

CARETAS DIGITALES,

DIGITAL IDENTITY
IN CENTRAL AMERICA





This research is licensed under Creative Commons Attribution 4.0 International (CC BY SA 4.0):
<https://creativecommons.org/licenses/by-sa/4.0/>

Edition: Iris Mojica
Layout: Juan Pablo Hoyos
Coordination: Lía Hernández
Research: Abdías Zambrano
Review: Alejandro Quiñonez and Marion Briancesco
Proofreading: Belisario Castillo

January, 2021



IPANDETEC Centroamerica is a non-profit organization based in Panama City, Panama, Central America which promotes the use and regulation of ICTs and the defense of Human Rights in the digital environment, through advocacy, public support, research, monitoring and follow-up of Internet legislative Public Policies in Central America.

This research was possible thanks to a donation from Privacy International.

INDEX

Index.	2
Introduction.	3
Methodology.	5
I. Current situation of countries subject of this study	6
1. Costa Rica.	7
2. Guatemala.	11
3. Panama.	14
II. Analysis of the study countries.	19
Test on digital identity systems. Costa Rica.	22
Test on digital identity systems. Guatemala.	27
Test on digital identity systems. Panama.	31
Conclusions and Recommendation.	35
Bibliography.	38

INTRODUCTION

For centuries, humans have struggled to find themselves. That search that is born from our origins, our family, relatives, friends, our ethnic group, passing through our religious confession and wealth, is the search for our identity.

According to English language dictionaries, identity is the set of characteristics of an individual or of a community that characterize it compared to others.

In this search, numerous groups of people have found among themselves, certain peculiarities that make them similar or equal, which has made them to live in society, form tribes, nations and states, united under a single identity.

As a consequence, most countries with a civil law system have identity documents with different names, depending on the country. This is in great contrast to countries that maintain the Anglo-Saxon system of law where it is considered that having this type of control and information could be dangerous for citizens' freedoms.

In the beginning, only people who the State recognized as citizens received this document, meaning, men. It is not, until the countries of Latin America recognized women with equal rights, then, the issue and distribution of identity documents to this population is extended. Even today there has been a trend in recent years to issue identity documents for minors.

With the emergence of new technologies, identity has gone from passports and registration books to databases and cloud computing, bringing with it the emergence of what is known as "digital identity".

Digital identity is described as the set of data available electronically, initially personal data, including banking information and statistics, images, news in which we appear and social networks. Our whole life rests online and many times without our consent.

Today, more than ever, our identities are in danger thanks to the emergence of digital identity. The largest platforms of the digital world know more about us than we do. All of our data is scattered across social media and all of our sensitive information can get into the wrong hands with a single leak.

For this reason, countries around the world seeking to ensure the transfer of data, have created international organizations and conventions that allow protecting personal data wherever they are, transferring them in a safe way, providing a correct level of security through international standards.

However, not all countries have made it a priority, thus leaving millions of people unprotected. On the other hand, the appearance of a new virus that is affecting all humanity, has changed our lives even more, affecting our identities in the digital world as well.

Governments have developed digital identity systems, compatible with applications that allow self-diagnosis, traceability and early warning of any issue.

In Central America, three countries already have or have had this type of tools and they are the protagonists of this study, in search of their digital identities, before and during the pandemic.

METHODOLOGY

The objective of this research is to preliminarily address the legal and institutional aspects of the digital identity systems of three Central American countries: Costa Rica, Guatemala and Panama, emphasizing their relationship with the health sector due to the pandemic of COVID-19. For this, we have used the series of reports made by **IPANDETEC** entitled “Central American Studies on Data Protection” that were published in 2019 and allow us to better understand the Central American reality on the legislation regarding privacy and the protection of personal data.

Comparisons must be made between these three countries to measure their level of development on digital identity, as well as their strengths and weaknesses. In addition to mapping their institutional environment, we have chosen a descriptive analytical approach.

First, the three countries chosen for this study and a short historical summary of each one will be presented. Subsequently, the legal framework following the Kelsen Pyramid will be analyzed to understand the situation in each specific country and the legal institutions that rule them.

In the best of cases, our aim is that in the future, it will be possible to analyze the level of maturity of Digital Identity Systems in Central America for which we are going to use an instrument developed by the Center for Internet and Society (CIS India) in its proposal “The Appropriate Use of Digital Identity”. This instrument allows to measure how legitimate, safe and respectful with Human Rights is a Digital Identity System, through a validation system of three factors. With this, we hope to have a first look at the strengths and weaknesses of the systems studied and thus be able to make proposals for improvement.

I. CURRENT SITUATION OF THE STUDY COUNTRIES SUBJECT OF THIS RESEARCH



COSTA RICA

Costa Rica is a country with a presidential government system, located in the center of Central America, shares borders with Panama and Nicaragua. This Central American country has a little more than 5 million people in its seven provinces. For decades, it has been recognized as one of the most stable and progressive countries in Latin America; an example of this is its high levels of development and competitiveness.

The country has undergone constant changes since its independence in 1821, through the Civil War of 1948. This last event greatly influenced its current development: the army was abolished, the banks were nationalized, the electoral body was integrated, the right was granted to vote for women and the Afro-Caribbean population, in addition to promulgating its current Constitution. The current political constitution of Costa Rica was created in 1949, after the incumbent president summoned a National Constituent Assembly. The approval and entry into force of said constitution took place on November 7 of that same year.

In the field of human rights, Costa Rica is a regional and global benchmark. Its capital is home to the Inter-American Court of Human Rights, a controversial body of the inter-American human rights system, as well as multiple agencies and non-governmental organizations; at the same time, it is the first and only country in Central America to allow same sex marriage.

LEGAL FRAMEWORK

When it comes to privacy and personal data protection, Costa Rica is a pioneer in the region. In its constitution, it recognizes the right to privacy and the inviolability of communications, except by judicial mandate. In addition, this same document recognizes in article 48 the action of habeas corpus and the appeal for protection, as mechanisms for the protection of the rights of people in general. However, habeas data is not considered, being subsumed in the two mentioned actions.

At the next legal level, we find the Law for the Protection of the Person against the processing of personal data (Law No. 8968) and its regulations. This law regulates the protection of personal data in Costa Rica, provides rights over citizens and their privacy, data transfer procedure, creates a regulatory authority, in addition to stipulating exceptions to consent and data management.

The Data Protection Law contains three exceptions to its application: when the databases are for exclusively internal, personal or domestic purposes, as long as they are not sold or marketed in any way. Likewise, article 8 states that the provisions of the law can be limited in six cases due to State security, security and exercise of public authority, prevention, prosecution, investigation, detention and repression of criminal offenses or infractions of deontology in professions related to database management that is used for statistical, historical or scientific research purposes when there is no risk that people will be identified for the adequate provision of public services and for the efficient ordinary activity of the State.

Regarding personal health data, this law contains a rule on prior, irrefutable and express consent. However, in article 9, it is stated that, although the processing of sensitive data such as health data is prohibited, these can be processed when it's necessary for prevention or for medical diagnosis, the provision of health care, medical treatment, or the management of health services.

On the other hand, some other regulations related to clinical data. Law No. 8239 Rights and duties of users of public and private health services contemplates in article 2 that patients and users of health services have the right to have confidentiality and respect of their medical records and all the information related to their illness, except when by special law notice must be given to the health authorities. Also, Law 9162 Unique Digital Health Record, provides in article 11 that all the information contained there is considered private information that contains sensitive data and the processing of such data is prohibited.

INSTITUTIONS

In Costa Rica, there are several institutions that have interference in the digital identity and the treatment of the personal data of citizens in the health sector, before and during the pandemic. Below, we provide a brief analysis of each of them

The **Inhabitants Data Protection Agency (La Agencia de Protección de Datos de los Habitantes-PRODHAB)** is the governing body for the protection of personal data in Costa Rica. Its functions include: ensuring compliance with data protection regulations, opening investigations and imposing sanctions, educating on personal data, among others¹.

The **Supreme Electoral Tribunal** is an independent entity whose functions include the electoral administration and the civil registry of Costa Ricans. Births, adoptions, deaths, among other events and civil acts, are registered in this institution. Upon reaching the age of majority, this entity issues an identity document called an identity card².

This document is granted to any national who reaches the age of 18 and is used in judicial proceedings, banking procedures, voting, among any other legal procedures that require the use of such document. The document contains a photograph of the person, a personal identity number, his signature, as well as other personal data of the person who owns it. On the back, you will find the person's fingerprint and a barcode with various personal information. The Supreme Electoral Tribunal (TSE) has expressed its intention to migrate to an identification system with biometrics and eliminate identity cards.

The **Ministry of Science, Technology and Telecommunications** is the ruling institution of science and technology in Costa Rica. Through it, various digital government initiatives are carried out following the Digital Transformation Strategy 4.0³.

(1). Agencia de Protección de Datos de los Habitantes (PRODHAB). Disponible en: <http://www.prodhab.go.cr/>

(2). Tribunal Supremo de Elecciones. Disponible en: <https://tse.go.cr/>

(3). Ministerio de Ciencia, Tecnología y Telecomunicaciones. Disponible en: <https://www.micit.go.cr/>

The health sector has two institutions: The Ministry of Health⁴ and the Costa Rican Social Security Fund (Caja Costarricense de Seguro Social, CCSS)⁵. The Ministry of Health is the one who dictates public health policies. The CCSS provides health services, pensions and social benefits to Costa Ricans.

COVID 19

During the pandemic, the Costa Rican authorities presented an update to an existing tool. **EDUS** or **Single Digital Health Record (Expediente Digital Único de Salud)** is an application of the Costa Rican Health Fund that can be downloaded in Android and iOS⁶ application online stores. The application allows affiliated individuals to verify their personal data, pending and previous medical appointments, as well as, request or cancel their appointments and that of their dependents in the medical care institution that is part of this system, being able to do validation of rights, prescribed medications, diagnoses and allergies as well.

In their update 4.1.0, they included the possibility of registering symptoms to calculate the risk for coronavirus and recommendations to be followed by the user after their results.

In the privacy policies of the application published on the institution's website, they affirm that they collect and process personal data as dictated by the Law on Protection of the Person against the processing of their personal data.

This policy explains that, when accessing this application, certain data is automatically collected such as IP address, device characteristics, operating system, language preferences, referring URL, device name, country, location, information on how and when you use our applications and other technical information. They share the information with third parties when there is consent, legal basis or vital interest.

(4). Caja Costarricense de Seguro Social. Disponible en: <https://www.ccss.sa.cr/>

(5). Ministerio de Salud de Costa Rica. Disponible en: <https://www.ministeriodesalud.go.cr/>

(6). Aplicación EDUS. Disponible en: https://play.google.com/store/apps/details?id=com.ccss.expedienteunico&hl=en_US&gl=US

However, the privacy policy does not clearly stipulate the maximum storage time limit. It mentions that the information will be kept in their systems for the time required by law, to later be eliminated or anonymized.

Finally, the policy clarifies to the user that, if at any time they believe that their data is being used illegally, they can exercise their rights to review, change or cancel their account at any time. You also have the right to file a complaint with your local personal data protection authority.

I. CURRENT SITUATION OF THE STUDY COUNTRIES SUBJECT OF THIS RESEARCH

GUATEMALA

Guatemala is a presidential republic founded in 1821 with more than 14 million people in its 22 departments. It shares borders with Honduras, Mexico and El Salvador.

Unlike other countries in the region, it had a civil war for decades, which has caused its levels of poverty and income inequality to be high. As a Proof of this is that 59.3% of the country is in poverty, registering an increase of 8.1% since the last measurement⁷. Despite this, its economy is the first in Central America.

In terms of human rights, the country maintains and presents structural challenges in terms of access to justice and impunity, citizen security, marginalization and discrimination that have severely affected the human rights of its inhabitants⁸.

(7) Encuesta de Condiciones de Vida (Encovi 2014). Sitio web: <https://www.ine.gob.gt/estadisticasine/index.php/usuario/encovi>

(8) Pueblos indígenas: diversidad, desigualdad y exclusión en Guatemala. Sitio web: <https://www.oas.org/es/cidh/multimedia/2016/guatemala/guatemala.html>

LEGAL FRAMEWORK

The Guatemalan constitution recognizes in article 24 the secrecy of communications and in article 31 the right to informative self-determination is recognized. This same document recognizes the action of legal protection as a mechanism for the protection of people's rights in general, and the habeas data action is contemplated in article 30 of Decree 57-2008 Law of Access to Public Information as an administrative resource and not as a constitutional guarantee.

Unlike other countries in the region, Guatemala is one of the Central American nations that does not have a personal data protection law. However, in regard to the State, there are certain rights regarding data processing included in Decree 57-2008, Law on Access to Public Information.

Regarding personal data of the health sector, Decree 27-2000 General Law for Combating the Human Immunodeficiency Virus HIV and the Acquired Immunodeficiency Syndrome AIDS and the Promotion, Protection and Defense of Human Rights of HIV-AIDS patients, contemplates in article 38 the right of patients to confidentiality. In this sense, the prohibition of referring to the patient's illness without prior consent is established.

Also, the Code of Ethics for medical professionals provides, in its article 47, that the doctor must not publish, by any written, digital or other means, photographs, diagnostic studies, names or any other indication that identifies their patients.

INSTITUTIONS

In Guatemala, there are several institutions that have involved in the digital identity and management of the personal data of citizens, in the health sector during the pandemic. Below, we provide a brief analysis of each of them.

The **National Registry of Persons** is the Guatemalan public entity in charge of the single registry of citizens, registration of acts, in addition to being in charge of issuing the Personal Identification Document⁹.

This document has been the object of evolution since its creation at the beginning of the Republic, known as the identity card. Currently, the document has the single identification code, name, gender, nationality, date of birth and issue, photo and signature of the person who owns it.

In addition, it has an internal chip that saves the person's facial features, their fingerprints and their signature. The document is used in civil, administrative and legal acts in which it is requested.

Ministry of Public Health and Social Assistance governing institution of health in Guatemala. The ministry has public hospitals, health centers, pharmacies, among other service centers nationwide¹⁰.

The **Guatemalan Social Security Institute** offers medical care and pensions for various reasons such as maternity, old age, disability and death¹¹.

(9) Registro Nacional de las Personas. Sitio web: <https://www.renap.gob.gt/>(8) Pueblos indígenas: diversidad, desigualdad y exclusión en Guatemala. Sitio web: <https://www.oas.org/es/cidh/multimedia/2016/guatemala/guatemala.html>

(10) Ministerio de Salud Pública y Asistencia Social. Sitio web: <https://www.mspas.gob.gt/>

(11) Instituto Guatemalteco de Seguridad Social. Sitio web: <https://www.igssgt.org/>

COVID 19

During the pandemic, the Guatemalan government introduced the Guatemalan Alert application. This was an application developed by In-telligent Properties LLC and used by the Guatemalan government to fight against the spread of coronavirus in the country. After multiple criticisms from international human rights organizations, concerned about the data protection given by the application, it was removed from Android stores.

In a later analysis, it was found that the application was sending the exact location of users to its developer, even when the application was not in use. In its privacy policy, it was detailed that the storage time of the data collected by the application was 10 years, without showing any justification.

I. CURRENT SITUATION OF THE STUDY COUNTRIES SUBJECT OF THIS RESEARCH

PANAMÁ

Panama is a presidential republic located in the southeast of Central America, sharing borders with Costa Rica and Colombia. The country of just over 4 million, according to the latest estimates, has 10 provinces and 5 indigenous regions.

The nation gained independence from Spain in 1821, however, unlike its Central American neighbors, it voluntarily joined Colombia. It is not until 1903 that this union ends and the construction of the Panama Canal begins, to be inaugurated in 1914. This work was administered together with the surrounding lands for decades, by the US military.

From the late 1960s to the 1980s, the country was ruled by the military who promulgated the current Constitution in 1972. In 1989, the country was invaded by US troops with a consequent return to democracy. Since then, the country has undergone drastic changes, especially in its economy.

In the economic area, its main sector is that of services, being notable its international banking sector, great logistics movement driven by the Panama Canal, in addition to having one of the airports with the highest traffic in the region.

LEGAL FRAMEWORK

The Constitution of Panama recognizes the right to secrecy of communications in article 29, and in article 42 the right to informational self-determination is recognized. This same document recognizes the action of habeas data as a mechanism for the protection of personal data.

At the next level, we can find Law 81 on Protection of Personal Data that regulates the data processing regime in Panama. However, this rule will still come into force in 2021. The rule contemplates the rights of the owner, the duties when processing the data, sanctions and the powers granted to the governing body.

This same law contemplates, in article 3, five exceptions to its application: for domestic purposes, those carried out by competent authorities for the prosecution of crimes, for the analysis of financial intelligence and national security, in compliance with international treaties, and data obtained through anonymization procedures.

Likewise, in article 8, nine exceptions to consent are included: when the data is owned by a public domain or source, collected in the exercise of the functions of the State, economic or financial data, with previous consent, are placed on lists of certain categories of people in the form of background information, those necessary for business relationships; They are carried out by private organizations for the exclusive use of their associates for statistical purposes or other benefits, in cases of medical or health emergencies, when the law requires so for historical, statistical or scientific purposes and when necessary, to achieve legitimate interests.

Regarding personal data of the health sector, the law has a special label to this data: sensitive data. Article 8 of the law indicates that, in the case of sensitive health data, consent must be prior, irrefutable and express

However, the Personal Data Protection Law of Panama does not regulate all personal data in the country.

For example, Law 26 By which measures of prophylaxis and control of the epidemic of acquired immunodeficiency syndrome (AIDS) and of the spread of the human immunodeficiency virus (HIV) provides in article 12 that the members of the health team who know or care for a sick person, must keep this information confidential. Also, Law 68, which regulates the rights and obligations of patients, regarding free and informed decision information, provides in article 13 that everyone has the right to have their health data kept confidentially, which includes that no one can access them without their authorization.

INSTITUTIONS

In Panama, there are several institutions that have participation in the digital identity, and management of personal data of citizens in the health sector during the pandemic. We provide a brief analysis of each of them below.

First, the habeas data appeal is determined by the courts at different levels. This will depend on the command and jurisdiction that the official or person responsible for the database has, in case they are responsible at a national level, the appeal must be resolved by the plenary session of the Supreme Court of Justice, while, if the person responsible has provincial or municipal command, it must be managed by a Superior Court.

On the other hand, the **Electoral Court of Panama**, through its National Civil Registry Office, is the governmental entity in charge of registrations and certifications of important events, and issue of legal documents, such as: births, deaths, marriages, divorces, among others. This institution grants a document known as a personal identity card that confirms the person's citizenship¹².

(12) Tribunal Electoral de Panamá. Sitio web: <https://www.tribunal-electoral.gob.pa/>

This document, created in 1916, allows Panamanians to confirm their identity and perform any legal act, including casting their vote in the country's popular elections. Since 1958, the taking of the person's fingerprints was included and monetary fines were established for those who did not process their identity card 3 months after reaching the age of majority, which is 18.

The document currently has the legal and usual name of the person, his/her identity number according to their place of birth, sex, date of birth, place of birth, signature and photograph, the date of issue and expiration of the document.

The regulatory body for personal data in the country is the **Autoridad Nacional de Transparencia y Acceso a la Información-National Authority for Transparency and Access to Information** (ANTAI)¹³. This power was conferred on the existing authority through the personal data protection law. This allows them to begin investigations and impose penalties if necessary.

In the field of innovation is the **Authority for Government Innovation** (AIG), an entity in charge of planning, coordinating, supervising and promoting the use of information technologies and communication with the government through modernization of the public sector¹⁴.

Regarding the health system, there are two governing institutions on the matter. There is the **Ministry of Health**¹⁵, whose mission is to guarantee the entire population access to comprehensive care, while the **Social Security Fund**¹⁶ maintains a duality of functions by providing health services and economic benefits, including pensions.

COVID 19

During the pandemic, the government of Panama has turned to technology as the best ally to fight the situation. Applications, bots, web pages, among other digital tools, have been developed to minimize the circulation and the maintenance of quarantine measures in health, education, social security, to name a few.

(13) Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI). Sitio web: <https://www.antai.gob.pa/>

(14) Autoridad para la Innovación Gubernamental (AIG). Sitio web: <https://aig.gob.pa/>

(15) Ministerio de Salud de Panamá. Sitio web: <http://www.minsa.gob.pa/>

(16) Caja de Seguro Social. Sitio web: <http://w3.css.gob.pa/>

The **Protect Yourself Panama Application**, an application for iOS and Android, allows positive coronavirus patients to maintain direct communication with health institutions. This application is based on open source technology such as GNU / Linux, OpenShift and React¹⁷.

When a patient is diagnosed as positive, the health personnel will ask him to create a profile on the platform. The patient will be able to register and access by facial recognition, although it is not specified if this is optional. The patient must report their symptoms daily to the medical team.

Protect yourself is the only technology developed in conjunction with the AIG that uses a geographic tracking system, which can be deactivated at any time by the user. Geo-location data is not correlated with any other user and the data is only used to create incidence statistics by sector.

The AIG website maintains a privacy statement where it specifies its work policy. However, this privacy policy is only framed within government websites, not including the applications or developments of each institution, much less does it contemplate Panamanian regulations on medical data.

So far, the institution has not published any application procedure manuals, although it states that they are in preparation. In response to a request for access to public information, it is detailed that **“digital certificates and high security standards”** are currently being used, without offering further details.



(17) Protegete Panamá. Sitio web: <https://play.google.com/store/apps/details?id=pa.gob.protegete&hl=es&gl=US>

II. ANALYSIS OF THE COUNTRIES SUBJECT OF THIS RESEARCH



II. ANALYSIS OF THE COUNTRIES SUBJECT OF THIS RESEARCH

COMPARATIVE ANALYSIS

Our research has focused on the three aforementioned countries: Costa Rica, Guatemala, and Panama for various reasons that we consider necessary to explain.

First, the three countries maintain a legal framework that, at first glance, seems identical, however, when conducting a comprehensive legal analysis we can see that they maintain differences between them that visualize how different the societies of Central America can be.

Second, the three countries have relied on technology and made use of it, in different ways and with different results, including with a very different approach to human rights.

Finally, their health systems, seeking to improve their services during the pandemic, have developed, together with other sectors, digital tools to counteract the effects of the global emergency situation without sometimes counting on the opinion of users.

We clarify that the data and discoveries that result from this study are not determinants of a superiority in public policies between one nation or another; if not, it will be able to show us which practices or which situations seem more desirable than others, exclusively, with respect to digital identity with an emphasis on health schemes.

COMPARING REALITIES

The Constitutions of the three countries analyzed recognize privacy directly or indirectly as a right. In the express case of Costa Rica, it talks about privacy and the inviolability of communications, in the case of Panama and Guatemala, the inviolability of communications is mentioned.

Of the three countries analyzed, only two have personal data protection laws. Of these two countries, only one maintains its law in force at the time of this study.

The Personal Data Protection Law of Costa Rica dates from 2011, while that of Panama is from 2019; For this reason, we can initially observe that Panamanian law is more up-to-date than Costa Rican law, obeying the digitization that has occurred in recent years. Similarly, Panamanian law introduces the right of portability of personal data, while leaving some powers of the European standard for the protection of personal data outside such as extraterritoriality and obviating the creation of a governing entity; rather, it gives the power to an existing institution, which is one of its great differences with the Costa Rican law that created the Agency for the Protection of Inhabitants' Data (PRODHAB).

Guatemala, despite not having a personal data protection law, its law on access to information is currently the only legal document that regulates personal data and sensitive data, as well as establishes a protection mechanism for both and it also typifies crimes in the matter.

Only Panama maintains the habeas data appeal at the constitutional level. Guatemala regulates it through a law, while Costa Rica still does not include this resource in its legal system.

The privacy of data in the health sector is regulated in the three countries in related regulations. For example, the law that dictates prophylaxis and control measures for the epidemic of acquired immunodeficiency syndrome (AIDS) in Panama provides that members of the health team who know or care for a sick person must keep confidentiality about this information. Also, the law that regulates the rights and obligations of patients regarding free and informed decision-making information, contemplates that everyone has the right to have their health data kept confidential.

This same situation occurs in similar regulations in Costa Rica and Guatemala. In the case of Costa Rica, the Law on the Rights and Duties of users of health care services establishes that patients and users of health care services have the right to have the confidential nature of their medical records and all medical records respected. information regarding your illness. Also, the Law that regulates the Single Digital Health Record contemplates that all information contained in the digital record is considered private information that contains sensitive data and the processing of such data is prohibited.

In the case of Guatemala, the Code of Ethics provides in article 47 that the doctor must not publish by any written, digital or any other means, photographs, diagnostic studies, names or any other indication that identifies the patient.

II. ANALYSIS OF THE COUNTRIES SUBJECT OF THIS RESEARCH

TEST ON DIGITAL IDENTITY SYSTEMS.

COSTA RICA.

This test has been designed taking as a reference the test on Digital Identity System prepared by the Center for Internet and Society (CIS India) with slight changes and additions that complement the Central American pandemic needs and particularities.

The test consists of three different stages: legality, human rights, and risk. Each of the stages with a number of questions with their answer.

A. LEGAL ASPECTS

1. Is the use of digital identity systems regulated by a current law?

Yes, in Costa Rican legislation there are various provisions that suggest a legalization of digital identity systems.

For example, the law on the protection of personal data regulates all those data processed or collected that appear in databases no matter if they are electronic or manual.

Another perfect example is health regulations. The Law that creates the Single Digital Health Record, ensuring a unique identification, consistent with the confidentiality and veracity that should govern the medical care process.

2. Does the law have a legitimate purpose?

Yes, these laws pursue the rights of privacy and protection of personal data, in addition to ensuring access to health.

3. Does the law clearly define the purposes that justify the use of digital identity?

Our research team does not recognize the real purposes that justify the use of digital identity in any of the previous legal documents mentioned. We believe that this may be due to the deliberate lack of regulations that expressly mentions or rule digital identity.

However, due to the legal documents mentioned above, we can assume that the justifications are diverse such as: providing a specialized health service, unique identification of patients and users of health services, so that your unique digital health record is known and include only the appropriate patient information.

4. Does the law explain clearly and in detail who could have access to the database of digital identity systems?

No. The personal data law speaks of private and public organizations that maintain databases, however, it does not clarify whether this includes digital identity and access to information.

On the other hand, the law that regulates that digital filing system belongs to the Costa Rican Social Security Fund, with the support and services of the Supreme Electoral Tribunal and the General Directorate of Migration and Immigration. It does not expressly mention whether these data can be accessed by a sector other than those previously mentioned.

5. Does the law regulate the use of the database of digital identity systems by private companies?

No, as in the previous answer, the databases of digital identity systems are not explicitly mentioned, however, the different regulations and guidelines studied include private actors.

6. Does the law clearly detail the data that can be stored?

No, the Law of Digital Clinical Record and the Law of Protection of Personal Data do not mention what data can be stored. However, the EDUS portable application handles basically, without being limited to:

- Type of identification, identification
- Name and surname
- Sex
- Date of Birth
- Age
- Exact Address
- Number of people living with the person
- User and email
- Risk test information
- Conditions and background.

7. Does the digital identity system provide adequate notification to the user?

No, none of the analyzed systems includes a notification to the user.

8. Do people have rights of access, correction, cancellation and opposition?

Yes, the personal data protection law and other guidelines grant the rights of:

A. Access: through the exercise of this right, the owners of personal data can verify if there is personal data of them in a database, what personal data is being processed by third parties, the purpose of the collection or use of that data, the origin of the aforementioned data, the way in which they are stored and if they have been transferred or will be transferred to a third party.

B. Correction: it is based on the possibility of the owner of the personal data to modify those data that are inaccurate or incomplete, and in the rectification request, indicate which data they want to be modified.

C. Cancellation: any person can request and obtain from the person responsible for handling personal data the deletion of their private information, at any time and under any circumstance. This right includes the right to be forgotten, which consists of the obligation that everyone responsible for a personal database has to suppress those that may affect its owner for a maximum period of 10 years. The foregoing implies that this type of data must be eliminated by its storer, not yet at the request of the owner of these.

D. Opposition: although it is not expressly incorporated as such, it is understood as a derivative of the right of informational self-determination that is guaranteed as a fundamental right, in order to control the flow of information that concerns each person in the terms of the article 4 of the Personal Data Law.

9. Are there mechanisms that provide civil and criminal reparation for violations of digital identity systems?

Not specifically, however, various criminal and civil guidelines provide remedies for some of these cases.

The fines stipulated by the data protection law are destined to updating Prodhab equipment, programs and systems.

B. HUMAN RIGHTS

1. Are data minimization principles followed in the collection, use and retention and storage of personal data for this kind of use given to data?

Yes, the law on the protection of personal data and regulations of the health sector includes principles, specifically those of topicality, truthfulness, accuracy and adequacy.

2. Does the law specify the type of access that the various actors have to personal data?

No, there is a legal vacuum in this regard, since there is no explicit explanation in the standard about the type of access that the various actors have.

3. Is the mandatory use of digital identity to access services something that excludes people from using the service?

Explicitly, there is no obligation to use digital identity to have access to health services in Costa Rica. However, the EDUS is used in all the centers of the Costa Rican Social Security Fund facilities , therefore, the system must be used in order to give a better service.

C. RISK

1. Are identification systems created taking into account potential risks?

Yes. EDUS data transfer is protected with the HTTPS protocol.



TEST ON DIGITAL IDENTITY SYSTEMS. **GUATEMALA.**

A. LEGAL ASPECTS

1. Is the use of digital identity systems regulated by a current law?

No, in Guatemala, as there is no personal data law, there is no digital identity regulation. However, it should be noted that the current law on access to public information mentions personal and sensitive data, but cannot be used as a regulator of digital identity systems, since it is not very specific.

2. Does the law have a legitimate purpose?

The answer to this question can be quite complex. Currently, there is no law that regulates digital identity in Guatemala, so it cannot be considered to have a legitimate objective. However, the law on access to public information regulates habeas data, including articles and provisions for the treatment and access to personal data.

3. Does the law clearly define the purposes that justifies the use of digital identity?

There is no law that regulates digital identity in Guatemala, so it cannot be considered an answer to this question. However, the law on access to public information regulates the personal information owned by people who need to provide such information, meaning the owner of the information.

4. Does the law explain clearly and in detail who can have access to the database of digital identity systems?

There is no law that regulates digital identity in Guatemala, so it cannot be considered an answer to this question. However, the law on access to public information mentions an enunciative and non-limiting list of institutions and organizations, including public entities, non-profit organizations, private companies, among others.

5. Does the law regulate the use of the database of digital identity systems by private institutions?

There is no law that regulates digital identity in Guatemala, so it cannot be considered an answer to this question. However, the law on access to public information is currently applied to them because of the access to public information since t of the subjects they are one of the subjects related to this law.

6. Does the law clearly detail the data that can be stored?

There is no law that regulates digital identity in Guatemala, so it cannot be considered an answer to this question. However, the law on access to public information describes personal data as any information concerning identified or identifiable natural persons.

On the other hand, sensitive personal data includes **“all the physical or moral characteristics of people, facts or circumstances of their private life or activity, such as: personal habits, racial origin, ethnic origin, ideologies and opinions policies, religious beliefs or convictions, physical or mental health states, sexual preference or life, moral and family situation or other intimate or private issues of a similar nature”**.

7. Does the digital identity system provide adequate or timely notification to the user?

No, none of the analyzed systems includes notifications to the user.

8. Do people have rights of access, correction, cancellation, and opposition?

There is no law that regulates digital identity in Guatemala, so it cannot be considered an answer to this question. However, the law on access to public information establishes the resource of habeas data, which safeguards the right of access and correction.

9. Are there any mechanisms that provide civil and criminal reparation for violations of digital identity systems?

There is no law that regulates digital identity in Guatemala, so it cannot be considered an answer to this question. However, it is worth adding that the law on access to information contemplates various resources in the administrative area, in addition to allowing criminal charges or penalties, which will be applied without affecting rightful civil responsibilities and the damages that could be caused by the commercialization or distribution of personal sensitive data.

B. HUMAN RIGHTS

1. Are data minimization principles applied in the collection, use and retention of personal data for this kind of usage?

As there is no personal data regulation in Guatemala, we consider that these principles are not followed.

2. Does the law specify the type of access that all those involved in personal data management have?

Currently, there is no legislation that protects personal data in Guatemala. However, the law on access to information mentions various players or required subjects, who can collect personal information, without specifying whether they can enter the database at their request or not.

3. Is the mandatory use of digital identity to have access to some services

Explicitly, there is no obligation in the use of digital identity to access services in Guatemala.

C. RISK

1. Are identification systems created taking into account potential risks?

The research team of this study did not find security any systems that is prepared to protect the potential risks to which identification systems can go through.



II. ANALYSIS OF THE COUNTRIES SUBJECT OF THIS RESEARCH

TEST ON DIGITAL IDENTITY SYSTEMS.

PANAMÁ.

A. LEGAL ASPECTS

1. Is the use of digital identity systems regulated by a current law?

Not expressly, as it is not mentioned in any law, digital identity systems. However, the law on the protection of personal data could be considered the document that regulates them when processing personal data.

2. Does the law have a legitimate purpose?

Yes, these laws pursue the rights of privacy and protection of personal data, in addition to ensuring access to the health system.

3. Does the law clearly define the purposes that justifies the use of digital identity?

Our research team does not clearly recognize the purposes that justifies the use of digital identity in any of the aforementioned legal documents. We believe that this may be due to the deliberate lack of regulations that expressly mentions digital identity.

However, due to the legal documents mentioned above, we can assume that the justifications are diverse such as: avoiding the change of newborns due to human made errors or as a result of criminal activities through the use of biometrics, medical care of pregnant women without personal identity documents, personal identification documents of deceased people as well as personal identification of patients.

4. Does the law clearly explain in detail who can have access to the database of digital identity systems?

The personal data protection law speaks of **“people who have access or processing of personal data, in public or private institutions.”** Similarly, public and private sector health personnel or doctors are mentioned in the health care guidelines.

However, it should be noted that, during the pandemic, the actors in this situation have greatly increased. Various public institutions have access to sensitive personal data. The Joint Task Force that includes a team of **MINSA doctors stationed at the Emergency Operations Center- Centro de Operaciones de Emergencia (COE) of the National Civil Protection System-Sistema Nacional de Protección Civil (SINAPROC).**

The COE is made up of the Governorate of the province, the Ministry of Health, CSS, the National Police, the National Civil Protection System (Sinaproc), the Ministry of Social Development and community leaders; all this is activated during emergencies. The Authority for Government Innovation (AIG) also has participation.

5. Does the law regulate the use of the database of digital identity systems by private institutions?

No, as in the previous answer the databases of digital identity systems are not explicitly mentioned, however, the different regulations and guidelines studied include private institutions.

6. Does the law clearly detail the data that can be stored?

Yes. The Law that regulates the rights of patients mentions that clinical records must contain certain information, including:

- Name and surname of the patient
- Date of Birth
- Gender
- Personal identity card
- Address of residence and telephone
- Family and personal, physiological and pathological history
- Medical history

7. Does the digital identity system provide adequate notification to the user?

No, none of the analyzed systems includes a notification to the user.

8. Do people have rights of access, rectification, cancellation and opposition?

Yes, the personal data protection law and other guidelines grant the rights of

Access: have access to the data that you have about the owner.

Correction: correct data that is incorrect or has expired.

Cancellation: delete data that should not be collected and processed, or those that have been collected without consent or are not proportional.

Opposition: refuse to process personal data.

9. Are there mechanisms that provide civil and criminal reparation for violations of digital identity systems?

Yes, various health or cybersecurity guidelines provide criminal or civil remedies. Likewise, the personal data protection law stipulates fines, the amount and payment of which must be paid before the regulatory authority and the funds can be used for education on personal data.

B. HUMAN RIGHTS

1. Are data minimization principles followed in the collection, use and retention of personal data for this use case?

Yes, the personal data protection law and health sector regulations include principles that seek to minimize the use, collection, and retention of data, providing protection to the owner of the data.

2. Does the law specify the type of access that the various actors have to personal data?

Yes, the Personal Data Protection Law together with the medical, credit and banking data laws specify the type of access that each sector must have

3. Is the mandatory use of digital identity to access services exclusive?

Explicitly, there is no obligation to use digital identity to access health services in Panama.

However, Panamanians, residents and foreigners who visit Panama during the pandemic do have the obligation to download the Protect Yourself with Health Application for monitoring symptoms during the first 15 days upon returning to the country, as well as positive patients from COVID-19

C. RISK

1. Are identification systems created taking into account potential risks?

Yes. Several identity systems are protected by the HTTPS protocol, SSL digital certificates, VPN connection, Rest type Web API.

CONCLUSION AND RECOMMENDATIONS

The research contained in this study gives interesting results on the situation, progress, and urgent needs of digital identity regulations or laws in three countries in the Central American region. Although only three countries have been studied, these may reflect a situation that may be replicated throughout the region. Although this study just analyzes those technologies developed to fight against the pandemic, specifically mobile applications, our recommendations and conclusions apply to situations that go beyond current and future emergency situations.

All Central American countries must update their public policies to the current needs that the existence of the Internet and the real impact and a growing use of technologies and connected population in this region. Failure to do so involves various problems, not only can it affect the rights of citizens, but also affects the economic and foreign investment attractiveness, as they are countries without legal security in terms of information and communication technologies.

Among the urgent changes in public policies, it is evident the need to promote laws that protect the personal data and digital citizenship of Central Americans. Currently, the General Regulation of Personal Data of the European Union is applied to European citizens anywhere in the world, which can be a starting point for Central American governments, adapting this international mechanism as the best practices to be applied to their national needs in order to visit, live and invest in these countries. Any public policy must be widely discussed through multisectoral consultations that include academia, the technical sector, and civil society.

It is necessary to discuss the creation of specialized entities in the protection of personal data in countries that do not have this kind of regulations, endow them with autonomy, qualified personnel and experts in the matter, with coercive powers and an independent budget that allow the exercise of their functions. By assigning such complex powers as data protection to an existing institution, problems can become up in the workflow that directly affect the citizen.

Another point that should be included in any proposal are the rights of Access, Rectification, Cancellation, and Opposition (ARCO), in addition to discussing the right of portability. The European framework also establishes the right to be forgotten, which has been controversial, so our recommendation is that it should be discussed deeply by the different sectors of their society. Within the discussion we recommend including extraterritoriality that protects the Central American citizen in any territory.

A viable alternative for the region is to discuss these policies at the regional level through the mechanisms provided by various regional and global organizations: The Central American Integration System-Sistema de Integración Centroamericano (SICA) and the Central American Parliament (PARLACEN), the Organization of American States (OAS) and the Latin American Parliament (PARLATINO), or the United Nations system (UN).

Government-run digital identity systems would do well to be audited by civil society, allowing for better development and opportunities of improvement. Those digital identity systems managed by private sector companies must comply with the requirements provided by the state institution in charge of regulating it, in addition to reviews by civil society.

Any technological initiative established during the pandemic should be widely discussed with the various sectors of society, in addition to having expert voices and a deep analysis of the benefits and disadvantages that the development and application of the aforementioned technologies entail. On the other hand, international organizations such as the World Health Organization have issued reports and recommendations on this issue, together with civil society experts from all continents. It is also possible to examine the experiences of other states or cities that have applied similar technologies based on human rights.

Central American States should analyze the option of adhering to international conventions that allow them to adapt their public policies to the same level as other regional blocs, which will allow uniformity in their policies for handling personal and sensitive data, together with a clear policy of cross-border flow of data. For example, Convention No. 108 of the Council of Europe establishes a uniform mechanism for all European states that adhere to it

On the other hand, before developing or implementing any technology, it is vital to examine the population and their behavior, their access to the internet and its quality, the number of devices they have to access the technology, the development of a communication strategy that drives confidence in the population based on data. Similarly, within this analysis, the best option for each individual's based on their income and social status, should be examined as well, implying that the use of technology is not an economic burden for citizens during the current emergency situation. For example, depending on the number of people in a country, it has been demonstrated the percentage of citizens who must actively use technology for its success, otherwise a weak and unsuccessful implementation can lead to failure and loss of investment in the implementation of digital identity systems.

BIBLIOGRAPHY

1. Bhandari V., Trikanad S., & Sinha A.. (2020). Governing ID. Principles for evaluation. 2021, de CIS India Sitio web: <https://cis-india.org/internet-governance/governing-id-principles-for-evaluation>
2. Constitución de la República de Costa Rica (1949). Sitio web: https://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=871
3. Ley No. 8968 de 2011. De Protección de la Persona frente al Tratamiento de sus Datos Personales. (2021) Sitio web: http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=70975&nValor3=85989&strTipM=TC
4. Decreto Ejecutivo No. 37554 de 2012. Reglamento a la Ley de Protección de la Persona frente al Tratamiento de sus Datos Personales. (2021). Sitio web:http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=74352
5. Ley No. 8239 de 2002. Derechos y deberes de las personas usuarias de los servicios de salud públicos y privados. (2021) Sitio web: https://www.ministeriodesalud.go.cr/gestores_en_salud/derechos%20humanos/leyes/leyusuariossalud.pdf
6. Ley No. 9162 de 2013. Expediente digital único de salud. (2021). Sitio web:http://www.pgrweb.go.cr/scij/Busqueda/Normativa/Normas/nrm_texto_completo.aspx?nValor1=1&nValor2=75700&nValor3=93998
7. Constitución de la República de Guatemala (1993). Sitio web: <https://www.ine.gob.gt/archivos/informacionpublica/ConstitucionPolitica dela Republica de Guatemala.pdf>
8. Decreto No. 57 de 2008. Ley de Acceso a la Información Pública. Sitio web: <https://transparencia.gob.gt/wp-content/uploads/2019/03/Decreto-57-2008.....pdf>
9. Decreto No. 27 de 2000. Ley General para el Combate del Virus de Inmunodeficiencia Humana VIH y del Síndrome de Inmunodeficiencia Adquirida SIDA. Disponible: http://www.sipi.siteal.iipe.unesco.org/sites/default/files/sipi_normativa/decreto_no_27-200-_ley_general_del_hiv-_guatemala.pdf

10. Alerta Guate. (2020, Marzo 24). APP_ALERTA GUATE_para control del Coronavirus [Video]. Youtube. Sitio web: <https://www.youtube.com/watch?v=UGBj3TcbnEY>
11. Constitución de la República de Panamá (1972). Sitio web: <https://www.ilo.org/dyn/travail/docs/2083/CONSTITUTION.pdf>
12. Ley No. 06 de 2002, de Acceso a la Información. Sitio web: https://www.kas.de/c/document_library/get_file?uuid=8772cd11-ab07-fc72-06a9-67a17f354d75&groupId=252038
13. Ley No. 03 de 2000, sobre las infecciones de transmisión sexual, el virus de inmunodeficiencia humana y el sida. Sitio web: https://www.hospitalsantotomas.gob.pa/download/transparencia/otros_documentos_y_normas/Ley-3-del-5-d-enero-de-2000-VIH-Y-SIDA.pdf
14. Ley 68 de 2003, que regula los derechos y obligaciones de los pacientes, en materia de información de decisión libre e informada. Sitio web: <http://www.css.gob.pa/Ley%2068%20del%2020%20de%20noviembre%20de%202003.pdf>
15. Resolución N° 945 de 2015 del Ministerio de Salud. Sitio web: https://www.gacetaoficial.gob.pa/pdfTemp/27842_B/52093.pdf

IPANDETEC 
CENTROAMÉRICA