencia sanitaria, existen sistemas automatizados que hacen públicos y abiertos los datos sobre la contratación pública en contextos de emergencia. Estas herramientas tecnológicas ponen en conocimiento de todos los interesados datos relacionados con el presupuesto asignado a la atención de la emergencia, las necesidades de compra y contratación de los Gobiernos, y los contratos celebrados, entre otros. De esta forma, se garantiza que los gastos se realicen con la urgencia y celeridad necesarias durante una emergencia, sin sacrificar la transparencia en las compras públicas.

Un ejemplo de solución tecnológica para aumentar la apertura y la publicidad en compras públicas de emergencia fue desarrollada en Estados Unidos: se trata de un **sistema automático de alertas a proveedores** sobre contratos con el Gobierno. El registro es gratis, permite a cualquier empresa ser parte de él, y se basa en un apareamiento entre la línea de negocios del aspirante que se va a contratar, con un sistema automático de búsqueda de procesos de contratación. Luego, el sistema envía alertas automáticas a los interesados por correo electrónico. Ello le ahorra tiempo de búsqueda a los potenciales proponentes y maximiza el nivel de publicidad de las oportunidades de negocio con el Gobierno. En este caso, la apertura mediada por la tecnología informa al mercado sobre necesidades urgentes de abastecimiento en tiempo real. Esto propicia un ambiente de control desde el sector privado y la sociedad civil, para que la declaratoria de emergencia no resulte en manipulación indebida de precios o de condiciones de suministro.

3.3. Analítica predictiva

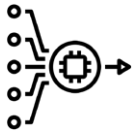
Las tecnologías que se alimentan de los datos abiertos y emplean técnicas de analítica predictiva permiten generar alarmas o valoraciones de riesgos de corrupción en las etapas iniciales de los procesos gubernamentales. Mediante diferentes técnicas de análisis de datos, estas tecnologías digitales y de la información generan un avance en la lucha contra la corrupción, pues permiten superar un rol reactivo hacia un rol preventivo. Esto es posible porque la inteligencia (Llinás, 2003) de las tecnologías digitales, a través de la ciencia de datos, tiene la capacidad de estimar la posible ocurrencia de fenómenos de corrupción con base en datos históricos.

Las técnicas de analítica predictiva pueden emplear algoritmos de aprendizaje[54] automático básico y profundo. Los algoritmos de aprendizaje básico se emplean para el análisis de datos estructurados. Un supervisor identifica explícita y previamente los riesgos de corrupción o comportamientos atípicos en cada una de las etapas del procedimiento en el que se busca alcanzar un mayor nivel de transparencia. Cuando los algoritmos detectan la presencia de los riesgos en el conjunto de datos analizado, se generan señales de alerta de colusión. Por otro lado, con los algoritmos de aprendizaje profundo, las computadoras pueden analizar datos estructurados y no estructurados (imágenes y textos). En lugar de ser programado explícitamente, el software aprende a identificar riesgos de corrupción a partir de datos. Un algoritmo establece los riesgos y los comunica a los competentes para realizar los procedimientos de control, y los exporta a otras bases de datos para su almacenamiento.

[54] Los algoritmos de aprendizaje se entrenan con «conjunto de datos de entrenamiento» que se comparan con el «conjunto de datos de validación» para verificar la construcción del algoritmo. Luego, se emplean los «conjuntos de datos de prueba» para medir el poder de predicción del algoritmo (Strusani, y Houngbonon, 2019).

Con sustento en las conclusiones de las personas encargadas, la herramienta refina su algoritmo, olvidando los casos descartados y recordando los riesgos de corrupción verificados.

Figura 3.5. Aprendizaje automático

	Aprendizaje automático básico (*basic learning*)	Aprendizaje automático profundo (*deep learning*)
Insumos (*Inputs*) 	Datos estructurados (tablas en formato Excel, CVS, tab)	Datos estructurados Datos no estructurados (textos, imágenes, videos, audios, correos electrónicos)
Aprendizaje (*Process*) 	Supervisado: un experto o supervisor establece las reglas o variables para analizar los datos. Quien etiqueta conoce el comportamiento de los datos que quiere predecir, y el algoritmo hace predicciones con los nuevos datos.	No supervisado: el algoritmo recibe y explora conjuntos de datos no etiquetados, e infiere o descubre patrones de comportamiento de similar en los datos, sin que se hayan establecido previamente reglas o predictores.
Salidas (*Outputs*) 	El software identifica el patrón de corrupción explícitamente definido por el supervisor.	El software identifica patrones de corrupción de acuerdo con el comportamiento de los datos, sin que medien predictores específicos de corrupción.

Fuente: CAF (2021).

3.3.1. Generación de banderas rojas

Las plataformas de sistemas de riesgo o de banderas rojas (*red flags*) parten de la información disponible para establecer peligros y crear patrones que permiten predecir un resultado esperado en un determinado proceso. La bandera se activa cuando el algoritmo identifica el riesgo, con el objeto de que se realice un análisis detallado del procedimiento en el que se generó la alerta. Cuando se produce una señal de advertencia, no necesariamente existe corrupción, pero sí la necesidad de una revisión detallada del caso.

Una de las innovaciones basadas en datos que aborda este enfoque preventivo y de vigilancia sobre la fase de adjudicación de los contratos y los precios fijados por los proponentes proviene del **Sistema Analítico de Indicadores de Colusión del Gobierno de Corea** (BRIAS[55], por sus iniciales en inglés), administrado por la Comisión Coreana de Comercio Justo (KFTC). BRIAS utiliza los datos abiertos generados por el sistema de contratación y compra pública del país (KONEPS) para construir un sistema automatizado de indicadores de riesgo o de banderas rojas respecto de posibles irregularidades o ineficiencias en la contratación. Dentro de este, la recolección de datos comienza desde el mismo momento en que un usuario se registra, bien sea como visitante, proponente o comprador, de modo que sus credenciales (la dirección IP, fechas y horas de visita, módulos visitados, comunicaciones, etc.) puedan ser usadas para propósitos estadísticos y analíticos.
El sistema calcula la probabilidad de corrupción en los procesos licitatorios seleccionados, y puede requerir información adicional para afinar los algoritmos. Estos evalúan la siguiente información:

- Número de proponentes por proceso licitatorio
- Tipo y método de selección del contratista
- Precio de la oferta ganadora del contrato
- Información financiera y organizacional de los proponentes

BRIAS recopila la información de KONEPS, y cada mes se realiza un proceso automatizado de analítica de datos, de acuerdo con un umbral mínimo presupuestario: licitaciones superiores a USD 423 800 y obras públicas desde USD 4,2 millones. En 2012, BRIAS detectó 40 casos de colusión que llevaron a la imposición de multas por USD 847 millones (OCDE, 2016).

[55] Bid Rigging Indicator Analysis System (BRIAS).

Otra plataforma predictiva interesante se desarrolló en Hungría, con el apoyo de Transparencia Internacional (2015). La herramienta de banderas rojas analiza los datos de contratación pública e identifica riesgos de corrupción con énfasis en prevención y alertas tempranas. Cada día, los datos del Diario Electrónico de Licitaciones (*Tender Electronic Daily* – TED) son analizados mediante algoritmos para detectar procesos de contratación con riesgos de corrupción, de acuerdo con 40 indicadores de riesgo construidos por expertos. Una vez es identificado el peligro, se puede requerir información complementaria, y solo se hacen públicos los casos con un «riesgo severo» (Comisión Europea, s. f.). Desde su implementación hasta finales de 2020, el sistema generó alertas tempranas para aproximadamente 20 000 contratos.

Las organizaciones de sociedad civil también cuentan con desarrollos importantes que facilitan el control ciudadano sobre el gasto público. En Perú, el algoritmo **FUNES**[56], desarrollado por la organización **Ojo Público**[57], busca vínculos de empresas que podrían determinar si salen ganadoras en una licitación pública. Desde principios de 2018, Ojo Público ha logrado extraer información de bases de datos públicas sobre contratos realizados por el Estado peruano para investigar posibles riesgos de corrupción a partir de conexiones políticas y financieras que identifica el aplicativo FUNES[58]. Este algoritmo se ha escrito a partir de un desarrollo ya probado por Mihály Fazekas, del **Government Transparency Institute**. Dicha aplicación se basa en un sistema de banderas rojas que FUNES calcula con base en el nivel de competencia de las licitaciones, su tiempo de publicación, sus criterios de evaluación, tiempo de evaluación de propuestas y adjudicación de contratos, y aportes de los contratistas a campañas políticas, entre otros aspectos[59].

Ojo Público hizo adaptaciones al contexto peruano, priorizando otros indicadores para poder identificar posibles patrones de corrupción, como, por ejemplo, los vínculos entre un político y la persona de la municipalidad o el Gobierno que va a contratar. De acuerdo con los hallazgos de FUNES, «entre 2015 y 2018, Perú entregó 110 mil adjudicaciones públicas a un único postor que no tuvo competencia y a compañías creadas poco antes de que se realicen las licitaciones, por el monto de S/ 57 mil millones (cerca de USD 16,8 millones)»[60]. Este desarrollo funciona a partir de una combinación de minería de textos, análisis de redes y valoración de riesgos para poder determinar un indicador de posible corrupción en un contrato público, y lo pone a disposición de la ciudadanía.

[56] En alusión al célebre cuento del escritor argentino Jorge Luis Borges llamado Funes el memorioso, cuyo protagonista, después de caerse de su caballo y sufrir una lesión en la cabeza, puede percibir las cosas con todo detalle y lo recuerda todo. Fue incluido en el libro Ficciones (1944).
[57] Ojo Público es un medio de comunicación investigativo en Perú. En 2015, recibió el Premio de Periodismo de Datos a la Mejor Investigación del Año, otorgado por la Red de Editores Globales (GEN). En 2016 obtuvo el tercer premio del Premio Latinoamericano de Periodismo de Investigación, otorgado por Ipys y Transparency International.
[58] Ver: https://ojo-publico.com/especiales/funes/
[59] Más detalles en Fazekas y Kocsis (2020).
[60] https://knightcenter.utexas.edu/blog/00-21439-peruvian-investigative-site-ojo-publico-develops-algorithm-track- possible-acts-corrupt

Recuadro 3.1.

Generación de banderas rojas.
Plataforma Tianguis Digital – Ciudad de México

El objetivo principal de la plataforma de compras públicas de la Ciudad de México, Tianguis Digital, desarrollada con el apoyo de CAF, es mejorar la eficiencia y transparencia de las contrataciones públicas de la ciudad a través de tres módulos informáticos.

El desarrollo tecnológico tiene tres fases importantes:

Fase I: su objetivo es facilitar la gestión digital, competencia e integridad con los procesos de contratación, por medio de juntas de aclaraciones en línea y un algoritmo que detecta el riesgo de corrupción.

Fase II: se encarga de apoyar el seguimiento y control público en todas las etapas del proceso de contratación, a través de un concurso digital y notificaciones automatizadas a proveedores sobre oportunidades de contratación.

Fase III: busca fomentar la participación e inclusión en contrataciones públicas en la etapa de ofertas, mediante la implementación de un tablero de control interno y un visualizador público de contrataciones.

Usando el Estándar de Datos para las Contrataciones Abiertas – EDCA (**OCDS por sus siglas en inglés Open Contracting Data Standard**), Tianguis permite identificar alertas en los procesos de contratación pública como períodos cortos de licitación, bajo número de oferentes en una licitación y porcentaje alto de contratos con enmiendas, entre otras. Estas alertas se muestran en el tablero de control para que los responsables de los procesos verifiquen y valoren los riesgos.

Fuente: Elaboración propia.

3.3.2. Combinación de *big data* y analítica visual

Los macrodatos tienen un enorme potencial para la gestión gubernamental y fortalecimiento de las herramientas en la lucha contra la corrupción. Estos grandes conjuntos de datos pueden emplearse para la construcción de algoritmos básicos de aprendizaje, a través de los cuales se establecen relaciones entre datos para predecir riesgos o alertas de corrupción. Una vez los riesgos son identificados, se construyen visualizaciones intuitivas, como

Estos grandes conjuntos de datos pueden emplearse para la construcción de algoritmos básicos de aprendizaje, a través de los cuales se establecen relaciones entre datos para predecir riesgos o alertas de corrupción.

redes/nodos, nubes, mapas y esquemas, que orientan y alertan a los analistas sobre casos que merecen un seguimiento e investigaciones particulares.

En Colombia, la Contraloría General de la República (CGR), entidad encargada de velar por el buen uso de los recursos públicos, desarrolló una Central de Información Contractual llamada OCÉANO. La plataforma recoge la información de diferentes fuentes que incluyen pero no se restringen a: los sistemas de compra pública, el Sistema de Información de Registro de Sanciones y Causas de Inhabilidades (SIRI), el Sistema de Identificación y Registro Civil, el Sistema de información de Impuestos y Aduanas Nacionales, y el Registro Único Empresarial y Social (RUES), entre otros.

Esta herramienta digital establece relaciones entre los contratos celebrados a nivel nacional y los analiza para detectar posibles casos de corrupción; a través de un análisis matricial de redes y construcción de vectores, ha permitido detectar irregularidades en la contratación que son prevenidas, controladas y sancionadas, como en los siguientes casos:

- Detección de «mallas de contratación»: nodos donde se encuentran personas naturales o jurídicas que controlan la contratación con el Estado en una o más regiones y en uno o más sectores, sin contar necesariamente con la idoneidad y experiencia requeridas para suscribir contratos con el Estado.

- El uso de registros mercantiles pertenecientes a personas fallecidas para contratar con el Estado.

- La adjudicación de contratos a compañías ya sancionadas o que, habiéndolo sido, usan otros vehículos corporativos para arroparse en ellos y volver a contratar con el Estado.

- Indicadores o coeficientes de concentración en la contratación pública.

La plataforma, que funciona en el marco de la recientemente creada **Dirección de Información, Análisis y Reacción Inmediata**, ha logrado analizar los datos de más de ocho millones de contratos entre 2014 y 2020, que superan en valor los USD 250 mil millones. La CGR estima que el 27 % de esa contratación se asigna a contratistas que se repiten, bien sea porque se camuflan en vehículos corporativos o porque constituyen empresas con actividades económicas muy disímiles. La CGR ha denunciado casos en que una misma persona se encarga en una entidad territorial de la adquisición de maquinaria, dotación de calzado, de la provisión de los refrigerios estudiantiles y hasta de la celebración de reinados. En otro **caso denunciado**, aparecen contratos por mercados, compra de gallinas, mantenimiento de instrumentos de cuerda, instalación de parques y alimentación escolar a cargo de la misma empresa. Los datos que alimentan estos instrumentos se obtienen por medio

de 5 420 fuentes de información, así como del acceso a una red integrada por 683 entidades, entre ellas, la Agencia Nacional de Infraestructura (ANI), el Departamento Nacional de Planeación (DNP) y el Departamento Administrativo Nacional de Estadística (DANE).

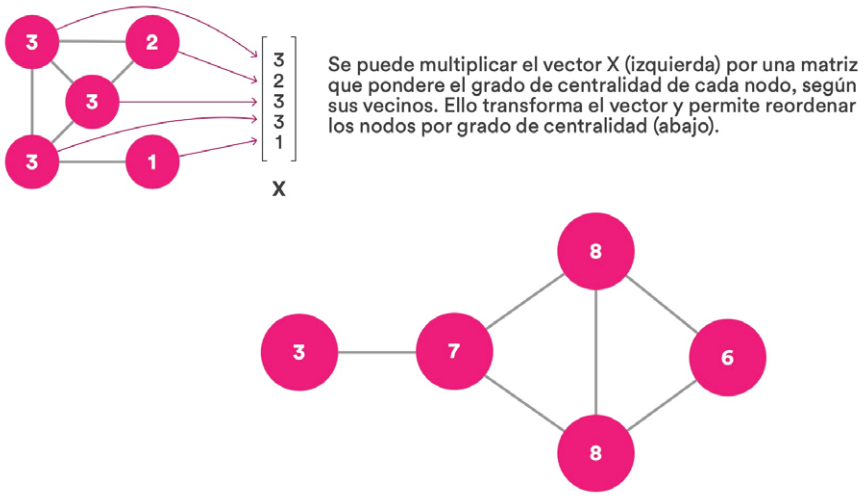
Para llegar a dichos hallazgos, OCÉANO construye conjuntos de nodos o mallas, de modo que el sistema es capaz de detectar con un dato identificador con qué contratos y entidades contratantes está conectado dicho dato, de modo que forma mallas o redes[61]. De acuerdo con la administración de OCÉANO, la **malla más grande** que se ha descubierto suma unos USD 31 mil millones, distribuidos en 208 000 contratos en una red de 19 000 integrantes. El análisis de esta información le ha permitido a la CGR denunciar casos en donde se adjudican contratos de modo presuntamente irregular.

El desarrollo de OCÉANO se basa en la combinación de análisis matricial de redes y construcción de vectores para predecir riesgos de corrupción en la contratación pública en tiempo real (ver figura 3.5). Una vez alimentado el sistema con los datos debidamente estructurados y depurados, cada uno de estos hace las veces de un nodo potencial que la plataforma analiza posteriormente, cuantificando sus repeticiones (esto es, conexiones) en otros contratos. Combinando los datos del número de enlaces que posee un nodo y la distancia entre nodos, se construye un Eigenvector[62], que sirve para progra-

[61] Estos grandes conjuntos de datos pueden emplearse para la construcción de algoritmos básicos de aprendizaje, a través de los cuales se establecen relaciones entre datos para predecir riesgos o alertas de corrupción.
[62] Un Eigenvector es el vector que, multiplicado por una matriz cuadrada, arroja el mismo vector multiplicado por un escalar (el Eigenvalor). Esto tiene un poder inmenso en ciencia de datos: si se conoce un Eigenvector para una transformación lineal de datos, se pueden calcular (predecir) vectores para arreglos de datos diferentes que guardan la misma proporción (el mismo Eigenvalor). Ver Simon y Blume (1994).

mar los algoritmos de intermediación y construir una red o malla de contratación con el Estado, expandiendo el grado de intermediación de un nodo, desde el más directo (cero intermediarios) hasta los más mediados. De esa construcción, resultarán por defecto unos nodos sobresalientes, al ser considerados intermediarios muy frecuentes por el algoritmo, y se considerarán como «de alto riesgo». Esa información se visualiza y constituye el punto de partida de la CGR para generar alertas tempranas en materia de contratación pública.

Figura 3.6. Red de transacciones criminales visualizadas a partir de datos tabulares



Fuente: Cetina (2020a).

En 2021, la Unidad de información de la Dirección de Información, Análisis y Reacción Inmediata (DIARI) de la CGR gestionó la conexión de **7 411** fuentes de información correspondiente a 878 entidades conectadas con el objetivo de consolidar insumos para los modelos de analítica. Durante el mismo año, se emitieron 758 alertas de riesgo, cuyo valor asciende a **USD 8 750 millones**. Por su parte, la Unidad de Reacción inmediata presentó los beneficios del control preventivo y concomitante, procesos que permitieron salvaguardar más de **USD 375 millones de pesos** en 28 proyectos que se terminaron, y activar 169 proyectos cuya inversión rodea los USD 1 850 millones.

Las herramientas digitales que usa la DIARI actualmente establecen relaciones entre los contratos celebrados a nivel nacional y los evalúa, para detectar posibles casos de corrupción, a través de un análisis matricial de redes y construcción de vectores. Esto ha permitido detectar irregularidades en la contratación que son prevenidas, controladas y sancionadas, como en los ejemplos descritos a continuación:

- Detección de “mallas de contratación”: nodos donde se encuentran personas naturales o jurídicas que controlan la contratación con el Estado en una o más regiones y en uno o más sectores, sin contar necesariamente con la idoneidad o experiencia requerida para suscribir contratos con el Estado.

- El uso de registros mercantiles pertenecientes a personas fallecidas para contratar con el Estado.

- La adjudicación de contratos a compañías ya sancionadas o que, habiéndolo sido, usan otros vehículos corporativos para arroparse en ellos y volver a contratar con el Estado.

- Indicadores o coeficientes de concentración en la contratación pública.

3.3.3. Inteligencia artificial y análisis de redes sociales

La inteligencia artificial, a través del desarrollo de algoritmos, permite que las computadoras analicen datos, aprendan de ellos, detecten patrones y, a partir de estos, pronostiquen cambios o sucesos antes de su ocurrencia. De este modo, por ejemplo, estiman la probabilidad de que un fenómeno de corrupción ocurra con base en unos riesgos preidentificados en un determinado procedimiento. Una vez estos son evidenciados, se generan alertas automáticas. Así, todos los interesados pueden realizar el seguimiento y corroborar o desmentir la existencia del riesgo detectado. Lo anterior posibilita un trabajo colaborativo para mitigar o denunciar riesgos de corrupción, así como un mayor control social e interacción del sector privado y los ciudadanos sobre el gasto público.

En Brasil, organismos de la sociedad civil crearon un robot de inteligencia artificial para analizar las declaraciones de gastos de los congresistas. Rosie es una innovación digital en código abierto que empodera a la sociedad civil que demanda transparencia y rendición de cuentas. Gracias a una campaña de financiamiento colectivo (o *crowdfunding*), la Operación Serenata de Amor pudo crear en 2017 a Rosie, un robot que utiliza inteligencia artificial para analizar los datos declarados por los parlamentarios e identificar gastos específicos sospechosos, por ejemplo, comprobantes de pago que indiquen que un senador estuvo en un mismo día y hora en dos lugares diferentes (Cordova y Gonçalves, 2019). Mensualmente, el Congreso recibe más de 200 000 solicitudes de reembolsos que se procesan, en gran medida, de manera manual, pero que dejaban registros en las bases de datos abiertas con las copias de los recibos utilizados para solicitar los reembolsos.

Los creadores de Rosie estudiaron las normas legales sobre desembolsos y las convirtieron en código software. Luego, analizaron las posibles formas de evadir las reglamentaciones y determinaron el registro que dejaría esa irregularidad en los datos existentes. En el momento en que **Rosie** identifica un gasto sospechoso, genera un *tweet* en un tono neutral para que los congresistas y ciudadanos contradigan o confirmen la información reportada. **Jarbas** es una plataforma que acompaña a Rosie y permite a los ciudadanos consultar y verificar la información que llega a Twitter.

Figura 3.7. Rosie

A finales de 2021, Rosie y Jarbas han permitido detectar más de **8 000 solicitudes de desembolso por un valor aproximado de USD 680 000**. Desde que comenzaron a operar, se estima que los gastos de los miembros del Congreso se han reducido en un 10 % (Cordova y Gonçalves, 2019).

3.3.4. Análisis de redes sociales y minería de datos

Las redes sociales generan, proporcionan y permiten compartir datos que juegan un papel importante en la lucha contra la corrupción. A través de la minería de datos, pueden descubrirse patrones o relaciones, en especial al cruzar varias fuentes de datos como transacciones electrónicas, registros bancarios, reportes de los empleadores, registros de compra de vehículos y publicaciones realizadas en redes sociales, entre otras.

Un caso famoso que ilustra este tipo de análisis ocurrió en Colombia, cuando **la joven hija de un funcionario de aduanas** publicaba en sus redes sociales unos patrones de consumo que no correspondían con el nivel de ingresos de su padre ni con la vida universitaria que aparentemente llevaba. El funcionario en cuestión fue hallado culpable por cobrar multimillonarios sobornos para permitir la operación de una red de contrabando en el puerto comercial de Buenaventura.

El caso colombiano fue producto del trabajo humano en el análisis de información dentro de internet y el cruce de diferentes fuentes. Pero esta labor puede automatizarse: la Administración de Hacienda y Aduanas del Reino Unido (HMRC[63], por sus siglas en inglés), mediante su sistema **Connect**, utiliza el análisis de redes sociales y la minería de datos que cruzan los registros tributarios de empresas y personas para descubrir actividades fraudulentas o no divulgadas.

Connect filtra grandes cantidades de datos para detectar redes de relaciones, con el fin de recuperar millones de libras que pierde el fisco como consecuencia de actividades económicas no declaradas (Houlder, 2017). Su algoritmo predictivo identifica a las personas con mayor riesgo de cometer fraude fiscal y ayuda a diseñar acciones preventivas a través de empujones o *nudges* comportamentales (Santiso, 2019). HMRC, por ejemplo, descubrió evasores fiscales luego de que aparecieran en un episodio de un programa de televisión gastando miles de libras de ingresos no declarados en lujosas bodas familiares; igualmente, los investigadores revisaron sus cuentas de Facebook, LinkedIn y Twitter.

3.3.5. *Machine learning* y análisis textual de auditoría

El *Analisador de Licitações, Contratos e Editais* (ALICE) es una herramienta desarrollada en 2017 por la Contraloría General de la Unión (CGU), de Brasil, para el análisis de los documentos de contratación y compra pública brasileños. ALICE toma la información del sistema de compra pública del país (Comprasnet, a cargo del Ministerio de Economía), baja los textos de los documentos del proceso contractual y genera un reporte de alertas tempranas por la valoración del riesgo que hace de los procesos de contratación.

La cantidad de información producida es de gran tamaño, y la CGU enfrenta muchos retos para ajustar el control a la velocidad con que se materializa el gasto público con cada nuevo contrato. De acuerdo con la entidad, se publican, en promedio, 250 edictos diarios en **Comprasnet,** y, en los dos últimos años, se gestionaron a través de esa plataforma más de 234 000 licitaciones por un monto superior a USD 22 000 millones. La CGU optó por generar un sistema de valoración de riesgos basado en una aplicación de *machine learning* llamada análisis textual.

ALICE toma el texto de los documentos colgados en la página web de **Comprasnet**. Los modelos de clasificación de texto funcionan asignando categorías a los datos, de acuerdo con su contenido: detecta tópicos o temáticas,

[63] Acrónimo para Hacienda del Reino Unido: Her Majesty's Revenue and Customs.

identifica las palabras clave y nombres (bien sean compradores o proveedores), entre otros datos, para determinar el perfil del contrato. Seguidamente, detecta combinaciones de palabras que pueden hacer un contrato más riesgoso o que merezca mayor atención por su cuantía, objeto, entidad contratante o plazos.

Diariamente, se seleccionan los contratos que contienen un texto que ALICE considera estratégico para la CGU. Luego de ello, se activa un sistema automático de envío de correos electrónicos a los auditores, informándoles sobre los de mayor interés para su análisis. Adicionalmente, las listas diarias y datos identificadores se almacenan en una base de datos centralizada. Entre 2018 y 2019, ALICE analizó contratos por cerca de USD 900 millones, de los cuales la CGU revocó unos USD 600 millones gracias a la plataforma[64].

La CGU ha desarrollado un concepto de **auditoría preventiva sobre contratos**, que se apoya en inteligencia artificial y reduce los tiempos y pasos para agotar los procesos desarrollados por los auditores. Con los reportes enviados por ALICE, estos deciden con base en factores de riesgo de su propio conocimiento cuáles licitaciones deben examinar. Cada auditor se reúne con las entidades para valorar y validar los riesgos identificados, y elabora y presenta un informe preliminar, al cual la entidad responde documentando sus acciones para mitigar los riesgos de corrupción. La respuesta es seguidamente monitoreada por la CGU. Según información suministrada por la entidad, este enfoque permitió corregir el curso de contratos por más de USD 1 000 millones entre 2018 y 2019.

3.3.6. Inteligencia artificial y sociedad civil

En 2016, Ucrania lanzó la plataforma de compras públicas electrónica ProZorro, como producto de un proceso colaborativo entre Gobierno y sociedad civil. ProZorro es un sistema electrónico híbrido basado en un modelo de código abierto, lo cual permite la colaboración entre la base de datos central y un número infinito de mercados comerciales que brindan el acceso frontal.

La plataforma permite acceder a todos los datos del proceso de contratación y tiene un módulo de análisis en línea. **Ello ha permitido reducir los cuellos de botella por corrupción y representó ahorros alrededor de USD 2,5 mil millones para la economía nacional entre 2016 y 2019 (OCDE, 2019)**. La rápida transformación digital y las mejoras introducidas aportaron transparencia e hicieron accesible para cualquier usuario la información pública sobre los contratos públicos (operación que representa el 15 % del PIB del país). Dado

[64] Información suministrada por la CGU.

el volumen (4 500 licitaciones por día), se requirió una estrecha supervisión para garantizar el cumplimiento, el acceso equitativo al mercado y los principios de libres competencia y concurrencia. En Ucrania, el Servicio Nacional de Auditoría realiza una revisión de los contratos con sustento en una lista cerrada de 35 indicadores de riesgo (Transparencia Internacional, 2018).

Sin embargo, no todas las iniciativas en materia de uso de datos para los programas anticorrupción provienen de las autoridades. Con el apoyo de Transparencia Internacional, la comunidad y 25 organizaciones de la sociedad civil (OSC) aprovecharon los datos abiertos disponibles en ProZorro para desarrollar un sistema de monitoreo a la contratación pública llamado **DoZorro**. Inicialmente, se realizó un trabajo para identificar los riesgos por parte de las OSC, que evolucionó hasta DoZorro, una plataforma que emplea *supervised learning* e inteligencia artificial (AI) para evaluar la probabilidad de riesgos de corrupción en los procesos contractuales (Transparencia Internacional Ucrania, 2017).

Debido a que las organizaciones y funcionarios corruptos se adaptan y reorganizan para ocultar sus actividades, DoZorro no utiliza fórmulas ni riesgos definidos, sino que se ajusta automáticamente. El sistema evalúa la probabilidad de riesgos de corrupción en las licitaciones de forma independiente, y luego los envía a las organizaciones de la sociedad civil de la comunidad DoZorro. Los hallazgos de los activistas se registran y, si las sospechas son correctas, el software recuerda su elección; si estaban equivocadas, las olvida (Transparencia Internacional, 2018). Así, a través de inteligencia artificial, el sistema mismo revalúa su modelo y recalcula los pesos de los indicadores para aumentar la precisión de la identificación de nuevas licitaciones riesgosas, volviéndose cada vez más preciso en la detección de señales de corrupción (Kucherenko, 2019).

Adicionalmente, la plataforma en línea permite a los proponentes dejar comentarios estructurados sobre la oferta, el comprador, otro postor, etc., y la parte a la que se dirige la queja debe documentar las actuaciones en caso de que haya violaciones al régimen de contratación. Si no se produce una reacción, el caso podría remitirse a uno de los expertos para su investigación. Si se valida la violación, se presenta la apelación a los organismos de control. El demandante también tiene la oportunidad de calificar la calidad de las respuestas del 1 al 5, y las ofertas en las que no hubo respuesta a la queja o donde la tasa de satisfacción fue inferior a 3 se marcan como riesgosas y se destacan en la plataforma. Esas licitaciones tienen prioridad para la revisión por parte de las organizaciones de la sociedad civil que supervisan las adquisiciones[65]. En 2020, DoZorro había descubierto irregularidades en 30 000 licitaciones por un valor estimado de USD 4 mil millones (ODP, 2020).

[65] Ver https://oecd-opsi.org/innovations/dozorro/. La página oficial de DoZorro está en cirílico.

3.3. Reflexiones finales y recomendaciones

Apoyar a los Estados para construir una agenda de uso de datos y tecnologías digitales como herramienta de prevención e investigación de la corrupción es una prioridad para la Dirección de Innovación Digital del Estado (DIDE) de CAF, creada en 2018. Esta tarea tiene dos niveles de intervención:

1. el primero busca asegurar la existencia y calidad de datos que tienen potencial para ser procesados por la ciencia de datos con fines de lucha contra la corrupción (ver capítulo 1), y
2. en el segundo, el objetivo es brindar asistencia técnica a los países para desarrollar plataformas que hagan un uso inteligente de la ciencia de datos con el fin de prevenir, detectar e investigar hechos de corrupción.

Esto permite que los Gobiernos pasen de un rol reactivo a otro proactivo y predictivo (esto es, inteligente) en la toma de decisiones y ejecución de programas y políticas para luchar contra la corrupción.

El éxito y la sostenibilidad de un enfoque de política pública, donde las tecnologías de datos se adoptan como dispositivo en la lucha contra la corrupción, requieren que los países adelanten una ambiciosa agenda digital anticorrupción que tenga en cuenta los siguientes aspectos:

- **En la era digital, la cadena de valor se agrupa hacia grandes conjuntos de datos. Los Gobiernos deben asegurar la infraestructura que les permita facilitar ese agrupamiento,** bien sea en lagos o en almacenes de datos, de modo que la reutilización de los mismos no se enfrente a barreras de acceso de tipo legal u operacional.

- De lo anterior, se entiende que **es importante que los Gobiernos inviertan en generar poder de computación para entrenar los algoritmos que usen los datos en la prevención del fraude** dentro de un sinnúmero de operaciones y transacciones que requieren sus recursos, como pagos de seguridad social, otorgamiento de licencias, entrega de subsidios y recaudo de impuestos, entre otras tareas.

- **Los Gobiernos pueden aprovechar el fenómeno de «gravedad de los datos»[66] para mejorar la toma de decisiones anticorrupción**. También,

[66] Concepto acuñado por el ingeniero Dave McCrory, quien señala que los «datos atraen más datos». Ver: https://datagravitas.com/

en materia de reformas institucionales, debido a la evidencia disponible y organizada que deja la infraestructura de datos. En el contexto actual, a medida que los conjuntos de datos se hacen mayores, se vuelven más difíciles de mover, por lo que resulta más barato dejar que los datos permanezcan en ciertos lugares.

La aplicación de estándares y prácticas internacionales para la producción, publicación y reutilización de los datos es una alternativa costo-efectiva para las estrategias anticorrupción.

- **La aplicación de estándares y prácticas internacionales para la producción, publicación y reutilización de los datos es una alternativa costo-efectiva para las estrategias anticorrupción.** Por ejemplo, la adopción del Programa Interamericano de Datos Abiertos (PIDA) ya cuenta con una serie de recomendaciones y medidas para producir y poner a disposición del público 30 conjuntos de datos que pueden ser usados en la lucha contra la corrupción.

- Se deben ajustar los marcos legales e institucionales para crear un entorno favorable que permita a las políticas de integridad apalancar tecnologías digitales y generar resultados.

  - **América Latina sigue necesitando reformas para mitigar la corrupción, la mayoría relacionadas con el Compromiso de Lima de 2018.** Es necesario hacer ajustes institucionales, como regular el conflicto de interés y facilitar el acceso a la información en la materia. La regulación del *lobbying* o cabildeo es otro aspecto pendiente puesto que, en consonancia con las buenas prácticas, ayudaría llevar registros formales y de público acceso de los cabilderos. Implementar registros unificados de beneficiarios finales mejoraría la efectividad de los mecanismos antilavado de dinero, así como de las convenciones antisoborno (ver capítulo 6).
  - **Los Gobiernos deben asegurar coordinación y ambientes colaborativos para que las estrategias anticorrupción basadas en datos funcionen.** Los diferentes departamentos o agencias pueden tener reservas frente a compartir los datos o cambiar el modo en que los gestionan, tal vez porque interpretan esas tareas como una renuncia a las competencias o al poder que les conceden la constitución y la ley en cada país. Esto ha dificultado que los Gobiernos consoliden una estrategia de datos anticorrupción coherente.

Finalmente, es importante recalcar que la agenda de integridad será determinante para la recuperación económica, como parte esencial de los programas de reactivación. Reducir los riesgos de corrupción contribuye a que el gasto de los Gobiernos se traduzca en una provisión efectiva de bienes públicos, los cuales no solo habilitan los mercados, sino que favorecen a los económicamente más vulnerables. En este sentido, la transformación digital de los Gobiernos es un componente necesario, más que complementario, para construir una agenda digital de integridad pública.

Recuadro 3.2.

Ciencia de datos para identificar riesgos de corrupción

En 2021, CAF, en asocio con la Red Interamericana de Compras Gubernamentales (**RICG**), lanzó la primera «**Guía para la identificación de riesgos de corrupción en contratación pública, utilizando la ciencia de datos**».

Se trata de un instrumento diseñado para que las agencias de compra pública interesadas en aprovechar las tecnologías digitales puedan reutilizar los conjuntos de datos que administran para contar con sistemas inteligentes de alerta que adviertan sobre irregularidades en los procesos de contratación y compras. Para ello, la guía desarrolla tres aspectos:

- Arquitectura institucional necesaria para que las unidades dentro de las agencias de compra pública incorporen diferentes conjuntos de datos como insumo para la toma de decisiones en materia de gestión de riesgos contractuales, monitoreo, evaluación, innovaciones, análisis y verificación.

- Flujos de información necesarios para que las fuentes de datos de las compras públicas se complementen con otras plataformas de datos abiertos, que se pueden asociar con las diferentes fases y variables de la contratación pública. Identificar los flujos de información y combinación de datos, facilita la identificación de anomalías en la compra pública.

- Identificación de alertas tempranas, banderas rojas y priorización de riesgos, con una breve hoja de ruta para crear un sistema de alertas tempranas con bases de datos, banderas rojas, algoritmos de agregación de indicadores, interfaz para la visualización de riesgos, y análisis y verificación de la información.

En Bogotá, se busca garantizar transparencia y rendición de cuentas en proyectos valorados en USD 7,3 billones, como la construcción de la primera línea de metro de la ciudad, hospitales, tratamiento de aguas residuales y malla vial (Iniciativa de Transparencia en Infraestructura, 2021).

Fuente: Elaboración propia.

4.

Blockchain y algunas aplicaciones en integridad pública

“

Una vez que la duda surge,
se extiende rápidamente”.

J. M. Keynes, Teoría general del empleo, el interés y el dinero

Blockchain y algunas aplicaciones en integridad pública

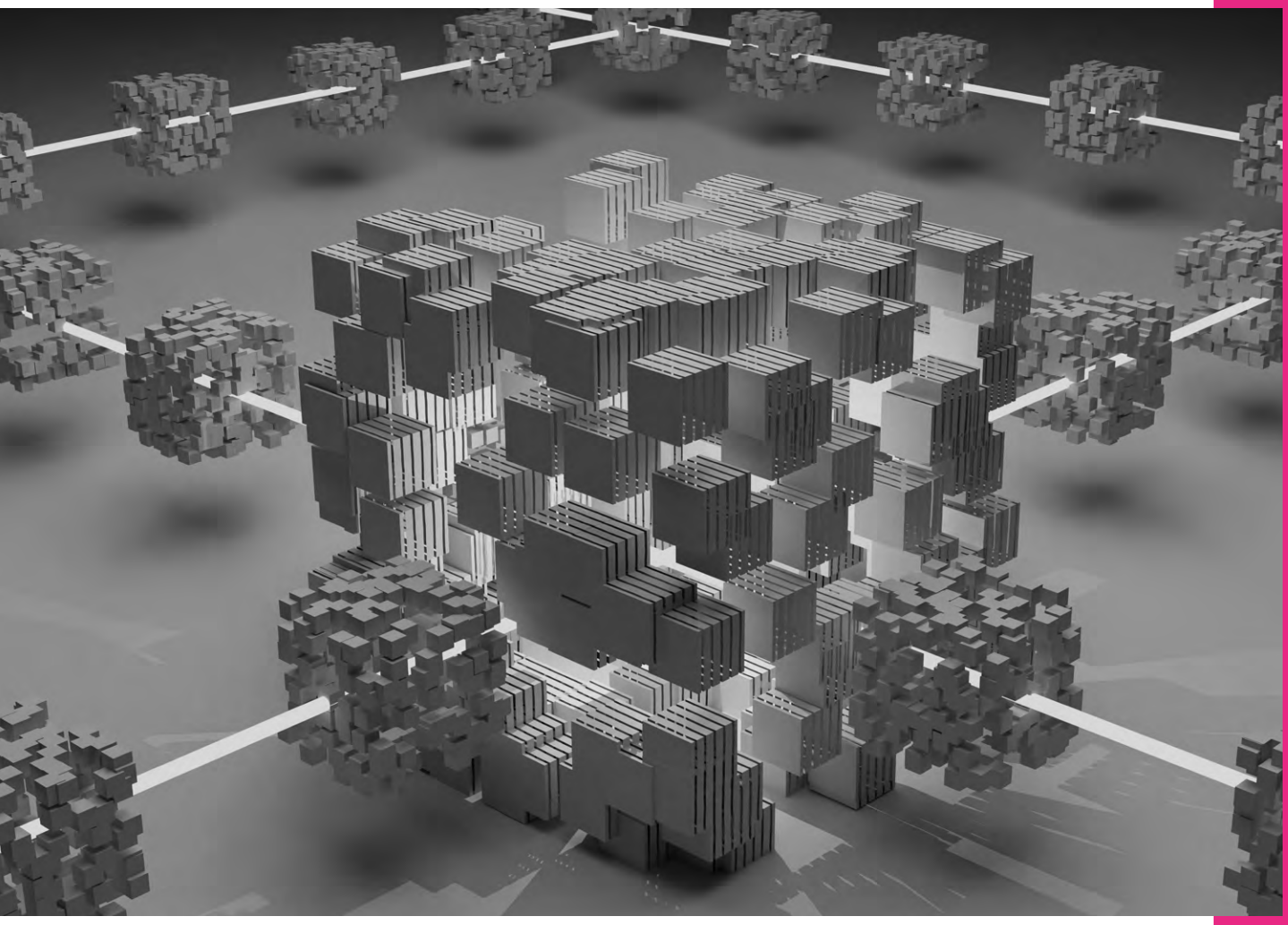
La falsificación es una práctica tan antigua como la escritura y el papel. Durante siglos, ha sido suficiente con alterar fechas, firmas u otros caracteres para modificar indebidamente registros, transfiriendo así derechos, bienes u obligaciones de modo ilícito. Curiosamente, la falsificación en la era digital –que no requiere del papel–, sigue siendo un problema. La perspectiva de un mundo en el que todos los datos de texto, audio, imágenes y video estén en formato digital en medios fácilmente modificables plantea la cuestión de cómo asegurar la integridad de estos registros; es decir, certificar cuándo y quién creó o modificó por última vez un documento, dato o archivo de manera abierta y verificable.

En un mundo basado en documentos físicos, se acudió al sello del medio documental o a la autenticación por autoridades notariales. En el ámbito digital, el problema está en sellar los datos, no el medio. Para resolver esto, Stuart Habert y Scott Stornetta (**1991**) desarrollaron procedimientos computacionalmente prácticos para el sellado de tiempo digital de los documentos, de modo que no fuera factible para un usuario deshacer o reenviar su documento, incluso con la colusión de un servicio de sellado. La técnica se basaba en una cadena de bloques de información, asegurada criptográficamente: el *blockchain*.

El uso del dinero en la era digital y las transacciones financieras digitales explican el origen de otra gran característica del blockchain: la imposibilidad de crear copias. La información como textos, video, imágenes y otros

puede existir en muchos lugares al mismo tiempo. Pero el dinero, entendido como registros en manos de una entidad, únicamente puede, en su formato de información, *existir una sola vez en un solo lugar*. Para que eso sea posible en el mundo digital, es indispensable asegurar que no existe una copia del mismo registro de dinero o que no se movilizan copias de este. En tal sentido, entidades como los bancos comerciales o centrales tienen la potestad casi exclusiva de garantizar que el dinero, como pieza de información, no pueda ser copiada, alterada ni duplicada.

Por contraste, *blockchain* se está utilizando como un «internet del dinero», que promete a sus usuarios la posibilidad de transar directamente entre ellos sin intermediación alguna (ver capítulo 5), es decir, **sin pedir licencia a un tercero para ocupar espacios o registros.** Algo similar sucede con el modelo de **identidad digital descentralizada**, que se contrapone al modo en que actualmente funciona la identidad digital (ver capítulo 5). Hoy en día, es normal que un usuario de cualquier servicio digital tenga múltiples identidades, que crea y mantiene para consumir diferentes aplicaciones. Esto genera enormes volúmenes de datos de usuarios con los proveedores de servicios, lo que ha



llevado a dos problemas: por un lado, los datos privados se guardan y se dejan a la discreción de las aplicaciones que el usuario utiliza; por otro, y como consecuencia del primer problema, la propiedad de los datos de este ya no es suya. La identidad digital descentralizada, por contraste, se fundamenta en la idea de que tal identidad pertenece a cada ciudadano y, por lo tanto, es este quien debe decidir a quién o dónde dar acceso a sus datos a través de credenciales verificables[67] que lleva en su dispositivo móvil y que se aseguran mediante la cadena de bloques.

El blockchain también ofrece una serie de propiedades que podrían ayudar a prevenir fenómenos de corrupción y recuperar la confianza de los ciudadanos en los Gobiernos. Aunque no existen evaluaciones que determinen de modo sistemático su efectividad en la reducción de la corrupción, hay casos de uso que están mostrando el potencial de dicha tecnología. Por ejemplo, Aliyev y Safarov (2019) identificaron casos de uso de *blockchain* para mejorar el sistema actual, a fin de **identificar casos de corrupción y brindar mayor transparencia en algunos procesos de los Gobiernos**.

Este capítulo explora el funcionamiento de la tecnología blockchain o cadena de bloques y su potencial uso en el control de la corrupción a partir de casos específicos que se han desarrollado, en su mayoría, como prueba de concepto. Dichas experiencias sirven de referencia para que los Gobiernos identifiquen en qué procesos puede el *blockchain* incluirse como herramienta de integridad. Es importante resaltar que esta innovación es relativamente nueva, y su impacto o efectividad en materia de prevención o reducción de fenómenos de corrupción aún necesita evidencia estadística. En este sentido, el capítulo se estructura así:

- Primero, se desarrollarán los conceptos básicos para entender el funcionamiento del *blockchain* y algunas características que se asocian con la transparencia y confianza en las actuaciones de las entidades gubernamentales.

- Segundo, se presentarán experiencias prácticas de la implementación de la tecnología de cadena de bloques en la lucha contra la corrupción.

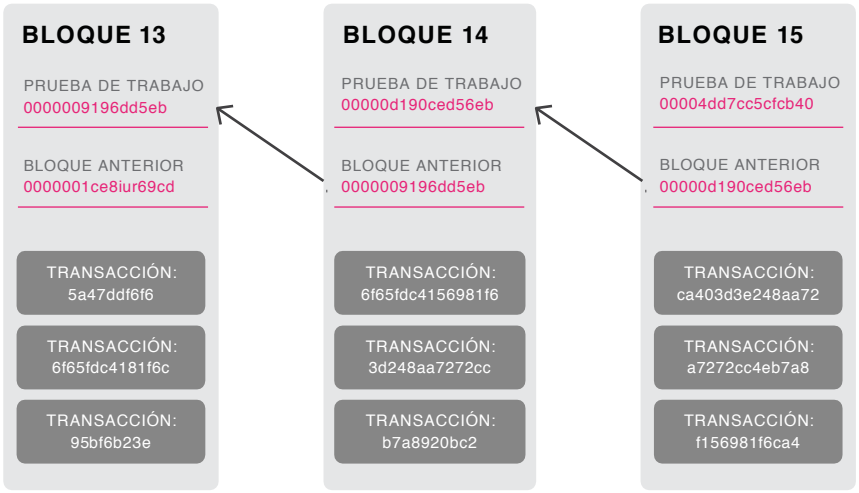
- Finalmente, se propone una serie de recomendaciones para los Gobiernos que tengan la intención de implementar esta innovación digital como herramienta de integridad.

[67] La identidad descentralizada funciona de modo que, al crear una cuenta, sea esta laboral, académica, etc., el usuario obtiene una credencial asociada a un conjunto de sus datos personales y que se inserta en blockchain. Los desarrolladores de este servicio le permiten al usuario escanear un ID y registrar una fotografía suya, para generar las credenciales verificables que luego utilizará con el fin de demostrar su identidad frente a distintas plataformas e instituciones.

4.1. Conceptos fundamentales del *blockchain*

Blockchain, **cadena de bloques o firmas digitales de información, es una tecnología de contabilidad distribuida (distributed ledger) que permite registrar transacciones en bloques.** Cada uno de estos contiene información de transacciones o bloques anteriores, creando una cadena en la que toda transacción cuenta con una pista de auditoría inmutable (ver gráfico 4.1) y es validada por todos los interesados o «nodos» de modo descentralizado en tiempo real (ver gráfico 4.2). Esta técnica se sustenta en un registro público distribuido, que siempre mantiene una lista creciente de registros o transacciones, reunidos en bloques, que son seguros contra cualquier revisión o adulteración, y completamente rastreables (CIAT, 2018).

Gráfico 4.1. Ilustración del registro de transacciones en *blockchain*



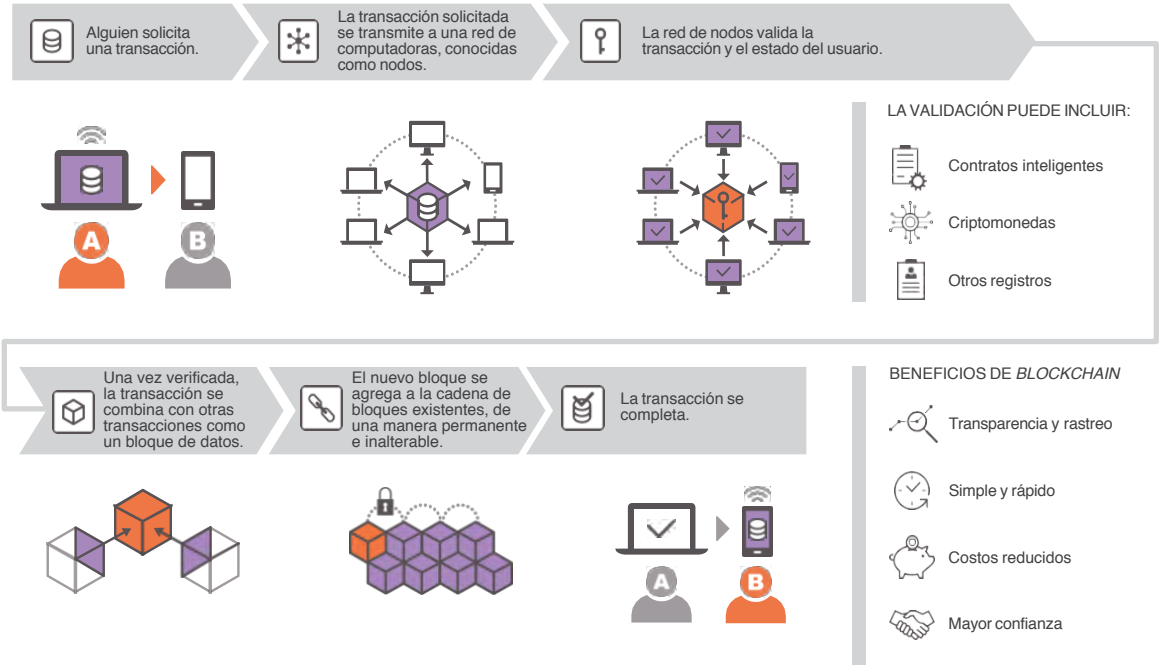
Fuente: English, M.D., Auer, S., y Domingue, J. (2015).

Un modo de entender el mecanismo que permite el funcionamiento descentralizado del *blockchain* es imaginar un documento de Google que no requiera cuentas o espacios de Google de por medio para modificar archivos, y en el cual cada modificación obedezca a ciertos parámetros que miles de usuarios validen. Aplicar esa lógica al mundo del dinero ha sido posible a través de las criptomonedas. Su desarrollador (una o varias personas), que usa el seudónimo de Satoshi Nakamoto, creó un mecanismo para registrar y

modificar la información como la propiedad de la moneda digital en un registro descentralizado, que está compartido y es accesible por millones de computadores o de miembros de una red.

Dichos registros son inalterables, es decir, no pueden ser borrados ni hackeados, lo que garantiza su inmutabilidad y trazabilidad. De modo que lo que va quedando en el registro del *blockchain* son bloques de modificación de información que todos los miembros de la red validan, en lugar de una entidad central. **Millones de miembros o unidades de computación en una red haciendo ese trabajo** implican una descentralización en el proceso de autenticación de las transacciones, a través de un protocolo de consenso distribuido. De este modo, un registro de *blockchain* va acumulando todas las transacciones hechas y debidamente validadas, las cuales no se pueden alterar ni eliminar. No obstante, existen diferentes clases de *blockchain* (ver tabla 4.1), con características particulares (Aarvik, 2020).

Gráfico 4.2. Ilustración del registro de transacciones en *blockchain*



Fuente: Atencio (2020).

Las transacciones validadas y aseguradas con tecnología *blockchain* funcionan bajo la lógica de un contrato inteligente. Dicho concepto, también conocido como **smart contract**, fue acuñado por Szabo (1996), quien consideró viable traducir las cláusulas contractuales a un lenguaje de programación computacional de carácter vinculante, que reemplazaría los contratos

en papel. Así, los contratos inteligentes son mecanismos de ejecución automática de obligaciones previstas en documentos contractuales, que hacen uso de códigos computacionales y evitan la necesidad de acudir al sistema jurisdiccional para que las obligaciones o prestaciones derivadas del contrato sean cumplidas (Padilla, 2020, p. 178).

La ilustración más sencilla de la utilización de instrumentos tecnológicos para la celebración de contratos es una máquina dispensadora[68] de bebidas que cuesta un dólar. La máquina tiene *almacenada* una regla: si recibe un dólar, debe expulsar la bebida. Cuando esto pasa, la máquina *verifica* que recibió efectivamente un dólar (y no, por ejemplo, un pedazo de papel). Luego de comprobar que se cumple la regla, procede a *ejecutar*: toma el dólar y expulsa la bebida. Los contratos inteligentes son, en realidad, piezas de información que codifican la lógica de los negocios para cumplir con tres tareas fundamentales: almacenar, verificar y autoejecutar reglas. Los contratos inteligentes facilitan así el intercambio de dinero, propiedad, acciones, servicios o cualquier cosa de valor de una manera algorítmicamente automatizada y sin conflictos (**Cong y He,** 2018).

[68] El registro más antiguo de una máquina dispensadora con esa lógica de contrato inteligente data del año 215 a. C. en Egipto, Pneumatika. Allí, los usuarios, al insertar una moneda, activaban una palanca que abría una válvula dispensadora de agua bendita (Raskin, 2017).

Tabla 4.1. Diferentes tipos de *blockchain*

Tipo		Características
Público	**Sin permiso**	La cadena de bloques es pública y cualquier persona puede participar sin permiso. Las criptomonedas como Bitcoin y Ethereum son un ejemplo de esta clase de blockchain. Dado que hay muchos nodos que deben llegar a un acuerdo, exigen gran velocidad de la red (rendimiento de transacciones) y escalabilidad (capacidad para admitir usuarios concurrentes). Algunas críticas se relacionan con el gran consumo de energía que exige su funcionamiento.
	Autorizado	Están abiertas para que todos las lean, pero solo personas autorizadas tienen la capacidad de escribir registros debido a una capa de control de gobierno que se encuentra en la parte superior. Las medidas de seguridad son más simples, las tasas de transacción más altas y el consumo de energía más bajo, ya que operan menos nodos dentro de la red. Como ejemplo, puede mencionarse la información sobre la cadena de suministro de una empresa.
Privado	**Autorizado**	Únicamente los participantes autorizados pueden consultar o acceder a la cadena de información, por lo que se reducen los costos anteriormente mencionados. No necesitan descentralización masiva para asegurar su red porque solo unos pocos tienen permiso para interactuar con el libro mayor, por lo tanto, tienden a ofrecer una mejor velocidad y escalabilidad.
	Controlado	La cadena de bloques es estrictamente supervisada por un nodo central unitario. Es similar a una base de datos centralizada tradicional.

Fuente: Aarvik (2020); **OCDE (s. f.).**

4.2. Aplicaciones de *blockchain* para combatir la corrupción

El valor de la tecnología *blockchain* en la lucha contra la corrupción reside en que sus registros son descentralizados, inalterables y rastreables. La corrupción en el sector público genera desconfianza entre los ciudadanos y las instituciones públicas. La transparencia de las decisiones gubernamentales y los registros públicos abiertos (ver capítulo 1) facilitan el seguimiento a las decisiones públicas, lo cual contribuye a reducir riesgos de corrupción mediante mecanismos de control ciudadano o institucional (ver capítulo 2). La tecnología *blockchain* va un poco más allá: permite que los mencionados registros queden a prueba de manipulaciones, de modo que agentes corruptos no puedan modificarlos, alterarlos o falsificarlos. De acuerdo con Santiso (2019), esto despliega un potencial en ciertos procesos, como la verificación de identidad, el seguimiento a las transferencias de los Gobiernos a los ciudadanos, el registro de la propiedad sobre ciertos activos, y la imparcialidad e integridad en los diferentes pasos dentro de la contratación pública.

La idea que inspira las aplicaciones de la tecnología *blockchain* en materia de integridad es relativamente simple: **la incorruptibilidad del juicio, a menudo difícil de encontrar en seres humanos, se obtiene de modo natural en un intérprete algorítmico que no tiene intereses en las transacciones** (Wood, 2014)[69]. En un sistema centralizado, una única autoridad puede mantener el registro y autorizar la realización de transacciones, como inscribir los títulos de propiedad inmueble, suscribir contratos de compras públicas y emitir dinero, entre otras. En ese sentido, si se pierde la confianza en el nodo central, habría una falla generalizada en el sistema que valida las transacciones (Davis, Lennerfors y Tolstoy, 2021).

La tecnología blockchain hace los registros accesibles, inmutables y seguros, impidiendo a las autoridades centrales actuar con excesiva discrecionalidad y permitiendo a los interesados consultar y validar las transacciones. Por ejemplo, en un proceso de contratación pública –que depende de registros documentando el cumplimiento de requisitos legales–, *blockchain* puede hacer rastreables las alteraciones a documentos como los términos de referencia. También, puede impedir que existan cambios en las licitaciones por fuera de los términos de ley, y garantiza la visibilidad de los procesos para todos los interesados, como proponentes, entidades públicas y sociedad civil.

[69] En particular, la confiabilidad e integridad de esta herramienta depende en gran medida de la calidad del código que subyace a la ejecución de los protocolos de verificación y consenso sobre cada pieza de información que queda en una cadena de bloques.

Dada la existencia de diferentes clases de blockchain, la eficiencia de esta tecnología depende en gran medida de su diseño y el contexto en el que se aplica (Aarvik, 2020). En ese sentido, antes de considerar la implementación de esta tecnología en un proceso determinado, es necesario considerar su adaptabilidad a necesidades específicas en materia de integridad pública (Davis *et al.*, 2021).

Gráfico 4.3. Propiedades principales del registro de transacciones en *blockchain*

Autenticidad y seguridad

Cada transacción genera un bloque de información que cuenta con una identidad única y es complemente rastreable.

Inmutabilidad

La información no puede ser alterada, eliminada, copiada o duplicada. En caso de que un bloque de información sea manipulado, todos los registros de transacción siguientes se ven afectados y se vuelven inválidos.

Contabilidad distribuida

La garantía de autenticidad y control sobre las transacciones no depende de una entidad única o centralizada, sino de todos los usuarios de la red o «nodos».

Privacidad

Las transacciones son privadas y la identidad de las personas naturales o jurídicas no está vinculada a la transacción. Esto no significa que los usuarios sean completamente anónimos, sino que los seudoanonimiza.

Fuente: Elaboración propia.

Las aplicaciones en materia de lucha contra la corrupción han sido identificadas por la OCDE (2018) e incluyen el reclutamiento de talento humano, la votación por medios electrónicos, las rendiciones de cuentas sobre administración de recursos públicos, el manejo de expedientes en decisiones judiciales y la contratación pública, entre las más destacables. Esta sección analiza algunas de estas aplicaciones, incluyendo las desarrolladas como *prueba de concepto*, que sirven como fuente de consulta para Gobiernos interesados en aplicar *blockchain* como dispositivo de integridad.

4.2.1. Asegurando la integridad en las contrataciones públicas con *blockchain*

La licitación pública manejada por medios digitales, como, por ejemplo, los portales electrónicos de contratación y compra públicas, se puede hacer aún más transparente si se utiliza la tecnología blockchain. Para ello, es necesario que la entidad gubernamental contratante publique y administre la licitación, utilizando estas redes para luego hacer uso de «contratos inteligentes» con el fin de que las partes puedan interactuar entre sí; así, una vez programado todo el proceso como contrato inteligente, no puede ser modificado. Por ejemplo, *blockchain* ya se ha usado **en Chile** para certificar las órdenes de compra, con el propósito de lograr trazabilidad en el proceso de licitación o compras del Gobierno.

De modo más específico, aplicar la cadena de bloques a las licitaciones públicas exige, primero, que al ser publicada la licitación, se programe cada paso del proceso en *blockchain*. Esto permite que sus registros sean inmutables e inalterables: tanto los proponentes como los administradores dentro de la licitación siguen dichos pasos bajo la dinámica de contratos inteligentes, es decir, se genera la ejecución automática de reglas u obligaciones derivadas del proceso de contratación.

Aplicar la cadena de bloques a las licitaciones públicas exige, primero, que al ser publicada la licitación, se programe cada paso del proceso en blockchain. Esto permite que sus registros sean inmutables e inalterables.

La tecnología *blockchain* hace los registros accesibles, inmutables y seguros, impidiendo a las autoridades centrales actuar con excesiva discrecionalidad y permitiendo a los interesados consultar y validar las transacciones. Por ejemplo, en contratación pública, puede asegurar la integridad del procedimiento porque todas las transacciones se sellan digitalmente, lo que hace rastreables las alteraciones a documentos como los términos de referencia; también, es posible impedir cambios en las licitaciones por fuera de los términos de ley. Asimismo, se pueden hacer consultas durante el proceso, denunciar irregularidades y solicitar rectificaciones, entre otros, de modo que no es factible seguir adelante con el proceso licitatorio si no se ha dado respuesta a las solicitudes, por ejemplo. Por otra parte, el *blockchain* garantiza la visibilidad de los procesos para todos los interesados o nodos, como proponentes, entidades públicas y sociedad civil. Por consiguiente, para que se materializara un acto corrupto, sería necesario que todos los nodos validaran o aceptaran la transacción.

Aunque no existe evidencia sistemática sobre el impacto de esta tecnología en la reducción de riesgos de corrupción dentro de la contratación pública, sí existen casos de uso que ilustran y suministran alternativas para diseñar una intervención con *blockchain* en estas transacciones. La experiencia del Programa de Alimentación Escolar en Colombia es descrita a continuación debido a que abarcó todo el proceso de compra pública, e ilustra cómo se articulan los conceptos de *blockchain* y contrato inteligente para administrar una licitación pública.

Blockchain en el programa de alimentación escolar (PAE)

En **Colombia**, la **Procuraduría General de la Nación** (PGN) desarrolló una *prueba de concepto* para la **aplicación de la tecnología *blockchain* autorizada** en la contratación del programa de alimentación escolar en la ciudad de Medellín[70]. El *blockchain* mostró aplicabilidad en varios aspectos de la contratación pública. En primer lugar, el mecanismo seudoanonimiza a los proveedores, pero no borra sus actuaciones dentro del proceso licitatorio, lo cual cierra la ventana para que se puedan conocer todos los proponentes y haya acuerdos irregulares entre empresas o entre un proponente y un funcionario para direccionar la licitación. En el momento en que los términos de referencia de la licitación se hacen públicos, no pueden ser alterados. Otro tanto sucede con los comentarios de los ciudadanos, que no pueden ser eliminados y quedan consignados. En ese sentido, las respuestas de la entidad contratante permanecen también registradas en *blockchain*, lo cual las hace inmodificables[71]. El sistema incluso impide avanzar con los siguientes pasos en la licitación si no se responden las preguntas de los diferentes proponentes.

Adicionalmente, las propuestas recibidas por la entidad contratante quedan anónimamente registradas en *blockchain* con los documentos adjuntos cuando los proveedores las envían; no pueden abrirse hasta el inicio del proceso de evaluación que está programado, bajo el modo de un contrato inteligente. De hecho, la entidad pública no conoce de dónde vienen las propuestas antes de comenzar el proceso de evaluación de las mismas. Posteriormente, debe calificarlas todas: el mecanismo de contrato inteligente no le permite avanzar a la fase de adjudicación sin que se califiquen todas las propuestas. Todo ello previene la existencia de acuerdos ilícitos que podrían hacerse con anterioridad para favorecer indebidamente a un oferente. Finalmente, este piloto adoptó una funcionalidad que le permitía a la PGN recibir alertas si existían cambios en los términos de referencia licitatorios, si existían comunicaciones por fuera de los plazos, o si se modificaban los plazos en alguna fase del proceso. Esto le daría la facilidad al organismo de control de actuar en tiempo real sobre el proceso de contratación pública.

El valor agregado de esta tecnología, respecto de cualquier otra, reside en la descentralización, inalterabilidad y posibilidad de rastreo de los registros. En caso de que exista alguna transacción irregular a lo largo del procedimiento de contratación, los registros cuentan con una identidad de autoría inmutable que puede rastrearse. Además, para que una conducta corrupta se materialice, se requiere el consenso de todos los nodos de la red.

[70] El Programa de Alimentación Escolar en Colombia es un mecanismo que fomenta el acceso y la permanencia escolar de los niños, niñas y adolescentes en edad escolar que están registrados en la matrícula oficial, a través del suministro de un complemento alimentario gratuito. El PAE ha sido objeto de redes de corrupción de modo recurrente en Colombia (Roseth et al., 2021), por lo que la PGN ha tratado de adoptar innovaciones digitales para mejorar los controles preventivos (ver capítulo 3).

[71] Es importante aclarar que puede surgir la necesidad de corregir los términos de referencia, puesto que se pueden presentar errores involuntarios. La ventaja del blockchain es que la versión anterior o con errores queda de todos modos grabada en el registro, así como la nueva versión, lo cual permite la trazabilidad absoluta del proceso.

Según el **Foro Económico Mundial, el uso de *blockchain*** en la lucha contra la corrupción en la contratación pública es prometedor, pero también presenta algunas limitaciones importantes. Estas incluyen privacidad y anonimato del proveedor, incertidumbre en cuanto a escalabilidad y acuerdos entre empresas por fuera de la plataforma, entre otros. También, identificó deficiencias regulatorias para el uso de *blockchains* públicos en el caso colombiano.

Contratación pública de emergencia durante la pandemia

Para contener el crecimiento de la pandemia de COVID-19, los Gobiernos de la región tuvieron que adquirir con carácter urgente suministros médicos como máscaras, respiradores, pruebas de contagio y vacunas, entre otros. Dichas erogaciones son particularmente vulnerables a la corrupción (Cetina, 2020), puesto que la rapidez que exige la compra pública de emergencia implica sacrificar principios como la libre competencia, libre concurrencia y selección objetiva en los procesos de compra pública. Sin embargo, la tecnología *blockchain* puede mejorar los niveles de integridad en estas transacciones, como se explica a lo largo de esta sección.

Estados Unidos desplegó soluciones basadas en blockchain en la contratación pública de emergencia para hospitales. Allí existen alrededor de **200 nuevos proveedores** de insumos para atender la pandemia. Satisfacer las necesidades de urgente abastecimiento en el contexto de pandemia era un reto: por una parte, no se podía contratar con los 200 proveedores o una proporción significativa de ellos para asegurar el abastecimiento, y tampoco había tiempo para que las entidades compradoras seleccionaran objetivamente a los más idóneos o competitivos, que respondieran a las necesidades hospitalarias durante los picos de la crisis sanitaria. En ese sentido, los hospitales optaron por adoptar la tecnología *blockchain* para garantizar un mínimo de **calidad y origen idóneos de los equipos médicos**.

En los procesos de adquisición de Estados Unidos, se puso a prueba un mecanismo para facilitar el contacto entre entidades compradoras y proveedores. Los proponentes crean un perfil en el portal de **IBM Rapid Supply Connect**, el cual queda guardado en *blockchain*; adicionalmente, suben datos necesarios para las entidades de Gobierno que adelantan compra pública, como información financiera, certificados de autoridades médicas e identificaciones fiscales. Luego, los hospitales pueden buscar en la cadena de bloques el equipo médico necesario y solicitar información sobre el proveedor, la cual se proporcionará de inmediato, una vez que el proveedor acepte compartirlo.

Las innovaciones del *blockchain* no solo ayudaron a hacer más íntegras las contrataciones, sino que simplificaron los procesos de selección de los contratistas o proveedores a partir de innovaciones como las siguientes:

- **El registro y validación como proveedor se hace una sola vez.** En un proceso de compra pública convencional, el proveedor debe suministrar información actualizada de licencias, posición financiera y dirección de la empresa, entre otros, para cada contratación. Con la tecnología *blockchain*, el proveedor, sencillamente, actualiza cada pieza de información conforme van sucediendo los cambios, y se postula a cada contrato con el Estado, lo cual simplifica el proceso inmensamente. Dado que los cambios permanecen en *blockchain*, todos los miembros de la red validan cada cambio y cada pieza de información, lo cual hace confiable al proveedor.

- Lo anterior, entonces, se convierte en una **identidad digital asegurada** que, para las entidades compradoras o contratantes, resulta muy valiosa, puesto que no tienen que verificar por sí mismas los datos identificadores del proveedor.

- La **idoneidad y experiencia del proveedor** (que generalmente debe acreditarse para ganar puntos y demostrar idoneidad) se registra de modo automático, debido a que cada transacción o contrato de suministro queda consignado y autenticado. Como esta información es inalterable, la entidad compradora no tiene que pedirla, sino, simplemente, consultarla y solicitar un nuevo suministro. Esa solicitud queda asentada igualmente en el *blockchain*. De este modo, todo el récord de abastecimiento es resguardado para cada compañía y cada entidad compradora.

- Todo lo anterior **reduce ventanas de fraude y barreras de entrada a nuevos proveedores**. Las compañías no ven la información y propuestas de otras, de modo que no pueden coludir para subir precios artificialmente. Por otra parte, aunque no necesariamente es competitivo, dado que la emergencia generalmente faculta a contratar de modo directo, el proceso de compra es guiado por un algoritmo de manera automática: la entidad compradora registra su necesidad de abastecimiento, y la plataforma le presenta un grupo de proveedores en capacidad de satisfacerla, de modo que cualquier compañía nueva que entre al registro tendrá ocasión de participar en la cadena de suministro y se reducirá la oportunidad de fijar los contratos por acuerdos indebidos entre funcionarios públicos y proveedores.

4.2.2. Transferencias monetarias

Los programas de transferencias sociales son particularmente vulnerables al fraude, y la tecnología blockchain se despliega para mitigar estos riesgos. La respuesta de emergencia ha consistido en implementar programas de transferencias monetarias (PTM) para quienes perdieron su sustento

económico durante la pandemia. Según la FAO y la CEPAL (2020), al menos 20 millones de personas se ubicaron por debajo de la línea de pobreza debido a la crisis sanitaria. Alrededor de 15 países de América Latina desarrollaron algún PTM con motivo de la pandemia (OCDE, 2020). La crisis consolidó el debate sobre la necesidad de una renta básica universal.

Sin embargo, **estos programas de emergencia son vulnerables a la captura, fraude y corrupción.** En Colombia, la prensa denunció que el programa Ingreso Solidario asignaba recursos a personas ficticias o fallecidas. Argentina presentó un problema similar con el programa Ingreso Familiar de Emergencia (IFE). De acuerdo con la denuncia de un diputado argentino, algunos ciudadanos paraguayos cruzaron la frontera para reclamar de manera irregular el subsidio. En Brasil, el Tribunal de Cuentas de la Unión detectó fraudes en el programa de ayudas de emergencia. Se denunció la entrega de ayudas a personas fallecidas, y otros ciudadanos no son elegibles para recibirlas, lo que podría generar un perjuicio económico de aproximadamente USD 185 millones.

La combinación de los algoritmos que desarrollan contratos inteligentes con aquellos que aseguran la información en blockchain es un elemento que permite reducir considerablemente el margen de discrecionalidad en los responsables de la entrega de dinero en los PTM.

Blockchain tiene un potencial para mitigar estos riesgos y el desvío de recursos en los PTM. Por ejemplo, el Programa Mundial de Alimentos (PMA) desarrolló el proyecto Building Blocks para determinar la viabilidad de incorporar la tecnología en PTM para más de 100 000 refugiados sirios en Jordania. En este caso, el *blockchain* tiene una naturaleza privada autorizada. Los nodos de la red son las organizaciones participantes en la respuesta humanitaria, entidades en busca de un espacio neutral y transparente para colaborar, realizar transacciones y compartir información de forma segura en tiempo real (PMA, 2021). Este desarrollo también representa una solución de identidad digital a refugiados indocumentados. El dinero en efectivo se almacena en una cuenta del beneficiario, cuyo valor y datos son validados por diferentes nodos en la cadena de bloques. Luego, a partir de un contrato inteligente, el efectivo que los beneficiarios reciben o gastan se paga a través de un proveedor de servicios financieros comerciales, y los pagos se almacenan en *blockchain,* integrados con tecnología de autenticación biométrica[72], de modo que el PMA tiene un registro inmutable de cada transacción.

El PMA estimó un ahorro de USD 2,4 millones con el uso del «*blockchain* humanitario», y ha invitado a otras agencias de las Naciones Unidas y actores humanitarios a colaborar en una red *blockchain* neutral para mejorar la cooperación, reducir la fragmentación y reforzar la eficiencia de las intervenciones para el desarrollo.

La combinación de los algoritmos que desarrollan contratos inteligentes con aquellos que aseguran la información en blockchain es un elemento

72 La efectividad de la autenticación biométrica en PTM fue probada por Muralidharan et al. (2016). Para más detalles, el lector puede remitirse al capítulo 2, sección 2.1.5, de este informe. No existen estudios similares que verifiquen la efectividad de una tecnología como el blockchain en PTM para, por ejemplo, reducir los pagos ilícitos o ficticios de las transferencias.

que permite reducir considerablemente el margen de discrecionalidad en los responsables de la entrega de dinero en los PTM. Aunque no existen evaluaciones sistemáticas sobre la efectividad del *blockchain* para reducir desvíos ilícitos de dinero en los PTM, la evidencia disponible sugiere que dicha tecnología puede complementar otras como la autenticación biométrica, cuya efectividad sí ha sido probada (ver capítulo 2, sección 2.1.5). Al requerir de un esquema descentralizado de validación de la identidad del beneficiario, así como de la transferencia o transacción a su favor, se vuelve casi imposible desviar los pagos a personas ficticias, fallecidas o no elegibles. Y aun si eso ocurriera, *blockchain* permitiría hacer la trazabilidad de qué pasó con esos recursos, lo que facilitaría inmensamente el rastreo para la recuperación del dinero.

4.2.3. Integridad en las cadenas de abastecimiento

La vacunación masiva contra el COVID-19 presenta un reto sin precedentes para los Gobiernos de la región, en materia de distribución y administración de las dosis bajo criterios de equidad y focalización. También, exige un balance entre la protección de los datos personales y uso de información personal para rastrear la pandemia y proteger derechos colectivos como la salud pública (Consejo Europeo, 2020). De acuerdo con **UNODC**, también han ido apareciendo fenómenos de corrupción, como la entrada en los mercados de vacunas falsificadas, el robo de estas dentro de los sistemas de distribución, y su administración bajo criterios de **nepotismo o favoritismo** político.

Superar esos retos exige asegurar la integridad en la cadena de abastecimiento de las vacunas, y, en este frente, la tecnología blockchain puede ser de utilidad. En 2019, IBM y la Administración de Alimentos y Medicamen-

tos de los Estados Unidos (FDA, por sus iniciales en inglés), KPMG, MERCK y Walmart diseñaron un **programa piloto** para identificar y rastrear medicamentos recetados y vacunas distribuidas dentro de Estados Unidos mediante el uso de *blockchain*. Para ese año, en este país, **aproximadamente la mitad de la población contaba con una prescripción médica**, lo que generó la necesidad de mejorar la transparencia y confianza en la cadena de suministro de medicamentos a través de enfoques innovadores (FDA, 2020). A fin de abordar los diferentes desafíos de la cadena de suministro farmacéutica, el proyecto piloto integró tecnología *blockchain* para sustituir el proceso de notificación manual fragmentada de retiro de medicamentos, por la generación de un registro común de alertas inmediatas de la recolección de medicinas (Treshock, 2020).

La tecnología blockchain, combinada con una nube híbrida, permite la creación de una cadena de distribución inteligente, en las que las dosis son monitoreadas en tiempo real y se optimiza su asignación. La experiencia del proyecto de distribución de medicamentos es utilizada en Estados Unidos para **verificar la calidad, origen y distribución de las vacunas contra el COVID-19.** Se implementó un *blockchain* de carácter privado autorizado para verificar la calidad, origen y distribución de las vacunas contra el COVID-19[73]. Las características propias del *blockchain* (inmutabilidad y descentralización distribuida) evitan la manipulación y adulteración de los datos sobre el proceso de entrega y administración. De este modo, y gracias a que el registro es accesible por las autoridades, se identifica cualquier potencial riesgo de corrupción en la cadena de suministro de vacunación, y se eliminan «zonas de sombra» en las que se pueden desarrollar actividades ilegales, como el uso del poder político para **evadir los turnos de vacunación por etapas priorizadas**. Al mismo tiempo, se garantiza la confidencialidad de los datos personales (Consejo Europeo, 2020). Lo anterior permite que todos los interesados conozcan y verifiquen en tiempo real la información relacionada con el proceso de vacunación, bajo criterios de seguridad en la información y transparencia en la vacunación.

4.2.4. Integridad en los flujos financieros

La tecnología blockchain también se desplegó para fortalecer la integridad de los flujos financieros. Quienes obtienen activos cometiendo actos de corrupción, generalmente, deben legitimar los ingresos ilícitamente obtenidos a través del proceso de lavado de dinero, con lo cual las ganancias ilícitas terminan movilizándose a través del sistema financiero internacional.

[73] UNODC ha documentado fenómenos de corrupción capaces de afectar los objetivos de salud pública, y sugiere medidas para reducir estos riesgos.

Se implementó un blockchain de carácter privado autorizado para verificar la calidad, origen y distribución de las vacunas contra el COVID-19. Las características propias del *blockchain* (inmutabilidad y descentralización distribuida) evitan la manipulación y adulteración de los datos sobre el proceso de entrega y administración.

Para ello, suelen usarse empresas fantasma que no desarrollan operaciones por sí mismas, pero que aparentan legalidad y movilizan recursos en el sistema financiero sin dar indicios de que son ficticias. Algo similar sucede con los entramados empresariales usados para evadir impuestos, en los que se movilizan flujos de fondos entre empresas fachada para evadir la jurisdicción de las autoridades tributarias.

En ese sentido, las regulaciones destinadas a contrarrestar este tipo de delitos exigen a los intermediarios financieros desarrollar políticas que permitan el conocimiento del cliente (KYC, por su sigla en inglés), así como del origen y del destino de sus recursos (antilavado de activos, AML, por su sigla en inglés). Sin embargo, la evidencia documentada por el **Banco Mundial** sugiere que, en desarrollo de dichas políticas, el sistema financiero termina negando servicios a empresas, a segmentos del mercado, e incluso a países enteros que parecen tener un mayor riesgo reputacional y producir bajas ganancias. Existe una práctica generalizada de reducir el riesgo de integridad negándoles servicios financieros a segmentos considerables de clientes, en lugar de juzgar el peligro con base en la evaluación discrecional de cada sujeto. Según el Banco Mundial, el efecto adverso de estas prácticas recae sobre los más vulnerables, que terminan excluidos de los mercados de crédito y de los flujos de fondos formales.

La tecnología blockchain puede ayudar a mitigar los riesgos que afectan la integridad en las operaciones financieras. Por ejemplo, Santiso (**2018**) señala que la creación de registros mercantiles a prueba de falsificaciones ayudaría a definir a los beneficiarios reales y evitar el lavado de dinero. Ramachandran y Rehermann (2017) muestran cómo dicha tecnología reduce los costos de cumplimiento normativo, mientras aumenta la transparencia de las transacciones.

En particular, blockchain tiene el potencial de reducir los costos de cumplimiento asociados con los requisitos KYC[74]. Por ejemplo, esta tecnología permite que un cliente registre un «bloque» mediante la introducción de la mayoría de los datos propios requeridos para el cumplimiento de KYC y AML, información que luego se codifica y almacena en *blockchain* (Ramachandran y Rehermann, 2017). Los mismos bancos podrían ser los nodos validadores de la información registrada por un cliente, de modo que este deberá ser consistente con todos y no tendrá incentivos por registrar distintas versiones sobre su información (por ejemplo, actividad económica, razón social, empresas controladoras y origen de recursos, entre otros) en diferentes entidades (Niforos, Ramachandran y Rehermann, 2017). Adicionalmente, cada vez que un banco incorpora un nuevo cliente, un representante de dicha entidad financiera podría acceder a la información KYC del usuario sin tener que solicitar la mayor parte y verificar por sí mismo cada nuevo dato. De este modo, la identidad de los clientes va evolucionando en el tiempo, a medida que acumula o

[74] Una encuesta de Thompson Reuters encontró que las actividades KYC cuestan, en promedio, USD 60 millones por año para las instituciones financieras.

transa activos, o cambia de facultades en materia de representación de otras personas naturales o jurídicas.

En cuanto a la prevención del lavado de activos, las potencialidades del blockchain siguen la misma línea de KYC[75], proveyendo una autoridad de certificación descentralizada que puede mantener el mapeo de identidades y transacciones. El potencial impacto positivo de esta innovación tecnológica tiene amplias implicaciones para una serie de servicios financieros, incluida la financiación del comercio o pagos transfronterizos. Un sistema de identidad *blockchain* permitirá a los usuarios finales poseer y controlar su identidad personal, reputación, datos y activos digitales; divulgar de forma segura y selectiva sus datos a las contrapartes; iniciar sesión y acceder a servicios digitales sin utilizar contraseñas; firmar digitalmente reclamos, transacciones y documentos; controlar y enviar valor en una cadena de bloques, e interactuar en el mercado a través de aplicaciones y contratos inteligentes. Todo ello facilitará una supervisión más eficaz por parte de los reguladores financieros, las fuerzas policiales y las administraciones tributarias.

4.2.5. Registros de titulación de tierras

Además de las transacciones gubernamentales, la tecnología blockchain se está usando para fortalecer la integridad de los registros públicos, en particular, los de propiedad de la tierra. Los sistemas de registro de titulación estatal tienen una relación importante con el acceso a crédito formal y mayores valor de la tierra, inversión en tierra e ingresos (Feder y Nishio, 1999). **Sin embargo, en la práctica, los sistemas de registro son ineficientes, lo que genera importantes riesgos de corrupción** (Van Niekerk, 2021). De acuerdo con cifras de **Transparencia Internacional**, el 20 % de los usuarios de servicios de registros de propiedad inmueble afirmó haber pagado un soborno para la realización de un trámite u obtención de información. En otros escenarios, las falencias del propio sistema son empleadas para registrar bienes producto de actividades corruptas.

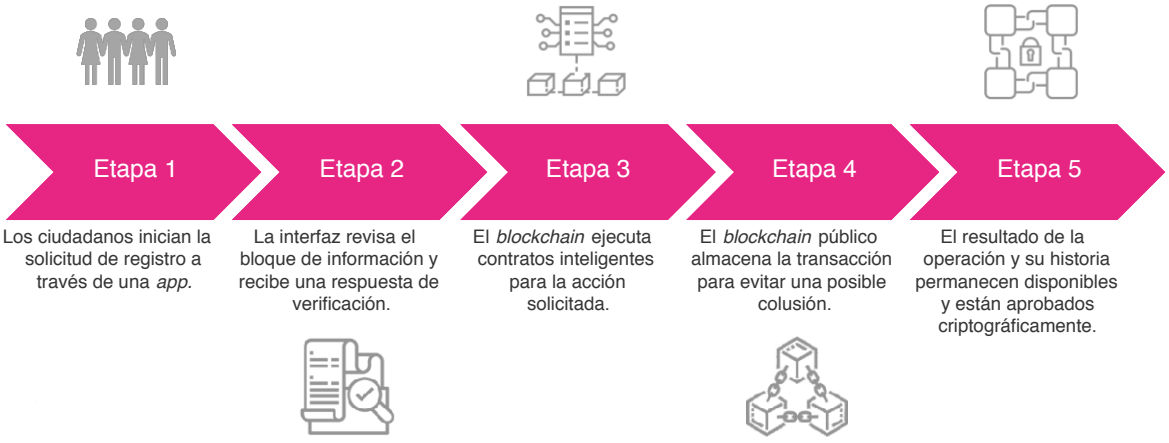
La tecnología blockchain puede optimizar los registros públicos, reduciendo la ineficiencia y aumentando los niveles de transparencia, como los relacionados con la adquisición de bienes inmuebles, permisos, concesiones y certificados. Países como **Brasil**, **Emiratos Árabes** y **Georgia** han apostado a la naturaleza inmutable de las cadenas de bloques y la posibilidad que ofrecen de verificar en tiempo real los derechos de propiedad como una solución para mejorar los sistemas de registro y transferencia de

[75] Una encuesta de Thompson Reuters encontró que las actividades KYC cuestan, en promedio, USD 60 millones por año para las instituciones financieras.

propiedad (Graglia y Mellon, 2018). Recientemente, el **Gobierno de Colombia** anunció el desarrollo de un proyecto piloto para adoptar la tecnología *blockchain* en los procesos de titulación de tierras para prevenir **fenómenos de corrupción** que se evidencian desde el año 2012.

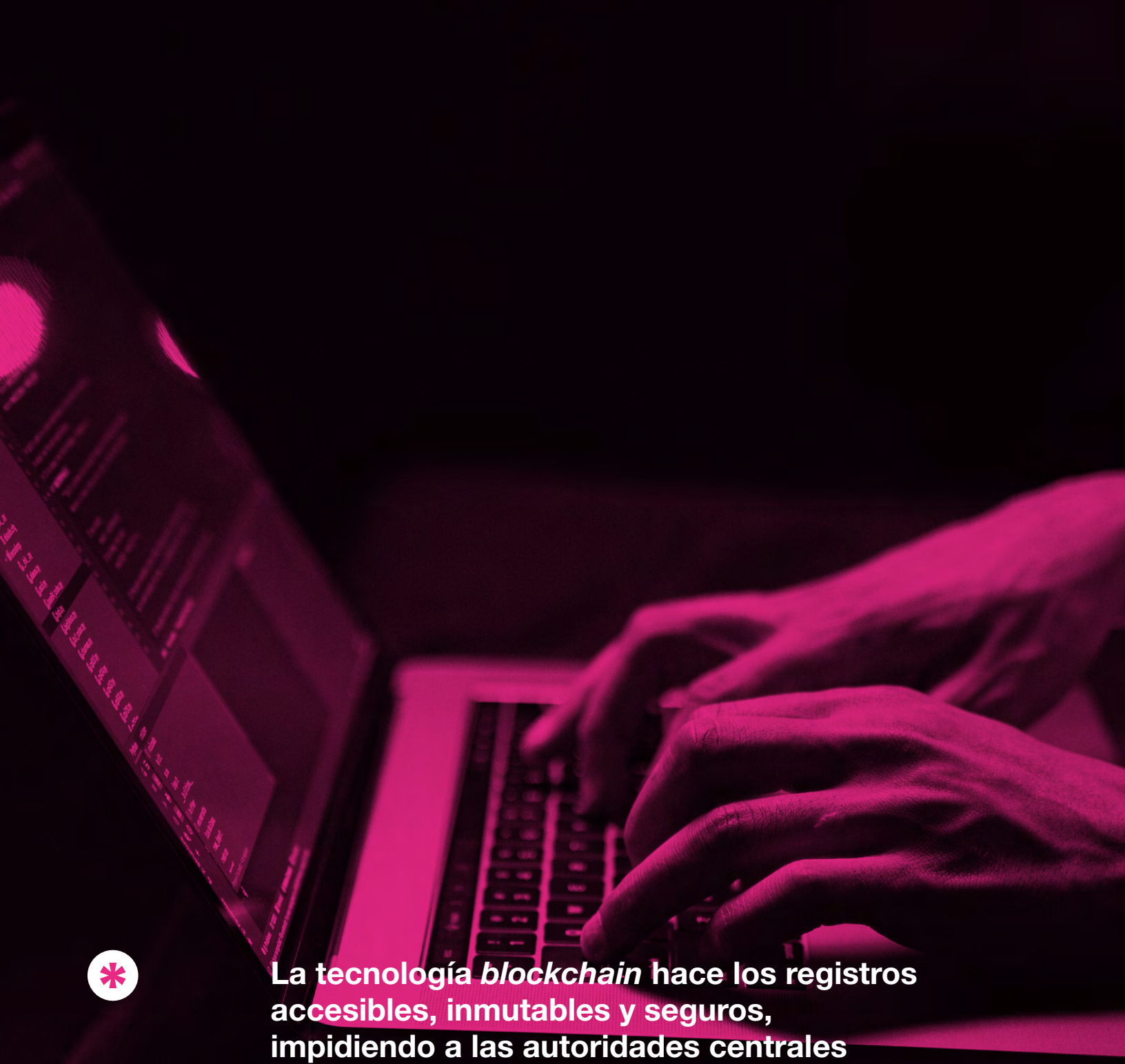
En la República de **Georgia**, encontramos un caso que ilustra cómo funciona el proceso de titulación de tierras basado en *blockchain*. A partir de una colaboración entre su Agencia Nacional de Registros Públicos (ANRP), su Departamento de Tierras del Estado y su Oficina de Inventario, se creó una base digital que contiene el registro de la propiedad, títulos de propiedad y fotografías satelitales de los inmuebles. El sistema logró reducir tanto los costos de registro (a menos del 0,1 % del valor del inmueble), como demoras en el proceso (a un día). Sin embargo, con el fin de resolver por completo la crisis de confianza en las agencias gubernamentales, en 2016, se inició un proyecto piloto para efectuar el registro de tierras o propiedad inmobiliaria a través de *blockchain* público autorizado, con sustento en el registro digital denominado NAPR ya existente, que redujo el tiempo de las transacciones de registro a solo 10 minutos[76]. Todo comienza con la solicitud de registro por parte de un ciudadano a través de una *app*. Luego, la interfaz revisa el bloque de información y recibe una respuesta de verificación. Seguidamente, el *blockchain* ejecuta contratos inteligentes para la acción solicitada y almacena la transacción para evitar una posible colusión. El resultado de la operación y su historia permanecen disponibles y aprobados criptográficamente (ver gráfico 4.5). Para **2018, se habían hecho públicos más de 1,5 millones de títulos de propiedad a través de la tecnología *blockchain***, y la confianza ciudadana en el Gobierno presentó mejoras (OCDE, 2019; Shang y Price, 2019).

Gráfico 4.5. **Proceso de registro de titulación de tierras basado en *blockchain***



Fuente: Shang y Price (2019).

[76] En el estudio presentado por Shang y Price (2019), no es claro si la implementación de la tecnología blockchain redujo los costos de las transacciones relacionadas con bienes inmuebles.



La tecnología *blockchain* hace los registros accesibles, inmutables y seguros, impidiendo a las autoridades centrales actuar con excesiva discrecionalidad y permitiendo a los interesados consultar y validar las transacciones.

4.3. Reflexiones finales y recomendaciones

Las propiedades de la tecnología *blockchain* (el registro inmutable y un esquema descentralizado de validación de transacciones) y las experiencias estudiadas en este capítulo **muestran un potencial como innovación tecnológica para afrontar fenómenos de corrupción y la recuperación de la confianza pública en las agencias estatales. Sin embargo, aún es necesario generar evidencia estadística en materia de evaluación de impacto y de valoración de la efectividad del blockchain** en la reducción de formas específicas de corrupción. En ese sentido, es importante que las diferentes iniciativas que utilizan esta tecnología en asuntos de integridad pública contengan mecanismos para evaluar su impacto e incluso su costo-efectividad.

También es importante tener en cuenta que blockchain no es una herramienta que deba aplicarse de modo indiscriminado a cada transacción en donde los Gobiernos necesiten asegurar integridad. Los ejemplos citados muestran un potencial que, en calidad de prueba de concepto, abre nuevas discusiones de política pública, disruptivas, acerca de cuáles innovaciones tecnológicas son más idóneas para luchar contra la corrupción en el futuro y para mejorar la gestión pública. Por ejemplo, el registro de beneficiarios finales son **nuevas áreas en las que blockchain** podría cambiar para siempre la forma como los Gobiernos luchan contra los fenómenos de corrupción que acuden a la falsificación y alteración indebida de registros para beneficios particulares.

Sobre este particular, los Gobiernos que busquen explorar el potencial del *blockchain* deben tener en cuenta los siguientes aspectos:

- **Esta no es una tecnología para guardar o asegurar bases de datos. Preservar su calidad e integridad es un insumo fundamental, y no un producto, del blockchain.** La calidad e integridad de las bases de datos son necesarias para desplegar la potencialidad de *blockchain* señalada en este estudio. Por ejemplo, para la aplicación de las transferencias monetarias, las bases de datos de los beneficiarios estaban resguardadas y aseguradas por el PMA. En el caso de Colombia, para la aplicación de *blockchain* en el programa de alimentación escolar, la base de datos que almacena los documentos del proceso contractual permanecía en un archivo llamado IPFS[77].

[77] Acrónimo para InterPlanetary File System, que corresponde a un sistema y una red diseñados para almacenar y compartir información en un sistema de archivos distribuidos. (https://ipfs.io/)

- **Los registros gubernamentales deben guardar correspondencia con la realidad que capturan sus datos.** En general, una agenda cuyo propósito sea asegurar la calidad y estructura de los datos (ver capítulo 1), así como la comunicación entre diferentes sistemas de información, es necesaria para que la agenda anticorrupción prospere.

- **Usar blockchain también implica repensar los procedimientos estatales, como la compra pública o la titulación de tierras.** Ello supone el rediseño y supresión de varias etapas de los procedimientos o intervenciones de funcionarios que ya no serían necesarios, gracias a las propiedades de la tecnología de cadena de bloques. En consecuencia, la adopción de *blockchain* en los procedimientos gubernamentales pone de manifiesto el reto de adaptar la legislación y los procedimientos vigentes.

- **Es importante formular una estrategia de inversión de recursos en infraestructura para mayor poder de cómputo,** puesto que es necesaria la incorporación de nodos y unidades validadoras de las transacciones que desarrollan cálculos complejos. Adicionalmente, el considerable **consumo de energía que exige** la adecuada aplicación de esta tecnología, derivado del funcionamiento de miles de servidores que validan las transacciones bajo algoritmo de prueba de trabajo, debe ser considerado como un costo importante para decidir en qué casos es racional acudir al *blockchain*.

- **Los Gobiernos necesitan avanzar en otros frentes complementarios, como la identidad digital, para extraer el mayor provecho de las propiedades que tiene el blockchain en la prevención del fraude a las transacciones.**

- Igualmente, el éxito en la implementación de la tecnología *blockchain* y cualquiera otra que busque contribuir en la lucha contra la corrupción depende de la **educación y participación ciudadanas**. Todos los interesados deben conocer y entender para qué sirve esta tecnología y por qué se está empleando en un procedimiento o intervención determinada.

- **Los riesgos y limitaciones de esta tecnología deben ser considerados por los Gobiernos antes de adoptarla, puesto que puede ser vulnerable a ataques cibernéticos y spamming.** Adicionalmente, el *blockchain* no captura el universo de las interacciones humanas que se desarrollan por fuera de línea, lo que incluye sobornos o acuerdos irregulares. Si el entorno institucional y cultural premian esas conductas, tal y como se señala en el **informe de CAF (2019) sobre integridad**, es muy poco lo que puede hacer la tecnología para prevenir la corrupción.

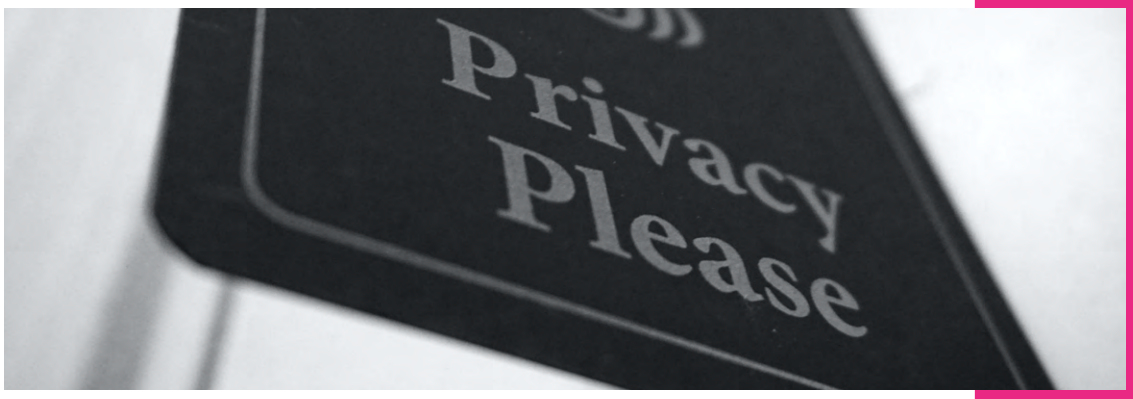
5.

Gestión de riesgos

“No es una fe en la tecnología.
Es la fe en las personas”.

Steve Jobs

Gestión de riesgos



A finales de 2020, la ciudad de **Tulsa** (Oklahoma), cuya población apenas supera los 400 mil habitantes, figuró en la lista *top ten* de la más reciente medición sobre ciudades digitales, elaborada por el **Centro de Gobierno Digital de los Estados Unidos** (CDG, por sus siglas en inglés). De acuerdo con el **reporte**, Tulsa invirtió en modernas soluciones de datos durante el último año con su programa *Urban Data Pioneers*, que aplica análisis de datos para responder mejor a problemas críticos. Por ejemplo, modelos predictivos para entender el riesgo de incendios domésticos, o el uso de Tableau para ayudar a las agencias de la ciudad a comprender mejor sus finanzas y tomar decisiones fiscalmente informadas.

Sin embargo, menos de seis meses después de obtenido el reconocimiento, Tulsa fue víctima de un **ciberataque** que suspendió gran parte de los servicios ciudadanos digitales y obligó a la ciudad a cerrar su red, interrumpiendo las comunicaciones por correo electrónico municipal, así como los pagos de facturas en línea. Según un comunicado de prensa emitido por el gobierno de la ciudad, casi 19 000 archivos, incluidos miles de citaciones policiales de Tulsa, fueron robados el pasado mayo de 2021, y compartidos en la **web oscura** a principios de esa misma semana.

El caso de Tulsa ilustra un fenómeno interesante: **aunque la transformación digital aporta importantes beneficios, también aumenta la exposición a una variedad de riesgos tecnológicos derivados de un ecosistema digital interconectado.** Si los riesgos de estas iniciativas no son administrados por los Gobiernos, es posible que la adopción de nuevas tecnologías les genere costos potencialmente equivalentes a la corrupción. Por ejemplo, la suplantación de identidad, la alteración de la información y el saboteo a su disponibili-

dad, e incluso el abuso de función pública para actividades como el tráfico de datos personales, de información privilegiada tributaria y el lavado de activos. Todo ello presenta un complejo panorama de riesgos en la adopción de tecnologías digitales para la gestión pública en general, y para la integridad en particular.

El reporte de CDG ha mostrado cómo la transformación digital de los Estados puede fortalecer la integridad pública y, con ello, el desarrollo institucional de los países. No obstante, los procesos de digitalización de los Gobiernos, abordados en los capítulos 1 y 2, así como las tecnologías específicas reseñadas en los capítulos 3 y 4, que tienen importantes aplicaciones en materia de lucha contra la corrupción, también están expuestas a fenómenos de tipo criminal y de uso indebido, lo cual puede deteriorar su potencial en las políticas de integridad pública.

En este capítulo, se presentan algunas tipologías de riesgos asociadas al desarrollo de tecnologías anticorrupción, y se exponen algunas recomendaciones para mitigarlos y lograr una efectiva integridad digital.

En este capítulo, se presentan algunas tipologías de riesgos asociadas al desarrollo de tecnologías anticorrupción, y se exponen algunas recomendaciones para mitigarlos y lograr una efectiva integridad digital. Es importante anotar que los riesgos señalados en esta sección no corresponden a una lista exhaustiva, sino, más bien, a una priorización de aspectos que requieren administrarse con mayor urgencia para asegurar una implementación efectiva de las innovaciones digitales en la lucha contra la corrupción.

- **Primero, se abordarán los retos que supone la transformación digital, relacionados con la adopción y protección de la identidad digital.** El desarrollo de plataformas e iniciativas de gobierno digital ha producido unos dividendos considerables en materia de integridad (ver capítulo 2). Sin embargo, el suministro de mejores servicios para los ciudadanos por medios digitales implica contar con mecanismos confiables de autenticación y verificación de identidad. Como veremos, esto no es un asunto que se reduzca a la simple asignación de un usuario y una contraseña, sino que implica la compilación de una gran cantidad de datos que componen la identidad de un ciudadano y que necesitan ser asegurados y resguardados. De este aseguramiento depende que no haya fraudes sobre los servicios ciudadanos a partir, por ejemplo, de la suplantación de identidad o la creación de identidades sintéticas. Los servicios digitales ayudan a que haya más integridad en el suministro de servicios a los ciudadanos, pero no significa que la digitalización en sí misma esté exenta de usos indebidos y fraudes.

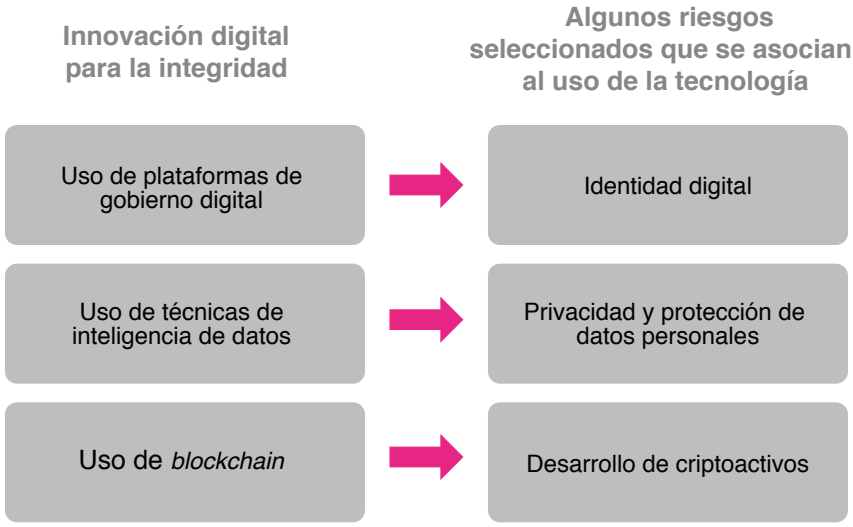
- **En segundo lugar, se analizarán los riesgos asociados a la privacidad y uso de los datos personales.** Las aplicaciones de tecnologías digitales para la prevención y detección de la corrupción que acuden a analítica descriptiva de patrones y a la analítica de redes (ver capítulo 3) requieren como insumo una gran cantidad de datos sensibles, como domicilios personales y laborales, vínculos de consanguinidad, estado civil y transacciones, entre otros. Asimismo, el funcionamiento de las plataformas de gobierno digital exige una cantidad de información personal para construir la identidad digital que habilita el suministro de servicios. Dichos desarrollos digitales en el ecosistema de integridad pública demandan gestionar riesgos por el uso indebido de los datos personales. No solo se trata de la protección de un derecho ciudadano, sino de la de un activo para los Gobiernos –como son los datos de los ciudadanos–, que se administra con unos fines específicos para salvaguardar el interés público[78]. En ese sentido, abordaremos la importancia de la privacidad por diseño en las plataformas, y del desarrollo legal para proteger los datos personales en usos indebidos, que podrían ir desde la suplantación hasta el tráfico para monetización no autorizada de los datos en publicidad dirigida.

[78] Piénsese, por ejemplo, en las apps de rastreo para contener la pandemia COVID-19, o en las plataformas de registro de identidad para validar el sufragio.

- En la **tercera** parte del capítulo, **se extenderá el análisis del uso de las tecnologías blockchain hacia el desarrollo de los criptoactivos**, puesto que dicha aplicación representa un riesgo considerable en materia de integridad. La encriptación y validación del *blockchain*, fuente de seguridad e integridad en algunos procesos de la gestión pública (ver capítulo 4), paradójicamente, facilitan actividades de lavado, puesto que permiten ocultar transacciones con activos financieros de naturaleza digital a través de criptoactivos[79] y monedas privadas. Prácticas de control al lavado que se emplean en la industria financiera son muy difíciles de aplicar en el ecosistema que valida las transacciones con criptoactivos.

Finalmente, se plantearán algunas condiciones habilitantes y recomendaciones para una agenda digital en la lucha contra la corrupción, orientada a mitigar los riesgos identificados y asegurar el éxito de la innovación digital en la agenda de integridad pública.

Figura 5.1. Innovaciones digitales anticorrupción y riesgos asociados



Fuente: Elaboración propia.

[79] En este reporte, se usa el término de criptoactivos como sustituto del concepto de criptomonedas, puesto que estas no necesariamente cumplen con las funciones que, de modo simultáneo, tiene el dinero: depósito de valor, unidad de cuenta y medio de pago. Tampoco se usa el concepto de moneda digital, puesto que esta última es la forma electrónica que puede tomar el dinero, debidamente respaldado por una autoridad como el banco central.

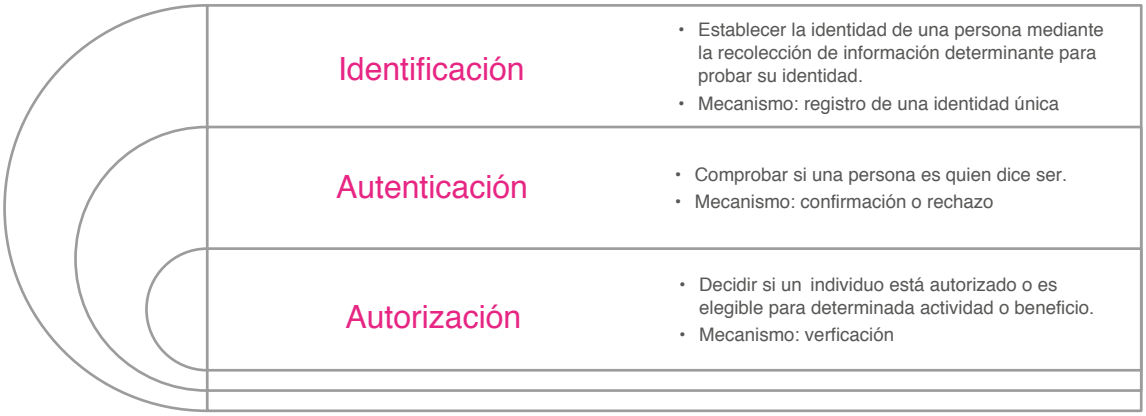
5.1 Identidad digital y administración de riesgos

Como resultado de la necesidad de proveer servicios del Estado a través de medios no presenciales, ha surgido el concepto de **«ciudadanía digital»** y el deber de los Gobiernos de crear y utilizar herramientas que faciliten la identificación y autenticación remota de clientes y ciudadanos mediante procedimientos como la identidad digital, las firmas digitales o los pagos digitales.

Esta herramienta también ha mostrado su potencial en la lucha contra la corrupción (ver capítulos 2 y 4) para la gestión de algunos servicios del Estado. Por ejemplo, en Nigeria, gracias al sistema de identificación y pago digital de nóminas de servidores públicos, se identificaron más de 43 000 «trabajadores fantasma», lo que generó ahorros para el Estado en el año 2011 (Gelb y Clark, 2013). Sin embargo, la adopción de esta tecnología no está exenta de la materialización de riesgos, lo que a su vez genera nuevos retos en su diseño e implementación (Beduschi, 2021).

La identificación corresponde a una combinación de características o atributos de una persona, que la hacen única en un contexto determinado. Los sistemas de identificación tienen varias finalidades: la *autorización,* la *autenticación* y la *identificación* (ver figura 5.2). Estas son herramientas decisivas para el desarrollo de los países, por diferentes razones. Primero, facilitan la interacción entre las personas, el Gobierno y las entidades privadas. En segundo lugar, permiten al Gobierno tomar decisiones y prestar servicios más eficientes. Y, tercero, aumentan la transparencia en las actuaciones gubernamentales (Banco Mundial, 2014). Por ello, el aseguramiento de la identificación de todas las personas, además de un derecho, constituye un **objetivo de desarrollo sostenible (16.9).**

Figura 5.2. Finalidades básicas de los sistemas de identificación

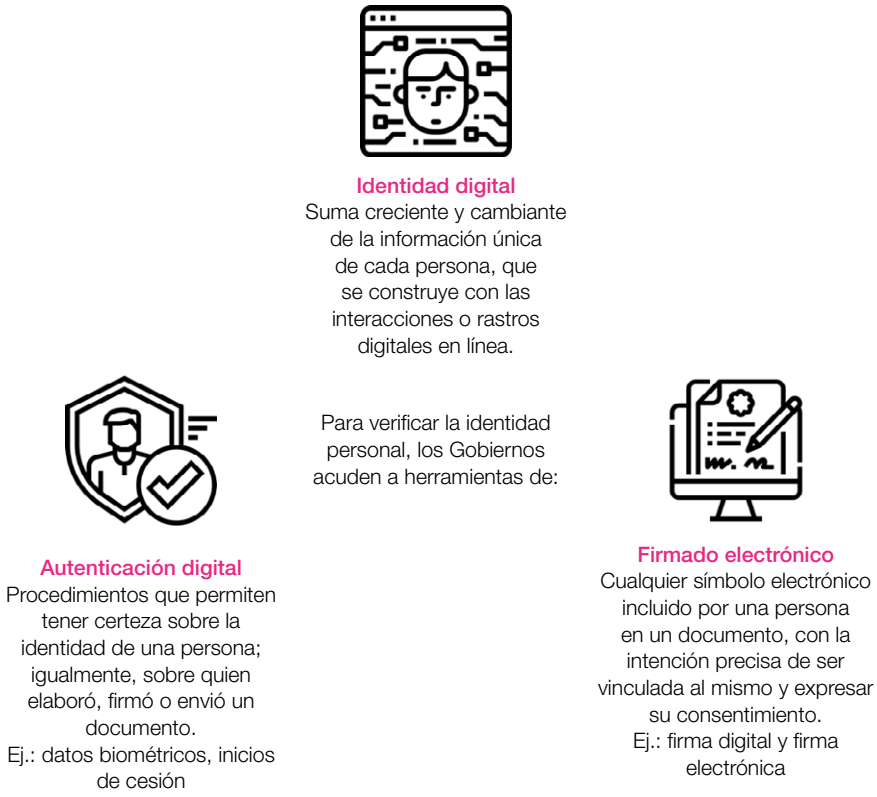


Fuente: Banco Mundial (2019).

Desde el punto de vista digital, la identificación comienza cuando un usuario inicia su relación con una institución o empresa, incorporando datos de su registro, su actividad, y el consumo o uso de algún servicio digital. Para ello, se identifica al usuario y se construye una relación de mutuo beneficio entre este y la plataforma que usa. El rápido crecimiento de la digitalización, las más recientes tecnologías y los nuevos comportamientos de los usuarios reevalúan el papel de la identidad digital en el suministro de servicios no presenciales. Esto se debe a que, gracias a la identidad digital, es posible el acceso remoto a la banca, beneficios gubernamentales, educación y muchos otros servicios críticos (autorización), los cuales necesitan la comprobación de datos que acrediten que un individuo es efectivamente la persona que dice ser (autenticación).

En el mundo digital, las actividades de identificación, autenticación y autorización no se agotan con la simple asignación de usuarios y contraseñas. Por ejemplo: características físicas, información sobre las finanzas y los impuestos, historiales de compra, registros legales, registros médicos e historia crediticia, entre otros (OCDE, 2019). Estos elementos permiten asignar una identidad, con determinados atributos, a una persona concreta. Esto implica que la identidad digital se crea con el tiempo, por medio de las interacciones, las cuales producen rastros digitales o historias de datos personales y comportamientos en línea. Sin embargo, como cualquier desarrollo tecnológico, también está acompañado de varios riesgos, siendo el principal el de fraude cibernético, ya sea de datos personales, financieros, de la vida privada o de preferencias, entre otros.

Figura 5.3. Ilustración de conceptos básicos relacionados con la identidad digital



Fuente: Elaboración propia.

5.1.1. Conceptos básicos de identidad digital

- **Identidad digital:** es la suma total de la creciente y cambiante masa de información única de cada persona, su perfil y el historial de sus actividades y transacciones en línea. En otras palabras, es lo que crean con el tiempo las interacciones, en forma de rastros digitales o historias de datos personales y comportamientos en línea, como, por ejemplo: información sobre las finanzas y los impuestos, historiales de compra, registros legales, registros médicos e historia crediticia, entre otros (OCDE, 2019). La identidad digital, así concebida, es un insumo necesario para poner en marcha innovaciones tecnológicas de integridad pública. Santiso (2021) señala algunos ejemplos que acuden al rastreo de datos de ciudadanos y sus interacciones en diferentes plataformas, incluidas redes sociales, para identificar potenciales evasores de impuestos, así como las redes detrás del escándalo Panamá Papers.

El gobierno digital implica incorporar las tecnologías desde el diseño y la concepción de los servicios de Gobierno (ver capítulo 2, sección 2.2). En el uso de servicios digitales de los Gobiernos (ver capítulo 2), es necesario verificar la identidad de los ciudadanos con los que interactúa el Estado para entregar bienes y servicios. Con ese fin, se acude a la autenticación digital y la firma digital.

- **Autenticación digital:** se refiere a procedimientos y herramientas para verificar la identidad o tener certeza acerca de la persona que ha elaborado, firmado o enviado un documento. En otras palabras, la autenticación permite comprobar, por ejemplo, que aquel que envió un mensaje o quiere acceder a una plataforma o servicio es realmente quien dice ser.

  La autenticación tradicional implica la inspección manual y personal de documentos de identidad y algunos soportes para determinar que son genuinos y que la persona es quien dice ser. Este proceso es menos seguro y presenta mayores oportunidades de corrupción debido a los potenciales errores humanos y a los altos niveles de discreción de los procedimientos (Banco Mundial, 2019).

  Por otro lado, la autenticación también puede hacerse remotamente, a través de **canales digitales**. Existen varias formas o herramientas de autenticación digital, como los inicios de sesión de cuenta o datos biométricos (reconocimiento facial o escaneos de ojos o huellas dactilares) para acceder a los servicios y realizar interacciones digitales, entre otros. Es así como el acceso a los perfiles digitales está condicionado por herramientas de autenticación que permiten demostrar que la persona que pretende acceder a un servicio digital es realmente aquella que está interactuando con la plataforma digital.

- **Firmado electrónico: hace referencia a cualquier símbolo basado en medios electrónicos, utilizado o adoptado por una determinada parte, con la intención precisa de vincularlo a un documento.** Con independencia de las reglas establecidas por las normas de cada país, para que los procedimientos de firmado electrónico tengan efectos jurídicos, deben cumplir con dos características fundamentales (Rincón, 2020): i) que no se haya modificado el contenido del documento electrónico (**integridad**), y ii) que exista certeza sobre la identidad de su autor (**autenticidad**).

  Al implementar mecanismos que prevean ambas características, se genera un entorno de plena identificación e integridad del documento y la exigencia de un mecanismo de autenticación con el mensaje de datos; por lo tanto, se logra suministrar consentimiento por un medio electrónico. Adicionalmente, en algunos ordenamientos jurídicos, se distinguen conceptualmente el «firmado electrónico» como categoría general, y la «firma

digital»[80] y la «firma electrónica»[81] como clases específicas del procedimiento (Rincón, 2020).

5.1.2. Riesgos relacionados con los sistemas de identidad digital

Una vez que la identidad digital se adopta para hacer más ágil y transparente el suministro de servicios de gobierno digital (o de cualquier otro en el ecosistema de economía digital), existe una exposición a riesgos que van más allá de las capacidades gubernamentales en gobierno digital (ver tabla 5.1). Dichos riesgos se derivan de la posibilidad que las redes criminales encuentran para explotar ilícitamente los datos almacenados y generar la identidad digital. En el mundo real, por ejemplo, el contacto físico se requiere para los procesos de autenticación y firmado, lo que impone una barrera natural a quien suplanta una identidad con el fin de reclamar dinero o exigir derechos (*i. e.*, físicamente, se puede estar una vez en un sitio y no en varios al tiempo). Pero, en el mundo digital, un mismo delincuente podría repetir tantas veces como fuera necesario el proceso de suplantación, al mismo tiempo, con solo robar los datos una única vez. Esto es posible porque autenticación e identidad digitales descansan en el mismo acervo de datos personales que pueden ser hurtados o usados indebidamente.

[80] La firma digital es un procedimiento matemático que permite garantizar los dos atributos propios de las comunicaciones electrónicas: la autenticidad y la integridad. Para poder tener una firma digital, es necesaria la intervención de un tercero de confianza denominado «entidad de certificación», que avala precisamente la identidad de quien aparece como titular de la firma digital. Este procedimiento asegura la autenticidad, pues determina la autoría, así como la integridad del contenido de los datos transmitidos gracias a la intervención de este tercero.

[81] Por su parte, la firma electrónica opera sin la intervención de un tercero. Se refiere a cualquier símbolo basado en medios electrónicos, utilizado o adoptado por una determinada parte, con la intención precisa de vincular o autenticar un documento para que cumpla con las características de una firma manuscrita. Sin embargo, para que esta firma se tenga como válida, debe existir un elemento de vinculación con el propio mensaje de datos enviado por el firmante, a través del cual pruebe su identidad en el mundo digital. Adicionalmente, se requiere que el firmante declare o acredite su voluntad respecto del contenido obrante en el documento firmado. En resumen, la diferencia entre las firmas electrónica y digital es exclusivamente probatoria, dado que la digital incorpora la autenticidad y la integridad de manera automática, mientras que la electrónica necesita demostrar el cumplimiento de estos dos atributos.

Tabla 5.1.

Riesgos de los sistemas de identificación digital (SID)

Exclusión		La implementación de SID que excluyen medios alternativos o informales para demostrar la identidad de las personas genera el riesgo de **marginar aún más a los grupos que no tienen conocimientos técnicos o acceso a los canales digitales**.
Violaciones de privacidad y seguridad		Inherentes a la captura, almacenamiento y uso de datos personales confidenciales, están los **riesgos asociados con violaciones de privacidad, robo y uso indebido de datos, fraude de identidad y discriminación**.
Vinculación con el proveedor o la tecnología		**La dependencia en una tecnología o un proveedor específico puede resultar en un «bloqueo»**, aumentando los costos (por ejemplo, licencias para software) y reduciendo la flexibilidad del sistema para satisfacer las necesidades de un país a medida que se desarrollan.
Tecnologías inadecuadas o insostenibles		Los sistemas **no ajustados a los contextos o de alto costo no han logrado garantizar los objetivos del desarrollo** y resultan insostenibles a mediano y largo plazo. Por ejemplo, algunos países han implementado costosas tarjetas inteligentes multipropósito, que no son utilizadas por los ciudadanos.
Infraestructura y conectividad limitadas		**Las áreas rurales y remotas carecen de la infraestructura básica de las TIC, de conectividad móvil e internet confiable. Esto puede crear dificultades al implementar sistemas de identificación digital** que requieren energía y conectividad durante la inscripción (por ejemplo, para la transferencia de datos o verificación de inscripción biométrica duplicada) y para la autenticación.
Sistemas de compra pública débiles		Los procesos para **la adquisición y gestión de SID son complejos** debido a la amplia gama de tecnologías disponibles y los diferentes tipos de adquisiciones que deben completarse. Como consecuencia de los procesos de adquisición deficientes y la **gestión inadecuada de los contratos** con proveedores, pueden darse adquisiciones fallidas, retrasos (por ejemplo, debidos a apelaciones), y bloqueo de proveedores y tecnología.
Insuficiente capacidad nacional de ciberseguridad		Los países de ingresos bajos y medianos, a menudo, presentan **brechas de capacidad en sus agencias centrales de ciberseguridad**, las cuales son necesarias para propiciar un entorno seguro para los SID.

Fuente: Banco Mundial (2019).

Adoptando el concepto de ciudadanía digital, el Gobierno de Colombia creó recientemente la **Carpeta Ciudadana Digital** (CCD). Esta actúa no solo como repositorio de los documentos que necesitan los ciudadanos para hacer trámites con las entidades públicas, sino como puerta de entrada para adelantarlos. Actualmente, existen 11 trámites. La expansión de la CCD a otros procedimientos y servicios ofrece un potencial inmenso en materia de integridad (ver capítulo 2, sección 2.2), así como de ahorro en tiempo y dinero para los usuarios y las entidades públicas. Sin embargo, también tiene una exposición al riesgo, al ser un repositorio centralizado de los datos de los ciudadanos con una sola llave de acceso (la fecha de expedición del documento de identidad).

La vulnerabilidad a la que pueden estar expuestos los sistemas de identificación digital se hizo evidente en Chile. En octubre de 2020, el Sistema de Identificación Digital, administrado por la División de Desarrollo Digital de la Presidencia de la República, habría sido objeto de un ciberataque (Agencia EFE, 2020). El sistema opera a través de la generación de una **clave única** e identificación biométrica para la realización de variados trámites públicos. Lo anterior generó una alarma para las autoridades y la ciudadanía sobre la sensibilidad de los sistemas de identificación y procesos de autenticación digital. En consecuencia, también evidenció el desafío que representa la seguridad cibernética.

El fraude en la autenticación digital

Los sistemas de autenticación digital deben ser lo suficientemente seguros para evitar el robo de identidad y proteger los datos personales. Para ello, los diseños que requieren varios niveles de autenticación, por ejemplo, confirmación de datos, claves de un solo uso y biometría, entre otros, son deseables. Sin embargo, es posible burlar los sistemas de autenticación a partir del robo de datos personales que, en algunos casos, se usan como verificadores de identidad (fechas de nacimiento, domicilios usados en el pasado o en el presente o relaciones comerciales de crédito). Con ello, un impostor puede suplantar la identidad de un usuario de una plataforma y acceder a servicios.

La incidencia de delitos asociados al fraude y robo de identidad ha aumentado considerablemente en esta década. La Encuesta Mundial sobre Delitos Económicos y Fraude de PricewaterhouseCoopers (PwC) para 2020, señaló que el 47 % de las empresas experimentaron un incidente en los últimos 24 meses, vinculado con los sistemas de autenticación (PwC, 2020). Esto último se ha presentado a través del mundo. Por ejemplo, en Europa, el 79 % de las organizaciones entrevistadas por la Asociación de Examinadores de Fraude Certificados denunciaron un aumento en los niveles desde el comienzo de la pandemia del COVID-19. Esto incluye desde el fraude con tarjetas de crédito y el *phishing* hasta el de identidad sintética, en el que alguien crea una identidad para estafar a una empresa.

El robo de identidad puede causar a la víctima daño financiero, reputacional, y también una pérdida de recursos para evitar las consecuencias del fraude.

En la mayoría de las legislaciones, el robo de identidad es un delito. Es un tipo de fraude en el que un impostor roba información individual de otra persona (o de una organización) y lo utiliza para obtener algún beneficio (por ejemplo, dinero o bienes). El robo de identidad puede causar a la víctima daño financiero, reputacional, y también una pérdida de recursos para evitar las consecuencias del fraude. El robo de identidad también afecta a organizaciones, ya sean públicas o privadas, provocando no solo daños económicos, sino a la reputación.

Al tener suficiente información sobre un individuo, las redes criminales se hacen cargo de la identidad para extraer recursos por medio de una amplia gama de delitos: por ejemplo, solicitudes falsas de préstamos y tarjetas de crédito, retiros fraudulentos de cuentas bancarias, uso fraudulento de llamadas telefónicas, o la obtención de otros bienes o servicios como acceso a línea telefónica.

Por ejemplo, en Estados Unidos, la Comisión Federal de Comercio (FTC) hace un seguimiento de las denuncias de fraude y robo de identidad de los consumidores que se han presentado ante los organismos policiales federales, estatales y locales, y las organizaciones privadas. Según sus datos, hubo 4,8 millones de informes de robo de identidad y fraude recibidos por la FTC en 2020, un 45 % más que los 3,3 millones de 2019, principalmente, debido al aumento del 113 % en las quejas de robo de identidad. De la misma forma, una evaluación de Interpol (2020) sobre la repercusión de la crisis sanitaria COVID-19 en la ciberdelincuencia reveló que el objetivo de las redes criminales pasó de los particulares y las pequeñas empresas a las grandes corporaciones, los Gobiernos y las infraestructuras críticas.

En **América Latina, se estima que este delito creció más de un 400 % en el año 2020** (Acosta, 2021), en mayor medida a través de correos electrónicos, con los cuales se busca la falsificación de documentos para acceder a contratos con el Estado, obtener créditos financieros y hasta hacer compras por internet. Asimismo, la suplantación de sitios web creció 358 %, con 4 353 casos en 2020, en comparación con los 951 reportados el año inmediatamente anterior (Acosta, 2021). Adicionalmente, el mismo reporte concluyó que las personas no son los únicos objetivos de la ciberdelincuencia con respecto a la suplantación de identidad.

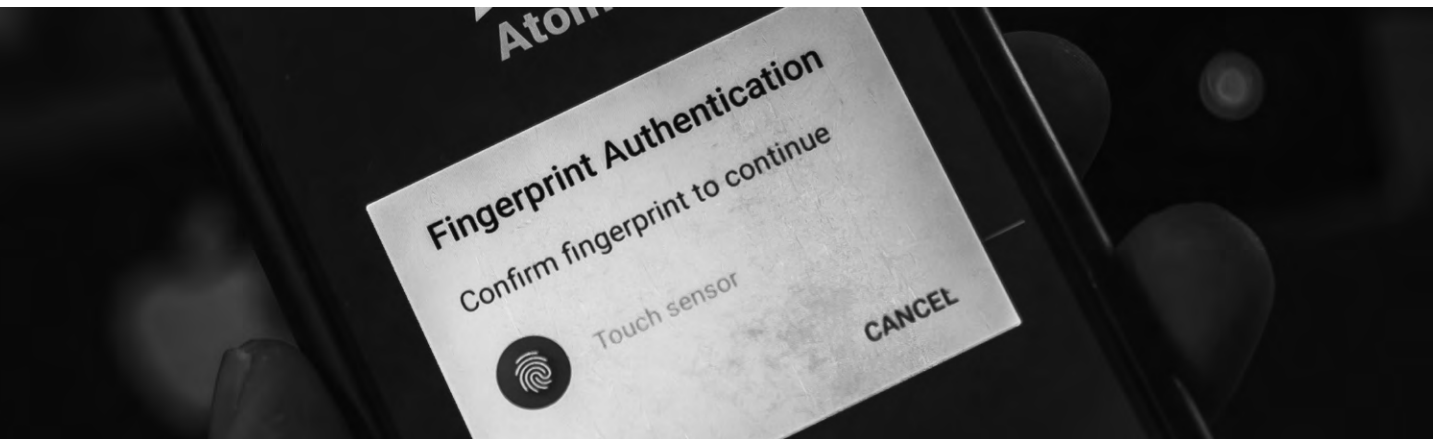
Es por ello que los datos personales, por definición de la identidad digital, deben ser protegidos. La protección no solo es un tema de custodia de la información para que no sea objetivo de piratas informáticos (lo cual hace parte del reino de los desarrolladores de sistemas). También, requiere un andamiaje institucional y legal, donde existe una responsabilidad por la recolección, administración, custodia y usos de los datos personales.

5.2. La protección de datos como elemento de integridad digital

Los sistemas digitales de servicios y los avances en big data permiten que las organizaciones que suministran plataformas tecnológicas obtengan información detallada sobre el acceso de los usuarios. Esta información incluye la ubicación geográfica, los patrones de uso e incluso los datos biométricos. Por ejemplo, a principios de 2020, Colombia logró aprovechar los datos sobre la población más vulnerable y administrarlos con entidades financieras que tienen fortalezas en sus servicios digitales para implementar las transferencias monetarias de supervivencia en la emergencia, sin necesidad de obligar a los beneficiarios a ir a los bancos o contar con tarjetas como medios de pago.

Igualmente, los datos masivos y la analítica sobre esos conjuntos de datos permiten detectar redes e incluso predecir riesgos de corrupción, gracias, en buena medida, a la posibilidad de identificar digitalmente a personas naturales y jurídicas dentro de estructuras susceptibles de ser consideradas criminales. En tal sentido, aun cuando los desarrollos digitales permiten simplificar trámites, eliminar la presencialidad y aplicar técnicas de análisis de datos para mejorar procesos como la detección temprana de riesgos de corrupción, existen amenazas implícitas relacionadas con la **privacidad** y **seguridad** de los datos personales, que subyacen al uso y al propósito de las tecnologías.

El concepto de «datos personales» incluye cualquier tipo de información sobre una persona. Esta puede ser «objetiva», como la edad, y «subjetiva», como opiniones o evaluaciones que dichos usuarios hacen sobre una plataforma o servicio por medios digitales. En cuanto al formato o



medio que contiene la información relevante, el concepto incluye aquella disponible en cualquier forma, como alfabética, numérica, gráfica, fotográfica, acústica, etc. Igualmente, la que se encuentra en papel, así como cualquiera almacenada digitalmente o en una cinta de video; por ejemplo, un sonido e imagen, los cuales son datos que pueden representar información sobre un individuo y, por lo tanto, considerarse como personales (Koch, s. f.).

El «procesamiento» es cualquier operación o conjunto de operaciones que se realice sobre datos personales, ya sea por medios automáticos, recopilación, grabación, organización, almacenamiento, adaptación, alteración, recuperación, consulta, uso, divulgación, transmisión, difusión, puesta a disposición, alineación, combinación, bloqueo, borrado o destrucción. En otras palabras, el procesamiento (y, por ende, la protección) debe estar presente en todo lo que haga la organización con los datos personales, pues cualquier acción será considerada como tal (Wachter y Mittelstadt, 2019). Al llevar a cabo estas operaciones, debe atenderse a cuestiones específicas, relacionadas con la calidad de los datos, el propósito para el cual fueron recolectados y las políticas de tratamiento (ver figura 5.5).

Figura 5.5. Aspectos que determinan el procesamiento de datos

Fuente: Elaboración propia.

- **¿Qué datos se protegen y por qué?** Dentro de las diferentes clasificaciones de datos personales, estos pueden dividirse en: (i) semiprivados (comportamiento financiero); (ii) privados (domicilio, correo electrónico), y (iii) sensibles (afiliación política o religiosa, orientación sexual, condicio-

nes de salud). Mientras más sensibles sean los datos o cuanto más vulnerables los participantes, más fuertes serán las normas de seguridad. En estos casos, es recomendable compartimentar el almacenamiento de datos. Por ejemplo, mantener datos sensibles estrictamente separados de otros personales, y cifrar las bases de datos. Adicionalmente, es recomendable especificar los métodos de conservación.

- **¿Cómo se protegen?** Las políticas de tratamiento de datos deben ser revisadas periódicamente, divulgadas y aceptadas por los usuarios, quienes han de expresar su consentimiento libre, específico e informado (Wilms, 2019). Adicionalmente, es necesario garantizar a los titulares de la información el derecho a acceder, rectificar, cancelar y oponerse a proporcionar sus datos personales.

- **¿Por cuánto tiempo se protegen?** El período para conservar los datos depende del propósito para el cual se recopilaron o procesaron. Cuando ya no son necesarios para cumplir el propósito de su procesamiento, deben eliminarse o mantenerse en forma anónima si sirven para usos históricos, estadísticos o científicos. De esta manera, se pueden determinar períodos de retención específicos, señalando la posibilidad de eliminarlos una vez que haya expirado el término; es decir, tan pronto dejen de ser necesarios conforme a los fines para los cuales fueron recolectados[82].

El acceso y utilización de estos datos por parte de personas no autorizadas o para fines distintos a los declarados en el momento de su recolección tienen la potencialidad de violar la intimidad de las personas y causar daños a los titulares de la información.

La protección de los datos se ha vuelto **especialmente sensible para los países en la fase de pospandemia** (Cetina, 2021), como es el caso de las aplicaciones móviles para asesoramiento sanitario o rastreo y contención del COVID-19. En particular, existe cierta opacidad sobre el uso que los Gobiernos harán de los datos de los ciudadanos cuando la vacunación logre inmunidad de rebaño en la población de cada país[83].

A lo largo de este informe, se han identificado procesos de digitalización gubernamental que son especialmente sensibles en materia de datos personales, como las compras públicas, la prestación de servicios de seguridad social y los sistemas de tributación. Lo anterior se debe a que la información asociada es de carácter semiprivado, privado o sensible, y, por ello, el acceso y utilización de estos datos por parte de personas no autorizadas o para fines distintos a los declarados en el momento de su recolección tienen la potencialidad de violar la intimidad de las personas y causar daños a los titulares de la información.

[82] De manera particular, la Ley 1581 de 2012 constituye el marco general de la protección de datos personales en Colombia. En ella, se incorporan los principios y obligaciones que tienen todos aquellos que realicen el tratamiento de datos personales, para garantizar la protección del derecho fundamental de habeas data y el derecho a la intimidad.

[83] Por ejemplo, en China, Alipay y WeChat implementaron la aplicación Health Code, utilizada para rastrear la exposición al coronavirus. Como lo afirma **Lei (2020)**, dichas empresas han hecho valer sus derechos contractuales para conservar los datos una vez que la crisis haya terminado, lo cual parece ir en contra del objetivo y la finalidad para la cual fueron recogidos.

En tal sentido, el tratamiento de datos personales es un proceso esencial en la implementación de estrategias digitales en contra de la corrupción, que debe garantizar privacidad y seguridad.

Mitigando los riesgos del uso indebido de los datos personales

Privacidad

La privacidad se considera un derecho fundamental para los seres humanos, el cual genera una obligación correlativa de los Gobiernos a la garantía de un nivel adecuado de protección con respecto a la información atribuida a un individuo. El Gobierno tiene la obligación de garantizar los derechos de los ciudadanos con respecto a la privacidad y el procesamiento, y que la recopilación de datos personales solo sea con fines legítimos (OCDE, 2010).

Sin embargo, su significado y sus límites pueden evaluarse a través de los riesgos relacionados con los datos del usuario frente a los beneficios de participar en la interacción del mundo digital, bien sea usando redes sociales, servicios digitales del Gobierno o transacciones de comercio electrónico. A medida que los usuarios y ciudadanos adoptan la tecnología, se crea una mayor carga para que las organizaciones administren la responsabilidad de mantener seguros los conjuntos de datos. Debido a estas demandas de privacidad y control, se han creado nuevas regulaciones, como el Reglamento General de Protección de Datos (GDPR) en Europa y la Ley de Privacidad del Consumidor de California (CCPA).

En general, las regulaciones desarrollan estándares y normas que conduzcan a la transparencia en la forma en que las instituciones solicitan el consentimiento sobre la captura y uso de datos, cumplen con sus políticas de privacidad y gestionan los datos que han recopilado. De hecho, el uso de plataformas tecnológicas implica el intercambio de información personal, como direcciones, datos de las tarjetas de crédito, geolocalización, hábitos de viaje, y preferencias individuales relacionadas con el uso de diversos bienes y espacios personales.

La puesta en práctica de protección en la privacidad de los datos implica introducir la **privacidad desde el diseño**, la cual busca garantizar el correcto tratamiento de los datos utilizados en cualquier tipo de actuación donde se utilicen plataformas digitales. Este principio sostiene que la privacidad de los datos debe aparecer al principio del proceso de planificación y diseño de las plataformas y servicios digitales. Esto supone:

1. **La privacidad como configuración por defecto.** El responsable de los datos, desde el principio y durante todo el ciclo de vida del tratamiento,

debe tener un sistema con una protección suficiente en cuanto a la recolección, almacenamiento, usos, circulación y acceso. Esto significa restringir el uso compartido, utilizar la minimización, eliminar los que ya no se utilizan y operar siempre sobre una base legal. También implica utilizar funciones de inclusión y exclusión voluntarias, y salvaguardar la información de los consumidores.

2. **La privacidad embebida en el diseño.** La información debe entenderse como un activo más en la gestión de los servicios digitales; por lo tanto, su protección debe ser embebida en la infraestructura de tecnología de la información y en los procesos, de la misma forma como se protege cualquier otro activo dentro de la gestión del Estado. Por su parte, este principio establece cómo la privacidad es una funcionalidad central de los servicios de gobierno digital. Por ende, es importante utilizar el cifrado y la autenticación, y probar las vulnerabilidades de forma regular. No importa si el proceso funciona como debe, las instituciones han de estar en constante búsqueda de un fallo de diseño si hay una vulnerabilidad de seguridad.

3. **Funcionalidad completa.** Dentro del principio, se establece cómo la protección de la privacidad sigue a los datos a lo largo de su ciclo de vida, desde su recolección hasta su eliminación o archivo. El cifrado y la autenticación son esenciales, pero hay que ir más allá. Por ejemplo, solo se deben recolectar los que se necesitan y para los que se tiene una base legal. Y cuando se termine con los datos, se deben utilizar métodos de borrado y destrucción que cumplan con la regulación para una protección de extremo a extremo.

4. **Visibilidad y transparencia.** Los componentes y operaciones deben ser visibles y transparentes a todos los usuarios por igual, constituyendo, dentro de las prácticas de la organización, un sistema sincronizado con los compromisos y los objetivos establecidos. En este principio, los interesados deben conocer sus prácticas de privacidad (y de tratamiento) y compartirlas abiertamente. El principio argumenta que se debe contar con una política de privacidad o de tratamiento de datos bien escrita, lo cual es esencial en cualquier jurisdicción. También, determina que debe haber un mecanismo para que los sujetos de los datos expresen sus quejas, hagan preguntas y pidan cambios.

5. **El respeto a la privacidad del usuario.** Por último, el sistema debe preservar los intereses privados de las personas que han suministrado información, ofreciendo medidas suficientes para la protección de la privacidad mediante los avisos apropiados sobre el uso, recolección, almacenamiento, circulación y acceso a los datos. Este último principio significa reconocer que, aunque se tengan los datos, estos pertenecen al usuario del que se hayan recogido. Por tanto, el interesado es quien puede conceder y retirar el consentimiento para su uso, y no al revés.

Seguridad

La seguridad de un sistema de información se refiere a la protección de la información y las herramientas contra accidentes, modificaciones, y acceso o destrucción no autorizada. La seguridad de la información, conocida como seguridad cibernética o informática, es un importante desafío y un componente vital en la relación de confianza entre los ciudadanos y sus Gobiernos. De la misma manera que la suplantación de identidad, los ciberataques pueden causar daños económicos, tanto por la interrupción de los sistemas de información y comunicación, como por la pérdida o alteración de información confidencial u otros datos importantes.

. La seguridad de la información, conocida como seguridad cibernética o informática, es un importante desafío y un componente vital en la relación de confianza entre los ciudadanos y sus Gobiernos.

La seguridad de las plataformas tecnológicas no es un asunto menor, y la administración de estos riesgos afecta a los sectores público y privado por igual. Su importancia viene escalando a medida que los ataques se hacen más frecuentes en el planeta. **Forbes** estima que, para 2025, el cibercrimen le puede costar al mundo unos USD 10,5 billones anuales, con efectos sensibles en la provisión de servicios públicos (como salud y transporte, por ejemplo). El costo de ese tipo de crímenes puede deberse a la escala de los ataques y de sus perpetradores. Por ejemplo, el caso Snowden expuso una cantidad de violaciones y accesos no autorizados a plataformas de Gobiernos y sector privado en varios países por autoridades de inteligencia (Wright y Kreissl, **2013**); ciberataques como el de **Sony** en 2014 y el brote *ransomware* **Wannacry** se han atribuido a Corea del Norte; otros, como el sufrido recientemente por el Banco Central de Nueva Zelanda, no dan pista **sobre su autor**; y el ataque al Comité Nacional Demócrata durante 2016 **se ha atribuido a Rusia**. Los Estados mismos comienzan a ser considerados actores en el mapa de riesgos a la seguridad de las plataformas tecnológicas.

Según Van Eeten (2017), los problemas de seguridad informática provienen de la gobernanza del internet y su concepción original. Internet no se diseñó desde su inicio pensando en administrar tráfico malicioso de modo diferenciado al tráfico benigno (ni siquiera para notar la diferencia). Fidler (2017) señala que las agencias de defensa e inteligencia involucradas en la financiación y el desarrollo de las versiones más tempranas del internet operaban bajo un modelo de amenaza diferente, interceptación y vigilancia del tráfico en la red (es decir, los datos que se movilizan), y que no tenía en cuenta la subversión de los nodos (miembros de la red) responsables de los datos. Con el tiempo, algunas capacidades para mitigar las amenazas de los nodos que se comportan mal se agregaron al diseño básico de la red en sí[84], pero la autoridad, también en términos de seguridad, residía, ante todo, en los propietarios de los nodos. Hoy en día, es necesario que la autoridad descanse en los Gobiernos.

84 Piénsese en puertos bloqueados, filtrado anti-spoofing, hundimiento del tráfico de comando y control de botnets, bloqueo del tráfico DDoS, etc.

En Europa, se han desarrollado algunos estándares en materia de seguridad y responsabilidad para los sistemas de gobierno digital, que pueden servir de modelo para América Latina. Por ejemplo, la Directiva 2013/40 UE del Parlamento y del Consejo Europeos tiene como objetivo penalizar cualquier acceso indebido[85] en el curso del procesamiento de datos, con la intención de obtener una transferencia ilegal de propiedad (Csonka, 2006). De esta forma, en Europa, la falsificación informática implica el acceso, la creación o alteración no autorizada de datos almacenados para que adquieran un valor probatorio diferente; por consiguiente, el curso de las transacciones legales, que se basa en la autenticidad de la información contenida en los datos, está sujeto a un fraude sancionable por la ley.

Otro ejemplo de relevancia es la regulación de Estados Unidos. Diferentes casos que involucran no solo fraude, sino también el robo y alteración de información confidencial a través del acceso no autorizado a computadoras se motivaron por decisiones judiciales. En 1990, en el caso **Estados Unidos contra Schreier**, se sancionó de manera ejemplar a los perpetradores por acceder al sistema de reservaciones informáticas de American Airlines y modificar información contenida en el mismo. En 1990, con la decisión **Estados Unidos contra Riggs**, se impusieron sanciones porque el procesado accedió sin permiso al archivo de computadora de emergencia de Bell South, con el objetivo de realizar modificaciones en los sistemas de la compañía de telecomunicación y copiar datos de los suscriptores del servicio.

Cada uno de estos casos tiene algo en común: aunque el sistema parece funcionar, los tribunales han sostenido que el acceso y la copia de datos no autorizados pueden causar daños a los propietarios o titulares de los datos. Por lo tanto, aun cuando no se haya alterado el sistema, el acceso, la alteración o copia de los mismos sin autorización trae consigo (en el menor de los delitos) violación a la privacidad de datos.

En América Latina, realizar la vulneración y alteración de los sistemas de cómputo para recibir servicios y transferencias electrónicas de fondos mediante manipulación de programas y afectación de los cajeros automáticos, entre otras, son conductas reguladas. Sin embargo, no hay un estándar en la protección de datos personales en todo el ciclo de tratamiento (recopilación, grabación, organización, almacenamiento, adaptación, alteración, recuperación, consulta, etc.) ni en acciones que impliquen accesos no autorizados a plataformas digitales y consulta, alteración o extracción de los datos.

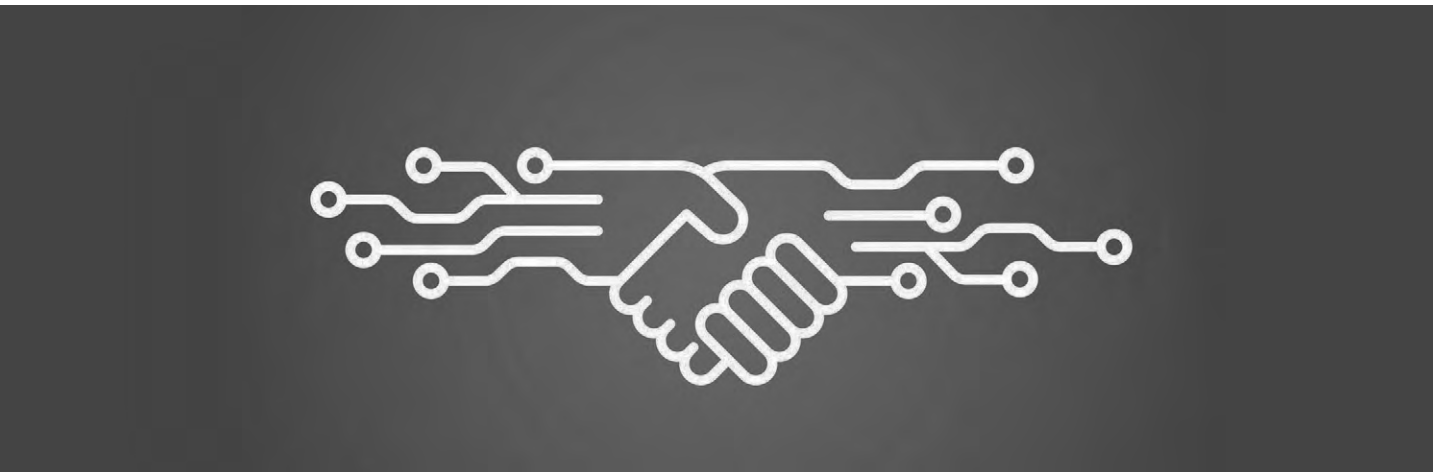
La carencia de estándares y el rol de las cortes y los jueces para determinar la responsabilidad en materia de seguridad de las plataformas digitales entre usuarios y propietarios obedece a que no existe un modelo

85 Incluye la introducción, alteración, eliminación y supresión de datos, así como la interferencia con el funcionamiento de un programa o sistema informático.

de gobernanza para la seguridad digital. Van Eeten (2017) documenta que la gobernanza de la seguridad ha pasado de los propietarios de dispositivos a los grandes intermediarios: es decir, los responsables de la seguridad sobre las plataformas ya no son los usuarios de los dispositivos de cómputo o nodos de información en la red, sino los desarrolladores de las plataformas como tal. Este cambio, generalmente, se asocia a beneficios como un control más centralizado sobre la seguridad de dispositivos y servicios, que llega a millones o incluso miles de millones de usuarios, de allí que también se generen economías de escala para suministrar servicios de seguridad.

Esta tendencia está impulsada por una racionalidad económica: reducción de costos de producción en los servicios digitales. La computación en la nube ofrece ganancias de eficiencia considerables en comparación con los consumidores y las empresas que poseen y mantienen su propia infraestructura digital. Además del costo, también hay una mayor confiabilidad: por ejemplo, Google es más competente para proteger la plataforma de Gmail que la mayoría de las empresas para proteger sus propios servidores de correo. En ese sentido, los Gobiernos encuentran más costo-eficiente acudir a estos grandes proveedores de servicios digitales para el correo, la computación en la nube y el resguardo de la información. Esto significa que el poder ha cambiado y seguirá pasando de los propietarios de los dispositivos a los operadores de la nube y a los proveedores de plataformas y dispositivos.

La OCDE (2011) se ha referido a estas empresas como intermediarias de internet. Sus prácticas de seguridad determinan cada vez más las de los Gobiernos y usuarios. El gran límite acá es que ni los Gobiernos ni la literatura en materia de seguridad digital encuentran una buena forma de evaluar lo que los grandes proveedores hacen. Los operadores de la nube, normalmente, no permiten auditar sus sistemas y servicios. Existe una asimetría de información fundamental, que impide acudir a evidencia sistemática para verificar cuáles modelos, prácticas y políticas son convenientes en la materia, a excepción del amparo de los datos personales y las leyes sobre protección de información sensible a la seguridad nacional de los países.



5.3. Riesgos en la tecnología *blockchain*: criptoactivos y monedas privadas

La tecnología *blockchain* tiene un potencial con respecto a la integridad pública (ver capítulo 4), gracias a que está basada en un protocolo de consenso distribuido y a que los registros que contiene quedan asegurados frente a posibles adulteraciones. De este modo, se genera confianza sobre la actividad y la seguridad de la generación de datos (Ko, Lee y Riu, 2018). Sin embargo, **la naturaleza descentralizada de esta tecnología también supone que los Gobiernos no son los únicos usuarios del blockchain, y que el sellado de datos y registros de utilidad pública no es su única aplicación posible.** Los privados están haciendo uso de esa misma tecnología para crear y poner en circulación los criptoactivos, lo cual genera algunos riesgos que deben ser considerados en materia de integridad.

> La ausencia de regulación nacional e internacional para la adopción de las tecnologías *blockchain* permite el desarrollo y expansión de criptoactivos sin controles estatales. Los criptoactivos son una forma de activo financiero digital, esto es, una representación digital de un valor que no ha sido emitido o garantizado por algún banco central o autoridad pública, y que no posee el estatus legal de moneda o dinero [...] Sin embargo, es aceptado como medio de intercambio por personas legales y jurídicas y pueden ser transmitidos, almacenados y comerciados por medios electrónicos[86] (Almeyda, 2020).

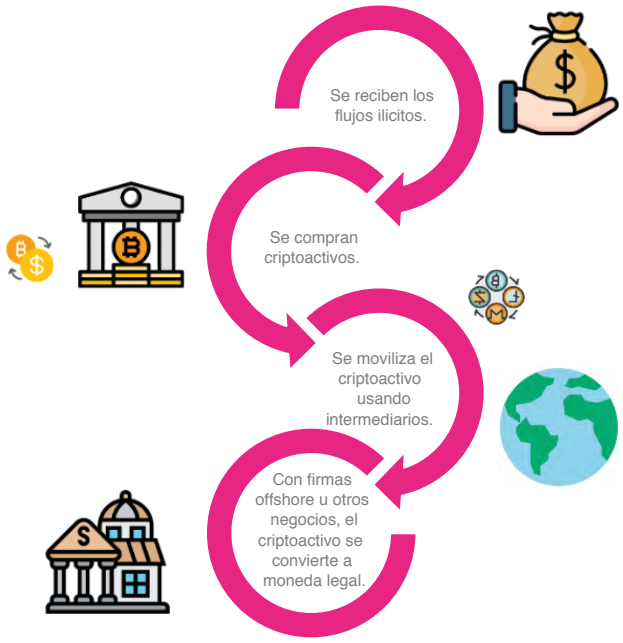
Dentro del actual ecosistema de innovación digital de la industria financiera como el **FinTech**[87], los criptoactivos corresponden a activos financieros digitales basados en principios de criptografía y tecnología *blockchain*[88], que posibilitan el desempeño de transacciones económicas seguras, descentralizadas y distribuidas. Por ende, es importante denotar que son un activo digital, el cual no es emitido por ninguna autoridad central (su emisión, de hecho, está abierta a cualquier persona que quiera desarrollar una), en el que se utilizan técnicas de encriptación para racionar la generación de unidades de moneda y verificar la transferencia de fondos.

[86] Definición que corresponde al regulador financiero alemán, Federal Financial Supervisory Authority, según Almeyda (2020).
[87] Para algunos observadores, el nuevo ecosistema FinTech podría reemplazar a los intermediarios tradicionales, por ejemplo, los bancos. Sin embargo, para otros expertos, los bancos e iniciativas FinTech tienen objetivos comunes y podrían complementar sus fortalezas (Arbache, 2020).
[88] La criptografía es utilizada en la tecnología blockchain. El hash, siendo el más utilizado, es un método para aplicar una función criptográfica a los datos, que identifica un mensaje de datos, de cualquier tamaño (por ejemplo, un archivo, texto o imagen). De manera general, permite individualizar el mensaje y, así, percibir si hubo variaciones; incluso el cambio más pequeño en la entrada (por ejemplo, un solo bit, una sola letra o una coma) dará como resultado un hash completamente diferente.

5.3.1. El cifrado en *blockchain* y su potencial para el lavado de activos

En los últimos años, las autoridades se han preocupado por el secretismo que implica el cifrado de las transacciones con criptoactivos, puesto que crea oportunidades para ocultar el origen y la propiedad de los fondos. En particular, las nuevas tecnologías *blockchain*, a través de los criptoactivos, podrían facilitar actividades de lavado de dinero a quienes lo obtienen de modo ilícito (por ejemplo, desde sobornos o desvío de fondos del Estado, hasta ingresos por tráfico de drogas). De acuerdo con la firma Chainalysis, especializada en criptografía forense, existe evidencia de redes de narcotráfico que convierten sus fondos en criptoactivos para luego enviarlos por todo el mundo y reconvertirlos en divisas. Según su último reporte, es difícil investigar esta actividad en casos individuales, así como capturar los recursos, porque cuando dichos fondos se convierten de monedas oficiales a criptoactivos en *blockchain*, no queda rastro de su origen.

Figura 5.6. Ilustración del lavado de dinero usando criptoactivos



Fuente: Elaboración propia.

El lavado de dinero es un delito intrínsecamente ligado con la corrupción. **Así como la tecnología blockchain puede ser una innovación digital para reducir la incidencia de la corrupción, también puede habilitarla a través**

de los criptoactivos, que se prestan fácilmente para que las redes criminales laven el dinero (ver figura 5.6). Chainalysis (2021) estima que los flujos ilícitos representaron el 0,34 % del volumen de transacciones de criptoactivos en 2020, en comparación con 2,1 % en 2019, ya que el nivel general de actividad criptográfica aumentó el año pasado. Aunque estas cifras puedan parecer insignificantes frente a las que se inyectan en el sistema financiero, el potencial de los criptoactivos para el lavado sigue presente y merece la atención de las autoridades reguladoras.

De hecho, ha surgido un grupo de empresas dedicadas a la analítica para ayudar a detectar actividades ilícitas en la industria. Pero, de acuerdo con el Financial Times, sus herramientas son más adecuadas para detectar delitos que tienen lugar en las propias cadenas de bloques, como robos, estafas y pagos de *ransomware*, que para cuantificar la cantidad de dinero proveniente de la comisión de delitos cometidos y que llega a los mercados de activos financieros digitales cifrados. En ese sentido, las cifras disponibles bien podrían estar subestimadas y el problema del lavado a través de criptoactivos quizás estaría creciendo en mayores proporciones.

5.3.2. Finanzas descentralizadas y la inaplicabilidad de las políticas de debida diligencia

El movimiento de los criptoactivos es posible gracias a la nueva industria dentro del entorno FinTech llamada DeFi (Decentralized Finance). Las plataformas DeFi buscan **reemplazar intermediarios financieros como bancos o corredores con contratos inteligentes**, comúnmente ejecutados en la *blockchain* Ethereum, que automatizaría la actividad del mercado. Aunque su estatus legal no es claro y sus estructuras varían, el atractivo de las plataformas DeFi es que reducirían los costos y acelerarían el comercio, utilizando activos financieros digitales. **La preocupación en materia de integridad es que el ecosistema DeFi compite y busca sustituir a las mismas entidades a las que los Gobiernos recurren para hacer cumplir las leyes antilavado** –banqueros, corredores y transmisores de dinero–, pero con la particularidad de que el ecosistema DeFi no proporciona servicio regulado alguno, puesto que no hace intermediación financiera y tampoco custodia fondos o dinero del público. Se trata, simplemente, de una **interfaz de código abierto** para que los usuarios interactúen con sus propios activos digitales.

De este modo, las plataformas del ecosistema DeFi no están obligadas, por ejemplo, a solicitar información sobre sus clientes ni a aplicar prácticas anti-

lavado como *Know Your Costumer* (o KYC). La obligación de KYC significa que los intermediarios deben conocer los nombres de sus usuarios, monitorear sus transacciones e informar a las autoridades sobre las actividades que generen sospechas de lavado de dinero o financiación de actividades terroristas. Además del desafío para la aplicación de la ley, algunos desarrolladores están trabajando para crear criptoactivos especialmente difíciles de rastrear, como **Monero, Zcash y Dash**, los cuales se conocen como *privacy coins*. Estos criptoactivos usan direcciones ocultas y crean nuevas direcciones para cada transacción. Condiciones de este tipo facilitan considerablemente el flujo de dineros de origen ilícito y la posibilidad de ocultarlos.

5.3.3. Mitigación de los riesgos del lavado: hacia una agenda regulatoria de los criptoactivos

El uso del blockchain para validar y encriptar transacciones con activos digitales ha tenido gran aceptación, al punto de que existen miles de criptoactivos disponibles en el mundo. La autoridad financiera de Nueva Zelanda estimó la existencia, en 2021, de **más de 4 000**, mientras que otras fuentes documentan **más de 6 000.** Debido a lo abierto que es el proceso de creación de estos productos, es relativamente fácil crear uno; aunque casi el 90 % del mercado total estaría concentrado en solo unos 20, como Bitcoin o Ethereum.

La apertura y descentralización subyacentes a los mecanismos de creación de criptoactivos y de desintermediación en el ecosistema DeFi genera una variedad de riesgos para la integridad de las operaciones económicas. Aunque no son objeto del presente estudio, deben considerarse para regular la adopción de la tecnología *blockchain* en la emisión de criptoactivos, así como en el uso de estos para desarrollar transacciones comerciales o financieras. Las monedas digitales han existido durante una década; sin embargo, los sistemas regulatorios que las gobiernan están muy fragmentados o son inexistentes. Ello permite que florezcan las actividades ilícitas, desde estafadores que «venden» Bitcoin y luego desaparecen con el efectivo sin agotar la compra, hasta el financiamiento del terrorismo y el lavado de dinero internacional (ver tabla 5.2).

Tabla 5.2. Riesgos de uso en los criptoactivos y el ecosistema DeFi

Pérdida de confianza		Los criptoactivos están sometidos a un alto grado de incertidumbre, pues no están respaldados por un banco central, una organización nacional o internacional, o activos u otro crédito. Además, su valor está estrictamente determinado por el valor que los participantes del mercado les asignan a través de sus transacciones. En consecuencia, un colapso de las actividades comerciales y una abrupta caída de valor puede significar una gran pérdida de confianza.
Riesgo cibernético o fraude		Los criptoactivos han atraído a redes criminales. Estos delincuentes pueden entrar en intercambios de cifrado, drenar carteras de cifrado e infectar computadoras individuales con malware que roba criptomonedas. A medida que las transacciones se realizan en internet, los piratas informáticos se dirigen a las personas, el manejo del servicio y las áreas de almacenamiento, a través de medios como la suplantación de identidad o el *phishing* y el *malware*.
Cumplimiento y reglamentación		Algunos países pueden impedir el uso de criptoactivos (como es el caso de China, que prohibió el uso del Bitcoin) o pueden afirmar que las transacciones infringen las regulaciones contra el lavado de dinero. Debido a la complejidad, la naturaleza descentralizada y al número significativo de participantes, dentro de los cuales encontramos remitentes, receptores (posiblemente lavadores de dinero), procesadores (plataformas de minería y comercio) y casas de cambio, no existe un único enfoque sobre el lavado de activos.
Mercado		Existe una cantidad finita de la moneda, lo que significa que puede sufrir problemas de liquidez, y la propiedad limitada puede hacerla susceptible a la manipulación del mercado. Además, dada su aceptación limitada y la falta de alternativas, la moneda puede parecer más volátil, impulsada por la demanda especulativa y exacerbada por el acaparamiento.

El desafío para los reguladores es encontrar instrumentos apropiados para abordar los riesgos que emanan de una mayor adopción de criptoactivos (Siwisa y Kern, 2021). Los instrumentos regulatorios existentes tienen limitaciones para abordar los riesgos de delitos financieros y de consumo, y de lavado de dinero. Por ejemplo, en una señal de avance sobre el

pensamiento regulatorio, el **Banco de Pagos Internacionales** (BPI)[89] declaró las criptomonedas como activos especulativos. Recomienda a las autoridades que primero deberían aclarar la clasificación regulatoria, basándose en las funciones económicas que se le otorguen al criptoactivo. Esto da forma a cuestiones como la protección del consumidor (cómo tratar los derechos de propiedad, el robo y la venta indebida); el uso minorista (quién puede comerciar legítimamente y en qué condiciones); el tratamiento como valores (instrumentos negociables utilizados para recaudar fondos al representar una promesa de pago en el futuro), y el tratamiento como activos genéricos (es decir, cosas tangibles o intangibles que se pueden poseer o controlar, por ejemplo, casas), entre otros aspectos.

En 2019, el Grupo de Acción Financiera (GAFI) introdujo directrices solicitando a los Gobiernos evaluar y mitigar los riesgos de lavado de activos y financiación del terrorismo asociados con las actividades de criptoactivos y los proveedores de servicios. Pidió que los proveedores de servicios estuvieran registrados y fueran supervisados por las autoridades nacionales competentes. Sin embargo, el GAFI informa que solo una cuarta parte de los países han adoptado dichas directrices y que algunas jurisdicciones cuentan con marcos contra el lavado de dinero usando criptoactivos, pero que los delincuentes podrían trasladarse rápidamente a países no regulados. El GAFI fomenta un mayor intercambio de información entre países respecto a operaciones financieras sospechosas con criptoactivos, lo cual es un reto, dado que es necesario eliminar el anonimato de las transacciones. Este último aspecto es justamente el atractivo de la tecnología *blockchain* y el cifrado en las monedas privadas.

[89] Establecido en 1930, el BPI es propiedad de 63 bancos centrales que representan a países de todo el mundo. Estos 63 países concentran alrededor del 95 % del PIB mundial. Su oficina central se encuentra en Basilea, Suiza y cuenta con dos oficinas de representación: Hong Kong y Ciudad de México. De América Latina, los bancos centrales de Argentina, Brasil, Chile, Colombia, México y Perú son accionistas. La misión del BPI es «apoyar la búsqueda de la estabilidad monetaria y financiera de los bancos centrales a través de la cooperación internacional y actuar como banco para los bancos centrales» (ver www.bis.org).

5.4. Reflexiones finales y recomendaciones

Las tecnologías digitales aplicadas a las políticas de integridad son un aliado invaluable para hacer más eficiente la lucha contra la corrupción. América Latina enfrenta retos sin precedentes en el marco de la emergencia sanitaria COVID-19: reducir la pobreza, las tensiones sociales y la desigualad, y promover un avance inclusivo para todos los ciudadanos. Ponerle un freno a la corrupción es indispensable para lograr los objetivos de la agenda de desarrollo, puesto que así se protegen los recursos públicos de intereses indebidos con el fin de asignarlos eficientemente a la provisión de bienes y servicios.

En este sentido, la incorporación de innovaciones digitales a las políticas de integridad pública exige la adopción de determinados mecanismos dentro de las mismas tecnologías. Es decir, así como se usan tecnologías digitales para la integridad, también existe una agenda de integridad para las mismas tecnologías y en su aplicación. Dicha agenda es considerable, si se tiene en cuenta que, solo desde el punto de vista tecnológico, se requiere que las plataformas desarrolladas cuenten con controles para verificar, por ejemplo, la veracidad de los datos que allí se procesan, o que existan protocolos de acceso y seguridad para autorizar operaciones sensibles a través de los sistemas de información.

En este apartado, tres áreas son de especial relevancia para salvaguardar la integridad en el desarrollo de las tecnologías, con un enfoque de mitigación de riesgos: (i) el fraude en la identidad digital; (ii) el uso indebido de datos personales, y (iii) el rol del blockchain en el desarrollo y expansión de los criptoactivos.

Es indispensable adoptar regulaciones para mitigar los riesgos que anteriormente no se consideraban prioritarios o relevantes, como la creación de identidades sintéticas por medios digitales o la emisión de monedas privadas digitales sin regulación alguna. Así como para Gutenberg habría sido muy difícil ver el potencial de su tecnología (*i. e.*, la imprenta) para impulsar la reforma protestante, hoy tampoco resulta fácil identificar cómo la aceleración digital afectará a instituciones como el Estado o el mercado, en particular si la adopción de innovaciones digitales para usos específicos como la lucha contra la corrupción tiene consecuencias diferentes a las originalmente concebidas en su diseño. A este respecto, algunos usos de las tecnologías podrían modularse para que no representen riesgos en el ecosistema de integridad.

- **La seguridad cibernética o informática es un importante desafío y un componente vital en la relación de confianza entre los ciudadanos y el Gobierno.** Las capacidades de ciberseguridad son determinantes a la hora de adoptar cualquier estrategia digital. Para ello, el análisis de los riesgos y amenazas antes de que ocurran es determinante, pues una vez los ciberdelincuentes atacan los sistemas, su recuperación demanda grandes recursos económicos, humanos y de tiempo. Adicionalmente, estos análisis deben ser periódicos, en la medida en que los riesgos pueden variar.

Es indispensable adoptar regulaciones para mitigar los riesgos que anteriormente no se consideraban prioritarios o relevantes, como la creación de identidades sintéticas por medios digitales o la emisión de monedas privadas digitales sin regulación alguna.

- **Los datos personales se pueden convertir en objeto de captura por redes de corrupción dentro de los Gobiernos, y del crimen organizado fuera de ellos.** Los ecosistemas de información contienen datos personales, frente a los cuales las agencias estatales deben garantizar privacidad y seguridad, lo cual implica la planificación, supervisión y control de la gestión de datos. Igualmente, es necesario adoptar un enfoque informado, basado en el riesgo, para confiar en los sistemas de identificación digital, con disposiciones de privacidad integradas.

- **Los estándares internacionales pueden servir como modelo para la creación de prácticas internas de administración de datos de identidad y acceso para individuos de acuerdo con sus roles**, con niveles de acceso de seguridad determinados para diferentes categorías de datos. De igual forma, pueden servir para mitigar los riesgos de delitos relacionados con la suplantación de identidad y la alteración de información, y para crear una confianza plena de los ciudadanos para interactuar en línea, pues sus datos personales solo serán accesibles para las entidades y fines autorizados.

- A modo enunciativo, pueden mencionarse los siguiente modelos: la **Resolución sobre Privacidad en la Era Digital**, adoptada por la Asamblea General de la ONU en 2018; las Directrices sobre la **Protección de la Privacidad y Flujos Transfronterizos** de Datos Personales de la OCDE de 2013; la Propuesta de Declaración de **Principios de Privacidad y Protección de Datos Personales** en las Américas, adoptada por el Comité Jurídico Interamericano de la OEA en 2012 y 2015, respectivamente; el Reglamento General de Protección de Datos de la UE (GDPR) de 2018, y la Ley de Privacidad del Consumidor de California (**CCPA**) de 2020.

- **Las redes de corrupción prosperan en un ecosistema interconectado por la tecnología digital, puesto que allí encuentra medios para movilizar dinero y ponerlo a salvo del imperio de la ley.** Los activos criptográficos basados en el desarrollo de las tecnologías *blockchain* significan que las autoridades tendrían dificultades para monitorear, detener o revertir las transacciones en esas vastas redes. El diálogo transfronterizo es imperativo, especialmente entre oficinas de tecnología y entre autorida-

des de inteligencia financiera, con el fin de reducir los riesgos de lavado de activos con escala transnacional.

- **La regulación ha respondido de modo muy lento frente a la aceleración digital.** Aunque los beneficios potenciales de *blockchain* ayudan a una mayor eficacia regulatoria como, por ejemplo, la adopción de políticas KYC (ver capítulo 4), esa misma tecnología permite ocultar transacciones en las redes de lavado de activos. En ese sentido, se requiere un enfoque regulatorio consistente para el uso de criptoactivos, alineando los criterios nacionales y otorgando un rol más preponderante a la regulación y la supervisión a nivel internacional, sin restringir la innovación. Para facilitar soluciones viables y un debate informado sobre la regulación de los activos financieros digitales basados en *blockchain*, también es necesario un diálogo estrecho y continuo entre los sectores público y privado.

6.

Recomendaciones de Política Pública

Recomendaciones de Política Pública

La aceleración digital que hoy experimenta el mundo es disruptiva, al menos, en tres aspectos: (i) el análisis de grandes conjuntos de datos con fines predictivos sobre fenómenos sociales es un hecho[90]; (ii) dichos ejercicios necesitan la concurrencia de varias disciplinas alrededor de la ciencia de datos para cumplir con su objetivo, y (iii) la funcionalidad predictiva de las tecnologías digitales no es su única virtud, sino que permiten también actuar de modo proactivo y preventivo frente a fenómenos indeseados como la corrupción.

El rol que las tecnologías basadas en datos tienen en materia de integridad pública es cada vez más reconocido por los Gobiernos, organismos multilaterales y sociedad civil. La prevención e investigación de fenómenos de corrupción pueden ser actividades más precisas y rápidas gracias a la aplicación de ciencia de datos o de tecnologías como el *blockchain* en la gestión de las entidades públicas.

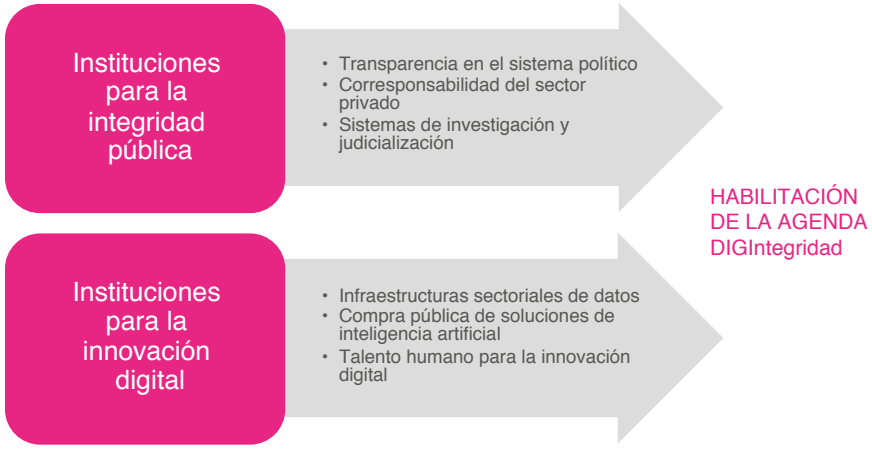
Sin embargo, la innovación digital, la aplicación de tecnologías basadas en datos y el gran poder de cómputo sobre los mismos no son una bala de plata para erradicar el problema de la corrupción. El contexto institucional y el marco de gobernanza que incluye aspectos como las relaciones entre el sector público y la empresa privada, y entre el Estado y la sociedad, son determinantes para que prosperen o no las redes de corrupción (CAF, 2019). En un entorno en donde las relaciones clientelares definen exclusivamente, y

[90] Esto no solo se aplica a fenómenos específicos de corrupción, como la suscripción indebida de contratos o el desvío de recursos públicos. Cetina (2021) suministra ejemplos de plataformas de inteligencia artificial que buscan predecir el crimen en zonas urbanas o la violación de leyes migratorias. Por otra parte, la industria de monetización de los datos personales (Zuboff, 2019) para propósitos de publicidad dirigida se basa en la predicción de comportamientos para consumir información.

por regla, si los bienes públicos se suministran o no, la innovación digital no podría contribuir para erradicar la corrupción.

Explotar al máximo el potencial de la digitalización en las políticas de integridad pública implica, por una parte, adoptar políticas de gestión de riesgos para que haya integridad en las mismas tecnologías, y, por otra, **exige modernizar las instituciones gubernamentales justamente en dos ámbitos, de modo separado: el de ajustes institucionales que promuevan la integridad, y el de adaptación de las autoridades públicas frente a la digitalización.** Dichos bloques se abordan en esta sección de recomendaciones de política pública para una implementación efectiva de las innovaciones digitales en materia de integridad pública.

Figura 6.1. Instituciones para la integridad y la innovación digital



6.1. Ajustes institucionales para la integridad en la era digital

América Latina tiene unos retos inmensos para adelantar reformas que sigan estándares internacionales en materia de prevención del soborno, del conflicto de interés y del abuso de la función pública para favorecer intereses privados (CAF, 2019; OCDE, 2017). Esos desafíos, sumados a que la apertura de datos e información aún necesita más desarrollo en el continente (Fumega, Scrollini y Zapata, 2021), crean limitaciones considerables para que la innovación digital contribuya efectivamente a la prevención de la corrupción.

Los enfoques tradicionales de lucha contra la corrupción, basados en creación de más normas punitivas que buscan sancionar delitos o faltas, han demostrado sus límites. Estas deben complementarse con normas e instituciones de tipo preventivo, que regulen algunos comportamientos en el servicio público y promuevan la corresponsabilidad con el sector privado en la política anticorrupción. La digitalización surge en este contexto como una alternativa adicional que permite facilitar la coordinación con el sector privado y la sociedad civil en la agenda de integridad pública.

Este informe ha mostrado cómo la ciudadanía, organismos de control, autoridades judiciales y entidades de la rama ejecutiva pueden concurrir a través de plataformas digitales y cooperar para prevenir fenómenos de corrupción. Adicionalmente, la aceleración digital está cambiando las reglas de juego en algunos procesos relacionados con la formulación e implementación de políticas públicas, como sucede con la telesalud, la teleducación y la justicia por vía remota, por lo que es importante que la agenda de integridad también se sintonice con dichos cambios.

América Latina necesita modernizar sus arreglos institucionales para que la agenda anticorrupción se sintonice con la aceleración digital y les permita a las tecnologías generar los dividendos de integridad. Garantizar un servicio público íntegro presupone regulaciones orientadas a generar estándares concretos de conducta. En la era digital, tanto los estándares de transparencia como su cumplimiento pueden registrarse masivamente en datos que hacen más efectivos y eficientes los ecosistemas de integridad. Este informe selecciona tres grupos estratégicos de recomendaciones para avanzar en la modernización institucional y en la agenda DIGIntegridad:

- **Transparencia en el sistema político:** las elecciones generan los primeros fenómenos de captura de los Estados por agentes corruptos, dada la necesidad de fondos para financiar las campañas políticas (CAF, 2019). La experiencia de grandes casos de corrupción en América Latina muestra que los acuerdos ilícitos se gestaron en la fase electoral.

- **Corresponsabilidad del sector privado:** las empresas privadas y la sociedad civil tienen fuertes incentivos para influir sobre las decisiones de la política pública. Adicionalmente, son actores importantes en los procesos electorales, al poder financiar campañas políticas. Su corresponsabilidad para generar integridad en las políticas públicas y evitar la captura del Estado debe ser parte de la estrategia de lucha contra la corrupción.

- **Sistemas de investigación y juzgamiento legítimos, ágiles y restaurativos:** en América Latina, resulta indispensable contar con una mayor capacidad de disuasión sobre los agentes corruptos a través de un sistema de justicia legítimo y que imponga sanciones efectivas. También, es determinante enfocar los procedimientos penales y disciplinarios hacia la recuperación de los recursos que se despilfarren o apropien, y a la reparación de las víctimas de la corrupción.

Transparencia en el sistema político

La transparencia en los procesos electorales no se restringe al conteo y escrutinio de votos. La integridad en este ámbito conlleva revelar información sobre la estructura corporativa de las campañas políticas, los montos de ingreso y gasto de las mismas, y la naturaleza de las personas naturales y jurídicas que financian las campañas, así como sus proveedores.

- **Los registros abiertos sobre los diferentes aspectos de la financiación de la actividad política deben someterse a estándares de transparencia activa (como pasa, por ejemplo, con la compra pública).** Los datos abiertos sobre la actividad de los partidos y movimientos políticos en época de elecciones son necesarios para hacer no solo la competencia electoral más transparente, sino para evitar captura temprana de intereses privados sobre la actividad política (CAF, 2019).

- Los datos de financiación de política y los de contratación pública pueden analizarse para encontrar relaciones y detectar posibles redes de corrupción entre financiación de campaña y contratación pública, una analítica de redes similar a la efectuada por la CGR en Colombia a través de la DIARI. Según un análisis presentado por la Misión de Observación Electoral (MOE), los donantes de campañas políticas reciben contratos multimillonarios después de que los candidatos financiados son elegidos, esto, a pesar de la existencia de expresas prohibiciones legales (MOE, 2018).

Las prácticas de uso de los datos y de medios digitales para movilizar campañas políticas también deben someterse a medidas de transparencia y escrutinio ciudadano, y de autoridades de vigilancia electoral.

- **La era digital también está modificando los procesos electorales, y requiere diseñar medidas de integridad para el uso de las nuevas tecnologías.** La adopción progresiva del voto electrónico o remoto plantea desafíos frente a la integridad y transparencia en el conteo y validación de los sufragios, en particular, porque la identidad digital debe tener robustos mecanismos de autenticación.

- **Las políticas de protección de los datos personales deben articularse con la integridad de las campañas electorales** para evitar, por ejemplo, iniciativas de publicidad dirigida, haciendo uso, no consentido por los ciudadanos, de datos originalmente recopilados para fines gubernamentales. Las prácticas de uso de los datos y de medios digitales para movilizar campañas políticas también deben someterse a medidas de transparencia y escrutinio ciudadano, y de autoridades de vigilancia electoral.

Corresponsabilidad del sector privado

Los intereses privados no son nocivos por sí mismos para la integridad pública; sí lo es ocultarlos y negociarlos en la sombra. La literatura en la materia reconoce que las políticas y los problemas públicos se forman en la arena política, que es donde confluyen los intereses públicos y los particulares (Dunn, 2018). Esa concurrencia es natural a la democracia y al Estado de derecho.

Es siguiendo ese principio que prácticas internacionalmente reconocidas en materia de integridad pública (OCDE, 2017) exigen **divulgar los intereses privados y trazar la línea punitiva con respecto a los medios usados para negociar los intereses.** Por ejemplo, se acepta el *lobby*, pero no el soborno; proyectos por iniciativa privada para las Asociaciones Público-Privadas (APP) en infraestructura, pero no la puerta giratoria para proponerlos y ejecutarlos.

- **América Latina necesita avanzar en la regulación del conflicto de interés[91] para los funcionarios públicos. Desarrollando marcos legales, creando órganos de aplicación y gestión de los conflictos, así como registros públicos de intereses y declaraciones patrimoniales** (CAF, 2019; De Michele y Dassen, 2018). Es importante que dichos registros estén en datos abiertos y tengan actualizaciones anuales disponibles para escrutinio y reutilización de diferentes instituciones y ciudadanos en el ecosistema de integridad.

- **Adicionalmente, se requiere un régimen de regulación del lobby o cabildeo, que permita llevar un registro público con la información**

[91] En términos generales, existe un conflicto cuando los intereses personales, laborales, económicos o financieros de una persona no pueden alinearse con las funciones del cargo que ejerce. Esto sucede porque los intereses personales podrían ir en contra del interés general (o colectivo) que se protege con el desempeño de sus deberes y responsabilidades oficiales.

corporativa de los cabilderos y sus clientes, y de las actividades de gestión de intereses de las personas naturales y jurídicas que se dedican al cabildeo (CAF, 2019; OCDE, 2021). Estos datos pueden ser de gran utilidad en la agenda de integridad. De un lado, la apertura de la información permite el escrutinio sobre el proceso de toma de decisiones públicas y las relaciones entre el sector privado y los funcionarios públicos. Igualmente, estos datos pueden ser usados con fines de analítica preventiva anticorrupción.

- **En el marco de la era digital, es importante que los Estados adopten esquemas de apertura para generar confianza sobre la toma de decisiones públicas.** En el proceso de aprobación de leyes, reglamentos o políticas, los esquemas organizados de desinformación por medio de redes sociales pueden entorpecer el interés público y posicionar agendas de grupos de interés limitado (OCDE, 2021), lo cual genera presión, mezclando presencia organizada tanto en medios digitales como en instancias de decisión política. Esto tiene el potencial de excluir por completo de las discusiones públicas a ciudadanos realmente afectados por ciertas disposiciones, lo que va en contra de los principios básicos de la participación democrática.

- **Finalmente, es importante avanzar en el desarrollo de un registro oficial de beneficiarios finales**[92]. CAF (2019) muestra que los Gobiernos de América Latina tienen deficiencias, incluso en la definición para efectos legales de lo que es un beneficiario final. Solo 5 de 26 países tienen una definición clara del concepto que, además, se ajusta a estándares del GAFI contra el lavado de dinero. La captura de la gestión del Estado por intereses privados se hace más factible cuando las personas naturales encuentran modos para ocultarse a través de vehículos corporativos para contratar con los Gobiernos, influir en las decisiones públicas e incluso incurrir deliberadamente en delitos como el lavado de activos. Los dividendos para los Gobiernos de contar con los registros de beneficiario final no solo ayudarían a evitar delitos relacionados con lavado de dinero, sino que podrían servir para hacer cumplir las normas tributarias y aumentar el recaudo de impuestos.

Sistemas de investigación y juzgamiento

Los procesos de investigación y sanción de la corrupción se pueden hacer mucho más efectivos gracias a las tecnologías digitales, que permiten recolectar, analizar y presentar datos sobre los riesgos y estructuras detrás de la corrupción de un modo rápido e intuitivo, sin perder información relevante (ver capítulo 3). Sin embargo, este potencial puede quedar perdido si

[92] Personas naturales que son los verdaderos dueños o controlantes, o quienes se benefician económicamente de un vehículo jurídico, como una sociedad mercantil, un fideicomiso, una fundación, etc.

los procesos judiciales o administrativos, en sus diferentes etapas, son lentos o complicados, o cuando las instituciones legales son manipuladas por los imputados para burlar el sistema de investigación y juzgamiento. Aunque el procedimiento penal en América Latina ha tenido en las últimas dos décadas unas reformas que pueden hacer más eficiente la justicia, estas medidas son más útiles para resolver casos de flagrancia u otros, donde los acuerdos de colaboración con las autoridades pueden lograrse rápidamente (CAF, 2019).

Es necesario fortalecer la formación y retención de talento que use efectivamente las tecnologías digitales en el ejercicio de funciones como la prevención, la investigación y la detección de la corrupción.

Los delitos de corrupción, en cambio, al pasar por ciertos protocolos para la recolección de evidencias y para la imputación ante los jueces, requieren un trabajo técnico articulado en el que concurren varias autoridades, lo cual hace lentos los procedimientos. Por ejemplo, para la extinción del dominio sobre bienes adquiridos ilícitamente, aun si las autoridades cuentan con la información y datos sobre los bienes que deben incautarse, se requiere una gran coordinación entre jueces, fiscales, Policía Judicial y otras autoridades competentes para agotar el procedimiento. Si dichos protocolos son complicados y toman mucho tiempo, el imputado puede insolventarse fácilmente[93], la justicia pierde su capacidad de disuasión, y se dilapidan los recursos o los medios económicos para reparar a las víctimas (incluso cuando estas sean las entidades del Estado).

Así como la digitalización por sí misma no hace más simples o eficientes los trámites (Roseth *et al.*, 2018), tampoco hace más efectiva la investigación o la judicialización de los hechos de corrupción. En tal sentido, se recomienda:

- **Con el fin de garantizar que los procesos contra los actores corruptos sean efectivos, simplificar los procedimientos y procesos de investigación, y fortalecer los organismos especiales para la lucha contra la corrupción.** Los términos de investigación, los recursos y herramientas con los que cuentan las autoridades judiciales y administrativas y los organismos de control deben ser lo suficientemente robustos para luchar con este fenómeno complejo y cambiante.

- **Promover el fortalecimiento de la coordinación de las autoridades judiciales y de organismos de control encargados de la agenda anticorrupción.** Una sola conducta corrupta puede dar lugar a diferentes procesos y regímenes de responsabilidad de los agentes estatales y privados involucrados. Con el fin de evitar la duplicación de esfuerzos, la dilación de los trámites y la impunidad y decisiones contradictorias frente a actores corruptos, el trabajo conjunto entre las autoridades es determinante.

- **Algo que podría contribuir a hacer más expedita y disuasiva la justicia es la delación compensada** (CAF, 2019). La negociación de las

93 Esto, en la era digital, pasaría, paradójicamente, gracias a las tecnologías que el mismo Gobierno habilita para agilizar trámites notariales, compraventa de inmuebles, traspasos de activos financieros y transacciones en el entorno FinTech, por citar solo algunos ejemplos.

penas a cambio de la confesión de los imputados y de su información sobre las redes criminales de las que hacen parte son un aliado invaluable para que la justicia aplique sanciones y desmantele las estructuras detrás de los fenómenos de corrupción. Es importante que dichas negociaciones también incluyan la entrega de información sobre los bienes, vehículos corporativos y otros activos adquiridos ilícitamente. De este modo, la justicia se vuelve disuasiva y restaurativa a la vez: reduce con su actuar los potenciales beneficios económicos de los corruptos y, también, puede recolectar bienes de valor económico para reparar a las víctimas de la corrupción.

6.2. Ajustes institucionales para la innovación digital en los Gobiernos

Las instituciones encargadas de la política anticorrupción no solo deben comprar o desarrollar soluciones digitales que faciliten su trabajo o lo hagan más efectivo, sino que deben contar con un ambiente que facilite la generación de soluciones innovadoras a los problemas propios de la prevención, investigación y detección de fenómenos de corrupción. Así como la locomotora requirió de ferrocarriles para mostrar su desempeño y generar aportes a la Revolución Industrial, los Gobiernos, en general, y las instituciones que luchan contra la corrupción, en particular, necesitan ajustar algunos aspectos de su entorno de innovación, antes de poner en marcha las tecnologías digitales para la integridad.

A este respecto, se requieren al menos las siguientes condiciones para facilitar la adopción de prácticas de innovación digital para las estrategias de integridad pública:

- **Infraestructuras organizadas de datos por cada sector de la gestión pública.** Puesto que los corruptos tienen estrategias diferentes y modalidades bien ajustadas al tipo de bien público que suministra el Estado (salud, educación, seguridad, justicia, infraestructura, etc.), los conjuntos de datos específicos a la gestión de cada sector aumentan la efectividad de las tecnologías digitales para la integridad.

- **Talento digital en los organismos responsables de la política anticorrupción.** La incorporación de tecnologías digitales en las estrategias de integridad pública da por sentados el conocimiento y la pericia de quienes las manejan y las utilizan. Este no siempre es el caso con los funcionarios públicos de América Latina, por lo que es necesario fortalecer la formación y retención de talento que use efectivamente las tecnologías digitales en el ejercicio de funciones como la prevención, la investigación y la detección de la corrupción. **La creación de unidades especializadas en ciencia e inteligencia de datos dentro de los organismos de control puede ayudar a resolver brechas digitales en el talento humano del ecosistema de integridad.**

- **Compra pública de inteligencia artificial.** Así como existen estándares especiales para garantizar la integridad y calidad en la contratación pública de infraestructura (Fajardo *et al.*, 2021), es igualmente estratégico para las entidades públicas desarrollar estándares especiales para la

estructuración de necesidades y procesos de abastecimiento de plataformas de inteligencia artificial con finalidades anticorrupción. Hay estándares de ética, así como de rendición de cuentas para esta tecnología, que influyen en su uso y calidad. Adicionalmente, las innovaciones digitales orientadas a mejorar los niveles de transparencia pueden ser compartidas y reutilizadas a través de código abierto por otras entidades públicas o la sociedad civil interesada en la lucha contra la corrupción.

Infraestructuras sectoriales de datos

En América Latina, persisten importantes retos en materia de calidad, utilidad y sostenibilidad de las iniciativas de datos abiertos de los Gobiernos relacionadas con integridad pública y prevención de la corrupción. Con la llegada de la pandemia, se volvió tangible la necesidad de tener la capacidad de aplicar políticas de datos para proteger el interés público. **En particular, es evidente la urgencia de adoptar prácticas ante las infraestructuras de datos en los siguientes frentes:**

- **Es necesario habilitar la interoperabilidad y vinculación de los datos mediante sistemas de gestión adecuados para administrar datos abiertos.** La interoperabilidad se relaciona con el uso de estándares para representar los datos, lo que significa que aquellos relacionados con las mismas cosas pueden reunirse fácilmente. La vinculación se relaciona con el uso de identificadores estándar dentro de un conjunto de datos, lo cual le permite a un registro conectarse a datos adicionales en otro conjunto (Coyle, Kay, Diepeveen, Tennison y Wdowin, 2020).

- **Dadas las especificidades sectoriales de la corrupción, es necesario mejorar los datos relevantes para prevenir la corrupción en estos sectores.** Aunque en materia de integridad ya se han definido los conjuntos de datos más estratégicos a través de iniciativas como el Programa Interamericano de Datos Abiertos (PIDA) (ver capítulo 1), es importante tener en cuenta que la corrupción también tiene una dimensión sectorial (Campos y Pradhan, 2007). Es decir, se presentan sutiles variaciones en la comisión de delitos o en la captura de instituciones y recursos públicos, según el sector que los corruptos busquen depredar. Puede que la captura de recursos en infraestructura sea más lucrativa a través de la contratación pública de grandes proyectos (CAF, 2019). Pero, en el sector de la salud, los delincuentes pueden considerar más lucrativo extraer recursos mediante la comisión de fraudes en los registros beneficiarios asegurados y servicios facturados.

En consecuencia, es importante que los Gobiernos definan infraestructuras de datos específicas para los sectores de la gestión pública, no solo con el propósito de una mejor administración y toma de decisio-

nes, sino para identificar con mayor precisión los riesgos de corrupción inherentes a cada uno. Puede ser que en el sector de infraestructura y obras públicas, los datos sobre proyectos de inversión y los contratos que los componen sean sumamente importantes en materia de integridad; pero quizás en el de salud, se requiera refinar la calidad de los datos sobre los reembolsos en el sistema de aseguramiento por servicios prestados.

Ees necesario que los Gobiernos adopten mecanismos de diálogo y cooperación regional e internacional que aseguren una estructura uniforme en los datos.

Asimismo, se deben fortalecer las respuestas coordinadas a través de una mejor interoperabilidad entre agencias gubernamentales y entre países, que posibilite una toma de decisiones más precisa, tanto a nivel global como nacional y local, para atacar las redes de corrupción. Con ese fin, es necesario que los Gobiernos adopten mecanismos de diálogo y cooperación regional e internacional que aseguren una estructura uniforme en los datos. Igualmente, la cooperación operativa permite que las experiencias (plataformas, aplicaciones, sistemas) se compartan con un formato de código abierto, que facilita el intercambio de información, comunicar acciones y discutir resultados. Esta cooperación ha sido impulsada entre las Contralorías de la región a través de la Organización Latinoamericana y del Caribe de Entidades Fiscalizadoras Superiores (OLACEFS) y la Organización Internacional de las Entidades Fiscalizadoras Superiores (INTOSAI).

Compra pública de inteligencia artificial

Las soluciones digitales que hacen uso de la IA para procesar los datos se enfrentan a una falibilidad inherente, que puede resumirse en la paradoja de Moravec[94]. Como consecuencia, en el desarrollo de la IA, la inversión de recursos para incrementar el poder de computación se enfoca en esos aspectos cognitivos sencillos que, si no son tenidos en cuenta, conducen a resultados imprecisos y sesgados (Cetina, 2021). La aplicación de soluciones de IA por parte de los Gobiernos pueden arrojar recomendaciones o predicciones imprecisas, en virtud de la falibilidad de esta tecnología. Adicionalmente, las soluciones de IA pueden entrar en conflicto con derechos fundamentales de los ciudadanos, sobre los que recaen las decisiones automatizadas de las plataformas (CAF, 2021; Cetina, 2021).

De manera general, cualquier estrategia gubernamental que se sustente en IA debe tener en cuenta las siguientes recomendaciones para el proceso de compra pública.

- **La compra pública responsable de tecnologías de IA comienza con una adecuada estructuración y planeación, que contempla esque-**

[94] Planteada de un modo informal, la paradoja propone que para las computadoras es muy fácil desarrollar tareas de razonamiento que los humanos encontramos muy complicadas (por ejemplo, calcular el logaritmo natural de 1 357); mientras que tareas cognitivas que para los humanos son sencillas (como reconocer un rostro humano) resultan muy difíciles para un computador.

mas de gobernanza de datos de obligatorio cumplimiento en los contratos con los proveedores. Los Gobiernos pueden encontrar más conveniente no hacerse cargo de desarrollar por sí mismos o *in-house* las soluciones de IA para prevenir la corrupción, sino comprarlas o pedir a privados que las desarrollen.

- **Los marcos que regulan las CPIA (compra pública de inteligencia artificial) deben incluir transparencia, así como aspectos de referencia común para la contratación, diseño, desarrollo y uso de sistemas basados en IA.** Igual que en grandes licitaciones como obras públicas o, en general, proyectos de alto impacto para el público, el uso estatal de los sistemas de inteligencia artificial debe regirse por estándares de contratación abierta, en el que se invita a todas las partes interesadas pertinentes a aportar, comentar y hacer control social sobre el proceso de compra pública, desde la estructuración de los términos de referencia hasta la entrega final del bien contratado, con un enfoque multidisciplinario (Consejo de Europa, 2019).

- **Tanto la planeación como la ejecución de la CPIA deben asegurar la participación de aquellos que han contribuido a la generación de datos o son afectados por las decisiones de los algoritmos.** En el caso de la lucha contra la corrupción, este desarrollo implicará adoptar mecanismos de diálogo entre entidades de la rama judicial, de inteligencia financiera, de la rama ejecutiva y de los organismos de control.

- **Deben incorporarse mecanismos de seguridad, confiabilidad, transparencia y explicabilidad, y adoptarse principios éticos en la estructuración de las compras públicas de las soluciones de IA (CAF, 2021).** Adicionalmente, deben existir procesos de rendición de cuentas y evaluación permanente de las plataformas y tecnologías digitales que gestionan datos con tecnologías de IA. Esto debe incluir medidas para garantizar la trazabilidad que documente los métodos para el entrenamiento de los algoritmos producidos; igualmente, los Gobiernos deben comunicar con claridad las características, limitaciones y posibles deficiencias del sistema de IA.

Talento humano para la era digital

- **Las innovaciones digitales y las técnicas de reutilización de los datos para mejorar la integridad pública exigen repensar las habilidades que se requieren de los funcionarios en las instituciones con competencias en la prevención, detección, investigación y sanción de la corrupción.** Impulsar exitosamente este proceso implica tener especialistas digitales dentro del elenco de los servidores públicos.

- Lo anterior no se restringe a contratar programadores, sino a **promover la concurrencia e interacción de equipos multidisciplinarios que incluyan abogados, científicos de datos, auditores e ingenieros, entre otros, y aprendan a reutilizar los datos y adoptar tecnologías digitales en el ejercicio de sus funciones.** De acuerdo con Ripani y Roseth (2021), en este ámbito, América Latina enfrenta grandes desafíos: el 51 % de los gerentes públicos reconoce tener un déficit severo o muy severo de habilidades de análisis de datos en sus equipos.

- En ese sentido, CAF (2021) propone que **las instituciones públicas adopten estrategias de desarrollo del equipo humano, partiendo de una medición de la preparación de los empleados públicos para utilizar las tecnologías digitales y acogerlas como herramientas útiles.** Tras esa medición, es necesario adoptar un plan de mejoramiento implementado en el marco de un proceso de manejo del cambio.

- **Para el ecosistema de integridad en concreto, este tipo de planes debe orientarse al desarrollo de una fuerza de trabajo con los perfiles y habilidades requeridos, que articule el uso de las tecnologías digitales con los procedimientos administrativos de prevención y vigilancia.** Para ello, es necesario contar con habilidades de adaptación permanente a los cambios esperados en la naturaleza de las tareas que se van a realizar, y desempeñarse satisfactoriamente en el nuevo entorno. Esto conlleva desarrollar habilidades blandas (aptitudes socio-personales) y duras (aptitudes especializadas o técnicas).

Los organismos encargados de la investigación y control de las actividades corruptas deberían contar con oficinas o unidades especializadas en ciencia e inteligencia de datos.

- **En particular, los auditores de contratos públicos deben saber consultar los datos de los portales de compra pública y apoyarse en las plataformas con el fin de identificar redes y patrones,** en lugar de solicitar carpetas y documentos para verificar la observancia de sellos, firmas y procedimientos. Esto también supone, por ejemplo, que aprendan y acudan a conceptos nuevos, como firma digital o autenticación por medios digitales (ver capítulo 5), que gradualmente simplifican los procesos burocráticos.

- **Los organismos encargados de la investigación y control de las actividades corruptas deberían contar con oficinas o unidades especializadas en ciencia e inteligencia de datos.** En 2020, la Procuraduría General de la Nación de Colombia creó la **Unidad de Gestión de Información e Inteligencia**. Dentro de sus funciones, se encuentra la de diseñar e implementar instrumentos que permitan contar con la información necesaria para identificar y gestionar riesgos de corrupción y de mala administración. En Perú, en 2021, en el marco de la **restructuración interna de la Contraloría General de República**, se creó la Subgerencia de Análisis de Datos, encargada, entre otras tareas, de formular políticas y estrategias en torno al almacenamiento y procesamiento de información para identificar riesgo en el uso de recursos públicos, y actos de corrupción.

- **Las instituciones internacionales pueden fomentar el intercambio de experiencias y buenas prácticas en el desarrollo de innovaciones digitales, en el marco de la agenda anticorrupción.** Organizaciones como la OLACEFS y la INTOSAI fomentan la cooperación entre los organismos de control en América Latina. Estas alianzas pueden expandirse a nivel global, gracias a la revolución digital.

REFERENCIAS

Aarvik, P. (2020). Blockchain as an anti-corruption tool. Case examples and introduction to the technology. *U4 Issue, 2020:7*. https://www.cmi.no/publications/7208-blockchain-as-an-anti-corruption-tool-case-examples-and-introduction-to-the-technology

Agencia EFE. (2020). Investigan un presunto hackeo de la división digital del Gobierno de Chile. https://www.efe.com/efe/america/economia/investigan-un-presunto-hackeo-de-la-division-digital-del-gobierno-chile/20000011-4368087

Agudelo, M. (2021). La economía y las industrias digitales basadas en el conocimiento. *Documentos de políticas para el desarrollo,* n.º 8. https://scioteca.caf.com/handle/123456789/1766

Aliyev, Z. y Safarov, I. (2019). *Logos, mythos and ethos of blockchain: An integrated framework for anti-corruption.* OECD Global Anti-Corruption & Integrity Forum.

Almeyda, N. (2020) Criptomonedas vs. criptoactivos: un problema de identidad con repercusiones jurídicas. Universidad Externado de Colombia. Tesis de Maestría en Derecho Económico con énfasis en Teoría del Derecho Económico y la Regulación. Recuperado de: https://bdigital.uexternado.edu.co/bitstream/handle/001/3591/GEADA-spa-2020-Criptomonedas_vs_criptoactivos_un_problema_de_identidad_con_repercusiones_juridicas?sequence=1&isAllowed=y

Andersen T. B.; Bentzen, J.; Dalgaard, C-J. y Selaya, P. (2011). Does the Internet Reduce Corruption? Evidence From U.S. States and Across Countries. World Bank Economic Review. 25(3): pp. 387-417.

Arbache, J. (2020). ¿Bancos o fintechs? CAF. Recuperado de: https://www.caf.com/es/conocimiento/visiones/2020/12/bancos-o-fintechs/

Ash, E.; Galletta, S. y Giommoni, T. (2020). *A Machine Learning Approach to Analyze and Support Anti-Corruption Policy.* WP Series ETH Zurich Center for Law & Economics.

Atencio, J. M. (2019). Los contratos inteligentes (*smart contracts*). En: Contract management/ compilado por Ricardo Antonio Parada; José Daniel Errecaborde. – 1.ª ed. - Ciudad Autónoma de Buenos Aires. Erreius. Errepar.

Atencio, J. M. (2020). Contratación pública y futuro: pensando en el *blockchain*. En: Temas de Derecho Administrativo – Erreius – Errepar.

Banco Mundial (2013). El registro de nacimientos: La llave para la inclusión social en América Latina y el Caribe. https://publications.iadb.org/es/publicacion/14834/el-registro-de-nacimientos-la-llave-para-la-inclusion-social-en-america-latina-y

Banco Mundial (2014). Digital Identity Toolkit. A guide for stakeholders in Africa. *World Bank*. https://openknowledge.worldbank.org/bitstream/handle/10986/20752/912490WP0Digit00Box385330B00PUBLIC0.pdf?sequence=1&isAllowed=y

Banco Mundial (2019). ID4D Practitioner's Guide (English). Identification for Development Washington, D.C.: World Bank Group. Recuperado de: http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide

Banco Mundial (2021). Global Identification Challenges by the Numbers. 2018 estimates. Recuperado de: https://id4d.worldbank.org/global-dataset/visualization

Bailard, C. S. (2009). Mobile phone diffusion and corruption in Africa. *Political Communication,* 26(3), pp. 333-353.

Banerjee, A.; Duflo, E.; Imbert, C.; Mathew, S. y Pande, R. (2020). E-governance, accountability, and leakage in public programs: Experimental evidence from a financial management reform in India. *American Economic Journal. Applied Economics,* 12(4), pp. 39-72.

Becker, G. S. y Stigler, G. J. (1974). Law enforcement, malfeasance, and compensation of enforcers. *The Journal of Legal Studies,* 3(1), pp. 1-18.

Beduschi, A. (2021). Rethinking digital identity for post-COVID-19 societies: Data privacy and human rights considerations. Data & Policy, 3, E15. doi:10.1017/dap.2021.15

BIS. (2001). *Customer Due Diligence for Banks, Basel Committee on Banking Supervision* (Bank for International Settlements). **http://www.bis.org/publ/bcbs77.pdf**

BIS. (2018). *BIS Annual Economic Report. V. Cryptocurrencies: Looking beyond the hype* (pp. 91-113).

Bjorkman, M. y Svensson, J. (2009). Power to the People: Evidence from a Randomized Field Experiment on Community-Based Monitoring in Uganda. *Quarterly Journal of Economics*, 124(2), pp. 735769.

Blockchain technology to prevent corruption in Covid-19 response: How can it help overcome risks? (s. f.). Cmi.No. Recuperado de: **https://www.cmi.no/publications/7259-blockchain-technology-to-prevent-corruption-in-covid-19-response-how-can-it-help-overcome-risks** (consulta realizada el 22 de octubre de 2021).

Blockchain, O. (s. f.). *OECD Blockchain Primer*. Secretary-General of the OECD. Recuperado de: **https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf** (consulta realizada el 9 de octubre de 2021).

Bojanic, D. y Madsen, E. (2014). *The Effect of Internet and Digital Media Freedom in Corruption*. **http://pure.au.dk/portal-asb-student/files/79187961/The_Effect_of_Internet_and_Digital_Media_Freedom_on_Corruption.pdf**

Bologna, J. (2014). Is the Internet an effective mechanism for reducing corruption experience? Evidence from a cross-section of countries. *Applied Economics Letters*, 21(10), pp. 687-691.

Bott, J. y Milkau, U. (2017). Central bank money and blockchain: A payments perspective. *Journal of Payments Strategy & Systems*, 11(2), pp. 145-157.

Brugués, F.; Brugués, J. y Giambra, S. (2018). *Political connections and misallocation of procurement contracts: Evidence from Ecuador*. **http://scioteca.caf.com/handle/123456789/1394**

CAF. (2019). RED 2019. Integridad en las políticas públicas: claves para prevenir la corrupción. Recuperado de: **http://scioteca.caf.com/handle/123456789/1503**

CAF. (2021a). *CAF promueve la transparencia y la rendición de cuentas en proyectos de infraestructura de Latinoamérica*. Caf.Com. **https://www.caf.com/es/actualidad/noticias/2021/05/caf-promueve-la-transparencia-y-la-rendicion-de-cuentas-en-proyectos-de-infraestructura-de-latinoamerica/**

CAF. (2021b) ExperiencIA: Datos e Inteligencia Artificial en el sector público. Recuperado de: **https://scioteca.caf.com/handle/123456789/1793**

Campos, J. y Pradhan, S. (2007). The Many Faces of Corruption: Tracking Vulnerabilities at the Sector Level. Washington, DC: World Bank. **https://openknowledge.worldbank.org/handle/10986/6848 License: CC BY 3.0 IGO.**

Cardona, D.; Cortés, J. y Wong, M. (2015). Diagnóstico de transparencia en municipios de Panamá. Estudio de caso de la segunda fase del programa de gobierno electrónico de la Organización de los Estados Americanos: municipios eficientes y transparentes. MuNet. *UPIICSA Investigación Interdisciplinaria*, 1(2), pp. 1-31.

Carvalho, R.; Marzagao, T.; Paula, E. y Ladeira, M. (2017). Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering. *15th IEEE International Conference on Machine Learning and Applications (ICMLA)*.

Castellón, P. y Velásquez, J. (2013). Characterization and Detection of Taxpayers with False Invoices using Data Mining Techniques. *Expert Systems and Applications*, 40(5), pp. 1427-1436.

Cetina, C. (2020a). *Blockchain e integridad: aplicaciones de política pública*. Caf.Com; CAF. https://scioteca.caf.com/handle/123456789/1651

Cetina, C. (2020b). *Tecnología para la integridad en tiempos del COVID-19*. Caf.Com; CAF. https://scioteca.caf.com/handle/123456789/1542

Cetina, C. (2020c). *Tres preguntas sobre el uso de los datos para luchar contra la corrupción*. Caf.Com; CAF. https://scioteca.caf.com/handle/123456789/1544

Cetina, C. (2021a). *Gobernanza de datos y capacidades estatales para la pospandemia*. Caf.Com; CAF. https://scioteca.caf.com/handle/123456789/1765

Cetina, C. (2021b). La aceleración digital de los Gobiernos e implicaciones de política pública. *Documentos de Políticas para el Desarrollo*, n.º 16. https://scioteca.caf.com/handle/123456789/1782

Cetina, C., Fonseca, H. y Zuleta, M. (2021). *Diagnóstico subregional de los datos del sistema de compra y contratación pública*. Organización de los Estados Americanos (OEA) y el Banco de Desarrollo de América Latina (CAF). http://ricg.org/wp-content/uploads/2021/05/Diagnostico-subregional-de-los-datos-del-sistema-de-compra-y-contratacion-publica.pdf

Cetina, C., Garay Salamanca, L. J., Salcedo-Albarán, E., y Vanegas, S. (2021). La analítica de redes como herramienta de integridad: el caso de la Procuraduría General de la Nación en Colombia. Caracas: CAF. Recuperado de: http://scioteca.caf.com/handle/123456789/1675

Chainalysis. (2021). The Chainalysis 2021 Crypto Crime Report.

Chêne, M. (2012). *Impact of community monitoring on corruption. U4 Anti-Corruption Resource*.

Chiesi, A. M. (2001). Network Analysis, Editor(s): Neil J. Smelser, Paul B. Baltes, *International Encyclopedia of the Social & Behavioral Sciences, Pergamon,* 2001, pp. 10499-10502, https://doi.org/10.1016/B0-08-043076-7/04211-X

Choi, J. W. (2014). E-Government and Corruption: A Cross-Country Survey. *World Political Science,* 10(2), pp. 217-236.

CIAT (2018) BLOCKCHAIN: Concepts and potential applications in the tax area. https://www.ciat.org/blockchain-concepts-and-potential-applications-in-the-tax-area-13/?lang=en

Consejo Europeo. (2020). Digital Solutions To Fight Covid-19. Data Protection Report. https://rm.coe.int/prems-120820-gbr-2051-digital-solutions-to-fight-covid-19-text-a4-web-/16809fe49c

Cong, L. W. y He, Z. (2018). *Blockchain Disruption and Smart Contracts*. National Bureau of Economic Research.

Cordova, Y. y Gonçalves, E. (2019) Rosie the Robot: Social accountability one tweet at a

time. Banco Mundial. https://blogs.worldbank.org/governance/rosie-robot-social-accountability-one-tweet-time

Cormen, T.; Leiserson, C.; Rivest, R. y Stein, C. (2001). Introduction to Algorithms (Segunda edición). MIT Press and McGraw-Hill

Corredor, O. (2018). *El PAE y la inasistencia escolar: el rol del tipo de contratación y la capacidad institucional del municipio*. Universidad del Rosario.

Coyle, D.; Kay, L.; Diepeveen, S.; Tennison, J. y Wdowin. J. (2020). The value of data - Policy Implications. Bennett Institute, University of Cambridge Open Data Institute. https://www.bennettinstitute.cam.ac.uk/publications/value-data-policy-implications/

Cruz, G. (2020). *GovTech y el futuro del Gobierno: el caso de Datasketch en Colombia*. Caf. Com; CAF. https://scioteca.caf.com/handle/123456789/1539

Csonka, P. (2006). The Council of Europe's Convention on Cybercrime and Other European Initiatives. *Revue Internationale de Droit Pénal, 77*(3), 473.

Datos Abiertos ChileCompra. (2021). Chilecompra.Cl. http://datosabiertos.chilecompra.cl

Datos básicos: La lucha contra la corrupción. (2021). Bancomundial.Org. https://www.bancomundial.org/es/news/factsheet/2020/02/19/anticorruption-fact-sheet

Davis, M.; Lennerfors, T.T. y Tolstoy, D. (2021). "Can blockchain-technology fight corruption in MNEs' operations in emerging markets?", *Review of International Business and Strategy*, Vol. ahead-of-print No. ahead-of-print. https://doi.org/10.1108/RIBS-12-2020-0155

De Michele, R. y Dassen, N. (2018). Conflicto de intereses: Desafíos y oportunidades para implementar un sistema efectivo de prevención y control. BID. http://dx.doi.org/10.18235/0001362

De Michele, R. y Pierri, G. (2020). *Transparencia y gobierno digital: El impacto de COMPR.AR en Argentina*. BID. http://dx.doi.org/10.18235/0002335

De Roux, D.; Pérez, B.; Moreno, A.; Villamil, M. y Figueroa, C. (2018). Tax Fraud Detections Using and Unsupervised Machine Learning Approach. *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining KDD '18.*

Deloitte. (2019). *Data governance has always been important, and a changing risk and regulatory landscape is accelerating the need for a strong, strategic program*. Deloitte. Com. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-rfa-data-governance-program-tmt-companies.pdf

Development Matters. (5 de agosto de 2021). *La digitalización como estrategia anticorrupción.* Oecd-Development-Matters.Org. https://oecd-development-matters.org/2021/08/05/la-digitalizacion-como-estrategia-anticorrupcion/

Digiampietri, L.; Trevisan, N.; Meira, L.; Jambiero, J.; Ferreira, C. y Kondo, A. (2008). *Uses of Artificial Intelligence in the Brazilian Customs Fraud Detection System*.

Digital Denmark – Experience Denmark's digitization. (s. f.). Digitaldenmark.Dk. Recuperado de: https://digitaldenmark.dk (consulta realizada el 22 de octubre de 2021).

Does the Internet reduce corruption? Evidence from US states and across countries. (2011). *The World Bank Economic Review.*

Domínguez, G. y Gerbasi, N. (2020). *Govtech y el futuro del gobierno: el ecosistema govtech en Brasil. Nuevas tecnologías y nuevas alianzas público-privadas para mejorar los servicios públicos*. http://scioteca.caf.com/handle/123456789/1582

Editorial La República S. A. S. (s. f.). *Delito de suplantación de identidad aumentó 409 % en 2020 debido a la pandemia*. Com.Co. Recuperado de: **https://www.asuntoslegales.com.co/actualidad/delito-de-suplantacion-de-identidad-aumento-409-en-2020-debido-a-la-pandemia-3151651** (consulta realizada el 22 de octubre de 2021).

e-Estonia — We have built a digital society and we can show you how. (Diciembre 10 de 2019). E-Estonia.Com. **https://e-estonia.com**

English, M.; Auer, S. y Domingue, J. (2015). *Block Chain Technologies & The Semantic Web : A Framework for Symbiotic Development.*

ESIP. (2018). *"E-SOCIAL SECURITY: ANTICIPATING THE FUTURE*. Esip.Eu. **https://esip.eu/images/pdf_docs/Scoping-paper-Workshop-1-Digital-tools-for-information-exchange.pdf**

Exploring blockchain technology for government transparency: Blockchain-based public procurement to reduce corruption. (s. f.). Weforum.Org. Recuperado de: **https://www.weforum.org/reports/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption** (consulta realizada el 22 de octubre de 2021).

Fajardo, G.; López, M.; Ramírez, A.; Román, C.; Silveira, A. y Zarama, D. (2021). *Gobernanza del sector de infraestructura y de las APP.* CAF. **https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html**

Fazekas, M. y Kocsis, G. (2020). Uncovering High-Level Corruption: Cross-National Objective Corruption Risk Indicators Using Public Procurement Data. British Journal of Political Science, 50(1), 155–164. **https://doi.org/10.1017/S0007123417000461**

Few, S. (2014). Data Visualization for Human Perception. En: The Encyclopedia of Human-Computer Interaction, 2nd Ed. INTERACTION DESIGN FOUNDATION.

FDA. (2020). *Blockchain Interoperability Pilot Project Report*. **https://www.merck.com/wp-content/uploads/sites/5/2020/07/FDA_DSCSA_Interoperability_Pilot_Project-Final_Report_Feb2020.pdf**

Fidler, B. (2017). Cybersecurity Governance: A Prehistory and its Implications. *Digital Policy Regulation and Governance*, 19(6), pp. 449-465.

FINRA. (2019). *Know Your Customer*. Finra.Org. **https://www.finra.org/rules-guidance/rulebooks/finra-rules/2090**

Freire, D.; Galdino, M. y Mignozzetti, U. (2020). Bottom-Up Accountability and Public Service Provision: Evidence from a Field Experiment in Brazil. *Research and Politics, 7*(2).

Fuente, G. (2014). El derecho de acceso a la información pública en América Latina y los países de la RTA: Avances y desafíos de la política. *En Transparencia & Sociedad.* Edición 2. **https://archives.cplt.cl/artic/20140701/asocfile/20140701161427/t_s_n2___web.pdf**

Garay, L. G.; Salcedo-Albarán, E. y Macías, G. (2018) Macrocorrupción y cooptación institucional: la red criminal "Lava Jato"

Garay, L. G.; Salcedo-Albarán, E. y Macías, G. (2021). Súper-red de corrupción en Venezuela.

Gallego, J. (2021). *Evidencia cuantitativa sobre el efecto de las iniciativas de gobierno digital en el fenómeno de la corrupción.*

Gallego, J.; Maldonado, S. y Trujillo, L. (2020). From Curse to Blessing: Institutional Reform and Resource Booms in Colombia. *Journal of Economic Behavior & Organization*, 178, pp. 174-193.

Gallego, J.; Rivero, G. y Martínez, J. (2021). Preventing rather than Punishing: An Early Warning System of Malfeasance in Public Procurement. *International Journal of Forecasting*, 37(1), pp. 360-377.

Gelb, A. y Clark, J. (2013). "Identification for Development: The Biometrics Revolution". Working Paper 315, Center for Global Development, Washington, DC.

Gigler, S. y Bailur, S. (2014). Closing the Feedback Loop: Can Technology Bridge the Accountability Gap? *Directions in Development--Public Sector Governance*;. Washington, DC: World Bank. https://openknowledge.worldbank.org/handle/10986/18408

Goede, M. (2019). E-Estonia: The E-Government Cases of Estonia, Singapore, and Curaçao. *Archives of Business Research*, 7(2). https://doi.org/10.14738/abr.72.6174

González, V. (s. f.). MuniDigital wants to be the "Spotify" of the Smart Cities. The Smartcity Journal. Recuperado de: https://www.thesmartcityjournal.com/en/sustainability/munidigital-wants-to-be-the-spotify-of-the-smart-cities

Grace, E.; Rai, A.; Redmiles, E. y Ghani, R. "Detecting fraud, corruption, and collusion in international development contracts: The design of a proof-of-concept automated system", 2016. IEEE International Conference on Big Data, Washington, DC, 2016, pp. 1444-1453.

Graglia, J. M. y Mellon, C. (2018). Blockchain and Property in 2018: At the End of the Beginning. *Innovations Technology Governance Globalization,* 12(1–2), pp. 90-116.

Granados, R. y Rodríguez, J. (2013). *Publicidad y transparencia en la actividad contractual de las administraciones públicas*.

Haafst, R. (2017). *On The Effect of Digital Transformation on Corruption: An inter-country analysis*. Unpublished. https://doi.org/10.13140/RG.2.2.10163.43044

Haber, S. y Stornetta, W. S. (1991). How to Time-Stamp a digital document. *Journal of Cryptology* 3, pp. 99-111. https://doi.org/10.1007/

Heller, N. (2017). *Estonia, the Digital Republic*.

Houlder, V. (2017). Ten ways HMRC can tell if you're a tax cheat. En: Financial Times. Diciembre 2017. https://www.ft.com/content/0640f6ac-5ce9-11e7-9bc8-8055f264aa8b

ID4D Practitioner's Guide (English). Identification for Development Washington, D.C. (2019). Worldbank.Org. http://documents.worldbank.org/curated/en/248371559325561562/ID4D-Practitioner-s-Guide

ILDA. (2020). *Barómetro Regional de Datos Abiertos para América Latina y el Caribe 2020*. https://barometrolac.org/wp-content/themes/odbpress/reporte-ILDA-ES.pdf

Insurance Information Institute. (s. f.). *Facts + Statistics: Identity Theft and Cybercrime*. Iii.Org. Recuperado de: https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (consulta realizada el 22 de octubre de 2021).

International Monetary Fund. Legal Dept. (2018). Colombia: Financial Sector Assessment Program – Detailed Assessment Report on Anti-Money Laundering and Combating the Financing of Terrorism. *IMF Staff Country Reports,* 18(314), p. 1.

Interpol. (2020). *Shift in targets from individuals to governments and critical health infrastructure*. https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19

Irwin, L. (2021). *Personal data vs. sensitive data: what's the difference?* https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data

Keefer, P. y Roseth, B. (2021). *Grand Corruption in the Contracting Out of Public Services: Lessons from a Pilot Study in Colombia*. IDB Working Paper Series.

Kelsen, H. (1949). *Teoría General del Derecho y del Estado*. Harvard University Press.

Kelsen, H. (2017). *General theory of law & state* (Hans Kelsen & A. J. Treviño, Eds.). Routledge.

Ko, T.; Lee, J. y Ryu, D. *Blockchain Technology and Manufacturing Industry: Real-Time Transparency and Cost Savings,* 10 Sustainability (Basel, Switzerland) 4274 (2018), available at **https://search.datacite.org/works/10.3390/su10114274**.

Koch, R. (2019, February 1). *What is considered personal data under the EU GDPR?* Gdpr.Eu. **https://gdpr.eu/eu-gdpr-personal-data/**

Kofax. (2020). *Global E-Signature Law: Best Practices for Assessing Risk*. **https://ordiginal.com/wp-content/uploads/2020/10/eb_global-e-signature-law_en.pdf**

KPMG. (2016). *New Electronic Tax Payment System Requirements*. **https://assets.kpmg/content/dam/kpmg/pdf/2016/06/id-kai-tax-news-flash-january-2016-electronic-tax-payment.pdf**

Laajaj, R.; Eslava, M. y Kinda, T. (2019). The costs of bureaucracy and corruption at customs: Evidence from the computerization of imports in Colombia. *SSRN Electronic Journal*. **https://doi.org/10.2139/ssrn.3334529**

Latin American Countries Encouraged to use KYC processes. (19 de marzo de 2019). *AU10TIX*. **https://www.au10tix.com/BLOG/LATIN-AMERICAN-COUNTRIES-ENCOURAGED-TO-USE-KYC-PROCESSES/**

Lauletta, M.; Rossi, M.; Cruz, J. y Arisi, D. (2019). *Monitoreando la inversión pública. El Impacto de MapaRegalías en Colombia*. BID.

Lewis-Faupel, S.; Neggers, Y.; Olken, B. A. y Pande, R. (2016). Can electronic procurement improve infrastructure provision? Evidence from public works in India and Indonesia. *American Economic Journal. Economic Policy*, 8(3), pp. 258-283.

Lizardo, R. (2018). *Gobierno electrónico y percepción sobre la corrupción. Un estudio comparativo sobre su relación en los países de Latinoamérica*. Universidad Complutense de Madrid.

Llinás, R. (2003). *El cerebro y el mito del yo*. Grupo Editorial Norma, Bogotá.

López Azumendi, S.; Facchina, M. y Zapata, E. (2021) Liderazgo público y participación privada y de ciudadanos: la transformación digital de la ciudad de Córdoba en Argentina. Policy Brief;24, Caracas: CAF. Recuperado de: **http://scioteca.caf.com/handle/123456789/1699**

Manual de Contrataciones Abiertas para el Estándar de Datos sobre Infraestructura — documentación de Open Contracting for Infrastructure Data Standards Toolkit - 0.9.3. (s. f.). Open-Contracting.Org. Recuperado de: **https://standard.open-contracting.org/infrastructure/latest/es/** (consulta realizada el 22 de octubre de 2021).

Makridakis, S. y Christodoulou, K. (2019). Blockchain: Current Challenges and Future Prospects/Applications. Future Internet. 11. 258. 10.3390/fi11120258.

Margetts, H. (2017). *In a digital society, governments should innovate with the best of them*. Foro Económico Mundial. **https://www.weforum.org/agenda/2017/02/digital-government-innovate-helen-margetts/**

Meeting new expectations. (27 de marzo de 2015). Deloitte.Com. **https://www2.deloitte.com/tr/en/pages/financial-services/articles/dcfs-know-your-customer.html**

Mendling, J.; Weber, I.; Aalst, W. V. D.; Brocke, J. V.; Cabanillas, C.; Daniel, F.; Debois, S.; Ciccio, C. D.; Dumas, M.; Dustdar, S.; Gal, A.; García-Bañuelos, L.; Governatori, G.; Hull, R.; Rosa, M. L.; Leopold, H.; Leymann, F.; Recker, J.; Reichert, M.; … Zhu, L. (2018). Blockchains for business process management – Challenges and opportunities. *ACM Transactions on Management Information Systems, 9*(1), pp. 1-16.

Miembros - Open Government Partnership. (1.º de marzo de 2019). Opengovpartnership.org. https://www.opengovpartnership.org/es/our-members/

MOE. (2018). Misión de Observación Electoral. *Democracias empeñadas. De financiadoras privadas a contratistas públicos.* Bogotá: Colombia. https://www.moe.org.co/publicacion/democracias-empenadas/

Moreno, A. y Teigland, R. (2018). *Blockchain, in The Rise and Development of FinTech 276* (Anonymous 1st).

Munidigital. (2021). *Experiences*. Munidigital.Tech. https://en.munidigital.tech/case-studies

Muralidharan, K.; Niehaus, P. y Sukhtankar, S. (2016). Building State Capacity: Evidence from Biometric Smartcards in India. *American Economic Review*, 106(10), pp. 2895-2929.

Muralidharan, K.; Niehaus, P. y Sukhtankar, S. (2020). Identity Verification Standards in Welfare Programs: Experimental Evidence from India. *NBER Working Paper, 26744.*

Muralidharan, K.; Niehaus, P.; Sukhtankar, S. y Weaver, J. (2021). Improving Last-Mile Service Delivery Using Phone-Based Monitoring. *American Economic Journal: Applied Economics*, 13(2), pp. 52-82.

Naciones Unidas. E-Gobierno Encuesta 2020*. Gobierno digital en la década de acción para el desarrollo sostenible*. (2020). Publicadministration.Un.Org; Departamento de Asuntos Económicos y Sociales de la ONU. https://publicadministration.un.org/egovkb/Portals/egovkb/Documents/un/2020-Survey/2020%20UN%20E-Government%20Survey%20(Spanish%20Edition).pdf

Nakamoto, S. y bitcoin.org, W. (s. f.). *Bitcoin: A peer-to-peer electronic cash system*. Bitcoin.Org. Recuperado de: https://bitcoin.org/bitcoin.pdf (consulta realizada el 22 de octubre 2021).

Naudé, W. (2020). *Artificial intelligence versus COVID-19 in developing countries: Priorities and trade-offs*. UNU-WIDER.

Niforos, M.; Ramachandran, V. y Rehermann, T. (2017). *Block Chain: Opportunities for Private Enterprises in Emerging Market*. International Finance Corporation.

Nuffield Council on Bioethics. (2020). *Beyond the exit strategy: ethical uses of data-driven technology in the fight against COVID-19*. https://www.nuffieldbioethics.org/publications/covid-19/webinar-beyond-the-exit-strategy-ethical-uses-of-data-driven-technology-in-the-fight-against-covid-19

OCDE. (2003). *OECD E-Government Flagship Report "The E-Government Imperative"*. Public Management Committee.

OCDE. (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD Publishing.

OCDE. (2016). Gobierno digital. En *Políticas de banda ancha para América Latina y el Caribe: Un manual para la economía digital*. OECD Publishing. https://doi.org/10.1787/9789264259027-15-es.

OCDE. (2017). SPECIAL FEATURE: Electronic services in tax administration. En *Revenue Statistics in Asian Countries 2017: Trends in Indonesia, Japan, Kazakhstan, Korea, Malaysia, the Philippines and Singapore.* OECD Publishing. https://doi.org/10.1787/9789264278943-4-en.

OCDE. (2019a). *Digital Government in Chile – Digital Identity*. OECD Digital Government Studies.

OCDE. (2019b). E-procurement to strengthen transparency and develop performance evaluation of public procurement in Kazakhstan. En *OECD Public Governance Reviews* (pp. 73-102). OCDE.

OCDE. (2019c). *Is there a role for blockchain in responsible supply chains?*

OCDE. (2019d). Aid by DAC members increases in 2019 with more aid to the poorest countries. **https://www.oecd.org/dac/financing-sustainable-development/development-finance-data/ODA-2019-detailed-summary.pdf**

OCDE. (2020). *Covid-19 en América Latina y el Caribe: Panorama de las respuestas de los gobiernos a la crisis.* OECD Publishing.

OCDE. (2021). *Guía de la OCDE sobre gobierno abierto para funcionarios públicos peruanos - OCDE*. **https://www.oecd.org/gov/open-government/guia-de-la-ocde-sobre-gobierno-abierto-para-funcionarios-publicos-peruanos.htm**

Olken, B. A. (2007). Monitoring corruption: Evidence from a field experiment in Indonesia. *The Journal of Political Economy*, 115(2), pp. 200-249.

Open contracting for infrastructure data standards toolkit — Open contracting for infrastructure data standards toolkit 0.9.3 documentation. (s. f.). Open-Contracting.Org. Recuperado de: **https://standard.open-contracting.org/infrastructure/latest/en/** (consulta realizada el 22 de octubre de 2021).

OpenDataCharter. (2015). *Carta Internacional de Datos Abiertos*. **https://opendatacharter.net/principles-es/**

Ortega, D. (2019). 5 grandes preguntas sobre Big Data y Evaluación de Impacto. CAF. **https://www.caf.com/es/conocimiento/visiones/2019/03/5-grandes-preguntas-sobre-big-data-y-evaluacion-de-impacto/**

Padilla, J. (2020). Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos. *Revista de Derecho Privado*, 39, pp. 175-201.

Paula, E. L.; Ladeira, M.; Carvalho, R. y Marzagao, T. (2017). "Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering," 15th IEEE International Conference on Machine Learning and Applications (ICMLA).

Peixoto, T. C.; Sifry, M. L.; Mellon, A. J. y Sjoberg, F. M. (s. f.). *Civic tech in the global south: Assessing technology for the public good*. World Bank Group. **http://documents.worldbank.org/curated/en/717091503398213001/Civic-tech-in-the-global-south-assessing-technology-for-the-public-good**

Peixoto, T. y Fox, J. (2016). *When Does ICT-Enabled Citizen Voice Lead to Government Responsiveness? WDR 2016 Background Paper*. Banco Mundial, Washington. **https://openknowledge.worldbank.org/handle/10986/23650 License: CC BY 3.0 IGO**

Peixoto, T. y Sifry, M. L. (2017). *Civic Tech in the Global South: Assessing Technology for the Public Good.* World Bank and Personal Democracy Press. **https://openknowledge.worldbank.org/handle/10986/27947** License: CC BY 3.0 IGO

Persson, A.; Rothstein, B. y Teorell, J. (2013). Why Anticorruption Reforms Fail – Systemic Corruption as a Collective Action Problem. *Governance*, 26(3), pp. 449-471.

Pring, C. y Vrushi, J. (2019). *Barómetro Global de la corrupción en América Latina y el Caribe 2019 – Opiniones y experiencias de los ciudadanos en materia de corrupción* (Transparencia Internacional). **https://transparenciacolombia.org.co/wp-content/uploads/gcb-lac-report-web.pdf**

Puertas, A. M. y Teigland, R. (2018). Blockchain. En *The Rise and Development of FinTech* (pp. 276-308). Routledge.

Puthal, D.; Malik, N.; Mohanty, S. P.; Kougianos, E. y Das, G. (2018). Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consumer Electronics Magazine*, 7(4), pp. 6-14.

PwC. (2020). *Fighting fraud: A never-ending battle. PwC's Global Economic Crime and Fraud Survey*. https://www.pwc.com/gx/en/forensics/gecs-2020/pdf/global-economic-crime-and-fraud-survey-2020.pdf

Ramachandran, V. y Rehermann, T. (2017). *Can blockchain technology address DE-risking in emerging markets?* International Finance Corporation, Washington, DC.

RAMCC (2020). Paraná aplicará el software MuniArbol para registro y control del arbolado. Red Argentina de Municipios frente al Cambio Climático. Recuperado de: https://ramcc.net/noticia.php?id=1075

Raskin, M. (2017). The Law and Legality of Smart Contracts, *Georgetown Law Technology Review*, 2017, 1 Geo. L. Tech. Rev. Recuperado de: https://georgetownlawtechreview.org/wp-content/uploads/2017/05/Raskin-1-GEO.-L.-TECH.-REV.-305-.pdf

Right to Information. (2019). *Global Right to Information Rating Map*. Global Right to Information Rating. https://www.rti-rating.org

Rincón, E. (2020). *Derecho del comercio electrónico y de internet* (1.ª edición). Tirant lo Blanch.

Rincón, E. (2021). *El desarrollo jurídico de Fintech. Las bases regulatorias de la Tecnología Financiera.* Tirant lo Blanch.

Ripani, L. y Roseth, B. (2021). ¿Qué significa el «futuro del trabajo» para los servidores públicos de América Latina y el Caribe? BID. https://blogs.iadb.org/trabajo/es/futuro-del-trabajo-para-los-servidores-publicos/

Romeu, J. y Rodríguez, J. (2013). *Publicidad y transparencia en la actividad contractual de las administraciones públicas.* https://doi.org/0.13140/2.1.4309.2801

Rosati, P. y Cuk, T. (2019). Blockchain Beyond Cryptocurrencies. In *Disrupting Finance* (pp. 149-170). Springer International Publishing.

Roseth, B.; Reyes, A. y Santiso, C. (2018). *Wait No More: Citizens, Red Tape and Digital Government*. Banco Interamericano de Desarrollo. https://publications.iadb.org/en/wait-no-more-citizens-red-tape-and-digital-government-executive-summary

Roseth, B.; Reyes, A. y Yee Amézaga, K. (2021). *Servicios públicos y gobierno digital durante la pandemia: perspectivas de los ciudadanos, los funcionarios y las instituciones públicas.* Banco Interamericano de Desarrollo. http://dx.doi.org/10.18235/0003122

Rossi, M.; Vásquez, A., y Cruz, J. (2020). *Divulgación de información y desempeño de la inversión pública: el caso de Costa Rica*. BID.

Rudin, C. (2012). Prediction: Machine Learning and Statistics. Spring. MIT OpenCourseWare, https://ocw.mit.edu. License: Creative Commons BY-NC-SA.

Ryvkin, D.; Serra, D. y Tremewan, J. (2017). I paid a bribe: An experiment on information sharing and extortionary corruption. *European Economic Review*, 94, pp. 1-22.

Santiso, C. (2020) El papel del Estado en la era digital post COVID-19. Recuperado de: https://www.caf.com/es/conocimiento/visiones/2020/08/el-papel-del-estado-en-la-era-digital-post-covid19/

Santiso, C. (27 de febrero de 2019). *Tecnología de integridad: tres formas en que los gobiernos pueden utilizar la tecnología para acabar con la corrupción*. apolitical. Recuperado de: https://apolitical.co/solution-articles/es/tecnologia-de-integridad-interrumpir-la-corrupcion

Santiso, C. (agosto de 2021). *La digitalización como estrategia anticorrupción.* Recuperado de:

Santiso, C. y Ortiz de Artiñano, I. (2020). Govtech y el futuro gobierno. Caracas: CAF y PublicTechLab de IE University de España. Recuperado de: http://scioteca.caf.com/handle/123456789/1645

Santiso, C. y Ortiz, I. (2020). Govtech y el futuro gobierno. Caracas: CAF y PublicTechLab de IE University de España. Recuperado de: http://scioteca.caf.com/handle/123456789/1645

Seco, A. (n. d.). *BLOCKCHAIN: Concepts and potential applications in the tax area (1/3)*. Ciat. Org. Recuperado de: https://www.ciat.org/blockchain-concepts-and-potential-applications-in-the-tax-area-13/?lang=en (consulta realizada el 22 de octubre de 2021).

Seco y Muñoz. (2018). Panorama del uso de las tecnologías y soluciones digitales innovadoras en la política y la gestión fiscal. Documento de trabajo, Washington, D.C.: IDB. Disponible en: https://publications.iadb.org/publications/spanish/ document/Panorama-del-uso-de-las-tecnolog%C3%ADas-y-soluciones-digitales-innovadoras-en-la-pol%C3%ADtica-y-la- gesti%C3%B3n-fiscal.pdf

Shang, Q. y Price, A. (2019). A blockchain-based land titling project in the Republic of Georgia. Innovations: Technology, Governance, Globalization, MIT Press, vol. 12(3-4), pp. 72-78, Winter-Sp. https://ideas.repec.org/a/tpr/inntgg/v12y2019i3-4p72-78.html

Sheffer, A.; Pizzigatti, P y Soares, F. (2014). "Transparency Portals versus Open Government Data. An Assessment of Openness in Brazilian Municipalities," Proceedings of the 15th Annual International Conference on Digital Government Research.

Sheth, H. y Dattani, J. (2019). Overview of blockchain technology. *Asian Journal of Convergence in Technology*, 05(01), pp. 1-4.

Simon, C. y Blume, L. (1994) Mathematics for economists. W.W. Norton & Company Inc. New York.

Solon, L.; Rigitano, H.; Carvalho, R. y Souza, J. (2016). "Bayesian Networks on Income Tax Audit Selection. A Case Study of Brazilian Tax Administration. BMA@UAI, pp. 14-20.

Sooväli-Sepping, H. (Ed.). (2020). *Informe sobre desarrollo humano de Estonia 2019/2020*. https://inimareng.ee/en/info.html

Strusani, D. y Houngbonon, G. V. (2019). The Role of Artificial Intelligence in Supporting Development in Emerging Markets. EMCompass,no. 69;. International Finance Corporation, Washington, DC. https://openknowledge.worldbank.org/handle/10986/32365

Superintendencia Financiera de Colombia, Circular Externa 027 de 2020.

Szabo, N. (1996) Smart Contracts: Building Blocks for Digital Markets https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html

Thackeray, J. (2019). *What are the Inherent Risks Associated with Cryptocurrency?* https://support.niftys.com/hc/en-us/articles/4405752761115-What-are-the-risks-with-buying-selling-NFTs-

The World Wide Web Foundation. (2018). *Open Data Barometer.* Leaders Edition. From Promises to Progress. Washington DC: World Wide Web Foundation. Recuperado de: https://opendatabarometer.org/doc/leadersEdition/ODB-leadersEdition-Report.pdf

Tiatasin, K. "IT Risk Management for E-Government Implementation Success" N.A. http://www.jba.tbs.tu.ac.th/files/Jba135/Article/JBA135KrongSiri.pdf

Transparencia Internacional. (2017). *Las personas y la corrupción. América Latina y el Caribe. Barómetro Global de la Corrupción.* Coralie Pring, editora. Berlín, Alemania. Recuperado de: **https://www.transparency.org/en/publications/global-corruption-barometer-people-and-corruption-latin-america-and-the-car**

Transparencia Internacional. (2019). *Barómetro Global de la Corrupción en América Latina y el Caribe 2019. Opiniones y experiencia de los ciudadanos en materia de corrupción*. Coralie Pring, Jon Vrushi, editores. Recuperado de: **https://images.transparencycdn.org/images/2019_GCB_LAC_Report_EN1.pdf**

Transparencia Internacional. (2021). CPI 2021 for the Americas: A Region In Crisis. **https://www.transparency.org/en/news/cpi-2021-americas-a-region-in-crisis**

Transparencia por Colombia y Monitor Ciudadano de la Corrupción. (2019). *Así se mueve la corrupción: Radiografía de los hechos de corrupción en Colombia 2016-2020*. Bogotá D.C., Colombia. Recuperado de: **https://www.monitorciudadano.co/documentos/hc-informes/2021/Radiografia-2016-2021.pdf**

Treshock, M. (2020). How the FDA is piloting blockchain for the pharmaceutical supply chain. **https://www.ibm.com/blogs/blockchain/2020/05/how-the-fda-is-piloting-blockchain-for-the-pharmaceutical-supply-chain/**

U.S. v. Sheirer, United States Court of Appeals, Tenth Circuit, 13 de julio de 1990. **https://www.casemine.com/judgement/us/5914898badd7b0493450420c#**

U.S. America, Plaintiff, v. Robert J. Riggs, also known as Robert Johnson, also known as Prophet, and Craig Neidorf, also known as Knight Lightning, Defendants. N.º 90 CR 0070. United States District Court, N.D. Illinois, E.D. 5 de junio de 1990. **https://law.justia.com/cases/federal/district-courts/FSupp/739/414/1610447/**

Valle-Cruz, D.; Sandoval, R. y Gil-García, J. R. (2016). "Citizens' perceptions of the impact of information technology use on transparency, efficiency and corruption in local governments," Information Polity, 21(3), pp. 321-334.

Van Eeten, M. (2017). "Patching security governance: An empirical view of emergent governance mechanisms for cybersecurity", Digital Policy, Regulation and Governance, Vol. 19, n.º 6, pp. 429-448. **https://doi.org/10.1108/DPRG-05-2017-0029**

Van Niekerk, M. (2021). How blockchain can help dismantle corruption in government services. Foro Económico Mundial. **https://www.weforum.org/agenda/2021/07/blockchain-for-government-systems-anti-corruption/**

Varian, H. (1992). Microeconomic Analysis. New York: Norton.

Volosin, N. (2015). *Open data, corruption and public procurement.* Montevideo: Iniciativa Latinoamericana por los Datos Abiertos (ILDA). Recuperado de: **https://zenodo.org/record/4562395#.YLd4ay0RppS**

Wachter, S. y Mittelstadt, B. (2018). *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*. Columbia Business Law Review. **https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3248829**

Waller, M.A. y Fawcett, S.E. (2013). Data Science, Predictive Analytics, and Big Data: A Revolution That Will Transform Supply Chain Design and Management. J Bus Logist, 34: pp. 77-84. doi:10.1111/ jbl.12010

Wilms, G. European University Institute, "Good data protection practice in research". (Abril de 2019). **https://www.eui.eu/documents/servicesadmin/deanofstudies/researchethics/guide-data-protection-research.pdf**

Wood, G. (2014). Ethereum: A secure decentralised generalised transaction ledger.

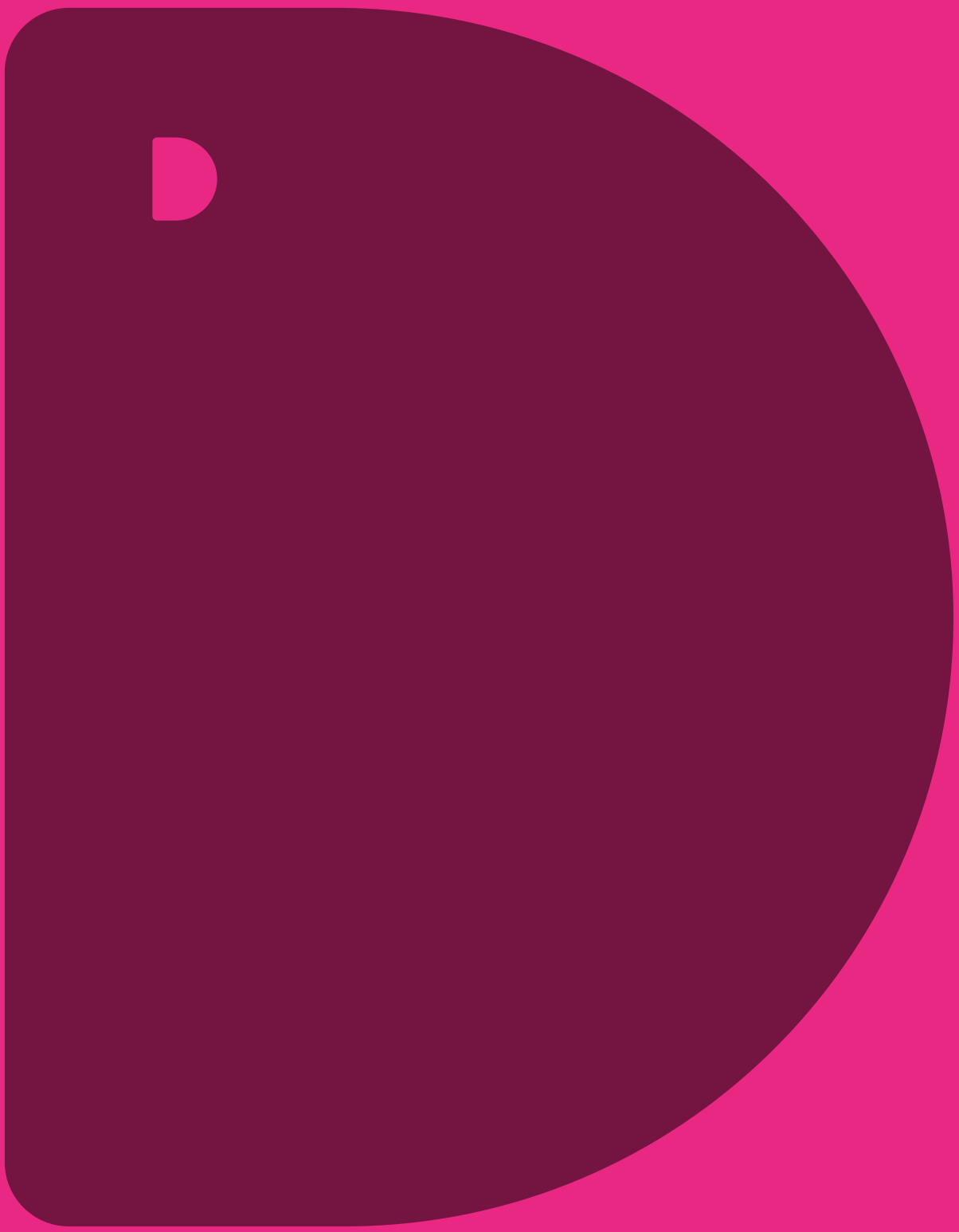
World Bank. (2017). Registering Property: Using information to curb corruption. En *Doing Business* (pp. 51-55). Banco Mundial.

Zamboni, Y. y Litschig, S. (2018). "Audit risk and rent extraction: Evidence from a randomized evaluation in Brazil". *Journal of Development Economics*, 134, pp. 133-149.

Zapata, E.; Scrollini, F. y Fumega, S. (2020). *¿Cuán abiertos están los datos públicos? El Barómetro de Datos Abiertos para América Latina y el Caribe 2020*. Recuperado de: https://scioteca.caf.com/handle/123456789/1710

Zuboff, S. (2019). The age of surveillance capitalism: the fight for a human future at the new frontier of power. New York: Public Affairs.

Zuleta, M. (2019). *Hacia una política de datos abiertos del Sistema de Compra Pública para los países miembros de la RICG.* Montevideo: Iniciativa Latinoamericana por los Datos Abiertos (ILDA). http://doi.org/10.5281/zenodo.4318938



CAF BANCO DE DESARROLLO DE AMÉRICA LATINA