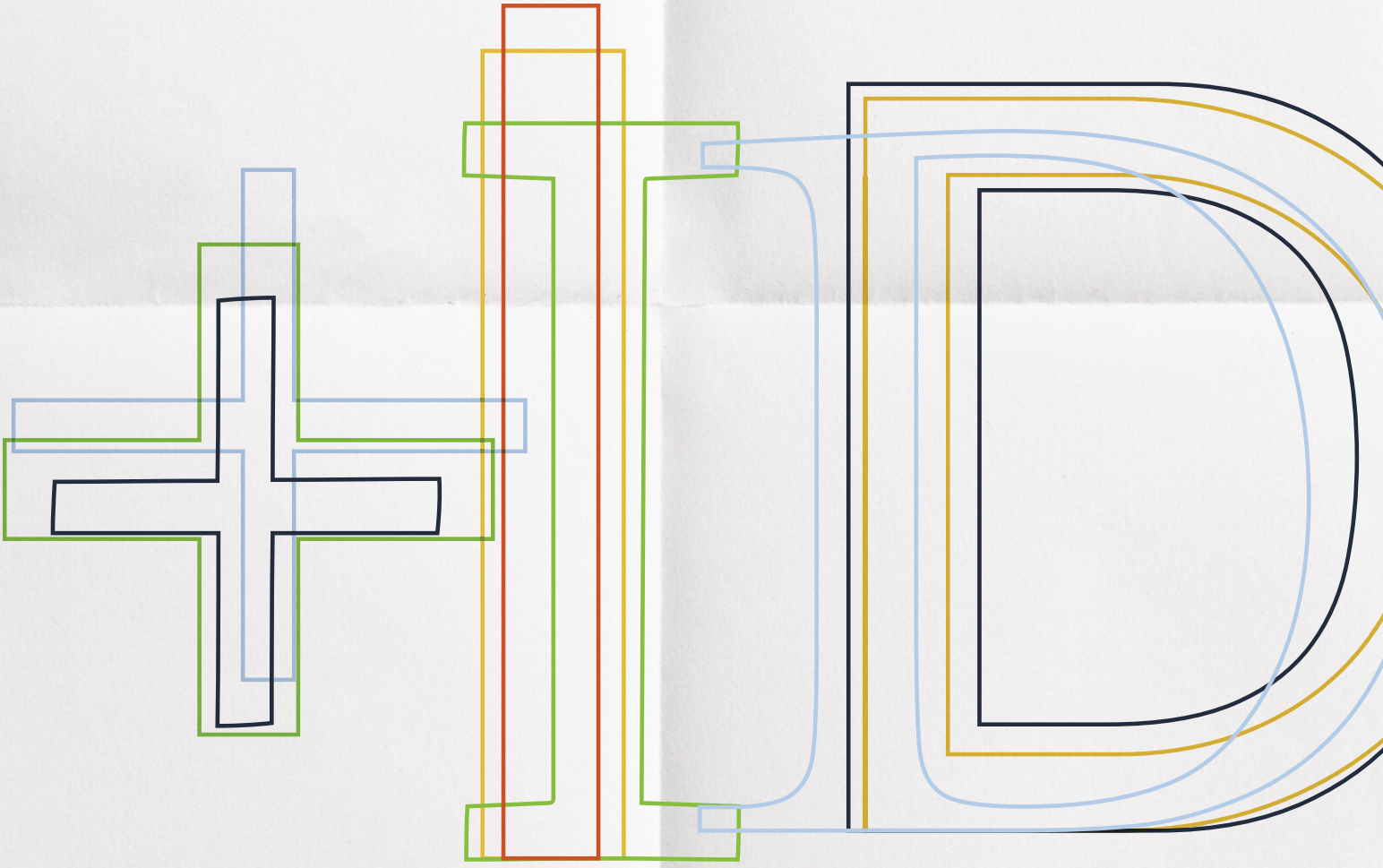
Identifying the Future

Building Scenarios for the Future of Digital Identification Systems in Latin America and the Caribbean



AUTHORS
Lourdes Gallardo Montoya
Arturo Muente Kunigami
Eugenia Valdez Tamayo

JEL Codes: H11, O21, O33

Keywords: digital identification, scenario planning, institutional capacity, digital transformation, digital literacy

Inter-American Development Bank
1300 New York Avenue, N.W.
Washington, D.C. 20577
www.iadb.org

Acknowledgements

This work stems from the scenario planning process carried out during 2019. The authors would like to thank all participants to these workshops: Elena Arias, Adela Barrio, Pablo Bachelet, Estefanía Calderón, Aitor Cubo, Rodrigo López, Mario Casco, Jennifer Nelson, Ariel Nowersztern, Cristina Pombo, María Ángeles Reyes, Florencia Serale, Luis Tejerina, Harold Villalba (IDB), Thea Anderson (Omidyar Networks), Julia Clark (The World Bank), Gemma Galdón (Eticas Consulting), Julián Najles, and Rebeca Omaña (Organization of American States). Gerard Drenth, Partner at Normann Partners, facilitated the process. Special thanks go to Jonas Hoffmann, Senior Associate at Normann Partners and Estefanía Calderón (IDB) for their valuable comments and recommendations.

Contents

Building Scenarios for the Future of Digital Identification Systems in Latin America and the Caribbean

Over the past few years, countries with diverse economic, demographic, and political contexts have rolled out digital identification systems with broad coverage, with a wide array of benefits for government, citizens, and private sector. Robust identification systems have been linked to facilitating access to social, economic, and financial services; improving public administration; and innovating on service delivery, among other benefits. In fact, the digital identification systems of Canada, Estonia, Israel, and Spain have been acknowledged as reference cases for countries looking to improve their own identity systems.

Among Latin American and Caribbean (LAC) countries, the characteristics of current identification systems are diverse, and they have different maturity levels. Some countries have invested in initiatives to modernize their identification systems, while others are still working with manual and paper-based processes. The rapid advances in technology on identity management is changing the way digital identification systems work. Several new technologies are being used in various aspects of the identity lifecycle.[1] This new landscape is creating opportunities to define strategies and work plans that can help close the existing gaps in legal and regulatory frameworks, privacy, trust, personal data protection, and inclusion.

Improving identification systems has become one of the main priorities of LAC countries, especially in cases where governments want to implement digital government initiatives that help introduce their population to the digital economy and improve service delivery. One of the main hurdles that governments face when designing these interventions is the constantly changing landscape, enabled to a large extent by technological changes and innovation. This in turn introduces a high degree of uncertainty with respect to any future development.

1 The identity lifecycle includes the following processes: registration, issuance, authentication, authorization and identity management. More information can be found in the following link: http://documents.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf

Introduction

The Inter-American Development Bank (IDB), through the Innovation in Citizen Services division (ICS) and with the support of the Knowledge Innovation and Communication sector (KIC), proposed to build a set of future scenarios as a way to approach this uncertainty and to prepare the IDB and its main stakeholders for the future of digital identification systems in the LAC region. We partnered with NormannPartners, a strategy firm with vast experience across the world working with private and public entities carrying out this type of exercises.

During the process, a wide group of stakeholders from government, multilateral entities, and other sectors actively participated. The whole process was insightful, from researching existing trends to creating the actual scenarios to testing our existing strategy. It created an opportunity to identify specific interventions that would avoid and/or to take advantage of potential events.

In general, the scenario planning exercise allowed us to identify:

- Specific areas related to digital identification that need to be included in the dialogue with our counterparts.
- Topics related to digital identification where further research is needed.
- Policy recommendations for the IDB and the countries we work with.

The report is divided into four parts. It begins by presenting some insights and recommendations that have been drawn from the scenarios that we created. The second part briefly describes the process of scenario planning and how it was carried out for digital identification. It then presents the three scenarios that were created, including a section that details each scenario in the context of the COVID-19 pandemic. Finally, section four presents a series of templates and a how-to guide for policymakers interested in using the scenarios to review their existing strategies.

The aim of this scenario exercise was to improve strategic decision making; the co-created scenarios must not be taken as predictions or projections. The overall aim of the report is to encourage an open discussion on the future of digital identification systems from a non-traditional point of view. Hopefully, it will spark innovative ideas that may inform our response to the challenges ahead and allow governments, private sector, civil society, and citizens at large to re-think their role in the digital identification ecosystem in the next 10 years.

POLICY RECOMMENDATIONS

Part

01

Scenarios were chosen because of their plausibility and to determine what, if anything, should be done to address such potential situations.

The scenarios that emerged from the process have been used to envision what could happen in the future. Scenarios were chosen because of their plausibility and to determine what, if anything, should be done to address such potential situations.

In a relatively new field subject to constant technological changes, no good or best practices have been in place long enough to withstand the test of time. In this context, any lesson learned from experience must be conditional, based on new—and future—developments. For example, fingerprint-based identification is not as trustworthy as it appeared to be years ago; identity theft is no longer a matter of financial loss but can now be used to violate fundamental human rights; and growing sophistication in cyber attacks increase the risk related to storing biometric information on local servers. Thus, the three scenarios that came out of the process—extreme yet plausible by design—provide us with elements that ought to be considered as part of the design of any digital identification policy.

This exercise identified six key dimensions that need to be emphasized throughout policy discussions going forward: (i) personal data protection and privacy, (ii) identity ecosystem, (iii) social inclusion, (iv) procurement of digital platforms, (v) responsible use of technology, and (vi) role of the government in digital identity. These dimensions are part of current conversations (some more than others), but the exercise highlighted their importance and has reframed the conversation to include new players and factors. We believe they should be considered critical parts of a comprehensive digital identity policy framework.

Personal Data Protection and Privacy

It is hard to prevent digital identification systems from storing personal data, which in many cases includes biometric information used for authentication. But even if governments manage to minimize the information stored in their servers, digital identification becomes the de facto link between information stored across different sectors and institutions. While this enhances administrative efficiency and effectiveness (e.g., schools may be able to verify current address, parenthood, and/or vaccination information for any given child automatically), it is also a potential vulnerability in

terms of privacy (e.g., a school principal could access medical information for any student).

Currently, entities in charge of digital identity initiatives do not systematically coordinate with data protection authorities and focus on the advantages that digital identification can bring to the digital economy. Moreover, many countries still lack data protection legislation. Most use cases for digital identification systems consider government entities and private companies as users, not citizens. Thus, many of the risks that citizens may be exposed to are often overlooked.

Digital identification systems should be designed to mitigate the potential for exposure of personal and private information that could be enabled by them. Going forward, it is recommended that entities in charge of digital identification systems consult with other stakeholders to better understand the implications, review relevant legal frameworks in place, and identify any intervention that would be required to further protect personal information once the digital identification system is in place. A "privacy by design" approach should be adopted, meaning that privacy and data protection considerations should be built into the design of the system from its inception.

Identity Ecosystem

A digital identity system is as valuable as the number of entities (and transactions) that accept it. Governments can invest in complex, secure, and comprehensive identification systems, but if no public or private entity or, more importantly, no citizen uses it, then it will be a waste of resources. Moreover, as economic activities expand their digital activities or completely transfer to the digital world, not having a trustworthy digital identification system can undermine economic development. To increase the usage of a digital identity system, governments need to understand the context in which such systems will be deployed. This context includes any pre-existing digital identifications and their level of sophistication and pervasiveness, internet access throughout the country, the degree of digital literacy of the population, and the quality of foundational identity systems, among other factors.

Unfortunately, governments rarely consider such a context. Digital identification initiatives rarely consider what other actors—public or private—are doing in terms of digital development. Most of the planning focuses on technology, that is, what kind of biometric information should be collected, where it should be stored, whether to add a digital signature, and if so, whether to base it on certificates. These are all important questions, but understanding the ecosystem in which the system will be rolled out is just as important, if not more so.

We recommend that digital identity solutions be user-centered and adapted to the country in which they are to be deployed. Opening a space during the design phase—from system functionality and specifications to legal requirements and regulations—to incorporate the views of potential governmental and nongovernmental partners and citizens is key.

Social Inclusion

Analyses of registration in several countries suggest that under-registration is more common among rural and poor segments of the population.

A digital identification system can unleash a series of benefits to citizens and governments. From reducing transaction costs and increasing access to goods and services to improving the coverage and targeting of social transfers, digital identification systems can dramatically improve people's quality of life. In this context, it is vital to include the entire population in the initiative. To do so, it is important to have a good understanding of the extent of coverage of the existing national identity system or of the system on which the digital identity system will be constructed. For example, according to UNICEF, there are approximately 4 million children under 5 in LAC who have not been registered. If these children are not registered, they most probably will not be included in any identification system. Analyses of registration in several countries suggest that under-registration is more common among rural and poor segments of the population. Paradoxically, in many cases the segments of the population that could benefit most from the implementation of a digital identification system are the least likely to be included.

Even though coverage is a metric in many evaluation frameworks for the implementation of digital identity systems, reaching 100 percent of the population is not a goal in all implementation plans. Admittedly, it is difficult

to reach people for whom there are no records, but a concerted effort to guarantee 100 percent coverage should be made.

Digital identity initiatives need to step away from a "build it and they will come" approach and be proactive in identifying, enrolling, and promoting usage among low-income and rural segments of the population. As much as digital identity systems can help close the divide in terms of access and quality of services, implementation that does not ensure 100 percent coverage may end up widening it.

Procurement of Digital Platforms

To a large extent, public procurement policies have not adapted to changes in digital technologies and the innovations they bring. From agile development to open standards, technology now allows governments to introduce flexibility into what until recently were long-term relationships with large, established vendors based on proprietary standards and restrictive (and costly) contracts. In the digital identification systems space, open-source applications are starting to appear, and a modular approach based on common open standards is possible and is expected to become a viable option for countries, regardless of where they are in the process. This will not only enable more flexible implementation but will also allow small and medium enterprises (SMEs) to enter the digital identification space, bringing with them innovation and cost reductions.

Today, although open-source platforms such as MOSIP or OpenCRVS are starting to showcase the potential of an open and modular approach to digital identification, most procurement of digital platforms still occurs under a single, multi-million dollar, multi-year contract. Moreover, even in countries where such a "one vendor takes all" approach is in place, data ownership, open standards, and clear data portability conditions are often missing in the contract. This is mainly due to a lack of understanding and underestimation of their importance on the part of public officials when negotiating such contracts.

Going forward, it will be important for government teams in charge of digital identity to fully understand the trade-offs between open and

proprietary solutions when procuring a digital identification platform. In particular, the use of open standards, a clear data governance framework, and requirements for data portability need to be promoted and included in all contracts.

Responsible Use of Technology

To a large extent, all scenarios that came from this exercise featured a controversial use of technology, either because it violated human rights or increased social discrimination and inequality. There is no better example that showcases the balance that needs to be struck between regulation—in this case, the interventions that governments need to put in place to guarantee basic human rights—and innovation, that is, the flexibility that the private sector needs to create and/or improve existing goods and services. Is increasing citizen security worth losing our privacy? Should better information security protocols trump potential innovative uses of devices and information to ease everyday tasks?

Regulation is often said to be slow and always lagging behind technology. This seems to be the case in digital identification systems. Currently, implementing most digital identification systems focuses on the benefits they bring to the economy, without paying much attention to the downside risks, which include potential violation of rights, systematic exclusion of segments of the population, and/or introduction of biases in policy design by analyzing incomplete information, to name a few.

Governments need to be aware and always monitoring the potential risks created by the use of technology. Opening communication channels with other actors, namely, civil society, academia, and the private sector, to help understand risks that appear with the implementation of new technologies is also recommended, since government officials tend to focus on the efficiency improvements brought about by technology rather than on the potential negative effects it may have on other aspects of citizens' lives.

Should better information security protocols trump potential innovative uses of devices and information to ease everyday tasks?

page 11

The Role of Government in Digital Identity

There are two main misconceptions regarding digital identification systems. The first one is that many governments believe they should provide a unique and reliable digital identification that can be used securely in the digital economy. The second is that governments see themselves as the end users of digital identification systems.

Regarding the first one, the role of government should be to guarantee that there is a reliable and secure digital identification system in place, regardless of who provides it. Most countries in the LAC region have opted for a model in which government has built a digital identification layer over an existing national identification system, to be used at least in the public sector. Some other countries have relied on the private sector for their digital identification requirements, and in some cases a federated system is in place by which several public and/or private entities perform identity authentication under a pre-established protocol and security standards.

Regarding the second one, governments need to understand that citizens are the main users of identification systems. This means that from system functionality to use cases to interface design, citizens need to be involved, and their feedback should be considered and incorporated. Identification systems do not need to be cutting edge; they merely need to be usable by everyday citizens.

TABLE 1.

INSIGHTS FROM SCENARIOS AND POLICY RECOMMENDATIONS

INSIGHTS FROM SCENARIOS	CONSEQUENCES	RECOMMENDATION
Personal data breaches and/or misuse can be caused by or aided by digital ID systems.	Digital ID systems could become a vulnerability in the cybersecurity space, undermining their usefulness and reliability.	Ensure a “privacy by design” approach.
National digital ID systems could end up being used by a small number of entities.	Different entities may create their own digital ID service, creating inefficiencies and confusion among citizens.	Reach out to the broader identity ecosystem, especially end users (citizens).

INSIGHTS FROM SCENARIOS	CONSEQUENCES	RECOMMENDATION
Only certain segments of the population may access and use the digital ID system.	Digital ID systems can exacerbate the digital divide, affecting vulnerable segments of the population.	Ensure 100% coverage and usability.
Governments may end up depending on one sole locked-in vendor.	The relationship with vendors and badly designed contracts may create locked-in environments, giving more power to the vendor and eliminating incentives for innovation.	Adopt a flexible procurement policy.
Under a misleading citizen security pretext, digital ID systems may be used to track citizens' whereabouts.	Digital ID technologies may be used for surveillance of citizens by public and private sector alike.	Introduce regulations and monitoring mechanisms for a responsible use of identification technology.
Governments may focus exclusively on the ID technology	Weak institutions that lack the capacity to create a safe and trustworthy environment for identification in the digital economy.	Have a clear understanding of the role of government in digital identification.

Table 1 summarizes these policy recommendations, along with the specific situations they intend to avoid. We believe that by considering the insights we have obtained from the application of future scenarios, our conversations across the region will be enriched, and thus we will be able to provide advice that focuses on future challenges as well as current ones. We hope it does the same with other organizations and governments that read this report.

CONTEXT AND METHODOLOGY

Part

02

Future of Digital Identification Systems in Latin America and the Caribbean

The birth registry or birth certificate is considered the first document (also called "breeder" document) that recognizes an individual's legal identity of an individual. Birth certificates are the basis of foundational[2] identification.[3] In LAC, most civil registry systems are linked to the national identification system.[4]

In LAC, the importance of the information managed by both civil registry and identification systems goes beyond ensuring a unique and secure identification for everyone: access to any transaction or service requires proof of identity by the user. Therefore, enabling tools or procedures that can facilitate identity verification in a secure way is key to accessing a number of public and private services. Having segments of the population that lack any form of identification, on the other hand, is a barrier to social and economic development.

A study conducted by the IDB to understand the potential economic benefits and social impact[5] of digital identification systems showed that the

2 Identity documents can be classified as foundational or functional. Foundational identification is the main identity that is characterized by being legal, unique, and universal. It includes specific characteristics of a person such as full name, date of birth, biometrics, unique identification number, among others. The functional identification is issued to access public and private services, based on records obtained from the citizen when he or she enrolls in programs or services. These records may include the driver's license, social security card, voter ID, tax identifier, or passport.
3 For the purpose of this report, the concept of identification is understood as "the determination of identity and recognition of who a person is" and identity as "the set of unique attributes and characteristics of a person." Reference: IDB (2015). Dictionary for Civil Registration and Identification.
4 The characteristics of identification systems differ from one country to another. A recent IDB study found disparities in how these systems are integrated: for example, 7 out of 20 countries analyzed (Bolivia, Brazil, El Salvador, Honduras, Nicaragua, Uruguay and Paraguay) present interoperability challenges between the civil registration and identification offices. More information can be found at https://publications.iadb.org/es/registros-civiles-y-oficinas-de-identificacion-analisis-y-fichas-de-pais.
5 The economic and social impact model, based on use cases and variables from pilot programs and experiences in developing countries, states that the improvement of identification systems has a catalytic effect on access to public and private services. For instance, it was found that the lack of trust identification mechanisms caused 20 percent of bank applications for savings account to be rejected, while a robust identification system can target the ghost or duplicate beneficiaries of cash transfer programs.

benefits of an identification system can be seen in different transactions and services. They include cost savings related to the elimination of duplicate identity databases for the provision of services, improving interoperability between services that require identity verification, and savings associated with better allocation of cash transfer programs.

Trusted digital identification systems can also improve the impact of financial inclusion initiatives and health and education programs, among others.

A unique identification is a unique code or number that links a set of unique attributes to a person, including a combination of biographic and/or biometric data. The basic information is then represented in a physical or digital credential that individuals can use to identify themselves. Today, as a result of the accelerated growth of the digital economy, modern identification systems rely on digital technologies rather than the paper-based systems that are still common in the region. As digital identification systems emerge, the information stored in these systems could also allow governments to better understand the needs of citizens, providing online services and valuable data to support the design and implementation of public policies. Trusted digital identification systems can also improve the impact of financial inclusion initiatives and health and education programs, among others.

A digital identification system is not only the institutional or technological infrastructure required to issue an identification card. It needs to consider and actively involve an entire ecosystem that supports interoperability among multiple entities, reducing the duplication of platforms or databases that store personal information. It also needs to have a robust civil registration service, and, as it migrates to digital platforms, it should also provide authentication services in and outside government to verify the identity of an individual and enable a greater number of online transactions.

What is scenario planning?

Scenario planning enables the leadership of an organization to perceive changes in its context, to uncover, question, and challenge its strategic assumptions, and to better prepare for plausible and significant changes in its context. It helps to improve an organization's strategy especially when the context is perceived as turbulent, uncertain, novel, and ambiguous (TUNA).[6]

6 Ramirez, R. and A. Wilkinson. 2016. Strategic Reframing: *The Oxford Scenario Planning Approach*. Please refer to https://global.oup.com/academic/product/strategic-reframing-9780198745693?cc=gb&lang=en&.

Scenarios are not forecasting. They are stories about plausible, relevant and challenging future contexts.

Scenarios are stories of the future context that describe how it might unfold, and that are plausible, relevant, and challenging. The insights from the future provide organizations with a set of lenses with which to generate new strategic insights. Even if it is impossible to predict how the future of digital identification systems in LAC will look in 2030 from a societal, political. or technological perspective, we can create plausible future scenarios enabling us to focus our thinking, sharpen our strategies and inform our decision making. In the scenario planning activity developed by the IDB, focusing in innovative processes was the main objective to leverage strategic insights and create exceptional value.

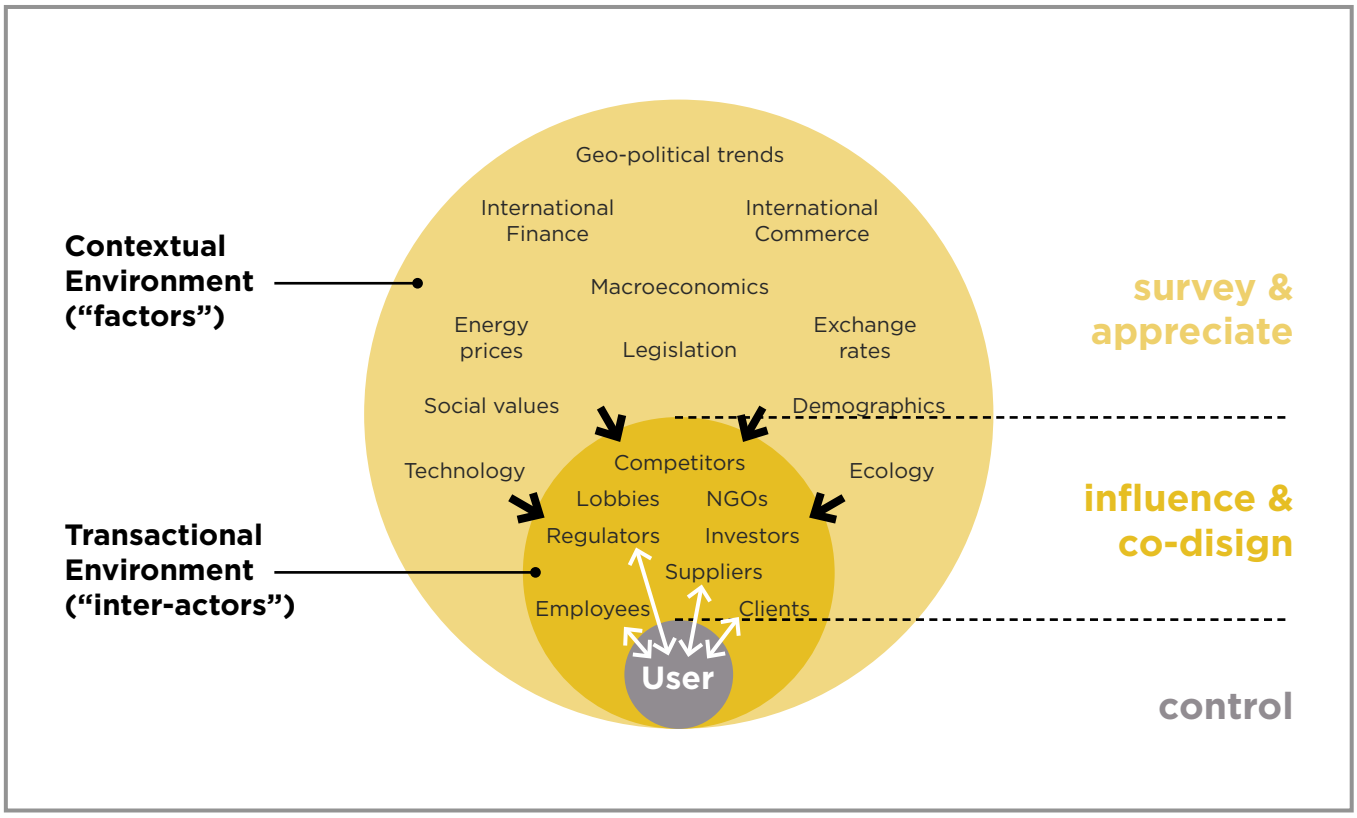
The Scenario Planning Process

A starting point for the process is the analysis of the contextual environment and how factors in it might evolve. The contextual environment is the "bigger picture" and the space where the stories are sketched out. Questions such as, what external factors shape the future of digital identification systems? and what are changes that might occur beyond our control? are crucial at this stage.

Once the stories have been sketched out and the contextual environment has detailed the uncertainties as drivers of change, the process evaluates how these different contexts affect the rules of the game in the transactional environment, and the way things are done. Analysis of the transactional environment tries to answer the questions, How might these factors in the contextual environment influence the actors with whom I engage? What new relationships can be formed? And How will they interact?

Finally, the process finishes by exploring the environment within your control. What are the challenges and opportunities for a specific actor in this scenario? What are the implications, and how might the changes implied by a scenario affect the user?

THE SCENARIO USER IN ITS TWO ENVIRONMENTS



Source: NormannPartners.

To accomplish these objectives and explore the future of digital identification systems in LAC, the scenario planning process included the development of the following activities:

- **Interviews with subject matter experts** to better understand mental models on how the world is configured and how things work in the context of digital identification systems.
- **Identification of relevant research topics** and unfolding practices that might be applicable to IDB's unique situation.
  Three **workshops** to: (i) define and develop the factors that will be part of each scenario; (ii) build different scenarios including outlines, narratives, and logic; and (iii) describe the implications of the scenarios.

Interviews with Subject Matter Experts

Scenario planning benefits from interviewing key experts, stakeholders, and decision makers prior to initiating the research process. Twenty-two experts[7] were interviewed to gather data about their area of expertise and draw out lessons learned from their experiences and ideas on the major changes that digital identification systems could have in the future. The purpose of the interviews was to understand the current and future dynamics in LAC countries geographies on identification systems, including digital and physical infrastructure, trust and privacy, interoperability, institutional capacity, people movements, and delivery of social services.

The following are the main ideas that emerged from the interviews:

IMPORTANT DRIVERS OR EVENTS THAT HAVE SHAPED THE ID SYSTEMS LANDSCAPE	MAJOR CHANGES OVER THE NEXT 10-15 YEARS	FUTURE CONTEXT FOR IDENTIFICATION SYSTEMS – CERTAINTIES	FUTURE CONTEXT FOR IDENTIFICATION SYSTEMS – UNCERTAINTIES	BIGGEST CHALLENGES WHEN IMPLEMENTING DIGITAL IDENTIFICATION SYSTEMS
• Gaps between regulation and technology • Criteria in terms of technology use • Data protection and privacy • Migratory flows • Electoral process • Human rights in technology • Gender identity • Cybersecurity infrastructure • Importance of birth registration • Online banking • Use of biometrics	• Improvements in procurement processes • Massive implementation of e-government initiatives • New skills related to digital knowledge • Demand for more data protection • De-risking initiatives • Social movements focused on technology • Citizens' active role on the development of solutions • Quality of products but not necessarily on technology	• New generation of activists for transparency and citizen participation • Gender parity in data science and technology • Digital standards and principles • Better legal frameworks on privacy and adequate regulation on data management • Personalization of services	• Technological changes to close the infrastructure gap • Regulation on how governments or private sector are using personal data • Inclusion of excluded populations • Legal and technologic protection of databases • Invasion of privacy	• Promotion of public policies to incentivize private sector participation • Data governance Interoperability between countries • Procurement of technology • Contingency plans if the technology fails • Vendor locking • Data collection and management • Regulation for the private sector • Prompt response for cyber attacks • Ethics on the use of data • Data quality • Improving trust in government

7 The areas of expertise included civil registration, identity management, international development, data protection, public policy, connectivity, broad brand, finance inclusion, digital rights, open data, citizen security, economics, transparency and digital government. Interviews were held in confidence and the content is non-attributable.

The scenario narratives were based on a co-creation session in which the factors in the contextual environment were analyzed and developed over a 10-year time frame.

Identification of Relevant Research Topics

The next step involved assessing a range of factors[8] that could shape the future of digital identification systems. The aim was to understand the entire ecosystem involved for developing a trustworthy, secure, and efficient digital identification system and identify which of these factors were the most uncertain in terms of having two or more possible ways they might evolve in the next 10 years. If digital identification systems are designed to ease access to public and private services and support the digital economy of the countries, technological and social factors will have an important role to play in promoting universal coverage, and the design of a secure, sustainable, and robust system that protects private information and creates trust among users. In particular, the prioritized topics were:

- **Telecom infrastructure:** Digital identification systems can promote online interactions between organizations and individuals. The development of robust telecom infrastructure will support transactions needed between different users, including procedures related to personal data registration and enrollment, identity verification, development of an authentication process with controlled access, and revocation when the credential is rescinded.
  - **Uncertainties**: What are plausible developments in connectivity? What will be the speed for adoption of 5G? Will telecom infrastructure fully cover rural areas?

- **Institutional capacity and e-services:** The use and development of applications in public information and communication technology (ICT) projects that leverage cloud computing, open government data, and verification processes require new procurement models to support more flexible and innovative software delivery. The procurement of digital technology should promote the use of innovative solutions that can facilitate certain types of data or process management, such as registration identification and authentication. Governments should make efforts to connect their institutions properly, defining levels of integration, data sharing, the procedures needed to verify the user's

8 Factors are issues, forces, ideas, trends, patterns, themes, or developments that are in the contextual environment and that facilitated the identification of a preliminary research agenda.

Research was carried out on each topic to understand its current context.

identity. In the LAC region, the management of identification systems lies within the government, and it is the government's responsibility to develop technical and administrative procedures focused on governance effectiveness, protection of personal data, and efficient service delivery. Therefore, governments need to establish the roles and competencies of the entities that manage the identification and registration systems, as well as for those who use its authentication services.

- **Uncertainties**: Will national digital identification systems be able to authenticate the identity of all citizens? Are governments interested in applying innovative practices to strengthen their identification systems?

— **Connectivity:** Connectivity capacity and internet penetration levels must be considered when a digital identification system is deployed. In rural areas, the lack of connectivity represents several challenges. Therefore, solutions to perform identification activities in offline circumstances should be designed. Additionally, the design, functionality, and maintenance of digital identification systems demand specific digital skills, and governments could attract specific talent by implementing hiring practices that ensure adequate technical capacity.

- **Uncertainties**: Will the internet penetration gap close in LAC countries?

— **Cybersecurity:** There is limited data on how cybercrimes are affecting the current digital identification systems, but it is known that cybercrime has become more sophisticated. The expansive use of ICT and the data exchange has risen certain concerns on how to protect the systems and response promptly to the different incidents like the use of ransomware to filter data from mobile and IoT devices, which mainly lack strong defenses; or online fraud as result of stolen personally identifiable information.

- **Uncertainties**: How will geopolitics impact cybersecurity? Will countries in LAC have cybersecurity policies and/or strategies in place?

— **Privacy and data protection:** Existing national identification systems in LAC collect biographic and biometric information. Verification and authentication procedures should follow specific standards to protect sensitive or private information. A limited or nonexistent data protection regulation could lead to identity theft and fraud issues,[9] mainly if an identity credential is being used to verify the identity of a user of digital services.

- **Uncertainties**: Will people take actions to protect their data privacy? Who will own data? Will LAC countries develop a data protection framework similar to GDPR regulations?

— **Identity theft:** A digital identification system stores personal data, including information related to name, surname, place and date of birth, address, parents' names, and biometrics (fingerprint, facial recognition), among others. The methods to store this information sometimes lack secure procedures, creating opportunities for information leakage.[10]
  - **Uncertainties**: Will the private and public sectors have procedures in place to promptly identify personal data leakages?

— **Trust and people's perceptions:** In the LAC region, trust in government is declining. In 2010, the latinobarometro survey showed that 45 percent of citizens in LAC countries expressed trust in the government; by 2018, trust in government had decreased to 22 percent.[11] Consequently, the institutional arrangement of the government and its capacity to protect personal information and guarantee its ethical use can increase this lack of trust. Increasing citizen's trust in governments may create opportunities to develop identification systems that can respond to the needs of the citizens.
  - **Uncertainties**: Who defines trust? How can trust in digital identity solutions provided by government be built?

— **Data ethics:** Digital identification systems capture sensitive personal information that could increase associated risks related to privacy, misuse of information, discrimination, and data leakages. Specific regulations

9 The Identity Theft Resource Center, in its 2017 Data Breach report, found that there were 1.579 data breaches, exposing 179 million records, only in the U.S. territory. Nearly 158 million social security numbers were exposed in the same year, and more than 27 percent of data breaches were medical or healthcare related. There is not enough information to measure the identity fraud impacts on the LAC region. The latest report of the Latin America and Caribbean Network Information Centre revealed that in 2013 the cost of identity theft exceeded US$1.100 million studies, and in the case of the banks, the robberies due to identity fraud surpassed the US$50 million per year.

10 The latest ThreatMetrix Cybercrime report found that in Q2 2018 cyberattacks had increased 20 percent in the LAC region, compared to the previous year, being Brazil the country where most attacks originated. Also, one quarter of all account registrations were rejected as fraudulent, since stolen and synthesized identities are leveraged to attack the growing e-commerce market showing a trend for monetizing stolen identities. ThreatMetrix Q1 report can be found in the following link: https://www.threatmetrix.com/press-releases/south-america-emerges-new-hotbed-identity-fraud-report-reveals-morphing-nature-global-cybercrime/. While the Q2 2018 report is available in the following link: https://www.threatmetrix.com/digital-identity-blog/cybercrime/latin-american-cybercrime-trends-attacks-increase/.

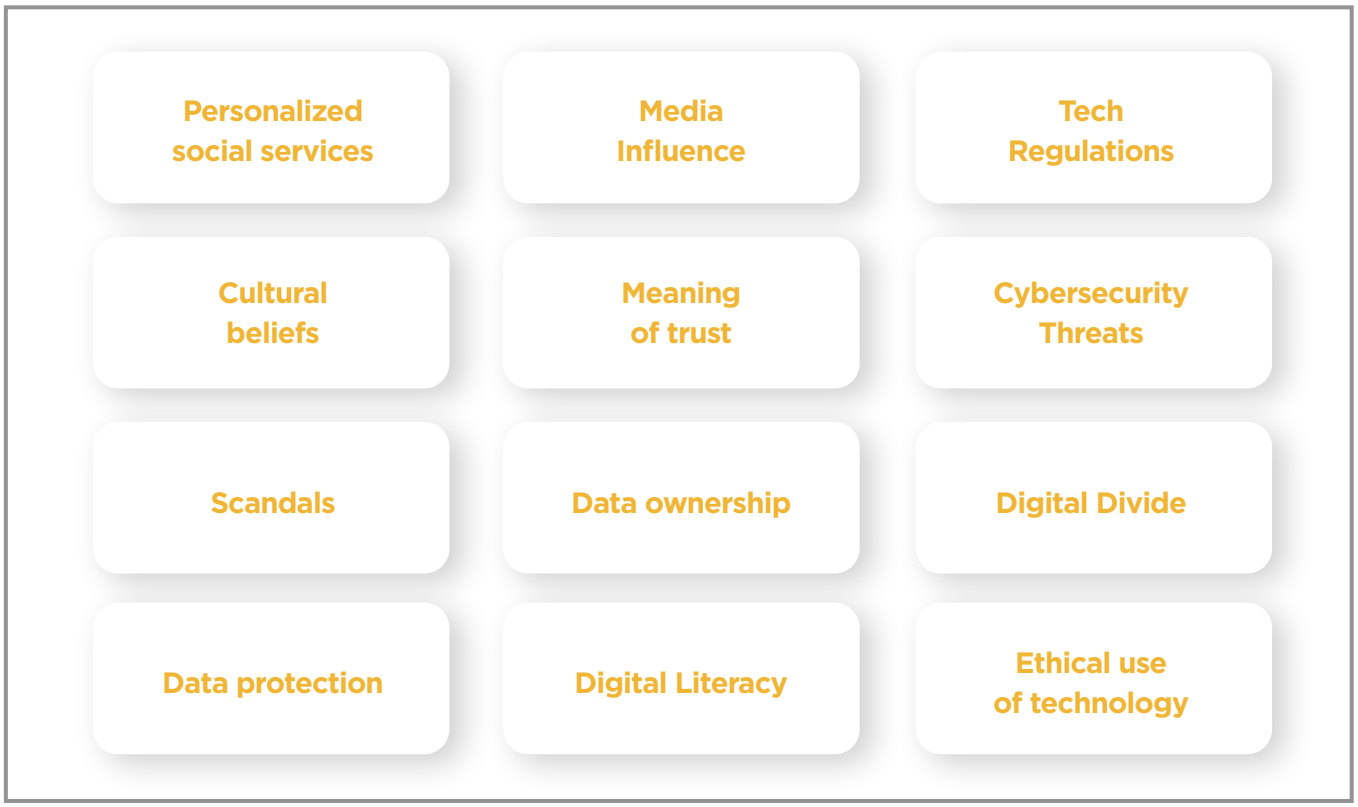
11 Latinobarometro report, 2018. Available in the following link: http://www.latinobarometro.org/latNewsShowMore.jsp?evYEAR=2018&evMONTH=-1.

to establish the ethical use of personal data and the mechanisms to prevent cyberattacks are highly recommended. Digital identification systems require strong legal frameworks that can ensure personal data protection, and even suggest user control of the information.

- **Uncertainties**: Which level of interoperability should be sought? How can vendor lock-in be prevented?

Research was carried out on each topic to understand its current context. The research included data collection to quantify progress on each topic, cross-reference information, and identify challenges, opportunities, trends, uncertainties, and threats. Also, several projection models were analyzed to understand how each area could develop for the upcoming years. Likewise, key factors were defined and classified as most/least knowledgeable and most/least challenging. This analysis made it possible to establish the major drivers for the composition of the scenario set.

SAMPLE OF FACTOR CARDS



Scenario Narratives

The scenario narratives were based on a co-creation session in which the factors in the contextual environment were analyzed and developed over a 10-year time frame, discussing how they might play out in the future. Key actors were identified and included in the stories, describing how they might interact or be influenced in each potential scenario.
Comparison charts between topics and scenarios were discussed to define their impact and to evaluate how challenging, plausible, and relevant each scenario could be.

SCENARIOS FOR THE FUTURE OF DIGITAL IDENTIFICATION SYSTEMS IN LAC

Part

03

The process delivered three scenarios for the future of digital identification systems in LAC, each depicting a plausible, challenging, and relevant story. The stories were named based on their storyline: "E-nequality," "Big Brother," and "Power to the People."

As part of the story telling and following a human-centered approach to help analyze the impact of each scenario, a persona profile was created to help visualize how citizens might react in each scenario. The profile used was:

Carmen

Age: 38 years old

Level of education: High school and technical degree

Lifestyle: Entrepreneur and single mom, low middle class, who lives in the city and participates in social movements.

Main worries: That her child can have access to technical education and a good and nutritional diet. Understand and stay informed on the technological changes that are taking place and help share with her community. Access to a friendly public transportation system. Complete the entrepreneurship program promoted by the government.

Interests: Participate in the community meetings of her indigenous community. Transfer extra money to her parents. Be a social-tech activist.

This section describes each scenario. A timeline for the main events has been outlined as well. A comparison chart of the three scenarios through specific topics has been included, highlighting some of the key messages of each of the stories.

Scenario 1: E-nequality

The year is 2030 and the digital revolution is firmly anchored in advanced digital identification systems. Government agencies use more authentication services than ever before. New solutions and procedures make data verification and the use of digital platforms easy.

People and goods are on the move, powered by digital services that know no borders. Regional integration once seemed like a grand dream: something every politician promised but struggled to deliver. Now the main trading blocs—Alianza del Pacífico, CACM, CARICOM, MercoSur—are more integrated than ever. Within countries, farms are more automated and digitally savvy, so more people are moving from towns and rural areas to large cities.

All this would seem desirable, but there is a darker side. Digital identification services once promised to reduce inequality. However, inequality is now more rampant than ever, both within and among countries.

5G brought innovation and high-speed connectivity, but only for those already connected, and not everyone is connected. The promise of 100 percent coverage of broadband and affordable connectivity for all never reached the more remote regions, and largely bypassed the poor. Only those with the required skills were able to take advantage of the digital bonanza.

Digital identification services once promised to reduce inequality. However, inequality is now more rampant than ever, both within and among countries.

The rest were left behind. Even though the unconnected—or under-connected—are many, they are underrepresented in government. Few civil society organizations focus on them as few donors provide money to close this technology gap, and their effort is sufficient. Professionals with limited knowledge in technological areas found it difficult to access jobs that allow them to make ends meet. Most of them notice that more job opportunities are available for professionals with high-tech experience, as companies are mainly recruiting workers in science, technology, engineering and mathematics to fill positions with higher salaries. And even with these incentives, some positions go unfilled.

At first, governments were reluctant to use technology, aware of the economic and technical resources that a modernization program could take. But the acceleration in technology use during the COVID-19 pandemic and

the demand to include everyone highlighted the need to support digital economy initiatives where the investment in better data bases became pivotal. Still, the emerging digital economy did not translate into higher income taxes. And the average income per household did not increase. Thus, a new generation of public-private partnerships was put in place to lure the talent required to automate more government functions.

Soon, the private sector started deploying proprietary platforms that supported all government services, gradually locking in the provision of services. At the same time, companies introduced schemes that exploited personal information collected through these platforms to better target products and develop new services. Civil society demanded more responsibility in the use of technology, but many citizens objected, believing that the benefits they were receiving outweighed the cost of losing some control over their personal information. Governments went along with these schemes, as they provide alternative sources of income that cover the cost of technological innovation, even though in many cases they violate privacy.

Citizens are divided. The first big divide is between those who are connected and have an ever-increasing digital footprint, and those who have little or no digital presence. The latter struggle to receive public services or must spend ever more time and money at the few available physical offices. For them, service standards are lower. They are part of a paper-based "bubble" that seems to have frozen in 2019.

The second big divide is with the connected citizens who live a different reality. Services are more effective and efficient, and citizens can see who in the public sector accesses their information. In fact, unless explicitly mentioned upfront, government officials need to ask permission from citizens to use their information for any specific purpose. Data is shared among sectors over a secure platform that uses newly created citizens' registries to link the information. All services are accessible regardless of the country of origin, as all systems are integrated among vendors in different countries. Most of these citizens (younger on average) argue that "privacy" has changed over the last decade, and that they do not mind the private sector mining their data to offer them things that, in any case, they probably need. In fact, a majority of individuals end up buying the products or services that are offered to them through the mining of personal information that sits on government servers. The calculation is greater convenience at the expense of reduced privacy.

A minority of connected citizens, however, are against the role that the private sector has adopted in this new era. They are against the idea of a sole monopolistic provider of technology to government, and they do not like the way private sector monetizes personal information. The private sector argues that none of its employees has actual access to personal information filed on the identification systems, and that all personalized advertisement and product placement that citizens receive is done through artificial intelligence algorithms. Their programmers, they argue, have access to the algorithms, but not to the data. Civil society organizations are trying to create awareness about the pitfalls of the current approach, but with only a minority of citizens supporting them, they have little influence.

Cybercrime is at an all-time low. Having a sole private sector provider, after all, allowed for a standard protocol, including high-level encryption and integrated mitigation measures. However, the number of identity theft cases has increased in the last few years. Since every citizen has been issued a digital identity to interact online, those that use it the least (mainly the unconnected) are the most common victims. Many go months without noticing until a company charges them for a credit card they did not request or until they discover that somebody else has been cashing out their annual benefits. Encryption has an expiration date, as they say, and it appears that the lack of competition made private vendors lower their guard.

Many voters wonder if the digital revolution improved their lives. Neo-populists, who promise to bring back simpler and better times, are surging in polls, and a new debate on privacy issues has emerged as the need to establish global principles.

E-nequality: A Day in the Life of Carmen

Carmen wakes up very early to get ready and prepare breakfast for her son, Carlos. During breakfast, she fights with him because he wants to eat Cheetos instead of the banana oatmeal that she prepared. Yet, she knows how to manage her son's stubbornness and gets ready to start a new day.

When her son takes the school bus, Carmen checks on her cellphone if the metro will arrive on time. Also, she checks trustworthy news by activating an app that filters reliable information on her phone. Before boarding the transmilenio, a scanning system verifies her ID by using facial recognition technology, and she is accepted as a passenger. Her biometric information is linked to the bank account that she uses to pay for public transportation and an automatic deduction to her account is applied.

Carmen is part of the Human Rights in Tech working group, and she attends their daily meeting. In today's discussion, the group needs to define strategies to promote connectivity at local communities, as Carmen's community is one of them. She is concerned that the lack of connectivity is causing barriers to access services provided by government and the private sector, and for her, it is important to not leave anybody behind.

Discussions on her working group surface concerns about privacy and the use of personal information. Specifically, Carmen has grown weary of people who are encouraging data sharing online in her community without analyzing the potential consequences. She is concerned about the use of data for political purposes and how it could impact her community. Furthermore, she needs to define a communication strategy for her community, so that they can make an informed decision whenever using an internet network connection.

At the office, while she is reviewing some documents, Carmen gets a notification on her watch. Once again, Carlos is in trouble at school. She opens the message sent by the school Principal, which contains a video of Carlos getting into a fight with another kid during lunch break. She heads immediately to the school. Carmen feels very anxious

when the school sends these types of notifications, because she is afraid Carlos will be profiled as a trouble maker due to school incidents that had been recorded before and uploaded to an online database that shares records of all students across the country.

At the end of the day, Carmen is conflicted between giving into the system and spending more time with Carlos to protect and guide him or continue creating awareness with her community on personal data sharing. Before going to bed, her watch asks her if she is depressed, showing as an option a bot-therapist that could help her to express her feelings.

Scenario 2: Big Brother

It's 2030. After decades of insecurity, corruption, and low trust in government, a wave of authoritarian governments sharing a similar mindset has emerged in Latin America and the Caribbean (LAC). Campaigning under the promise of solving the problems of increasing crime and corruption that have been plaguing the region by pushing new technologies and data solutions, these governments have strengthened the police forces, which are using drone technology equipped with cameras to track suspects; big data, machine learning, and predictive analytics to prevent crime; and facial recognition technology in security cameras to monitor suspicious behavior.

The perception of security and strong propaganda claiming a massive drop in crime has led citizens to blindly trust government, eliminating any type of demand for accountability in the use of personal data and a complete lack of checks and balances. The private sector has offered their assistance and willingness to work on a regulatory framework to mitigate reputational risks and possible data leakages, but governments have been more interested in deploying technology systems solutions and finding partners to support their initiatives.

The adoption of the universal digital identification system by governments as the only mechanism to access public services has led to a detailed identification of citizens.

Given the lack of resources and capacity on the part of LAC public actors, international banks and funders have extended support for the acquisition of new technology and equipment, which represented a huge investment. Initially, grants and loans approved for the countries were aimed at fighting the COVID-19 pandemic, preventing crime, and reducing insecurity. Likewise, multilateral organizations suggested legal framework reforms, which governments did not take into consideration. Big tech companies quickly identified the opportunity and partnered with these authoritarian governments to provide cheap technological solutions. Now, governments are locked into these large companies for the supply of products and services.

Online services are now mandatory, enabling cross-border services among certain countries and substantially increasing the digital economy. Online transactions reached a record high, and small and medium size companies focused on hardware and tech services are striving to create a new digital elite. The region has reached a substantial tax collection rate because online services and transactions have increased the number of businesses and made it easier for new companies to interact in a regional market.

There is mass adoption and acceptance of a universal digital identification system launched and managed by private tech companies. Their original objective when they entered the regional market was to help citizens remember their various passwords and provide an easy way to manage their personal data. However, it is now the only way to access public services. No privacy frameworks were put in place with the creation of the new identification system. This led to the government's expansion of the use of data and AI to subjugate citizens, followed by a new sphere of crimes, mainly those related to biometric data hacks, data breaches and vulnerabilities in the identification system.

The adoption of the universal digital identification system by governments as the only mechanism to access public services has led to a detailed identification of citizens, including those who were once marginalized. Governments are in control of detailed medical records and academic transcripts. However, even though there is now universal access to public services through the digital ID, quality is still lacking. Hospitals are not well equipped, and lines continue to be long, increasing the value of face-to-face interactions with a doctor.

Censorship is more common as governments filter the use of social media under the slogan "protected citizens, harmonious society." A new social scoring system linked to universal digital identity is used to determine access to services, punishing and excluding certain minority groups that are suddenly not eligible to vote, access credit, or access public services. The huge data footprint created by everyone, together with the blind belief in technology's assertiveness, have led to automated algorithm-driven preemptive sanctions, seeking to avoid criminal activity before it happens.

Cybersecurity presents a critical challenge for governments. With increased frequency and sophistication of malicious cyber activity, countries lack concrete actions and procedures to address cyber threats, increasing their vulnerability. Small breaches are kept silent, but the "long night" attack that completely shut down Mexico City for weeks raised red flags and forced the government to deploy a media campaign attributing the attack to "adversaries who want to destabilize the region." On the other hand, many suspect that these cyberattacks are just scapegoats for gross mistakes that come from ill-designed algorithms.

Sporadically, small groups of civil society organizations step up to voice their concerns on the unethical use of data for surveillance and control but are quickly identified and shut down by the police, alleging possible criminal activity and conspiring against national interest. Non-tech-savvy and digitally illiterate populations—mostly living in rural areas—are among the most vulnerable, being forced to interact in a digital space with no knowledge of privacy rights and personal data management. However, many are willing to lose their privacy if it means a more secure and crime-free environment. They remember the days of rampant violence from Central American gangs and South American drug lords.

Cross-border data flows between like-minded rulers are being used to control migration flows. People's access to travel is being restricted, following algorithms based on their digital profile, and large migrant movements caused by the negative effects of climate change are being registered by using biometrics for control. Likewise, rural populations are struggling due to climate change-related natural disasters that are affecting access to mine fields and sources of well-paid jobs. This is a main concern for governments due to the demand for mineral resources for the development of more devices and updated technology. This threatening situation raises the price of authentication services, creating an additional revenue source for governments and the private sector, which negatively impacts citizens' trust in government.

Big Brother: A Day in the Life of Carmen

Early in the morning, Carmen receives an email confirming her and both of her children as beneficiaries of a cash transfer program. For the last three months, the government did not deposit the money that helps her cover the grocery expenses for her two children. After reading that email, Carmen gets ready and heads to the closest financial entity to withdraw some cash. She is grateful that she is finally banked, and she remembers the difficulty her parents had when she was growing up in accessing financial services; it seemed impossible. By using her fingerprints, the cashier confirms her identity, and Carmen can get enough cash to buy additional fruits and vegetables for the week.

After visiting the bank, she plans to go to the tax agency. For her, it is important to declare her income, since it is the main information that the government examines to target potential beneficiaries for social and economic programs. At the tax agency, Carmen notices that many people are called in line before she is, so she decides to speak to the manager. He mentions that she may need to come back another day because there is a problem with the system and the officer can't access her profile. This has happened before, and Carmen wonders whether she will receive the services to which she is entitled.

Disappointed, Carmen hurries to one of her daily meetings. While she waits at the bus stop for the next van, she begins wondering what the Bank and the tax agency do with her biometric information, since both places asked for her fingerprints and took a photo of her. On the one hand, she feels that by capturing this information they should improve the service delivery without errors in identifying the users, but on the other hand, she is worried about the misuse of her personal information and the potential consequences that this may have. She suspects that the tax agency may have issues in terms of privacy protection.

In the van, two women are speaking about their children's schools. Carmen remembers that she needs to schedule a meeting with the school's principal. In her opinion, the education that her children are receiving is poor, and the curriculum hasn't been updated for the last three years. She tries to schedule an appointment through the school's extranet via her mobile phone, but an email confirmation shows that her complaint needs to be filed at the Ministry of Education. To facilitate this petition, the email includes the address of the closest office where she can submit the complaint according to her current location. Carmen knows that submitting a complaint will be a waste of her time.

In the afternoon, Carmen attends a weekly social community meeting. The main discussion focuses on the quality of social services and how they are responding to the needs of vulnerable populations. The government has promised that all social services will be personalized, but Carmen doesn't feel this has been achieved. Her children go to a school that is 10km away from her district, and the school transportation to bring them back home is inadequate. Her children need to walk for at least 15 minutes from the bus stop to get home, and even though security has increased and she now does not fear for her or her children's lives in the streets, she is aware that access to some social services is still not ideal.

While the group is discussing how the government has not substantially improved social services despite having everything online, Carmen wonders if the government might be targeting her because she participates in these meetings. She is concerned that significant delays in providing benefits and many bureaucratic obstacles on all the services that she needs to access are a consequence of her "activist work" with her community. Back home, at bedtime, Carmen reflects on the need to be a part of those community meetings. She recognizes she is better off than her parents in terms of security and connectivity, and even though services are not the best, she wants to continue receiving the government benefits for her children. She really wants to give them a better future.

Scenario 3: Power to the People

It is 2030. Despite efforts to bring stability to countries affected by the lack of opportunities, violence, and food shortages in Latin America and Caribbean, migration continued to destabilize the region. The dramatic sanitary and economic consequences following COVID-19 led people across the region to migrate in record numbers due to persistent and increasing levels of violence, economic instability, and widespread hunger, fueled by the effects of natural disasters and occasional epidemics. The increase in migratory flows renewed social tensions in recipient countries against migrants and strained the delivery of social services to these economic refugees and to the local population.

Efforts to digitalize government ramped up in the late 2010s. The Lima Group, in coordination with UNHCR, called for the issuance of digital identification to migrants at border crossings to ease their access to social services and increase security. Interoperability between countries' systems was a key goal in the design of these systems. However, vulnerabilities to the security frameworks were not properly addressed, leading to frequent data breaches.

As social tensions stemming from migration in the region increased, some countries used these digital identification systems to discriminate against migrants by excluding them from social programs. As citizen insecurity continued to plague the region, governments used biometric information from identity systems for surveillance purposes. These efforts began with good intentions, but in some countries, they were also used to target migrant populations, impacting citizens. Amid eroding trust in government, more people believed that digital corruption was widespread.

These incidents generated a regional uproar led by civil society about the lack of privacy and data protection rights, impacting governments and the business of large technology companies.

In 2014, Wikileaks revealed the extent of surveillance when it posted some governments' target lists, which included political leaders, social activists, journalists, and athletes, among others. At the same time, a massive data breach of migrant children's identity information in Colombia, Peru, and Mexico was ultimately traced to an organized international crime group that had corrupted members of the security forces in these countries to find "blank slate" identities that could be sold on the black market.

These incidents generated a regional uproar led by civil society about the lack of privacy and data protection rights, impacting governments and the business of large technology companies that provide the backbone to

digital government systems and store data. Inspired by the Arab Spring and in collaboration with European activists, civil society groups led to the Data Spring of 2026 which, aided by social media, contributed to the fall of two large governments in the region and set the stage for the rise of new political leaders that campaigned for a renewed and engaged digital citizenship, with rights and responsibilities in the digital economy.

This renewed engagement fostered the adoption of GDPR-III in 2028 by a large number of countries in the region. Now, the new generation of digital citizens has become the main driver demanding sound policy and regulatory frameworks that protect privacy, and data ownership, and that holds governments and the private sector accountable on the transparent and ethical use of technology and data.

Large private companies fought back, and the GAFAM cartel came together to try to lobby for more lenient regulatory frameworks without success. Pressure from the international community, especially from European countries that helped finance and build capacity in local civil society, was key to achieving the change in government.

However, the relationship with civil society is a challenge that governments are still grappling with, since regulation watchdogs from tech-savvy local NGOs are constantly overseeing their use of technology and data. Large government capital allocations go to cybersecurity to prevent incidents that might lead to continued uproar by civil society, reducing governments' ability to invest in other important areas of development, such as infrastructure for roads, schools, and hospitals.

Private investment in the region has stagnated. Big tech companies were able to adapt their data and technology frameworks to comply with GDPR-III and the increased policy and regulation, but this has also deterred local entrepreneurs and SMEs to further invest in the region since compliance has increased operational and administrative costs.

The population as a whole is better off, receiving personalized public services and managing their personal data. However, there is a constant struggle to finance these activist groups, and a downward spiral is a continuous threat if citizen engagement and pressure to use technology for good is somehow diminished.

Power to the People: A Day in the Life of Carmen

Carmen is an active member of society, committed to creating awareness of the importance of privacy and personal data. Today, she wakes up with a couple of new ideas. She needs to engage more actors to the citizen participation forum that is willing to review the updated procedures for the deployment of digital identification for minors. She prepares her regular cup of coffee, takes some bites of her cheese sandwich, and drops an apple into her bag. She needs to hurry up. It will take her at least 30 minutes to get to her co-work office, since one of the biking trails is under repair.

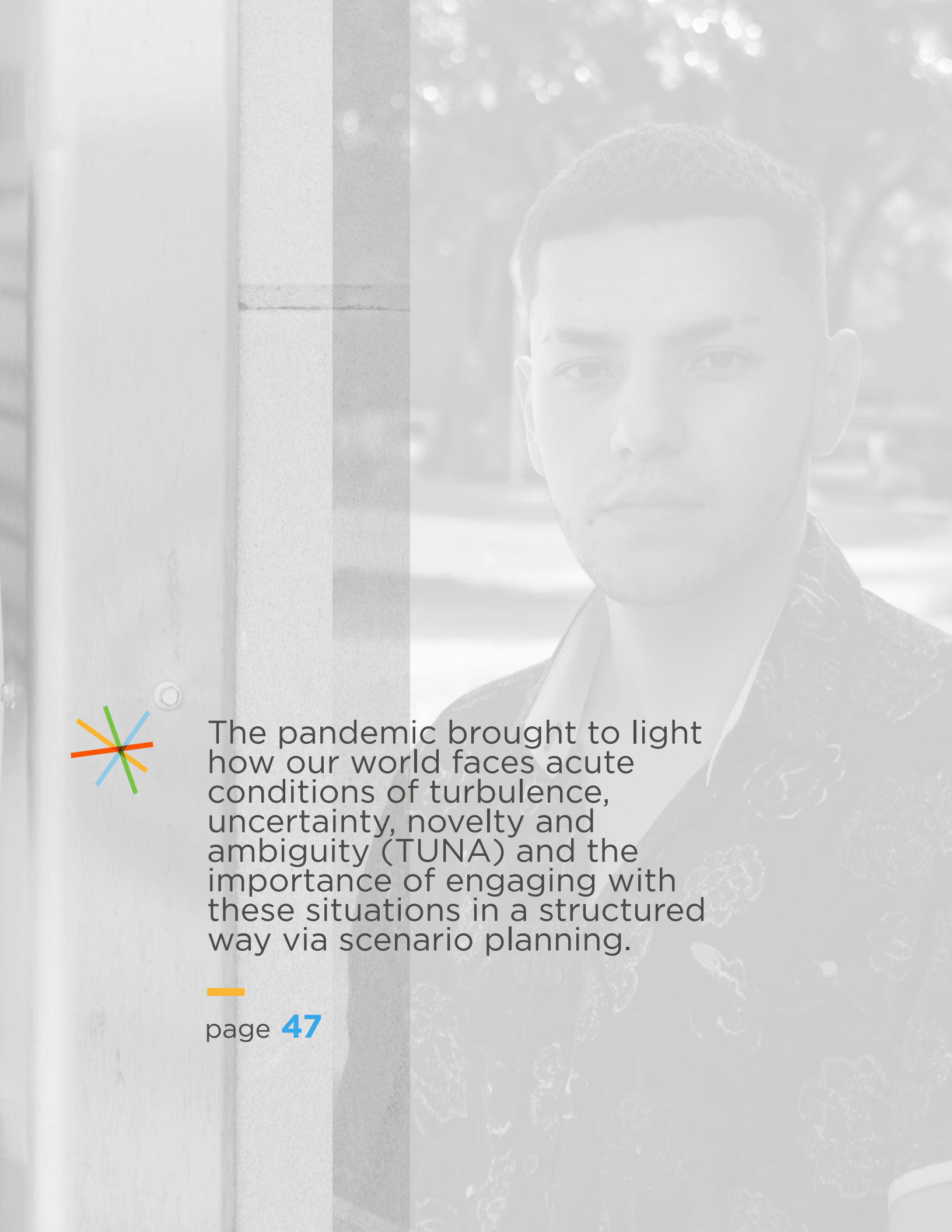
In her shared office, Carmen reads her emails and a message gets her attention. A private tech company wants to sponsor the growth of the platform that is hosting the forum, and the company offers her a position as communications director due to her active role as a civil society representative. Carmen is suspicious of the proposal. The forum is a non-profit platform sponsored by citizens. Being financed by a private company or even by the government could create a lot of conflict of interest, and Carmen is committed to avoiding this. Minutes later, Andrew, a civil society advocate, sends her an email. The forum is lacking funds, and an e-payment is needed to maintain the platform online and updated. In the last two years, maintenance costs have increased due to the size of the platform and fees for the firewall solution required to protect the identity of the participants.

It is almost lunchtime, and Carmen needs to pick her kids up at school. Lunchtime is her favorite time of the day to catch up with the kids. Every weekday, they go to a small restaurant next to her Andean organic food store, they eat the regular lunch menu, and Carmen hurries her kids to finish their meal. At 2:00 p.m., she begins her shift at the store.

Once at the store, she gets a WhatsApp message. A meeting with government officials was scheduled for later today. They plan to share the changes on the privacy and personal data regulation for minors. She immediately forwards the message to the WhatsApp forum group, and 15 members confirm their availability to attend. The government promised a consultation with civil society before publishing the regulation. While participating in the conversation with the group chat, Carmen's son texts her. A math exam has been scheduled for tomorrow and he needs Carmen's help. This text surprises her, because

her son is sitting next to her. She is probably spending too much time dealing with many things on the side. She puts away her cellphone and helps her son.

Once the store closes, Carmen heads home along with her partner and children. Andrew calls her. He needs to know if some emergency funds are available. The forum website will collapse if payment is not processed within three days. Carmen is worried and she is constantly thinking how this important wave of civil society engagement will be maintained. She fears a backward spiral, where because of lack of resources citizen engagement and pressure to use technology for good is somehow diminished. At night she starts working on a sustainability plan for the forum. She believes that a solution can be found, and that more people will engage with the civil society mission. She is certain that commitments and changes can happen.



The pandemic brought to light how our world faces acute conditions of turbulence, uncertainty, novelty and ambiguity (TUNA) and the importance of engaging with these situations in a structured way via scenario planning.

2020 TO 2030: SCENARIOS TIMELINES

	2020	2022	2025	2027	2030
E-nequality	Governments are required to be more efficient and improve efficiency and effectiveness of public expenditures for the provision of better services.	Digitalized and automated services increase, implementing the use of digital ID for all transactions.	New research data on technology reflects an important gap between connected and disconnected population; while Governments in LAC sign new public – private partnerships.	Private sector deploys platforms to support government services; which now are more effective and efficient, as well as accessible for those that are connected.	All citizens have a digital identity to interact online and a new debate on privacy concerns and new cyberattacks arises.
Big Brother	Crime and corruption problems are increasing in LAC.	Governments invest in new technologies and data solutions to target crime and corruption practices.	Digital identification systems are used to access all online public services. The digital economy in the region is increasing, while ethics and privacy on the use of personal data is breaking apart.	Governments are managing a lot of information which is being used to personalize services, provide access to finance, and control migration flows.	Personalized digital profiles have been developed and authentication services are creating revenues for governments.
Power to the People	Migratory flows keep increasing in the region, while intervention actions are being discussed to respond to the crisis.	Digital identifications are issued to migrants at border crossings to ease their access to social services and increase security.	The Wikileaks scandal is still under investigation while a massive data breach containing private information of migrant children was reported. Civil society groups start demanding more data privacy and protection.	Governments agree to adopt the GDPR-III and several negotiations are being organized. The Data Spring takes place.	Civil society has an active role in promoting the ethical use of technology.

Scenario comparison chart

	E-NEQUALITY	BIG BROTHER	POWER TO THE PEOPLE
Geopolitics	• Regional Integration is in good shape. • The main trading blocs—Alianza del Pacífico, CACM, CARICOM, MERCOSUR—are more integrated.	• International banks and funders extended support for acquisition of technology and equipment.	• European organizations helped finance civil society's Digital Spring in LAC.
People movements	• Knowledge services and goods are on the move, powered by digital services that know no border. • Farms are more automated, so people can move from small towns and rural areas to big cities.	• People's access to travel is being restricted based on their digital profile. • Large migrant movements caused by the negative effects of climate change are being registered using biometrics for control.	• Migration destabilized the region. • Substantial migration due to persistent and increasing levels of violence, economic instability, and widespread hunger.
Role of civil society	• Few civil society organizations focus on the unconnected or under-connected. • Few donors provide money to close the technology gap. • Some civil society groups are demanding more responsibility in the use of technology, but their voices are weak. • Citizens are divided between those who are connected and those who have little or no digital presence.	• Blindly trust their governments. • No demand for accountability in the use of personal data and a complete lack of checks and balances.	• Protests led by civil society about the lack of privacy and data protection rights led to the Data Spring of 2026. • Digital citizens are the main drivers that demand sound policy and regulatory frameworks. • Hold governments and private sector accountable on the transparent and ethical use of technology and data.
Privacy/ trust/use of data	• Companies have introduced schemes to exploit personal information to better target products and develop new services. • For the under-connected, citizens' privacy is blatantly violated, but connected citizens are happy to have their data mined for specific purposes.	• No privacy frameworks put in place, leading to government expansion of the use of data and AI to subjugate citizens. • Censorship, filter use of social media. • New social score system linked to a universal digital identification system used to determine access to public services, voting, and access to credit.	• Initial use of the digital identification systems to discriminate against migrants by excluding them from social programs and use of biometric information for surveillance purposes. • Renewed engagement fostered the adoption of GDPR-III.

	E-NEQUALITY	BIG BROTHER	POWER TO THE PEOPLE
Role and shape of private sector	• New public-private partnerships were put in place to lure talent required to digitize and automatize governments. • Deployed proprietary platforms that support all government services, locking in the provision of services. • Monopolistic providers of technology for government. • Monetizing personal information.	• Big tech companies partnered with government to provide cheap technological solutions, locking in governments for product and service supply. • Launches and manages the universal digital identification system used by governments.	• Private sector in the region has stagnated. • Increased policy and regulations have deterred local entrepreneurs and SMEs to further invest in the region.
How the vulnerable are served	• Inequality is more rampant than ever. • The promise of 100 percent coverage of broadband and affordable connectivity for all never reached the more remote regions. • Under-represented in government. • Struggle to receive public services or must spend more time and money at the few physical offices. • Service standards are lower.	• Forced to interact in the digital space with no knowledge of privacy rights and personal data management. • Rural populations struggling due to climate change related natural disasters. • Quality in public services is still lacking.	• Population is better off, receiving personalized public services and managing their personal data.
Cybersecurity	• Increase in number of identity thefts, the unconnected are the most frequent victims. • Lack of competition in the private sector has increased vulnerability to cybercrime.	• Critical challenge for governments. Countries lack concrete actions and procedures to address cyber threats. • Increased frequency and sophistication of malicious cyber activity.	• Large government capital allocations go to cybersecurity to prevent incidents that might lead to continued uproar by civil society.
Role of government in digital economy and/ or digital identity	• Substantial investments in infrastructure that facilitated the digital economy, benefiting segments of the population with more digital skills. • Focus on efficiency and quality of service makes governments rely on the private sector with little attention to regulations on privacy or inclusion.	• Government slowly builds a surveillance system based on digital identification with the initial objective of public safety.	• Digital identification systems are developed with an emphasis on service provision without the necessary data protection mechanisms (from legal framework to cyber security). • After huge breaches, governments adopt a more responsible role and involve civil society as a key partner in monitoring digital identification policies and practices.

COVID-19 Pandemic

This scenario set was developed prior to the COVID-19 pandemic. The pandemic brought to light how our world faces acute conditions of turbulence, uncertainty, novelty and ambiguity (TUNA) and the importance of engaging with these situations in a structured way via scenario planning. Moreover, the acceleration in the use of digital tools by government, citizens, and organizations, the resurgence of cybercrime, and the increase in technology that uses personal data (such as contact-tracing apps) show the importance of engaging in a conversation about plausible future scenarios for digital identification systems.

As of August 2020, the severity and duration of the impacts on health and the economies of LAC are causing uncertainty. Although the pandemic may bring significant changes to the region, the scenario set presented above appeared plausible, relevant, and challenging at the time of writing. The following is an outline of early warning signs of the scenarios unfolding given the COVID-19 pandemic.

	E-NEQUALITY	BIG BROTHER	POWER TO THE PEOPLE
Geopolitics	• Inequality gap in access to healthcare system, tele-working. • Online education increases gaps and digital divide (or unconnected were left behind in educational outcomes and overall social welfare).	• Google and Apple partnering to provide contact tracing apps. • Restriction on travel/ movement based on health records • Centralized State model with strong social cohesion seems more able to cope with turbulence.	• Social tensions given poor management of pandemic and economic consequences. • City level of action proved more effective than national level in taking concrete measures to face the crisis.
People movements	• Countries closing borders due to pandemic. • Migrants deciding to return to their countries due to economic crisis.	• Travel restrictions based on health records.	• Migrant support networks expand. • Digital spaces for advocacy are growing because of the lockdown.
Role of civil society	• Civil society grew complacent as digital services guaranteed access to services throughout the crisis. • Civil society advocates for more inclusive digital services and the reduction of digital gaps.	• Citizens afraid to gather and protest over fear of contagion. • Growing concerns of government's concentration of power and control due to increased surveillance over contact tracing apps and technology.	• European movements against government's use of personal health data, increase privacy concerns. • Civil society assessing government tools to fight the pandemic. • Civil society advocating for stronger data protection laws.

	E-NEQUALITY	BIG BROTHER	POWER TO THE PEOPLE
Privacy/trust/ use of data	• Digital divide and skills make people aware (or not) of the use of their personal data. • Tech designed to track and trace patients is obligatory for essential workers, having to accept terms of use that infringe on human rights.	• To guarantee access to health information, social services and employment, people do not question giving government access to their data, including location. • Due to the emergency, governments may use personal information, but it is a thread that they will continue after the pandemic.	• Social media data is being used to track citizens with a concern from civil society. • Citizens not trusting governments to host their data because of weak regulations. • Other types of governance data models emerge (Data Trusts) to use citizen personal data.
Role and shape of private sector	• Collaboration emerges between big tech companies and lean startups with governments to deliver medical supplies and other basic services.	• Big tech companies' partner with governments to provide cheap technological solutions to track contagion and social distancing, accelerating the launching of a universal digital identification system. • China rolls out 5G in the region.	• Digital startups emerge at the local level. • People start to understand the value of their personal data collected by the private sector.
How the vulnerable are served	• Digital divide affects how vulnerable communities are served. • Lack of access to online services due to connectivity and digital tools. • Financial inclusion is also affecting access to social benefits during the pandemic.	• Government is monitoring movements through digital services. • Vulnerable communities are being tracked.	• Some local organizations are helping communities and replacing government services.
Cybersecurity	• The rapid shift to a more connected workplace during the pandemic increased vulnerability to cybercrime.	• Online spaces/movements are more vulnerable to hacks/ threats.	• Social movements are supporting citizens in being aware of cybercrimes/fake news/online harassment.
Role of government in digital economy and/or digital identity	• Governments attempt to deploy tech and enable digital identity schemes. • The rapid development of this tools might not consider privacy or cybersecurity aspects of the solution.	• Driven by the concern of public safety, governments invested heavily on surveillance systems and technology, using private providers of data to track citizen's social distancing and movements. • Little attention is paid to data protection mechanisms.	• People are more aware of how digital identity can give them access to services, but some privacy concerns emerge.

HOW TO USE THE DIGITAL IDENTIFICATION SYSTEMS SCENARIOS

Part

04

Those who use the scenarios should apply them to their own views and context.

The scenario planning approach is one of the methodologies being used by the IDB to support programming processes at the country and sector levels. This process on the future of digital identification systems in LAC was intended to support robust identity systems in the region and strengthen e-government agendas, with the idea that our stakeholders and individuals that work on or can be impacted by the evolution of digital identification systems in the region could use this material.

The following toolkit was conceived for the use of civil servants and policymakers in charge of national identification offices. It is not intended to create new scenarios (this will not replicate the methodology described in Section 2) but to allow any entity or citizens to systematically reflect on the scenarios described in Section 3. In particular, the following templates should help:

- Read and reflect on each scenario
- Challenge assumptions
- Identify implications of the scenarios for their work.
  - What are the biggest challenges that these stories bring?
  - What opportunities arise?
- Windtunnel or test current digital identification strategies against the scenarios and ask:
  - In these worlds, what should we do more of? What should we do less of?
  - What new collaborations should we develop now to prepare for this world?
- Inform decision making
- Identify priorities
- Engage in interesting conversations

Those who use the scenarios should apply them to their own views and context and understand that the scenarios presented here are stories of what might happen to the context of digital identification systems in LAC. By using them, readers can identify potential actions they can take and then later decide what they choose to do in the form of strategy. A set of templates are presented below to help guide discussions on the three scenarios and their implications for digital identification systems.

For the following exercises, it is recommended to form three groups with four or five participants each. Each group should be diverse and gender balanced and must include officials who work directly with the identification offices as well as officials who collaborate in entities that use or could benefit from digital identification services.

STEP 1: Ghost Scenario 2030

The ghost scenario is a story that describes what you are currently planning for. Imagine you could tell the story of the future of digital identification systems in 2030 for which you are preparing for. What would it look like?
Instructions: In working groups, write a story that describes how the current identification system of your country works. Include background information about the points listed below:

Institutional capacity	
Telecom infrastructure	
Legal framework	
Cybersecurity	
Privacy and use of data	
Geopolitics	
Role of the civil society	
People movements	
Others	
Main description of the current scenario	

STEP 2: Engaging with the Scenarios

Instructions: Each working group should read the three scenarios and answer the following questions. After answering the questions, share and discuss your answers with the other working groups.

	E-NEQUALITY	BIG BROTHER	POWER TO THE PEOPLE
How different is this scenario form your ghost scenario? *List the most salient differences*			
Is there anything you find surprising about the scenario? *Explain why you find it challenging*			
Are there any assumptions from your ghost scenario that might be challenged?			

STEP 3: SWOT Analysis

Instructions: Analyze and describe how each scenario impacts your current context.

	E-NEQUALITY	BIG BROTHER	POWER TO THE PEOPLE
Opportunities			
Threats			
Strengths			
Weaknesses			
Winners: *which actors/ institutions/individuals benefit from this scenario*			
Losers: *which actors/ institutions/individuals lose from this scenario*			
New Entrants *which actors/ institutions/individuals appear in this scenario*			

STEP 4: Time to Compare

How would these future scenarios impact your strategic objectives and operational footprint?

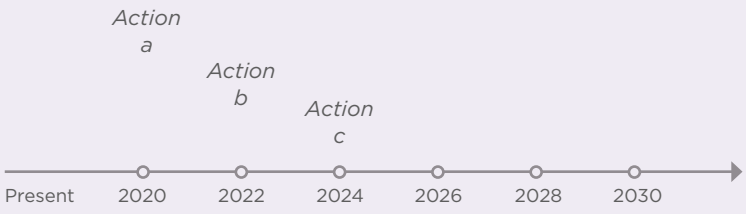
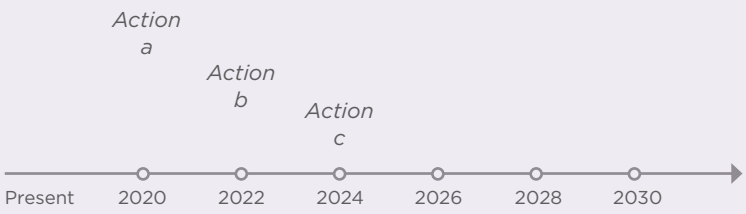
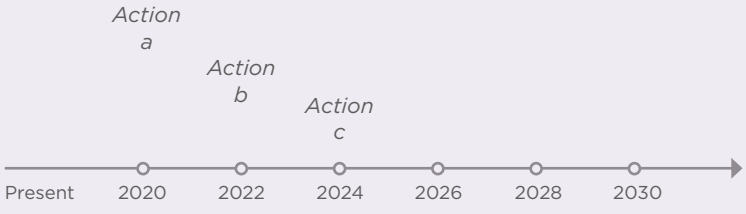
Instructions: Work with all the participants in a plenary session and together complete the following chart

	CURRENT (GHOST) SCENARIO	SCENARIO: E-NEQUALITY	SCENARIO: BIG BROTHER	SCENARIO: POWER TO THE PEOPLE
Strategic objectives • Financial sustainability / growth • Current customers (user satisfaction) • Technology management • Institutional management • Training / knowledge development				
Operational objectives • Human resources • Delivery services • Hours of operation • Customer service • Operation cost				
How would the selected future scenario impact your strategic objectives and operational footprint? Strategic objectives				
Operational objectives				

STEP 5: Work on your own strategy

Instructions:

1. Complete the chart. Each strategy or action plan could be elaborated by each working group or by all the participants

Identify (3) potential strategies or action plan for each described impact (part 4)	**STRATEGY 1**	**Timeline for strategy 1** 
	STRATEGY 2	**Timeline for strategy 2** 
	STRATEGY 3	**Timeline for strategy 3** 

2. For each identified strategy, define:

Actions to take now (in the next year)	
Actions to take in the near future (in the next two years)	
Actions to take in the future (in the next five years)	
Detailed timeline for each activity	
Define indicators and monitoring plan for each action	

3. Complete the following chart / future work plan

OBJETIVE	ACTIVITY (related with the planned action)	RESULT/PRODUCT	INDICATOR	RESPONSIBLE ACTORS	ASSOCIATED RESOURCE	DATE


IDB
Improving lives