CAF BANCO DE DESARROLLO DE AMÉRICA LATINA

RESUMEN EJECUTIVO

Digintegridad:

La transformación digital de la lucha contra la corrupción

Temas asociados: Blockchain, Corrupción, Compras públicas, Crisis sanitaria, COVID-19, Datos Abiertos, Gobierno Digital, Gobierno Inteligente, Integridad, Inteligencia Artificial, Riesgos Tecnológicos

Tiempo estimado de lectura: 15 minutos

Nota de CAF –banco de desarrollo de América Latina–

Director de Innovación Digital del Estado:
Carlos Santiso

Elaboración de la nota:
Camilo Cetina, Paula Cruz Manrique

Coordinadora de la publicación:
Nathalie Gerbasi.

Revisión y comentarios:
Anabella Abadi, Gustavo Fajardo, Nathalie Gerbasi, Carlos Santiso y Pablo Sanguinetti.

Los escándalos de corrupción sin precedentes en América Latina que se han conocido en la última década sugieren que la región se enfrenta a desafíos estructurales que combinan una corrupción endémica con debilidad institucional. La lucha contra la corrupción y la impunidad, en ese sentido, es parte fundamental de la agenda de desarrollo y las políticas de reactivación pos-pandemia.

La aceleración de la transformación digital aparejada a la globalización de la economía afecta de modo ambivalente la agenda de integridad en los gobiernos.

- **Por un lado, la globalización y la tecnología brindan oportunidades sin precedentes para que la corrupción crezca** en tamaño y capacidad de daño, puesto que al usar el ciberespacio las redes criminales operan sin territorialidad alguna, ocultan fácilmente flujos ilícitos de dinero, y limitan las capacidades jurisdiccionales para su detección y sanción.

- Pero, **por otro lado, se están logrando mejoras sistémicas en la gobernabilidad y acción colectiva gracias a las nuevas tecnologías** que ayudan a suministrar servicios automatizados y con procesos de gestión pública más visibles gracias a los datos abiertos y registros cada vez más públicos.

Este reporte ofrece un análisis integral de las oportunidades que ofrecen las tecnologías digitales como dispositivos para la integridad pública y lucha contra la corrupción. Indaga los "dividendos de integridad" derivados de la digitalización creciente de los gobiernos y el uso cada vez más intenso de las nuevas tecnologías y la inteligencia de datos en la prevención de la corrupción. En el Reporte de Economía y Desarrollo RED 2019 "Integridad en las políticas públicas: claves para prevenir la corrupción" CAF (2019), CAF analizó de modo integral los avances y desafíos de la agenda anticorrupción en América Latina e identificó diferentes frentes de acción y reforma institucionales para promover mayor integridad en las políticas públicas. En este nuevo informe se profundiza el papel que tienen los datos, las nuevas tecnologías y la innovación digital en la implementación de políticas de integridad eficaces.

Estructura de este reporte y principales mensajes

El reporte ***DIGintegridad*** sostiene que la incorporación de tecnologías digitales brinda un gran potencial para mejorar las políticas públicas para la prevención, detección e investigación de fenómenos de corrupción. También propone que la adopción de las tecnologías digitales en integridad pública puede estructurarse en un **orden secuencial:**

- Primero, se debe **asegurar que exista una infraestructura de datos abiertos,** los cuales son el insumo fundamental para implementar las grandes innovaciones digitales contra la corrupción. Para ello es importante que **las políticas de transparencia activa y datos abiertos ser articulen con las políticas de gobierno digital** generando así un ecosistema que garantiza la calidad, vigencia y reusabilidad de conjuntos de datos de especial interés en materia de integridad pública.

- En segundo lugar, los gobiernos pueden recurrir **a técnicas de inteligencia de datos que hagan más eficientes las tareas de prevención, detección e investigación de los actos de corrupción.** El uso óptimo de dichas tecnologías exige desarrollar una infraestructura con gran poder de cómputo. A partir de allí los gobiernos pueden **adoptar tecnologías más sofisticadas como la inteligencia artificial y tecnología *blockchain* para prevenir actos de corrupción** en procesos de la gestión pública especialmente vulnerables a riesgos de integridad (e.g. compra pública, otorgamiento de licencias).

- Adicionalmente, y a medida que se integran las tecnologías digitales en las políticas de integridad pública, **los gobiernos deben incorporar medidas para la gestión de riesgos en la adopción de nuevas tecnologías,** derivadas del potencial uso indebido que puede amenazar la integridad de las mismas.

- Finalmente se debe generar un **entorno institucional para que el uso de las tecnologías digitales sea sostenible en el largo plazo.** Esto implica, por ejemplo, garantizar la formación de talento humano para la era digital; adoptar reformas que habiliten la innovación pública, y profundizar las reformas a la justicia hacia un esquema más restaurativo que asegure la recuperación de los recursos públicos y la reparación de las víctimas de hechos de corrupción.

Figura 1 – Estructura del Informe y Propuesta de Política de Digitalización para la Integridad

Fuente: Elaboración Propia.

Condiciones para la transformación digital anticorrupción

El reporte recomienda a los gobiernos consolidar unas condiciones mínimas que se requieren para incorporar tecnologías digitales en las políticas de integridad y lucha contra la corrupción. La razón fundamental es que l**a existencia de datos abiertos y servicios básicos digitalizados de gobierno, preceden al desarrollo tecnológico en procesos más complejos como la prevención, detección e investigación de fenómenos de corrupción.** En ese sentido, es importante que los gobiernos consoliden una agenda en tres frentes preliminares:

- **Políticas públicas de gobierno digital,** en particular la digitalización de los trámites y registros públicos, y la automatización de procesos administrativos como la contratación pública.
- **Implementación del principio de transparencia activa,** de modo que las principales decisiones y procesos de la gestión estatal sean considerados información pública. Dicha información debe ser accesible **en formato de datos abiertos** con la calidad, completitud y estructura necesarias que permitan su reutilización efectiva.
- **Organización y puesta a disposición de 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 mayor control de la corrupción.

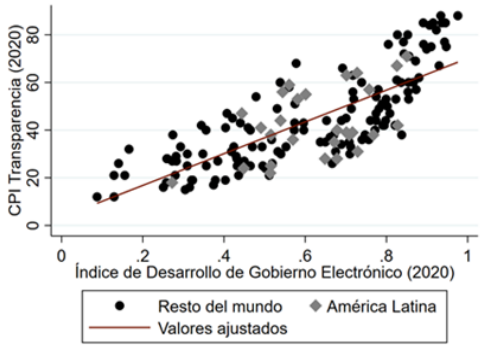
Digitalización del gobierno

Con la digitalización y simplificación de los trámites y la automatización de los procesos administrativos, los gobiernos pueden limitar la discrecionalidad de las autoridades públicas y reducir así las interacciones que dan lugar a conductas de corrupción. Adicionalmente, **la digitalización del Estado hace posible la centralización de datos que contienen información sobre los procesos llevados a cabo por las administraciones públicas.** 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.

Estos datos e información, cuando son de público acceso, tienen el potencial de fomentar mayores niveles de transparencia e integridad del Estado. Existe una clara **correlación entre la digitalización del Estado y el control de la corrupción de acuerdo a múltiples indicadores agregados.** Por ejemplo, países con mayores valores en el Índice de Desarrollo de Gobierno Electrónico (IDGE) de Naciones Unidas también muestran mejores resultados en el Índice de Percepción de la Corrupción (IPC) de Transparencia Internacional, como muestra el Gráfico 1 (puntajes mayores en el IPC indican 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 del Gráfico 1 se sustituye el IDGE con el Índice de Adopción Digital del Banco Mundial. En los paneles C y D se sustituye el IPC con, respectivamente, la medida de control de la corrupción de los Indicadores de Gobernanza Mundial del Banco Mundial, y una medida de auto-reporte de pago de sobornos de Transparencia Internacional. En todos los casos, se mantiene la misma relación[1].

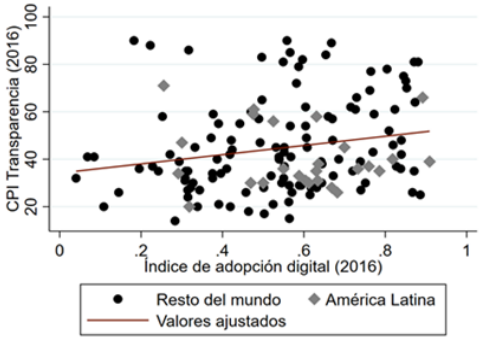
Gráfico 1 - Correlación entre digitalización y corrupción en países de América Latina

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 indican mayor desarrollo electrónico, y el Índice de Percepción de la Corrupción de *Transparency International* (eje vertical), en el que valores mayores indican menor percepción de corrupción. La línea continua representa la correlación entre las variables. La muestra la componen 161 países de todo el mundo.

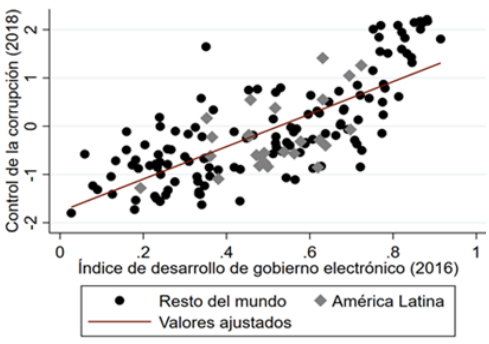
Panel B. Adopción digital y transparencia



Nota: Se reporta el Índice de Adopción Digital del Banco Mundial (eje horizontal), en el que valores más altos indican mayor adopción digital, y el Índice de Percepción de la Corrupción de *Transparency International* (eje vertical), en el que valores mayores indican menor percepción de corrupción. La línea continua representa la correlación entre las variables. La muestra la componen 144 países de todo el mundo

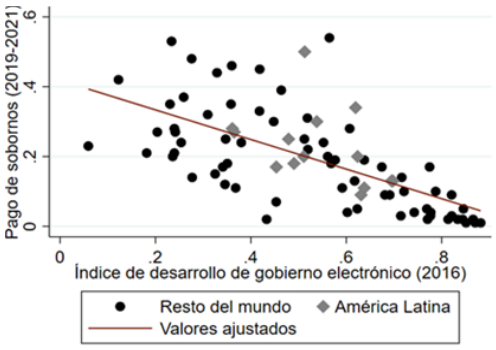
1 En el panel D, el signo de la correlación es negativo porque el indicador de corrupción usado allí toma valores mayores cuando la corrupción es alta, al contrario que en los indicadores de los otros paneles.

Panel C: Gobierno electrónico y control



Nota: Se reporta el Índice de Desarrollo de Gobierno Electrónico de las Naciones Unidas (eje horizontal), en el que valores más altos indican mayor desarrollo electrónico, y el indicador de control de la corrupción de los Indicadores de Gobernabilidad Mundial del Banco Mundial (eje vertical), en el que valores más altos indican mejores resultados. La línea continua representa la correlación entre las variables. La muestra la componen 155 países de todo el mundo.

Panel D: Gobierno electrónico y pago de sobornos

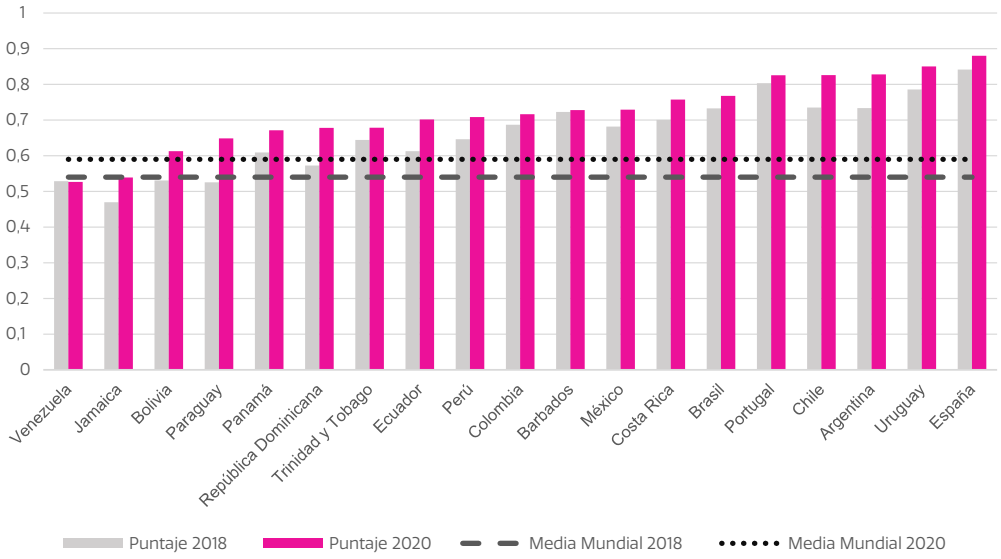


Nota: Se reporta el Índice de Desarrollo de Gobierno Electrónico de las Naciones Unidas (eje horizontal), en el que valores más altos indican mayor desarrollo electrónico, y el indicador de Pago de Sobornos del Barómetro Global de Corrupción de *Transparency International* (eje vertical), que señala 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 82 países de todo el mundo

América Latina está avanzando en el desarrollo en sus políticas de gobierno digital. De acuerdo con el E-Government Development Index (EGDI) de Naciones Unidas, el cual es liderado por Dinamarca, Corea y Estonia, 17 de los 19 países miembros de la CAF se situaron por encima del promedio mundial[2] (ver Gráfico 2).

2 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 EDGI 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 acerca mucho al máximo de 1.

Gráfico 2 - Resultados EDGI para los países miembros de CAF 2018 y 2020.



Fuente: ONU, 2020. La escala EDGI va de 0 a 1, Dinamarca (0.9758), Corea (0.9560) y Estonia (0.9473) fueron los países líderes en el 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.

Los avances que está teniendo América Latina en materia de digitalización pueden ser un catalizador importante para progresar en una agenda renovada de integridad y prevención de la corrupción. Para ello la digitalización y la tecnología deben complementarse con regulaciones y arreglos institucionales que faciliten la transparencia activa y los datos abiertos.

Transparencia activa y datos abiertos

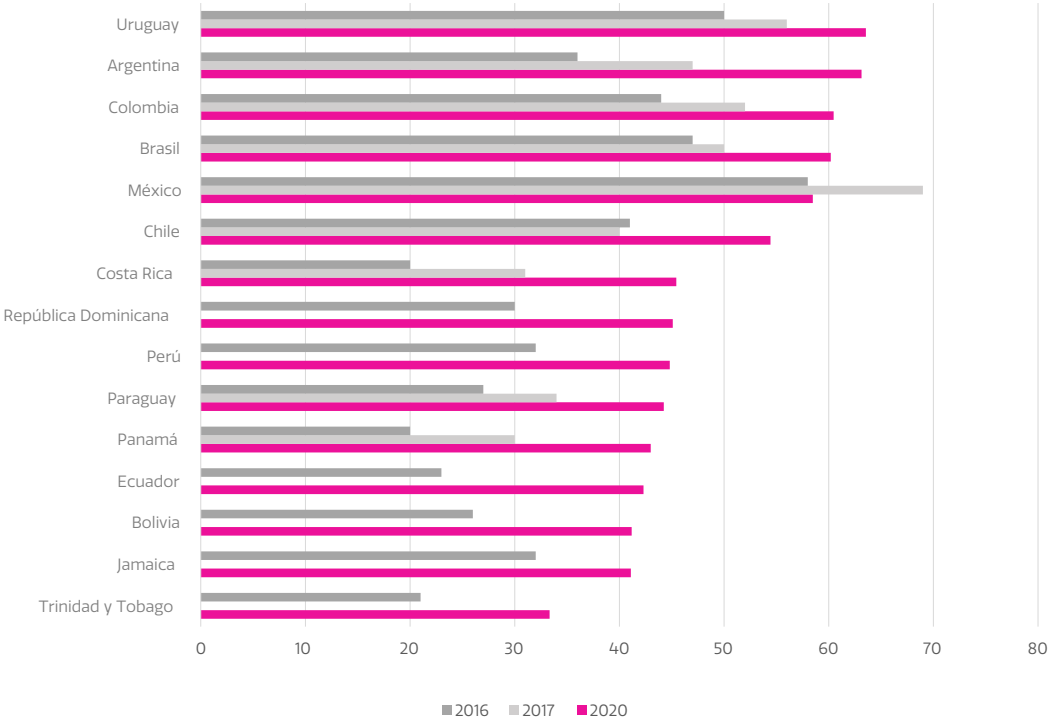
El concepto de transparencia no sólo exige la publicidad en las actuaciones de las instituciones y autoridades públicas. La transparencia implica que además de permitir a los ciudadanos que conozcan las actuaciones del Estado, también puedan ejercer un control sobre las decisiones de las autoridades públicas que les afectan.

Adicionalmente, la transparencia activa obliga a las agencias del gobierno a publicar de manera sistemática, periódica y oportuna, sin que medie requerimiento alguno, toda aquella información y 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 sobre las acciones que toman las autoridades públicas e incluso entidades privadas que suministran servicios públicos.

La regulación en materia de acceso a la información pública en América Latina tiene casi

tres décadas **y gracias al principio de transparencia activa, así como a la digitalización de la información, los gobiernos están transitando hacia la apertura de datos.** De acuerdo con el Barómetro Regional de Datos de Abiertos para América Latina y el Caribe de 2020, que mide la preparación[3], implementación[4] e impacto de los datos abiertos,[5] la región mostró un crecimiento marginal comparado con los resultados de 2016, con una calificación promedio de 40,38 en una escala que va de 0 a 100. Esto refleja una desaceleración de la agenda de apertura de datos (Zapata, Scrollini & Fumega 2020).

Gráfico 3 – Resultados del Barómetro Regional de Datos de Abiertos para América Latina y el Caribe para los países miembros de CAF 2016, 2017 y 2020



Fuente: Zapata, Scrollini & 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.

3 Se refiere a la disposición de los gobiernos, ciudadanos y empresarios para asegurar la apertura de los datos.
4 Corresponde al grado en que los gobiernos publican conjuntos de datos clave de forma accesible, oportuna y abierta.
5 Identifica hasta qué punto hay evidencia de que la publicación de datos abiertos de gobierno ha tenido impacto positivo en una variedad de sectores del país.

Conjuntos de datos y usos en integridad pública

Una vez que los países habilitan una infraestructura y gobernanza de datos a partir de sus políticas de gobierno digital, es posible ajustar los estándares de transparencia activa de modo que el acceso a la información pública se base en conjuntos de datos abiertos. **De esta forma, los ciudadanos pueden acceder a datos abiertos, ejercer control sobre las actuaciones estatales mientras se previene la corrupción al menos desde tres ámbitos,** como se detalla a continuación:

- **Límites a las decisiones discrecionales y reducción de la burocracia.** Los conjuntos de datos abiertos no sólo provienen de la necesidad de publicar información sobre las actuaciones de los gobiernos; también de la digitalización de servicios que reducen la burocracia y simplifican procesos. Por ejemplo, la digitalización de la compra pública, que en principio buscaba hacer más eficientes y rápidos los complejos procesos de contratación gubernamental, ahora permite a los ciudadanos acceder a datos e información sobre los recursos invertidos en compras y contrataciones públicas. Gracias a ello es posible ejercer control sobre factores de riesgo como las modalidades de licitación y contratación, puesto que los procesos cerrados y discrecionales presentan más riesgo de corrupción.

- **Procesos de rendición de cuentas** por medios digitales y en tiempo real. La rendición de cuentas como un ejercicio de transparencia activa es posible a partir de plataformas que capturan diferentes fuentes de datos para presentar integralmente la gestión pública en sectores específicos. Por ejemplo, los aplicativos de MapaInversiones en países como Colombia y Costa Rica integran información del ciclo presupuestal y de la ejecución de grandes proyectos de inversión, para mostrar a los ciudadanos el avance de obras y asignación de recursos para la entrega de bienes públicos.

- **Control social y la participación ciudadana.** La sociedad civil organizada está haciendo uso de los datos abiertos a través de iniciativas impulsadas desde las startups civic-tech y gov-tech, para acercar a los ciudadanos a la gestión pública y presentarles la información relevante en materia de control, con simplicidad y bajo costo. Por ejemplo, en octubre de 2019, Paraguay introdujo una aplicación móvil llamada "*PresupuestApp*",que no sólo sirve para realizar consultas sobre presupuestos y gastos aprobados de cualquier institución pública, sino que también permite a los ciudadanos reportar o denunciar irregularidades ante el Ministerio de Hacienda.

Una agenda de datos abiertos consolidada permite a los gobiernos avanzar en la adopción de estándares de apertura internacionalmente reconocidos, en áreas de especial interés para la integridad pública como la contratación, la tributación, el gasto público, la infraestructura, la función pública, entre otros. 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 más de 30 conjuntos de datos que pueden ser usados en la lucha contra la corrupción. La aplicación de iniciativas como el PIDA permite estandarizar las tareas de producción, publicación y reutilización de los datos, para contar con información útil en programas e iniciativas anti-corrupción.

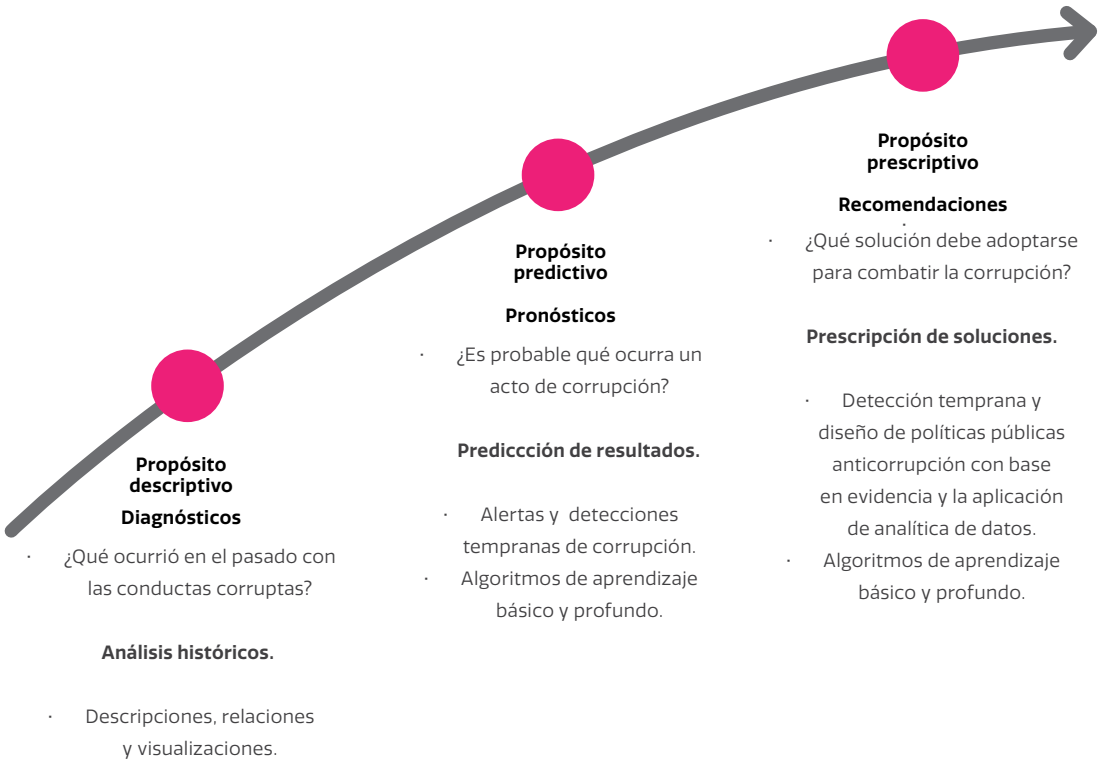
Tecnologías digitales para la integridad (I): Inteligencia de datos

Los datos abiertos y las infraestructuras de datos, abren la posibilidad de tomar grandes conjuntos de datos 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 macro-datos 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: diagnostico, descriptivo, predictivo y prescriptivo)[6]. 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 2). Sin embargo, para efectos de este informe las experiencias

Figura 2 - Evolución del propósito del uso de datos como estrategia anticorrupción



Fuente: Elaboración propia.

6 Ver: https://www.oracle.com/business-analytics/data-analytics/

Modelos Descriptivos

Los desarrollos en *DIGIntegridad* con propósitos descriptivos generalmente reutilizan conjuntos de datos abiertos para identificar anomalías que puedan estar asociadas a riesgos de corrupción. El acceso libre y directo a la información sobre las actuaciones del gobierno que es posible gracias las políticas de transparencia activa y datos abiertos, combinado con el uso de programas y plataformas para procesar los conjuntos de datos, permiten una comprensión integral de la gestión pública y de los fenómenos de corrupción.

Una de las aplicaciones más efectivas que 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, 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 e información que la alimentan.

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, revelar la existencia de redes complejas y rastrear movimientos de flujos de dinero. De este modo, la analítica descriptiva hace 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.

Por ejemplo, consultar el portal del *Financial Crimes Enforcement Network* (**FINCEN**) acerca de la actividad de lavado de activos con uso de tarjetas de débito en los Estados Unidos arroja más de 37.000 resultados. El detalle de las transacciones allí consignadas genera un volumen de datos que no resulta fácilmente analizable a partir de operaciones mentales y métodos tabulares[7]. Para poder analizar información de escalas similares, la Organización de 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), que se alimentan de los reportes que hacen las Unidades de Inteligencia Financiera de los países. Los aplicativos de ONU permiten recolectar, analizar y diseminar los datos sobre redes de lavado, además de crear 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.

Modelos Predictivos

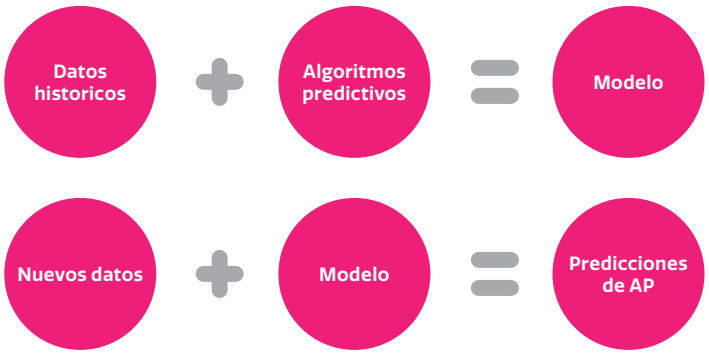
Los modelos predictivos **permiten estimar u otorgar un valor numérico o puntuación de probabilidad, a la ocurrencia de un fenómeno o conducta particular.** Así, el interés que suscita esta técnica para las políticas de integridad pública está en que puede estimar la probabilidad de ocurrencia de actos de corrupción en determinadas actuaciones públicas. Para estimar esa probabilidad se realizan análisis estadísticos, consultas y algoritmos automáticos de aprendizaje a conjuntos de

7 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.

datos nuevos e históricos, creando modelos predictivos (Ver Figura 3).

Estas tecnologías digitales 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 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 (Llinás, 2003).

Figura 3. Mecanismo de la analítica predictiva



Las técnicas de analítica predictiva (AP) de datos pueden sustentarse en aprendizajes automáticos básicos y profundos. La AP sustentada en aprendizaje automático básico (*basic machine learning*) requiere de un trabajo de identificación de los riesgos específicos[8] 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 éstos dentro los datos estructurados analizados, generado 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 (CAF, 2021). Así es posible detectar y/o predecir posibles casos de corrupción.

Un ejemplo de AP en prevención de corrupción es el Sistema Analítico de Indicadores de Colusión del Gobierno de Corea (BRIAS, 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 coreana (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 éste, 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

8 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, cambios súbitos en los objetos sociales de las sociedades contratitas, son algunos ejemplos de riesgo en la contratación pública (Cetina, 2020a).

credenciales (la dirección IP, fechas y horas de visita, módulos visitados, comunicaciones, etc.) se utiliza con propósitos estadísticos y analíticos, para determinar riesgos de colusión y corrupción en la contratación pública.

Otro ejemplo es el Analisador de *Licitações e Editais* (ALICE) es una herramienta desarrollada en 2017 por la Controladoria-Geral da União (CGU) de Brasil para el análisis de los documentos de contratación y compra pública brasileros. ALICE toma la información del sistema de compra pública del Brasil (*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. 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, identifica las palabras clave, identifica nombres (bien sea compradores o proveedores), entre otros datos para determinar el perfil del contrato. Luego detecta combinaciones de palabras que pueden hacer a un contrato más riesgoso o que merezca más atención por su cuantía, objeto, entidad contratante, o plazos.

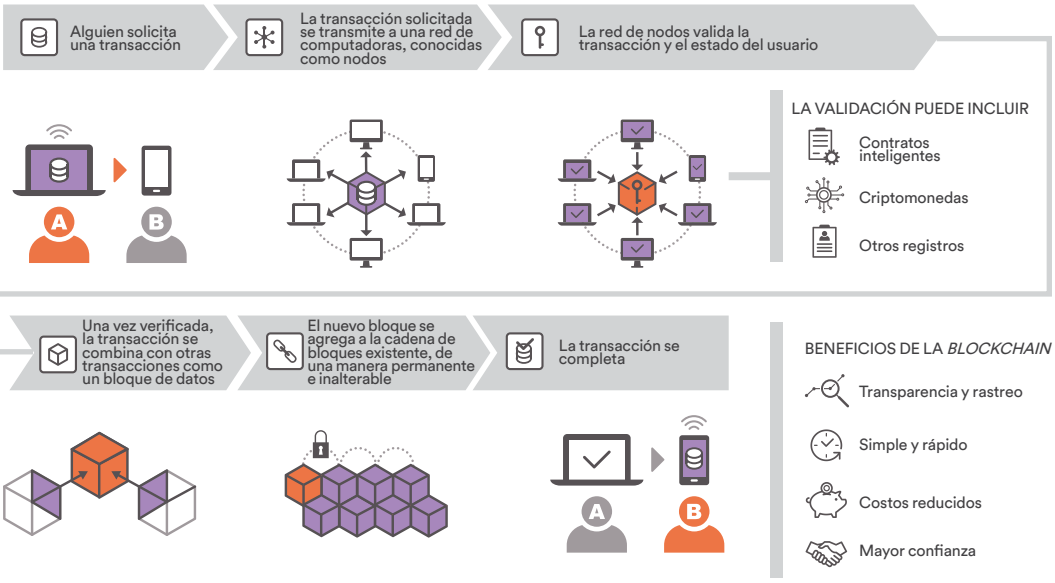
Diariamente son seleccionados los contratos que contienen un texto que ALICE considera que merece la atención de los auditores de la CGU. Luego de ello **se activa un sistema automático de envío de correos electrónicos a los auditores informándoles de los contratos de mayor interés** para su análisis. Adicionalmente, las listas diarias y datos identificadores de los contratos se almacenan en una base de datos centralizada.

Tecnologías digitales para la integridad (II): *Blockchain*

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 facilitan el seguimiento a las decisiones gubernamentales, lo cual contribuye a reducir riesgos de corrupción mediante mecanismos de control ciudadano y/o institucional. **La tecnología *blockchain* va más allá: permite que los mencionados registros queden a prueba de manipulaciones de modo que agentes fraudulentos no puedan modificarlos, alterarlos o falsificarlos.** 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.

Blockchain o la "cadena de bloques o firmas digitales de información" es una tecnología de contabilidad distribuida ("*distributed ledger*") que permite registrar transacciones en bloques de información. Cada bloque contiene información de transacciones o bloques anteriores, creando una cadena de información en la que toda transacción cuenta con una pista de auditoría inmutable y es validada por todos los interesados o "nodos" de modo descentralizado en tiempo real (Ver Figura 4). 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 son completamente rastreables (CIAT, 2018).

Figura 4 – Paso a paso del funcionamiento de la tecnología *blockchain*



Fuente: Atencio (2020)

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 que documentan el cumplimiento de requisitos legales– *blockchain* puede asegurar la integridad del procedimiento porque hacen rastreables las alteraciones a documentos como los términos de referencia; también puede impedir que existan cambios en las licitaciones por fuera los términos de ley. Ademas, el blockchain garantiza la visibilidad de los procesos para todos los interesados o nodos como proponentes, entidades públicas y sociedad civil. Así para que se materialice un acto corrupto sería necesario que todos los nodos validaran o aceptaran la transacción. Finalmente, debido a que la tecnología blockchain opera bajo la lógica de los contratos inteligentes (smart contracts), se garantiza la continuidad y transparencia del procedimiento de contratación. Los contratos inteligentes traducen al lenguaje de programación un grupo de cláusulas contractuales, de forma que cuando se verifica una regla, automáticamente se ejecuta la obligación (tal como ocurre con una máquina dispensadora de bebidas que al verificar que recibe un monto específico de dinero, expulsa la bebida ejecutando así la regla).

Esta tecnología está siendo sometida a pruebas mediante proyectos piloto. Por ejemplo, **en Colombia, la Procuraduría General de la Nación (PGN) desarrolló una prueba de concepto para la aplicación de la tecnología blockchain autorizado en la contratación del programa de alimentación escolar en la ciudad de Medellín.** El blockchain mostró aplicabilidad en varios aspectos de la contratación pública, como sigue:

- En primer lugar, el mecanismo *blockchain* pseudoanonimiza 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. Aunque la pseudoanonimización es posible independientemente del uso de blockchain, la ventaja de aplicar dicha tecnología está en que por una parte cualquier alteración en la pseudoanonimización queda registrada; y no es posible seguir con el proceso licitatorio sin haber pseudoanonimizado a los proponentes

- Una vez que los términos de referencia de la licitación se hacen públicos, éstos no pueden ser alterados. Igualmente sucede con los comentarios de los ciudadanos que no pueden ser eliminados y quedan registrados.

- Adicionalmente, las propuestas recibidas por la entidad contratante quedaban anónimamente registradas en *blockchain* con los documentos adjuntos cuando los proveedores las enviaban; no pueden abrirse hasta el inicio del proceso de evaluación que está programado. De hecho, la entidad pública no conoce de dónde vienen las propuestas antes de comenzar el proceso de evaluación de las mismas.

- Todo lo anterior ayuda a prevenir la existencia de acuerdos ilícitos que con anterioridad se pueden hacer para favorecer indebidamente a un oferente.

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.

El aporte del blockchain en la lucha contra la corrupción en la contratación pública es prometedor, pero también cuenta con algunas limitaciones importantes. Estas limitaciones incluyen privacidad y anonimato del proveedor, incertidumbre en cuanto a escalabilidad, acuerdos entre empresas por fuera de la plataforma, entre otros.

Las aplicaciones de la tecnología blockchain para mejorar la integridad en otras transacciones están apenas explorándose. No existe aún una evidencia sistemática que determine un efecto probado del blockchain sobre los riesgos de corrupción en la gestión pública. Sin embargo, la literatura disponible documenta un uso creciente para asegurar la integridad dentro de transacciones especialmente sensibles, a través de esta tecnología. Otros ejemplos en este frente son:

- **Integridad en la distribución de vacunas contra el COVID-19:** De acuerdo con UNODC, la vacunación masiva representa un reto sin precedentes para los gobiernos del mundo. En este marco, se han presentado fenómenos de corrupción como la falsificación, el robo de vacunas e irregularidades dentro de los sistemas de distribución relacionados con nepotismo o favoritismo político. En Estados Unidos la tecnología blockchain de carácter privado autorizado se utilizó para verificar la calidad, origen, distribución de las vacunas contra el COVID-19[9]. Las características propias blockchain (inmutabilidad y descentralización distribuida) evitan la manipulación y adulteración de los datos sobre el proceso de entrega y administración.

- **Registros de titulación de tierras:** La tecnología blockchain puede optimizar los registros públicos, reduciendo la ineficiencia y aumentando los niveles de

9 UNODC ha documentado fenómenos de corrupción como la entrada en los mercados de vacunas falsificadas, el robo de vacunas dentro de los sistemas de distribución, y la administración de vacunas bajo criterios de nepotismo o favoritismo.

transparencia, como los relacionados con la adquisición de bienes inmuebles, permisos, concesiones y certificados. En el 2016, la república de Georgia aprovechó su base digital de registros de la propiedad, para iniciar un proyecto piloto de registro de tierras a través de blockchain. La aplicación basada en tecnología blockchain pública autorizada redujo el tiempo de las transacciones de registro a sólo 10 minutos. Todo inicia 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 permanece disponible y aprobado criptográficamente. Para el 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 Prince, 2019).

- **Integridad en las transferencias monetarias no condicionadas:** *Blockchain* puede mitigar estos riesgos y desvío de recursos en las transferencias monetarias de los gobiernos para dar medios de subsistencia a los ciudadanos más vulnerables. Por ejemplo, el Programa Mundial de Alimentos (PMA) desarrolló el proyecto "***Building Blocks***" para determinar la viabilidad de incorporar la tecnología *blockchain* entre más de 100.000 refugiados de 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 que buscaban un espacio neutral y transparente para colaborar, realizar transacciones y compartir información de forma segura en tiempo real (PMA, 2021). El dinero en efectivo se almacena en una cuenta del beneficiario, cuyo valor y datos quedan validados por diferentes nodos en la cadena de bloques. Posteriormente, el efectivo que los beneficiarios reciben o gastan se paga a través de un proveedor de servicios financieros comerciales, y los pagos quedan almacenados en *blockchain*. 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, reforzar la eficiencia de las intervenciones para el desarrollo.

Consideraciones de Política Pública

Gestión de los riesgos tecnológicos

Así como existen tecnologías digitales para la integridad, los gobiernos deben garantizar la integridad en el uso de las tecnologías. Las tecnologías específicas reseñadas con 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. Por ejemplo: el abuso de función pública para actividades como el tráfico de datos personales o de información privilegiada tri-

butaria; el lavado de activos; el robo de datos para suplantación de identidad, entre otros, son riesgos que pueden generar costos potencialmente equivalentes a la corrupción.

El informe distingue tres tipos de riesgo de especial interés para los gobiernos. Cada uno de ellos está asociados a los tres grupos de desarrollo digital que se abordaron en el informe, esto es, al gobierno digital, a la inteligencia de datos y al *blockchain*.

Identidad digital

El primer factor de riesgo está en la identidad digital. Los sistemas de identificación facilitan las interacciones entre las personas, el Gobierno y las entidades privadas; el aseguramiento de la identificación de todas las personas además de un derecho, constituye un **objetivo de desarrollo sostenible (16.9). La identificación corresponde a una combinación de características o atributos de una persona que la hacen única dado un contexto determinado.** Así, en el mundo digital las actividades de identificación, autenticación y autorización, no se agotan con la simple asignación de "*Usuarios y Contraseñas*". La identificación implica un procedimiento mediante el cual, se recopilan elementos, tanto internos como externosal individuo, como características físicas, información sobre las finanzas y los impuestos, historiales de compra, registros legales, registros médicos, historia crediticia, entre otros (OECD, 2019). Estos elementos permiten asignar una identidad, con determinados atributos, a una persona concreta.

Los Sistemas de Identidad Digital (SDI) pueden ser objeto de redes criminales que buscan robar datos y suplantar la identidad para acceder a bienes o servicios. Administrar este riesgo no se limita a generar disposiciones para violaciones de privacidad y seguridad, inherentes a la captura, almacenamiento y uso de datos personales confidenciales. También existen riesgos si existe dependencia de una tecnología o un proveedor específico; o si la infraestructura y conectividad en un país es muy limitada generando dificultades para implementar sistemas de identificación digital que requieren energía y conectividad para la transferencia de datos o verificación de inscripción biométrica duplicada. Las capacidades técnicas e institucionales para las agencias centrales de ciberseguridad, son necesarias para propiciar un entorno seguro para los sistemas de identificación digital; al igual que para estructurar los procesos de adquisición de SDI (compra pública) para no terminar con adquisiciones fallidas, retrasos (por ejemplo, debido a apelaciones) y bloqueo de proveedores y tecnología.

Protección de datos personales

El segundo factor de riesgo está en la protección de los datos personales. Aun cuando los desarrollos digitales permiten simplificar trámites o aplicar técnicas de análisis de datos para mejorar procesos como la detección temprana de riesgos de corrupción, **existen riesgos implícitos relacionados 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 que puede ser "objetiva" (como edad, género o domicilio) y "subjetiva" como opiniones o evaluaciones de esa persona sobre una plataforma o servicio por medios digitales.

Los datos personales están sujetos a una protección debido a que la privacidad se considera un derecho fundamental en un Estado de Derecho. En ese sentido, se 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. La puesta en práctica de protección en la privacidad de los datos, va más allá de la adopción de Leyes

de Protección de datos personales. Implica introducir la privacidad desde el diseño; así, el responsable de los datos, desde el principio y durante todo el ciclo de vida del tratamiento, debe contar con mecanismos de protección para la recolección, almacenamiento, usos, circulación, acceso y destrucción de los datos.

Otro frente de riesgos sobre los datos personales está en la seguridad de los sistemas de información donde éstos se administran. La seguridad se refiere a la protección y dispositivos contra: accidentes, acceso no autorizado, modificaciones o destrucción no autorizada. La seguridad de la información, conocida como seguridad cibernética o seguridad informática, es un importante desafío y un componente vital en la relación de confianza entre los ciudadanos y sus gobiernos. De la misma forma 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.

Aunque en América Latina existen algunas regulaciones para protección de datos personales,[10] no sucede así con los mecanismos de gobernanza para la ciberseguridad para prevenir accesos no autorizados a plataformas digitales y consulta, alteración o extracción de los datos. Van Eeten (2017) documenta que **la responsabilidad para la gobernanza de la seguridad ha pasado de los propietarios de dispositivos a los grandes intermediarios.** 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. La OECD (2011) se ha referido a estas empresas como intermediarias de Internet. Sus prácticas de seguridad determinan cada vez más la seguridad de gobiernos y de ciudadanos por igual. El gran límite acá es que existe una asimetría de información fundamental que impide acudir a evidencia sistemática para verificar cuáles modelos, prácticas y políticas son convenientes en materia de seguridad para proteger los datos.

Uso del blockchain para los criptoactivos

Finalmente, el tercer factor de riesgo está en la ausencia de regulación nacional e internacional para la adopción de las tecnologías blockchain que permite el desarrollo y expansión de criptoactivos sin controles estatales. **Los criptoactivos corresponden a activos financieros digitales desarrollados a partir de criptografía y tecnología *blockchain*[11], que permiten el desempeño de transacciones económicas seguras, descentralizadas y distribuidas y cuya emisión es abierta a quien quiera emitir el criptoactivo.**

La descentralización y el cifrado en que está basado el *blockchain*, permiten la emisión de los criptoactivos y facilitan actividades de lavado de dinero. Existe evidencia sobre redes de narcotráfico que convierten sus fondos en criptoactivos para luego enviarlos por todo el mundo y volver a convertirlos en

10 Aunque no necesariamente para todo el ciclo de tratamiento - recopilación, grabación, organización, almacenamiento, adaptación, alteración, recuperación, consulta, etc

11 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 cualquier 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 cambios en los datos; incluso el cambio más pequeño en la entrada (por ejemplo, cambiar un solo bit, una sola letra o una coma) dará como resultado un hash completamente diferente.

divisas. Adicionalmente, es difícil para las autoridades investigar esta actividad en casos individuales, así como capturar los recursos, porque cuando dichos fondos se convierten desde las monedas oficiales a criptoactivos en *blockchain*, no queda rastro de cómo se hizo originalmente el dinero.

La implementación de soluciones basadas en blockchain deben soportarse es un marco regulatorio consistente. **El desafío para los reguladores es encontrar instrumentos apropiados para abordar los riesgos que emanan del uso del blockchain y la adopción de criptoactivos.** Los instrumentos regulatorios existentes tienen limitaciones para abordar los riesgos de delitos financieros y de consumo y de lavado de dinero. El **Banco de Pagos Internacionales** (BPI)[12] recomienda a las autoridades que primero deberían adelantar la agenda regulatoria basándose en las funciones económicas que se le otorguen al criptoactivo. En 2019, el Grupo de Acción Financiera (GAFI) introdujo **directrices** solicitando a los gobiernos a 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 estén registrados y supervisados por las autoridades nacionales competentes.

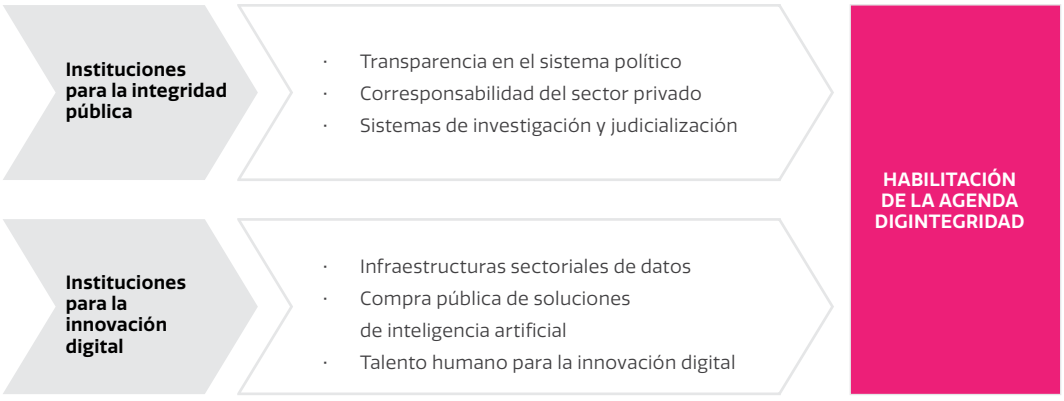
Recomendaciones de política y ajuste institucional

El rol que las tecnologías basadas en datos tienen en materia de integridad pública está siendo cada vez más reconocido por los gobiernos, organismos multilaterales y sociedad civil. 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 enmarca 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 ese sentido, explotar al máximo el potencial de la digitalización en las políticas de integridad pública **exige modernizar las instituciones gubernamentales en dos ámbitos de modo separado: los ajustes institucionales que promuevan la integridad; y la adaptación de las autoridades públicas a la era digital.** Las recomendaciones de política pública para una implementación efectiva de las innovaciones digitales en materia de integridad pública se inscriben en esos dos ámbitos (Ver Figura 5)

12 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 BIS 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)

Figura 5 – Instituciones para la integridad y la innovación digital



América Latina necesita modernizar sus arreglos institucionales para que la agenda anticorrupción se sintonice con la aceleración digital y le permita a las tecnologías generar dividendos 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 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.

Paralelo a la modernización del ecosistema de integridad en los gobiernos, también se requieren unos ajustes en el ecosistema de innovación digital para el sector público, de modo la adopción de herramientas digitales dentro de las estrategias de integridad pública sea sostenibles en el tiempo. Este reporte destaca al menos tres ámbitos para esta modernización, como sigue:

- **Infraestructuras organizadas de datos por cada sector y código abierto.** Puesto que los corruptos tienen estrategias diferentes y modalidades bien ajustadas al tipo de bien público suministra el Estado (salud, educación, seguridad, justicia, infraestructura, etc.), los conjun-

tos de datos específicos a la gestión del sector aumentan la efectividad de las tecnologías digitales para la integridad. Adicionalmente, las innovaciones digitales orientadas a mejorar los niveles de transparencia pueden ser compartidas y reutilizadas por otras entidades públicas o la sociedad civil interesada en la lucha contra la corrupción. Esto ocurre, por ejemplo, con la plataforma de visualización de obras de Buenos Aires **BAObras** y en el portal **Tianguis Digital** de ciudad de México.

- **Talento digital en los organismos responsables de la política anticorrupción.** La incorporación de tecnologías digitales en las estrategias de integridad pública da por sentado el conocimiento y pericia de quienes las manejan y las utilizan. Esto no es el caso completamente en 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 sus funciones, como es el caso de la prevención, investigación y detección de la corrupción. Por ejemplo, dentro del ecosistema de integridad debería comenzar con la creación de unidades especializadas en ciencia e inteligencia de datos dentro de los organismos de control.

- **Compra pública de inteligencia artificia**l. Así como existen estándares especiales para poder garantizar la integridad y calidad en la contratación pública de infraestructura (Fajardo, 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. Existen estándares de ética, así como de transparencia y rendición de cuentas para esta tecnología, que influyen en su uso y calidad.

REFERENCIAS

- CAF (2019). RED 2019. Integridad en las políticas públicas: claves para prevenir la corrupción. Retrieved from http://scioteca.caf.com/handle/123456789/1503

- CAF (2021) ExperiencIA: Datos e Inteligencia Artificial en el sector público. Retrieved from: https://scioteca.caf.com/handle/123456789/1793

- 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

- Fajardo, G., López, M., Ramírez, A., Román, C., Silveira, A., & Zarama, D. (2021). *Gobernanza del sector de infraestructura y de las APP.* CAF. https://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatf-recommendations.html

- FINRA. (2019). *Know your customer*. Finra.Org. https://www.finra.org/rules-guidance/rulebooks/finra-rules/2090

- 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. & Macías, G. (2018) Macrocorrupción y Cooptación Institucional: La Red Criminal "Lava Jato"

- Garay, L. G., Salcedo-Albarán, E. & Macías, G. (2021) Súper-red de corrupción en Venezuela.

- 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.
- Munidigital. (2021). E*xperiences. Munidigital.Tech.* https://en.munidigital.tech/case-studies
- NACIONES UNIDAS E-GOBIERNO ENCUESTA 2020 G*obierno 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., & bitcoin.org, W. (n.d.). *Bitcoin: A peer-to-peer electronic cash system.* Bitcoin.Org. Retrieved October 22, 2021, from https://bitcoin.org/bitcoin.pdf
- Naudé, W. (2020). A*rtificial intelligence versus COVID-19 in developing countries: Priorities and trade-offs*». UNU-WIDER.
- OECD. (2011). *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. OECD Publishing
- OECD. (2016). Gobierno digital. I*n 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
- OpenDataCharter. (2015). *Carta Internacional de Datos Abiertos.* https://opendatacharter.net/principles-es/
- Padilla, J. (2020). Blockchain y contratos inteligentes: aproximación a sus problemáticas y retos jurídicos. *Revista de Derecho Privado* , 39, 175–201.
- Roseth, B., Reyes, A., & 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
- Transparencia Internacional (2019). *Barómetro Global de la Corrupción América Latina y el Caribe 2019. Opiniones y Experiencia de los ciudadanos en materia de corrupción.* Coralie Pring, Jon Vrushi, Editores.
- Transparencia Internacional. (2017). *Las personas y la corrupción. América Latina y el Caribe.* Barómetro Global de la Corrupción. Coralie Pring, Editora. Berlín, Alemania. Retrieved from: https://www.transparency.org/en/publications/global-corruption-barometer-people-and-corruption-latin-america-and-the-car
- van Eeten, M. (2017), "Patching security governance: an empirical view of emergent governance mechanisms for cybersecurity", Digital Policy, Regulation and Governance, Vol. 19 No. 6, pp. 429-448. https://doi.org/10.1108/DPRG-05-2017-0029
- WEF, (2020) *Exploring Blockchain Technology for Government Transparency: Blockchain-Based Public Procurement to Reduce Corruption.* (17 de Junio de 2020). https://www.weforum.org/reports/exploring-blockchain-technology-for-government-transparency-to-reduce-corruption
- Zapata, E., Scrollini, F. & Fumega, S. (2020). ¿Cuán abiertos están los datos públicos? El barómetro de datos abiertos de América Latina y el Caribe 2020. Retrieved from http://scioteca.caf.com/handle/123456789/1710

caf.com
@AgendaCAF
innovaciondigital@caf.com