CAF DEVELOPMENT BANK
OF LATIN AMERICA

EXECUTIVE SUMMARY:

DIGIntegrity:

Digitally transforming the fight against corruption

Related topics:
Artificial Intelligence, Blockchain, Corruption,
Digital Government, Data Analytics, Integrity,
Smart Government,Technological Risks,
Public Procurement, Open Data

Estimated reading time: 15 minutes

A Note from CAF -Development Bank of Latin America-

State Director of Digital Innovation:
Carlos Santiso

Elaboration of the note:
Camilo Cetina, Paula Cruz Manrique

Publication coordinator:
Nathalie Gerbasi

Review and comments:
Anabella Abadi, Carlos Santiso, Gustavo Fajardo,
Nathalie Gerbasi and Pablo Sanguinetti.

The ideas and statements contained in this publication are the sole responsibility of the authors and do not represent the official position of CAF -Development Bank of Latin America-.

Editor: CAF

Vice President of Knowledge:
Pablo Sanguinetti

Graphic design:
Good;) Comunicación para el desarrollo sostenible

EXECUTIVE SUMMARY

DIGINTEGRITY: DIGITALLY TRANSFORMING THE FIGHT AGAINST CORRUPTION

The unprecedented corruption scandals in Latin America that have come to light in the last decade suggest that the region is facing structural challenges that combine endemic corruption with institutional weakness. The fight against corruption and impunity, in that respect, is a fundamental part of the development agenda and post-pandemic reactivation policies.

The acceleration of digital transformation accompanied by the globalization of the economy is having an ambivalent effect on governments' integrity agendas.

- **On the one hand, globalization and technology provide unprecedented opportunities for corruption to grow in size,** thus facilitating the concealment of illicit flows of money, and hindering jurisdictional capacities for detection and punishment.

- **But, on the other hand, systemic improvements in governance and collective action are being achieved thanks to new technologies** that help provide automated services and make public management processes more visible through open data and increasingly public records.

This report analyzes the opportunities offered by digital technologies as devices for public integrity and anti-corruption policies. It explores the "integrity dividends" derived from the growing digitization of governments and the increasingly intensive use of new technologies and data intelligence in the prevention of corruption. In 2019, CAF – Development Bank of Latin America undertook a comprehensive analysis of the progress and challenges of the anti-corruption agenda in Latin America and identified different fronts for action and institutional reform to promote greater integrity in public policies. This new report addresses the role of data, new technologies, and digital innovation in the implementation of effective integrity policies.

Report structure and key messages

The **DIGIntegrity** report argues that the incorporation of digital technologies has huge potential to improve public policies for the prevention, detection, and investigation of corruption phenomena. It also proposes that the adoption of digital technologies in public integrity can be structured in a **sequential order:**

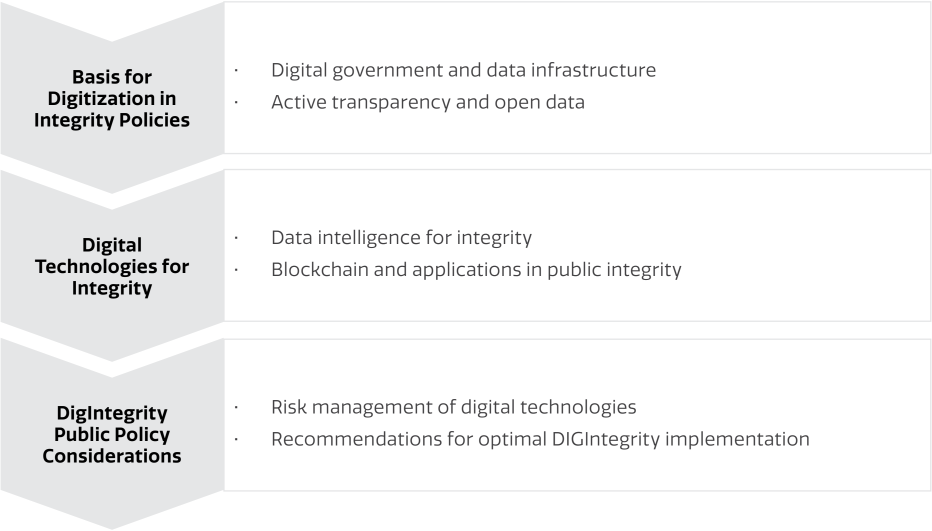
- First, **open data infrastructure** is essential. It is the cornerstone for implementing major digital innovations against corruption. To this end, it is important that **active transparency and open data policies are articulated with digital government policies** to generate an ecosystem that guarantees the quality, validity, and reusability of datasets of special interest in terms of public integrity.

- Second, governments can leverage **data intelligence techniques that make the tasks of preventing, detecting, and investigating acts of corruption more efficient.** Optimal use of such technologies requires the development of a computationally powerful infrastructure. From there, governments can **adopt more sophisticated technologies like artificial intelligence and blockchain technology to prevent acts of corruption** in public management processes that are especially vulnerable to integrity risks (e.g., public procurement, licensing).

- In addition, as digital technologies are integrated into public integrity policies, **governments should incorporate risk management measures when adopting new technologies,** due to the potential for misuse that can threaten their integrity.

- Finally, **an institutional environment must be created to ensure the long-term sustainability of the use of digital technologies.** This implies, for example, guaranteeing digital skills training; improving public procurement of artificial intelligence; and deepening justice reforms in favor of a more restorative scheme that ensures the recovery of public resources and the reparation of victims of corruption.

Figure 1 - Report Structure and Proposed Policy on Digitalization for Integrity



Basis for Digitization in Integrity Policies

- Digital government and data infrastructure
- Active transparency and open data

Digital Technologies for Integrity

- Data intelligence for integrity
- Blockchain and applications in public integrity

DigIntegrity Public Policy Considerations

- Risk management of digital technologies
- Recommendations for optimal DIGIntegrity implementation

Source: Authors.

Conditions for anti-corruption digital transformation

This report recommends that governments consolidate the minimum conditions required to incorporate digital technologies into their integrity and anti-corruption policies. The fundamental reason is that **the existence of open data and basic digitalized government services precedes technological development in more complex processes such as the prevention, detection and investigation of acts of corruption/corruption phenomena.** In this regard, it is important that governments consolidate an agenda on three preliminary fronts:

- **Digital government public policies**, in particular the digitization of public procedures and records, and the automation of administrative processes such as public procurement.

- **Implementation of the principle of proactive transparency,** so that the main decisions and processes of state management are considered public information. Such information must be accessible in **open data format** with the quality, completeness and structure necessary to allow its effective reuse.

- **Organization and availability of datasets with a recognized use in terms of integrity,** as well as some applications through which the reuse of data enables accountability initiatives and greater control of corruption.

Digitalization of government

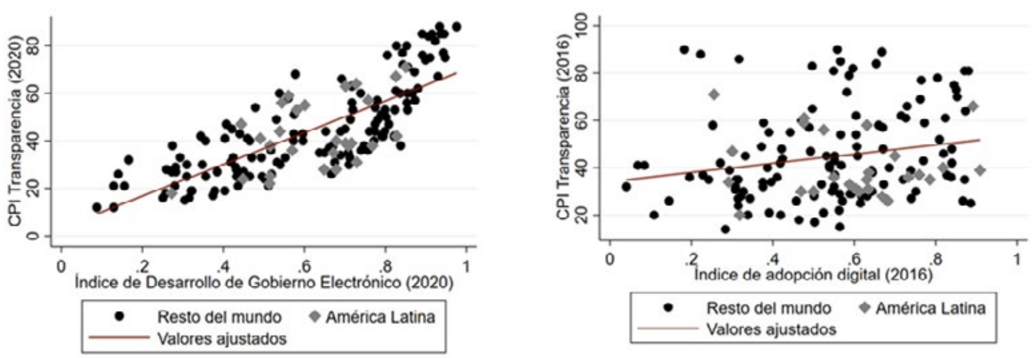
With the digitalization and simplification of procedures and the automation of administrative processes, governments can limit the discretional power of public authorities and thus reduce interactions that give rise to corrupt behavior. In addition, **the digitalization of the State makes it possible to centralize data containing information on the processes carried out by public administrations.** The digitalization of government services and public records implies the generation of a considerable amount of datasets, and also requires that citizens be able to access information related to digitized services and processes.

This data and information, when publicly accessible, have the potential to foster higher levels of transparency and integrity of the State. **According to multiple aggregate indicators, there is a clear correlation between the digitalization of the State and the control of corruption.** For example, countries with higher values in the United Nations E-Government Development Index (EGDI) also show better results in Transparency International's Corruption Perceptions Index (CPI), as shown in Graph 1 (higher CPI scores indicate lower perception of corruption in the country). The correlation of the use of alternative measures of digitization or corruption is robust. For example, in Panel B of Chart 1 the GDI is replaced with the World Bank's Digital Adoption Index. In Panels C and D, the CPI is replaced with, respectively, the World Bank's World Governance Indicators (WGI) control of corruption indicator and Transparency International's self-reported bribe payment indicator. In all cases, the same relationship is maintained.[1]

Chart 1 – Correlation between digitization and corruption in Latin American countries

Panel A. Electronic government & transparency

Panel B. Digital adoption & transparency

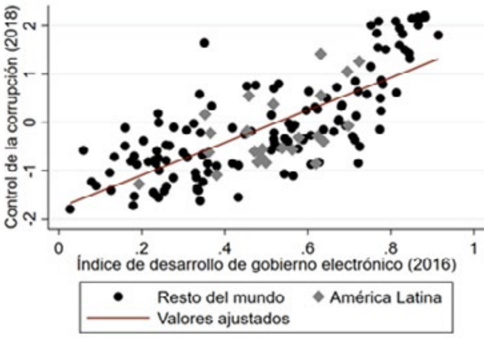


Note: The figure shows the United Nations E-Government Development Index (horizontal axis), where higher values indicate greater e-development, and the corruption control indicator of the World Bank's Worldwide Governance Indicators (vertical axis), where higher values indicate better results. The solid line represents the correlation between the variables. The sample is composed of 155 countries worldwide.

Note: The figure shows the World Bank's Digital Adoption Index (horizontal axis), where higher values indicate higher digital adoption, and Transparency International's Corruption Perceptions Index (vertical axis), where higher values indicate lower perception of corruption. The solid line represents the correlation between the variables. The sample is composed of 144 countries from around the world.

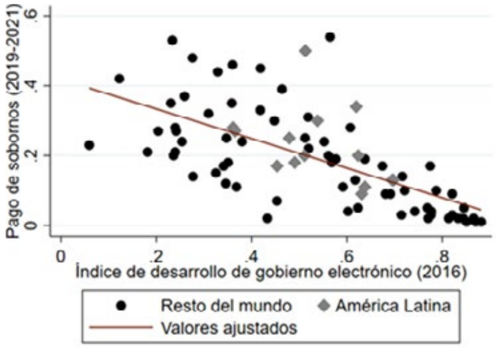
[1] In panel D, the sign of the correlation is negative because the corruption indicator used there takes higher values when corruption is high, contrary to the indicators in the other panels.

Panel C: Electronic government & control



Note: The figure shows the United Nations E-Government Development Index (horizontal axis), where higher values indicate greater e-development, and the corruption control indicator of the World Bank's Worldwide Governance Indicators (vertical axis), where higher values indicate better results. The solid line represents the correlation between the variables. The sample is composed of 155 countries worldwide.

Panel D: Electronic government & bribe payments

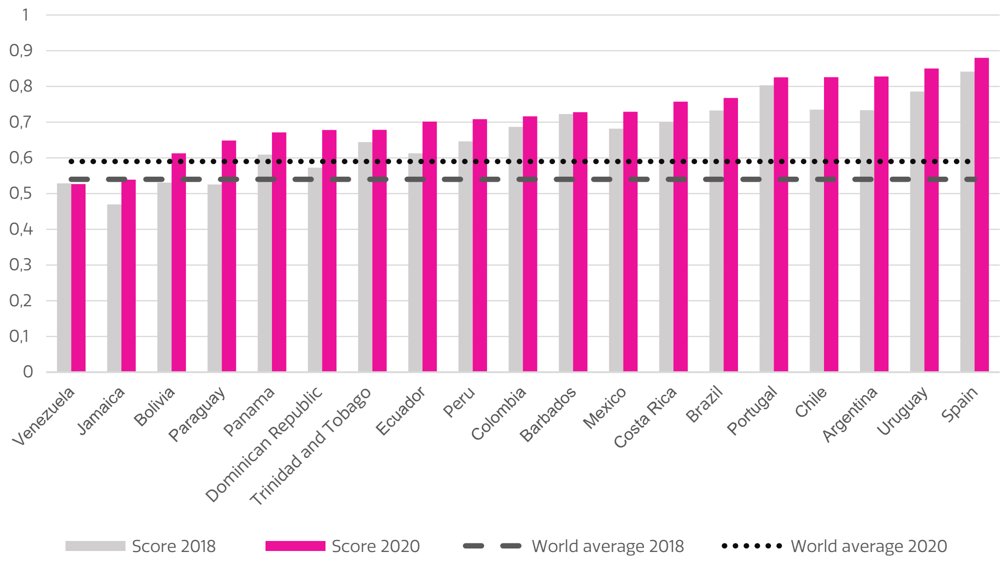


Note: The figure shows the United Nations E-Government Development Index (horizontal axis), where higher values indicate greater e-development, and the Bribe Payment indicator from Transparency International's Global Corruption Barometer (vertical axis), which indicates the percentage of users of public services who report having paid a bribe to receive those services. The solid line represents the correlation between the variables. The sample is composed of 82 countries around the world.

Latin America is making progress in the development of its digital government policies. According to the United Nations E-Government Development Index (EGDI), which is led by Denmark, Korea and Estonia, 17 of the 19 CAF member countries scored above the world average in 2020[2] (see Graph 2).

[2] Jamaica and Venezuela, with scores of 0.5391 and 0.5268, respectively, were the two CAF member countries that ranked below the EDGI world average in the 2020 measurement. Globally, it is worth noting that Denmark (0.9758), Korea (0.9560) and Estonia (0.9473) ranked the highest with scores very close to the maximum (1).

Chart 2 – EDGI scores for CAF member countries (2018 & 2020).



Source: UN, 2020. The EDGI scale ranges from 0 to 1, Denmark (0.9758), Korea (0.9560) and Estonia (0.9473) were the leading countries in 2020. The global average refers to the average score of the 193 countries included in the measurement for the years 2018 and 2020.

The progress Latin America is making in digitalization can be an important catalyst for progress on a renewed integrity and corruption prevention agenda. To this end, digitization and technology must be complemented by regulations and institutional arrangements that facilitate active transparency and open data.

Active transparency and open data

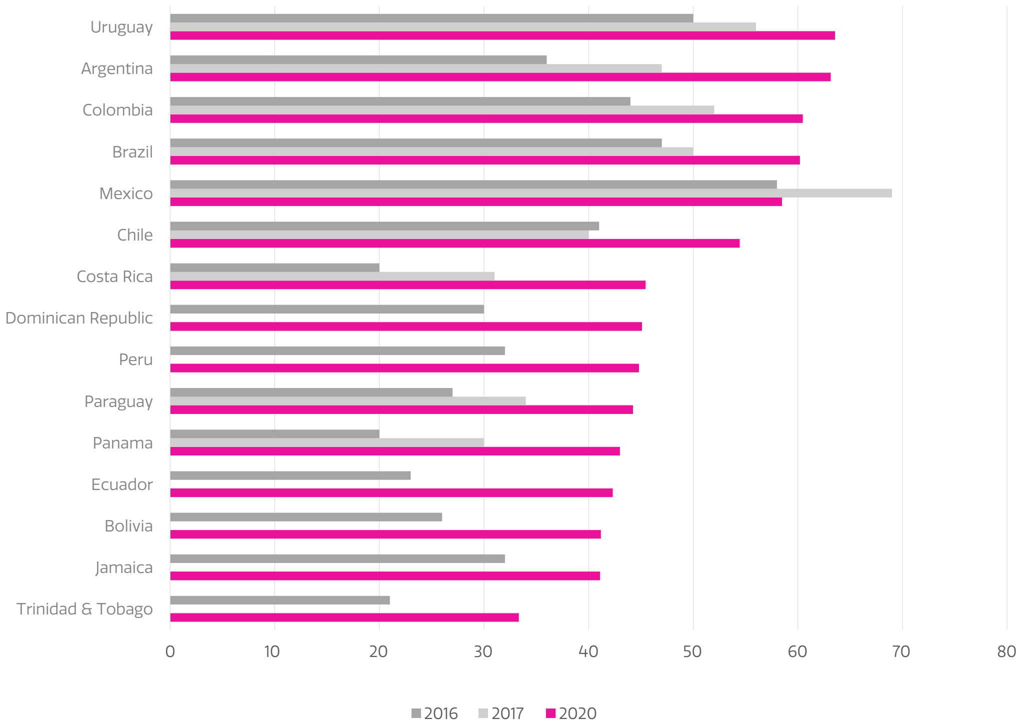
The concept of transparency not only requires publicizing the actions of public institutions and authorities, it also implies that citizens must be empowered to exercise control over the decisions of public authorities that affect them, in addition to raise awareness of the State's actions.

Additionally, proactive transparency requires government agencies to publish systematically, periodically and in a timely manner, without any requirement whatsoever, all information and data that are not specifically subject to legal or constitutional reservations. In this respect, any person, regardless of their status (citizen, foreigner, natural or legal person, adult or minor) and without the need to prove a particular interest or condition, has the right to access information on public authorities and even private entities that provide public services.

While regulation on access to public information in Latin America is almost three decades old, **thanks to the principle of active transparency, as well as the digitization**

of information, governments are moving toward open data. According to the 2020 Regional Open Data Barometer for Latin America and the Caribbean, which measures readiness, implementation and the impact of open data, the region showed marginal growth compared to the 2016 results, with an average score of 40.38 on a scale ranging from 0 to 100. This reflects a slowdown in the open data agenda (Zapata, Scrollini & Fumega 2020).

Chart 3 - Results of the Regional Open Data Barometer for Latin America and the Caribbean for CAF member countries 2016, 2017 and 2020.



Source: Zapata, Scrollini & Fumega (2020). The scale ranges from 0 to 100, a score of 100 shows higher levels of readiness, implementation and openness. The United Kingdom leads the ranking with a score of 76.

[3] This sub-index measures the willingness of governments, citizens and businessmen to ensure the openness of data..

[4] This sub-index assesses the degree to which governments publish key datasets in an accessible, timely and open fashion.)

[5] This sub-index evaluates the extent to which the publication of open government data has had a positive impact on a variety of sectors in the country.

Datasets and their use in public integrity

Once countries enable data infrastructure and governance based on their digital government policies, it is possible to adjust active transparency standards so that access to public information is based on open datasets. **Open data enables at least three forms of corruption prevention,** as outlined below:

- **Limits to discretionary decisions and reduction of bureaucracy.** Open datasets not only come from the need to publish information on t governments' actions; they also come from the digitization of governments' services that reduce bureaucracy and simplify processes. For example, the digitization of public procurement, which in principle seeks to make complex government contracting processes more efficient and faster, now allows citizens to access data and information on the resources invested in public procurement and contracting. This makes it possible to exercise control over risk factors such as bidding and contracting modalities, since closed and discretionary processes present a greater risk of corruption.

- **Accountability processes** through digital means and in real time. This is possible through platforms that capture different data sources to comprehensively present public management in specific sectors. For example, the MapaInversiones applications in countries like Colombia and Costa Rica integrate information from the budget cycle and the execution of large investment projects to demonstrate to citizens the progress of works and the allocation of resources for the delivery of public goods.

- **Civic control and citizen participation.** Organized civil society is making use of open data through initiatives promoted by civic-tech and gov-tech startups, to bring citizens closer to public management and present them with relevant information on control, simply and at a low cost. For example, in October 2021, Paraguay introduced a mobile application called "PresupuestApp," which not only allows citizens to make inquiries about budgets and approved expenditures of any public institution, but they can also report or denounce irregularities to the Ministry of Finance.

A consolidated open data agenda allows governments to advance in the adoption of internationally recognized standards of openness, in areas of special interest for public integrity such as procurement, taxation, public spending, infrastructure, civil service, among others. For example, Inter-American Open Data Program to Prevent and Fight Corruption (PIDA, by its acronym in Spanish) adopted by the Summit of the Americas in 2018 contains a set of recommendations to leverage more than 30 datasets that can be used in the fight against corruption. The implementation of initiatives like PIDA makes it possible to standardize the tasks of production, publication and reuse of data, in order to have useful information in anti-corruption programs and initiatives.

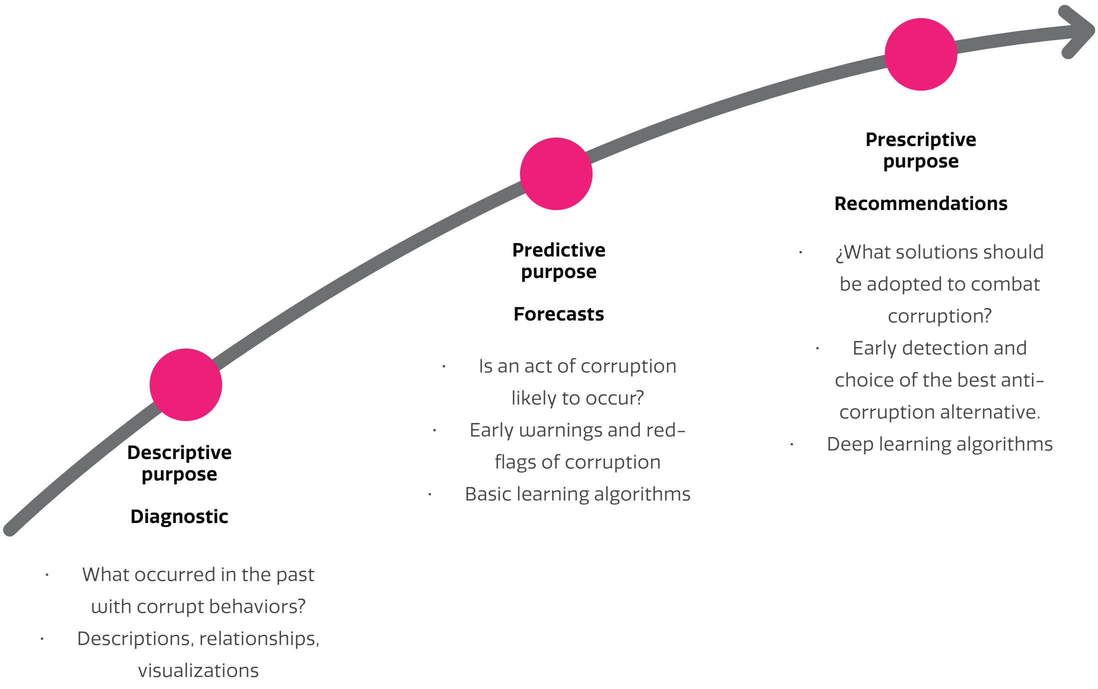
Digital technologies for integrity (I): Data intelligence

Open data and data infrastructure open up the possibility of taking large datasets and reusing them to prevent corruption phenomena. This can be done by combining predictive analytics with the application of computing power for big-data processing.

Several governments are adopting a disruptive approach in their corruption-risk mitigation schemes, which **consists of using digital technologies and data processing to prevent, detect, and investigate corruption.** These innovations can make intelligent use of data through **descriptive and predictive models (although the literature**

distinguishes four major uses: diagnostic, descriptive, predictive and prescriptive)[6]**.** They also represent an incremental advance in the fight against corruption in that they allow increasingly sophisticated analysis in the early and timely identification of acts of corruption. The conclusions drawn from the analysis of this information also serve to adjust public integrity policies based on evidence (see Figure 2).

Figure 2 - Evolution of the purpose of using data as an anti-corruption strategy.



Descriptive purpose

Diagnostic

- What occurred in the past with corrupt behaviors?
- Descriptions, relationships, visualizations

Predictive purpose

Forecasts

- Is an act of corruption likely to occur?
- Early warnings and red-flags of corruption
- Basic learning algorithms

Prescriptive purpose

Recommendations

- ¿What solutions should be adopted to combat corruption?
- Early detection and choice of the best anti-corruption alternative.
- Deep learning algorithms

Source: Own elaboration.

[6] See: https://www.oracle.com/business-analytics/data-analytics/

Descriptive Models

Developments in DIGIntegrity for descriptive purposes generally reuse open datasets to identify anomalies that may be associated with corruption risks. Free and direct access to information regarding government actions made possible by proactive transparency and open data policies, combined with the use of programs and platforms to process the datasets, allows for a comprehensive understanding of public management and corruption phenomena.

One of the most effective applications of technology and descriptive data analytics is **visualization,** which, although by itself does not generate new information, transforms the structure of data representation. Since humans find it easier to understand information in graphical representations than in more complex structures, visual tools make it possible to process a large amount of data and present it in a clear and simple way. The contribution of visualization lies in its ability to simplify representation without losing information; not the data and information that feed it.

Visualizations make it possible to identify features that are difficult to detect with simple manual observation of databases. Tools based on the use of mathematical techniques to translate multidimensional data such as frequencies, moments, relationships or links into rather intuitive figures such as networks, nodes, clouds, heat maps and hierarchical schemes ("treemapping") are very useful for detecting hidden relationships, demonstrating the existence of complex networks and tracing the movement of money flows. In this way, **descriptive analytics makes it possible to detect relationships, patterns and anomalies among the data. These findings guide and alert analysts to cases that merit particular follow-up and investigation.**

For example, querying the Financial Crimes Enforcement Network **(FINCEN)** website for debit card money laundering activity in the United States yields more than 37,000 results. In order to analyze information on similar scales, the United Nations (UN) developed a platform for detecting money laundering networks (GoAML) and another for exchanging financial intelligence information (GoINTEL), which are fed by the reports made by Financial Intelligence Units in monitored countries. The detail of the recorded transactions generates a volume of data that cannot be analyzed by using tabular methods.[7] The UN applications make it possible to map money laundering networks and create an interface so that the movements of persons or corporations under investigation can be detected in real time by the intelligence, investigation and prosecution units, so that they can confirm (or rule out) the existence of a network of illicit money movements.

Predictive models

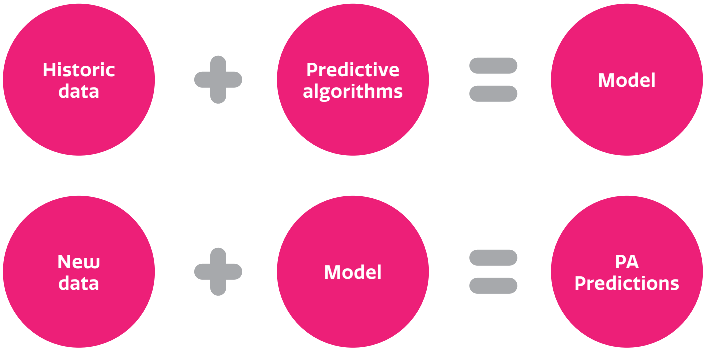
Predictive models **make it possible to estimate or assign a numerical value or probability score to the occurrence of a particular phenomenon or behavior.** Thus, this technique is of interest for public integrity policies because it can determine the probability of occurrence of acts of corruption in some public actions. To determine this probability, statistical analysis, queries and automatic learning algorithms are performed on new and historical datasets, creating predictive models (See Figure 3).

These digital technologies generate an advance in the fight against corruption because they make it possible to overcome a reactive role in favor of a preventive role. This is possible because the intelligence of

[7] That is, by examining functions and values in simple arrays of rows and columns, and then selecting data cells of interest.

digital technologies, through data science, has the ability to emulate human intelligence, anticipate changes in the environment and predict the occurrence of phenomena of interest (Llinás, 2003).

Figure 3. Mechanism of predictive analytics



Predictive data analytics techniques can be based on either basic or deep machine learning. Basic machine learning requires the identification of specific risks[8] or atypical behaviors at each stage of the procedure in order to achieve a higher level of transparency. Once the corruption risks are programmed into the models, the algorithms detect their presence in the analyzed data, generating warning signals. In addition, deep machine learning algorithms can also be used to analyze both structured and non-structured data. Deep learning algorithms, unlike basic learning algorithms, perform several iterations of the data training process after partitioning the unstructured dataset. Thus with no previous programming of corruption proxies or predictors, such algorithms identify patterns stemming from past corruption investigations, generate models applicable to new data and thus detect and/or predict possible corruption cases.

An example of PA in corruption prevention is the Korean Government's Collusion Indicator Analytic System (BRIAS), managed by the Korean Fair Trade Commission (KFTC). BRIAS uses the open data generated by the Korean Public Procurement and Contracting System (KONEPS) to build an automated system of risk indicators or red flags for potential procurement irregularities or inefficiencies. Within this system, data collection starts from the moment a user registers, either as a visitor, bidder or buyer, so that their credentials (IP address, dates and times of visit, modules visited, communications, etc.) are used for statistical and analytical purposes to determine risks of collusion and corruption in public procurement.

[8] For example, in the public procurement sector there are lists of warning signs at each stage of the procurement chain (Volosin 2015). Successive additions to contracts, long delays between the award of the contract and the actual start date of fulfillment, sudden changes in the business purpose of the contracting companies, are some examples of risk in public procurement (Cetina, 2020a).

Another example is the **Analisador de Licitações e Editais (ALICE)—a tool for the analysis of public procurement, bids, and tenders—, which was developed in 2017 by Brazil's Controladoria-Geral da União (CGU)** [Office of the Comptroller General of the Federal Government]. ALICE takes information from Brazil's public procurement system (Comprasnet, run by the Ministry of Economy), downloads the texts of the contracting process documents and generates an early warning report based on its risk assessment of the contracting processes. ALICE takes the text of the documents posted on the Comprasnet website. The text classification models work by assigning categories to the data according to its content: it detects topics or themes, identifies keywords, identifies names (either buyers or vendors), among other data to determine the contract profile. It then detects combinations of words that may make a contract more risky or deserve more attention due to its amount, scope, contracting entity, or terms.

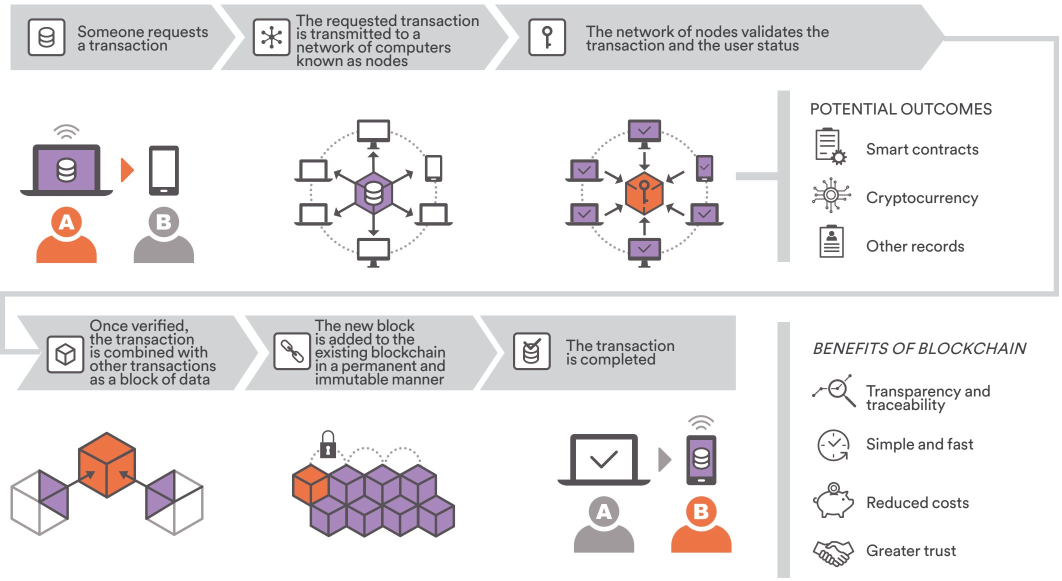
On a daily basis, ALICE flags contracts containing text deemed worthy of the attention of CGU auditors. **An automatic system is then activated and e-mails are sent to the auditors indicating which contracts are in need of further analysis.** In addition, daily lists and contract identifiers are stored in a centralized database.

Digital technologies for integrity (II): Blockchain

Corruption in the public sector generates distrust between citizens and public institutions. Transparency of government decisions and open public records facilitate the monitoring of government decisions, which helps to reduce corruption risks through citizen and/or institutional control mechanisms. **Blockchain technology goes further: it makes open public records tamper-proof so that fraudulent agents cannot modify, alter, or falsify them.** This unlocks potential in certain processes such as identity verification, tracking transfers from governments to citizens, recording ownership of certain assets, and fairness and integrity at each step of the public procurement process.

Blockchain or "digital signatures of information" is a public distributed ledger technology that allows for transactions to be recorded in blocks of information. Each block contains information from previous transactions or blocks, creating an information chain in which every transaction has an immutable audit trail and is validated by all stakeholders or "nodes" in a decentralized way in real time (See Figure 4). This technique is supported by a public distributed registry that always maintains a growing list of records or transactions, gathered into blocks, which are secure against any revision or adulteration and are fully traceable (CIAT, 2018).

Figure 4 - How blockchain technology works: Step by step


Someone requests a transaction
The requested transaction is transmitted to a network of computers known as nodes
The network of nodes validates the transaction and the user status
A
B
POTENTIAL OUTCOMES
Smart contracts
Cryptocurrency
Other records
Once verified, the transaction is combined with other transactions as a block of data
The new block is added to the existing blockchain in a permanent and immutable manner
The transaction is completed
A
B
BENEFITS OF BLOCKCHAIN
Transparency and traceability
Simple and fast
Reduced costs
Greater trust

Source: Atencio (2020)

Blockchain technology makes records accessible, immutable, and secure, preventing central authorities from acting with excessive discretion and allowing stakeholders to consult and validate transactions. For example, in a public procurement process—which relies on records documenting compliance with legal requirements—blockchain can ensure the traceability of alterations to documents such as terms of reference; it can also prevent changes to tenders that would violate legal terms; and it ensures the visibility of processes for all stakeholders, including bidders, public entities, and civil society.

This technology is being tested through pilot projects. For example, **in Colombia, the Procuraduría General de la Nación (PGN, by its acronym in Spanish) [the Inspector General's Office] developed a proof of concept for the application of authorized blockchain technology in the contracting of the school food program in the city of Medellín.** Blockchain showed applicability in several aspects of public procurement, as follows:

- First, the blockchain mechanism assigns a pseudo-anonymous identifier to suppliers but does not erase their actions within the bidding process, which renders it impossible for bidders to be identified, preventing irregular agreements between companies or between a bidder and an official to influence the bidding.

- Once the bidding terms of reference are made public, they cannot be altered. Likewise, citizen comments cannot be eliminated and are kept on record.

- Additionally, the bids received by the contracting entity remain anonymously registered in blockchain with the attached documents sent by suppliers; they cannot be opened until the scheduled start date of the evaluation process. In fact, the public entity does not know where the proposals come from before starting the proposal evaluation process.

- · All of the above helps to prevent the existence of illicit agreements that could be made in advance and would unduly favor a particular bidder.

The added value of this technology, with respect to any other, lies in decentralization, immutability and traceability of the records. In case there is any irregular transaction throughout government's procurement procedure, blockchain keep author's identity immutable records that can be traced. Also, for a corrupt conduct to take place a consensus of all nodes in the network would be required.

The contribution of the blockchain in the fight against corruption in public procurement is promising, but it also has some important limitations. Those include suppliers' privacy and anonymity, uncertainty regarding scalability, bid rigging and collusion behaviors between bidding companies outside the platform, among others.

Applications of blockchain technology to improve integrity in other transactions are just being explored. There is no systematic evidence yet that determines a proven effect of blockchain on corruption risks in public management. However, the available literature documents a growing use to ensure integrity within especially sensitive transactions using this technology. Other examples on this front include:

- **Integrity in the distribution of COVID-19 vaccines:** In the United States, blockchain technology was used to verify the quality, origin and distribution of COVID-19 vaccines.[9] The blockchain's inherent characteristics (immutability and distributed decentralization) prevent manipulation and adulteration of data regarding the delivery and administration process.

- **Prevention of money laundering:** The blockchain can be adopted as a decentralized certification authority that can maintain the mapping of identities and money transactions between individuals across financial institutions. A blockchain identity system allows end users to own and control their personal identity, reputation, data and digital assets. This facilitates oversight by financial regulators, law enforcement and tax administrations, which would have a reliable source of information and immediate access to blockchain records.

- **Integrity in unconditional cash transfers:** Blockchain can mitigate these risks and diversion of resources in government cash transfers to provide livelihoods to the most vulnerable citizens. For example, the World Food Programme (WFP) developed the **"Building Blocks"** project to determine the feasibility of incorporating blockchain technology among more than 100,000 refugees in the Middle East. Cash is stored in a beneficiary's account, whose value and data are validated by different nodes on the blockchain. Then, based on a smart contract, the cash that beneficiaries receive or spend is paid through a commercial financial services provider, and the payments are stored in blockchain.

[9] UNODC has documented corruption phenomena like market entry of counterfeit vaccines, theft of vaccines within distribution systems, and the administration of vaccines under nepotism or favoritism.

Public Policy Considerations

Technological risk management

Just as there are digital technologies for integrity, governments must ensure integrity in the use of technologies. The specific technologies outlined above with important anti-corruption applications are also exposed to criminal and misuse phenomena, which can undermine their potential in public integrity policies. For example: the abuse of public functions for activities such as trafficking of personal data or privileged tax information, money laundering, data theft for identity fraud, among others, are risks that can potentially generate costs equivalent to corruption.

This report distinguishes three types of risk of particular interest to governments. Each is associated with the three clusters of digital development addressed in this report, namely digital government, data intelligence, and blockchain.

Digital identity

The first risk factor is digital identity. Identification systems facilitate interactions between individuals, government, and private entities; ensuring the identification of all individuals is not only a right, but also a **sustainable development goal (16.9).** **Identification corresponds to a combination of characteristics or attributes of a person that make him or her unique in a given context.** Thus, in the digital world, identification, authentication, and authorization activities do not end with the simple assignment of *"Users and Passwords."* Identification involves a procedure by which elements, both internal and external, are collected to assign an identity, with certain attributes, to a specific person.

Digital Identity Systems (DIS) can be targeted by criminal networks seeking to steal data and impersonate someone (identify theft) to access goods or services. Managing this risk is not limited to making provisions for privacy and security breaches inherent in the capture, storage, and use of sensitive personal data. Risks also exist if there is dependence on a specific technology or vendor; or if the infrastructure and connectivity in a country is very limited, which can make it difficult to implement digital identification systems that require power and connectivity for data transfer or verification of duplicate biometric enrollment. Technical and institutional capabilities for central cybersecurity agencies are needed to enable a secure environment for digital identification systems, as well as to structure DIS procurement processes (public procurement) so as not to end up with failed procurements, delays (e.g., due to appeals) and vendor and technology lock-in.

Protection of personal data

The second risk factor is the protection of personal data. Even when digital developments make it possible to simplify procedures or apply data analysis techniques to improve processes such as the early detection of corruption risks, **there are implicit**

risks related to the privacy and security of personal data, which underlie the use and purpose of technologies. The concept of "personal data" includes any type of information about an individual that can be "objective" (like age, gender, or physical address) and "subjective" (like opinions or evaluations of that individual about a platform or service via digital means).

Personal data is subject to protection because privacy is considered a fundamental right under the rule of law. In that regard, a correlative obligation of governments is generated to guarantee an adequate level of protection with respect to the information attributed to an individual. The implementation of data privacy protection goes beyond the adoption of personal data protection laws. It implies introducing privacy by design; thus, the data controller, from the beginning and throughout the life cycle of the data processing, must have protection mechanisms for the collection, storage, uses, circulation, access, and destruction of data.

Another risk front regarding personal data is the security of the information systems used to manage them. Security refers to protection and devices against: accidents, unauthorized access, modifications, or unauthorized destruction. Information security, known as cybersecurity or data security, is a major challenge and a vital component in the relationship of trust between citizens and their governments. In the same way as identity theft, cyber-attacks can cause economic damage, through the interruption of information and communication systems and/or through the loss or alteration of confidential information or other important data.

Although in Latin America there are some regulations for personal data protection,[10] this is not the case with governance mechanisms for cybersecurity to prevent unauthorized access to digital platforms and consultation, alteration, or extraction of data. Van Eeten (2017) **documents that the responsibility for security governance has shifted from device owners to large intermediaries.** For example, Google is more proficient at securing the Gmail platform than most companies are at securing their own mail servers. The OECD (2011) has referred to these companies as Internet intermediaries. Their security practices increasingly determine the security of governments and citizens alike. The big limit here is that there is a fundamental information asymmetry that prevents the use of systematic evidence to verify which security models, practices, and policies are appropriate for protecting data.

Use of blockchain for cryptoassets

Finally, the third risk factor is the adoption of blockchain technologies in the development and expansion of cryptoassets without more regulation. **Cryptoassets correspond to digital financial assets created from cryptography and blockchain technology,[11] which allow the performance of secure, decentralized, and distributed economic transactions and whose issuance is open to whoever wants to issue the cryptoasset.**

The decentralization and encryption on which the blockchain is based allow the issuance of

[10] Although not necessarily for the entire processing cycle—collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, etc.

[11] Cryptography is used in blockchain technology. The hash, being the most widely used, is a method of applying a cryptographic function to data, which identifies any data message of any size (e.g., a file, text, or image). In general, it enables the individualization of the message and thus, perceive if there were changes in the data; even the smallest change in the input (e.g., changing a single bit, a single letter, or a comma) will result in a completely different hash.

cryptoassets and facilitate money laundering activities. There is evidence of drug trafficking networks converting their funds into cryptoassets and then sending them around the world and converting them back into foreign currency. Additionally, it is difficult for authorities to investigate this activity in individual cases, as well as to capture the resources, because when such funds are converted from official currencies to cryptoassets on blockchain, there is no trace of how the money was originally made.

The challenge for regulators is to find appropriate instruments to address the risks originating from the use of blockchain and the adoption of cryptoassets. Existing regulatory instruments are limited when it comes to addressing financial and consumer crime and money laundering risks. The **Bank for International Settlements** (BIS)[12] recommends that authorities first make progress with their regulatory agenda based on the economic functions to be granted to the cryptoasset. In 2019, the Financial Action Task Force (FATF) introduced **guidelines** asking governments to assess and mitigate the money laundering and terrorist financing risks associated with cryptoasset activities and service providers. It called for service providers to be registered and supervised by competent national authorities.

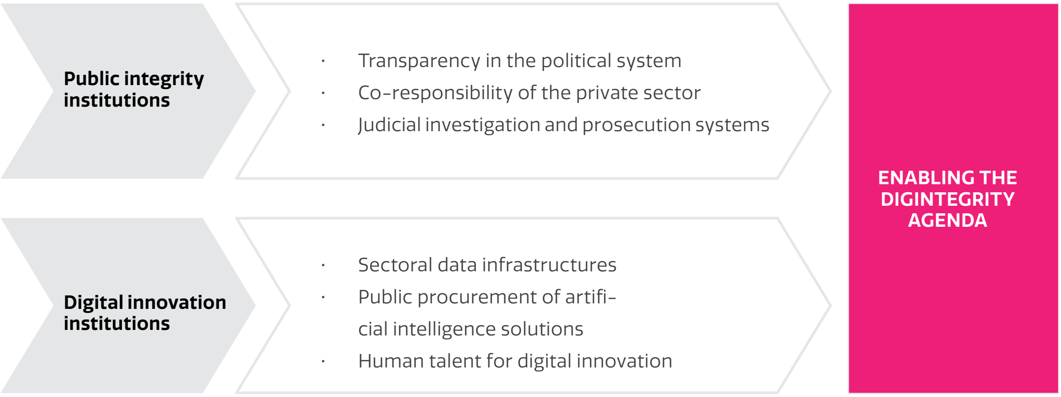
Policy recommendations and institutional alignment

The role that data-driven technologies play in public integrity is increasingly being recognized by governments, multilateral organizations, and civil society. However, **digital innovation, the application of data-driven technologies, and big data computing power are not a 'silver bullet' to eradicate the problem of corruption.** The institutional context and the governance framework that frames aspects such as relations between the public sector and private enterprise, and between the state and society, are determinants for whether or not corruption networks thrive (CAF, 2019).

In this regard, fully exploiting the potential of digitalization in public integrity policies **demands that government institutions modernize in two separate areas: institutional adjustments that promote integrity; and the adaptation of public authorities to the digital era.** Public policy recommendations for the effective implementation of digital innovations in public integrity fall into these two areas (see Figure 5).

[12] Established in 1930, the BIS is owned by 63 central banks representing countries around the world. These 63 countries account for about 95% of the world's GDP. Its head office is located in Basel, Switzerland, and it has two representative offices in Hong Kong and Mexico City. In Latin America, the Central Banks of Argentina, Brazil, Chile, Colombia, Mexico and Peru are shareholders. The BIS's mission is to "support central banks' pursuit of monetary and financial stability through international cooperation, and to act as a bank for central banks" (See www.bis.org)

Figure 5 – Public integrity and digital innovation institutions


Public integrity institutions
Transparency in the political system
Co-responsibility of the private sector
Judicial investigation and prosecution systems
Digital innovation institutions
Sectoral data infrastructures
Public procurement of artificial intelligence solutions
Human talent for digital innovation
ENABLING THE DIGINTEGRITY AGENDA

Source: Own elaboration.

Latin America needs to modernize its institutional arrangements so that the anti-corruption agenda is attuned to digital acceleration and allows technologies to generate integrity dividends. This report highlights three strategic groups of recommendations to drive institutional modernization and the DIGIntegrity agenda:

- **Transparency in the political system:** Elections generate the first phenomena of state capture by corrupt agents, given the need for funds to finance political campaigns (CAF, 2019). The experience of major corruption cases in Latin America shows that illicit agreements were gestated in the electoral phase.

- **Co-responsibility of the private sector:** Private companies and civil society have strong incentives to influence public policy decisions. In addition, they are important actors in electoral processes as they can finance political campaigns. Their co-responsibility to generate integrity in public policies and avoid state capture should be part of the strategy to fight corruption.

- **Legitimate, agile, and restorative investigation and prosecution systems:** In Latin America, it is essential that a greater capacity to deter corrupt agents through a legitimate justice system that imposes effective sanctions be developed. It is also crucial to focus criminal and disciplinary proceedings on the recovery of resources that are squandered or misappropriated and on reparations for the victims of corruption.

At the same time as modernizing the integrity ecosystem in governments, adjustments are also required in the digital innovation ecosystem for the public sector to ensure the long-term sustainability of the adoption of digital tools within public integrity strategies. This report highlights three main areas of focus for modernization efforts. They are:

- **Organized sector-specific data infrastructures and open source.** Since perpetrators of corruption have different strategies and modalities well-adjusted to the type of public good provided by the state (health, education, security, justice, infrastructure, etc.), sector-specific datasets increase the effectiveness of digital technologies for integrity. Additionally, digital innovations aimed at improving transparency levels can be shared and reused by other public entities or civil society interested in the fight against corruption. This is the case, for example, with the Buenos Aires **BAObras** works visualization platform and Mexico City's **Tianguis Digital** portal.

- **Digital talent in anticorruption policy agencies.** The incorporation of digital technologies in public integrity strategies assumes that those who handle and use them have the knowledge and expertise required. This is not necessarily the case for Latin American public officials, so it is necessary to strengthen the training and retention of talent that effectively uses digital technologies in carrying out their functions, as in the prevention, investigation and detection of corruption. For example, within the integrity ecosystem, specialized units in data science and intelligence should first be created within the control agencies.

- **Public procurement of artificial intelligence.** Just as there are special standards to ensure integrity and quality in public procurement of infrastructure (Fajardo, 2021), it is equally strategic for public entities to develop special standards for the structuring of needs and procurement processes of artificial intelligence platforms for anti-corruption purposes. There are ethical standards, as well as transparency and accountability standards for this technology, which influence its use and quality.

REFERENCES

- 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 custome*r. 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 BANCO DE DESARROLLO
DE **AMÉRICA LATINA**

caf.com
@AgendaCAF
innovaciondigital@caf.com