Estudio Centroamericano de Protección de Datos,

EL SALVADOR

José Edmundo Osorio Morales

Diagramación: Isabel Valladares
Edición: Raúl Altamar
Coordinación: Sara Fratti
Autoría: José Edmundo Osorio Morales

Enero 2019.

IPANDETEC
INSTITUTO PANAMEÑO DE DERECHO Y NUEVAS TECNOLOGÍAS

Instituto Panameño de Derecho y Nuevas Tecnologías -IPANDETEC- 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.

1. Marco jurídico constitucional

El marco legal y la jurisprudencia salvadoreña brindan importantes garantías para proteger el derecho a la privacidad digital y la protección de los datos personales, bajo la interpretación del segundo párrafo del Artículo 2 de la Constitución de la República[1], donde se señala:

Art. 2.-"Toda persona tiene derecho a la vida, a la integridad física y moral, a la libertad, a la seguridad, al trabajo, a la propiedad y posesión, y a ser protegida en la conservación y defensa de los mismos.

Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

Iniciando un proceso para activistas de derechos digitales, legisladores y aplicadores ley, se debe contar con instrumentos legales que garanticen la protección de la información personal y datos personales de miles de habitantes, y a la vez ejercer con mayor claridad los mecanismos como el hábeas data e autodeterminación informativa. Por tales efectos, la protección de datos personales se encontrará diseminada en una serie de normativas secundarias que toman en cuenta factores como los siguientes:

- Privacidad e intimidad personal en las tecnologías de la información y comunicaciones.
- Consentimiento en la transferencia de la información personal.
- Regulación de datos personales en base de datos y centros de distribución.
- Seguridad de la información personal.

En este sentido, en el artículo 24 del texto constitucional se determina el derecho a la intimidad de las comunicaciones.

Art. 24.- "La correspondencia de toda clase es inviolable. Interceptada no hará fe ni podrá figurar en ninguna actuación, salvo en los casos de concurso y quiebra. Se prohíbe la interferencia y la intervención de las comunicaciones telefónicas".

[1] Asamblea Constituyente. Constitución de la República de El Salvador, Decreto Legislativo N.° 38. Disponible en: https://www.oas.org/dil/esp/Constitucion_de_la_Republica_del_Salvador_1983.pdf

2. Marco jurídico ordinario

Estos esfuerzos buscan determinar cuál será el mecanismo efectivo en la protección de la privacidad e intimidad personal en nuestra legislación, con la intención que se ajuste al modelo integral del ciudadano en la prestación de los servicios públicos en línea y a la protección de los derechos al consumidor en entidades privadas y financieras. Por ello, es relevante separar en este estudio dos grupos normativos; el primero que regula la protección de datos de carácter personal en las entidades que conforman el sector gubernamental, y el segundo que regula la protección de datos personales en sectores como las telecomunicaciones y servicios financieros, considerando importante citar las normativas siguientes.

Como se observará, los derechos sobre la protección de datos personales no se han desarrollado con amplitud en el país, dejando de considerar nuevas reglas para la custodia y transferencia de los mismos. A pesar de ello, varios activistas de derechos digitales y expertos, han recomendado la formulación de una ley marco, que tenga como objetivo unificar estos grupos. Actualmente se discute una iniciativa de ley con el objetivo que el titular de los mismos y partes interesadas puedan tener un balance entre el respeto sus derechos en línea, sin frenar el desarrollo de Internet, el uso efectivo de las telecomunicaciones y el avance de las tecnologías de la información y comunicación.

2.1. Ley de Acceso a la Información Pública

La Ley de Acceso a la Información Pública[2] es actualmente la norma más amplia en lo que respecta al derecho a la protección de datos personales en El Salvador. Su marco de actuación es el conjunto de instancias gubernamentales o privadas que administran servicios públicos. Sus artículos se complementan del art. 31 al 38, lo que hace referencia a lo siguiente:

Art. 31. “Toda persona, directamente o a través de su representante, tendrá derecho a saber si se están procesando sus datos personales; a conseguir una reproducción inteligible de ella sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su petición, en los términos de esta ley. El acceso a los datos personales es exclusivo de su titular o su representante”.

[2] Asamblea Legislativa de la República de El Salvador. Ley de Acceso a la Información Pública, Decreto Legislativo Nº. 534. Disponible en: http://www.redipd.org/legislacion/common/legislacion/elsalvador/Decreto_N534.pdf

2.2. Ley de Firma Electrónica

La Ley de Firma Electrónica[3] es la norma que habilita la necesidad de contar con mecanismos tecnológicos para salvaguardar la privacidad, como puede ser el uso de cifrado, estableciendo una serie de reglas para el adecuado tratamiento de datos personales en las empresas prestadoras de servicios autorizados para la emisión de firma certificada y digital. Cuando existe un servicio de almacenamiento de datos electrónicos la ley obliga cumplir con ciertas reglas.

Art. 5 “El tratamiento de los datos personales que precisen los prestadores de servicios de certificación y los prestadores de servicio de almacenamiento de documentos electrónicos para el desarrollo de dichas actividades, se sujetarán a las siguientes reglas:

A. Para la expedición de certificados electrónicos al público y para el almacenamiento de documentos electrónicos, los prestadores de servicios únicamente podrán recabar datos personales directamente de los firmantes.

B. Se prohíbe que se cedan los datos personales de los usuarios. Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de servicios en relación con la firma electrónica certificada. El titular podrá solicitar la rectificación o cancelación de los datos personales, cuando éstos fueren inexactos o incompletos.

C. El responsable del registro de datos y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, estarán obligados a la confidencialidad de los mismos y al deber de guardarlos. Obligaciones que subsistirán aún después de finalizar sus relaciones con el responsable del registro de datos”.

Es importante tener en cuenta que ambas disposiciones responden principalmente a las necesidades del gobierno central de fomentar iniciativas del Gobierno Abierto, El acceso a la Información Pública y el Gobierno Electrónico en el país, al igual que establecer acciones que ayuden a desarrollar la competitividad económica con el comercio electrónico. Sin embargo, pueden ser utilizadas en favor de los derechos de protección de datos personales en línea.

[3] Asamblea Legislativa de la República de El Salvador. Ley de Firma Electrónica, Decreto Legislativo N° 133.

2.3. Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas

La Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas[4] tiene por objeto garantizar el derecho al honor, a la intimidad personal y familiar y a la propia imagen en temas como la confiabilidad, la veracidad, la actualización y el buen manejo de los datos de consumidores o clientes, relativos a su historial de crédito. Conforme al artículo 1 de la ley, determina su objeto:

Artículo 1.- "La presente Ley tiene por objeto garantizar el derecho al honor, a la intimidad personal y familiar y a la propia imagen en el tema de la confiabilidad, la veracidad, la actualización y el buen manejo de los datos de consumidores o clientes, relativos a su historial de crédito, incorporados o susceptibles de ser incorporados a una agencia de información de datos administrada por una persona jurídica, debidamente autorizada conforme a la presente Ley. Asimismo tiene por objeto regular la actividad de las personas jurídicas públicas o privadas, que tengan autorización para operar como agencias de información de datos y a los agentes económicos que mantengan o manejen datos sobre el historial de crédito de los consumidores o clientes".

2.4. Ley de Protección al Consumidor

La Ley de Protección al Consumidor[5] es la normativa que limita a los empresas poder compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la prestación de servicios de información, sin la debida autorización. El artículo 18 determina las prohibiciones de los proveedores:

Art.18 "Queda prohibido a todo proveedor:
g) Compartir información personal y crediticia del consumidor, ya sea entre proveedores o a través de entidades especializadas en la prestación de servicios de información, sin la debida autorización del consumidor".

[4] Asamblea Legislativa de la República de El Salvador. Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas, Decreto Legislativo N° 695.

[5] Asamblea Legislativa de la República de El Salvador. Ley de Protección al Consumidor, Decreto Legislativo N°776.

2.5. Ley General de Telecomunicaciones[6]

La regulación que se focaliza en proteger la intimidad personal y los derechos de confidencialidad en los datos personales de los usuarios cuando hagan uso de sus comunicaciones. Por lo tanto se cita:

Art. 29. “Son derechos de los usuarios:
b) Al secreto de sus comunicaciones y a la confidencialidad de sus datos personales no públicos, teniendo en cuenta lo mencionado en el Título V-Bis, Capítulo Único de la presente ley”.

[6] Asamblea Legislativa de la República de El Salvador. Ley General de Telecomunicaciones, Decreto LegislativoN°142.

3. Definiciones sobre datos personales

La protección de datos personales y la determinación de los datos sensibles únicamente se encuentran definidas en la Ley de Acceso a la Información Pública, la Ley de Firma Electrónica y la Ley Especial contra Delitos Informáticos y conexos, a efectos de contar con definiciones propias dentro del marco legal salvadoreño.

En la Ley de Acceso a la Información Pública en su artículo 6 determina lo siguiente:

A. "Datos personales: la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra análoga.
B. Datos personales sensibles: los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral y familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar el derecho al honor, a la intimidad personal y familiar y a la propia imagen".

En la Ley de Firma Electrónica, artículo 3 regula los datos personales como:

A. "Datos Personales: Cualquier información numérica, alfabética, gráfica o fotográfica o de cualquier otro tipo, concerniente a personas naturales identificadas o identificables.
B. Datos Personales de Alcance Público: Datos que no afectan la intimidad del titular de la misma, como los datos relativos al estado familiar de la persona entre otros, y que pueden estar contenidos en registros públicos".

Por su lado, el artículo 3 de la Ley Especial contra Delitos Informáticos y Conexos[7] establece su propia definición de datos personales a la luz de esa normativa penal:

A. "Datos Personales: es la información privada concerniente a una persona, identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico u otra similar;
B. Datos Personales Sensibles: son los que corresponden a una persona en lo referente al credo, religión, origen étnico, filiación o ideologías políticas, afiliación sindical, preferencias sexuales, salud física y mental, situación moral, familiar y otras informaciones íntimas de similar naturaleza o que pudieran afectar al derecho al honor, a la propia imagen, a la intimidad personal y familiar".

[7] Asamblea Legislativa de la República de El Salvador. Ley Especial contra Delitos Informáticos y Conexos, Decreto LegislativoN°260.

3.1. Principios de tratamiento de datos personales

En el año 2015 el Instituto de Acceso a la Información Pública (IAIP), en conjunto con la Red de Iberoamericana de Protección de Datos Personales[8] (REDIPD) y la Unión Europea con el programa Eurosocial, desarrollaron los Principios de Protección de Datos en El Salvador en el Manual Operativo de la Protección de Datos Personales, documento diseñado para ampliar la importancia en el tratamiento de los datos de carácter personal dentro de las instituciones del sector gubernamental. El manual ha desarrollado los siguientes principios:

A. "Licitud: el principio de licitud sujeta, en primer lugar, la recogida de datos personales a medios lícitos, esto es, que no han de obtenerse con infracción legal. De la misma manera, los sistemas de datos personales, esto es, la instauración de sistemas automatizados de procesamiento de información personal deberá respetar las atribuciones legales o reglamentarias en vigencia. Cada entidad pública que realice procesamiento de datos personales, en consecuencia, deberá sujetarse a las atribuciones, permisiones, limitaciones y regulaciones específicas o sectoriales que se refieran a la materia o temática desarrollada por dicho ente.

Se considera que es compatible con tales fines lícitos, el tratamiento de datos personales que responda a fines históricos, estadísticos o científicos, siempre y cuando se salvaguarden las garantías derivadas de la protección de datos personales".

B. "Calidad de los datos: el tratamiento de datos personales deberá ser exacto, adecuado, actual, pertinente y no excesivo, respecto de las atribuciones legales de la dependencia o entidad que los posea.

La exigencia de calidad tiene que ver directamente con la naturaleza del tratamiento de datos personales, toda vez que siempre habrá que revisarse que los datos tratados y recopilados son los necesarios para cumplir con el fin público. Lo anterior implica, por supuesto, que no son excesivos o que se hayan recopilado a destajo para cumplir otras funciones no expresamente señaladas en el fin legal para el cual fueron recopilados".

C. "Exactitud: este principio está profundamente unido al principio de calidad. Los datos que sean tratados han de ser exactos, es decir, no incompletos ni imprecisos con respeto a los fines para los que se justificó su recopilación. Si los datos no son exactos y precisos deberán de ser suprimidos o rectificados. Por lo tanto, es deber del encargado o responsable del banco de datos hacer un análisis de los registros para observar si la información contenida tiene algún grado de inexactitud. Si es así, deberá procurar completar los datos, sustituirlos o eliminarlos, todo esto de oficio".

[8] Chirinos, Alfredo. Manual operativo de protección de datos en El Salvador.Pág. 46.

D. "Acceso y corrección: la garantía de protección de datos se satisface, muchas veces, asegurando el derecho de los ciudadanos a acceder a sus datos, revisarlos y proceder a las correcciones de aquellas informaciones inexactas, imprecisas o falsas. Es por ello que la garantía de acceso es una de las más importantes para el ciudadano y la parte más visible del ejercicio de este derecho. Es así, entonces, que los encargados o responsables del procesamiento de datos deben almacenarse de tal manera que garanticen el ejercicio de estos derechos de acceso y corrección en el marco de las reglamentaciones y de los lineamientos que han sido establecidos por el Instituto de Acceso a la Información".

E. "Información: se deberá hacer del conocimiento del Titular de los datos, al momento de recabarlos y de forma escrita, el fundamento y motivo de ello, así como los propósitos para los cuales se tratarán dichos datos".

F. "Seguridad: se deberán adoptar las medidas necesarias para garantizar la integridad, confiabilidad, confidencialidad y disponibilidad de los datos personales mediante acciones que eviten su alteración, pérdida, transmisión y acceso no autorizado".

[8] Chirinos, Alfredo. Manual operativo de protección de datos en El Salvador.Pág. 46.

4. Derechos ARCO

Los Derechos ARCO, o los llamados mecanismos de control del ciudadano para el Acceso, Rectificación, Corrección y Oposición (ARCO), son fundamentales en el sistema jurídico de nuestro país, teniendo la posibilidad el titular de conocer qué datos tienen los entes públicos o empresas que brindan servicios financieros, o de aquellas que transfieren información de carácter personal para fines comerciales; facultando al ciudadano poder acceder a ellos donde sean depositados, rectificarlos en caso de errores, cancelarlos si dejaron de ser necesario y oponerse a su tratamiento y venta, si estos fueron obtenidos sin su consentimiento.

Los derechos ARCO se ejercen a toda persona sin discriminación alguna, tratándose de derechos independientes, por lo que el ejercicio de alguno no es condicionante ni impedimento para ejercer otro. Por tanto, es fundamental que cualquier persona los conozca y ejercitar sus los derechos ARCO sobre sus datos de carácter personal.

Los derechos ARCO determinan un requisito indispensable para su aplicación: la identificación del interesado o, en su caso, del representante legal de solicitar su ejercicio. Por lo que toda persona tiene derecho a que se le informe gratuitamente del origen de sus datos, y saber a qué otras personas o entidades públicas o privadas ha sido transferida su información, para que el titular pueda realizar acciones a su favor en caso sea incorrecta; si no está actualizada en documentos o registros públicos o privados, con el derecho ARCO se abren múltiples posibilidades para transparentar el tratamiento de la información en los sistemas de datos y registros físicos.

En el ámbito de la protección de datos personales en las entidades del sector privado, también puede solicitarse que se destruyan aquellos datos que sean inexactos o incompletos, o aquellos que no cumplan el principio de adecuación con la finalidad para la que fueron recabados, como lo expresa el art. 21 de la Ley de Protección al Consumidor:

Art. 21.- **“Obligaciones de entidades especializadas en la prestación de servicios de información.** Las entidades especializadas en la prestación de servicios de información estarán obligadas a permitir al consumidor el acceso a la información de sus datos, así como a solicitar la actualización, modificación y eliminación de los mismos, de forma gratuita. Asimismo, tendrán la obligación de corregir la información falsa, no actualizada o inexacta en un plazo máximo de diez días contados a partir de la recepción de la solicitud del interesado. Las entidades especializadas a las que se refiere el presente artículo, no podrán obtener ninguna clase de información personal del consumidor, si no es con la debida autorización de éste, y únicamente en las condiciones en que la misma haya sido conferida”.

5. Consentimiento

El marco normativo en protección de datos personales prohíbe a todo encargado del tratamiento de la información personal de entidades públicas y privadas, que bajo cualquier título se destine datos personales con fines distintos para lo cual han sido obtenidos. La Ley de Acceso a la Información Pública establece la prohibición de difusión:

Art. 33. “Los entes obligados no podrán difundir, distribuir o comercializar los datos personales contenidos en los sistemas de información administrados en el ejercicio de sus funciones, salvo que haya mediado el consentimiento expreso y libre, por escrito o por un medio equivalente, de los individuos a que haga referencia la información”.

Sin embargo, en la misma Ley existe una excepción que permite hacerlo, y es cuando la persona de quien se obtiene los datos exprese su voluntad o autorice su distribución o difusión, estableciendo:
Art. 34. “Los entes obligados deberán proporcionar o divulgar datos personales, sin el consentimiento del titular, en los siguientes casos:

A. Cuando fuere necesario por razones estadísticas, científicas o de interés general, siempre que no se identifique a la persona a quien se refieran.

B. Cuando se transmitan entre entes obligados, siempre y cuando los datos se destinen al ejercicio de sus facultades.

C. Cuando se trate de la investigación de delitos e infracciones administrativas, en cuyo caso se seguirán los procedimientos previstos en las leyes pertinentes.

D. Cuando exista orden judicial.

E. Cuando contraten o recurren a terceros para la prestación de un servicio que demande el tratamiento de datos personales. Los terceros no podrán utilizar los datos personales con propósitos distintos a aquellos para los cuales se les hubieren proporcionado y tendrán las responsabilidades legales que genere su actuación”.

Por otra parte, el Reglamento de la Ley de Acceso a la Información Pública, en sus artículos 39 al 43, explica la forma en que puede otorgarse dicho consentimiento. Conforme éste, explica que cuando el ente obligado recibe una solicitud de documentos con datos personales incluidos, debe notificar al titular de los datos, quien tendrá cinco días para contestar si está de acuerdo. En caso de no contestar, se entenderá como negativa.

En este punto es importante citar que en El Salvador en la práctica algunas entidades privadas que prestan servicios financieros, al momento de contratar con personas naturales adicionan al contrato una cláusula en la que el dueño de los datos personales autoriza de manera automática la distribución o comercialización de los mismos. En este caso podría existir un vicio en el consentimiento, donde el dueño de la información podrá aplicar los derechos ARCO.

6. Sujetos Obligados

Dentro de su marco de actuación se encuentran los órganos del Estado, sus dependencias, las instituciones autónomas, las municipalidades o cualquier otra entidad u organismo que administre bases de datos de personas naturales o ejecute acciones contra los mismos dentro la administración pública en general. La Ley de Acceso a la Información Pública amplía a lo siguiente:

Art. 32. “Los entes obligados serán responsables de proteger los datos personales y en relación con éstos, deberán:

A. Adoptar procedimientos adecuados para recibir y responder las solicitudes de indagatoria, actualización, modificación y supresión de datos personales.

B. Usar los datos exclusivamente en el cumplimiento de los fines institucionales para los que fueron solicitados u obtenidos.

C. Procurar que los datos personales sean exactos y actualizados.

D. Rectificar o completar los datos personales que fueren inexactos o incompletos.

E. Adoptar medidas que protejan la seguridad de los datos personales y eviten su alteración, pérdida, transmisión y acceso no autorizado.

F. Analizar las obligaciones y responsabilidades que poseen los sujetos vinculados, como adoptar medidas de seguridad, notificar, etc.”.

7. Autoridad competente

7.1 Instituto de Acceso a la Información Pública

Desde 2011, la autoridad competente ha sido asumida legalmente por el Instituto de Acceso a la Información Pública[9], siendo la encargada de capacitar y brindar la asistencia necesaria a los entes obligados. Esto ha creado las condiciones para buen el tratamiento de las bases de datos en el sector gubernamental, con políticas y lineamientos para el manejo, tratamiento, seguridad y protección, así como establecer instrumentos que resulten necesarias para el cumplimiento de las funciones que la ley establece en el tema.

A partir de 2017, El Instituto aprueba la creación de la Unidad de Datos Personales, la cual brinda capacitación y asistencia técnica en la implementación de la normativa, teniendo las atribuciones[10]:

- **Difusión, asistencia y promoción.** El IAIP y su unidad son los responsables de la difusión de las disposiciones legales y reglamentarias aplicables al tratamiento de datos personales, además de brindar asistencia tanto a los titulares de datos como a los responsables de los sistemas que los contienen. A esta tarea se suma la de realizar acciones de promoción en la materia, por ejemplo, mediante el desarrollo de eventos que fomenten la profesionalización de los servidores públicos sobre la protección de datos personales.
- **Registro.** Es responsable de llevar un registro de los sistemas de datos personales en posesión de los entes públicos, quienes deben notificar al Instituto la creación, modificación o supresión de sistemas de datos personales.
- **Facultades normativas.** Tiene facultades normativas, ya sea de orden general, que se concretan en disposiciones de orientación como los “Lineamientos”, o bien particular, mediante la emisión de dictámenes y pronunciamientos específicos.
- **Facultad revisora.** Es la instancia ante la cual los particulares pueden presentar un recurso de apelación si consideran que la respuesta a su solicitud de un derecho les agravia. Las resoluciones que emita serán definitivas, inatacables y obligatorias.

[9] Op. Cit. Pág. 67.
[10] Ibíd.

8. Procedimientos y Sanciones

Dentro del orden jurisdiccional de El Salvador existen diferentes instancias para interponer recursos cuando exista alguna vulneración de los derechos de protección de datos personales. En este caso, habitualmente cuando se trata de entidades públicas, el titular de los mismos puede usar el recurso de apelación, a través de la cual se recurre al Instituto de Acceso a la Información Pública, por ser el ente rector que conoce de la apelación en las negativas en esta materia. La ley estipula la siguiente regla:

Artículo 38.- **"Recurso de apelación.** Contra la negativa de entrega de informes, de la consulta directa, rectificación, actualización, confidencialidad o supresión de datos personales, procederá la interposición del recurso de apelación ante el Instituto. También procederá dicho recurso en el caso de falta de respuesta en los plazos a que se refiere el artículo 36 de esta ley".

Por otra parte, la Ley Especial contra Delitos Informáticos y Conexos, determina las sanciones finales en la indebida Utilización de Datos Personales, siendo sancionado de la siguiente forma:
Artículo 24.- "El que sin autorización utilice datos personales a través del uso de las Tecnologías de la Información y la Comunicación, violando sistemas de confidencialidad y seguridad de datos, insertando o modificando los datos en perjuicio de un tercero, será sancionado con prisión de cuatro a seis años".

Esta última se aplica también en la Ley de Firma Electrónica, Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas, Ley de Protección al Consumidor y Ley General de Telecomunicaciones.

[9] Op. Cit. Pág. 67.
[10] Ibíd.

9. Buenas prácticas en la protección de datos personales en El Salvador

Por un lado, la normalización de la gestión documental y la protección de datos personales del historial clínico en el Sistema Nacional de Salud es una buena práctica que es importante reconocer en el presente estudio.

Para finales del 2017, El Instituto de Acceso a la Información Pública (IAIP) en coordinación con el Instituto Salvadoreño del Seguro Social (ISSS) y el Ministerio de Salud (MINSAL), todas instancias del sector Gubernamental, ejecutaron el proyecto denominado Normalización de la gestión documental y la protección de datos personales del historial clínico en el Sistema Nacional de Salud, una iniciativa que cuenta con el apoyo técnico de Programa para la Cohesión Social en América Latina EUROsocial (EUROsociAL+). Esta alianza busca el fortalecimiento institucional, apoyando iniciativas que mejoren los procesos de diseño, reforma e implementación de políticas públicas con enfoque en las áreas de género, gobernanza y políticas sociales.

El proyecto tiene como propósito asegurar buenas prácticas en la implementación de políticas públicas que garanticen la protección de datos de carácter personal en el área sanitaria, con datos contenidos en las historias clínicas, tanto físicas como electrónicas, en el Sistema Integrado de Salud salvadoreño. Esto a través de una adecuada gestión documental y con el reconocimiento de los derechos de Acceso, Rectificación, Cancelación y Oposición (ARCO) a fin de lograr una acertada, rápida y eficaz atención a las personas usuarias de los servicios de salud.

Actualmente el proyecto se encuentra en ejecución inicial, y está conformado por un equipo multidisciplinario de las instituciones que conforman el Sistema Público de Salud. La alianza de instituciones discuten una propuesta de normativa y lineamientos para la normalización de la gestión documental, de archivos y la protección de datos personales en los expedientes clínicos de salud, por lo que la Dirección de Tecnologías de Información y Comunicaciones (DTIC) del MINSAL desarrolló un sistema de información en Software Libre especial, basado en la necesidad del MINSAL y del país[11], para el registro y resguardo de la información de pacientes, garantizando principios de seguridad y legalidad en datos sensibles.

[11] Ministerio de Salud. MINSAL e ISSS presentan resultados de estudio para la protección de datos personales en los expedientes clínicos. Disponible en: https://www.salud.gob.sv/17-04-2018-minsal-e-isss-presentan-resultados-de-estudio-para-la-proteccion-de-datos-personales-en-los-expedientes-clinicos

10. Marco Institucional para la Transformación Digital de El Salvador

En El Salvador existen dos propuestas de Políticas Públicas enfocadas en implementar la transformación digital del país y respeto de los derechos digitales. Ambas buscan dinamizar y modernizar los servicios de la ciudadanía, junto con la reducción de la brecha digital con herramientas y normativas que impulsen la innovación, la competitividad; y que a la vez demanden más uso y aplicación de tecnologías disruptivas entre la sociedad civil, la academia y las alianzas público-privadas.

Las actuales Agendas y Estrategias incluyen:

1. La Cámara Salvadoreña de Tecnologías de la Información y Comunicación (CASATIC), a través de su Comité de políticas públicas, en el año 2016 elaboró una propuesta denominada Agenda Digital ES.

2. El Órgano Ejecutivo, por medio de la Secretaria Técnica y de Planificación de la Presidencia y la Dirección de Gobierno Electrónico, aprobaron la Estrategia de Gobierno Digital 2018-2022.

Ambas propuestas elevan el diálogo y la necesidad de elaborar normativas que garanticen la institucionalidad, el respeto de los derechos digitales y que también activen la economía digital del país, con cimientos concretos en el desarrollo y ejecución de institucionalizar la gobernanza digital. Entre las normas se encuentran en primera línea en el debate están:

1. La Ley de Protección de Datos Personales
2. Ley de Gobierno Digital
3. Decretos Ejecutivos para la Gobernanza Digital

En las normativas se ha propuesto la creación de una entidad rectora de carácter público, con estructuras de gobernanza en internet que proveerán la organización de un país Digital que le otorgue no solo una existencia legítima dentro del gobierno salvadoreño, sino también la autoridad necesaria para llevar a cabo el programa, con la efectiva incidencia en la construcción de acuerdos entre los actores privados e instituciones de gobierno que utilizan datos personales y servicios en línea.

Referencias

Asamblea Constituyente. **Constitución de la República de El Salvador, Decreto Legislativo N.° 38.** Disponible en: https://www.oas.org/dil/esp/Constitucion_de_la_Republica_del_Salvador_1983.pdf

Asamblea Legislativa de la República de El Salvador. **Ley de Acceso a la Información Pública, Decreto Legislativo N°. 534.** Disponible en: http://www.redipd.org/legislacion/common/legislacion/elsalvador/Decreto_N534.pdf

Asamblea Legislativa de la República de El Salvador. **Ley General de Telecomunicaciones, Decreto LegislativoN°142.**

Asamblea Legislativa de la República de El Salvador. **Ley de Firma Electrónica, Decreto Legislativo N° 133.**

Asamblea Legislativa de la República de El Salvador. **Ley Especial contra Delitos Informáticos y Conexos, Decreto LegislativoN°260.**

Asamblea Legislativa de la República de El Salvador. **Ley de Protección al Consumidor, Decreto Legislativo N°776.**

Asamblea Legislativa de la República de El Salvador. **Ley de Regulación de Servicios de Información sobre el Historial de Crédito de las Personas, Decreto Legislativo N° 695.**

Chirinos, Alfredo. **Manual operativo de protección de datos en El Salvador.** Documento de Trabajo nº 26 Serie: Guías y Manuales Área: Institucionalidad Democrática, 2015.

Ministerio de Salud. **MINSAL e ISSS presentan resultados de estudio para la protección de datos personales en los expedientes clínicos.** Disponible en: https://www.salud.gob.sv/17-04-2018-minsal-e-isss-presentan-resultados-de-estudio-para-la-proteccion-de-datos-personales-en-los-expedientes-clinicos