CARETAS DIGITALES,

IDENTIDAD DIGITAL EN EL CENTRO DE AMÉRICA

IPANDETEC
CENTROAMÉRICA

Edición: Iris Mojica
Diagramación: Juan Pablo Hoyos
Coordinación: Lía Hernández
Investigación: Abdías Zambrano
Revisión: Alejandro Quiñonez y Marion Briancesco

Enero, 2021.

IPANDETEC
CENTROAMÉRICA

IPANDETEC Centroamérica es una organización sin fines de lucro, basada en la Ciudad de Panamá, que promueve el uso y regulación de las TIC y la defensa de los Derechos Humanos en el entorno digital a través de la incidencia, investigación, monitoreo y seguimiento legislativo de Políticas Públicas de Internet en Centroamérica.

Esta investigación se realizó gracias al donativo de Privacy International.

INDICE

INTRODUCCIÓN

Durante siglos, el ser humano ha batallado por encontrarse a sí mismo. Esa búsqueda que nace desde nuestros orígenes, nuestra familia, allegados, amigos, nuestra etnia, pasando por nuestra confesión religiosa y riqueza, es la búsqueda de nuestra identidad.

Según el Diccionario de la Real Academia de la Lengua Española, identidad es el conjunto de rasgos propios de un individuo o de una colectividad que lo caracterizan frente a los demás.

En esa búsqueda, numerosos grupos de personas han hallado, entre ellos, ciertas particularidades que los hacen semejantes o iguales, lo que los ha impulsado a vivir en sociedad, formar tribus, naciones y estados, reunidos bajo una sola identidad.

Como consecuencia de ello, la mayoría de los países con sistema de derecho civil cuentan con documentos de identidad con diferentes nombres, dependiendo del país. Esto contrasta de gran forma con los países que mantienen el sistema de derecho anglosajón donde se considera que el contar con este tipo de control e información podría ser peligroso para las libertades de los ciudadanos.

En un inicio, solo las personas que el Estado reconocía como ciudadanos recibían este documento, es decir, los hombres. No es, sino hasta que los países de Latinoamérica reconocieran a la mujer en igualdad de derechos, que se extiende la fabricación y entrega de documentos de identidad a esta población. Incluso, hoy en día se ha visto una tendencia durante los últimos años a la fabricación de documentos de identidad para menores de edad.

Con la aparición de las nuevas tecnologías, la identidad ha pasado de los pasaportes y libros de inscripción a bases de datos y nubes electrónicas, trayendo consigo la aparición de lo que se conoce como “identidad digital”.

La identidad digital es descrita como el conjunto de datos disponibles de forma electrónica, en un principio datos personales, incluyendo información bancaria y estadísticas, imágenes, noticias en las que aparecemos y redes sociales. Toda nuestra vida reposa en línea y muchas veces sin que nosotros lo hayamos decidido así.

Hoy, más que nunca, nuestras identidades corren peligro gracias a la aparición de la identidad digital. Las grandes plataformas del mundo digital conocen más de nosotros que nosotros mismos. Todos nuestros datos están dispersos en las redes sociales y toda nuestra información sensible puede quedar en las manos equivocadas con una sola filtración.

Por ello, el mundo busca asegurar la transferencia de datos, ha creado organismos y convenios internacionales que permiten proteger los datos personales estén donde estén, transferirlos de una forma segura, brindando un correcto nivel de seguridad mediante estándares internacionales.

Sin embargo, no todos los países lo han considerado una prioridad, dejando así sin protección a millones de personas. Por otro lado, la aparición de un virus que afectó a toda la humanidad y ha volcado aún más nuestras vidas, con ella, nuestras identidades al plano digital.

Los gobiernos han desarrollado sistemas de identidad digital, compatibles con aplicaciones que permitan el autodiagnóstico, la trazabilidad y la alerta temprana.

En el centro de América, tres países cuentan o han contado con este tipo de herramientas y son los protagonistas de este estudio en la búsqueda de sus identidades digitales, antes y durante la pandemia.

METODOLOGÍA

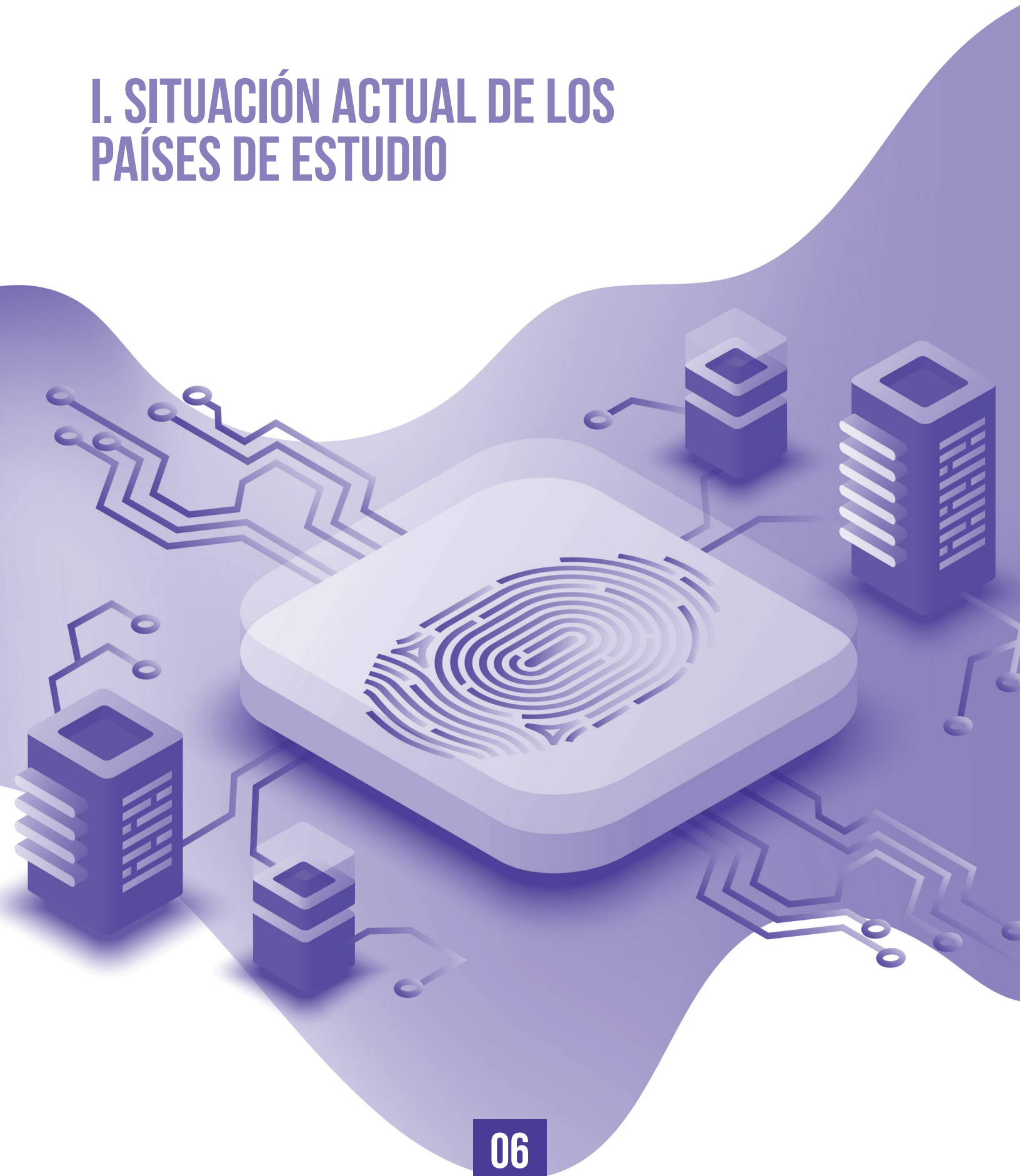
El objetivo de esta investigación es abordar de forma preliminar los aspectos legales e institucionales de los sistemas de identidad digital de tres países de Centroamérica: Costa Rica, Guatemala y Panamá, haciendo hincapié en su relación con el sector de la salud por motivos de la pandemia de COVID-19. Para ello, se ha empleado como punto de partida la serie de reportes realizados por **IPANDETEC** titulados "Estudios Centroamericanos de Protección de Datos" que fueron publicados en el 2019 y que permiten conocer mejor la realidad centroamericana sobre la legislación relativa a la privacidad y la protección de los datos personales.

Es preciso establecer comparaciones entre estos tres países para medir su nivel de desarrollo sobre la identidad digital, así como sus fortalezas y debilidades. Además de mapear su ecosistema institucional, hemos escogido una metodología analítico descriptiva.

Primero, se presentarán los tres países escogidos para este estudio y un pequeño resumen histórico de cada uno. Posteriormente, se analizará el marco legal siguiendo la Pirámide de Kelsen para comprender la situación en el país y las instituciones jurídicas que los rigen.

En el mejor de los casos, buscamos que en un futuro sea posible analizar el nivel de madurez de los Sistemas de Identidad Digital en Centroamérica para el cual vamos a emplear un instrumento desarrollado por el Centro para Internet y la Sociedad (CIS India) en su propuesta "The Appropriate Use of Digital Identity". Este instrumento permite, a través de un sistema de validación de tres factores, medir qué tan legítimo, seguro y respetuoso con los Derechos Humanos es un Sistema de Identidad Digital. Con ello, esperamos tener un primer vistazo de las fortalezas y debilidades de los sistemas estudiados y así poder hacer propuestas de mejora.

I. SITUACIÓN ACTUAL DE LOS PAÍSES DE ESTUDIO



COSTA RICA

Costa Rica es un país con un sistema de gobierno presidencialista, localizado en el centro de América Central, colindante con Panamá y Nicaragua. El país centroamericano cuenta con un poco más de 5 millones de personas en sus siete provincias. Durante décadas, ha sido reconocido como uno de los países más estables y progresistas de Latinoamérica, muestra de esto son sus altos niveles de desarrollo y competitividad.

El país ha vivido cambios constantes desde su independencia en 1821, pasando por la Guerra Civil de 1948. Este último suceso influyó grandemente en su desarrollo actual: se abolió el ejército, se nacionalizaron los bancos, se integró el ente electoral, se concedió el derecho a voto a la mujer y a la población afrocaribeña, además de promulgar su actual Constitución. La actual constitución política de Costa Rica fue creada en el año 1949, luego de que el presidente en ejercicio convocara a una Asamblea Nacional Constituyente. La aprobación y entrada en vigencia de dicha constitución tuvo lugar el día 7 de noviembre de ese año.

En el campo de los derechos humanos, Costa Rica es un referente regional y global. Su capital es hogar de la Corte Interamericana de Derechos Humanos, organismo contencioso del sistema interamericano de derechos humanos, además de múltiples organismos y organizaciones no gubernamentales; al mismo tiempo es el primer y único país de Centroamérica en permitir el matrimonio igualitario.

MARCO LEGAL

En cuanto a la privacidad y la protección de datos personales, Costa Rica es un pionero en la región. En su Constitución, reconoce el derecho a la privacidad y a la inviolabilidad de las comunicaciones, excepto mediante mandato judicial. Además, este mismo documento reconoce en el artículo 48 la acción de habeas corpus y la acción de amparo como mecanismos de protección de los derechos en general de las personas. Sin embargo, no se contempla el habeas data, quedando subsumido en las dos acciones mencionadas.

En el siguiente nivel legal, encontramos la Ley de Protección de la Persona frente al tratamiento de sus datos personales (Ley No. 8968) y su reglamento. Esta ley regula la protección de datos personales en Costa Rica, brinda derechos sobre los ciudadanos y su privacidad, procedimiento de transferencia de datos, crea una autoridad reguladora, además de estipular excepciones al consentimiento y tratamientos de los datos.

La Ley de Protección de Datos contiene tres excepciones a su aplicación: cuando las bases de datos sean para fines exclusivamente internos, personales o domésticos, siempre y cuando no sean vendidas o comercializadas de cualquier forma. Asimismo, en el artículo 8 se señala que las disposiciones de la ley se pueden limitar en seis supuestos por seguridad del Estado, seguridad y ejercicio de la autoridad pública, prevención, persecución, investigación, detención y represión de las infracciones penales o de las infracciones de la deontología en las profesiones para el funcionamiento de bases de datos que se utilicen con fines estadísticos, históricos o de investigación científica cuando no exista riesgo de que las personas sean identificadas para la adecuada prestación de servicios públicos y para la eficaz actividad ordinaria del Estado.

Respecto a datos personales de salud, esta ley contiene una norma sobre el consentimiento previo, irrefutable y expreso. Sin embargo, en el artículo 9, se señala que, aunque está prohibido el tratamiento de datos sensibles como son los de salud, estos sí pueden ser tratados cuando resulte necesario para la prevención o para el diagnóstico médico, la prestación de asistencia sanitaria o tratamientos médicos, o la gestión de servicios sanitarios.

Por otro lado, algunas otras normativas regulan conexamente los datos clínicos. La ley No. 8239 Derechos y deberes de las personas usuarias de los servicios de salud públicos y privados contempla en el artículo 2 que los pacientes y usuarios de servicios de salud tienen derecho a hacer que se respete el carácter confidencial de su historia clínica y de toda la información relativa a su enfermedad, salvo cuando por ley especial, deba darse noticia a las autoridades sanitarias. También, la Ley 9162 Expediente Digital Único de Salud, contempla en el artículo 11 que toda la información contenida se considera información privada que contiene datos sensibles y se prohíbe el tratamiento de dichos datos.

INSTITUCIONES

En Costa Rica, son varias las instituciones que tienen injerencia en la identidad digital y el tratamiento de los datos personales de los ciudadanos en el sector salud, desde antes y durante la pandemia. A continuación, brindamos un breve análisis de cada una de ellas.

La **Agencia de Protección de Datos de los Habitantes (PRODHAB)** es el ente rector de la protección de datos personales en Costa Rica. Dentro de sus funciones están: velar por el cumplimiento de la normativa de protección de datos, abrir investigaciones e imponer sanciones, educar sobre datos personales, entre otros[1].

El **Tribunal Supremo de Elecciones** es una entidad independiente que tiene entre sus funciones la administración electoral y el registro civil de los costarricenses. En esta institución se inscriben los nacimientos, adopciones, defunciones, entre otros eventos y actos civiles. Al cumplir la mayoría de edad, esta entidad emite un documento de identidad llamado cédula de identidad[2].

Este documento se le concede a todo nacional que cumpla los 18 años y es utilizado en diligencias judiciales, trámites bancarios, votaciones, por mencionar alguno de los actos. El documento contiene una fotografía de la persona, un número de identidad personal, su firma, además de otros datos personales del portador. En la parte posterior, se encuentra la huella dactilar del portador y un código de barra con diversa información personal. El TSE ha manifestado su intención de migrar a identificación con biometría y eliminar las cédulas de identidad.

El **Ministerio de Ciencia, Tecnología y Telecomunicaciones** es el rector de la ciencia y la tecnología en Costa Rica. A través del mismo, se adelantan diversas iniciativas de gobierno digital siguiendo la Estrategia de Transformación Digital 4.0[3].

(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/

El sector salud mantiene dos instituciones: el Ministerio de Salud[4] y la Caja Costarricense de Seguro Social (CCSS)[5]. El Ministerio de Salud es quien dicta la política pública de salud. La CCSS brinda servicios de salud, pensiones y prestaciones sociales a los costarricenses.

COVID 19

Durante la pandemia, las autoridades costarricenses presentaron una actualización a una herramienta existente. **EDUS** o **Expediente Digital Único en Salud** es una aplicación de la Caja Costarricense de Salud que puede ser descargada en las tiendas de aplicaciones de Android y iOS[6]. La aplicación permite a sus asegurados verificar sus datos personales, citas médicas pendientes y anteriores, así como, solicitar o cancelar sus citas y la de sus dependientes en el establecimiento de salud adscrito, validación de derechos, medicamentos prescritos, diagnósticos y alergias.

En su actualización 4.1.0 incluyeron la posibilidad de registro de síntomas para el cálculo de riesgo por coronavirus y recomendaciones a seguir por el usuario posterior al resultado.

En las políticas de privacidad de la aplicación publicadas en el sitio web de la institución afirman recabar y tratar los datos personales según lo dictado por la Ley de Protección de la Persona frente al tratamiento de sus datos personales.

Esta política explica que, al acceder a esta aplicación, automáticamente se recaban ciertos datos como dirección IP, características del dispositivo, sistema operativo, preferencias de idioma, URL de referencia, nombre del dispositivo, país, ubicación, información sobre cómo y cuándo utiliza nuestras aplicaciones y otra información técnica. Comparten la información con terceros cuando haya consentimiento, base legal o interés vital.

(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/detailsid=com.ccss.expedienteunico&hl=en_US&gl=US

Sin embargo, la política de privacidad no estipula claramente el tiempo máximo de almacenamiento. La misma menciona que se mantendrá la información en sus sistemas el tiempo exigido por ley, para posteriormente eliminarse o anonimizarse.

Finalmente, la política aclara al usuario que, si en algún momento cree que se está haciendo uso ilegal de sus datos puede ejercer sus derechos de revisar, cambiar o cancelar su cuenta en cualquier momento. También tiene derecho a presentar una queja ante su autoridad local de protección de datos personales.

I. SITUACIÓN ACTUAL DE LOS PAÍSES DE ESTUDIO

GUATEMALA

Guatemala es una república presidencialista fundada en 1821 con más de 14 millones de personas en sus 22 departamentos. Mantiene fronteras con Honduras, México y El Salvador.

A diferencia de otros países de la región, tuvo una guerra civil durante décadas, lo que ha provocado que sus niveles de pobreza y desigualdad de ingresos sean altos. Prueba de esto es que el 59.3 % del país se encuentra en pobreza, registrando un incremento del 8.1% desde la última medición[7]. A pesar de esto, su economía es la primera de Centroamérica.

En el plano de los derechos humanos, el país mantiene y presenta desafíos estructurales en materia de acceso a la justicia e impunidad, seguridad ciudadana, marginación y discriminación que han afectado en forma severa los derechos humanos de sus habitantes[8].

(7) Encuesta de Condiciones de Vida (Encovi 2014). Sitio web: https://www.ine.gob.gt/estadisticasine/index.php/usuario/encovi
(8) Pueblos indigenas: diversidad, desigualdad y exclusión en Guatemala. Sitio web:https://www.oas.org/es/cidh/multimedia/2016/guatemala/guatemala.html

MARCO LEGAL

La constitución de Guatemala reconoce en el artículo 24 el secreto de las comunicaciones y en el artículo 31 se reconoce el derecho a la autodeterminación informativa. Este mismo documento reconoce la acción de amparo como mecanismo de protección de los derechos en general de las personas, y la acción de habeas data se contempla en el artículo 30 del Decreto 57-2008 Ley de Acceso a la Información Pública como un recurso administrativo y no como una garantía constitucional.

A diferencia de otros países de la región, Guatemala es una de las naciones centroamericanas que no cuenta con una ley de protección de datos personales. Sin embargo, respecto del Estado, existen ciertos derechos sobre el tratamiento de datos incluidos en el Decreto 57-2008 Ley de Acceso a la Información Pública.

Referente a datos personales del sector salud, el Decreto 27-2000 Ley General para el Combate del Virus de Inmunodeficiencia Humana VIH y del Síndrome de Inmunodeficiencia Adquirida SIDA y de la Promoción, Protección y Defensa de los Derechos Humanos ante el VIH-SIDA contempla en el artículo 38 el derecho de los pacientes a la confidencialidad. En ese sentido, se establece la prohibición de hacer referencia a la enfermedad del paciente sin previo consentimiento.

También, el Código Deontológico de los profesionales médicos contempla, en su artículo 47, que el médico no debe publicar por ningún medio escrito, digital o de cualquier otra índole, fotografías, estudios diagnósticos, nombres o cualquier otro indicio que identifique a sus pacientes.

INSTITUCIONES

En Guatemala, son varias las instituciones que tienen injerencia en la identidad digital y tratamiento de los datos personales de los ciudadanos en el sector salud durante la pandemia. A continuación, brindamos un breve análisis de cada una de ellas.

El **Registro Nacional de Personas** es la entidad pública guatemalteca encargada del registro único de ciudadanos, inscripción de actos, además de ser el encargado de la emisión del Documento Personal de Identificación[9].

Este documento ha sido objeto de evolución desde su creación a los inicios de la República, conocido como cédula de vecindad. Actualmente, el documento cuenta con el código único de identificación, nombre, género, nacionalidad, fecha de nacimiento y de emisión, foto y firma del portador.

Además, cuenta con un chip interno que guarda los rasgos faciales del portador, sus huellas y su firma. El documento es utilizado en actos civiles, administrativos y legales en los que se solicite.

Ministerio de Salud Pública y Asistencia Social: institución rectora de la salud en Guatemala. El ministerio cuenta con hospitales públicos, centros de salud, farmacias, entre otros centros de servicio a nivel nacional[10].

El **Instituto Guatemalteco de Seguridad Social** ofrece atención médica y pensiones por diversas razones como lo es la maternidad, vejez, invalidez y muerte[11].

(9) Registro Nacional de las Personas. Sitio web: https://www.renap.gob.gt/(8) Pueblos indigenas: 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

Durante la pandemia, el gobierno de Guatemala presentó la aplicación Alerta Guate. Esta fue una aplicación desarrollada por In-telligent Properties LLC y utilizada por el gobierno de Guatemala para combatir la propagación del coronavirus en el país. Después de múltiples críticas de organismos internacionales de derechos humanos, preocupados por la protección de datos que brindaba la aplicación, fue removida de las tiendas para Android.

En un análisis posterior se pudo encontrar que la aplicación enviaba la ubicación exacta del usuario a su desarrollador, inclusive cuando la aplicación no estaba en uso. En su política de privacidad se detalló que el tiempo de almacenamiento de los datos recabados por la aplicación era de 10 años, sin mostrar una justificación.

I. SITUACIÓN ACTUAL DE LOS PAÍSES DE ESTUDIO

PANAMÁ

Panamá es una República presidencialista localizada al sureste de Centroamérica, frontera con Costa Rica y Colombia. El país de poco más de 4 millones, según las últimas estimaciones, cuenta con 10 provincias y 5 comarcas indígenas.

La nación se independizó de España en 1821, sin embargo, a diferencia de sus vecinos centroamericanos, se unió voluntariamente a Colombia. No es hasta 1903 que finaliza esta unión e inicia la construcción del Canal de Panamá, inaugurado en 1914. Esta obra fue administrada junto a los terrenos colindantes, durante décadas, por militares estadounidenses.

Desde finales de los 60 hasta los 80, el país estuvo gobernado por militares quienes promulgaron la actual Constitución en 1972. En 1989, el país fue invadido por tropas norteamericanas con un consecuente retorno de la democracia. Desde entonces, el país ha sufrido cambios vertiginosos, especialmente en su economía.

En el área económica, su principal sector es el de servicios, siendo notable su sector bancario internacional, gran movimiento logístico impulsado por el Canal de Panamá, además de contar con uno de los aeropuertos con mayor tráfico en la región.

MARCO LEGAL

En la Constitución de Panamá se reconoce el derecho al secreto de las comunicaciones en el artículo 29, y en el artículo 42 se reconoce el derecho a la autodeterminación informativa. Este mismo documento reconoce la acción de hábeas data como un mecanismo de protección de los datos personales.

En el siguiente nivel, podemos encontrar la Ley 81 Sobre Protección de Datos Personales que regula el régimen de tratamiento de datos en Panamá. Sin embargo, esta norma todavía entrará en vigencia en 2021. La norma contempla los derechos del titular, los deberes al tratar los datos, sanciones y las facultades que se le conceden al ente rector.

Esta misma ley contempla, en el artículo 3, cinco excepciones a su aplicación: para fines domésticos, los que realizan autoridades competentes para la persecución de delitos, para el análisis de inteligencia financiera y seguridad nacional, en cumplimiento de tratados internacionales, y los datos obtenidos mediante procedimientos de anonimización.

Así mismo, en el artículo 8, se incluyen nueve excepciones al consentimiento: cuando los datos son de dominio o fuente pública se recolectan en el ejercicio de las funciones del Estado, son datos económicos o financieros y media consentimiento, se ubican en listas de ciertas categorías de personas en la forma de antecedentes, los necesarios para las relaciones comerciales; los realizan organizaciones privadas para uso exclusivo de sus asociados con fines estadísticos u otros beneficios, en casos de urgencia médica o sanitaria, cuando la ley lo ordena con fines históricos, estadísticos o científicos y cuando sea necesario para lograr intereses legítimos.

Respecto a datos personales del sector salud, la ley reviste de un carácter especial a estos datos: datos sensibles. El artículo 8 de la ley indica que, en el caso de datos sensibles de salud, el consentimiento debe ser previo, irrefutable y expreso.

Sin embargo, la Ley de Protección de Datos Personales de Panamá no regula todos los datos personales en el país.

Por ejemplo, la Ley 26 Por la cual se dictan medidas de profilaxis y control de la epidemia del síndrome de inmunodeficiencia adquirida (SIDA) y de la propagación del virus de la inmunodeficiencia humana (VIH) contempla en el artículo 12 que los integrantes del equipo de salud que conozcan o atiendan a una persona enferma, deben guardar confidencialidad sobre esta información. También la Ley 68 que regula los derechos y obligaciones de los pacientes, en materia de información de decisión libre e informada, contempla en el artículo 13 que toda persona tiene derecho a que se mantenga confidencialidad sobre sus datos de salud, lo que incluye que nadie pueda acceder a ellos sin su autorización.

INSTITUCIONES

En Panamá, son varias las instituciones que tienen injerencia en la identidad digital y tratamiento de los datos personales de los ciudadanos en el sector salud durante la pandemia. A continuación, brindamos un breve análisis de cada una de ellas.

Primeramente, el recurso de hábeas data es resuelto por los tribunales de justicia en sus diferentes niveles. Esto dependerá del mando y jurisdicción que tenga el funcionario o responsable de la base de datos, en caso de que sea responsable a nivel nacional, el recurso debe ser resuelto por el pleno de la Corte Suprema de Justicia, mientras que, si el responsable tiene mando provincial o municipal, lo debe atender un Tribunal Superior.

Por otro lado, el **Tribunal Electoral de Panamá**, mediante su Dirección Nacional de Registro Civil es el ente gubernamental encargado de inscripciones y certificaciones de los hechos vitales y actos jurídicos, tales como: nacimientos, fallecimientos, matrimonios, divorcios, entre otros. Esta institución otorga un documento conocido como cédula de identidad personal que confirma la ciudadanía del portador[12].

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

Este documento, creado en 1916, le permite al panameño confirmar su identidad y realizar cualquier acto legal, incluyendo emitir su voto en las elecciones populares del país. Desde el año 1958, se incluyó la toma de huellas dactilares del portador y se establecieron multas pecuniarias a quien no tramitase su cédula 3 meses después de cumplir la mayoría de edad.

El documento actualmente cuenta con el nombre legal y el de uso del portador, su número de identidad según su lugar de nacimiento, sexo, fecha de nacimiento, lugar de nacimiento, firma y fotografía del portador del portador, la fecha de expedición y expiración del documento.

El ente regulador de los datos personales en el país es la **Autoridad Nacional de Transparencia y Acceso a la Información** (ANTAI)[13]. Esta facultad le fue conferida a la existente autoridad mediante la ley de protección de datos personales. Esto le permite iniciar investigaciones e imponer sanciones.

En el campo de la innovación se encuentra la **Autoridad para la Innovación Gubernamental (AIG)**, entidad encargada de planificar, coordinar, supervisar y promover el uso de las tecnologías de la información y comunicación en el gobierno mediante la modernización del sector público[14].

Respecto al sistema de salud, existen dos instituciones rectoras en la materia. Está el **Ministerio de Salud**[15], cuya misión es garantizar a toda la población el acceso a la atención integral, mientras que la **Caja de Seguro Social**[16] mantiene una dualidad de funciones al proveer servicios de salud y prestaciones económicas, incluyendo pensiones.

COVID 19

Durante la pandemia, el gobierno de Panamá ha recurrido a la tecnología como mejor aliada para luchar contra la situación. Se han desarrollado aplicaciones, bots, páginas webs, entre otras herramientas digitales para minimizar la circulación y el mantenimiento de las medidas de cuarentena en materia de salud, educación, seguridad social, por mencionar algunos.

(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/

La aplicación Protégete Panamá, una aplicación para iOs y Android, permite a los pacientes positivos de coronavirus mantener una comunicación directa con instituciones de salud. Este aplicativo está basado en tecnología de código abierto como GNU/Linux, OpenShift y React[17].

Cuando un paciente es diagnosticado como positivo, el personal de salud le solicitará que cree un perfil en la plataforma. El paciente podrá registrarse y acceder mediante reconocimiento facial, aunque no se especifica si esto es opcional. El paciente debe reportar diariamente sus síntomas al equipo médico.

Protégete es la única tecnología desarrollada en conjunto con la AIG que utiliza sistema de rastreo geográfico, el cual puede ser desactivado en cualquier momento por el usuario. Los datos de ubicación geográfica no son correlacionados con ningún otro usuario y los datos solamente son utilizados para crear estadísticas de incidencia según sector.

El sitio web de la AIG mantiene una declaración de privacidad donde especifica su política de trabajo. Sin embargo, esta política de privacidad solamente se enmarca dentro de los sitios web gubernamentales, sin incluir las aplicaciones o desarrollos de cada institución ni mucho menos contempla la normativa panameña en materia de datos médicos.

Hasta el momento, la institución no ha publicado manuales de procedimiento de los aplicativos, aunque afirma, se encuentran en confección. En respuesta a una solicitud de acceso a la información pública, se detalla que en la actualidad se utilizan **"certificados digitales y altos estándares de seguridad",** sin ofrecer mayores detalles.

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

II. ANÁLISIS DE LOS PAÍSES DE ESTUDIO

ANÁLISIS COMPARATIVO

Nuestra investigación se ha enfocado en los tres países arriba mencionados: Costa Rica, Guatemala, y Panamá por diversas razones que nos parece necesarias explicar.

Primero, los tres países mantienen un marco legal que, a simple vista, parece idéntico, sin embargo, al realizar un análisis legal integral podemos ver que entre ellos mantienen sendas diferencias que visualizan lo diferente que pueden ser las sociedades del centro de América.

Segundo, los tres países han confiado en la tecnología y han hecho uso de ella, en diferentes formas y con diferentes resultados, inclusive con un abordaje de los derechos humanos muy diferente entre sí.

Por último, sus sistemas de salud, en busca de perfeccionar sus servicios durante la pandemia, han desarrollado junto a otros sectores, herramientas digitales para contrarrestar los efectos de la situación de emergencia mundial sin contar en ocasiones con la opinión de los usuarios.

Aclaramos que los datos y descubrimientos que resulten de este estudio no son determinantes de una superioridad en las políticas públicas entre una nación u otra; si no, nos podrá poner de manifiesto qué prácticas o qué situaciones parecen más deseables que otras, exclusivamente, respecto de la identidad digital con énfasis en los esquemas de salud.

COMPARANDO REALIDADES

Las Constituciones de los tres países analizados reconocen la privacidad directa o indirectamente como un derecho. En el caso expreso de Costa Rica, se habla sobre la intimidad y la inviolabilidad de las comunicaciones, en el caso de Panamá y Guatemala, se menciona la inviolabilidad de comunicaciones.

De los tres países analizados, solamente dos cuentan con leyes de protección de datos personales. De estos dos países, solo uno mantiene su ley vigente al momento de realizar este estudio.

La Ley de Protección de Datos Personales de Costa Rica data del año 2011, mientras que la de Panamá es del año 2019; por esta razón podemos observar en un principio que la ley panameña es más actualizada que la costarricense, obedeciendo a la digitalización que ha sucedido durante los últimos años. De igual forma, la ley panameña introduce el derecho de portabilidad de los datos personales, mientras que deja algunas facultades del estándar europeo de protección de datos personales por fuera como la extraterritorialidad y obvia crear una entidad rectora, más bien, le da la facultad a una institución ya existente, lo cual es una de sus grandes diferencias con la ley costarricense que creó la Agencia para la Protección de Datos de los Habitantes (PRODHAB).

Guatemala, a pesar de no tener una ley de protección de datos personales, su ley de acceso a la información actualmente es el único documento legal que regula lo referente a los datos personales y datos sensibles, así como establece un mecanismo de protección de estos y tipifica delitos en la materia.

Solo Panamá mantiene el recurso de habeas data a nivel constitucional. Guatemala lo regula mediante una ley, mientras que Costa Rica todavía no incluye este recurso en su ordenamiento.

La privacidad de los datos del sector salud están regulados en los tres países en normas conexas. Por ejemplo, la ley en la que se dictan medidas de profilaxis y control de la epidemia del síndrome de inmunodeficiencia adquirida (SIDA) en Panamá contempla que los integrantes del equipo de salud que conozcan o atiendan a una persona enferma, deben guardar confidencialidad sobre esta información. También la ley que regula los derechos y obligaciones de los pacientes en materia de información de decisión libre e informada, contempla que, toda persona tiene derecho a que se mantenga confidencialidad sobre sus datos de salud.

Esta misma situación se da en normas parecidas en Costa Rica y Guatemala. En el caso de Costa Rica, la Ley sobre Derechos y Deberes de las personas usuarias de los servicios de salud contempla que los pacientes y usuarios de servicios de salud tienen derecho a hacer que se respete el carácter confidencial de su historia clínica y de toda la información relativa a su enfermedad. También, la Ley que regula el Expediente Digital Único de Salud contempla que, toda información contenida en el expediente digital se considera información privada que contiene datos sensibles y se prohíbe el tratamiento de dichos datos.

TEST SOBRE SISTEMAS DE IDENTIDAD DIGITAL. COSTA RICA.

Este test ha sido diseñado tomando como referencia el test sobre Sistema de Identidad Digital elaborado por el Centro para Internet y la Sociedad (CIS India) con ligeros cambios y adiciones que complementen las necesidades y particularidades centroamericanas pandémicas.

El test consiste en tres etapas diferentes: legalidad, derechos humanos, y riesgo. Cada una de las etapas con un número de preguntas con su contestación.

A. LEGALIDAD

1. ¿Es el uso de sistemas de identidad digital regulado por una ley vigente?

Sí, en la legislación costarricense existen diversas disposiciones que dejan entrever una legalización de los sistemas de identidad digital.

Por ejemplo, la ley de protección de datos personales regula todos aquellos datos tratados o recabados que figuren en bases de datos automatizadas o manuales.

Otro perfecto ejemplo son las regulaciones sanitarias. La Ley que crea el Expediente Digital Único de Salud, asegurando una identificación única, congruente con la confidencialidad y veracidad que debe regir el proceso de atención médica.

2. ¿Tiene la ley un objetivo legítimo?

Sí, estas leyes persiguen los derechos de privacidad y protección de datos personales, además de asegurar el acceso a la salud.

3. ¿Define la ley claramente los propósitos que justifican el uso de la identidad digital?

Nuestro equipo de investigación no reconoce con claridad los propósitos que justifiquen el uso de la identidad digital en ninguno de los documentos legales antes mencionados. Creemos que esto puede ser por la falta deliberada de una normativa que mencione expresamente la identidad digital.

Sin embargo, por los documentos legales mencionados anteriormente, podemos suponer que las justificaciones son diversas cómo: brindar un servicio especializado de salud, identificación unívoca de pacientes y usuarios de los servicios de salud, a efectos de que su expediente digital único de salud sea conocido e incluya solo la información del paciente que corresponda.

4. ¿La ley explica de forma clara y detallada quienes son los actores que pueden tener acceso a la base de datos de los sistemas de identidad digital?

No. La ley de datos personales habla de organismos privados y públicos que mantengan bases de datos, sin embargo, no aclara si esto incluye la identidad digital y el acceso a la información.

Por otro lado, la ley que regula el expediente digital es de la Caja Costarricense del Seguro Social, con el apoyo y los servicios del Tribunal Supremo de Elecciones y de la Dirección General de Migración y Extranjería. No menciona expresamente si estos datos podrán ser accedidos por otro sector diferente a los mencionados.

5. ¿La ley regula el uso de la base de datos de los sistemas de identidad digital por actores privados?

No, como en la respuesta anterior, no se mencionan explícitamente las bases de datos de los sistemas de identidad digital, sin embargo, las diferentes regulaciones y directrices estudiadas incluyen actores privados.

6. ¿La ley detalla claramente los datos que pueden ser almacenados?

No, la Ley de Expediente Clínico Digital y la Ley de Protección de Datos Personales no mencionan qué datos pueden ser almacenados. Sin embargo, la aplicación portatil EDUS maneja en un principio, sin limitarse a:

- **Tipo de identificación, identificación**
- **Nombre y apellidos**
- **Sexo**
- **Fecha de nacimiento**
- **Edad**
- **Dirección exacta**
- **Cantidad de personas que viven con él**
- **Usuario y correo electrónico**
- **Información del test de riesgo**
- **Condiciones y antecedentes**

7. ¿El sistema de identidad digital proporciona una notificación adecuada al usuario?

No, ninguno de los sistemas analizados incluye una notificación al usuario.

8. ¿Tienen las personas, derechos de acceso, rectificación, cancelación y oposición?

Sí, la ley de protección de datos personales y otras directrices conceden los derechos de:

A. Acceso: a través del ejercicio de este derecho, el titular de los datos personales puede verificar si existen datos personales suyos en una base de datos, qué datos de carácter personal están siendo tratados por parte de terceros, la finalidad de ese tratamiento, el origen de los citados datos, la forma en la cual se almacenan y si se han transferido o se van transferir a un tercero.

B. Rectificación: es la posibilidad del titular de los datos personales de modificar aquellos datos que sean inexactos o incompletos, debiendo en la solicitud de rectificación, indicar qué datos desea que se modifiquen.

C. Cancelación: toda persona puede solicitar y obtener del responsable del manejo de los datos personales la eliminación de su información privada, en cualquier momento y circunstancia. Dentro de este derecho se incluye el derecho al olvido, el cual consiste en la obligación que tiene todo responsable de una base de datos personales de suprimir aquellos que le puedan afectar a su titular por un plazo máximo de 10 años. Lo anterior implica que este tipo de datos debe ser eliminada por su almacenador, aún no medie solicitud del titular de estos.

D. Oposición: aunque no está expresamente incorporado como tal, se entiende como un derivado del derecho de autodeterminación informativa que se garantiza como un derecho fundamental, con el objeto de controlar el flujo de informaciones que conciernen a cada persona en los términos del artículo 4 de la Ley de Datos Personales.

9. ¿Existen mecanismos que brinden una reparación civil y penal resultado de violaciones a sistemas de identidad digital?

No específicamente, sin embargo, diversas directrices penales y civiles brindan reparaciones en estos casos.

Las multas que estipula la ley de protección de datos son destinadas a la actualización de equipos y programas de la Prodhab.

B. DERECHOS HUMANOS

1. ¿Se siguen los principios de minimización de datos en el recopilación, uso y retención de datos personales para este caso de uso?

Sí, la ley de protección de datos personales y regulaciones del sector salud incluyen principios, específicamente los de actualidad, veracidad, exactitud y adecuación.

2. ¿La ley especifica el tipo de acceso que los diversos actores tienen sobre los datos personales?

No, hay un vacío legal en este aspecto, ya que no existe en la norma una explicación explícita sobre el tipo de acceso que tienen los diversos actores.

3. ¿El uso obligatorio de la identidad digital para acceder a servicios es excluyente?

Explícitamente, no existe una obligatoriedad en el uso de la identidad digital para acceder a los servicios de salud en Costa Rica. Sin embargo, la utilización del EDUS se da en todos los centros de la Caja Costarricense de Seguro Social por lo que, para una mejor atención, debe utilizarse el sistema.

C. RIESGO

1. ¿Los sistemas de identificación están creados, teniendo en cuenta riesgos potenciales?

Sí. La transferencia de datos del EDUS está protegida con el protocolo HTTPS.

TEST SOBRE SISTEMAS DE IDENTIDAD DIGITAL.
GUATEMALA.

A. LEGALIDAD

1. ¿Es el uso de sistemas de identidad digital regulado por una ley vigente?

No, en Guatemala, al no existir una ley de datos personales, no existe una regulación de identidad digital. Sin embargo, cabe recalcar que la actual ley de acceso a la información pública menciona los datos personales y sensibles, pero no puede ser utilizado como un regulador de los sistemas de identidad digital.

2. ¿Tiene la ley un objetivo legítimo?

La respuesta a esta pregunta puede ser compleja. Actualmente, no existe una ley que regule la identidad digital en Guatemala, por lo que no puede considerarse que tenga un objetivo legítimo. Sin embargo, la ley de acceso a la información pública regula el habeas data, incluyendo artículos y disposiciones para el tratamiento y el acceso a los datos personales.

3. ¿Define la ley claramente los propósitos que justifican el uso de la identidad digital?

No existe una ley que regule la identidad digital en Guatemala, por lo que no puede considerarse respuesta a esta interrogante. Sin embargo, la ley de acceso a la información pública regula la información personal contenida por los sujetos obligados.

4. ¿La ley explica de forma clara y detallada quienes son los actores que pueden tener acceso a la base de datos de los sistemas de identidad digital?

No existe una ley que regule la identidad digital en Guatemala, por lo que no puede considerarse respuesta a esta interrogante. Sin embargo, la ley de acceso a la información pública menciona un listado enunciativo y no limitativo de sujetos obligados, entre ellos, entidades públicas, organizaciones sin fines de lucro, empresas privadas, entre otros.

5. ¿La ley regula el uso de la base de datos de los sistemas de identidad digital por actores privados?

No existe una ley que regule la identidad digital en Guatemala, por lo que no puede considerarse respuesta a esta interrogante. Sin embargo, actualmente se les aplica la ley de acceso a la información pública por ser uno de los sujetos obligados por esta ley.

6. ¿La ley detalla claramente los datos que pueden ser almacenados?

No existe una ley que regule la identidad digital en Guatemala, por lo que no puede considerarse respuesta a esta interrogante. Sin embargo, la ley de acceso a la información pública describe datos personales como cualquier información concerniente a personas naturales identificadas o identificables.

Por otro lado, los datos personales sensibles incluyen **"todas las características físicas o morales de las personas, a hechos o circunstancias de su vida privada o actividad, tales como: los hábitos personales, de origen racial, el origen étnico, las ideologías y opiniones políticas, las creencias o convicciones religiosas, los estados de salud físicos o psíquicos, preferencia o vida sexual, situación moral y familiar u otras cuestiones íntimas de similar naturaleza".**

7. ¿El sistema de identidad digital proporciona una notificación adecuada al usuario?

No, ninguno de los sistemas analizados incluye una notificación al usuario.

8. ¿Tienen las personas, derechos de acceso, rectificación, cancelación y oposición?

No existe una ley que regule la identidad digital en Guatemala, por lo que no puede considerarse respuesta a esta interrogante. Sin embargo, la ley de acceso a la información pública establece el recurso de habeas data, el cual salvaguarda el derecho de acceso y rectificación.

9. ¿Existen mecanismos que brinden una reparación civil y penal resultado de violaciones a sistemas de identidad digital?

No existe una ley que regule la identidad digital en Guatemala, por lo que no puede considerarse respuesta a esta interrogante. Sin embargo, vale añadir que la ley de acceso a la información contempla diversos recursos en el área administrativa, además de permitir sanciones penales, las cuales se aplicarán sin perjuicio de las responsabilidades civiles correspondientes y los daños que se pudieran generar por la comercialización o distribución de datos personales, datos sensibles o personales sensibles.

B. DERECHOS HUMANOS

1. ¿Se siguen los principios de minimización de datos en el recopilación, uso y retención de datos personales para este caso de uso?

Al no existir una normativa de datos personales en Guatemala, consideramos que no se siguen estos principios.

2. ¿La ley especifica el tipo de acceso que los diversos actores tienen sobre los datos personales?

Actualmente, no existe una legislación que proteja los datos personales en Guatemala. Sin embargo, la ley de acceso a la información menciona diversos actores o sujetos obligados, que pueden recabar información personal, sin especificar si estos pueden ingresar a la base de datos a su solicitud.

3. ¿El uso obligatorio de la identidad digital para acceder a servicios es excluyente?

Explícitamente, no existe una obligatoriedad en el uso de la identidad digital para acceder a servicios en Guatemala.

C. RIESGO

1. ¿Los sistemas de identificación están creados, teniendo en cuenta riesgos potenciales?

El equipo investigador de este estudio no encontró sistemas de seguridad que protejan los riesgos potenciales a los que pueden ser sometidos los sistemas de identificación.

TEST SOBRE SISTEMAS DE IDENTIDAD DIGITAL.
PANAMÁ.

A. LEGALIDAD

1. ¿Es el uso de sistemas de identidad digital regulado por una ley vigente?

No de forma expresa, al no mencionarse en ninguna ley, los sistemas de identidad digital. Sin embargo, la ley de protección de datos personales podría considerarse el documento que los regula al tratar datos personales.

2. ¿Tiene la ley un objetivo legítimo?

Sí, estas leyes persiguen los derechos de privacidad y protección de datos personales, además de asegurar el acceso a la salud.

3. ¿Define la ley claramente los propósitos que justifican el uso de la identidad digital?

Nuestro equipo de investigación no reconoce con claridad los propósitos que justifiquen el uso de la identidad digital en ninguno de los documentos legales antes mencionados. Creemos que esto puede ser por la falta deliberada de una normativa que mencione expresamente la identidad digital.

Sin embargo, por los documentos legales mencionados anteriormente, podemos suponer que las justificaciones son diversas cómo: evitar el cambio de neonatos por error humano o como resultado de actividades delictivas mediante el uso de biometría, atención de embarazadas sin documentos de identidad personal, identificación de occisos e identificación del paciente.

4. ¿La ley explica de forma clara y detallada quienes son los actores que pueden tener acceso a la base de datos de los sistemas de identidad digital?

La ley de protección de datos personales habla de **"personas que tengan acceso o tratamiento de datos personales, en organismos públicos o privados."** De forma parecida, se menciona en las directrices sanitarias al personal de salud o doctores del sector público y privado.

Sin embargo, cabe destacar que, durante la pandemia, los actores se han visto extendidos. Diversos organismos públicos tienen acceso a los datos personales sensibles. **La Fuerza de Tarea Conjunta que incluye un equipo de médicos del MINSA apostados en el Centro de Operaciones de Emergencia (COE) del Sistema Nacional de Protección Civil (SINAPROC)**.

El COE está conformado por la Gobernación de la provincia, Ministerio de Salud, CSS, Policía Nacional, Sistema Nacional de Protección Civil (Sinaproc), Ministerio de Desarrollo Social y líderes comunitarios, y es activado durante emergencias. La Autoridad para la Innovación Gubernamental (AIG) también cuenta con acceso.

5. ¿La ley regula el uso de la base de datos de los sistemas de identidad digital por actores privados?

No, como en la respuesta anterior no se menciona explícitamente las bases de datos de los sistemas de identidad digital, sin embargo, las diferentes regulaciones y directrices estudiadas incluyen actores privados.

6. ¿La ley detalla claramente los datos que pueden ser almacenados?

Sí. La Ley que regula los derechos de los pacientes menciona que los expedientes clínicos deben contener ciertos datos, entre ellos:

- **Nombre y apellidos del paciente**
- **Fecha de nacimiento**
- **Sexo**
- **Cédula de identidad personal**
- **Dirección de domicilio y teléfono**
- **Antecedentes familiares y personales, fisiológicos y patológicos**
- **Historial clínico**

7. ¿El sistema de identidad digital proporciona una notificación adecuada al usuario?

No, ninguno de los sistemas analizados incluye una notificación al usuario.

8. ¿Tienen las personas, derechos de acceso, rectificación, cancelación y oposición?

Sí, la ley de protección de datos personales y otras directrices conceden los derechos de:

Acceso: tener acceso a los datos que se tienen del titular.

Rectificación: corregir datos que estén incorrectos o hayan caducado.

Cancelación: eliminar datos que no deban ser recolectados y tratados, o aquellos que hayan sido recolectados sin consentimiento o no sean proporcionales.

Oposición: negarse al tratamiento de datos personales.

9. ¿Existen mecanismos que brinden una reparación civil y penal resultado de violaciones a sistemas de identidad digital?

Sí, diversas directrices sanitarias o de ciberseguridad brindan reparación por la vía penal o civil. Igualmente, la ley de protección de datos personales estipula multas, cuyo monto y pago deberán ser cancelados ante la autoridad reguladora y los fondos pueden ser destinados a educación sobre datos personales.

B. DERECHOS HUMANOS

1. Sí, la ley de protección de datos personales y regulaciones del sector salud incluyen principios, específicamente los de actualidad, veracidad, exactitud y adecuación.

Sí, la ley de protección de datos personales y regulaciones del sector salud incluyen principios que buscan minimizar el uso, recopilación, y retención de datos, brindando una protección al titular de los datos.

2. ¿La ley especifica el tipo de acceso que los diversos actores tienen sobre los datos personales?

Sí, la Ley de Protección de Datos Personales junto a las leyes de datos médicos, crediticios y bancarios especifican el tipo de acceso que debe tener cada sector.

2. ¿La ley especifica el tipo de acceso que los diversos actores tienen sobre los datos personales?

Explícitamente, no existe una obligatoriedad en el uso de la identidad digital para acceder a los servicios de salud en Panamá.

Sin embargo, los panameños, residentes y extranjeros que visiten Panamá durante la pandemia, sí cuentan con la obligación de descargar la aplicación Protégete con Salud para un monitoreo de síntomas durante los primeros 15 días al regresar al país, al igual que los pacientes positivos de COVID-19.

C. RIESGO

1. ¿Los sistemas de identificación están creados, teniendo en cuenta riesgos potenciales?

El equipo investigador de este estudio no encontró sistemas de seguridad que protejan los riesgos potenciales a los que pueden ser sometidos los sistemas de identificación.

CONCLUSIÓN Y RECOMENDACIONES

La investigación que contiene este estudio arroja interesantes resultados de la situación, progreso, y urgentes necesidades de la identidad digital en tres países de la región centroamericana. A pesar de que solamente se examinan tres estados, estos pueden reflejar una situación que se replica en toda la región. Aunque este estudio solamente analiza solamente tecnologías desarrolladas para combatir la pandemia, especificamente aplicaciones moviles, nuestras recomendaciones y conclusiones aplican para otras situaciones que no sean la actual o de emergencia.

Los estados de Centroamerica deben actualizar sus políticas públicas a las necesidades actuales que supone la aparición del internet y una mayor utilización de tecnologías y personas conectadas en esta región. El no hacerlo supone diversos problemas, no solamente puede afectar los derechos de los ciudadanos, sino el atractivo economico y de inversión extranjera al ser estados sin seguridad juridica en materia de tecnologías de la información y comunicación.

Dentro de los urgentes cambios en políticas públicas está la necesidad de impulsar proyectos de ley que protejan los datos personales y la ciudadanía digital de los centroamericanos. Actualmente, el Reglamento General de Datos Personales de la Unión Europea es aplicado a los ciudadanos europeos en cualquier parte del mundo, lo que puede ser un punto de inicio para los gobiernos centroamericanos, adaptando este mecanismo internacional a sus necesidades nacionales. Cualquier política pública debe ser ampliamente discutida a través de consultas multisectoriales que incluyan la academia, el sector técnico y la sociedad civil.

Es necesario discutir la creación de entidades especializadas en protección de datos personales en los países que no existan, dotarlas de autonomía, personal calificado y experto en la materia, con facultades coercitivas y un presupuesto independiente que permitan el ejercicio de sus funciones. Al asignar facultades tan complejas como lo es la protección de datos a una institución existente, puede crearse problematicas en el flujo de trabajo que afecten directamente al ciudadano.

Otro punto que debe incluirse en cualquier propuesta son los derechos de Acceso, Rectificación, Cancelación, y Oposición (ARCO), además de discutir el derecho de portabilidad. El marco europeo establece también el derecho al olvido, el cual ha sido polémico, por lo que nuestra recomendación es que sea largamente discutido por los diferentes sectores. Dentro de la discusión recomendamos incluir la extraterritorialidad que proteja al ciudadano centroamericano en cualquier territorio.

Una alternativa viable para la región es discutir estas políticas a nivel regional a través de los mecanismos que brindan diversos organismos regionales y globales: Sistema de Integración Centroamericano (SICA) y el Parlamento Centroamericano (PARLACEN), la Organización de Estados Americanos (OEA) y el Parlamento Latinoamericano (PARLATINO), o el sistema de Naciones Unidas (ONU).

Los sistemas de identidad digital administrados por el gobierno harían bien en ser auditados por la sociedad civil, permitiendo un mejor desarrollo de los mismos. Aquellos sistemas de identidad digital administrados por empresas del sector privado deben cumplir con los requerimientos que provea el sector estatal, además de revisiones por parte de sociedad civil.

Toda iniciativa tecnologíca instaurada durante la pandemia debe ser ampliamente discutida con los diversos sectores de la sociedad, además de contar con voces expertas y un profundo analisis de los beneficios y desventajas que suponen el desarrollo y aplicación de las mencionadas tecnologías. Por otra parte, organizaciones internacionales como la Organización Mundial de la Salud ha emitido informes y recomendaciones en este tema junto a expertos de sociedad civil de todos los continentes. También se puede examinar las experencias de otros estados o ciudades que hayan aplicado tecnologías parecidas en base a derechos humanos.

Los estados centroamericanos deben analizar la opción de adherirse a convenios internacionales que les permita adecuar sus políticas públicas al mismo nivel que otros bloques regionales, lo que permitirá una uniformidad en sus políticas de manejo de datos personales y sensibles, junto a una clara política de flujo de transfronterizo de datos. Por ejemplo, el Convenio No. 108 del Consejo de Europa instaura un mecanismo uniforme para todos los estados europeos que se adhieren al mismo.

Por otro lado, antes de desarrollar o implementar cualquier tecnología, es vital examinar la población y su comportamiento, su acceso a internet y la calidad del mismo, la cantidad de dispositivos que pueden acceder a la tecnología, el desarrollo de una estrategia de comunicación que impulse confianza en la población basada en datos. De igual forma, dentro de ese analisis debe examinarse la mejor opción para la economia personal de cada ciudadano, implicando que la utilización de la tecnología no sea una carga economica para los ciudadanos durante la actual situación de emergencia. Por ejemplo, dependiendo de la cantidad de personas en un país, se ha demostrado el porcentaje de ciudadanos que deben utilizar activamente la tecnología para su éxito, de lo contrario una debil y malograda implementación puede suponer el fracaso y pérdida de inversión en la implementacion de sistemas de identidad digital.

BIBLIOGRAFÍA

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-evalution

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.aspxparam1=NRTC&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.aspxnValor1=1&nValor2=75700&nValor3=93998

7. Constitución de la República de Guatemala (1993). Sitio web: https://www.ine.gob.gt/archivos/informacionpublica/ConstitucionPoliticadelaRepublicadeGuatemala.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