

**Título:** Relaciones de interoperabilidad entre el Sistema de Justicia y la Administración pública con vistas a garantizar la prestación de los servicios jurídicos

**Año:** 2025

**Temática:** Interoperabilidad

**Participantes:**

MC.s. Yurixa Varela Graverán

Dra.C. Mercedes de Armas Alonso

MC.s. Yudith Cutiño Turro

**Expertos:** No

**Programa:** No

**Estado de la investigación:** Concluida



## **CENTRO DE INVESTIGACIONES JURÍDICAS**

### **INFORME DE INVESTIGACIÓN**

# **RELACIONES DE INTEROPERABILIDAD ENTRE EL SISTEMA DE JUSTICIA Y LA ADMINISTRACIÓN PÚBLICA CON VISTAS A GARANTIZAR LA PRESTACIÓN DE LOS SERVICIOS JURÍDICOS**

|          |                                 |
|----------|---------------------------------|
| Autoras: | M.Sc. Yurixa Varela Graverán    |
|          | Dra.C. Mercedes de Armas Alonso |
|          | M.Sc. Yudith Cutiño Turro       |

2025

**TÍTULO DEL PROYECTO: RELACIONES DE INTEROPERABILIDAD ENTRE EL SISTEMA DE JUSTICIA Y LA ADMINISTRACIÓN PÚBLICA CON VISTAS A GARANTIZAR LA PRESTACIÓN DE LOS SERVICIOS JURÍDICOS**

**TIPO DE PROYECTO:** Aplicada, de desarrollo e innovación

**ENTIDAD EJECUTORA PRINCIPAL:** Centro de Investigaciones Jurídicas (CIJ), MINJUS.

Dirección: Neptuno N.873 e/ Oquendo y Soledad, Centro Habana, La Habana.

Teléfono: 78775631

**INVESTIGADORES:**

M.Sc. Yurixa Varela Graverán

Dra.C. Mercedes de Armas Alonso

M.Sc. Yudith Cutiño Turro

**OTROS INVESTIGADORES ASOCIADOS:**

**POSIBLES CLIENTES:** Dirección de Informatización, Ministerio de Justicia de Cuba.

**BENEFICIARIOS IDENTIFICADOS:** El Sistema de Justicia en su conjunto y otras instituciones del país que brindan servicios públicos, el Gobierno.

**DURACIÓN:** Enero 2025-Noviembre 2025.

## ÍNDICE

|   |  |
|---|--|
| <b>INTRODUCCIÓN</b>   |  |
| <b>PRINCIPALES RESULTADOS</b>   |  |
| <b>I. PARTICULARIDADES DE SISTEMAS INTEROPERABLES QUE FUNCIONAN EN DIFERENTES PAÍSES</b>  |  |
| <b>II. CARACTERIZACIÓN DE PRÁCTICAS EXITOSAS DE INTEROPERABILIDAD EN SISTEMAS JURÍDICOS DE DIFERENTES PAÍSES</b>  |  |
| <b>III. EXPERIENCIAS LEGISLATIVAS EXISTENTES A NIVEL INTERNACIONAL ACERCA DE LAS RELACIONES DE INTEROPERABILIDAD ENTRE SISTEMAS DIVERSOS</b>  |  |
| <b>IV. PRINCIPALES PRESUPUESTOS A TENER EN CUENTA PARA ELABORAR LAS PROPUESTAS DE NORMAS, POLÍTICAS Y DIRECTRICES PARA DESARROLLAR EL ECOSISTEMA DE INTEROPERABILIDAD EN EL MINISTERIO DE JUSTICIA.</b> |  |
| <b>BIBLIOGRAFÍA</b>   |  |

## INTRODUCCION

Desde el 2018 fueron definidos los tres pilares de la Gestión del Gobierno basado en ciencia e innovación. Uno de ellos es la informatización de los procesos para facilitar la toma de decisiones, así como agilizar las acciones. (Díaz-Canel, 2021). En este contexto se hace un llamado a fomentar el desarrollo de productos y servicios de facturación nacional, la interoperabilidad, el uso de estándares internacionales y promover el empleo de tecnologías de código abierto, así como aumentar la percepción de riesgos asociados a la ciberseguridad, minimizar las vulnerabilidades de los sistemas y cambiar la conceptualización y diseños de los procesos para que se haga un uso eficiente y efectivo de los datos.

Entre los ejes estratégicos de la política para la transformación digital se vislumbra la necesidad de crear el entorno habilitador normativo e institucional que contribuya a la construcción de una sociedad digital socialista, abierta, inclusiva, participativa, basada en derechos, que analice y evolucione el marco regulatorio para estos temas. También, el relacionado con la infraestructura tecnológica, conectividad y acceso digital refiere la importancia de dotar a los actores sociales de facilidades y capacidades tecnológicas de avanzada que les permitan interconectarse y acceder a los servicios con mayor calidad y seguridad, priorizando la industria nacional, garantizando la interoperabilidad y la disponibilidad de plataformas transversales, que contribuyan a la racionalidad, eficacia y eficiencia de este proceso. (MINCOM, 2024).

En la actualidad, el país se encuentra inmerso en una transformación digital, de la cual el MINJUS no está exento. Al respecto se realizan esfuerzos para digitalizar el sector público y establecer la coordinación que ello implica a nivel nacional para evitar la fragmentación digital de los trámites, los servicios y los datos.

En esta coyuntura, se impone la interoperabilidad y estandarización de los datos los cuales constituyen temas prioritarios que harán que no se obstaculice la construcción de un sector público basado en datos, como uno de los elementos claves para avanzar en las etapas de Gobierno electrónico establecidas en Cuba.

A los efectos de esta investigación la Interoperabilidad<sup>1</sup> se entiende de manera sintetizada como la habilidad o capacidad de dos o más sistemas, componentes, organizaciones o entidades para intercambiar información y servicios, así como utilizar estos de manera efectiva y transparente. No se limita solo a la tecnología, sino que también incluye aspectos

---

<sup>1</sup> Elaboración propia del equipo de investigación a partir del estudio de varios conceptos de (Febles, 2022).

organizativos, legales y semánticos para trabajar de manera eficiente y sin barreras. Definiendo el aspecto tecnológico como la capacidad de los sistemas técnicos para conectarse y comunicarse, el semántico como la comprensión común de los datos intercambiados (significado y contexto) y el organizativo como la alineación de procesos, políticas y estándares entre organizaciones. (Febles, 2022)

La interoperabilidad en los servicios jurídicos desempeña un papel crucial en la integración de plataformas digitales, facilitando la interacción y el intercambio de información y servicios entre diferentes sistemas legales y administrativos. Entre otras funciones y beneficios se encuentran la reducción de costos al evitar duplicidades y la mejora de la eficiencia en la gestión de trámites, servicios o casos. Además, de cumplirse una normativa establecida, el intercambio de datos se realiza dentro de un marco legal que respeta la privacidad y la seguridad de la información, permitiendo la toma de decisiones basada en datos completos y precisos.

En igual sentido agiliza la coordinación entre las diferentes entidades que prestan servicios jurídicos, fomentando la colaboración entre organizaciones y sectores y facilitando una comunicación fluida entre tribunales y oficinas legales, lo que optimiza la administración de justicia al permitir un acceso rápido a documentos y registros importantes. Al promover la colaboración interinstitucional, se crea un entorno más inclusivo y accesible para los ciudadanos que requieran este tipo de servicios. Al mismo tiempo promueve la innovación al permitir el uso compartido de recursos y conocimientos.

Por otra parte, entre las principales ventajas está garantizar la eficiencia operativa. Al integrar sistemas heterogéneos, se reducen tiempos de espera y errores en los procesos legales, los usuarios pueden acceder a información actualizada en tiempo real, lo que es vital para una respuesta rápida en situaciones legales. Asimismo, un sistema interoperable respetuoso de las normas jurídicas, genera mayor confianza entre los ciudadanos en el uso de plataformas digitales, fortaleciendo la confianza pública. La interoperabilidad no solo mejora el funcionamiento interno de los sistemas jurídicos, sino que garantiza un servicio más accesible, rápido y seguro para los usuarios.

En el 2008 empezó a desarrollarse el proceso de informatización en el Ministerio de Justicia, comenzando la migración digital por el Registro Civil. Para consolidar la tarea se ha estructurado un plan estratégico que contempla las acciones, los responsables y las fechas de su cumplimiento e implementación. Todo lo anterior en coordinación con empresas como XETID, DESOF, entre otras.

No obstante, aun cuando se aprecian avances en la digitalización de la información, la creación de bases de datos mediante el empleo de software y programas informáticos, la publicación de las leyes mediante la Gaceta, en el acercamiento de algunos servicios a la población, mediante el uso tecnológico, no se han logrado los resultados esperados.

El MINJUS tiene la responsabilidad no solo de crear un sistema interoperable hacia lo interno, sino de concluir éste para interconectar el servicio con otras instituciones de la administración pública lo que permitiría mejores prestaciones a la ciudadanía desde el Portal del Gobierno.

Al respecto, a pesar de sus beneficios, la interoperabilidad enfrenta retos a tener en cuenta, como pueden ser la falta de estándares comunes, donde diferentes sistemas pueden usar formatos o protocolos incompatibles; las barreras legales y regulatorias ya que las normativas pueden limitar el intercambio de información; la resistencia al cambio pues las organizaciones pueden ser reacias a modificar sus procesos o sistemas, así como la seguridad y privacidad porque el intercambio de datos debe garantizar la protección de la información sensible.

La interoperabilidad es un pilar para la integración y eficiencia en un mundo cada vez más interconectado. Su implementación efectiva requiere no solo soluciones prácticas y técnicas, sino también un enfoque holístico que considere aspectos teóricos, organizativos, legales y semánticos.

Con el avance de tecnologías como la Inteligencia Artificial, el Internet de las cosas y el Blockchain, entre otros, la interoperabilidad se vuelve aún más compleja. Estos avances requieren sistemas que puedan comunicarse de manera fluida y segura, lo que impulsa la necesidad de estándares globales y colaboración interdisciplinaria.

El presente proyecto guarda relación con la línea de investigación del Departamento de Informatización del MINJUS sobre la transformación digital en esta institución para los próximos años. Tiene como:

### **Problema científico**

¿Cuáles son los fundamentos teóricos y prácticos que permiten sustentar las relaciones de interoperabilidad entre el Sistema de Justicia y la Administración Pública con vistas a garantizar la prestación de los servicios jurídicos?

### **Objetivo general**

Analizar los fundamentos teóricos y prácticos que permiten sustentar las relaciones de interoperabilidad entre el Sistema de Justicia y la Administración Pública con vistas a garantizar la prestación de los servicios jurídicos.

### **Objetivos específicos**

1. Examinar particularidades de sistemas interoperables que funcionan en diferentes países.
2. Caracterizar prácticas exitosas de interoperabilidad en sistemas jurídicos de diferentes países.
3. Identificar experiencias legislativas existentes a nivel internacional acerca de las relaciones de interoperabilidad entre sistemas diversos.
4. Determinar los principales presupuestos a tener en cuenta para elaborar las propuestas de normas, políticas y directrices del Sistema de Interoperabilidad en el Sistema del Ministerio de Justicia.

Por la complejidad del tema es importante un acercamiento a la problemática desde la ciencia y la innovación

El MINJUS tiene la particularidad de contar con representación en los municipios, las provincias y también con dependencias que brindan diferentes y variados servicios a la ciudadanía, por lo que la estructura, el funcionamiento, la atención a la población y los servicios que presta serían un buen comienzo para sumar otras entidades dentro del mismo sector y otras que permitan optimizar la eficiencia en estos temas.

Al respecto existen antecedentes que conducen a dar pasos en función de lograr estos cambios en Cuba. Sin embargo, la documentación analizada hasta el momento permite plantear que los estudios sobre el tema se concentran en la parte técnica de cómo desarrollar las herramientas, careciendo de suficientes aspectos teóricos, prácticos y normativos a tener en cuenta para un funcionamiento óptimo de lo que se quiera obtener en cuanto a sistemas interoperables.

## **PRINCIPALES RESULTADOS**

### **PARTICULARIDADES DE SISTEMAS INTEROPERABLES QUE FUNCIONAN EN DIFERENTES PAÍSES**

El Gobierno Electrónico (GE) entendido como el uso de las tecnologías de información (TI) en la gestión pública, y visto como un fenómeno multidimensional es necesario conceptualizarlo como una amalgama de elementos y aplicaciones interrelacionados, los cuales no necesariamente tienen los mismos objetivos y prioridades. Los países de

Iberoamérica dentro de los que se encuentra Cuba, no son una excepción. En los últimos años, importantes iniciativas se han puesto en marcha, destacándose Brasil. En este desde el año 2004 existe una arquitectura e-PING (Estándares de Interoperabilidad de Gobierno Electrónico) que define un conjunto mínimo de premisas, políticas y especificaciones técnicas que reglamentan la utilización de las TIC en la interoperabilidad de servicios de gobierno electrónico (Santos, 2008).

La interoperabilidad, entendida como la capacidad mediante la cual sistemas heterogéneos, no sólo tecnológicos, pueden intercambiar información y procesos técnicos o datos, no es algo nuevo dentro del sector público. Sin embargo, cada vez más, este término toma importancia entre las administraciones públicas como consecuencia del propósito de satisfacer de mejor manera las necesidades y expectativas del ciudadano y, por tanto, de implantar proyectos de Gobierno más sofisticados y complejos que requieren la colaboración de dos o más órganos administrativos (Gascó y Roy, 2006; Gil-García, 2007; Mayer-Schönberger, 2005; Scholl y Klischewski, 2007). A pesar de estos intensos y concentrados esfuerzos, el panorama de interoperabilidad en la región no es homogéneo y, en este sentido, los diversos países han adoptado estrategias diferentes.

Hoy día, la interoperabilidad es clave en el desarrollo de diversos proyectos que buscan la agilización de trámites, a través de la integración de procesos de diversas administraciones públicas que entre sí deben interoperar, tanto respecto de la información que los órganos y entidades intercambien, como de la interconexión de redes y sistemas tecnológicos; así como de modo principal, en la prestación eficaz y eficiente de servicios electrónicos a los usuarios, preferentemente desde una plataforma única que les interconecte. Bien resume este planteamiento Cerrillo y Martínez, al plantear de manera concisa la idea de cómo “mediante las tecnologías de la información y la comunicación, las Administraciones públicas pueden crear portales a través de los cuales los ciudadanos se relacionan con las Administraciones públicas independientemente de los órganos competentes para tramitar los procedimientos en los que estén interesados”. (Cerrillo 2006, p. 32; esto es conocido como servicios a través de “ventanilla única” o “one-stop-shopping”).

La Declaración de Interoperabilidad de Valencia, la define en función de su relación con el Gobierno Electrónico, indicando que “... la interoperabilidad es un elemento multidimensional, que integra los aspectos técnico, semántico, organizativo, jurídico y cultural, exigiendo la existencia de equipos humanos especializados y multidisciplinares dentro de las administraciones y el fomento de grupos de trabajo interadministrativos y de

órganos de composición mixta público-privada de interoperabilidad. El elemento clave para que la interoperabilidad sea real es el factor humano. Es fundamental la formación y la especialización de las organizaciones y de los responsables y empleados públicos, orientando su gestión y acción burocrática y pública hacia la coordinación, la interoperabilidad y hacia la compartición de tecnología, información y conocimiento...” (Acero, 2009).

Ahora bien, para que la relación entre Interoperabilidad y Gobierno Electrónico genere una efectiva integración entre servicios públicos y las entidades que los ofrecen, esta deberá estar basada en una serie de principios rectores. Diversos autores se refieren a este punto, entre los cuales destacan las ideas fundamentales contenidas en el documento “Bases para una Estrategia Iberoamericana de Interoperabilidad” y que se resumen a continuación (Criado, 2010) en los principios de:

- Igualdad: “aplicado a la interoperabilidad implica que el uso de medios digitales no debe generar restricciones o limitaciones para los ciudadanos que decidan relacionarse con las Administraciones Públicas por otros medios (...)”.
- Accesibilidad: “se refiere a las necesidades especiales de las personas con discapacidades, así como a la facilidad de uso de los servicios públicos gubernamentales en los que participen diferentes agentes (...)”.
- Legalidad: “se concreta en el mantenimiento general de las garantías jurídicas dentro de los intercambios digitales de la misma manera que suceden en el medio físico. La interoperabilidad entre diferentes Administraciones Públicas no deja de requerir un estricto cumplimiento de la normativa aplicable en cada caso, de forma que todos los actores implicados en las interacciones en Internet dispongan de una efectiva protección de sus derechos, siendo asimismo responsables de todas sus acciones dentro de esta dimensión digital (...)”.
- Privacidad: “en el ámbito de la interoperabilidad supone una atención central a las cuestiones de privacidad que derivan de la colaboración entre diferentes Administraciones Públicas y de la relación con los ciudadanos (...)”. En criterio del suscrito, este principio es más amplio, en cuanto lo que se reconoce es el derecho a la autodeterminación informativa de la persona y a partir de este, la protección de los datos personales y la garantía a los derechos fundamentales de la persona; por lo que la tutela de este principio es al respeto de los derechos de la persona en el tratamiento de su información personal en los servicios públicos que se integran a través de la plataforma de interoperabilidad.

- Responsabilidad: “(...) Considerando la colaboración de diferentes Administraciones Públicas en procesos administrativos o en la prestación de servicios públicos por medios digitales, cada una de ellas deberá responsabilizarse de sus propias actuaciones, facilitando que se rindan cuentas ante los ciudadanos por los actos realizados en esta dimensión telemática de la misma manera que de los llevados a cabo por medios tradicionales (...)”.
- Adecuación tecnológica: (...) la interoperabilidad requiere la promoción de estándares abiertos y del software libre, de cara a garantizar la seguridad y la sostenibilidad del Gobierno electrónico en el futuro. Con ello se debe evitar cualquier limitación en el derecho de los ciudadanos a elegir las tecnologías que desee para relacionarse con las Administraciones Públicas. De hecho, se debe prever el desarrollo de diferentes dispositivos digitales y electrónicos de acceso, como el computador, la televisión digital terrestre, los teléfonos celulares, así como otros que puedan aparecer, de manera que el acceso quede garantizado independientemente de los desarrollos tecnológicos futuros realizados por cada país”.
- Proporcionalidad: “implica requerimientos de seguridad adecuados a la naturaleza de la relación que se establezca con el sector público dentro de entornos de colaboración entre diferentes Administraciones Públicas (...)”. Este principio debe entenderse en un contexto de equilibrio entre la seguridad de la información y las obligaciones de coordinación y colaboración entre organizaciones, en el marco de los procesos administrativos con el objetivo de brindar servicios públicos electrónicos integrados.
- Conservación: “supone la garantía de que los datos, información y comunicaciones por medios telemáticos conservan las mismas condiciones de mantenimiento que por medios tradicionales. En los procesos interoperables de Gobierno electrónico, todos los agentes intervinientes se responsabilizarán de que la conservación se lleva a efecto de la mejor manera posible, teniendo en cuenta sus particularidades, así como entendiendo los diferentes requerimientos nacionales en esta materia”.
- Reutilización: parte de la base de “generar repositorios compartidos que permitan la reutilización de componentes que colaboren en la interoperabilidad entre las Administraciones Públicas y el desarrollo de acuerdos regionales de colaboración (...). Además, se facilitará la cesión de derechos de propiedad intelectual de aplicaciones para ponerlas a disposición de diferentes Administraciones...”. En este sentido, quien escribe considera también la posibilidad de mantener las fuentes de información sin necesidad de integrarlas en grandes bases de datos, pero con una garantía de acceso a la información

pertinente a cualquier dependencia autorizada para solicitarlo, estableciendo para estas únicamente los requisitos y condiciones necesarias para tutelar efectivamente los derechos de las personas.

- Eficiencia: “hace referencia a que las organizaciones que conforman el sector público de los países deben garantizar la existencia de procesos y soluciones a los problemas de los ciudadanos de una manera económicamente lo más óptima posible y ofreciendo los resultados esperados. Lo anterior debe consolidarse mediante la prestación de servicios interoperables que se fundamenten en la generación de economías de escala ligadas a inversiones compartidas, esfuerzos coordinados y soluciones replicables” (Tomado de: Criado 2010, Pp. 10-12. Por su parte, Poggi 2008c, pp. 35-41, plantea una categorización distinta de los principios que rigen la relación entre Interoperabilidad y Gobierno Electrónico, enumerando los siguientes postulados: a) Foco en la Sociedad, b) Subsidiaridad -cada instancia deberá resolver las medidas propias para integrar sus procesos-, c) Vulgaridad -en cuanto a divulgación y apropiabilidad de las herramientas por los usuarios-, d) Neutralidad tecnológica, e) Multilateralidad y f) Asincronía y Asimetría-gradualidad y respeto a diferencia entre organizaciones).

La interoperabilidad es clave en la era tecnológica, y en materia de gobierno electrónico su rol es también trascendental para el avance de las políticas públicas y la productividad de los Estados. De esta forma, al contar con claridad en relación al aspecto conceptual, corresponde ahora también abordar cómo lograr la integración efectiva de la interoperabilidad en la actividad pública. El mejor entorno para el crecimiento de la interoperabilidad se da cuando esta se basa en la utilización de estándares abiertos por parte de todos los actores que intervienen en los procesos tecnológicos. De este modo, el Estado puede contribuir para alcanzar mejores condiciones de interoperabilidad si se adoptan políticas públicas de Gobierno Electrónico que fomenten el uso de estándares abiertos en la sociedad y estableciendo estos como norma general en la interacción con la Administración con las consecuentes ventajas para garantizar el acceso a todos los usuarios, eliminando barreras de discriminación tecnológica. En relación con la idea antes dicha, los planes, directrices y normas en materia de tecnología adoptadas en la Unión Europea, sintetizan muy bien el imperativo vínculo que existe entre interoperabilidad y estándares abiertos en el marco del Gobierno Electrónico, lo cual se ilustra en el párrafo siguiente:

“En efecto, la adhesión a estándares abiertos parece el único camino para facilitar que los diversos actores puedan participar utilizando sus opciones tecnológicas preferidas, sin verse

condicionados a la utilización o adquisición de entornos tecnológicos concretos, a la vez que se facilita una mayor concurrencia en el mercado. La citada Comunicación de la Comisión sobre Interoperabilidad reconoce que los estándares, especificaciones e interfaces abiertos son cruciales para la interoperabilidad; y cuando el Plan de Acción Europe 2005 encomendó a la Comisión Europea la elaboración del Marco Europeo de Interoperabilidad, declaró que éste se basaría en normas abiertas” (Ministerio de Administraciones Públicas de España 2006, p, 28; citado en Salas 2007, p, 248).

Es importante acotar que, lamentablemente en el EIF versión 2.0, publicado en diciembre de 2010, la comisión Europea cedió a las presiones de la industria tecnológica que basa su desarrollo en estándares propietarios, evitando así utilizar el término estándares abiertos en el documento, modificando este por términos imprecisos y ambiguos -como por ejemplo: especificaciones abiertas- y dejando el peso de la determinación en el rol que juegan las organizaciones desarrolladoras de estándares -las cuales, no en todas las ocasiones son capaces de garantizar el cumplimiento con los requisitos que un estándar abierto, según el propio EIF en su primera versión, debe cumplir para ser considerado como tal.

Lo anterior, conlleva un retroceso en tanto que los Estados podrán implementar soluciones tecnológicas basadas en estándares propios de una empresa o conglomerado de estas, el cual, además de atentar contra la neutralidad tecnológica -entendida en su acepción más amplia-, puede ser causa de una complicación en la interconexión de los sistemas de información de los distintos miembros de la Unión Europea -dependiendo del estándar cerrado que utilicen sus proveedores de tecnología; pero ante todo, podría originar discriminación tecnológica en contra de aquellos ciudadanos cuyas terminales y dispositivos no sean interoperables con aquel estándar que el proveedor de la Administración utiliza -se privilegia el interés privado y las prácticas más simplistas para las entidades públicas, por sobre el interés público, representado en la accesibilidad e interoperabilidad para todos los ciudadanos, razón de ser de los servicios públicos que se prestan.

Existen importantes experiencias de utilización intensiva de las Tecnologías de la Información (TI) en la gestión pública a nivel internacional. El 75% de los países cuenta con una estrategia de interoperabilidad, al menos entendida como una línea dentro de una política más general de Gobierno electrónico (GE). Ello confirma el aumento de una visión global sobre el papel de la colaboración intergubernamental en materia tecnológica.

Otro de los puntos claves para conocer cómo se despliega la interoperabilidad en las administraciones de Iberoamérica se refiere a los organismos impulsores de esta materia en

los gobiernos nacionales. En la segunda columna de la Tabla 2 se observa que todos los países estudiados, salvo Guatemala, cuentan con una unidad responsable del fomento de la interoperabilidad de e-Gobierno. Ello confirma el interés mostrado por los países en esta materia, que se ha abierto camino mayoritariamente en los organigramas ministeriales. Asimismo, se pueden considerar otros aspectos, como la naturaleza de tales organismos y su ubicación dentro del organigrama gubernamental. A continuación se muestra un cuadro en el que aparecen los organismos responsables de la interoperabilidad en algunos países de Iberoamérica.

| <b>Países</b> | <b>Denominación de las autoridades responsables</b>   | <b>Organismo al que pertenece</b>                                |
|---------------|---|--|
| Argentina     | Oficina Nacional de Tecnologías de Información, Subsecretaría de Tecnologías de Gestión, Secretaría de Gabinete | Jefatura de Gabinete de Ministros                                |
| Brasil        | Secretaria de Logística e Tecnologia da Informação  | Ministério do Planejamento, Orçamento e Gestão                   |
| Colombia      | Programa Gobierno en Línea  | Ministerio de Tecnologías de la Información y las Comunicaciones |
| Costa Rica    | Secretaría Técnica de Gobierno Digital  | Ministerio de Planificación Nacional y Política Económica        |
| Chile         | Área de Gobierno Electrónico, Secretaría Ejecutiva de Estrategia Digital  | Ministerio de Economía, Fomento y Turismo                        |
| Ecuador       | Subsecretaría de Informática  | Secretaría Nacional de la Administración Pública                 |
| El Salvador   | Unidad de Gobierno Electrónico e Integración de Sistemas, Dirección de Innovación Tecnológica e Informática     | Presidencia de la República                                      |
| España        | Dirección General para el Impulso de la Administración Electrónica  | Ministerio de la Presidencia                                     |
| Guatemala     | Unidad de Tecnologías de Información, Centro de Apoyo Estratégico   | Vicepresidencia de la República                                  |
| México        | Unidad de Gobierno Electrónico  | Secretaría de Función Pública                                    |
| Nicaragua     | Dirección General de Tecnología   | Ministerio de Hacienda y Crédito Público                         |
| Panamá        | Autoridad Nacional para la Innovación Gubernamental   | Ministerio de la Presidencia                                     |

|           |   |   |
|-----------|---|---|
| Perú      | Oficina Nacional de Gobierno Electrónico e Informática  | Presidencia del Consejo de Ministros  |
| Portugal  | Agência para a Modernização Administrativa, Secretária de Estado da Modernização Administrativa     | Presidência do Conselho de Ministros  |
| Uruguay   | Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el | Presidencia de la República   |
| Venezuela | Centro Nacional de Tecnologías de Información   | Ministerio del Poder Popular para la Ciencia, Tecnología e Industrias Intermedias |

El cuadro muestra la diversidad en cuanto a denominación de los organismos y unidades creadas para el fomento de la interoperabilidad de GE en cada uno de los países. Muchos de esos organismos incluyen en su nombre el concepto de gobierno electrónico, gobierno en línea, gobierno digital, gobierno de gestión electrónica o administración electrónica, no siendo de igual manera en casos como el de Argentina, Brasil, Portugal o Venezuela, donde se opta por el término tecnologías de la información dentro de las denominaciones seleccionadas. Además cabe apuntar el caso pionero de Panamá, donde se utiliza la acepción innovación gubernamental para caracterizar su unidad directiva.

A su vez existen organismos de coordinación interna de cara a la consolidación de la interoperabilidad de GE en todos los entes dentro del nivel central de gobierno. En este sentido, no todos los países iberoamericanos disponen de este tipo de organismos coordinadores, ni en todos los casos se entienden de la misma manera, por lo que no se han podido identificar patrones comunes o conclusiones cerradas sobre su alcance y contenidos. Evidentemente, la propia estructura interna de los gobiernos es diferente en cada país, así como las competencias atribuibles en cada caso. Lo realmente importante es que la naturaleza de los organismos de este tipo manifiesta, al menos en cierta medida, la capacidad para concertar actuaciones de interoperabilidad en el conjunto de la administración nacional.

En lo que respecta a los departamentos ministeriales de adscripción, la variedad es también aquí la nota predominante, si bien se puede encontrar algún patrón compartido como muestra la siguiente tabla.

| <b>Países</b> | <b>Órganos de coordinación interna</b>   |
|---------------|--|
| Argentina     | Comité Técnico Asesor  |
| Brasil        | Coordenação e-PING, Secretaria de Logística e Tecnologia da Informação                       |
| Colombia      | Comisión Intersectorial de Políticas y Gestión de Información para la Administración Pública |

|             |  |
|-------------|--|
| Costa Rica  | Comisión Interinstitucional de Gobierno Digital  |
| Chile       | Comités ejecutivo, jurídico, técnico, operativo y representantes del administrador de esquemas y metadatos, Secretaría Ejecutiva de Estrategia Digital                                       |
| Ecuador     | En construcción. Comité para la interoperabilidad de ámbito estatal que incorpore las cinco funciones del Estado: ejecutiva, legislativa, judicial, electoral y participación ciudadana      |
| El Salvador | Foro RED-GOES. Directores de tecnologías de las dependencias del gobierno central  |
| España      | Consejo Superior de Administración Electrónica   |
| Guatemala   |  |
| México      | Consejo Técnico, Comisión Intersecretarial para el Desarrollo de Gobierno Electrónico  |
| Nicaragua   | Comisión de Gobierno Electrónico de Nicaragua  |
| Panamá      | Consejo Nacional para la Innovación Gubernamental  |
| Perú        | Comité de Interoperabilidad en la Administración Pública   |
| Portugal    | ICT Network Board (con representantes de todas las administraciones portuguesas), Agência para a Modernização Administrativa   |
| Uruguay     | Área de Normas y Estándares Tecnológicos, Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento, y Consejo de Informática Pública |
| Venezuela   | Centro Nacional de Tecnologías de Información  |

La idea central que se puede observar es que la interoperabilidad se encuentra vinculada a ministerios próximos o muy cercanos al entorno presidencial, demostrando con ello la importancia que conceden los máximos dirigentes nacionales a esta vertiente de la actividad pública. En efecto, esa dependencia de la Presidencia de la República o Ministerio de la Presidencia dota de carácter sustantivo a las políticas de GE, dado que desde ahí es mucho más factible su diseminación al conjunto de la estructura gubernamental nacional. Al mismo tiempo, esto demuestra el carácter transversal y horizontal de las políticas de interoperabilidad de GE, que afectan al resto de las políticas públicas.

Existen un grupo de áreas o ámbitos de acción pública por decirlo de otra manera en los que se han llevado a cabo proyectos de interoperabilidad de GE por parte de los países iberoamericanos. En este sentido, se pueden identificar cuatro sectores de especial interés para desarrollar proyectos interoperables: Compras públicas, tributos, seguridad social y trámites generales. De manera complementaria se puede afirmar que, junto a lo anterior, los países perciben que determinados sectores cuentan con un mayor potencial de beneficio como consecuencia de su desarrollo. En particular, suelen incluirse áreas como la sanidad, la

justicia, el comercio o los tributos, aunque no existe al respecto una visión homogénea en todos los países.

Los beneficios estudiados por la literatura son también percibidos como tales por las administraciones públicas que han puesto en marcha proyectos de interoperabilidad; (Criado, Gascó y Jiménez, 2010) resumen algunas de estas oportunidades haciendo referencia a:

- La posibilidad de cooperar entre niveles de gobierno y agencias de la administración sin distinción del nivel de desarrollo tecnológico; es decir, combinando diferentes tipos de tecnologías en los back offices de los organismos implicados.
- La simplificación de la actividad administrativa y de los procesos de negocio/gobierno, lo que tiene como consecuencia una mayor eficiencia en el quehacer de las administraciones públicas.
- La posibilidad de utilizar más fácilmente estándares abiertos y aplicaciones tecnológicas, lo que puede llevar a una reducción del coste en tecnología.
- La reutilización de datos y funcionalidades que puede redundar en una disminución de los costes de desarrollo de sistemas de información.
- La mejora de la toma de decisiones como consecuencia de la obtención de datos agregados y de información de mayor calidad.
- La promoción de la cooperación internacional en ámbitos en los que se requieren nuevas herramientas.
- La mayor sencillez en la realización de trámites por el ciudadano o usuario de los servicios públicos (por ejemplo, ahorro de tiempo o de dinero).
- La mayor capacidad de promover la transparencia y la rendición de cuentas ante los stakeholders.
- La consecución de una visión integral e integrada de los servicios públicos tanto por parte de las administraciones públicas como de los beneficiarios y otros actores implicados, independientemente del número de organismos o procesos que intervengan en su confección final.

En estrecho vínculo con los beneficios señalados los ámbitos de gobierno más relevantes para poner en marcha proyectos de interoperabilidad de manera general son tres: comercio e intercambio de mercaderías); aduanas, fronteras y movimientos migratorios; y seguridad. Dada la escasa experiencia en materia de interoperabilidad entre países, esta situación pareciera lógica puesto que tiene que ver, por un lado, con el intercambio de bienes y servicios y migraciones de población entre países, algo que ocurre frecuentemente, y, por el

otro, con la posibilidad de aumentar la percepción de seguridad, lo que es importante teniendo en cuenta el alto nivel de riesgo percibido que existe en algunos de los países de Iberoamérica.

Al respecto (Criado, Gascó y Jiménez, 2010, p-35) afirman: “Los Estados iberoamericanos experimentan una creciente circulación de personas entre ellos, así como con terceros países, de manera que actuaciones de interconexión entre los sistemas aduaneros facilitará que estos procesos se realicen de una manera ordenada y siguiendo los intereses de los respectivos actores involucrados, así como evitando situaciones indeseadas. Además, todo ello facilitará un servicio más eficiente y cercano a la ciudadanía y las empresas, en la medida que se dispone de una información más robusta y consistente”. Asimismo, “las amenazas que experimenta la seguridad de los Estados iberoamericanos por parte de la delincuencia internacional convierten esta dimensión en una de las más relevantes de cara a promover iniciativas transfronterizas de colaboración. En particular, la posibilidad de compartir datos e información sobre narcotráfico, terrorismo, trata de personas y demás amenazas a la seguridad que son comunes a la mayoría de los países de la región resulta de especial interés, siempre teniendo en cuenta que en este ámbito es donde se deben extremar las medidas de garantía para evitar el acceso de terceros a los datos de las Administraciones Públicas involucradas en los intercambios” (Criado, Gascó y Jiménez, 2010, p. 36).

Es importante destacar que ya en la segunda década de este siglo, existen otros sectores, que han descubierto en la interoperabilidad una vía rentable para expandir y facilitar la gestión de su servicio. Tenemos el caso de Argentina con un nivel de desarrollo de GE aplicado a Educación, donde la disposición de los servicios, el uso de la tecnología, hasta ahora, ha traído muchos beneficios para la gestión, el sistema y demás usuarios. Los servicios dispuestos en sus sitios responden a las necesidades puntuales del área y de la jurisdicción a la cual pertenecen.

En materia de interoperabilidad, es importante hacer notar que, hoy en día, los países europeos son los que a nivel mundial dictan la pauta en este tema, conjugando al sector público y al sector privado. Experiencias exitosas como por ejemplo la del Gobierno de Estonia, un país cuya situación geográfica y climática es compleja, en el cual, mediante la concreción de una iniciativa para la integración del acceso a los servicios públicos por medios digitales, a través de un documento de identificación electrónico que permite a los ciudadanos gestionar y tramitar remotamente sus requerimientos ante la Administración contando con altos grados de aprobación y satisfacción respecto del valor agregado y calidad de los

servicios brindados; lo cual es una muestra de la relevancia y potencial que este tema tiene en un futuro cercano (Criado 2008, p.44).

En este sentido, los beneficios de la interoperabilidad se refieren a tres aspectos diferenciados: por un lado técnicos, como la posibilidad de utilizar estándares abiertos y la reutilización de datos y funcionalidades; por otro lado, organizativos en materia de fortalecimiento de las capacidades de la Administración, en la toma de decisiones, la mejor coordinación, o la simplificación de la actividad administrativa; y también de las políticas públicas, puesto que refuerzan la imagen pública, promoviendo los principios de transparencia y de rendición de cuentas (Cerrillo, 2016, p-285). En consecuencia, se puede afirmar que cuando se alude a la interoperabilidad se hace referencia a un criterio recurrente para garantizar la conexión y el intercambio de información entre las distintas Administraciones, y garantizar que estas no se convirtieran en islas inaccesibles.

En los últimos años se ha incrementado la necesidad de la interoperabilidad o cooperación tecnológica, debido a la relevancia ante la necesidad de llevar a buen término proyectos de gobierno electrónico cada vez más complejos, muchos de los cuales requieren la colaboración, en mayor o menor medida, de dos o más órganos administrativos.

Recientemente se ha puesto de manifiesto que la consolidación de los beneficios de las iniciativas de gobierno electrónico implantados depende, en gran medida, de las posibilidades de compartir información y recursos que se presentan entre diferentes niveles de la administración, sobre todo en aquellos entornos más descentralizados. Los proyectos de interoperabilidad todavía son el gran reto al que tiene que enfrentarse el sector público, puesto que los niveles de colaboración interorganizacional y confianza mutua que dichos proyectos requieren suelen estar condicionados por ajustes institucionales, estructuras organizativas y procesos de gestión que todavía motivan a trabajar aisladamente y fomentan la aparición de “islas” de trabajo. La implementación de este tipo de servicios requiere levantar muchas barreras y resolver complejos problemas tecnológicos, semánticos, organizativos, jurídico-normativos y culturales, entre otros.

El principio de interoperabilidad interadministrativo constituye el pilar sobre el que se sustenta la posibilidad de diseñar una Administración más inteligente, y eficiente en sus actuaciones. La interoperabilidad, en el contexto de las TIC, es la posibilidad de que dispositivos y sistemas tecnológicos hablen el mismo idioma. En lo estrictamente técnico, su relevancia recae en determinar las posibilidades de interconexión y transmisión de información entre dos o más partes; pero también confluyen en este la determinación precisa

de los términos de comunicación, la organización y el establecimiento de acuerdos o normatividad en la definición de estándares.

En Iberoamérica y otras regiones del mundo existen experiencias de interoperabilidad que trascienden más allá del ámbito técnico, en el que se produce la interacción e intercambio de datos entre sistemas según un método definido para contemplarse de manera más integral en esa capacidad o habilidad de trabajar u operar de manera sinérgica en la ejecución de las tareas o funciones de una o más unidades, secciones, organizaciones. Así pues, la interoperabilidad no es sólo una cuestión tecnológica. Parte, por un lado, de principios que tratan de la diversidad de componentes con la utilización de diversos productos de múltiples proveedores en diferentes organizaciones pero, además, tiene como objetivo la definición de políticas, normas y estándares para la consecución de la cooperación entre los sistemas de diferentes organizaciones públicas (Criado, 2010, p-5).

Se nos presentan en la región de Iberoamérica experiencias como en Chile que atiende una guía de servicios del Estado que ofrece a las personas una alternativa de fácil y cómodo acceso a la oferta de información y servicios disponibles en el sector público. Reúne más de 1 700 fichas con orientación sobre beneficios, programas y trámites, entre las que destacan más de 420 servicios que pueden realizarse a través de Internet. Se organiza la información en tres grandes canales: Personas, Empresas y organizaciones e Instituciones. Cada ficha informativa puede descargar el contenido en audio, formato mp3 por lo que las personas con alguna discapacidad visual acceden sin dificultades a la información. Posee 400 trámites en línea. Su motor de búsqueda está basada en tecnología Google SiteSearch, permite acceder de forma rápida a información relevante de más de 500 sitios web pertenecientes a organizaciones e instituciones del Estado Chileno.

El Portal de Uruguay es un sitio que organiza la información y trámites del Estado de forma que los ciudadanos tengan un único punto de entrada donde puedan informarse e interactuar con todos los organismos. Una de sus principales herramientas es (buscador.gub.uy) implementado en tecnología basada en Google. Brinda servicios de búsqueda de la mejor calidad, bajo estándares a los que los usuarios están habituados. En el portal se pueden comenzar trámites directamente sin necesidad de dirigirse al sitio del organismo, como resulta el caso de acceso a Uruguay Concurso, la ventanilla única de oferta laboral de la Administración Central.

El PSCE- pe es un portal considerado oficialmente la ventanilla única de servicios público del Estado en Internet. Cuenta con 36 753 trámites de 378 instituciones públicas. Proporciona

cerca de 270 servicios públicos en línea. Se creó con los objetivos de brindar información al ciudadano sobre los servicios del Estado desde un único punto de entrada en Internet, proporcionar servicios públicos en línea; desarrollar el GE y apoyar los esfuerzos del Estado para la simplificación administrativa y descentralización.

En Brasil el diseño de la Plataforma de Interoperabilidad por dominio-br resultó de una ardua discusión con el Ministerio de Planeamiento. La idea en este modelo fue definir plataformas por dominios de negocios, algunos de ellos son los dominios: social (salud, vivienda entre otros), educación, (educación, ciencia y tecnología) emprendimiento, empresa y gestión financiera del estado entre otros. No es obligatorio que cada dominio se separe, esto va a depender de los volúmenes de intercambio entre ellos y la complejidad de implementación.

Requiere de infraestructuras tecnológicas más pequeñas y adicionalmente el mayor volumen de intercambio de información se da al interior de un dominio, si bien existen intercambios entre dominios, estos son menores y por lo tanto se privilegia el intercambio dentro del dominio.

Por otra parte, este modelo permite que su puesta en marcha sea alineada con las prioridades de la política pública y del gobierno. Asimismo simplifica la integración vertical (gobierno central, gobiernos regionales y municipales), la mirada habitual en el diseño de estos procesos de intercambio de información son mirar más bien al estado en forma horizontal y por capas, perdiendo de vista el enfoque centrado en el ciudadano a la hora de rediseñar el proceso.

Colombia se nos presenta con su Modelo Integrado de Planeación y Gestión-co, con el fin de proporcionarle a la ciudadanía los bienes y servicios que necesitan y de atender oportunamente sus exigencias. Paralelamente a lo anterior y teniendo en cuenta las variadas solicitudes de información relacionadas con la gestión de las entidades, por parte de instancias de gobierno, surge la necesidad de armonizarlas en un instrumento metodológico y en una herramienta que facilite el registro de los avances de la gestión, como insumo para la evaluación y control de los resultados de las entidades de la Rama Ejecutiva del Orden Nacional.

### **Modelos Organizacionales de Gobernanza Digital en diferentes países**

| <b>Países</b>     | <b>Modelo</b>              | <b>¿En qué consiste?</b>   | <b>Pros</b>  | <b>Contras</b>   | <b>Marco Legal</b>  |
|-------------------|----------------------------|--|--|--|---|
| Estonia/<br>Chile | Gobernanza<br>centralizada | Un organismo central (Ministerio o agencia) coordina la transformación | <ul style="list-style-type: none"> <li>✓ Coordinación eficiente de políticas y recursos.</li> <li>✓ Estandarización</li> </ul> | <ul style="list-style-type: none"> <li>✓ Burocracia y lentitud en la toma de decisiones.</li> <li>✓ Menos interoperabilidad</li> </ul> | Leyes específicas de Transformación digital e interoperabilidad |

|                      |   |  |   |  |  |
|----------------------|---|--|---|--|--|
|                      |   | digital del país, regulando todos los servicios digitales, tecnologías y políticas a nivel nacional.   | zación de servicios y tecnologías.<br>✓ Fuerte control de seguridad y protección de datos.  | espacio para la innovación regional.<br>✓ Rígido ante cambios rápidos.   | d.<br>Ejemplo en Estonia: Ley de Identificación Electrónica, Ley de Archivos y Ley de Registro de la Población.                  |
| Inglaterra/Colombia  | Gobernanza basada en datos abiertos       | El gobierno publica datos accesibles a ciudadanos y empresas, fomentando la transparencia, innovación y el desarrollo de nuevas soluciones digitales a partir de esos datos. | <ul style="list-style-type: none"> <li>✓ Fomenta transparencia y rendición de cuentas.</li> <li>✓ Mejora la toma de decisiones basada en datos.</li> <li>✓ Impulsa la innovación.</li> <li>✓ Flexibilidad en la implementación.</li> <li>✓ Digitalización integral en múltiples sectores.</li> <li>✓ Alto nivel de inclusión digital.</li> <li>✓ Coordinación clara y flexible entre sectores.</li> </ul> | <ul style="list-style-type: none"> <li>✓ Requiere fuertes medidas de seguridad para proteger la privacidad.</li> <li>✓ Posibles problemas éticos en el uso de datos.</li> <li>✓ Capacidades desiguales para usar datos.</li> <li>✓ Conflictos de intereses entre sectores.</li> <li>✓ Duplicación de esfuerzos o recursos.</li> <li>✓ Riesgos de sobrecargar al sector privado con obligaciones regulatorias.</li> <li>✓ Desafíos en transparencia.</li> </ul> | Leyes de datos abiertos y transparencia. Ejemplos: Ley de Datos Abiertos en Reino Unido y Ley 1712 de Transparencia en Colombia. |
| Brasil/Finlandia     | Gobernanza Descentralizada                | Permite que autoridades locales implementen soluciones tecnológicas adaptadas a sus necesidades dentro de un marco regulador flexible del gobierno central.                  | <ul style="list-style-type: none"> <li>✓ Fomenta la innovación local y regional.</li> <li>✓ Adaptación rápida a necesidades locales.</li> <li>✓ Inclusión de áreas geográficas diversas</li> </ul>  | <ul style="list-style-type: none"> <li>✓ Falta de interoperabilidad entre sistemas</li> <li>✓ Dificultad de coordinación a nivel nacional</li> <li>✓ Puede generar desigualdades tecnológicas.</li> </ul>  | Normativas federales y locales. Ejemplo: Marco Legal de Gobierno Digital Descentralizado en Brasil.                              |
| México/Corea del Sur | Modelo Híbrido con Enfoque Multisectorial | Combina enfoques centralizados y descentralizados. Los sectores (salud, educación, transporte)   | <ul style="list-style-type: none"> <li>✓ Soluciones adaptadas a cada sector.</li> </ul>   | <ul style="list-style-type: none"> <li>✓ Complejidad de coordinación entre actores</li> </ul>  | Leyes sectoriales específicas. Ejemplo: Ley de Innovación Tecnológica en   |

|                   |  |  |   |  |   |
|-------------------|--|--|---|--|---|
|                   |  | desarrollan soluciones bajo un marco nacional, permitiendo la adaptación a sus necesidades.  |   |  | Corea del Sur.  |
| Singapur /Uruguay | Colaboración Público-Privada o Gobernanza Colaborativa | El gobierno colabora con empresas privadas para desarrollar e implementar proyectos de transformación digital, compartiendo recursos, infraestructura y conocimientos. | <ul style="list-style-type: none"> <li>✓ Aprovecha la experiencia y recursos privados.</li> <li>✓ Promueve innovación y eficiencia.</li> <li>✓ Reducción de carga financiera para el gobierno.</li> <li>✓ Fomenta la colaboración público-privada.</li> </ul> | <ul style="list-style-type: none"> <li>✓ Riesgo de priorizar intereses privados.</li> <li>✓ Posible falta de transparencia.</li> <li>✓ Contratos complejos y riesgos de corrupción.</li> <li>✓ Altos costos de implementación y burocracia.</li> </ul> | Regulado por marcos de asociaciones público-privadas (APP). Ejemplo: Ley de Concesiones en Uruguay. Leyes que fomentan la colaboración entre el sector público, privado y sociedad civil. Ejemplos: Ley 18331 de Protección de Datos Personales, Ley 18381 de Acceso a la Información Pública, y Ley 18600 de Documento Electrónico y Firma Electrónica de Uruguay. |

### ***CARACTERIZACIÓN DE PRÁCTICAS EXITOSAS DE INTEROPERABILIDAD EN SISTEMAS JURÍDICOS DE DIFERENTES PAÍSES***

Considerando que la mayor parte de las instituciones de un país iniciaron sus bases de datos digitales en programas que no conversaban entre sí -entre otras razones, porque no era el objetivo inicial, porque fueron construidas por diferentes proveedores, por razones de costos o idiosincrasia, etc.-, la transición hacia un sistema de datos públicos interoperable requiere de una estructura de gobernanza robusta y una planificación que permita a los actores el traspaso

a sistemas técnicos y semánticos. Estos últimos permiten una organización eficiente y un nivel de seguridad adecuado para el resguardo de la información.

Teniendo en cuenta lo anterior se hace indispensable definir que para esta investigación por sistemas exitosos se entenderá a aquellos que han sido implementados por otros países e instituciones sin presentar problemas en su evolución y desarrollo, cuentan con una metodología ya escrita sobre su funcionamiento, así como la puesta en marcha, en orden cronológico, de los diferentes momentos y procesos. Además, en la actualidad se implementan de forma generalizada a nivel mundial.

En particular, el “Modelo de implementación de la interoperabilidad gubernamental” fue desarrollado por el Instituto Latinoamericano y del Caribe de Planificación Económica y Social (ILPES), en el contexto del proceso de asistencia técnica al Gobierno de Costa Rica a través del Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) de España.

En un informe de CEPAL (Naser y Concha, 2011), el gobierno electrónico “es un concepto de gestión que fusiona la utilización intensiva de las TIC, con modalidades de gestión, planificación y administración, como una nueva forma de gobierno”, y su implementación supone un cambio de paradigma para todas las entidades que forman parte la administración pública.

Autores como Rantanen (2019) y Finger (2003), ligan el concepto de gobierno electrónico al de gobernanza electrónica o e-gobernanza. Rantanen, citando a Calista y Melitski, distingue estos términos como distintos pero complementarios. La gobernanza electrónica tiene en cuenta el empleo de la web e Internet para examinar la forma en que el Estado lleva a cabo sus gestiones democráticas utilizando las interacciones en red con los ciudadanos para impulsar la transparencia y la participación.

En este sentido, se define gobernanza digital como “la articulación y concreción de políticas de interés público con los diversos actores involucrados (Estado, sociedad civil y sector privado), con la finalidad de alcanzar competencias y cooperación para crear valor público y la optimización de los recursos de los involucrados, mediante el uso de tecnologías digitales”. (CEPAL/AECID, 2021, p-14)

En cambio, el gobierno electrónico, “proporciona servicios gubernamentales por vía electrónica, normalmente a través de la web, para reducir el carácter físico de las transacciones de los clientes recreándolas virtualmente” (Rantanen, 2019). En conclusión, el gobierno electrónico es un sistema de servicios digitales para la ciudadanía, y para su

implementación se requiere un conjunto de medidas que, por un lado, permitan el paso desde el gobierno “tradicional” al electrónico, y por otro, regulen la gestión de la democracia utilizando tecnologías de información y comunicación.

Para la implementación de lo anterior Rantanen propone un “ecosistema de gobierno electrónico”, el cual se define como “un sistema sociotécnico complejo que incorpora a ciudadanos, organizaciones, empresas y organismos gubernamentales, y que utiliza plataformas electrónicas para crear y distribuir valor a sus participantes.” (Rantanen, 2019).

La propuesta de este grupo de investigadores permite visualizar que la implementación de un sistema de gobierno electrónico supone tomar en consideración, no sólo los sistemas tecnológicos dentro del aparato público, sino la mirada de la ciudadanía, de organizaciones civiles y privadas, y del propio Estado, donde el foco final es la una gestión pública más eficiente, que entregue mejores servicios a la ciudadanía y que mejore los procesos democráticos.

En términos generales, puede afirmarse que los beneficios de la interoperabilidad tienen que ver con cuestiones relacionadas con los objetivos que pretenden alcanzar los programas de gobierno electrónico entre los que se incluyen operaciones y servicios gubernamentales altamente ágiles, centrados en el ciudadano, responsables, transparentes, efectivos y eficientes. Para el logro de dichos objetivos, es vital, la integración de recursos gubernamentales de información y procesos, y por tanto la interoperación de sistemas de información interdependientes. Los sistemas de información necesitan comunicarse e intercambiar información para lograr mayor productividad (Galliers, 2006). A través de los avances de la tecnología en comunicación de computadores se logra interconectar esos sistemas, pero eso no es suficiente para lograr la capacidad de mejora deseada.

En el sector jurídico existen experiencias satisfactorias donde se ha logrado interoperabilidad entre los sistemas de información. Han sido visibles los avances en el área de la actividad registral para lograr la vinculación de los sistemas de gestión de Registro Civil y Estadísticas Vitales (CRVS) y de gestión de identidad, perteneciente al Centro Internacional de Investigaciones para el Desarrollo (IDRC), auspiciado por el Departamento de Asuntos Globales de Canadá.

La vinculación de los sistemas CRVS y de gestión de identidad transformó la forma en que los gobiernos que lo asumieron, prestan servicios y empoderan a su población. Estos países desarrollaron sus sistemas desde puntos de partida diversos y con rumbos muy variados.

En 2015 se crearon el Centro de Excelencia para los Sistemas de Registro Civil y Estadísticas Vitales en el Centro de Investigación de Desarrollo Internacional (IDRC) y el Global Partnership for Sustainable Development Data (GPSDD). En este marco se unieron los líderes del mundo para hacer frente a la necesidad de promover el desarrollo sostenible y fomentar una vida digna para todos derecho de las personas a ser reconocidas legalmente, a contar con un registro de su nacimiento, defunción y otros hechos vitales para proteger sus derechos fundamentales, a facilitar el acceso a los servicios sociales, y a participar de la vida política y económica.

Como está consagrado en la Declaración Universal de Derechos Humanos, todos los individuos tienen derecho a ser reconocidos ante la ley, y los estados tienen la obligación de crear marcos legislativos que sean reconocidas por el estado. El estado civil incluye un conjunto de elementos que individualizan a una persona natural como titular de derechos y obligaciones, y ayudan a establecer la posición legal de una persona natural en una familia y en una sociedad. A través de los elementos del estado civil, uno puede establecer si una persona está casada soltera o divorciada, si nació o no dentro de lo sí fue adoptada, así como si al fallecer, su capacidad como titular de derechos y obligaciones ha cesado. El estado civil se basa en los vínculos resultantes de la paternidad, la relación y/o el matrimonio. El elemento esencial del estado civil es la posición legal de una persona natural en relación con su familia.

En la actualidad aproximadamente el 50 por ciento de las defunciones en el mundo no están registradas. Y en aquellas que sí lo están, la causa de muerte a menudo no se registra ni se codifica adecuadamente. El registro de otros eventos vitales, como el matrimonio o el divorcio, es igualmente insatisfactorio y afecta la capacidad de las personas para ejercer una serie de derechos humanos, con consecuencias particularmente negativas para las mujeres y sus derechos derivados del estado civil registrado.

La expansión de la identidad digital la gobernanza electrónica y la tecnología biométrica han aumentado rápidamente el interés y a inversión en sistemas de identidad por parte de gobiernos socios de desarrollo y actores del sector privado. El subregistro de hechos vitales de un gran porcentaje de la población crea desafíos adicionales para los gobiernos que aún tienen que decidir cómo reformar y fortalecer sus sistemas de registro civil y estadísticas vitales (CRVS, por sus siglas en inglés) y sus sistemas de gestión de identidad. También existe una falta de comprensión y orientación sobre cómo deben vincularse los sistemas de registro civil y gestión de identidad.

En muchos países esto es consecuencia de la debilidad de los sistemas de registro civil, que carecen tanto de oferta como de demanda, por parte de la población, de servicios de registro y gestión de identidad. Además, los procesos tradicionales en papel se están trasladando al ámbito digital, lo que obliga a las autoridades a repensar y rediseñar los procesos internos vinculados al registro de información de identidad y a la emisión de credenciales de identificación.

Un enfoque holístico del registro civil y las estadísticas vitales y la gestión de la identidad integra o fortalece la cooperación entre estos elementos a través de un marco legal propicio y arreglos institucionales efectivos, asegurando el registro universal de la identidad desde el nacimiento hasta la muerte. La interoperabilidad técnica ha proporcionado una serie de beneficios para garantizar que todas las categorías población desde el nacimiento hasta la muerte reflejen su información de identidad en el sistema.

La interoperabilidad digital entre el registro civil digitalizado y los sistemas de gestión de identidad automatizan estos procesos, eliminando la necesidad de que los ciudadanos inviertan su tiempo y dinero para comunicar información entre las autoridades interesadas. La eficiencia resultante en el intercambio de datos no solo contribuye a ahorrar costos para los ciudadanos, sino que también contribuye a una mejora considerable de los procesos generales de gobernanza.

Algunos países han introducido el uso de números de identificación únicos (NIU), que se asignan a cada ciudadano como un requisito obligatorio de acuerdo con la ley pertinente. Las bases de datos de identidad y registro utilizan este identificador para buscar de manera eficiente todos los registros pertenecientes a una persona específica.

#### Modalidades de implementación y arreglos institucionales

Existen experiencias de implementación de diversos países en cuanto a los arreglos institucionales, Entre los enfoques más simples, los registros civiles se agregan en un registro civil central y se implementan como una base de datos electrónica que es interoperable con la base de datos de gestión de identidad. En países como Ecuador, Kirguistán, Namibia y los Países Bajos, estos se integran en un sistema que funciona como un registro digital de población nacional que almacena o se enlaza con la biometría personal.

Al reconocer los beneficios de agregar diferentes tipos de información personal, los registros de población en algunos países se han ampliado para incluir otros tipos de datos personales requeridos por el gobierno para la prestación de servicios, tales como ciudadanía, residencia,

derecho al voto y otra información. Estos sistemas pueden implementarse como una arquitectura de base de datos coherente, o como un sistema de bases de datos interconectadas e interoperables, a menudo en diferentes ubicaciones y operadas por diferentes autoridades.

Por ejemplo, en Armenia, el registro civil digitalizado está bajo la autoridad del Ministerio de Justicia, mientras que el registro de la población está bajo la autoridad de la policía, que también es responsable de la gestión de la identidad cada vez que se registra un nuevo evento vital en el registro civil, la información se comunica digitalmente a la policía, donde se utiliza para actualizar el registro persona en el registro de la población. En el caso del registro de nacimientos los funcionarios de registro pueden acceder a todos los datos necesarios para el registro de nacimientos, tales como los datos sobre la madre del niño, el sexo del niño, la hora de nacimiento y la cantidad de niños nacidos, a través del sistema electrónico de certificados médicos.

En Perú, donde tanto el registro civil como la gestión de la identidad son responsabilidad de una sola autoridad, la plataforma digital se basa en dos bases de datos: un registro civil digitalizado y un sistema de gestión de identidad digitalizado. El sistema de registro civil digitalizado está diseñado como una base de datos de registros escaneados de eventos vitales. Cada registro digitalizado también contiene el NIU de la persona, lo que permite a los operadores del sistema buscar todos los eventos vitales registrados vinculados a esa persona. El sistema de gestión de identidad también puede buscar esta información en la base de datos del registro civil cada vez que una persona solicita una tarjeta de identidad.

Cada vez que se registra y digitaliza un nuevo evento vital, se comunica al sistema de gestión de identidad, y los operadores serán notificados de este cambio cada vez que la persona vuelva a solicitar un documento de identidad. En Kirguistán, la información de identidad del registro de tarjetas de identificación nacionales y la información de la dirección del registro de residentes han permitido que el Sistema de Registro Estatal desarrolle una aplicación que puede extraer e imprimir listas de votantes directamente desde un registro único de la población en correspondencia con los límites predeterminados de los colegios electorales.

En los Países Bajos, por ejemplo, una vez que se inscribe en el registro de población la información proveniente de las actas de registro civil, este registro digital es prueba suficiente de los hechos vitales registrados, y está disponible para el acceso por parte de todas las autoridades de la administración pública y proveedores de servicios. Como la información ya está disponible en línea, los certificados de nacimiento en papel no se proporcionan al completar el registro de nacimiento y sólo se pueden emitir si se solicitan específicamente.

Los sistemas digitalizados para el registro civil no tienen por qué ser creados para atender únicamente el registro de eventos vitales. En muchos países, estos sistemas se han ampliado para cubrir notificaciones de nacimientos y defunciones en centros médicos con la introducción de un software especializado que es una extensión de la plataforma principal de registro civil digital en las instalaciones médicas para garantizar que los datos esenciales sobre la identidad del niño, tales como la fecha de nacimiento y el lugar de nacimiento, sean capturados inmediatamente después del nacimiento, así como información médica relevante para la compilación de estadísticas vitales.

El registro civil y los sistemas de gestión de identidad se han convertido en el principal proveedor de datos de identidad para los procesos de gobernanza. Se utilizan no solo para la inscripción en servicios específicos, sino también para evaluar cómo debe cambiar el acceso a los servicios a medida que cambian las características de la identidad. El matrimonio y el divorcio son eventos que generalmente afectan una variedad de derechos. Pero el desencadenante más común para los cambios en la prestación de servicios es el registro de defunción. Existe una gama de servicios gubernamentales que dependen de la comunicación oportuna de actualizaciones en los datos de identidad.

En este contexto y sobre los sistemas interoperables Europa se encuentra en la avanzada. Algunos países ya implementan la interoperabilidad jurídica en el ámbito de la contratación pública, en dicho funcionamiento tienen establecidas las normas que rigen dicha actuación. En tal sentido exponen la importancia de la interoperabilidad como principio jurídico propio del funcionamiento de la administración electrónica, a la vez que analizan los diferentes elementos regulatorios contenidos en el ordenamiento. Valoran como fundamental que los medios electrónicos habiliten vías de automatización y utilización de herramientas basadas en el Bigdata. (Sánchez, 2022).

En igual continente un grupo de especialistas, desarrollan una investigación enmarcados en un proyecto I+D+i titulado “Ejes de la justicia en tiempos de cambio”. Una de las aristas que analizan es la interoperabilidad de sistemas de gestión procesal y debido proceso, así como las experiencias a nivel nacional y europeo para alcanzar una verdadera digitalización de la justicia. (Llorente, 2022).

Este estudio refiere que el objetivo de la interoperabilidad es y ha sido una constante en los últimos años, puesto que el legislador es consciente que asegurar una verdadera interconexión de datos entre administraciones públicas hace que se refuercen los niveles de transparencia y seguridad, así como un reforzamiento de las garantías procesales constitucionales. Por tanto,

una plena interoperabilidad asegura cumplir el imperativo constitucional de ofrecer un proceso con todas las garantías. (Llorente, 2022).

Para el investigador español Eduardo Gamero la interoperabilidad es el desafío más importante que se le plantea a la gestión de la administración pública en la primera mitad del presente siglo XXI. Este autor define la necesidad de mantener marcos obligatorios de interoperabilidad al mayor nivel territorial posible. (Gamero, 2009).

Otro investigador europeo llamado Enrique Alonso García, realiza un análisis de la categoría Interoperabilidad legal, llegando a la conclusión de que existe esta cuando: las condiciones de uso se pueden determinar claramente y con rapidez y facilidad para cada uno de los datos, listado de datos y bases de datos; las condiciones jurídicas para su uso que impone cada dato, listado de datos y bases de datos permitan la creación y uso de productos combinados o derivados y los usuarios pueden acceder legalmente y utilizarlos. (Alonso, 2016).

Desde la región latinoamericana el investigador Raimundo Roberts realizó un estudio de la regulación que sobre sistemas de interoperabilidad tienen países como Costa Rica, la provincia de Neuquén en Argentina y Estonia. Concluyó que el desarrollo de sistemas de interoperabilidad para la gestión del gobierno electrónico es un elemento fundamental para el uso de la información entre los servicios que se brindan y comprende dos elementos fundamentales: por un lado, una estructura que armonice la gobernanza, la legislación, las capacidades técnicas, su seguridad y la atención a la ciudadanía; y por otro un plan de modernización de un sistema de administración pública analógico, con un sistema de información estancos, a un sistema de administración pública digitalizado, conectado y robusto. (Roberts, 2023).

Alejandra Naser en su obra *Gobernanza Digital e interoperabilidad gubernamental: una guía para su implementación* ofrece aspectos metodológicos a tener en cuenta en el diseño de un sistema interoperable gubernamental, en este caso en particular se basa en la asistencia prestada al Ministerio de Ciencia Tecnología y Telecomunicaciones de Costa Rica. (Naser, 2021).

Por su parte, Carlos Jiménez en su artículo *Interoperabilidad en la administración de justicia: experiencias y buenas prácticas en un ámbito complejo*, plantea que uno de los pilares fundamentales de la modernización tecnológica es la interoperabilidad, en cuanto contribuye decisivamente en garantizar el funcionamiento armónico y cohesionado de los distintos

sistemas, organizaciones, procesos y aplicaciones existentes que en el ámbito de la justicia son numerosos dada la variedad de actores implicados. (Jiménez, 2010).

Otros investigadores relacionados con el Derecho plantean que con la llegada de las tecnologías de la información se les impone importantes transformaciones en las actividades y labores que hasta el momento realizaban, simplificándolos considerablemente, si se aprovecha al máximo las bases de datos y el trabajo con estos, facilita a los profesionales la oportunidad de ser mucho más eficientes y de disponer de más tiempo para dedicarse a asuntos relacionados con el conocimiento y los equipos de trabajo. Aunque, recomiendan reflexionar sobre el marco jurídico más adecuado teniendo en consideración que se trata de información sensible de la que es obligación, tanto ética como legal, hacer un uso responsable (Huapaya, 2022).

La interoperabilidad en el contexto cubano permite comprender cómo se pueden superar las barreras tecnológicas y regulatorias, para lograr una integración efectiva de los sistemas de información en un entorno centralizado. El Esquema Nacional de Interoperabilidad Cubano (ENIC v 3.0) tiene como objetivo principal soportar la estrategia de Cuba de proveer servicios digitales centrados en el ciudadano, facilitando la interoperabilidad de servicios y sistemas entre administraciones públicas, así como entre administraciones y el público (ciudadanos y empresas), a nivel nacional. Este crea las condiciones necesarias para garantizar el adecuado nivel de interoperabilidad técnica, semántica y organizativa de los sistemas y aplicaciones empleados en el país, que permita el ejercicio de derechos y el cumplimiento de deberes a través del acceso a los servicios públicos digitales, a la vez que redundando en beneficio de eficacia y eficiencia del gobierno digital (Jhones, Fernández, & Estrada, 2022).

Aunque en la actualidad restan una cantidad importante de problemas por resolver en materia de interoperabilidad, ya hoy se puede contar con un procedimiento que servirá como material de consulta a las entidades cubanas entre las que destaca el Ministerio de Justicia, inmersas en el proceso de transmisión y recepción de información, además de notificar o gestionar sucesos; así como exportar e importar datos.

En el caso de nuestro país uno de los aspectos importantes en la transformación digital es desarrollar de manera funcional y constante el Gobierno electrónico como uno de los proyectos a ejecutar para implementar el Plan de Desarrollo 2030 con un enfoque en la relación Gobierno-ciudadanía con un gobierno digital más eficiente, eficaz y transparente que revolucione la administración pública. (Figueredo, 2017; Puig, 2019; Antón, 2019; Danet,

2020; Puig, 2021; Wolpes, 2022; Brito, 2022; Rodríguez, 2022, Morales, 2022; Perera, 2023; Antón, 2024).

En el 2022 un grupo de investigadores encabezados por Allan Pierra Fuentes pertenecientes al Parque Científico Tecnológico de La Habana y a la Universidad de las Ciencias Informáticas desarrollaron un estudio titulado “Principios para el desarrollo, uso y aplicación de las TIC en el Gobierno” con el objetivo de proporcionar un instrumento y realizar una evaluación equilibrada de las perspectivas que ofrece el uso del software libre y de código abierto dentro de la administración pública, utilizando el análisis sociotecnológico en las condiciones histórico concretas de Cuba.

Como resultado propusieron cuatro principios que resumen en el modelo de las Cuatro S: Seguridad, Soberanía Tecnológica, Socio-adaptabilidad y Sostenibilidad. Plantean que estos principios no contradicen los criterios de código abierto, ni sustituyen las cuatro libertades del movimiento del software libre, sino que sumados a estas pretenden contribuir al necesario proceso de transformación digital, vista como una continuidad de la informatización de la sociedad, que busca poner la tecnología en función del desarrollo humano y del mejoramiento de la calidad de vida de la población. Este trabajo propone un marco para analizar las condiciones para la adopción del código abierto en las organizaciones del sector público en Cuba. (Pierra, 2022).

Otro elemento que ponen de relieve es que en Cuba predomina la percepción, por parte de las autoridades del país de que no puede apostarse por el software propietario como un camino viable para el desarrollo tecnológico, y que a la vez conduzca a la independencia en este mismo ámbito. Factores económicos de obtención de licencias, de adquisición de software propietario a través de internet y la posibilidad latente de reclamaciones por parte de algunos fabricantes, entre muchas otras complejidades, conduce a optar por otra modalidad de software, menos atados a restricciones legales y más accesible desde el punto de vista económico. (Pierra, 2022).

La Plataforma Articulada para el Desarrollo Integral Territorial (PADIT), de conjunto con otras organizaciones extranjeras y del país una Guía para la Gestión del Gobierno Digital en los municipios cubanos, pone énfasis en la transparencia, la participación popular, la rendición de cuentas y la gestión eficaz del gobierno en los territorios. Apunta hacia una perspectiva transversal de la tecnología acentuando la transformación global de culturas de trabajo, prácticas, propósitos y dispositivos tecnológicos a partir de su digitalización, así como su articulación en redes socio técnicas y con un enfoque de innovación.

En el Derecho algunos investigadores sostienen que desde el llamado Derecho cibernético debe ser entendido como un sistema de normas coherentes que alcancen por una parte, a las relaciones jurídicas, cuyo objeto se refiere a bienes y servicios tecnológicos, y por otro, a aquellas relaciones jurídicas donde se emplean esos medios en alguna de las etapas de su realización, con independencia de la consideración de su objeto, pudiendo ser un bien o servicio en el ámbito de lo digital o no (Frosini, 1968; Pérez Luño, 1978, 2009; Correa, 1987; Tellez, 2018; Jover, 2019, Citados por Amoroso, 2022, p-23).

“La cibernética y sus ramificaciones (por ejemplo, la informática, la robótica, la automática y la Inteligencia Artificial), al trascender como herramientas al ámbito jurídico, ayudan a comprender cuál sería el nuevo estado de existencia y si es necesario que así sea, porque lo cierto es que el Derecho que se ha construido y ha llegado hasta nuestros días, se erige sobre una cultura de papel, y hoy la sociedad tiene necesidad de responder a las exigencias de la transformación digital, signada por el desarrollo de cualquier relación social y mediada por las tecnologías digitales que necesitan desarrollarse en un ámbito de relaciones de confianza y seguridad jurídica” (Amoroso, 2022, p-25).

Para Amoroso, (2022) es creciente el reto que imponen las tecnologías disruptivas al Derecho, las cuales a su vez deben ser asimiladas en los entornos jurídicos, porque pueden aportar una infraestructura para la integración completa de la administración electrónica, como modo natural del funcionamiento de esta con la debida seguridad jurídica en el tráfico documental, ampliándose además el universo de derechos y convirtiéndose en herramientas perfectas para potenciar principios básicos que rigen el funcionamiento de la Administración Pública y la eficacia. Se impone que se vean estos fenómenos como de Derecho, más allá de una denominación específica que solo viene a adjetivarlo para aludir a un segmento normativo del orden jurídico, que sirve como marco regulador para el empleo de las TIC, cuando lo necesario es legislar cada vez desde la perspectiva holística y sistémica, para abordar estos temas desde una mirada humanista.

En el MINJUS también se avanza en la informatización camino a la transformación digital y la creación de un sistema interoperable, al respecto tenemos:

- La Ficha Única del Ciudadano (FUC), como mecanismo de identificación se encuentra en uso o en habilitación en 62 entidades.
- Se trabaja en el Sistema Único de Identidad Nacional (SUIN).

- El 99% de las oficinas del Registro del Estado Civil, brindan servicios digitales desde el entorno de internet.
- Digitalizado el 99% del registro de las familias cubanas vulnerables y el 96% del de consumidores.
- Se amplía el uso de mecanismos de opinión y aclaración de temas por vías digitales.

Uno de los países con mayor éxito en cuanto a sistemas interoperables en general y en los sistemas jurídicos en particular es Estonia. Sobre esta metodología se ampliará en el objetivo siguiente, ya que sirvió de base para identificar los presupuestos necesarios para desarrollar un ecosistema de interoperabilidad en el MINJUS.

***EXPERIENCIAS LEGISLATIVAS EXISTENTES A NIVEL INTERNACIONAL ACERCA DE LAS RELACIONES DE INTEROPERABILIDAD ENTRE SISTEMAS DIVERSOS.***

El año 2010 marcó un momento importante para la consolidación de proyectos de interoperabilidad en la región Iberoamericana con la creación del Centro Latinoamericano de Administración para el Desarrollo (CLAD) encargado de la elaboración del llamado Marco Iberoamericano de Interoperabilidad (MII). Dicho Marco se erigió como un mecanismo que ordenara la producción de conocimiento en materia de interoperabilidad y se constituiría en una guía en la que los países iberoamericanos pudieran apoyarse para la toma de decisiones relacionadas con la colaboración entre Estados en este ámbito.

Existe cierta experiencia acumulada en relación con proyectos de interoperabilidad intra administrativa, horizontal o, incluso, vertical, en cambio no ocurre lo mismo en el ámbito de la interoperabilidad entre administraciones de diferentes países. En este campo, el paradigma de colaboración lo constituye la Unión Europea, que ya en el año 2004 publicaba su Marco Europeo de Interoperabilidad y en el 2010 presentó su segunda versión.

En Iberoamérica, no hay prácticamente precedentes de iniciativas de interoperabilidad entre países, siendo los más consolidados el Acuerdo Complementario al Acuerdo de Cooperación Técnica entre el Gobierno de la República Argentina y el Gobierno de la República Federativa del Brasil para la Implementación del Proyecto “Interoperabilidad de Gobierno Electrónico”, suscrito por ambos Estados en febrero de 2008, y el Convenio de Colaboración para la Prestación de Servicios de Validación de los Certificados Electrónicos de España y Portugal, cuya firma tuvo lugar en septiembre de 2009.

La ausencia de proyectos de estas características en la región y, por tanto, la consecuente necesidad de contar con una guía que pautara el actuar de los países en este campo dio lugar, en septiembre de 2007, a la publicación del llamado Libro Blanco de interoperabilidad de gobierno electrónico para América Latina y el Caribe. Su objetivo era programar una serie de actividades prioritarias que aseguraran, en un corto tiempo, contar con un entorno y una plataforma de interoperabilidad regional eficientes, que potenciaran el crecimiento con equidad de los países dentro de mercados ampliados, con seguridad jurídica, en un ambiente de convergencia de normas y disciplina, así como también, de avances en infraestructura y conectividad (CEPAL, 2007).

A pesar de constituir un importante aporte, el Libro Blanco no profundizaba en algunas cuestiones y presentaba, sobre todo, deficiencias en relación con la interoperabilidad organizativa, la gobernanza de la interoperabilidad y la evaluación de las iniciativas de interoperabilidad. Por ello, a principios del año 2010, el CLAD encarga la elaboración de un Marco Iberoamericano de Interoperabilidad (MII), que definiera fundamentos básicos, aceptados colectivamente, para facilitar que los gobiernos y administraciones públicas de la región, sea cual sea su nivel y tipo de relación, puedan colaborar, si así lo desean, en el uso de las tecnologías de la información y las comunicaciones para mejorar su desempeño, ofrecer nuevos servicios públicos o reforzar los procesos de gobernanza de las políticas públicas que implican a dos o más Estados.

En la XII Conferencia Iberoamericana de Ministros de Administración Pública y Reforma del Estado (Buenos Aires, 1 y 2 de julio de 2010), se presenta como propuesta el documento del MII, pero éste se aprueba con el título de “Bases para una Estrategia Iberoamericana de Interoperabilidad”.

Estas Bases definen la interoperabilidad como la habilidad de organizaciones y sistemas dispares y diversos para interactuar con objetivos consensuados y comunes y con la finalidad de obtener beneficios mutuos. En este sentido, la interacción implica que las organizaciones involucradas compartan información y conocimiento a través de sus procesos de negocio, mediante el intercambio de datos entre sus respectivos sistemas de tecnología de la información y las comunicaciones (Criado, Gascó y Jiménez, 2010). Así pues, en el contexto de las Bases, la interoperabilidad no es sólo una cuestión tecnológica. Parte, por un lado, de principios que tratan de la variedad de componentes con la utilización de diversos productos de múltiples proveedores en diferentes organizaciones; pero, además, tiene como objetivo la

definición de políticas, normas y estándares para la consecución de la cooperación entre los sistemas de diferentes organizaciones públicas.

En particular, la segunda parte de la primera década de este siglo ha servido como punto de arranque para la mayoría de las actuaciones de los países de la región de cara a mejorar la colaboración intergubernamental. De hecho, durante los dos últimos años se han producido la mayor parte de las normativas en los países de la región. A su vez, en aquellos casos en que todavía no se puede dar por comenzada una estrategia de interoperabilidad, se ha mostrado una nítida voluntad de emitir actuaciones en breve lapso de tiempo e, incluso, algunos países dan cuenta de que se encuentran en proceso de discusión dentro del ejecutivo o el legislativo.

Los países iberoamericanos que incursionaron en el mundo de los sistemas interoperables han aprovechado, en la medida de lo posible, documentos y marcos de interoperabilidad ya elaborados por otros, tanto dentro como fuera de la región. Los referentes más utilizados han sido el Libro Blanco de Interoperabilidad ya mencionado y el Marco Europeo de Interoperabilidad. En relación con los marcos ya elaborados u otros documentos de país, han sido utilizados como referentes la información elaborada por: Brasil, Chile, España y Colombia; mientras que los referentes externos han sido: Reino Unido, la Unión Europea y Canadá. Como se observa, la necesidad de encontrar referentes en la región es clara, tanto por lo que respecta a documentos de alcance general (el Libro Blanco) como a instrumentos desplegados por otros países iberoamericanos.

En relación con las posibilidades que un Estado tiene respecto de la aplicación de estándares abiertos que garanticen la interoperabilidad, el Gobierno de Chile ha incorporado en las propuestas programáticas de la nación en materia tecnológica, un concepto denominado imparcialidad tecnológica informada, que el autor Francisco Salas define como: “la política pública que busca lograr, entre otras cosas, la interoperabilidad de sistemas informáticos y el acceso ciudadano a los servicios del gobierno electrónico mediante la adquisición de productos que incluyan estándares abiertos, pero procurando siempre respetar al máximo los principios jurídicos de igualdad, no discriminación y libre competencia entre diferentes tecnologías y programas informáticos” (Salas, 2007). Según este autor la imparcialidad tecnológica informada es un estadio superior al principio de neutralidad tecnológica; a pesar de lo anterior, el tratamiento que algunos autores dan a este último postulado, se inspira en instrumentos normativos europeos como por ejemplo la Ley 11/2007, de Administración Electrónica en España, que incorpora en su concepción el derecho de accesibilidad y la utilización de estándares abiertos para alcanzar la neutralidad tecnológica (Acero, 2009). En

un sentido similar, la ley suprema de Costa Rica establece una definición de neutralidad tecnológica en el artículo 2 inciso a) del Proyecto de Ley de la República de Costa Rica).

El tema de la utilización de estándares abiertos como mecanismo para fomentar la interoperabilidad sirve como estandarte para fundamentar el principio de imparcialidad tecnológica informada, pues en él se conjuga adecuadamente la neutralidad tecnológica, entendida como “la aplicación del principio de igualdad (y los que de él se derivan) en las contrataciones públicas que garantiza a los participantes que el Estado no se inclinará o favorecerá una tecnología en particular sobre otra al momento de demandar o decidir la adquisición de un bien o servicio” (Salas 2007, p.204), aspecto de suma importancia pues la provisión de equipo y aplicaciones tecnológicas definirá las grandes líneas que sobre la materia siga la Administración Pública en el rediseño de sus procesos y la prestación de los servicios públicos electrónicos.

A lo anterior se suma la aspiración máxima de acceso a la información pública por los usuarios y el intercambio interoperable de estos datos entre administraciones, ciudadanos y el sector productivo, lo cual sólo es alcanzable cuando el factor determinante en el abastecimiento de bienes y servicios tecnológicos lo constituye el libre acceso y la interoperabilidad.

De conformidad con el planteamiento anterior, una correcta política pública de Gobierno Electrónico que considere entre sus principios la imparcialidad tecnológica informada, incorporará acciones que propendan a fomentar la interoperabilidad a través del uso de estándares abiertos.

A continuación, la tabla contiene algunos de los países que cuentan con leyes o regulaciones para garantizar sistemas de interoperabilidad más seguros.

| PAÍSES  | LEYES   | ELEMENTOS DE INTERÉS   |
|---------|---|--|
| Estonia | <p><b>Ley de Archivos:</b> Estipula los principios para recopilar, evaluar, archivar, preservar y acceder a los documentos archivados, así como el reglamento general para las actividades de archivo. Además, establece las pautas para los registros privados introducidos en el registro de archivos y para su transferencia de propiedad. La Ley de Archivos se aplica a los documentos electrónicos y a los documentos en cualquier otra presentación.</p> <p><b>Ley de Registro de Población:</b> Establece los principios para uno de los principales fundamentos de una sociedad digital: el código único de identificación</p> | <p>Los expertos argumentan que se debe evitar el exceso de regulación en temas digitales.</p> <p>Tener demasiadas leyes especiales puede ser un obstáculo para el desarrollo de las tecnologías, las cuales están en un proceso de renovación continua. Sin embargo, sí recomiendan que la identificación electrónica y las firmas digitales cuenten con una regulación especial, de forma que</p> |

|  |  |  |
|--|--|--|
|  | <p>personal. De conformidad con esta ley, el código de identificación de Estonia es un código único de 11 dígitos, de por vida y obligatorio para todas las personas que trabajan y viven en Estonia, incluidos los e-residentes. El código de identificación es un elemento fundamental del proceso de autenticación electrónica. Además de emplearse en las transacciones electrónicas, se utiliza en todos los demás contextos donde es necesaria la identificación personal, es decir, cada persona tiene su propio código único.</p> <p><b>Ley de Identificación Electrónica y Servicios de Confianza para las Transacciones Electrónicas:</b> Regula la identificación electrónica y los servicios de confianza para las transacciones electrónicas, y la organización de la supervisión estatal hasta donde no están regulados por el Reglamento de la UE 910/2014 relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior (eIDAS). Este reglamento reemplazó la Directiva de la UE 1999/93/EC, y debido a este cambio en la legislación europea, la legislación de Estonia también cambió. Los reglamentos de la UE son directamente aplicables en todos los Estados Miembros. Por tanto, el principal acto legal que otorga estatus legal a las firmas digitales y que estipula los requisitos para tales firmas y servicios de confianza que los garantizan es ahora el Reglamento de la UE, y la legislación nacional se encarga de cualquier problema pendiente.</p> <p><b>Ley de Información Pública:</b> La Ley de Información Pública abarca a las agencias gubernamentales nacionales y locales, y a otras entidades legales tanto de derecho público como privado, que son responsables de la prestación de servicios públicos en áreas tales como educación, salud y servicios sociales u otros servicios públicos. Las personas tienen derecho a realizar consultas y los titulares de la información relevante tienen la obligación legal de responder. Además, están obligados a mantener los sitios web y a publicar información relevante en línea. Estas entidades deben asegurarse de que la información no esté “desactualizada, sea inexacta o engañosa”. Actualmente, esta ley también regula el área temática que antes estaba cubierta por la extinta Ley de Bases de Datos. Desde la perspectiva de la e-gobernanza, la Ley de Información Pública regula: La gestión del sistema nacional de información (responsabilidad de la Autoridad del Sistema de Información). La capa de intercambio de datos del sistema de información X-Road (cuyos detalles se encuentran en el reglamento de X-Road). Las medidas de seguridad para otros sistemas de información.</p> <p><b>Ley de Documentos de Identidad:</b> Esta ley establece un documento de identidad obligatorio y regula la</p> | <p>las firmas electrónicas y los documentos electrónicos sean válidos incluso como prueba en los tribunales.</p> <p>También señalan que es importante formular normas para la protección de datos, puesto que los datos electrónicos se perciben como menos seguros y esta percepción puede ser un obstáculo para la adopción de las transacciones electrónicas.</p> |
|--|--|--|

expedición de documentos de identidad a ciudadanos y extranjeros por parte de la República de Estonia. Además de otras funciones, el documento de identidad también se puede utilizar para realizar transacciones electrónicas, como se explicó anteriormente.

**Ley de Protección de Datos Personales:** La ley protege los derechos y libertades fundamentales de las personas en el curso del procesamiento de sus datos personales. La supervisión independiente y las disposiciones claras con respecto a la responsabilidad del procesamiento de datos son los fundamentos del sistema de protección. En mayo del 2018 entró en vigor el nuevo Reglamento de la UE 2016/679, el Reglamento General de Protección de Datos (GDPR por sus siglas en inglés). Es directamente aplicable y reemplazó partes de la ley nacional existente de protección de datos. A finales del 2018 entró en vigor una nueva ley nacional para regular los asuntos que no cubre el GDPR. Las nuevas reglas se adaptan mejor a los datos electrónicos, enfatizan la privacidad del diseño y fortalecen la protección de los datos privados. Sin embargo, la naturaleza personal de los datos, no su forma, sigue siendo el factor determinante.

**Ley de Comunicaciones Electrónicas:** El propósito de esta ley es crear las condiciones necesarias para promover el desarrollo de redes y servicios de comunicaciones electrónicas, al mismo tiempo que se garantiza la protección de los intereses de los usuarios de dichos servicios. La ley estipula los requisitos para las redes y servicios de comunicaciones electrónicas disponibles públicamente, y para la supervisión estatal en relación con el cumplimiento de los requisitos. Sirve como legislación sectorial específica para la Ley de Competencia.

**Ley de Contratación Pública:** La legislación de contratación pública incluye disposiciones legales que facilitan el desarrollo adicional de soluciones electrónicas en la contratación pública (por ejemplo, subastas electrónicas, sistemas de compra dinámicos, catálogos electrónicos, etc.).

**Ley de Servicios para la Sociedad de la Información:** Esta ley se basa en la Directiva 2000/31/CE de la UE sobre algunos aspectos legales de los servicios de la sociedad de la información, en particular el comercio electrónico, en el mercado interno europeo. Establece los requisitos relativos a los proveedores de servicios de la sociedad de la información, así como la organización de supervisión y responsabilidad en caso de infracciones.

**Ley de Secretos de Estado e Información Clasificada de Estados Extranjeros:** La ley garantiza la seguridad y las relaciones exteriores de la República de Estonia, protegiendo los secretos de Estado y la

|   |   |  |
|---|---|--|
|   | <p>información clasificada de los Estados extranjeros contra la divulgación o el acceso a esta información por personal no autorizado.</p> <p><b>Ley de Emergencia:</b> En esta ley se encuentra el marco legal para la gestión de crisis, incluida la preparación para una emergencia y su resolución, así como la garantía de la operación continua de los servicios esenciales. La ley también regula la declaración, resolución y el término de situaciones de emergencia, y el uso de las Fuerzas de Defensa y la Liga de Defensa para resolver una emergencia, realizar trabajos de rescate y garantizar la seguridad.</p>  |  |
| <p>Sistema provincial de gobierno electrónico de Neuquén.</p> <p><b>ARGENTINA</b></p> | <p><b>Ley N° 3290-2021, que crea el Ecosistema de Integrabilidad:</b> Esta ley provincial institucionaliza en su artículo 1° una “red de componentes que garantizan la seguridad, confidencialidad, trazabilidad y no repudio en el intercambio de datos, procesos y servicios digitales realizados entre los sistemas informáticos que usan las personas humanas o las distintas entidades jurídicas, para brindar evidencia legal de dichos intercambios en todas las situaciones”. Asigna asimismo a las autoridades encargadas del cumplimiento de la nueva regulación y adecúa la regulación provincial y federal existente.</p> <p><b>Ley N°2819-2012, Ley de Desburocratización de trámites ante todos los Organismos dependientes de los tres Poderes del Estado Provincial.</b> Establece que las personas pueden ser atendidas presencial o virtualmente, que los organismos públicos deben acudir a sus propios archivos para recabar la información de los usuarios y que esta no es exigible a los ciudadanos.</p> <p><b>Ley Provincial N° 2578 de Firma Digital:</b> Adapta la legislación provincial a la nacional (Ley Nacional 25506) sobre firma digital y, como señala su artículo octavo, “autoriza a emplear la firma digital o la firma electrónica en los actos internos de la Administración Pública provincial y en aquellos actos que excediendo la órbita interna se celebren con instituciones, organismos o cualquier otro tipo de entes públicos o privados”.</p> <p><b>Decreto N°0405/1991 y Plan Maestro de Gobierno Electrónico de 2003.</b> Establece una política provincial de informática para los servicios públicos, así como la organización institucional de la política, mientras que el plan de gobierno electrónico, que es descrito más adelante, contiene las metas, definiciones y pasos a seguir por el gobierno provincial en el desarrollo de su gobierno electrónico.</p> <p><b>Referencial IRAM N°14-1 y 14-2.</b> Elaboradas por el Instituto Argentino de Normalización y Certificación, son normas técnicas específicas para estandarizar la</p> | <p>La norma IRAM 17610: Ecosistema Digital de Integrabilidad (EDI) establece los requisitos para un ecosistema digital donde diversos sistemas y aplicaciones coexistan e intercambien información de manera segura y eficiente.</p> <p>Esta norma, pionera en Argentina y Latinoamérica, busca superar los desafíos de la integración de sistemas a nivel multiorganizacional, yendo más allá de la interoperabilidad para facilitar la innovación.</p> <p>La norma busca plasmar las bases conceptuales, mejores prácticas y requisitos para la conformación, operación y evolución de un EDI2.</p> <p>Alcance: La norma se proyecta en ámbitos territoriales y jurisdiccionales, siendo aplicable a empresas, estados, la industria del software e instituciones académicas.</p> <p>Estructura: La norma combina la estructura normativa estandarizada con componentes del marco de interoperabilidad europeo, adaptándolos a la realidad nacional.</p> <p>Se compone de:</p> <p>Requisitos específicos y recomendaciones:</p> <p>Dimensión técnica: abarca seguridad, interoperabilidad, gestión de servicios, metadatos y</p> |

|                          |   |  |
|--------------------------|---|--|
|                          | <p>calidad de aplicaciones informáticas y su Integrabilidad, en especial para la provincia de Neuquén.</p> <p>La Norma IRAM 17610, con un estándar nacional de interoperabilidad digital basado en las mejores prácticas de Estonia y la Unión Europea. Define los estándares para el intercambio de información entre entidades, establece un contenedor digital para la transmisión segura de datos y alinea los procesos de las provincias y otras instituciones bajo un marco unificado. La adopción de esta norma no solo facilitó la expansión de X-Road, sino que también contribuyó a reducir la complejidad y los costos de integración para las nuevas instituciones que se sumaban al sistema.</p> <p>El desarrollo de normas nacionales como la IRAM 17610 permitió estandarizar los procesos y garantizar que el ecosistema digital siguiera creciendo de manera coherente.</p>  | <p>arquitectura de información.</p> <p>Dimensión organizacional: se centra en la colaboración, acuerdos de interoperabilidad, gestión de seguridad y gestión de servicios.</p> <p>Dimensión de gestión: aborda la gestión de riesgos, definición de métodos de trabajo, comunicación de metas operativas, formación continua y mejora del EDI.</p> <p>Métodos de ensayo: permiten verificar el cumplimiento de los requisitos.</p> <p>Evaluación de conformidad: demuestra el cumplimiento de los requisitos.</p> <p>Principios: La norma se basa en 14 principios fundamentales:</p> <ul style="list-style-type: none"> <li>Enfoque en las personas.</li> <li>Proactividad en los servicios</li> <li>Solo una vez (once only). Eficacia y eficiencia</li> <li>Digital primero Seguridad de la información compartida</li> <li>Subsidiariedad y cobertura.</li> <li>Colaboración y participación</li> <li>Neutralidad tecnológica. Inclusión y acceso</li> <li>Reutilización Conservación de la información</li> <li>Confianza Multilingüismo</li> </ul> |
| <p><b>Costa Rica</b></p> | <p><b>Ley de Protección al Ciudadano de Exceso de Requisitos y Trámites Administrativos y en la Ley de Certificados, Firmas Digitales y Documentos Electrónicos, por medio del Decreto Ejecutivo N° 35776</b>, de Promoción del Modelo de Interoperabilidad en el Sector Público, se crea una instancia para ejecutar la adecuada coordinación y articulación de la Interoperabilidad en la Administración Pública.</p> <p>Para ello se estableció, en el artículo 3°, un Equipo Interinstitucional de Interoperabilidad, adjunto a la Secretaría Técnica de Gobierno Digital, integrada por representantes de diversos órganos públicos. Esta norma obliga a las instituciones públicas a brindar el acceso en línea y la disponibilidad permanente de la información legalmente disponible, para el buen funcionamiento de los servicios de interoperabilidad acorde a la normativa vigente y al Modelo de Interoperabilidad del Gobierno (e-mig). Las entidades públicas deberán transferir datos de manera uniforme y</p> | <p>Creación de una instancia para ejecutar, organizar y dirigir la articulación de la interoperabilidad en la administración pública.</p> <p>Estableció una norma para el funcionamiento en las que incluye los nombramientos de las personas y sus funciones a desarrollar</p>  |

|                             |  |   |
|-----------------------------|--|---|
|                             | <p>eficiente entre varias organizaciones y sistemas sin importar su origen o proveedor, fijando las normas, las políticas y los estándares necesarios para la consecución de esos objetivos (artículo 6°). Este decreto ejecutivo fue derogado por el artículo 1° del decreto ejecutivo N° 40951 del 12 de febrero de 2018.</p>  |   |
| <p><b>R. Dominicana</b></p> | <p>Creó la arquitectura digital gubernamental en la Oficina Gubernamental de Tecnologías de la Información y Comunicación (OGTIC) junto a la creación de un conjunto de normas técnicas conocidas como “NORTIC”, que regulan el uso de tecnologías de la información en las instituciones públicas.</p> <p>Entre estas normas, la “NORTIC A4” define los lineamientos para la interoperabilidad, especificando cómo deben interactuar las instituciones y qué datos pueden o no compartirse, permitiendo la creación de un ecosistema coherente, donde cada institución conoce sus responsabilidades y las mejores prácticas para compartir información de manera segura y efectiva.</p> <p>La NORTIC A4 ha sido fundamental para que las instituciones públicas se adapten a la interoperabilidad, facilitando la implementación de X-Road como plataforma central.</p> <p>La creación de un marco normativo sólido, como las NORTIC, es fundamental para garantizar que las instituciones sigan las mismas reglas y que el sistema sea seguro y eficiente. Este marco legal también ayuda a superar las barreras relacionadas con la protección de datos y la privacidad, asegurando que la información sensible sea manejada de manera adecuada.</p> <p>En República Dominicana, la OGTIC actúa como la entidad responsable de coordinar la interoperabilidad, asegurando que todas las instituciones sigan los mismos protocolos y compartan datos de manera eficiente. Esta gestión centralizada ha sido esencial para evitar la duplicación de esfuerzos y garantizar la sostenibilidad del sistema.</p> | <p>La normativa aplica a todos los organismos del Estado dominicano bajo el Poder Ejecutivo que intercambien datos ciudadanos para la prestación de servicios públicos.</p> <p>Busca estandarizar los procesos de interoperabilidad para:</p> <p>Mejorar la calidad de los servicios públicos.</p> <p>Aumentar la transparencia y la rendición de cuentas.</p> <p>Reducir costos administrativos.</p> <p>Aumentar la eficiencia operativa.</p> <p>La norma se basa en los principios de:</p> <p>Transparencia: Permitir que otros organismos, ciudadanos y empresas comprendan las reglas, procesos, datos y toma de decisiones.</p> <p>Reusabilidad: Fomentar la reutilización de datos y servicios para evitar la duplicación de esfuerzos.</p> <p>Inclusión: Asegurar que los servicios sean accesibles para todos.</p> <p>Seguridad y Privacidad: Garantizar la seguridad y confidencialidad de la información.</p> <p>Eficiencia: Disponer de la capacidad para lograr los objetivos de interoperabilidad.</p> <p>Efectividad: Asegurar que la interoperabilidad cumpla con los objetivos para los que fue diseñada.</p> <p>Dimensiones de la interoperabilidad: La normativa abarca cuatro dimensiones:</p> |

|  |  |  |
|--|--|--|
|  |  | <p>Legal: Define las normas y estatutos que habilitan la interoperabilidad, asegurando que el intercambio de información se ajuste al marco jurídico.</p> <p>Organizacional: Promueve la colaboración entre organismos para la definición de procesos y responsabilidades en la interoperabilidad.</p> <p>Semántica: Garantiza que la información intercambiada se interprete de manera inequívoca, utilizando estándares para la definición de datos y metadatos.</p> <p>Técnica: Establece las especificaciones técnicas, como interfaces, protocolos y formatos de datos, para la interconexión de sistemas.</p> <p>Categorías de certificación:</p> <p>Categoría A: Para organismos que proveen datos.</p> <p>Categoría B: Para organismos que consumen datos.</p> <p>Categoría C: Para organismos que proveen y consumen datos.</p> <p>Comité de Implementación y Gestión de Estándares TIC (CIGETIC):</p> <p>Cada organismo debe conformar un CIGETIC mediante resolución oficial para planificar, implementar y dar seguimiento a la certificación NORTIC.</p> <p>El CIGETIC debe estar integrado por representantes de diversas áreas del organismo, incluyendo tecnología, jurídica, planificación y acceso a la información.</p> <p>Responsabilidades: La norma define las responsabilidades del organismo solicitante de la certificación y de la OGTIC durante el proceso.</p> <p>Interoperabilidad en Salud: La NORTIC 4 dedica un capítulo a la interoperabilidad en el sector salud, estableciendo estándares</p> |
|--|--|--|

|                        |  |   |
|------------------------|--|---|
|                        |  | <p>específicos para el intercambio de información médica.</p> <p>Estándares técnicos:</p> <p>Obliga a los organismos a utilizar la Plataforma Única de Interoperabilidad (basada en X-Road) para el intercambio de información.</p> <p>Define requisitos para servidores de seguridad, gestión de accesos, manejo de contraseñas y planes de recuperación ante desastres.</p> <p>Establece directrices para la creación de APIs, incluyendo el uso de estándares como REST, JSON y OAuth 2.0.</p> <p>Promueve el uso de estándares internacionales como HL7 para la interoperabilidad en salud.</p>   |
| <p><b>Colombia</b></p> | <p>El Decreto 620 de 2020 fue clave para establecer las reglas que rigen la interoperabilidad en el país. Este decreto define los requisitos técnicos y legales que deben cumplir las entidades para compartir información de manera segura y eficiente. Regula el uso de tecnologías de la información en las entidades públicas y asegura que el intercambio de datos se realice de manera segura y estandarizada.</p> <p>Destacó la importancia de un ente central que coordine los esfuerzos de las instituciones sin limitar su autonomía, asegurando que la interoperabilidad se mantenga alineada con las necesidades del país.</p> | <p>El Decreto 620 de 2020 de Colombia establece el marco normativo para los servicios ciudadanos digitales, incluyendo la interoperabilidad como un servicio esencial. Este decreto busca garantizar un flujo de información adecuado entre los sistemas de las entidades públicas colombianas.</p> <p>Estas son las reglas principales para la interoperabilidad que se encuentran en el Decreto 620 de 2020:</p> <p>Interoperabilidad como servicio esencial: El decreto define la interoperabilidad como un servicio esencial para garantizar un flujo de información adecuado entre los sistemas de las entidades públicas.</p> <p>Marco de Interoperabilidad: El decreto establece que las entidades deben seguir un Marco de Interoperabilidad. Este marco define los lineamientos, estándares y protocolos que deben cumplir las entidades para garantizar la interoperabilidad de sus sistemas.</p> <p>Vinculación obligatoria: Las</p> |

|  |  |   |
|--|--|---|
|  |  | <p>entidades públicas colombianas están obligadas a vincularse a los servicios ciudadanos digitales, incluyendo la interoperabilidad. Deben seguir la guía emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para la preparación, adecuación, integración, uso y apropiación de estos servicios.</p> <p>Rol del Articulador: El decreto designa un “Articulador” (la Agencia Nacional Digital) para coordinar y facilitar la interoperabilidad entre las entidades públicas. Las funciones del Articulador incluyen:</p> <p>Acompañar a las entidades en la creación, diseño, implementación o adecuaciones técnicas de los trámites y servicios que se expondrán a través de los servicios ciudadanos digitales, asegurando que cumplan con el Marco de Interoperabilidad.</p> <p>Poner a disposición de las entidades los servicios de interoperabilidad que ya estén implementados o hayan sido publicados en la plataforma de interoperabilidad del Estado colombiano, siempre y cuando cumplan con el nivel 3 de madurez según el Marco de Interoperabilidad.</p> <p>Apoyar la configuración, habilitación y exposición de los servicios de intercambio de información.</p> <p>Mediar y coordinar el intercambio de información entre las entidades, integrando los servicios habilitados o expuestos, según las reglas y políticas del Marco de Interoperabilidad.</p> <p>Actualización de la información: Las entidades deben mantener actualizada la información sobre sus trámites y servicios en el Sistema Único de Información de Trámites (SUIT). Deben</p> |
|--|--|---|

|                         |  |  |
|-------------------------|--|--|
|                         |  | <p>especificar en el SUIIT cómo utilizan la interoperabilidad para simplificar los trámites y evitar solicitar información que ya esté disponible en otras entidades.</p> <p>Seguridad de la información: El decreto enfatiza la importancia de la seguridad y privacidad de la información en la interoperabilidad. Las entidades deben cumplir con la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y otras normas relacionadas.</p> <p>Evaluación del impacto en la protección de datos: Antes de implementar servicios ciudadanos digitales, los proveedores deben evaluar el impacto en el tratamiento de datos personales, incluyendo la finalidad del tratamiento, los tipos de datos, las medidas de seguridad y los mecanismos para garantizar los derechos de los titulares de los datos.</p> <p>Oficial de Protección de Datos: Se requiere que las entidades designen un Oficial de Protección de Datos para garantizar el cumplimiento de la normativa de protección de datos personales en la prestación de los servicios ciudadanos digitales.</p> |
| <p><b>Guatemala</b></p> | <p>Ley de simplificación de trámites administrativos. Aunque La falta de una ley de protección de datos y la ausencia de un marco claro para la interoperabilidad y una entidad que centralice la tarea obstaculiza el progreso hacia una digitalización completa del gobierno. Deben complementarse con una estrategia legislativa más amplia que aborde aspectos como la ciberseguridad y la firma electrónica avanzada.</p> | <p>Tiene como experiencia que la ausencia de una entidad que centralice la tarea obstaculiza el progreso de la interoperabilidad</p>   |

***PRINCIPALES PRESUPUESTOS A TENER EN CUENTA PARA ELABORAR LAS PROPUESTAS DE NORMAS, POLÍTICAS Y DIRECTRICES PARA DESARROLLAR EL ECOSISTEMA DE INTEROPERABILIDAD EN EL MINISTERIO DE JUSTICIA.***

A partir de la información analizada llegamos a la conclusión de que para desarrollar un ecosistema de interoperabilidad en el Ministerio de Justicia sería conveniente avanzar al

unísono en la digitalización de los servicios junto a la elaboración de una única ley para la Interoperabilidad en el país, apoyada con una Metodología de trabajo para ejecutar el funcionamiento en la práctica por parte de las instituciones miembros. Al mismo tiempo velar que las distintas políticas de custodia de datos no obstaculicen o impidan la interoperabilidad. Tener una cláusula que permita establecer normas habilitantes si los avances tecnológicos o actualizaciones sobre procedimientos lo ameritan.

Partimos de ese criterio teniendo en cuenta que la interoperabilidad busca conectar entidades que operan bajo diferentes reglamentos, culturas institucionales y enfoques técnicos mediante la digitalización y automatización de procesos. Este reto se supera mediante la creación de normativas comunes y estándares que faciliten la integración de los sistemas. Estas regulaciones permiten la coordinación de datos y el cumplimiento de los estándares necesarios para asegurar que la información intercambiada sea precisa, segura y accesible para las entidades que la necesiten sin duplicidad de trabajo, información, personas, procesos y esfuerzos, minimizando errores y retrocesos.

Cualquier decisión sobre la arquitectura tecnológica a implementar, implica más que solo adoptar una tecnología desde una mirada micro al interior de las instituciones; requiere una reorganización de los procesos y una alineación de los sistemas de información para permitir un intercambio efectivo posterior de datos entre las instituciones públicas, incluidos los servicios jurídicos.

Es esencial establecer acuerdos sobre los datos que se intercambiarán, asegurando una comprensión semántica clara entre las instituciones. Lo que conlleva a la creación de un estándar semántico, donde se definan los nombres, etiquetas y variables que deben utilizarse para describir e intercambiar datos. Esto evita malentendidos y garantiza que todas las instituciones utilicen el mismo lenguaje cuando se refieren a conceptos clave como nombres, delitos, información financiera, entre otros datos.

Es importante establecer un marco regulatorio que defina claramente cómo las instituciones deben interactuar dentro del ecosistema de interoperabilidad. Revisar las leyes existentes para identificar aquellas que podían obstaculizar la interoperabilidad y hacer las modificaciones necesarias para facilitar el intercambio de datos.

Un marco de interoperabilidad también debe incluir acuerdos sobre cómo se gestionarán los datos, garantizando que los sistemas heredados y nuevos se desarrollen con la interoperabilidad en mente. Esto asegura que, a medida que se implementen nuevas

tecnologías, estas puedan integrarse fácilmente en el ecosistema sin generar incompatibilidades.

Al respecto el Decreto Ley 370/2018 sobre la informatización de la sociedad contiene algunos elementos a tener en cuenta para desarrollar con efectividad un sistema interoperable en el MINJUS y que posteriormente se integre sin mayores contratiempos a la Plataforma Nacional con su Gobierno Electrónico. Entre estos define:

- Responsables de orientar tareas y acciones relacionadas con el proceso de informatización en primer lugar al Ministerio de las Comunicaciones y en segundo lugar a las FAR y al MININT.
- El Ministerio de las Comunicaciones organiza, norma y estandariza la actividad informática en los órganos y organismos del Estado.
- El Ministerio de las Comunicaciones promueve la integración de las redes institucionales y de uso público para el acceso a los servicios.
- El Ministerio de las Comunicaciones debe fomentar un sistema de centros de datos con condiciones tecnológicas y de seguridad.
- El Ministerio de las Comunicaciones potencia el despliegue de la banda ancha para la cobertura nacional.
- El Ministerio de las Comunicaciones promueve servicios en línea entre las instituciones y ciudadanos con prioridad en los servicios y trámites de la población, la gestión del gobierno y el comercio electrónico.
- El Ministerio de las Comunicaciones garantiza el diseño e instrumentación de un sistema que perfeccione, armonice y desarrolle el marco legal que sustente el proceso de informatización de la sociedad, así como el control y fiscalización de su cumplimiento.
- El Ministerio de las Comunicaciones debe coadyuvar a que los procesos de informatización se desarrollen con un análisis organizacional y con un enfoque sistémico integrado.
- El Ministerio de Comunicaciones tiene que establecer una plataforma nacional que incentive la generación de contenido y generalice la posibilidad de socializarlos.

- El Ministerio de las Comunicaciones es el responsable de elaborar, establecer y controlar el plan para la migración de programas y aplicaciones informáticas propietarios hacia plataformas de código abierto de producción nacional.
- El Jefe de la Oficina Nacional de Estadísticas e Información con el Ministerio de las Comunicaciones establece los procedimientos, normativas y estándares tecnológicos que garanticen la interoperabilidad de la información a nivel nacional y la comparabilidad con el ámbito internacional.
- Los ministerios de las FAR y el MININT definen los requerimientos técnicos, organizativos y de seguridad de los servicios de interés para el país, soportados en sus infraestructuras tecnológicas y los organismos organizan sus servicios de las TIC en coordinación con ellos para garantizar seguridad y defensa nacional.
- El MINJUS propone y emite las disposiciones jurídicas para dotar de validez legal los documentos en formato digital.
- El MINJUS aprueba las disposiciones jurídicas que resulten necesarias para el intercambio de los documentos en formato digital, relacionadas con el comercio electrónico.
- Las entidades que tengan a su cargo registros públicos son responsables de su informatización.
- Cada organismo determina los servicios que brinda a la población, facilitan y optimizan los trámites y el acceso a la información, así como la atención ciudadana en línea y son responsables del uso de las plataformas tecnológicas que proteja los datos del usuario y garanticen la veracidad y autenticidad de la información.

Para lograr el éxito de un ecosistema de interoperabilidad también se debe decidir desde un inicio los factores claves siguientes:

- ✓ Liderazgo: Necesidad de contar con un líder o grupo que impulse y dé continuidad al proyecto. Pensado no como persona individual sino como grupo o institución rectora de la interoperabilidad desde lo macro. Responsable de su desarrollo, control y evolución.
- ✓ Institucionalidad: Formalización de los equipos de trabajo y los procesos de interoperabilidad desde un pensamiento micro.
- ✓ Recursos: Asignación adecuada de presupuestos y apoyo institucional.

- ✓ Acuerdos: Establecimiento de acuerdos claros entre las instituciones sobre los procesos, tecnologías y normativas a utilizar.
- ✓ Capacidades técnicas: Formación adecuada en interoperabilidad para todos los actores involucrados.
- ✓ Modelo de madurez: Evaluar periódicamente qué tan preparada está cada institución para afrontar los retos de la interoperabilidad a mayor escala.

***Después de contemplado lo anterior la pregunta que sigue sería: ¿Qué entender por ecosistema de interoperabilidad para la plataforma del MINJUS?***

Para establecer una definición se propone abarcar los siguientes conceptos, de manera general se entenderá como la habilidad o capacidad de dos o más sistemas, componentes, organizaciones o entidades para intercambiar información y servicios, así como utilizar estos de manera efectiva y transparente. No se limita solo a la tecnología, sino que también incluye aspectos organizativos, legales y semánticos para trabajar de manera eficiente y sin barreras. Definiendo el aspecto tecnológico como la capacidad de los sistemas técnicos para conectarse y comunicarse, el semántico como la comprensión común de los datos intercambiados (significado y contexto) y el organizativo como la alineación de procesos, políticas y estándares entre organizaciones. (Febles, 2022)

La interoperabilidad involucra diversos retos a la hora de lograr un intercambio efectivo de información y mejorar los servicios para la ciudadanía, retos que no están relacionados directamente con la capacidad técnica, sino pensar en las personas como ejecutoras, participantes y beneficiarias de la interoperabilidad.

Si tomamos en cuenta la relación de la interoperabilidad con las entidades y los servicios y beneficios que estas proveen a la ciudadanía, podemos ampliar su definición y entender a la interoperabilidad como: La capacidad de las organizaciones para intercambiar información y conocimiento dentro de los límites de sus procesos de negocio, interactuando hacia objetivos mutuamente beneficiosos. Este intercambio debe realizarse dentro del marco de la protección de la ética y la seguridad y de manera ágil, eficiente y transparente, permitiendo a las organizaciones la toma de decisiones basadas en hechos. Además, la colaboración tendrá el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades mediante el intercambio de datos entre sus sistemas (Huaiquilican, s.a).

De manera simplificada, la interoperabilidad es la capacidad que poseen dos o más sistemas o componentes para intercambiar información y utilizar la información intercambiada de

manera efectiva y si tiene como propósito hacer que el MINJUS funcione como una sola Entidad eficiente que les brinde a sus ciudadanos información oportuna, trámites y servicios en línea ágiles. Las entidades deben ser conscientes del impacto de la interoperabilidad en la sociedad, asumir con compromiso y dar el primer paso para estar digitalmente conectados y articulados para llegar a ser un solo Sistema.

En cada organización o institución deben abordarse los aspectos de las cuatro dimensiones de la interoperabilidad para lograr que un intercambio de información entre entidades sea posible permitiendo establecer alguna metodología a seguir para alcanzar el éxito de un proyecto determinado. Estos cuatro dominios planteados son: Legal, Organizacional, Técnico y Semántico. Cada uno de estos tiene distintos subdominios y aspectos de los mismos.

Lograr la capacidad de que las organizaciones interactúen con vistas a alcanzar objetivos comunes que sean mutuamente beneficiosos y que hayan sido acordados previa y conjuntamente, recurriendo a la puesta en común de información y conocimientos entre las organizaciones, a través de los procesos empresariales a los que apoyan, mediante el intercambio de datos entre sus sistemas de TIC respectivos (Marco Europeo de Interoperabilidad, citado por Roberts, 2023).

#### ***A continuación la interrogante que sigue sería: ¿qué plataforma interoperable utilizar?***

El equipo de investigación propone el modelo de Ecosistema digital de Interoperabilidad X-ROAD de Estonia como base por varios argumentos, aunque a partir del estudio de las buenas prácticas de proyectos en otros países, determinadas ideas brindan integralidad en el análisis y se han tenido en cuenta para la propuesta (Vivas, s.a; Huaiquilican, s.a; Arm, 2019; Ríos-Campo, 2021; Roberts, 2023; Espinosa, 2024; Menchú, 2024; Ardilla, 2024). Entre ellas podemos mencionar:

#### ***Desde el punto de vista político tiene las siguientes similitudes con el sistema cubano:***

-Estonia es una República Parlamentaria.

-Su Jefe de Gobierno -el Primer Ministro- es nombrado por el Presidente y aprobado por el Parlamento. Es responsable del poder ejecutivo del que está investido el Gobierno.

-El Jefe del Estado -el Presidente- es elegido por el Parlamento o colegio electoral por un periodo de cinco años.

-El Parlamento, formado por 101 diputados, es elegido por sufragio directo cada cuatro años.

-El país está dividido en 15 provincias y 79 municipios.

-El sector público de Estonia se fijó como objetivo el desarrollo de la administración electrónica y el gobierno comenzó a desarrollar bases de datos, a potenciar un entorno seguro para el intercambio de información y para la certificación digital, así como a promover la creación de servicios de carácter electrónico.

-El siguiente paso fue crear una ley relacionada con la telecomunicación y el acceso a Internet para todos sus ciudadanos.

-El Sistema de Información de las Sesiones de Gobierno, conocido como e-Gabinete, es una herramienta eficaz que el Gobierno estonio usa para agilizar sus procesos de toma de decisiones. En esencia, el sistema es un planificador y una base de datos multiusuario que mantiene la información relevante organizada y actualizada en tiempo real, brindando a los ministros y ministras una visión general clara de cada aspecto en discusión. Mucho antes de que comience la sesión semanal del Gabinete, los ministros y ministras acceden al sistema para revisar cada tema de la agenda y formular sus posiciones personales. Si tienen alguna objeción o les gustaría hablar sobre algún tema, marcan la casilla correspondiente. Así, sus posiciones son visibles para otros miembros del Gabinete antes de la reunión, y las decisiones que no han recibido objeciones se adoptan sin debate, lo que ahorra un tiempo considerable. Además, las decisiones tomadas en las reuniones del Gabinete pueden enviarse por correo electrónico a las partes interesadas o publicarse en una web, incluso cuando la reunión todavía está celebrándose.

-Entre las ventajas principales se resumen en que los ministros y ministras están mejor organizados, facilita la participación a distancia en reuniones mediante dispositivos audiovisuales, no hay necesidad de llevar a todas partes grandes pilas de papel, el tiempo promedio de las sesiones se ha reducido de 4 a 5 horas a solo 30 a 90 minutos, se reduce el impacto ambiental y los procesos de toma de decisiones son más transparentes y comprensibles.

-El e-Voto por internet o voto telemático es un sistema que permite a los votantes participar en elecciones nacionales o locales desde cualquier parte del mundo emitiendo su voto en línea a través de una computadora conectada a internet. Se utiliza como método de votación adicional para aumentar la participación en las elecciones.

- La e-democracia reside en el apoyo y la mejora de los procesos y las instituciones democráticas mediante la tecnología. Ofrece a los ciudadanos una oportunidad más de participar en procesos políticos y es una parte integral del desarrollo de la gobernanza

electrónica (e-gobernanza). La democracia electrónica se asocia a menudo con el voto por internet (e-voto), que en Estonia está disponible desde el 2005. Sin embargo, es un método de votación adicional y corresponde a una democracia representativa en lugar de participativa. Por lo tanto, debe distinguirse de la participación electrónica (e-participación), en la que se habilitan oportunidades de consulta y diálogo entre el Gobierno.

-Cuenta con un portal de inicio de sesión único [www.eesti.ee](http://www.eesti.ee) que brinda a los usuarios un acceso sencillo a varios servicios electrónicos y proporciona al Gobierno una plataforma sólida y cómoda para integrar y promover nuevos servicios e intercambiar de manera sistemática con la ciudadanía porque incluye dentro de las estructuras al Portal del Gobierno. Tiene como ventajas que se facilita un único punto de contacto. Se ofrece un acceso fácil a todos los servicios electrónicos. La plataforma facilita promover nuevos servicios cómodamente.

***Desde el punto de vista económico facilita:***

-Después de independizarse de la Unión Soviética, optó por fomentar la economía digital y la innovación tecnológica masiva, debido a que era un país diminuto y carente de recursos naturales propios.

-Se apoyó para el desarrollo en el talento humano especializado que poseía.

-La economía de Estonia es innovadora y basada en el conocimiento, utilizando nuevas tecnologías y modelos de negocio y formas flexibles de empleo. Se han creado condiciones favorables para la I + D y la innovación en el sector privado, y los investigadores y las empresas están cooperando. El entorno empresarial de Estonia atrae a personas a trabajar allí, crear empresas o participar en negocios virtuales, invertir y crear y probar nuevas soluciones que beneficien a la sociedad en general.

-El Banco Interamericano de Desarrollo ha venido acercando a los países de América Latina y el Caribe a la experiencia de Estonia desde hace varios años. La visión 2025 del BID tiene como uno de sus cinco pilares la economía digital. Además, de otros bancos en países como Canadá y miembros de la Unión Europea.

-La banca en línea segura y fácil de usar de Estonia es conocida en todo el mundo. Desde 2016, la Ley de Prevención del Blanqueo de Capitales y del Financiamiento del Terrorismo autoriza a las instituciones financieras a verificar en línea la identidad de una persona, de acuerdo con los requisitos y el procedimiento para la identificación de personas y la verificación de la identidad por medio de tecnologías de la información. Tiene entre otras

ventajas como que no es necesario presentarse en la sucursal, las transacciones en línea son más baratas, el cliente y el proveedor de servicios ahorran tiempo y dinero, los servicios son accesibles las 24 horas y los 7 días de la semana y se ofrece acceso seguro desde cualquier lugar con conexión a internet.

-En relación con impuestos y aduana ha aumentado el número de contribuyentes, se reduce el costo administrativo para la el Consejo de Impuestos y Aduanas, las declaraciones de impuestos pueden presentarse en 3 a 5 minutos, los contribuyentes reciben sus reembolsos en 5 días, la recaudación de impuestos es transparente y eficiente y ha ayudado a reducir drásticamente el tiempo que personas y empresas necesitan para presentar sus declaraciones de impuestos. Además, en la medida en que estos se implementan permanecen en constante actualización simplificando considerablemente los trámites.

-El estacionamiento móvil es un sistema cómodo que facilita a los conductores el pago del estacionamiento en la ciudad con su teléfono móvil.

-La e-boleto es una solución de boletería introducida junto con la implementación de boletos personalizados para los sistemas de transporte público locales. Es más fácil verificar la validez de los boletos porque se guardan en tarjetas y tienen que validarse durante cada viaje. Es un sistema práctico y optimizado para el cliente, ya que no necesita adquirir un boleto físico. Los pasajeros pueden cargar dinero en su cuenta en línea a través del teléfono móvil o en puntos de venta presenciales. Proporciona datos a la administración de la ciudad para analizar el uso del transporte público.

-El registro e-Negocios o registro empresarial electrónico es una plataforma en línea vinculada a la base de datos oficial que incluye datos en tiempo real de todas las entidades legales registradas en Estonia. El registro empresarial electrónico también alberga el Portal de Registro de Empresas en línea, una plataforma en el internet que permite a los empresarios enviar solicitudes electrónicas, documentos e informes anuales al registro comercial. También tiene como ventajas que permite revisar los datos generales de la empresa y la información sobre los impuestos atrasados, controlar en tiempo real el procesamiento de datos y el registro de modificaciones de empresas, verificar las prohibiciones de negocios y de emprendimiento de ciudadanos estonios, visualizar las relaciones entre empresas y personas, acceder a informes anuales, estatutos, datos de prendas civiles y mercantiles, entre otros.

-El e-administración de carreteras permite la verificación del historial del vehículo, baja temporal del vehículo, certificado de instructor, canje de licencia de conducción provisional, autorización de transporte, canje de licencia de conducción.

-Es el primer país en ofrecer e-Residencia, una identidad y un estado digitales emitidos por el gobierno que brinda acceso al entorno empresarial transparente de Estonia. Los emprendedores residentes en Internet de todo el mundo pueden iniciar una empresa con sede en la UE y gestionar su negocio desde cualquier lugar, completamente en línea. La e-Residencia Estonia ha hecho historia con el plan supranacional de residencia electrónica en el mundo. La identificación electrónica para no residentes emitida por el Estado permite la autenticación segura y la firma electrónica de documentos, lo que representa un avance hacia la idea de un país sin fronteras. Al respecto permite la firma digital de documentos y contratos. Facilita verificar la autenticidad de los documentos firmados. Se pueden cifrar y transmitir documentos de forma segura. Permite establecer una empresa en línea en Estonia y administrarla desde cualquier parte del mundo. Pueden realizarse operaciones en banca electrónica y transferencias de dinero. Facilita el acceso a diversos servicios electrónicos. Pueden Declarar impuestos en línea (la e-residencia no implica la residencia fiscal automática).

En temas económicos de manera general ahorran recursos a través de procesos automatizados, se facilita la colaboración entre instituciones, se favorece una mayor transparencia y se reduce la corrupción.

***Desde lo social con el ciudadano como centro de actuación:***

-Se ha convertido en un modelo a seguir para los gobiernos que desean aprovechar las nuevas tecnologías para mejorar la eficacia y eficiencia en las relaciones ciudadano-Estado.

-Mejora la administración pública que tiene como finalidad proveer mejores servicios e incrementar la satisfacción de los ciudadanos.

-Los estonios confían y utilizan las soluciones en línea porque son rápidas, seguras y convenientes.

-Facilita la colaboración entre diferentes actores y la participación activa de la comunidad.

-La información procesada muestra a Estonia, como un gobierno digital exitoso, cuyos proyectos más destacados son: Mejora en la eficacia del Gobierno, voto electrónico, salud electrónica, declaración de impuestos electrónica, negocio electrónico y residencia electrónica.

-El acceso favorece la participación y el control fomenta la confianza. Se enfoca en los ciudadanos y en los derechos de los ciudadanos, no en la máquina pública digital.

-Es una increíble historia de éxito basada en la asociación entre un Gobierno con visión del futuro, un sector de las TIC proactivo y una población dinámica con conocimientos tecnológicos.

-La e-salud contiene un sistema nacional que integra historias clínicas electrónicas con datos de diferentes proveedores de atención médica para generar un solo archivo electrónico con un registro completo para cada paciente. El sistema contiene información sobre diagnósticos, visitas al médico, pruebas, tratamientos hospitalarios, medicamentos recetados, entre otros. Tiene entre sus ventajas el que se reduce significativamente la burocracia administrativa para los médicos, se puede acceder a información crítica en situaciones de emergencia, los servicios de salud son más fáciles de usar para el paciente, el sistema de salud es más eficiente y recopilan datos sobre las tendencias de salud de forma automatizada.

-La e-Prescripción es el servicio de prescripción electrónica y es un sistema centralizado y sin papel para emitir y manejar recetas médicas, que se expiden electrónicamente a través de formularios en línea. Todos los hospitales y farmacias del país están conectados al sistema. El paciente solo tiene que presentar su tarjeta de identificación en la farmacia. Entonces, el farmacéutico recupera la información del paciente del sistema y rellena la receta. Entre otras ventajas tiene que no se requieren citas médicas para las renovaciones de rutina, lo que ahorra tiempo tanto a los pacientes como a los médicos. Los pacientes no necesitan hacer un seguimiento de las recetas en papel. Se reduce el papeleo en los hospitales y las farmacias.

-La e-Escuela se ha convertido en uno de los servicios electrónicos más utilizados en Estonia.

-La e-justicia avanza en la integración de servicios jurídicos y en agilizar todos los trámites relacionados con estos. El investigador Margus Arm junto a un Colectivo de Autores (2019) en el artículo E-Estonia: La e-Gobernanza en la práctica refiere que el Sistema de Información de la Corte (KIS) es el sistema de información (SI) único utilizado por los tribunales estonios de los tres niveles para todo tipo de casos judiciales. Los procesos judiciales totalmente automatizados y las herramientas de comunicación electrónica hacen del sistema judicial estonio uno de los más efectivos del mundo.

El sistema permite registrar todos los casos, audiencias y fallos judiciales en un solo lugar, asignar automáticamente los casos a jueces y juezas, emitir citaciones, publicar las sentencias en la web oficial y recopilar metadatos. Si un ciudadano presenta una reclamación a través del

e-Archivo Público (archivo electrónico), todos los documentos necesarios se cargan automáticamente en el KIS y el secretario o secretaria judicial puede iniciar un nuevo caso con unos pocos clics.

El procedimiento es el mismo para los casos penales enviados al tribunal desde la oficina del fiscal. Cuando un tribunal carga un documento en el KIS, se envía a través del X-Road al e-Archivo, un sistema integrado para los procedimientos que permite el intercambio simultáneo de información entre las partes (SI de la fiscalía, de la policía y de la prisión). Las partes que participan en los procedimientos también pueden presentar documentos al tribunal y hacer un seguimiento del proceso a través del e-Archivo Público al iniciar sesión con una tarjeta de identificación o Mobile-ID.

Estos investigadores reconocen entre las ventajas del sistema las siguientes:

- Se aceleran los procedimientos judiciales.
- Permite a los jueces y juezas manejar mejor su carga de trabajo.
- Reduce el tiempo dedicado a la publicación de casos judiciales.
- Permite la generación automática de documentos, como órdenes judiciales estándar.
- Proporciona una mejor visión de los casos y procedimientos.

Por su parte el sistema e-Notaría es una plataforma en línea creada específicamente para ayudar a notarios en su trabajo diario y permitirles una comunicación electrónica fácil con las agencias gubernamentales, incluidas las consultas de registro.

El sistema es propiedad de la Cámara de Notarios el Centro de Registros y el Centro de Registros y Sistemas de Información (RIK) administra los servidores. También proporciona soporte y capacitación al usuario y se ocupa del desarrollo continuo del sistema. La plataforma e-Notaría solo pueden utilizarla los notarios y los empleados de notarías, por ejemplo, diputados de notarios, abogados, secretarios, recepcionistas y empleados de archivos. e-Notaría permite a los usuarios consultar dieciséis registros diferentes.

En relación con lo anterior mencionan como ventajas que:

- Se pueden programar las actividades notariales.
- Permite la preparación de acuerdos, con firma digital.
- Pueden realizarse consultas fiables a registros estatales.
- Es posible reenviar documentos a los registros estatales.

- Se minimizan los trámites en papel, la impresión y las entradas duplicadas de datos.
- Se reduce la burocracia entre los notarios y los clientes, de modo que los notarios hacen negocios de una forma más rápida.

Otro servicio electrónico importante es el e-Registro de la Propiedad, que está enlazado con la base de datos oficial que recoge información sobre la propiedad y los derechos reales limitados que gravan las hipotecas sobre bienes inmuebles en Estonia. Este registro electrónico ha transformado la forma de realizar las transacciones de propiedades en el país, eliminando la necesidad de visitar una oficina pública y pasar horas esperando para que un funcionario público revise los documentos.

Este sistema sin papel ha reducido significativamente el tiempo de proceso para las transacciones de terrenos. Como herramienta esencial para el mercado inmobiliario, garantiza la transparencia, ya que muestra el propietario registrado, indica los límites de las propiedades y proporciona otra información relevante (también información catastral, gravámenes e hipotecas, entre otros) a compradores potenciales. Además, las empresas también se benefician de la comodidad de acceder instantáneamente a la información del registro de terrenos, y de la capacidad de conocer quién es el propietario o propietaria con solo unos clics.

Las principales ventajas radican en que se consulta fácilmente la información general de una propiedad. Se accede cómodamente a los documentos del registro de la propiedad. Es un sistema transparente que reduce el fraude inmobiliario y la corrupción. Ahorra tiempo, reduce los costos administrativos y erradica el uso de papel en la administración.

***Desde el punto de vista técnico soluciona y aporta en los siguientes aspectos:***

-Es uno de los países más avanzados del mundo en transformación digital, donde el 99% de los trámites públicos y privados se hacen online; el celular actúa como documento de identidad, medio de pago y herramienta de firma de cualquier documento y donde el tiempo de creación de empresas es de tres horas.

-Sufrió un ataque informático importante, donde fueron inutilizadas sus infraestructuras críticas, lo que llevó al país a fortalecer el sistema desde el punto de vista de seguridad.

-X-Road, es una plataforma segura de intercambio de datos de código abierto, que permite el acceso a 3000 procedimientos/servicios diferentes. La protección de datos está garantizada mediante el uso de tecnología blockchain.

- Ha sido implementada con éxito en más de 1000 organizaciones en Estonia y otros países.
- Países que han tenido sistemas interoperables propios decidieron implementar X-Road.
- X-Road ofrece una serie de ventajas sobre otras plataformas, incluyendo su flexibilidad, escalabilidad, código abierto y compatibilidad con otras provincias de la región.
- Está diseñada para permitir que diferentes organizaciones intercambien información de manera segura y eficiente, utilizando una infraestructura basada en la nube y de arquitectura modular.
- Su plataforma de código abierto utiliza criptografía de alta calidad y está diseñada para ser altamente escalable.
- Es gratuita.
- Tiene experiencia y éxito, evidenciando madurez y confiabilidad que la posicionan como una solución de alto rendimiento.
- Al tener flexibilidad y escalabilidad su arquitectura permite adaptarla a las necesidades específicas de cada organización, facilitando su crecimiento y expansión a medida que el ecosistema digital se expande.
- Al basar el software de código abierto, la convierte en una solución transparente, accesible y libre de costos de licencia.
- X-Road cuenta con una comunidad colaborativa al tener un grupo de personas de todo el mundo que usan y mejoran la plataforma, compartiendo sus experiencias, ideas y soluciones.
- X-Road permite el desarrollo compatible de la arquitectura de interoperabilidad de las provincias de la región, lo que facilita la integración y el intercambio de datos a nivel regional/nacional.
- La firma digital con sellados de tiempo garantizados por el Estado permite a las personas comunicarse con el Estado o con las empresas.
- En Estonia, los fundamentos más importantes han sido la identificación electrónica o eID (la identidad digital segura) y X-Road (la capa de intercambio de datos para los sistemas de información). Cada estonio tiene una identidad digital emitida por el Estado.
- El sistema proporciona a los ciudadanos un acceso fácil a sus datos y también pueden comprobar que no se utilicen incorrectamente.

-X-Road permite que varias organizaciones y sistemas de información sean interoperables o, en otras palabras, que puedan trabajar juntos para que el ciudadano solo tenga que aportar sus datos una vez.

-Interconexión de las capas de enlace de datos entre dos países.

-X-Road proporciona e-servicios seguros y de alta calidad para ciudadanos, agencias gubernamentales y el sector privado.

-X-Road ofrece las mejores prácticas de Estonia y Europa en la utilización de nuevas tecnologías.

-X-Road es la plataforma que están instalando la mayoría de los países de la región latinoamericana con resultados exitosos, incluso aquellos donde se han desarrollado otros sistemas interoperables propios.

A partir de los criterios de funcionamiento y concentración de información (Naser, 2021) los sistemas interoperables según la bibliografía analizada se clasifican de la siguiente manera:

***Interoperabilidad bilateral o descentralizada:*** En este tipo de interoperabilidad, cada institución establece acuerdos con otras para intercambiar datos, en general a través de un cruce de archivos. Aquí, sin embargo, se originan problemas como la duplicación de archivos y un desorden en la consistencia de los datos, además de constatarse la existencia de acuerdos con múltiples instituciones que a su vez cruzan datos con otras entidades. Si bien este intercambio bilateral constituye un buen primer paso, es necesario evolucionar rápidamente hacia modelos más sostenibles, con un mejor esquema de calidad de datos y de reusabilidad de las integraciones.

***Interoperabilidad centralizada:*** Consiste en montar una gran base de datos a la que todas las instituciones participantes aportan información según las necesidades y donde a su vez pueden solicitar datos. Este tipo de interoperabilidad tiene la ventaja de que los datos están centralizados en un solo lugar y son consistentes. Sin embargo, todavía existe un riesgo elevado de que haya duplicados e inconsistencias entre ellos, debido a que se encuentran tanto en la institución productora como en la base central. Otra desventaja de esta modalidad es que, aunque posibilita hacer consultas de datos, no permite actualizarlos en la fuente o en la institución que los produce pues estas no son interoperables entre sí.

***Interoperabilidad federada con datos en la fuente:*** En este tipo de interoperabilidad, cada institución u organismo produce sus datos e interopera con un ente rector federado. Este, a su vez, canaliza las transacciones hacia el organismo consumidor que solicita los datos y también

genera transacciones de actualización de información de una institución u organismo a otro. El sistema federado registra las transacciones que circulan por su intermedio, pero no almacena bases de datos salvo en aquellos casos en que son necesarias para generar informes que competen a su función federada.

***Interoperabilidad mixta:*** Este tipo combina en dependencia de las necesidades, país, instituciones y objetivo de la interoperabilidad.

### ***Necesidad de la creación de una estrategia de interoperabilidad***

La investigadora Alejandra Naser (2021), teniendo en cuenta una propuesta de la CEPAL sobre este tema estableció varios pasos para organizar una estrategia de interoperabilidad gubernamental los cuales se reflejan a continuación:

#### **A. Paso 1:** Sensibilización, homologación de lenguaje y participación

1. El porqué de la interoperabilidad gubernamental
2. Principales beneficios de la interoperabilidad
3. Principales barreras para la interoperabilidad
4. Gestión del cambio para la interoperabilidad
5. Factores críticos para el éxito de las iniciativas de interoperabilidad
6. Marcos de referencia
7. Otras experiencias

#### **B. Paso 2:** Marco de referencia a utilizar

1. Dimensiones de la interoperabilidad
2. Dominios de la interoperabilidad
3. Principios y recomendaciones de la interoperabilidad

#### **Paso 3:** Situación actual, conceptos, encuesta y métricas

1. Encuesta de diagnóstico
2. Indicadores de impacto

#### **D. Paso 4:** Establecimiento de la estrategia de interoperabilidad

1. Propuesta de valor
2. Ejemplo de propuesta de valor

#### E. Paso 5: Servicios de interoperabilidad

1. Servicios de interoperabilidad legal
2. Servicios de interoperabilidad organizacional
3. Servicios de interoperabilidad semántica
4. Servicios de interoperabilidad técnica
5. Servicios de gobernanza de los servicios públicos integrados

#### F. Paso 6: Procesos de interoperabilidad

1. Gobernanza estratégica de la interoperabilidad
2. Gobernanza de la interoperabilidad
3. Gobernanza de las personas
4. Gobernanza de los servicios públicos integrados
5. Soporte a la interoperabilidad
6. Habilitante de identificación digital
7. Habilitante de ciberseguridad

#### G. Paso 7: Estructura organizacional de interoperabilidad

1. Comité directivo de implementación de la interoperabilidad
2. Comité técnico de implementación de la interoperabilidad
3. Líder de interoperabilidad gubernamental
4. Invitados técnicos y personal de consulta
5. Gestión del cambio
6. Gestión de la comunicación y la difusión.
7. Gestión de personas
8. Gobernanza de la interoperabilidad
9. Gobernanza de los servicios públicos integrados
10. Apoyo para la interoperabilidad

#### H. Paso 8: Modelos de interoperabilidad

1. Interoperabilidad bilateral o descentralizada
2. Interoperabilidad central
3. Interoperabilidad federada con datos en la fuente

#### I. Paso 9: Estrategia de implementación

1. Fase higiénica
2. Fase de madurez
3. Fase permanente
4. Identificación de iniciativas

En Costa Rica se programó un taller técnico de interoperabilidad gubernamental y se diseñó una Estrategia de Interoperabilidad en tres etapas para ejecutarlas en un año. Recientemente en el 2024, en el IV Congreso de Tecnología Transformación digital e interoperabilidad en el sector de la Justicia desarrollado en Guatemala con la participación de expertos en el tema con presencia de varios países de la región latinoamericana llegaban a la conclusión de que a partir de las experiencias se hacía necesario implementar un plan de acción de interoperabilidad que contemplara los aspectos:

-La Necesidad de un Marco Común. El principal objetivo de este plan es definir la interoperabilidad como una meta que mejore tanto la eficiencia como la seguridad en términos más amplios, en todo el sector público y en particular en el sector justicia.

-Integración de Instituciones Clave. Un punto crucial en la discusión fue la importancia de integrar a todas las instituciones clave bajo un marco de intercambio seguro de información. Para esto, es fundamental contar con la participación de instituciones clave como justicia, gobierno, entidades encargadas de garantizar la seguridad en el país y otros organismos.

-El Rol de una Autoridad Central. Uno de los temas más discutidos fue la creación de una autoridad central que supervise y gestione el ecosistema de interoperabilidad. A pesar de que la naturaleza de X-Road permite también un modelo descentralizado, los ponentes coincidieron en que contar con una entidad que coordine estos esfuerzos sería altamente beneficioso. Sin embargo, en ausencia de una institución centralizada, como un Ministerio de Tecnología, los panelistas recomendaron que las instituciones que ya están avanzadas en temas de interoperabilidad tomen la batuta hasta que se establezca un ente rector formal.

-Marco Jurídico y Normativas. Resaltaron la importancia de contar con leyes que garanticen el intercambio de datos seguro y el sistema de interoperabilidad en su conjunto.

-Estrategia de Implementación Técnica: Reconocieron los grandes beneficios de X-Road es su arquitectura modular y su uso de contenedores, lo que facilita su despliegue y su integración con las infraestructuras existentes en cada institución.

-Capacitación y Desarrollo de Capacidades. La capacitación del personal la consideraron un tema fundamental para asegurar el éxito del plan. Coincidieron en que, para que la interoperabilidad funcione, es crucial que tanto los equipos técnicos como los funcionarios públicos reciban una formación adecuada. A medida que más instituciones se unan al ecosistema de X-Road, será necesario establecer unidades de capacitación que puedan preparar a los equipos en temas de interoperabilidad, seguridad de datos y administración de la plataforma.

-Plan de Sostenibilidad. La importancia de crearlo para que garantice la continuidad del proyecto a largo plazo. Esto incluye no solo asegurar los recursos financieros necesarios para el mantenimiento de la plataforma, sino también establecer estrategias de actualización y mejoras tecnológicas para que siga siendo una solución eficiente y segura en el futuro.

-Monitoreo y Evaluación. La necesidad de implementar mecanismos de monitoreo y evaluación para medir el avance y el éxito del plan. Se destacó la importancia de establecer mecanismos que permitan evaluar el rendimiento de la interoperabilidad en términos de eficiencia, seguridad y satisfacción de los ciudadanos. Además, se sugirió la creación de un comité de seguimiento que supervise y coordine los esfuerzos entre las instituciones participantes.

-El Valor de los Pilotos y la Importancia de Empezar Pequeño. Este enfoque permitió a los responsables del proyecto aprender de los errores y ajustar la implementación antes de escalarla a nivel nacional. Una de las principales lecciones fue la importancia de probar la tecnología sin comprometer grandes recursos de entrada, lo que minimizó los riesgos y permitió generar confianza en el sistema.

***El proceso de implementación incluye:***

-La creación de una Autoridad central o habilitarla que coordine todo lo relacionado con la interoperabilidad.

-Determinar una entidad encargada de la Administración de la plataforma, de los más implicados en la interoperabilidad. El objetivo principal es garantizar la gestión transparente,

eficiente y óptimamente equilibrada de los sistemas de información del sector público. Es la que admite la interoperabilidad de las bases de datos, la gestión del ciclo de vida de los sistemas de información y la reutilización de datos al proporcionar metadatos completos y actualizados de los sistemas de información del sector público. Incluye establecer y actualizar una arquitectura legal, organizativa, semántica y técnica.

-El establecimiento del estado legal de la solución de intercambio de datos.

-La configuración de sistemas técnicos.

-La creación de servicios electrónicos.

### ***Requisitos previos***

-Identificador único por entidad. Para que la información entre una sola vez al sistema. Es común en la actualidad que se solicita la misma información de identificación para cualquier gestión.

-Realizar un Marco eID (Identificación Individual Digital).

-Desarrollar un Marco técnico y regulatorio para firmas digitales.

-Tener los registros digitalizados.

-Para garantizar un intercambio de datos uniforme se debe crear un marco regulatorio para el intercambio electrónico de datos.

-Determinar los procedimientos y reglamentos fiables y legítimos de la autoridad rectora con recursos suficientes.

### ***Desarrollo de políticas y directrices.***

-Elaborar un marco general de interoperabilidad. A partir de la necesidad de confeccionar una directiva que contemple la voluntad política del Gobierno para su desarrollo.

-Construir un marco específico que contenga el compromiso de las entidades involucradas para colaborar y compartir información. Este compromiso implica que se deben superar barreras organizativas y establecer acuerdos y colaboraciones entre diferentes actores gubernamentales. Elaborar una metodología de trabajo para las instituciones que participan que contenga aquellos elementos que deben respetar las organizaciones al establecer sistemas internos de interoperabilidad. Es un desafío importante que la interoperabilidad se adopte hacia el interior de las entidades, las cuales deberán llevar a cabo una transformación cultural

para capacitarse y adaptarse a las nuevas formas de intercambio de información y además colaborar entre sí para alinear y coordinar procesos que hagan fluido el intercambio.

-Definir la arquitectura de interoperabilidad.

-Establecer normas para la arquitectura semántica. Implica la adopción de estándares y vocabularios compartidos para la interpretación correcta de la información.

-Desde la arquitectura técnica normar la definición del tipo de Servidor, lenguaje de programación, autenticación y autorización y metadatos.

-Evaluación del marco de e-gobernanza.

-Elaborar y normar la política para el intercambio de datos.

-Confeccionar una metodología que contenga los parámetros a llenar para garantizar una auditabilidad eficiente micro y macro.

-Establecer las directrices para realizar controles rutinarios y sistemáticos a cualquiera de los componentes del sistema.

-Instituir reglas explícitas para el reciclaje de datos, asegurando la interoperabilidad de los sistemas.

### ***Desarrollo de legislaciones***

-Es necesario que exista el marco legal adecuado, que otorgue a las entidades las facultades y mecanismos necesarios para intercambiar información de manera segura y confiable, lo que implica la revisión y la actualización de las leyes y regulaciones existentes: Legislaciones y normativas para el sector público y de las TICs.

-Establecer las normas de intercambio de datos. Definición de datos/información en el contexto técnico e interoperable. Es necesario que se establezcan las medidas adecuadas que garanticen la confidencialidad, integridad y disponibilidad de los datos compartidos, así como cumplir con las regulaciones y políticas de privacidad.

-Legislar sobre la arquitectura legal, estableciendo elementos de obligatorio cumplimiento para garantizar un intercambio efectivo. Entre otros sobre el compartir y reutilizar los metadatos de manera obligatoria y se exige por ley.

-Que la Ley garantice el libre acceso a los contenidos individuales de los ciudadanos en la plataforma garantizado la democracia; regular el uso, la distribución y la modificación de los contenidos de la plataforma.

-Regular la arquitectura organizativa. La documentación y el intercambio de bases de datos públicas y los metadatos de los sistemas de información deben ser obligatorios y aplicados por ley.

-Establecer las normas de seguridad/ciberseguridad.

-Regular sobre cómo actuar y qué hacer ante los rápidos cambios tecnológicos y los procesos de adaptabilidad del sistema a estos cambios. Empleo efectivo de normas habilitantes, definición de en qué consisten estas para los contextos tecnológicos.

### ***Capacidad organizacional***

-Definición de la estructura, los roles y las responsabilidades de las organizaciones coordinadoras.

-Apoyo al establecimiento de centros de intercambio de datos.

-Definición de las instituciones/organizaciones que formarán parte del sistema.

-Abarcar los aspectos relacionados con las estrategias de cada organización para adoptar el cambio cultural interno que la interoperabilidad conlleva, adopción de nuevas tecnologías, redefinición de procesos, etc.

### ***Soporte técnico***

-Instalación de equipos y programas.

-Creación e instalación de soluciones para registros básicos que permitan la conexión de sus servicios a los sistemas de interfaz de usuarios (front-end).

-Desarrollo e instalación de soluciones para sistemas de interfaz de usuarios (front-end) que respondan a las necesidades de los funcionarios públicos, los ciudadanos y el sector privado.

### ***Educación y sensibilidad***

-Realizar eventos de sensibilización.

-Disponer de materiales, análisis y trabajos de investigación.

-Capacitación para administradores de centros para la plataforma.

-Capacitación para administradores de sistemas de información.

-Formación para desarrolladores de servicios.

-Formación para legisladores de normativas sobre componentes técnicos a tener en cuenta.

## *Seguridad/ciberseguridad*

- Autenticación
- Control de Acceso
- Integridad de mensaje
- Confidencialidad
- Referencia temporal
- Prueba de envío/recepción
- Integridad de registros de intercambio

El Ministerio de Justicia desarrolla una estrategia hacia la transformación digital. En este sentido avanza hacia la digitalización de los servicios, facilitando la creación de una base de datos nacional. Además, tiene una estructura desde la nación hasta los municipios que proponemos pudiera ser el piloto para probar la tecnología X-ROAD. También desarrolla la inteligencia artificial para optimizar tiempo, logrando calidad y agilidad en los servicios que brinda a la ciudadanía, en estos aspectos cuenta con la colaboración de instituciones como XETID y DATYS.

Partiendo de la idea de realizar un piloto en pequeño para una posterior implementación en el país deben seguir los siguientes pasos:

- ✓ **Prueba de Concepto:** tiene como objetivo demostrar la viabilidad tecnológica y práctica de un producto, método o idea propuesta. Busca validar que la solución propuesta puede funcionar en la práctica. Implica la creación de un entorno de pruebas que simule el funcionamiento real y, a partir de este, se desplegará un caso de uso para evaluar su efectividad y prepararse para el eventual despliegue del entorno de interoperabilidad.
- ✓ **Análisis del ecosistema:** identificar los elementos de la estructura y el modelo organizativo para la institución.
- ✓ **Identificación del Operador de la plataforma:** Se designa como Operador a la entidad o departamento que administra. En este caso el Departamento de Informatización del MINJUS.
- ✓ **Identificación de los miembros de la plataforma:** Los Miembros son las entidades que requieren participar en el intercambio de datos a través de la plataforma.

- ✓ **Identificación de los Sistemas de Información (SI):** es el conjunto de componentes tecnológicos que almacenan la información de una entidad, que contiene los datos de las instituciones o estructuras que participan y pueden proporcionar la información necesaria.
- ✓ **Identificación de los Servidores de Seguridad (SS):** Los Servidores de Seguridad son los componentes de la plataforma que facilitan la comunicación entre los Sistemas de Información. Cada SI debe conectarse a un SS, que será propiedad de un miembro de la plataforma. Por lo tanto, la comunicación en la red se lleva a cabo entre los SS.
- ✓ **Identificación del Servidor Central (SC):** Toda implementación de X-Road requiere un Servidor Central. En nuestra situación, el SC será propiedad de MINJUS y será operado por el Departamento de Informatización, que actúa como el Operador de central de la plataforma.

La implementación de iniciativas de interoperabilidad demanda un cambio de paradigma que comprende, al menos, los siguientes aspectos:

- Cambio cultural: servir a la ciudadanía. Por consiguiente, el usuario (ciudadano) está en el centro de la gestión de la institución.
- Cambios en los procesos: diseñados para servir a los habitantes del país, procurando eficiencia y eficacia en el servicio.
- Cambios en la institución: se organizan de manera coordinada y armoniosa, propiciando la visión compartida de sus aspectos estratégicos.
- Cambio en las formas de relación: se propicia una relación cercana con la ciudadanía, garantizando un trato igualitario y no discriminatorio.

Según Naser (2021) es frecuente que las iniciativas de interoperabilidad no fluyan con la urgencia que se requiere. Esto se debe a diversos factores entre los más reiterados menciona:

- ✓ Barreras de competencias. Las instituciones no cuentan con personal con las competencias, la dedicación y las atribuciones suficientes para impulsar iniciativas de interoperabilidad.
- ✓ Barreras tecnológicas. Las diversas instituciones y organizaciones emplean tecnologías de información incompatibles para procesar e intercambiar datos.

- ✓ Barreras conceptuales. Las partes que interoperan someten la información de interés común para las instituciones u organizaciones a distintas conceptualizaciones e interpretaciones.
- ✓ Barreras organizacionales. Las distintas instituciones y organizaciones tienen diferentes estructuras organizativas y personas asignadas con diversas responsabilidades y niveles de autoridad.
- ✓ Barreras originadas en las leyes y en la normatividad. Cada país y cada institución tienen un conjunto de leyes y normas que deben considerarse en la definición del modelo de interoperabilidad.
- ✓ Barreras por intereses políticos o pérdida de poder. La interoperabilidad contribuye a la transparencia en el tratamiento de la información entre instituciones y a la independencia del ciudadano en los puntos presenciales de atención, fuentes de poder e influencia (no siempre bien gestionada).

Como en cada organización o institución deben abordarse las cuatro dimensiones de la interoperabilidad, permitiendo establecer alguna metodología a seguir para alcanzar el éxito de un proyecto, pasaremos a analizar los diferentes elementos formativos de estas. Estos cuatro dominios planteados son: Organizacional, Técnico, Semántico y Legal.

### **Desde el punto de vista organizacional**

Avanzar hacia la interoperabilidad en la administración pública diaria requiere cambios organizativos y administrativos considerables. Sin esos cambios, los beneficios esperados quedarán en solo un sueño. Según (Arm, 2019) en el caso particular de Estonia se implementó lo que se llamó formulación de políticas impulsada por el desarrollo, y no desarrollo impulsado por las políticas, durante los primeros 5 a 10 años de su planificación e implementación de e-gobierno. Muchos aspectos de la política y la estrategia del e-gobierno se establecieron solo después de su implementación tecnológica.

La política básica de e-gobierno se fijó cuando el Parlamento adoptó los Principios de la Política de Información. Estos principios se revisaron y se actualizaron mientras se preparaba la Estrategia de la Sociedad de la Información. Entre ellos se mantienen los siguientes:

- ✓ El desarrollo de la sociedad digital es una decisión estratégica para mejorar la competitividad del Estado y aumentar el bienestar general de sus ciudadanos.

- ✓ El sector público lidera el camino en la búsqueda de los principios para el desarrollo de la sociedad digital. Se garantizará la protección de las libertades y derechos fundamentales, los datos personales y la identidad. Los individuos son los propietarios de sus datos personales y podrán controlar cómo se utilizan.
- ✓ El sector público organizará sus procesos para garantizar que los ciudadanos, empresarios y organismos públicos tengan que proporcionar cualquier dato una sola vez.
- ✓ La sociedad digital se desarrollará en cooperación entre los sectores públicos, privados y terceros, así como todas las demás partes, incluidos los usuarios de soluciones de las TIC.
- ✓ La continuidad de la lengua y la cultura de Estonia se garantizará cuando se desarrolle la sociedad digital.
- ✓ La sociedad digital se creará para todos los residentes del país, y también se prestará especial atención a la integración de los grupos sociales con necesidades especiales, al desarrollo regional y al fortalecimiento de las iniciativas locales. Todo el mundo debería tener acceso al internet.

Con el objetivo de crear y gestionar la sociedad digital mediante el desarrollo de ejes fundamentales accesibles, relevantes, innovadores y sostenibles de la e-gobernanza este país se trazó varios ejes a tener en cuenta para lograr un desarrollo exitoso de la interoperabilidad. Estos ejes contemplan los aspectos que a continuación se mencionan:

- ❖ Gestión de la ciberseguridad
- ❖ Legislación
- ❖ Democracia electrónica
- ❖ Instituciones y su papel en la gobernanza electrónica
- ❖ Programas educativos
- ❖ Infraestructura de interoperabilidad y habilitadores
  - ✓ Red de Internet
  - ✓ Identidad electrónica
  - ✓ Intercambio seguro de datos - X-Road
  - ✓ Catálogo de soluciones de interoperabilidad

- ✓ Sistema de direcciones
- ✓ Registros de base
- ✓ Portales de servicios
- ✓ Infraestructura de datos abiertos
- ✓ Infraestructura de datos espaciales
- ✓ Sistema de seguridad informática
- ✓ Nube gubernamental

Al respecto de las cuestiones organizativas el Ministerio de Asuntos Económicos y Comunicación de Estonia es el que ha desarrollado los principios de las políticas de información y la legislación de apoyo, y ha asumido la responsabilidad de supervisar a las organizaciones estatales oportunas. Principalmente, son los ministerios pertinentes y las agencias estatales quienes manejan los desarrollos del e-gobierno. Cada departamento gubernamental, ministerio o empresa elige su propia tecnología, a partir de principios acordados de forma conjunta.

De manera general se han basado en el desarrollo de políticas centralizadas, pero con una implementación descentralizada, con una neutralidad de las plataformas tecnológicas, un modelo funcional para la protección de datos personales, medidas para eliminar la brecha digital, un sector público transparente y eficiente y manteniendo una sistemática orientación al ciudadano o el cliente.

La ciberseguridad la manejan desde un enfoque organizativo para garantizar el eficiente funcionamiento de la plataforma sin que sufra alteraciones por agentes externos. Al respecto aplican la filosofía del diseño seguro a los sistemas electrónicos y la sociedad digital.

Utilizan “ciberseguridad” como un término general para la protección de datos o informaciones digitales, datos personales en formato electrónico, seguridad informática, seguridad de red, seguridad de los servicios electrónicos, seguridad de las TIC y seguridad cibernética, entre otros. La ciberseguridad es uno de los temas más importantes en el país, ya que la sociedad digital depende en gran medida de su infraestructura de TIC y servicios electrónicos. Por tanto, el país se ha asegurado de que las soluciones electrónicas no sean un talón de Aquiles para la sociedad, sino una base segura para el desarrollo moderno. En este contexto, la ciberseguridad no es el freno que restringe la digitalización, sino el habilitador que hace posible la innovación digital rápida (Arm, 2019).

Para manejar estas ciberamenazas, se debe contar con la legislación y la capacidad organizativa adecuadas para la seguridad básica, la gestión de incidentes y crisis, además de procedimientos, herramientas y habilidades para combatir los delitos informáticos, y la capacidad para las operaciones militares. En Estonia desarrollaron el Marco Nacional de Ciberseguridad que ayuda a organizar la ciberseguridad a nivel nacional y a comprender cómo debe organizarse el área de ciberseguridad a nivel estatal, y los roles y responsabilidades que deben compartirse. El gobierno necesita un estándar en ciberseguridad y capacidad de gestión de incidentes.

Entre los aspectos destacados de la ciberseguridad destacan a X-Road como un modelo seguro para el Internet, lo ven como el “territorio protegido” de Estonia en el ciberespacio. Todas las e-soluciones de Estonia, que utilizan varias bases de datos, utilizan X-Road. Todos los datos salientes están firmados y encriptados digitalmente. Todos los datos entrantes son autenticados y registrados.

En Estonia, las funciones y responsabilidades de ciberseguridad más importantes se comparten entre el Ministerio de Asuntos Económicos y Comunicaciones, el Ministerio del Interior y el Ministerio de Defensa.

La Autoridad del Sistema de Información de Estonia, en la jurisdicción del Ministerio de Asuntos Económicos y Comunicaciones, es responsable de la implementación práctica de las tecnologías de interoperabilidad y la ciberprotección. El Equipo Nacional de Respuesta a Emergencias Informáticas (en inglés CERT) está ubicado en esta Autoridad, así como en la Unidad de Protección de la Infraestructura de Información Crítica (en inglés CIIP). Todo lo anterior regulado mediante legislaciones, normativas y directrices de ciberseguridad.

En la cabeza organizativa se encuentra el Gobierno con la **Oficina del Gobierno** la cual tiene la función de apoyar al Gobierno de la República de Estonia y al Primer Ministro en la planificación e implementación de las políticas y en garantizar la buena gobernanza. Se le subordina el CONSEJO DE E-ESTONIA. Es una entidad de coordinación de la sociedad de la información liderada por el Primer Ministro. Dirige el desarrollo de la sociedad digital y la e-gobernanza del país, en especial la implementación de la agenda digital nacional y la UNIDAD DE COORDINACIÓN DE SEGURIDAD NACIONAL Y DEFENSA que asesora al Primer Ministro en temas de seguridad nacional —incluida la ciberseguridad— organiza los asuntos del Comité de Seguridad del Gobierno y coordina la seguridad y la defensa nacional.

El **Ministerio de Asuntos Económicos y Comunicaciones** desarrolla las políticas y coordina el progreso de la sociedad digital de Estonia y la ciberseguridad nacional. Cuenta con las siguientes organizaciones subordinadas relacionadas con la gobernanza electrónica y la ciberseguridad: Autoridad del Sistema de Información de Estonia. Autoridad Reguladora Técnica. Fundación de Internet de Estonia. Fundación Infocomunicación del Estado. Cada una con funciones específicas a cumplir.

El **Ministerio del Interior** y sus agencias trabajan para garantizar que todos los residentes de Estonia se sientan seguros, para proteger las fronteras del país y para mantener el orden público. El Ministerio es responsable de las políticas de administración de identidades—incluida la e-identidad—, la lucha contra el ciberdelito y el ciberterrorismo, y la gestión de crisis. El Ministerio tiene las siguientes organizaciones subordinadas relacionadas con la gobernanza electrónica y la ciberseguridad: Oficina de la Policía y de la Guardia de Fronteras. Servicio de Seguridad Interna de Estonia. Centro de Informática y Desarrollo.

Una función más amplia del servicio es mantener la seguridad nacional mediante la recopilación de información, la aplicación de medidas preventivas y la investigación de delitos. Una función importante del servicio relacionada con la sociedad de la información es la verificación de seguridad de los usuarios de secretos de Estado y la información clasificada de Estados extranjeros. La misión del centro de Informática y Desarrollo es proporcionar, desarrollar y mantener comunicaciones, sistemas de información y servicios para el Ministerio del Interior y sus organizaciones subordinadas. El centro también gestiona el Registro de Población de Estonia.

El **Ministerio de Defensa** con sus subordinaciones es responsable de organizar la defensa nacional —incluida la ciberdefensa— evitando los ataques contra Estonia y garantizando que el país sea capaz de defenderse contra amenazas externas.

El **Ministerio de Justicia** con sus organizaciones subordinadas es responsable del desarrollo de la política legislativa nacional y de la administración de los registros nacionales, como el Registro de Empresas, con la gobernanza electrónica y la ciberseguridad. Se le subordinan el Centro de Registros y Sistemas de Información. Inspectoría de Protección de Datos. Instituto Forense de Estonia.

El Centro de Registros y Sistemas de Información tiene como objetivo establecer un entorno innovador que brinde e-servicios bien integrados para la implementación más eficiente de las políticas estatales, legales y penales. Desarrolla y administra los registros y los sistemas de

información de muy alta importancia para el Estado y sus ciudadanos, por ejemplo, el e-Registro de Empresas, el sistema de e-Notaría, el e-Catastro, el Sistema de Información de las Cortes, el Registro de Supervisión de Libertad Condicional, el Registro de Reclusos, la Base de datos de Antecedentes Penales, el e-Archivo y el Boletín Oficial del Estado, entre otros.

La Inspección de Protección de Datos es una organización independiente que supervisa a las entidades del sector público y privado con respecto a sus derechos y obligaciones de protección de datos. Defiende los derechos constitucionales de los ciudadanos a obtener información sobre las actividades de las autoridades públicas. La inviolabilidad de la vida privada y familiar en el uso de datos personales. Acceder a los propios datos que se conservan.

La responsabilidad del **Ministerio de Educación e Investigación** es desarrollar la estrategia nacional de educación en TIC e integrar las TIC en todos los niveles del sistema educativo. Cuenta con los Archivos Nacionales como organización subordinada relacionada con la gobernanza electrónica y la ciberseguridad. Entre otras funciones, los Archivos Nacionales: Participan en el desarrollo de la gestión nacional de registros electrónicos. Desarrollan y ponen en práctica los archivos digitales hasta su máximo potencial. También se le subordina el Consejo para la Educación y la Juventud (HARNO), que tiene la misión de desarrollar y gestionar los sistemas de información educacional, los e-servicios y fomenta, desarrolla y pone a prueba la innovación en las áreas de la educación y la juventud.

En esencia en el organigrama organizativo de Estonia las entidades reguladoras de las políticas son:

- Ministerio de Asuntos Económicos y Comunicaciones
- Ministerio del Interior
- Ministro de Defensa
- Ministerio de Justicia
- Ministerio de Educación e Investigación

Las entidades que participan como ejecutoras, muchas subordinadas a las anteriores son:

- Autoridad del Sistema de Información.
- Autoridad Reguladora Técnica.
- Fundación Internet de Estonia.

- Fundación Infocomunicaciones del Estado.
- Policía y Guardia de Fronteras.
- Servicio de Seguridad Interna.
- Centro de Informática y Desarrollo.
- Fundación Nacional de Sociedad Civil.
- Fuerzas de Defensa (Cibercomando).
- Liga de Defensa.
- Servicio de Inteligencia Exterior.
- Centro de Registros y Sistemas de Información.
- Inspección de Protección de Datos.
- Instituto Forense de Estonia.
- Consejo para la Educación y la Juventud (HARNO)
- Archivos Nacionales

También se integran universidades del ámbito académico como grupo de expertos, entidades de negocios relacionadas con desarrollo tecnológico, ONGs.

| <b>Servicio de interoperabilidad organizacional</b>                                   |  |   |
|---|--|---|
| <b>Servicio</b>   | <b>Responsabilidad de la institución de interoperabilidad</b>  | <b>Responsabilidad de otras instituciones</b>   |
| Alineamiento de los procesos institucionales  | Entender globalmente (de extremo a extremo) los procesos institucionales asociados a servicios al ciudadano y la función de las instituciones dentro de dichos procesos. | Participar activamente en el levantamiento, la especificación y el rediseño de los procesos involucrados en el ofrecimiento de un servicio interoperable al ciudadano |
| Estructura clara de la relación entre los proveedores de servicios y los consumidores | Estructurar claramente la relación entre los proveedores de servicios y los consumidores.  | Participar activamente en la especificación del papel de la institución (proveedora o consumidora) en el ofrecimiento de un servicio interoperable al ciudadano.      |
| Contribución a la formalización de la asistencia                                      | Contribuir a formalizar la asistencia mutua, la  | Establecer, en conjunto con las otras instituciones   |

|   |  |  |
|---|--|--|
| mutua, la actuación conjunta y los procesos institucionales interconectados | actuación conjunta y los procesos institucionales interconectados (por ejemplo, mediante memorandos de entendimiento y acuerdos de prestación de servicios (APS) entre las instituciones participantes). | involucradas en un servicio interoperable, los acuerdos de asistencia y los niveles de servicios necesarios. |
|---|--|--|

**Desde el punto de vista técnico**

Con una alta tasa de penetración de internet, servicios de e-gobierno generalizados y comercio electrónico integrados en la vida cotidiana de los individuos y las organizaciones, Estonia se ha convertido en un modelo del acceso gratuito a la red como motor de desarrollo para la sociedad. De hecho, en el país se considera que el acceso a internet es un derecho humano. Miles de lugares públicos disponen de conexiones inalámbricas (WiFi) certificadas y la cobertura de las redes digitales de telefonía móvil (banda ancha móvil 4G) abarca casi todo el territorio. La velocidad de descarga máxima disponible de la conexión 4G en dispositivos de alta movilidad es de 100 Mbit/s (Arm, 2019).

La generación está conformada geográficamente por tres partes distintas:

La RED TRONCAL NACIONAL, conecta las redes troncales regionales en ciudades y centros más grandes. El equipo utilizado en la red troncal nacional permite transportar e intercambiar grandes cantidades de información entre diferentes ubicaciones y operadores.

La RED TRONCAL REGIONAL (milla intermedia, red de retorno), Conecta varias redes de acceso que agregan el tráfico local más arriba en la red. Es el enlace de conexión entre las redes de acceso y la red troncal nacional. También conecta los dispositivos de red de la región entre ellos, lo que permite que se transmitan datos.

La RED DE ACCESO (último kilómetro de la conexión), es la parte de la red más próxima al consumidor y la que conecta sus dispositivos al punto de conexión de la red troncal regional más cercana. Estonia cuenta con redes cableadas e inalámbricas.

Entre los elementos que tienen en cuenta para la generación de proyectos de colaboración de banda ancha entre el sector público y el privado están las siguientes etapas:

-ESTABLECIMIENTO DE OBJETIVOS. El plan de banda ancha debe definir objetivos concretos para la cobertura en el municipio o la región, esquematizando la situación existente

de la infraestructura de banda ancha, el mercado, los servicios, y la competencia, entre otros, así como la previsión de la demanda, del mercado y de los desarrollos tecnológicos.

-CREACIÓN DE MODELOS. Los modelos deben basarse en una comprensión clara del alcance deseado de la intervención en el mercado y de los riesgos que se deben tomar. Posteriormente, se puede tomar una decisión sobre el tipo y nivel de intervención, es decir, para el mercado mayorista (infraestructura y nivel de conexión) o el minorista (nivel de servicio), y la extensión del proyecto (a nivel nacional, regional, red completa, red troncal o red de acceso).

-PLAN DE NEGOCIO Y FINANCIAMIENTO. El proyecto se puede implementar a partir de un plan de negocios a largo plazo. Aunque obtener ganancias no es el objetivo de los proyectos públicos de banda ancha, un plan de negocios es la base tanto de la financiación como de la operación. Se debe reunir un paquete de financiamiento de tarifas de usuarios de la red, subvenciones y préstamos a largo plazo para financiar el proyecto.

-PLAN DE ACCIÓN E IMPLEMENTACIÓN. El plan de acción debe cubrir las actividades detalladas de planificación, construcción y comercialización de la red. La supervisión del proyecto, el control de los resultados y los procedimientos para realizar posibles cambios también deben acordarse al principio.

El siguiente paso desde el punto de vista técnico es contar con un sistema integral de identificación electrónica, autenticación y firma electrónica. La identificación electrónica y los servicios de confianza para transacciones electrónicas están regulados por la Ley de Identificación Electrónica y Servicios de Confianza para las Transacciones Electrónicas y el reglamento directamente aplicable eIDAS (No. 910/2014) de la UE.

Para otorgar firmas electrónicas, las tarjetas de identificación se utilizan con el programa de código abierto aprobado por el gobierno llamado DigiDoc, desarrollado y mantenido por la Autoridad del Sistema de Información de Estonia. Las firmas electrónicas creadas con las eID emitidas por el Gobierno son tan legalmente vinculantes como las manuscritas, al igual que las firmas electrónicas creadas con Smart-ID.

En Estonia, la identidad de una persona se basa en un código de identificación individual permanente denominado código de identificación personal (CIP), que se introdujo en 1992. El CIP se genera de acuerdo con la Norma estonia EVS 585:2007 Código Personal. Estructura, la Ley de Registro de Población y un reglamento sobre la generación de los CIP. De conformidad con la Ley de Registro de Población, el CIP es una combinación única de

números basada en el sexo y la fecha de nacimiento, que permite la identificación de una persona específica. El CIP no se considera información personal confidencial y es público según sea necesario para identificar a una persona. La nueva versión consolidada de la Ley de Registro de Población entró en vigor el 1 de enero del 2019, mientras que los principios básicos del registro de población se mantuvieron sin cambio alguno.

Todos los certificados contienen el CIP, que se utiliza como clave principal para la mayoría de las bases de datos que contienen información personal, tanto en el sector público como en el privado. Además, los archivos firmados electrónicamente contienen un certificado del firmante (que a su vez contiene su CIP), que permite identificarlo definitivamente. Los datos en la tarjeta de identificación (es decir, el archivo de datos y los certificados) están disponibles para cada terminal de tarjeta, ya que no están protegidos contra lectura. El certificado de autenticación está disponible para el proveedor de servicios al iniciar sesión correctamente. El certificado de firma electrónica está disponible para todos los que vean el documento firmado electrónicamente. Como resultado, el CIP en el archivo de datos o en el certificado está disponible durante cada transacción electrónica con cualquier tipo de portador de eID (Procedimiento de Formación y Distribución del Número de Identificación Nacional).

La infraestructura de clave pública (PKI por su sigla en inglés) permite la autenticación segura y la firma electrónica, y proporciona un medio para la transferencia segura de datos cifrados. Estonia utiliza una PKI nacional, lo que significa que el Estado se compromete a garantizar la existencia y el funcionamiento de la infraestructura de clave pública. Aunque una gran parte de los servicios relacionados con la PKI se compran del sector privado (por ejemplo, emisión de certificados, confirmación de validez de certificados, distribución de la clave pública), la preparación del entorno de generación de claves (por ejemplo, tarjeta de identificación o tarjeta SIM) y la personalización de los documentos -problemas más importantes de PKI- aún los maneja el Estado:

**MINISTERIO DEL INTERIOR:** redacta la legislación que determina los tipos y requisitos de los documentos de identidad electrónicos. **La OFICINA DE LA POLICÍA Y DE LA GUARDIA DE FRONTERAS:** emite documentos de identidad personales (electrónicos) que permiten la autenticación electrónica segura y la firma electrónica (tarjeta de identificación u otras tarjetas inteligentes).

**MINISTERIO DE ASUNTOS ECONÓMICOS Y COMUNICACIONES:** redacta la legislación que regula los servicios de identificación electrónica y de confianza para transacciones electrónicas. **La AUTORIDAD DEL SISTEMA DE INFORMACIÓN (RIA):**

desarrolla aplicaciones de software, necesarias para usar la PKI (middleware de la tarjeta de identificación, incluidos los controladores, software de utilidad y del cliente). Determina los requisitos de calidad y fiabilidad de los servicios de la PKI.

La tarjeta de identificación es el único documento de identificación obligatorio en Estonia. Tiene un suplemento digital llamado Digital ID (Digi-ID), que es un documento electrónico emitido por el Estado para la identificación electrónica y la creación de firmas electrónicas.

Los documentos en formato ID1 —definidos por el estándar ISO/IEC 7810— se basan en la tecnología PKI e incorporan dos certificados, uno para la autenticación y el otro para las firmas electrónicas. Cada clave privada depende del uso de un PIN diferente.

La tarjeta de identificación de Estonia proporciona acceso digital a todos los servicios electrónicos seguros disponibles. El chip de la tarjeta transporta archivos incrustados que, mediante el cifrado de clave pública RSA o ECC, permiten que se utilicen como prueba definitiva de identificación en un entorno electrónico. Puede usarse para identificación personal, para firmar documentos electrónicamente y para funciones de cifrado de datos. Las tarjetas de identificación requieren un lector de tarjetas especial, y para las firmas electrónicas, el programa especial DigiDoc (Especificaciones de la solicitud de la tarjeta Certificados y validez).

El Mobile-ID es un documento electrónico de identificación personal que permite el uso de un teléfono móvil para la identificación y las firmas electrónicas. El 99% de los dispositivos en el mercado son compatibles con el Mobile-ID. Con el Mobile-ID, la tarjeta SIM funciona simultáneamente como tarjeta de identificación y como lector de tarjetas de identificación. No puede utilizarse para el cifrado de documentos. Sin embargo, tiene la gran ventaja de no requerir un lector de tarjetas especial, por lo que resulta más cómodo y flexible para los usuarios. En el 2011, Mobile-ID fue promovido al estado de documento nacional de identificación electrónica en Estonia, lo que significa que funciona en condiciones iguales a la tarjeta de identificación.

El Mobile-ID requiere una tarjeta SIM especial que habilita el servicio y que se suministran con applets dedicados al Mobile-ID durante la producción. La solución estonia de identificación móvil basada en PKI corresponde a los algoritmos criptográficos de seguridad ECC y SHA2. Nivel de evaluación: EAL4+ (Soluciones SK ID. Seguridad). También se usa un canal de SMS, es decir, que los teléfonos no inteligentes también son compatibles con la solución Mobile-ID.

Las tres organizaciones principales que participan en la emisión y operación de Mobile-ID y la infraestructura asociada en Estonia son:

-LA OFICINA DE LA POLICÍA Y DE LA GUARDIA DE FRONTERAS es la agencia gubernamental responsable de emitir documentos de identificación personal a ciudadanos estonios y otros residentes, según lo exigido por la Ley de Documentos de Identidad;

-TODOS LOS OPERADORES DE REDES MÓVILES (ORM) líderes en Estonia actúan como Autoridades de Registro y ofrecen tarjetas SIM con capacidad de identificación móvil;

-LA AUTORIDAD DE CERTIFICACIÓN mantiene la infraestructura electrónica necesaria para Mobile-ID y es el proveedor del servicio Mobile- ID en nombre de los ORM.

La herramienta para la firma electrónica es DigiDoc Client, es un programa incluido en el paquete eID y un sistema de uso amplio en Estonia para compartir y firmar documentos electrónicamente, ya que la mayoría de los dispositivos de los usuarios finales lo admiten. Puesto que las firmas electrónicas tienen el mismo valor legal que las firmas manuscritas en Estonia, se requiere una plataforma segura y fácil de usar para que las entidades gubernamentales, empresas y personas puedan transferirse archivos.

Cada usuario de eID puede firmar un documento electrónicamente y enviarlo a otras partes. Mientras que los usuarios tienen el programa DigiDoc, los proveedores de e-servicios utilizan partes del programa de código abierto proporcionados por la Autoridad del Sistema de Información. Tiene como ventajas el intercambio rápido de documentos. Reducción de gastos de negocios directos e indirectos. Menor riesgo de falsificación y fraude gracias a sellos de tiempo y certificados seguros.

Los componentes básicos del programa utilizados para la autenticación están disponibles públicamente para todos. Por lo tanto, cualquier organización puede crear aplicaciones y procesos de negocios basados en la tarjeta eID como dispositivo de identificación central. Esto ha dado como resultado una adopción generalizada de las funcionalidades de la tarjeta eID.

Los sellos electrónicos los utilizan los organismos legales, como compañías y oficinas estatales, para certificar documentos en grandes cantidades de manera electrónica.

X-Road es el componente principal de la infraestructura de intercambio de datos de Estonia y la columna vertebral de e-Estonia. La experiencia de X-Road fue una de las referencias para diseñar el modelo conceptual para el marco de interoperabilidad europeo. En la actualidad, el modelo estonio se ajusta por completo al modelo conceptual de servicios de la UE.

Los principios de diseño técnico para X-Road proporcionan una plataforma de intercambio de datos distribuida, segura, interorganizacional y unificada.

**ADMINISTRACIÓN DISTRIBUIDA:** X-Road es un sistema completamente distribuido y resistente con administración distribuida que no centraliza los datos ni cambia su propiedad.

**SISTEMA SEGURO:** se ha diseñado a fin de satisfacer los requisitos de seguridad para la interoperabilidad gubernamental y organizativa. X-Road garantiza la autenticidad, la integridad y el no repudio de los datos intercambiados, lo que da como resultado la alta disponibilidad de servicios y la confidencialidad de dichos datos.

**HETEROGENEIDAD:** X-Road conecta sistemas de información construidos en cualquier plataforma. No prescribe ninguna herramienta ni tecnología en particular para el uso interno de las organizaciones.

**FIABILIDAD:** X-Road no tiene un solo punto de falla. Todos los componentes de la infraestructura pueden hacerse redundantes para una alta resiliencia contra fallas y ataques. Los componentes disponibles en una red pública o compartida emplean medidas de protección contra ataques de denegación de servicio.

**CON FEDERACIÓN DE IDENTIDAD:** X-Road permite acuerdos bilaterales entre diferentes instalaciones de X-Road.

**FACILIDAD DE IMPLEMENTACIÓN:** la implementación de la infraestructura de X-Road es rápida y eficiente. eGA ofrece una versión piloto que se puede instalar e implementar muy cómodamente, y con oportunidades de revisión inmediata.

**FACILIDAD DE USO:** X-Road es fácil de adaptar. Todas las comunicaciones se basan en servicios web y, por tanto, cualquier desarrollador puede utilizarlas fácilmente con el adaptador X-Road. Además, el acceso a cualquier otra organización es uniforme. Solo hay una interfaz de programación de aplicaciones, con un conjunto de reglas que deben seguir todos los desarrolladores.

### ***Componentes principales de X-Road***

Los componentes centrales de X-Road constituyen la base tecnológica para ejecutar el marco X-Road. Tres componentes integrales proporcionan la capacidad tecnológica para la capa de intercambio de datos X-Road:

**SERVIDOR DE SEGURIDAD.** El servidor de seguridad actúa como una puerta de enlace entre los sistemas de información de los proveedores de servicios y la infraestructura de X-

Road. Transmite las solicitudes y los mensajes de respuesta mientras proporcionan una capa protectora. Todos los mensajes se intercambian a través de un canal criptográficamente seguro. Además, los mensajes están firmados digitalmente y con sellado de tiempo para garantizar la autenticidad de las transacciones a largo plazo.

REGISTRO (SERVIDOR CENTRAL). El registro de X-Road mantiene la información sobre las autoridades de certificación y los servicios de confianza aprobados, así como sobre los miembros X-Road y los servidores de seguridad. Los servidores de seguridad de los miembros pueden solicitar esta información para determinar si la consulta procede de otros miembros de X-Road, o para encontrar las direcciones de los servicios, etcétera. La autoridad rectora de X-Road es quien mantiene el registro. En Estonia, las funciones de autoridad rectora están a cargo de la Autoridad del Sistema de Información de Estonia.

SISTEMA DE MONITOREO. El sistema de monitoreo recibe información sobre las transacciones de los servidores de seguridad, y la pone a disposición de los administradores del sistema central. El sistema de monitoreo no puede ver los datos reales intercambiados entre socios, sino que reconoce que los datos se intercambian. X-Road contiene estaciones de monitoreo locales, y cada una de ellas recopila continuamente información (de estado, mensajes de error e información de consulta) desde la puerta de enlace local. La información detallada del sistema —como el uso de la CPU y de la memoria, el número de consultas pendientes y mucho más— le brinda al administrador del sistema una descripción completa y precisa del estado de sus servidores y servicios.

El sistema de monitoreo ayuda a la gerencia a tomar decisiones en varios niveles, y permite: Probar que el sistema está funcionando correctamente. Identificar los picos de uso para la planificar la capacidad. Comprender y mejorar los mecanismos de e-gobernanza. Mejorar la seguridad detectando anomalías. Comprender mejor a sus usuarios a partir de los informes de uso de datos. Tomar decisiones a partir de las estadísticas operativas, como qué servicios se han utilizado, cuántas veces, cuál es el tiempo de respuesta promedio, etcétera. Tomar decisiones en función de la métrica del servidor de seguridad disponible, la supervisión del entorno X-Road (los detalles de los servidores de seguridad como el sistema operativo, la memoria, el espacio en disco, la carga de la CPU, los procesos en ejecución y los paquetes instalados, etcétera

SERVICIOS DE CONFIANZA

Proporcionan servicios de certificación y de sellado de tiempo. En casos más simples, puede prestarlos la autoridad de gobierno de X-Road o cualquier autoridad de certificación, que por lo general ofrecen servicios de certificación estándar como: Emisión de certificados para autenticación, firmas digitales y encriptación. Comprobación de validez del certificado. Sellado de tiempo.

## PORTALES

Los portales son un tipo importante de usuario de X-Road. Aunque los portales no son una parte central de X-Road, el sistema incluye soporte para este tipo de soluciones. Permiten a los ciudadanos acceder a los e-servicios gubernamentales. Aceptan la construcción de servicios complejos (agregados). Soportan varios medios de autenticación basados en el sistema nacional de e-identificación. Son accesibles a través de computadoras y dispositivos móviles.

## AUTORIDAD DE GOBIERNO DE X-ROAD

La operación de X-Road en Estonia está garantizada por una autoridad de gobierno central, concretamente por la Autoridad del Sistema de Información de Estonia. Su tarea más importante es garantizar el estado legal del sistema X-Road y la información intercambiada mediante el cumplimiento de las políticas pertinentes. También es responsable de dirigir el desarrollo continuo de X-Road y de garantizar su estabilidad y su integridad.

La autoridad de gobierno de X-Road también es responsable de formular la política de seguridad de la infraestructura, que incluye: Requisitos de seguridad para los miembros de la infraestructura (por ejemplo, requisitos de autenticación de usuario). Categorías de seguridad aplicables a los servicios y sistemas de información, que permiten a los proveedores de servicios especificar formalmente listas de requisitos de seguridad que sus usuarios deben cumplir. Listado de proveedores de servicios de certificación y sellado de tiempo de confianza.

## MIEMBROS DE X-ROAD

Los miembros de X-Road son entidades que desean comunicarse entre sí. El requisito previo es que cada miembro tenga un sistema de información para conectarlo a los sistemas de otros miembros a través de un servidor de seguridad, y que use los servicios de infraestructura X-Road y PKI. Para unirse a X-Road, todos los posibles miembros deben asegurarse de que cuentan con suficientes medidas de seguridad. La autoridad de gobierno de X-Road se reserva el derecho de revisar las políticas de seguridad y los procedimientos operativos. Los derechos

de acceso para usar el servicio se otorgan a las organizaciones clientes después de suscribir los contratos oportunos. Las reglas de acceso siempre las define el proveedor del servicio y las regula por la autoridad de gobierno de X-Road.

A diferencia de los consumidores que realizan solicitudes a través de X-Road, los proveedores de datos utilizan X-Road para responder a las solicitudes y compartir datos. Por lo tanto, los proveedores de datos deben cumplir dos requisitos adicionales para usar X-Road: Manejar un registro (base de datos), que debe estar inscrito ante la autoridad de gobierno de X-Road (Autoridad del Sistema de Información de Estonia). Tener un servidor adaptador, conocido como componentes de integración.

## INTERCAMBIO DE DATOS ENTRE PAÍSES

X-Road es la primera plataforma mundial que puede utilizarse para la interacción transfronteriza de registros y sistemas de información. Para implementar los servicios de datos transfronterizos, los centros X-Road deben suscribir un acuerdo de federación que describa las responsabilidades organizativas y legales de los países involucrados y entre ellos.

## SISTEMA DE SEGURIDAD INFORMÁTICA

La seguridad informática es un proceso continuo, cuyo objetivo es garantizar la confidencialidad, integridad y disponibilidad de los datos y activos. El objetivo es encontrar un equilibrio entre estos tres componentes.

El sistema de seguridad de referencia ISKE, de tres niveles de TI, garantiza un nivel de seguridad suficiente para los datos procesados en los sistemas de TI. El nivel de seguridad necesario se logra mediante la implementación de medidas de seguridad estándar organizativas, de infraestructura o físicas, y técnicas.

La preparación y el desarrollo de ISKE se basa en una norma de seguridad de la información alemana, el Manual de Protección de Referencia de las TI (IT-Grundschutz en alemán), que se ha desarrollado continuamente para adaptarse a la situación de Estonia. Sistema de seguridad de referencia ISKE de tres niveles de TI <https://www.ria.ee/en/iske-en.html>

Un sistema de referencia de tres niveles significa que se han desarrollado tres conjuntos diferentes de medidas de seguridad para tres requisitos de seguridad diferentes (distintas bases de datos y sistemas de información pueden tener diferentes niveles de seguridad).

## PROCESO SIMPLIFICADO PARA LA IMPLEMENTACIÓN DE ISKE:

-Mapeo de bases de datos.

-Mapeo de sistemas de información y otros activos informáticos.

-Identificación de enlaces entre bases de datos, sistemas de información y otros activos informáticos.

-Identificación de la clase de seguridad y nivel requeridos para las bases de datos.

-Identificación de la clase y nivel de seguridad requerida para los sistemas de información y otros activos informáticos.

-Identificación de los módulos típicos, que cumplen con los sistemas de información y otros activos informáticos.

-Identificación de las medidas de seguridad requeridas para los sistemas de información y otros activos informáticos.

Estonia fue el primer estado nación en el mundo que implementó la tecnología blockchain o cadena de bloques en sistemas de producción. Utiliza la solución KSI Technology Stack de Guardtime. Un sistema de gobierno interactúa con el blockchain KSI al enviar una impresión digital, es decir, un valor hash de un activo digital (por ejemplo, una entrada en un registro) en la infraestructura de KSI, y luego se devuelve una firma basada en blockchain que proporciona una prueba criptográfica de la integridad, tiempo y atribución de origen, es decir, qué entidad generó la firma. Este enfoque elimina los problemas de privacidad y cumplimiento, ya que los datos nunca se almacenan en el blockchain.

A diferencia de las estrategias de firma digital tradicionales, por ejemplo, la infraestructura de clave pública (PKI por sus siglas en inglés), que dependen de la criptografía de clave asimétrica, KSI solo utiliza la criptografía de función hash, lo que permite que la verificación se base únicamente en la seguridad de las funciones hash y la disponibilidad de un registro contable público, por lo general conocido como blockchain. Un blockchain es un registro público distribuido de eventos, un registro de eventos con la funcionalidad de solo anexar (append-only) donde cada nuevo evento está criptográficamente vinculado al anterior. Las nuevas entradas se crean utilizando un protocolo de consenso distribuido.

El blockchain KSI cumple dos propósitos esenciales en los sistemas del gobierno de Estonia:

- **Ciberseguridad mejorada.** El registro de activos en el blockchain KSI fija su estado en el tiempo y controla constantemente el estado de los activos mediante una nueva verificación a escala. Esto proporciona un verdadero conocimiento de la situación en los sistemas gubernamentales y permite detectar cualquier intento de manipulación.

- **Auditabilidad eficiente.** Los registros del blockchain KSI se pueden verificar de forma independiente, sin necesidad de autoridades fiables. Esto lo convierte en una herramienta eficaz para garantizar el cumplimiento y aumentar la confianza. Como las firmas KSI no caducan, la autenticidad de los datos se puede verificar prácticamente de manera indefinida.

El principal valor del blockchain está en crear confianza. El blockchain KSI ayuda a garantizar que los datos de una persona no se utilicen indebidamente. La tecnología blockchain ayuda a detectar:

- Quién consulta o cambia los datos digitales de salud de una persona, y cuándo.
- Cuándo se cambió la información sobre una empresa en el de e-Registro Empresarial y por qué.
- Quién cambió los datos (y cuándo y cómo) sobre los bienes inmuebles en el e-Registro de la Propiedad o las declaraciones documentadas en el sistema de e-Cortes.

La Autoridad del Sistema de Información de Estonia es un proveedor de servicios integrales para el Gobierno que garantiza el acceso a la red blockchain KSI a las agencias estatales a través de la infraestructura de X-Road. Los registros estatales seleccionados respaldados por la tecnología blockchain son el Registro de Salud, el Registro de la Propiedad, el Registro Empresarial, el Registro de Sucesión, el Sistema de Tribunales Digitales, los Anuncios Oficiales del Estado y la Gaceta Estatal, entre otros.

La misma tecnología se utiliza para abordar los desafíos de la ciberseguridad en diversos sectores, desde la defensa y el sector aeroespacial, hasta los seguros y las telecomunicaciones.

Para contribuir al desarrollo de la sociedad de la información, la República de Estonia ha realizado una inversión significativa en tecnología y soluciones de nube. La tecnología de nube es una de las tendencias futuras para la e-gobernanza (Agenda Digital 2020 para Estonia).

Las ventajas de la tecnología de nube son:

- Mejora la rentabilidad del sector público porque favorece el ahorro en inversiones de equipos y programas, y aumenta la eficiencia de las autoridades del sector público.
- Mejora la capacidad de seguridad de la información del sector público, ya que los servicios públicos se estandarizarán a través de la nube gubernamental y ya no dependerán de una institución específica.

- Armoniza la calidad de los servicios.
- Permite proporcionar servicios ininterrumpidos de alta calidad incluso en el caso de soluciones de uso estacional a gran escala (por ejemplo, la presentación de declaraciones de impuestos).
- Apoya la innovación y la rápida implementación de nuevas soluciones tecnológicas.
- Mejora la competencia relacionada con el alojamiento y la administración de sistemas de información al simplificar el acceso de las autoridades a expertos de alto nivel en tecnología de alojamiento de servidores.
- Es una energía eficiente y ecológica.

| <b>Servicio de interoperabilidad técnica</b>                                   |   |  |
|--|---|--|
| <b>Servicio</b>  | <b>Responsabilidad de la institución de interoperabilidad</b>   | <b>Responsabilidad de otras instituciones</b>  |
| Definición y promoción de arquitecturas tecnológicas para la interoperabilidad | Definir y promover arquitecturas tecnológicas abiertas y flexibles, contribuyendo en las especificaciones de interfaz, servicios de interconexión, servicios de integración de datos, presentación e intercambio de datos y protocolos de comunicación seguros. | Contribuir y sancionar la especificación, el diseño, las restricciones y las posibilidades de las arquitecturas de la institución con miras a su integración en la plataforma de interoperabilidad.  |
| Suministro y gestión de un catálogo de servicios                               | Proveer y gestionar un catálogo de servicios de interoperabilidad entre instituciones.  | Publicar y mantener en el catálogo todos los servicios de interoperabilidad que estén bajo su administración y control (se incluye descripción, niveles de servicio comprometido, interfaces de programación de aplicaciones y documentación técnica para la implementación de estos servicios). |
| Suministro y gestión de un catálogo de esquemas y metadatos                    | Proveer y gestionar un catálogo de esquemas y metadatos.  | Publicar y mantener en el catálogo el listado de esquemas y metadatos utilizados en los servicios y documentos electrónicos.   |

|   |  |  |
|---|--|--|
| Suministro y gestión de un directorio de datos  | Proveer y gestionar un directorio de datos (arquitectura de información/datos, modelo ontológico)  | Listado de datos disponibles a partir de los servicios de interoperabilidad publicados en el catálogo de servicios, donde se detalla la descripción y el responsable de cada dato.   |
| Suministro y administración de un gestor de convenios   | Proveer y administrar un gestor de convenios (aplicación) global y específico entre instituciones.   | Mantener actualizada la aplicación que facilita la tramitación de convenios electrónicos estándar, entre consumidor y proveedor de servicios de interoperabilidad, entregando los permisos y las credenciales de acceso para autorizar el suministro del servicio. |
| Suministro y administración de un registro de trazabilidad  | Proveer y administrar un registro de trazabilidad.   | Mantener actualizado el registro resultante de cada servicio de interoperabilidad para que los actores involucrados conozcan y verifiquen las operaciones que se hayan realizado respecto de un determinado servicio interoperable.                                |
| Suministro y administración de un sistema de monitoreo  | Proveer y administrar un sistema de monitoreo.   | Mantener actualizado el sistema de monitoreo que realiza consultas periódicas a todos los servicios de interoperabilidad definidos en el catálogo de servicios, a fin de identificar y notificar de manera oportuna y proactiva las fallas en el servicio.         |
| Suministro y administración de un gestor de autorizaciones  | Proveer y administrar un gestor de autorizaciones que permita a las personas naturales autorizar o desautorizar el uso de sus datos personales, mediante el uso de su identidad digital. | n/a  |
| Identificación de los servicios adecuados para que se invoquen y organicen para prestar el servicio público | Garantizar que las necesidades se identifiquen y que los servicios adecuados se invoquen y organicen para prestar un servicio público.   | Formalizar los servicios demandados por la ciudadanía y las interdependencias que estos tienen con otras instituciones.  |
| Suministro y gestión de   | Proveer y gestionar un   | Publicar y mantener en el  |

|  |   |   |
|--|---|---|
| un catálogo de fuentes de información y servicios internos de cada institución                   | catálogo de fuentes de información (aplicaciones) de cada institución.  | catálogo el listado de sistemas y aplicaciones desde donde se obtienen los servicios y documentos electrónicos interoperables.  |
| Suministro y gestión de un catálogo de recursos reutilizables                                    | Proveer y gestionar un catálogo de recursos reutilizables de interoperabilidad entre instituciones.             | Publicar y mantener en el catálogo de recursos reutilizables los módulos, componentes y servicios que puedan reutilizar otras instituciones.                                      |
| Suministro y gestión de un catálogo de fuentes de información y servicios externos               | Proveer y gestionar un catálogo de fuentes de información y servicios externos utilizados por cada institución. | Publicar y mantener el catálogo de fuentes de información y servicios externos, identificando el proveedor y documentando las características técnicas y el uso de estas fuentes. |
| Suministro y administración de un mecanismo de seguridad y privacidad de acceso a la información | Proveer y administrar un mecanismo de seguridad y privacidad de acceso a la información interoperable.          | Hacer uso de las funcionalidades y los ambientes del mecanismo de seguridad y privacidad de acceso a la información interoperable.  |

### **Desde el punto de vista Semántico**

Este dominio aborda la capacidad de los sistemas y tecnologías para conectarse y compartir datos de manera efectiva. Incluye aspectos como los protocolos de comunicación, la arquitectura de sistemas y la infraestructura tecnológica. Es importante la tangibilidad de los datos, así como la compatibilidad de estos.

En la plataforma X-ROAD en relación con la arquitectura semántica el Sistema de administración del sistema de información estatal (RIHA) almacena los metadatos de las bases de datos públicas, registros y sistemas de información.

Establece que los recursos disponibles deben estar en:

- ✓ Formato legible por humanos y máquinas (XML, OWL);
- ✓ Formato sólo legible por humanos (PDF);
- ✓ Formato sólo legible por máquina (CSV, WSDL).

Cuenta con una infraestructura de datos abiertos y espaciales. Los datos abiertos permiten mayor transparencia, si bien los gobiernos y las empresas recopilan una amplia variedad de datos, no siempre los comparten de manera que el público pueda encontrarlos, utilizarlos o

comprenderlos fácilmente. Para permitir el uso efectivo de los datos, deben enviarse en un formato legible por máquina. Se deben establecer reglas explícitas para el reciclaje de datos, asegurando la interoperabilidad de los sistemas de información, los servicios y la infraestructura que apoyan el reciclaje de datos.

El uso efectivo de datos espaciales es esencial para aplicaciones gubernamentales como el uso del suelo y la administración de bienes raíces, los impuestos a la propiedad, la administración de activos e infraestructuras, la ordenación territorial, el transporte, la administración de recursos naturales, la protección medioambiental, la agricultura y la aplicación de la ley, entre otros.

Como parte del ecosistema de e-gobernanza, la infraestructura de datos espaciales debe cumplir y basarse en las normas, regulaciones y políticas generales vigentes. Algunas normas específicas deben ser aplicadas, o al menos recomendadas, por las regulaciones nacionales:

- ISO 19115:2003 “Metadatos de Información Geográfica”.
- ISO/TS 19139:2007 “Metadatos de Información Geográfica-Implementación del esquema XML”. Estándares del Consorcio Geoespacial Abierto (OGC por sus siglas en inglés), como WMS, WFS o KML, entre otros.
- Principios y metodologías INSPIRE (recomendado).
- Los servicios y recursos de datos deben cumplir con los estándares de OGC.
- Un sistema aplicado de coordinación o proyección geográfica a nivel nacional.
- Todas las agencias responsables de la producción de datos espaciales deben introducir y mantener una gestión adecuada de metadatos.

Además de las regulaciones generales sobre la infraestructura y la práctica de la e-gobernanza, al menos los siguientes temas del Sistema de direcciones deben estar regulados por ley:

- Estándar de dirección (tipos, componentes, formato) y procedimientos de mantenimiento de datos de dirección (operaciones RD).
- Principios generales de creación y asignación de topónimos.
- Principios de soporte multilingüe y traducción de direcciones.
- Interoperabilidad.

| <b>Servicio de interoperabilidad semántica</b>   |   |  |
|--|---|--|
| <b>Servicio</b>  | <b>Responsabilidad de la institución de interoperabilidad</b>   | <b>Responsabilidad de otras instituciones</b>  |
| Contribución a la formación, la comprensión y el tratamiento de los datos y la información             | Contribuir a la formación, la comprensión y el tratamiento de los datos y la información como un bien público valioso.  | Designar a las contrapartes de datos e información de la institución, que serán responsables de la interoperabilidad de los servicios. |
| Contribución a garantizar que el formato y el significado de la información intercambiada sean exactos | Contribuir a garantizar que el formato y el significado de la información intercambiada sean exactos, se comprendan y conserven en todos los intercambios entre las partes. | Participar y sancionar respecto del significado exacto de la información intercambiada por la institución con otras instituciones.     |
| Establecimiento de normas y contribución a la creación de vocabularios y esquemas                      | Normar y contribuir a la creación de vocabularios y esquemas para describir los intercambios de datos.  | Participar y sancionar respecto del significado exacto de la información intercambiada por la institución con otras instituciones.     |
| Gestión para que exista una descripción del formato exacto de la información                           | Gestionar para que exista una descripción del formato exacto de la información que se va a intercambiar en términos de gramática y formato.                                 | Participar y sancionar respecto del formato exacto de la información que se va a intercambiar en términos de gramática y formato.      |
| Garantía de que todas las partes que se comunican entiendan de la misma manera los elementos de datos  | Garantizar que todas las partes que se comunican entiendan de la misma manera los elementos de datos que se intercambian.   | Participar y sancionar respecto del significado exacto de la información intercambiada por la institución con otras instituciones.     |

### **En cuanto al marco legal**

Como se pudo apreciar en la información procesada estos procesos de modernización deben de ir acompañados de un marco legal y otro marco técnico. Las normas legales establecen derechos y obligaciones para los actores sociales (individuos u organizaciones). Mientras que las normas técnicas son reglas y criterios (definiciones, requisitos, recomendaciones, etc.) que establecen las condiciones mínimas que debe reunir un producto, proceso o servicio, para que sirva al uso al que está destinado, siendo elaboradas por comités de expertos y aprobadas por organismos de desarrollo de estándares, pero que a su vez este debe estar regulado por principios jurídicos.

A la hora de definir el marco legal de un Ecosistema Digital de Interoperabilidad (EDI) (Arm, 2019) se debe tener en cuenta:

- ✓ Evitar la regulación excesiva, porque conlleva el riesgo de crear estructuras paralelas de gobernanza.
- ✓ Es esencial revisar las leyes existentes para garantizar que los métodos de e-gobierno sean aceptables.
- ✓ Es importante determinar legalmente quién es la autoridad responsable (por ejemplo, para llevar a cabo reformas, controlar la calidad y la accesibilidad de los servicios y recibir quejas, etc.).
- ✓ Deben estipularse normas de protección de datos y un sistema de cumplimiento.
- ✓ La ley debe establecer una forma segura de identificación en línea.
- ✓ La ley de tecnologías de la información y las comunicaciones (TIC), así como la ley de competencia (específica del sector o general) es importante para garantizar un acceso adecuado a internet.
- ✓ La e-gobernanza puede ser una herramienta importante para garantizar un mejor acceso a la información y facilitar la participación democrática, pero la tecnología debe considerarse principalmente como una herramienta y no como un factor determinante para estructurar dicho acceso y participación.

Al respecto el primer paso es llevar a cabo una revisión exhaustiva de la legislación existente, incluida la legislación secundaria relevante, que deberían realizar preferiblemente expertos legales. El objetivo principal de este análisis es identificar las áreas que necesitan modificaciones legales para facilitar una transición sin problemas a la e-gobernanza (por ejemplo, regulaciones sobre firmas digitales, documentos electrónicos, bases de datos interoperables, etc.). Idealmente, este análisis debe llevarse a cabo al mismo tiempo que la planificación de tecnologías aplicables, ya que las regulaciones deben complementar las soluciones tecnológicas. El resultado de este análisis legal integral es una descripción general de la legislación relevante que destaque los cambios necesarios, los medios para lograrlos y que ofrezca sugerencias para modificaciones legislativas.

Las siguientes áreas del derecho son ejemplos de los aspectos que se deben revisar en todo lo relacionado con la interoperabilidad.

- Derecho administrativo (incluido el procedimiento administrativo).

- Competencias de las instituciones gubernamentales.
- Legislación de protección de datos (protección de la privacidad).
- Acceso a la información.
- Legislación de documentos de identidad.
- Ley de TIC (por ejemplo, provisión de servicios de Internet), incluidas las licencias y autorizaciones.
- Derecho de la competencia.
- Ley de contratación pública.
- Derecho contractual.
- Ley de procedimiento penal (normas para la práctica de pruebas).

Por otra parte (Vivas, s.a) recomienda tener en cuenta también:

- ✓ Crear y dar entidad jurídica regulada al EDI gubernamental, estableciendo sus principales características, que se traducen en derechos y obligaciones de sus miembros.
- ✓ Establecer el no repudio de los intercambios digitales. Este es un punto muy importante y constituye la validez jurídica de la interoperabilidad de datos, procesos y servicios digitales. Impacta en la gestión pública y en los ciudadanos.
- ✓ Establecer una autoridad de aplicación del EDI. La autoridad de aplicación deberá reglamentarse teniendo en cuenta sus “dos caras”, por un lado, la que regula, ordena y fiscaliza, y, por otro lado, la del servicio técnico, que es la que conecta, opera, gestiona los derechos de acceso (al EDI, a los datos), entre otros.
- ✓ Establecer la gobernanza del ecosistema digital. Se refiere al modelo que adoptará la gestión pública gubernamental para la toma de decisiones en la operación, gestión y evolución del EDI.
- ✓ Definir el alcance, en cuanto a los poderes del Estado y las instancias de membresía de otros actores. Lo que redundará en los tipos y grupos de datos, procesos y servicios digitales que quedan incluidos, seguros, confiables, trazables y no repudiables, en el marco del EDI.

En relación al marco técnico, la norma Argentina IRAM 17610-1 Ecosistema Digital de Integrabilidad-Requisitos (Vivas, s.a), se define que cada organización miembro debe cumplir con:

| <b>Características</b> | <b>Subcaracterísticas</b>   |
|------------------------|---|
| Seguridad              | Autenticación<br>Control de Acceso<br>Integridad de mensaje<br>Confidencialidad<br>Referencia temporal<br>Prueba de envío/recepción<br>Integridad de registros de intercambio |
| Tangibilidad           | Visibilidad   |
| Compatibilidad         | Interoperabilidad   |

Para este autor teniendo en cuenta los aspectos legales y técnicos reflejados anteriormente la implementación de X-Road como entorno de interoperabilidad tiene el potencial de transformar la capacidad de gestionar y compartir información de manera efectiva y segura cumpliendo con el marco definido por la norma IRAM 17610 y las recomendaciones del Consejo Federal de la Función Pública (CoFeFuP) y del Marco Europeo de Interoperabilidad. Los beneficios en términos de eficiencia operativa, transparencia y cumplimiento normativo son significativos.

En Costa Rica se proponen normas habilitantes en el momento de establecer la gobernanza de interoperabilidad (organizativas, semánticas, legal y técnica), también para las cuestiones relacionadas con la ciberseguridad.

El investigador Arm (2019) plantea que las regulaciones deben abordar la naturaleza de las transacciones y la sensibilidad de los datos, manteniendo la tecnología relativamente intacta. Valora que el trabajo legal esencial radica en analizar la legislación existente e identificar las deficiencias, así como las áreas donde la ley puede presentar obstáculos para el desarrollo de la e-gobernanza.

Sin embargo, refiere que ciertos aspectos, como la identificación electrónica y las firmas digitales, necesitan una regulación especial porque son conceptos sin equivalentes comparables en un mundo presencial que se basa en el uso de papel. Los problemas obvios o que se conocen desde hace siglos en el mundo ordinario pueden necesitar una regulación en el mundo virtual, como por ejemplo, qué dispositivos se pueden usar para firmar.

Comenta además, que debería prestarse una atención especial a la legislación de protección de datos, ya que los datos electrónicos por lo general se perciben como menos seguros. Incluso si

tal percepción puede ser incorrecta, puede hacer que las personas desconfíen de las transacciones electrónicas o que se abuse de las lagunas en la seguridad de los datos. Para estos investigadores La ley y la tecnología deben trabajar juntas, con soluciones técnicas aplicadas para proteger los datos, y la ley debe exigir tales soluciones.

Recomiendan que es esencial contar con expertos legales al principio del proceso de planificación para evitar obstáculos regulatorios y para prevenir situaciones en las que la implementación tardía de las regulaciones podría dificultar la aplicación de los e-servicios. Se debe evitar el exceso de regulación y, paradójicamente, el riesgo es mayor si el análisis legal se pospone a una etapa posterior.

Los asuntos más apremiantes que hay que resolver son garantizar que las firmas electrónicas y los documentos (datos electrónicos) sean válidos, incluso como prueba en los tribunales, y que las transacciones realizadas electrónicamente se acepten de la misma manera que las no electrónicas.

Además, para garantizar el acceso a internet también es importante la legislación de las TIC, que puede ser específica del sector o parte de la ley de competencia. Estonia no cuenta con una legislación específica sobre e-gobernanza, pero hay varias leyes que la afectan.

| <b>Servicio de interoperabilidad legal</b>  |  |   |
|---|--|---|
| <b>Servicio</b>   | <b>Responsabilidad de la institución de interoperabilidad</b>  | <b>Responsabilidad de otras instituciones</b>   |
| Alineamiento de las normativas/leyes intra-e interinstitucionales                       | Garantizar que las organizaciones que operan sobre la base de diferentes marcos jurídicos, políticas y estrategias puedan trabajar juntas. | Identificar las leyes y normativas que regulan, restringen o posibilitan el ofrecimiento de un servicio interoperable al ciudadano.               |
| Establecimiento de acuerdos claros sobre cómo abordar las diferencias en la legislación | Establecer acuerdos claros sobre cómo abordar las diferencias en la legislación (incluida la opción de adoptar nueva legislación).         | Coordinar con las contrapartes normativas/legales de las instituciones involucradas en el ofrecimiento de un servicio interoperable al ciudadano. |

En relación con nuestro país en la siguiente tabla se resume una actualización del tema legal, apoyado en un estudio comparativo con otros países.

| LEGISLACIÓN                     | CONTENIDO  | ÁREAS QUE NECESITAN MODIFICACIONES LEGALES PARA FACILITAR UNA TRANSICIÓN SIN PROBLEMAS A LA INTEROPERABILIDAD   | ELEMENTOS NUEVOS A TENER EN CUENTA A PARTIR DE ESTUDIOS COMPARATIVOS   |
|---------------------------------|--|---|--|
| <p>DECRETO-LEY No. 370/2018</p> | <p>Sobre la informatización de la sociedad en Cuba</p> | <p>Título: Sobre <u>la transformación digital de la sociedad en Cuba.</u><br/> Artículo 1: El Estado promueve y <u>garantiza</u> el acceso a las tecnologías para toda la ciudadanía....<br/> Artículo 2: Eliminar <u>gradualmente</u>, para que un sistema interoperable funcione todos deben estar interconectados: población e instituciones mediante Internet.<br/> Artículo 3: Agregar transmisión y recepción de <u>información y servicios ...voz, datos, textos, videos e imágenes y documentos legales de cualquier índole que contengan firmas electrónicas certificadas.</u><br/> Artículo 5 inciso c: cambiar el término favorecer <u>por garantizar</u>, inciso g: cambiar el término favorecer <u>por garantizar</u> y agregar <u>sector no estatal de la economía (MIPYMES)</u> y al final <u>y a toda la ciudadanía en general</u> <u>agregar un inciso dentro de los objetivos que contenga garantizar el acceso a INTERNET para todos para desarrollar el gobierno electrónico y la interoperabilidad de los servicios públicos.</u><br/> Artículo 6: agregar <u>en función de brindar un servicio público con eficiencia y calidad a toda la población.</u><br/> Capítulo II: <u>agregar un artículo que establezca que todas las organizaciones deben registrarse para organizar sus sistemas propios por las normas establecidas para garantizar la interoperabilidad de los servicios.</u><br/> Capítulo III, Artículo 9, inciso g <u>cambiar redacción enfocarla en la necesidad de crear bases de datos que permitan establecer un Centro de Datos Nacional para establecer la interoperabilidad y facilitar el Gobierno Electrónico.</u></p> | <p><b>Estonia</b> Los expertos argumentan que se debe evitar el exceso de regulación en temas digitales.<br/> Tener demasiadas leyes especiales puede ser un obstáculo para el desarrollo de las tecnologías, las cuales están en un proceso de renovación continua. Sin embargo, sí recomiendan que la identificación electrónica y las firmas digitales cuenten con una regulación especial, de forma que las firmas electrónicas y los documentos electrónicos sean válidos incluso como prueba en los tribunales.<br/> También señalan que es importante formular normas para la protección de datos, puesto que los datos electrónicos se perciben como menos seguros y esta percepción puede ser un obstáculo para la adopción de las transacciones electrónicas.<br/> <b>Argentina</b> La norma IRAM 17610: Ecosistema Digital de Integrabilidad (EDI) establece los requisitos para un ecosistema digital donde diversos sistemas y aplicaciones coexistan e intercambien información de manera segura y eficiente.<br/> Esta norma, pionera en Argentina y Latinoamérica, busca superar los desafíos de la integración de sistemas a nivel multiorganizacional, yendo más allá de la interoperabilidad para</p> |

|  |   |  |
|--|---|--|
|  | <p>Título II, Capítulo I, Artículo 13: <u>definir y hacer mención sobre la inteligencia artificial.</u></p> | <p>facilitar la innovación.</p> <p>La norma busca plasmar las bases conceptuales, mejores prácticas y requisitos para la conformación, operación y evolución de un EDI2.</p> <p>Alcance: La norma se proyecta en ámbitos territoriales y jurisdiccionales, siendo aplicable a empresas, estados, la industria del software e instituciones académicas.</p> <p>Estructura: La norma combina la estructura normativa estandarizada con componentes del marco de interoperabilidad europeo, adaptándolos a la realidad nacional.</p> <p>Se compone de:</p> <p>Requisitos específicos y recomendaciones:</p> <p>Dimensión técnica: abarca seguridad, interoperabilidad, gestión de servicios, metadatos y arquitectura de información.</p> <p>Dimensión organizacional: se centra en la colaboración, acuerdos de interoperabilidad, gestión de seguridad y gestión de servicios.</p> <p>Dimensión de gestión: aborda la gestión de riesgos, definición de métodos de trabajo, comunicación de metas operativas, formación continua y mejora del EDI.</p> <p>Métodos de ensayo: permiten verificar el cumplimiento de los requisitos.</p> <p>Evaluación de conformidad: demuestra el cumplimiento de los requisitos.</p> <p>Principios: La norma se basa en 14 principios fundamentales:</p> <p>Enfoque en las personas.</p> <p>Proactividad en los servicios</p> <p>Solo una vez (once only).</p> |
|--|---|--|

|  |  |   |
|--|--|---|
|  |  | <p>Eficacia y eficiencia<br/> Digital primero Seguridad de la información compartida<br/> Subsidiariedad y cobertura.<br/> Colaboración y participación<br/> Neutralidad tecnológica.<br/> Inclusión y acceso<br/> Reutilización Conservación de la información<br/> Confianza Multilingüismo</p> <p><b>Dominicana</b> La normativa aplica a todos los organismos del Estado dominicano bajo el Poder Ejecutivo que intercambien datos ciudadanos para la prestación de servicios públicos.<br/> Busca estandarizar los procesos de interoperabilidad para:<br/> Mejorar la calidad de los servicios públicos.<br/> Aumentar la transparencia y la rendición de cuentas.<br/> Reducir costos administrativos.<br/> Aumentar la eficiencia operativa.<br/> La norma se basa en los principios de:<br/> Transparencia: Permitir que otros organismos, ciudadanos y empresas comprendan las reglas, procesos, datos y toma de decisiones.<br/> Reusabilidad: Fomentar la reutilización de datos y servicios para evitar la duplicación de esfuerzos.<br/> Inclusión: Asegurar que los servicios sean accesibles para todos.<br/> Seguridad y Privacidad: Garantizar la seguridad y confidencialidad de la información.<br/> Eficiencia: Disponer de la capacidad para lograr los objetivos de interoperabilidad.<br/> Efectividad: Asegurar que la</p> |
|--|--|---|

|  |  |  |
|--|--|--|
|  |  | <p>interoperabilidad cumpla con los objetivos para los que fue diseñada.</p> <p>Dimensiones de la interoperabilidad: La normativa abarca cuatro dimensiones:</p> <p>Legal: Define las normas y estatutos que habilitan la interoperabilidad, asegurando que el intercambio de información se ajuste al marco jurídico.</p> <p>Organizacional: Promueve la colaboración entre organismos para la definición de procesos y responsabilidades en la interoperabilidad.</p> <p>Semántica: Garantiza que la información intercambiada se interprete de manera inequívoca, utilizando estándares para la definición de datos y metadatos.</p> <p>Técnica: Establece las especificaciones técnicas, como interfaces, protocolos y formatos de datos, para la interconexión de sistemas.</p> <p>Categorías de certificación:</p> <p>Categoría A: Para organismos que proveen datos.</p> <p>Categoría B: Para organismos que consumen datos.</p> <p>Categoría C: Para organismos que proveen y consumen datos.</p> <p>Comité de Implementación y Gestión de Estándares TIC (CIGETIC):</p> <p>Cada organismo debe conformar un CIGETIC mediante resolución oficial para planificar, implementar y dar seguimiento a la certificación NORTIC.</p> <p>El CIGETIC debe estar integrado por representantes de diversas áreas del organismo, incluyendo</p> |
|--|--|--|

|  |  |  |
|--|--|--|
|  |  | <p>tecnología, jurídica, planificación y acceso a la información.</p> <p>Responsabilidades: La norma define las responsabilidades del organismo solicitante de la certificación y de la OGTIC durante el proceso.</p> <p>Interoperabilidad en Salud: La NORTIC 4 dedica un capítulo a la interoperabilidad en el sector salud, estableciendo estándares específicos para el intercambio de información médica.</p> <p>Estándares técnicos: Obliga a los organismos a utilizar la Plataforma Única de Interoperabilidad (basada en X-Road) para el intercambio de información. Define requisitos para servidores de seguridad, gestión de accesos, manejo de contraseñas y planes de recuperación ante desastres. Establece directrices para la creación de APIs, incluyendo el uso de estándares como REST, JSON y OAuth 2.0. Promueve el uso de estándares internacionales como HL7 para la interoperabilidad en salud.</p> <p><b>Colombia</b> El Decreto 620 de 2020 de Colombia establece el marco normativo para los servicios ciudadanos digitales, incluyendo la interoperabilidad como un servicio esencial. Este decreto busca garantizar un flujo de información adecuado entre los sistemas de las entidades públicas colombianas. Estas son las reglas principales para la interoperabilidad que se encuentran en el Decreto 620 de 2020:</p> |
|--|--|--|

|  |  |  |   |
|--|--|--|---|
|  |  |  | <p>Interoperabilidad como servicio esencial: El decreto define la interoperabilidad como un servicio esencial para garantizar un flujo de información adecuado entre los sistemas de las entidades públicas.</p> <p>Marco de Interoperabilidad: El decreto establece que las entidades deben seguir un Marco de Interoperabilidad. Este marco define los lineamientos, estándares y protocolos que deben cumplir las entidades para garantizar la interoperabilidad de sus sistemas.</p> <p>Vinculación obligatoria: Las entidades públicas colombianas están obligadas a vincularse a los servicios ciudadanos digitales, incluyendo la interoperabilidad. Deben seguir la guía emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) para la preparación, adecuación, integración, uso y apropiación de estos servicios.</p> <p>Rol del Articulador: El decreto designa un “Articulador” (la Agencia Nacional Digital) para coordinar y facilitar la interoperabilidad entre las entidades públicas. Las funciones del Articulador incluyen:</p> <p>Acompañar a las entidades en la creación, diseño, implementación o adecuaciones técnicas de los trámites y servicios que se expondrán a través de los servicios ciudadanos digitales, asegurando que cumplan con el Marco de</p> |
|--|--|--|---|

|  |  |  |
|--|--|--|
|  |  | <p>Interoperabilidad.</p> <p>Poner a disposición de las entidades los servicios de interoperabilidad que ya estén implementados o hayan sido publicados en la plataforma de interoperabilidad del Estado colombiano, siempre y cuando cumplan con el nivel 3 de madurez según el Marco de Interoperabilidad.</p> <p>Apoyar la configuración, habilitación y exposición de los servicios de intercambio de información.</p> <p>Mediar y coordinar el intercambio de información entre las entidades, integrando los servicios habilitados o expuestos, según las reglas y políticas del Marco de Interoperabilidad.</p> <p>Actualización de la información: Las entidades deben mantener actualizada la información sobre sus trámites y servicios en el Sistema Único de Información de Trámites (SUIT). Deben especificar en el SUIT cómo utilizan la interoperabilidad para simplificar los trámites y evitar solicitar información que ya esté disponible en otras entidades.</p> <p>Seguridad de la información: El decreto enfatiza la importancia de la seguridad y privacidad de la información en la interoperabilidad. Las entidades deben cumplir con la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y otras normas relacionadas.</p> <p>Evaluación del impacto en la protección de datos: Antes de implementar servicios ciudadanos digitales, los</p> |
|--|--|--|

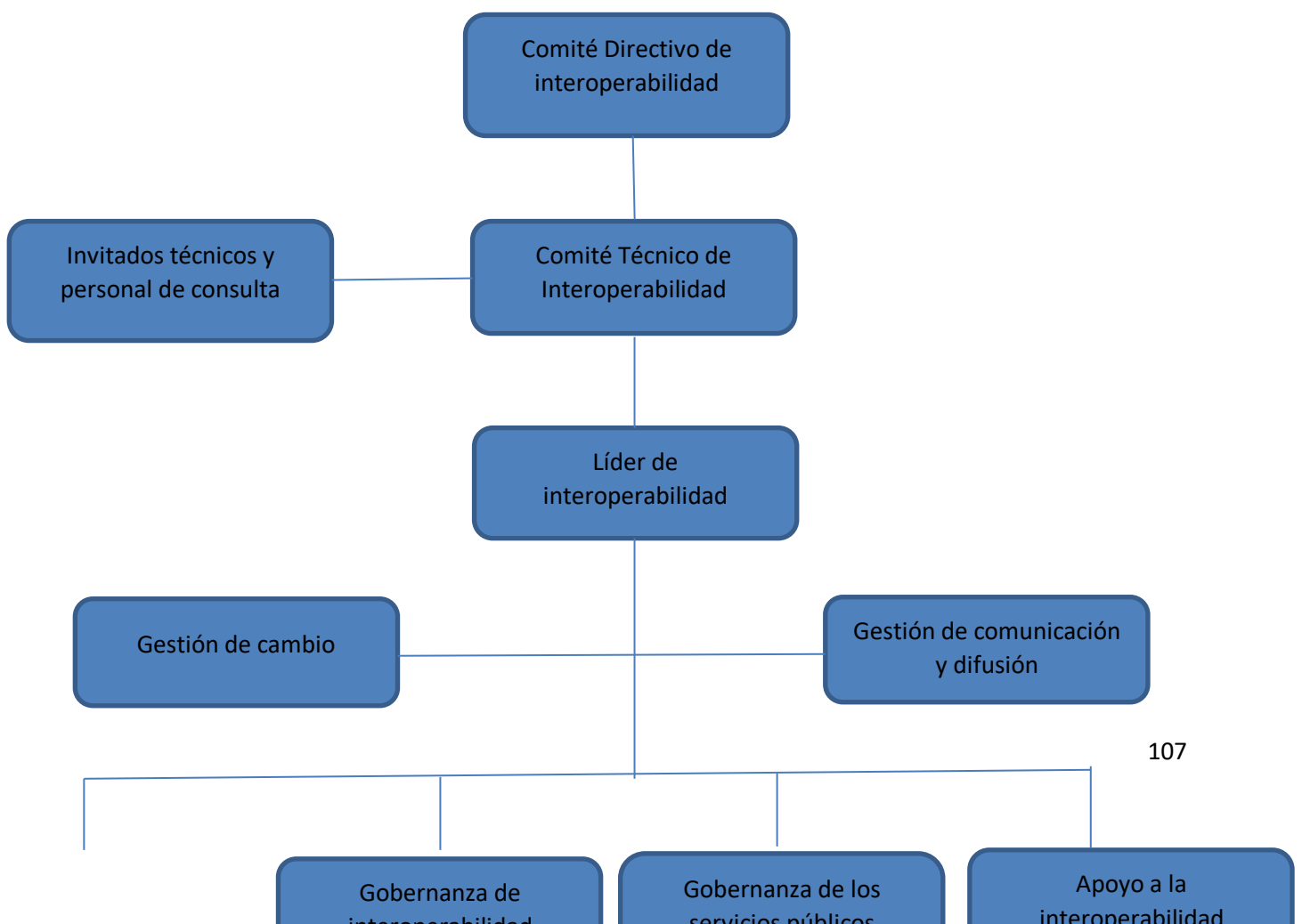
|                  |   |  |   |
|------------------|---|--|---|
|                  |   |  | <p>proveedores deben evaluar el impacto en el tratamiento de datos personales, incluyendo la finalidad del tratamiento, los tipos de datos, las medidas de seguridad y los mecanismos para garantizar los derechos de los titulares de los datos.</p> <p>Oficial de Protección de Datos: Se requiere que las entidades designen un Oficial de Protección de Datos para garantizar el cumplimiento de la normativa de protección de datos personales en la prestación de los servicios ciudadanos digitales.</p> |
| Decreto 359/2019 | Sobre el desarrollo de la industria cubana de programas y aplicaciones informáticas | <p>Artículo 7, inciso d agregar y la interoperabilidad.</p> <p>Artículo 8, inciso h. revisar y tener en cuenta a la hora de legislar sobre interoperabilidad , dice el Ministerio de las Comunicaciones coordina los esfuerzos nacionales de investigación, desarrollo e innovación en el terreno de las aplicaciones, programas informáticos y servicios asociados; supervisa la protección de sus resultados, en especial los que tengan mayor utilización en los frentes estratégicos del país</p> <p>Estipula que el Ministerios de Ciencia, Tecnología y Medio Ambiente y de Cultura: 1) Proponen o emiten las normas jurídicas relacionadas con la propiedad intelectual y el derecho de autor, respectivamente, en el ámbito del desarrollo, producción y comercialización de programas y aplicaciones informáticas, así como los mecanismos que garanticen la protección del patrimonio nacional del sector. Se deben revisar estas normas a la hora de legislar sobre el tratamiento de los datos para la interoperabilidad.</p> <p>Establece que el Ministerio de Finanzas y Precios:1) Implementa mecanismos fiscales que estimulen el desarrollo y la comercialización de la Industria para el</p> |   |

|  |   |   |  |
|--|---|---|--|
|  |   | mercado nacional y la exportación. Se deben revisar esos mecanismos.<br>Artículo 22. Los ministerios de Comunicaciones, del Interior y de las Fuerzas Armadas Revolucionarias, coordinan y establecen las acciones que permiten alcanzar paulatinamente las condiciones de fiabilidad, estabilidad y seguridad de los programas, aplicaciones y servicios informáticos que respalden la Seguridad y Defensa Nacional. Tener en cuenta para interoperabilidad. |  |
| Decreto 360                              | Sobre la seguridad de las tecnologías de la información y las telecomunicaciones y la defensa del ciberespacio nacional | Este Decreto íntegramente se debe tener como punto de referencia para legislar todo lo relacionado con la interoperabilidad.  |  |
| Anexo Acuerdo 8611                       | Estrategia de desarrollo de la infraestructura de banda ancha en Cuba   | Este acuerdo facilita la interoperabilidad, en la medida en que se desarrolle mejores condiciones técnicas para realizarla con efectividad.   |  |
| Resolución 181/2016<br>Acuerdo 7939/2016 | Anexo Metodología para la preparación progresiva de la introducción del protocolo                                       | Revisarla comprende elementos organizativos que competen también a la interoperabilidad.  |  |

|   |   |   |  |
|---|---|---|--|
|   | ipv6 en las redes de datos, sistemas y aplicaciones informáticas del país |   |  |
| Resolución 141/2020                                       | Migración a código abierto  | Revisar contiene obligaciones técnicas.   |  |
| Resoluciones 128/2019<br>129/2019<br>126/2019<br>105/2021 | Sobre la seguridad informática  | Contiene elementos técnicos y organizativos sobre la seguridad informática. Específicamente norma lo relacionado con la seguridad de las operaciones y la seguridad de las redes. Elementos importantes a tener en cuenta en la interoperabilidad.  |  |
| Ley 149   | Sobre la protección de datos personales                                   | Tener como punto de partida para todo lo que se legisle dentro de la interoperabilidad sobre el tratamiento de los datos ya que establece que la existencia de registros, archivos, bases de datos u otros medios de carácter público o privado, físico o digital, por medio de los cuales se almacena, tramita, brinda y se utiliza la información personal, así como el libre acceso a estos datos, puede vulnerar el derecho de su titular y otros derechos con los que se relaciona, de no regularse adecuadamente. |  |
| Decreto 45/2021   | Sobre el desarrollo de la automatización en Cuba                          | Tener como punto de partida para todo lo que se legisle dentro de la interoperabilidad  |  |
| Decreto 35  | Espectro radioeléctrico   | Tener como punto de partida para todo lo que se legisle dentro de la interoperabilidad  |  |

## PROPUESTA DE ESTRUCTURA DE GOBERNANZA DIGITAL MINJUS

### ESTRUCTURA DE LA INTEROPERABILIDAD



Gobernanza de personas

Desarrollo de habilidades

Desarrollo de  
capacidades

***Comité directivo de implementación de la interoperabilidad:*** Equipo con directivos de las instituciones invitadas que resuelve las temáticas estratégicas y estructurales de la institucionalidad de implementación de la interoperabilidad. Una base de conformación de este comité está dada por las instituciones proveedoras de información clave para interoperar (registro, tributos e instituciones por dominio específico a abordar).

***Comité técnico de implementación de la interoperabilidad:*** Equipo con representantes técnicos de las instituciones invitadas que resuelven las temáticas operacionales y técnicas de la institucionalidad en cuanto a la implementación de la interoperabilidad. Cada institución participa de una o más mesas de especialidad de la interoperabilidad: mesa de interoperabilidad normativa/legal, mesa de interoperabilidad organizacional, mesa de interoperabilidad semántica y mesa de interoperabilidad técnica. Se sugiere que se definan instituciones responsables por cada dominio, que rotarán en el cargo por períodos a definir.

***Líder de interoperabilidad:*** Responsable de implementar la estrategia de interoperabilidad país y de gestionar los alcances, el presupuesto, los equipos de trabajo y los hitos en dicha implementación, así como la relación con los directivos de negocio y técnicos de las instituciones que interoperan. Responde directamente al comité directivo de implementación

de la interoperabilidad y se apoya en el comité técnico de implementación de la interoperabilidad, invitados técnicos, personal de consulta y gestión del cambio.

***Invitados técnicos y personal de consulta:*** Hay instituciones permanentes, que se sugiere que acuden a resolver problemáticas específicas. Ante una dificultad que no pueda resolver el comité técnico, se cuenta con esta instancia para convocar a otros especialistas en temas puntuales.

***Gestión del cambio:*** Equipo a cargo de la definición e implementación de los planes de contención, entrenamiento y comunicación, que se coordina con cada institución que interviene en la implementación de un servicio dirigido al ciudadano, coordinando los cambios internos y externos. Contribuye en la identificación de las personas que influyen en los cambios a implementar y aquellas que reciben su impacto.

***Gestión de la comunicación y la difusión:*** Equipo a cargo de mantener bien informado al universo de personas que influyen en los cambios a implementar y aquellas que reciben su impacto, por segmento de usuarios y comunicación, rescatando las retroalimentaciones que se dan en la comunidad de usuarios y gestionando dichas comunidades.

***Gestión de personas:*** Equipo a cargo del desarrollo de las habilidades y capacidades necesarias tanto en los equipos internos de las instituciones como en las comunidades de usuarios de los servicios interoperados. Se vela por contar con la dotación necesaria y se programan e implementan los entrenamientos definidos.

***Gobernanza de la interoperabilidad:*** Responsable de gestionar a los especialistas normativo/legales, organizacionales, semánticos y técnicos para que sean una contraparte efectiva respecto de las instituciones en sus ámbitos y definan los estándares y las buenas prácticas de su disciplina. El control del cumplimiento de esta acción queda supeditado al modelo de interoperabilidad centralizado.

***Gobernanza de los servicios públicos integrados:*** Responsable de velar por la existencia, en cada institución que interopere, de estructuras, funciones y responsabilidades relativas a la entrega y el funcionamiento de los servicios interoperados, acuerdos de nivel de servicios, establecimiento y gestión de convenios de interoperabilidad, procedimientos de gestión de cambios y planes para la continuidad de las operaciones, recuperación en caso de catástrofe y calidad de los datos.

***Apoyo para la interoperabilidad:*** Responsable de gestionar los componentes presupuestarios, administrativos y financiero-contables de la institución de interoperabilidad, de modo que

permitan asegurar la disponibilidad oportuna de la infraestructura (instalaciones, equipos, licencias) y velar por la sostenibilidad de la institución en estos términos.

En relación con las diferentes categorías de la gobernanza de la interoperabilidad se propone:

## **CONCLUSIONES**

Los acelerados cambios en un contexto digital plantean un nuevo mapa de desafíos que crean la necesidad de desarrollar modelos de gestión de las organizaciones en la actual sociedad del conocimiento con una transformación sociotecnológica sustentada en las nuevas capacidades del procesamiento de la información, garantizando el intercambio armonioso entre la ciudadanía y las instituciones.

El sector jurídico no puede permanecer impasible ante esta transformación, por tal razón es menester, crear modelos de innovación integrales que confluyan la estrategia, la cultura, los procesos y las capacidades hacia el diseño de una estrategia digital que incremente presencia y relevancia en los medios digitales. Esta transformación debe estar alineada con una generación de líderes que promuevan este cambio cultural hacia la transformación digital que requiere la tecnología como motor.

En la tecnologización de la justicia diversas tecnologías como la digitalización, la automatización y la inteligencia artificial, convergen retroalimentándose para promover cambios de manera general y de forma particular en la práctica laboral y la eficiencia de los servicios.

El proyecto de interoperabilidad busca conseguir que los sistemas y aplicaciones informáticas que actualmente manejan las diferentes instituciones públicas puedan conversar mutuamente. Permite organizar la información, facilitando el acceso a los datos de manera ágil, segura y oportuna, sin tener que desplazarse físicamente, producto de ello, se optimizan los procesos y se reducen los costos y tiempos para todos. Aunque esta transformación trae consigo un efecto legal al propiciar que los servicios jurídicos tengan que innovar sus procesos de tal forma que garanticen eficiencia, calidad, legalidad y seguridad en los procedimientos, servicios que se brinden y documentación que se emita, a la vez que debe garantizar la confidencialidad y protección de los datos personales.

En plena construcción de una convivencia cotidiana caracterizada por la libre disponibilidad de información, la transformación digital crea un abanico de posibilidades y oportunidades, sin embargo, no se debe soslayar los riesgos derivados de un uso indebido o el

desconocimiento de su funcionamiento. Por esta razón debe implementar estrategias que garanticen el cumplimiento de las normas y configuren el derecho más preparado ante la transformación digital.

Se necesita crear una única legislación que valide todo lo relacionado con el proceso de interoperabilidad, que incluye la transición del papel al documento electrónico en los diferentes trámites del llamado Gobierno Electrónico, no solo abarcando los procesos de información en línea, sino también que el mismo trámite sea realizable en línea, incluyendo pagos, firma digital, etc.

El sistema de interoperabilidad más éxito es el de Estonia, llamado “X-ROAD”, puesto en práctica en ese y otros países de diversas regiones, así como en instituciones. También es el más completo al permitir el vínculo con disímiles organizaciones a la vez y además probado en el sistema de justicia de ese país. Tiene una mirada multisectorial.

El ecosistema X-ROAD, si bien cuenta en sentido general con un modelo de gobernanza centralizada, tiene la particularidad de permitir sistemas heterogéneos, y no solo una base de datos central, sino una estructura de intercambio descentralizada donde cada institución mantiene el control de sus datos, a la vez que permite que estos se comuniquen de forma segura y estandarizada. En este aspecto el dominio semántico juega un rol fundamental al establecer códigos que eliminen la duplicidad de la información. Aunque, de establecer convenios de colaboración o acceso a determinada tecnología tener presente en el contrato que este país recientemente se abstuvo en la votación de la Resolución que presenta Cuba en la ONU en contra del Bloqueo.

Existen normativas y decretos leyes en Cuba que contienen regulaciones que se deben tener en cuenta y mantener para garantizar un sistema seguro de interoperabilidad. Otras requieren modificar algunos artículos para una implementación efectiva y regulada.

Los presupuestos que se brindan, con un carácter holístico, contienen los cuatro componentes básicos a tener en cuenta en los sistemas interoperables: semántico, organizacional, legal y técnico, transversalizado por elementos que brindan seguridad y transparencia, así como lo que conlleva la protección de los datos que deben circular a lo interno como a lo externo del ecosistema y la seguridad nacional.

Se debe destacar que aun cuando se requiere de una base tecnológica fuerte para su implementación y desarrollo sistemático y continuo, las cuestiones organizativas, incluida los cambios necesarios de la cultura organizacional, semánticas y legales juegan un rol

fundamental, ya que de la definición de los procesos, las diferentes responsabilidades y la gobernanza conjunta depende su éxito.

## BIBLIOGRAFÍA

- (s.a) (2024). IV Congreso de Tecnología. Transformación digital e interoperabilidad en el sector de la Justicia. Agencia Internacional Antinarcoóticos y Aplicación de la Ley, Guatemala.
- Aguilar Villanueva, L. F. (2016). Gobernanza y gestión pública, Ciudad de México, Fondo de Cultura Económica.
- Alfaro A., Rodrigo y otros. (2005). “Introducción al Gobierno Electrónico: Actores y Dimensiones”. Valparaíso, Chile: Ediciones Universitarias de Valparaíso, Pontificia Universidad Católica de Valparaíso.
- Alfonso Velásquez, Olga. La Interconexión de Redes de Telecomunicaciones. Madrid, España: REUS, 2006.
- Alonso García, Enrique (2016). Interoperabilidad Legal. Revista Privacidad y Derecho Digital, 3 Madrid.
- Amoroso, Yarina (2022). *Derecho para la transformación digital en Cuba*. En *Habilitando la transformación digital*, T-II. Editorial UH. P-23 a 52.
- Antón, Susana (2019). ¿Cómo Cuba ordena jurídicamente el proceso de informatización?. Disponible en [Http://www.gramna.cu/cuba](http://www.gramna.cu/cuba).
- Antón, Susana (2024). Gobierno digital en Cuba: avances y perspectivas de una agenda. Disponible en [Http://www.gramna.cu/cuba](http://www.gramna.cu/cuba).
- Ardila Armirola, Pedro Manuel (2024). Regulación normativa de la identidad digital en Colombia: acerca de su funcionamiento, operatividad y garantía de protección. Monografía Jurídica de Grado. Pontificia Universidad Javeriana, Facultad de Ciencias Jurídicas, Bogotá, Colombia.
- Arm, Margus; Colectivo de Autores (2019). E-Estonia. La e-Gobernanza en la práctica. E-Governance Academy Foundation. La traducción la realizó el Banco Interamericano de Desarrollo (BID), Sector de Instituciones para el Desarrollo, División de Innovación para Servir al Ciudadano.

- Barros, A.; T. Campero y P. Cabello (2016). Estudio para una gobernanza digital en Chile, Santiago, Ministerio de Hacienda/Ministerio Secretaría General de la Presidencia. <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.alejandrobarrros.com/wp-content/uploads/2016/07/Gobernanza-Digital-en-Chile.pdf&ved=2ahUKEwjn5ayZl4KMAxXpTDABHW2vAfEQFnoECBQQAQ&u sg=AOvVaw0rU9nNsPsC6eUErqtMc-Q>
- Brito, Magda (2022). *Avances en la implementación del Gobierno digital en Cuba*. En *Habilitando la transformación digital*, T-II. Editorial UH. P-53 a 60.
- Cabrera Cuevas, Marcelino José y Colectivo de Autores (2022). Guía para el diálogo sobre el diseño y uso eficiente, de calidad y ético de herramientas tecnológicas en la justicia civil. *Revista Justicia Digital*. Universidad de Granada.
- Calderón Sánchez, D. y D. A. Palma Álvarez (eds.) (2018). “Gobernanza multidimensional”, Bogotá, Universidad Santo Tomás.
- Capdeferro Villagrasa, O. (2020). “La inteligencia artificial del sector público: desarrollo y regulación de la actuación administrativa inteligente en la cuarta revolución industrial”, *Revista de Internet, Derecho y Política*.
- Castillo Blanco, F. (2020). “Un sistema de empleo público distópico: ¿sería preciso reformar el EBEP?”, *Documentación Administrativa*, 7,.
- Cerrillo I Martínez, Agustí. *A las puertas de la Administración Digital: una guía detallada para la aplicación de las Leyes 39/2015 y 40/2015*, Madrid: INAP, 2016.
- Cerrillo Martínez, Agustí (2006). *Órganos Colegiados Electrónicos*. Navarra, España, Editorial Thomson- Aranzadi.
- Colectivo de Autores (2021). *Guía para la gestión del gobierno digital en los municipios cubanos*. PADIT.
- Criado, J. Ignacio; Gascó, Mila; y Jiménez, Carlos E. (2010), “Bases para una estrategia iberoamericana de interoperabilidad”, Caracas, CLAD (Documentos Clave: Estado, Administración Pública y Sociedad; N° 18).
- Criado, J. I. (2008). “Una aproximación al Gobierno electrónico desde la Interoperabilidad”, conferencia dictada ante el Consejo Nicaragüense de Ciencia y Tecnología de la Vice Presidencia del Gobierno de Nicaragua, en Managua, Nicaragua, el 10 de junio.

- Danet Ruas, Octavio (2020). Informatización de la sociedad cubana. Cómo ordenar este proceso. Disponible en [Http/www.researchgate.net](http://www.researchgate.net).
- Delpiazzo, Carlos E (2006). Desafíos jurídicos relacionados al Gobierno Electrónico: con especial referencia a la Administración Electrónica, exposición pronunciada en el “Seminario sobre Políticas públicas para el Gobierno Electrónico”, Montevideo, Uruguay, 23 de marzo.
- Deza Padilla, Juan Fernando (2023). Inteligencia Artificial en la administración de justicia: Una revisión sistemática. Revista Climatología, V-23, edición especial para las Ciencias Sociales.
- Díaz-Canel, M (2021). ¿Por qué necesitamos un sistema de gestión del gobierno basado en ciencia e innovación? Revista Anales de la Academia de Ciencias de Cuba, 11 (1).
- Epstein, S. (1996). *Impure Science: Aids, Activism, and the Politics of Knowledge*. University of California Press.
- Espinosa, Victor I; Antonia Pino (2024): E-Government as a Development Strategy: The Case of Estonia, *International Journal of Public Administration*, Disponible en: <https://doi.org/10.1080/01900692.2024.2316128>.
- Expósito Gázquez, A. (2022). “El principio de interoperabilidad como base para las actuaciones y servicios administrativos personalizados, proactivos y automatizados”, *Revista Vasca de Administración Pública*, 122.
- Febles Estrada, A., Saavedra López, E (2024). “Interoperabilidad para el gobierno digital: Estudio de casos Cuba y Bolivia” *Revista Cubana de Transformación Digital*. Consultado en febrero de 2025 <https://orcid.org/0000-0002-5742-9719>
- Febles Estrada, Arlyn (2022). *La interoperabilidad, habilitando para la transformación digital*. En *Habilitando la transformación digital*, T-I. Editorial UH. P-167 a 185.
- Fernández Rodríguez, T. R. (2015). “Una llamada de atención sobre las notificaciones electrónicas en la novísima Ley de Procedimiento Administrativo Común de las Administraciones Públicas”, *Revista de Administración Pública*, 198.
- Figueredo, Oscar Reynaldo (2017). Diputados analizan política integral para el perfeccionamiento de la informatización de la sociedad en Cuba. Disponible en [Http://www.cubadebate.cu/noticias](http://www.cubadebate.cu/noticias).

- Gaceta Oficial (2019). Decreto Ley 370/2018 Sobre la informatización de la sociedad en Cuba.
- Gamero Casado, Eduardo (2009). Interoperabilidad y administración electrónica: conéctense por favor. *Revista de Administración Pública*, 179, Madrid.
- García, Gil. (2006). “Integrating Conceptual Approaches to E- Government, en M. Khosrow-Pour, *Encyclopedia of E-Commerce, E-Government and Mobile CommerceG*”. Hershey, PA: Idea Group Inc.
- Gascó, Mila (2011), “Los retos de la colaboración: ¿a qué, si no a eso, pretendemos hacer frente con la interoperabilidad?”, en *Revista del CLAD Reforma y Democracia*, N° 49, Caracas, pp. 185-202.
- Galliers, R. D., Markus, M. L., Newell, S., (Eds.), *Exploring Information Systems Research Approaches.*, New York, NY: Routledge, 2006.
- Gunter, T. D., & Terry, N. P. (2005). The emergence of national electronic health record architectures in the United States and Australia: models, costs, and questions. *Journal of Medical Internet Research*, 7(1), e3.
- Hernández Sampieri, Roberto (2014). *Metodología de la Investigación*. ED Mc Graw He Education, VI Edición.
- Herrero, R., y Guerra, J. (2017). Seguridad de la Información en entornos de salud. HL7 LATAM NEWS.
- Hess, D. C., Wang, S., Hamilton, W., Lee, S., Pardue, C., Waller, J. L., Gross, H., Nichols, F., Hall, C., & Adams, R. J. (2005). REACH: Clinical feasibility of a rural telestroke network. *Stroke*, 36(9), 2018–2020. <https://doi.org/10.1161/01.STR.0000177534.02969.e4>.
- Huaiquilian Ale, Cesar (s.a). Interoperabilidad en el Sector Público. Universidad Nacional de Rio Negro. Tesis de Licenciatura, Documento PDF.
- Huapaya Chumpitaz, Mario (2022). Transformación digital en el Derecho. *Revista de investigación de sistemas e informática*, 15(2): 77-85. Disponible en: <https://doi.org/10.15381/risi.v15i2.24423>.
- Jasanoff, S. (2004). *States of Knowledge: The Co-Production of Science and the Social Order* (S. Jasanoff (ed.)). Routledge.

- Jasanoff, S., & Kim, S. H. (2013). Sociotechnical Imaginaries and National Energy Policies. *Policy Imaginations*, 22(2), 189–196 <https://doi.org/10.1080/09505431.2013.786990>.
- Jiménez, Carlos (2010). Interoperabilidad en la administración de justicia: experiencias buenas y prácticas en un ámbito complejo. XV Congreso internacional del CLAD sobre la reforma del estado y de la administración pública, República Dominicana.
- Jhones, A. R., Fernández, T. D., & Estrada, A. F. (2022). *Habilitando la Transformación Digital*. Tomo I. La Habana: UH.
- Jorquera Beas, D. (2011). “Gobernanza para el desarrollo local”, Documento de Trabajo, N° 6, Santiago, Centro Latinoamericano para el Desarrollo Rural (RIMISP).
- Lezcano, José María (2023). La interoperabilidad en la administración de justicia bonaerense y la calidad del dato como elemento clave para el acceso a derechos. Universidad de La Plata, Argentina.
- Lindberg, D. A. B. (1965). Electronic Retrieval of Clinical Data Electronic Retrieval of Clinical Data. *The Journal of Medical Education*, 40(8).
- Llorente Sánchez, Mercedes y Colectivo de autores (2022). *Digitalización de la justicia: prevención, investigación y enjuiciamiento*. Ed Thomson Reuters Avanzadi.
- López Castro, M. B. (2021). “De la interoperabilidad de la bolsita a la Cobertura Universal de Salud”. Un análisis sobre la agenda política y los sentidos de los sistemas de información. *Cuestiones de Sociología*, 25, e127. <https://doi.org/10.24215/23468904e127>.
- Manzano Peláez, E. (2021). “El cambio comienza desde dentro: avanzando en la administración digital”, *El Consultor de los Ayuntamientos*, 2, Consultado el 4/ 03/ 25 <https://www.google.com/url?sa=t&source=web&rct=j&opi=89978449&url=https://www.aranzadilaley.es/revistas/consultorayuntamientos.html&ved=2ahUKEwjp6PKtjvGLAxXgSDABHca3JOAQFnoECBwQAQ&usq=AOvVaw3f9MPiSzQ0gy5XG8Wh7iM6>
- Martín Palacios, P. “Administración electrónica y derechos digitales”, *Derecho Digital e Innovación*, 9, (2021). Consultado el 4/ 03/ 25 <https://dialnet.unirioja.es/ejemplar/587310>

- Menchú, Walter; Colectivo de Autores (2024). Mejores Prácticas de Gobernanza e Institucionalidad para la Transformación Digital. Revista Marcando el rumbo. Centro de Investigaciones Económicas Nacionales Guatemala.
- MICOM (2017). Política integral para el perfeccionamiento de la informatización de la sociedad en Cuba.
- MICOM (2021). Compendio de documentos regulatorios. Telemática e informática.
- MICOM (2024). Política para la transformación digital, agenda digital cubana y estrategia de inteligencia artificial.
- Miranda Bonilla, Haideer (2022). Inteligencia artificial y justicia. Revista de la Facultad de Derecho de México. Tomo LXXII, Número 284, Septiembre-Diciembre. DOI:<http://10.22201/fder.24488933e.2022.284.83394>.
- Monsalve Moreno, M. (2006) “Métricas para la Interoperabilidad de la Información en el Gobierno Electrónico”. Memoria para optar al título de Ingeniero Civil en Computación. Santiago, Chile: Departamento de Ciencias de la Computación, Facultad de Ciencias Físicas y Matemáticas Universidad de Chile.
- Montes de Oca, F. (2002). Gobierno Electrónico (Capítulo). En Monge, Ricardo y otro. Costa Rica hacia la economía basada en el conocimiento. San José, Costa Rica: Litografía e Imprenta LIL.
- Morales, Medardo (2022). *Plataformas cubanas de Gobierno digital*. En *Habilitando la transformación digital*, T-II. Editorial UH. P-74 a 82.
- Naser, Alejandra (2021). Gobernanza Digital e interoperabilidad gubernamental, una guía para su implementación. CEPAL. Disponible en: [Http/www.cepal.org/es/publications](http://www.cepal.org/es/publications)
- Ochoa, Carlos (2015). Muestreo no probabilístico por Bola de Nieve. Disponible en [Http://www.netquest.com](http://www.netquest.com).
- Oszlak, O. (2006). Burocracia estatal: política y políticas públicas. POSTData. Revista de Reflexión y Análisis Político, 11– 56.
- Oszlak, O., & O’Donnell, G. (1995). Estado y políticas estatales en América Latina: hacia una estrategia de investigación. REDES, 2(4), 99– 128.

- Oszlak, O., y Gantman, E. (2007). La agenda estatal y sus tensiones: gobernabilidad, desarrollo y equidad. Iberoamericana. *Nordic Journal of Latin American and Caribbean Studies*, 37(1), 79– 110.
- Palomar Olmeda, A (2007.). La actividad administrativa efectuada por medios electrónicos. Navarra, España: Editorial Thomson- Aranzadi.
- Perera, Alina (2023). La IA: el bienestar posible. Disponible en <Http://www.presidencia.gob.cu/es/noticias>.
- Pérez Salomón, Omar (2012). Fidel Castro, soldado de las ideas. Tecnología y medios de comunicación. Editora Política, La Habana.
- Pierra, Fuentes, A; Rodríguez Figueredo, H; Fuentes Rodríguez, JM; Montesinos, R (2022). Principios para el desarrollo, uso y aplicación de las TIC en el Gobierno. *Revista Universidad y Sociedad*, 14 (4), 369-378.
- Poggiese, Héctor; Redín, María Elena; Cerezo, Matías; y Carllinni, José Manuel (2008), “El Foro de Responsables Informáticos de administración pública nacional: una lectura interpretativa”, en *Interoperabilidad en la administración pública*, Jefatura de Gabinete de Ministros (ed.), Buenos Aires, JGM, Secretaría de Gabinete y Gestión Pública.
- Puig Meneses, Yaima (2019). El proceso de informatización de la sociedad cubana es un hecho. Disponible en <Http://www.gramna.cu/cuba>.
- Puig Meneses, Yaima (2021). De la transformación de la sociedad a la transformación digital en Cuba. Disponible en <Http://www.presidencia.gob.cu>.
- Quesada, Rodolfo (2025). “Ciudadanos: Los Mensajeros del Estado”, publicado en Blog Efiqúicia, 2009. <http://efiquicia.roqz.net/2009/09/16/ciudadanos-los-mensajeros-del-estado/> (acceso febrero).
- Quintero, Rodrigo (2009). Separata de Modulo Componentes Éticos y Jurídicos, Diploma de Gobierno Electrónico y Gestión Publica. Santiago, Chile: INAP, Universidad de Chile.
- Rantanen, M. M., Koskinen, J. y Hyrynsalmi, S. (2019). "E-Government Ecosystem: A new view to explain complex phenomenon," 2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics

- (MIPRO), 2019, pp. 1408-1413, doi: 10.23919/MIPRO.2019.8756909. Disponible en: <https://ieeexplore.ieee.org/document/8756909> (enero, 2023).
- Rincón Cárdenas, E. (2006). *Manual de Derecho de Comercio Electrónico y de Internet*. Bogotá, Colombia: Centro Editorial Universidad del Rosario.
- Rincón Cárdenas, Erick; Martínez Molano, Valeria (2021). Un estudio sobre la posibilidad de aplicar la inteligencia artificial en las decisiones judiciales. *Revista Direito*, V-17, Nro1.
- Ríos-Campos, Carlos; Colectivo de Autores (2021). Estonia y Singapur: Casos de éxito de la Transformación Digital. *South Florida Journal of Development*, Miami, p.7758-7777 v. 2, n. 5, oct/dec.
- Roberts, Raimundo (2023). *Interoperabilidad en Gobierno electrónico. Conceptos y regulación extranjera, Estonia, Costa Rica y provincia del Neuquén*. Biblioteca del Congreso Nacional de Chile, 37052.
- Robkin, R (2010). “A Short History of Interoperability”. Ponencia presentada en el FDA-Continua-CIMIT Workshop, en Silver Spring, Maryland, Estados Unidos, 25 al 27 de enero.
- Rodríguez, Yunier (2022). *El observatorio de Gobierno digital en Cuba: un enfoque desde ciencia, política pública y ciudadanía*. En *Habilitando la transformación digital*, T-II. Editorial UH. P-60 a 73.
- Sala Constitucional de la Corte Suprema de Justicia de Costa Rica. Voto 6195-07. San José, Costa Rica, 2007b.
- Salas Ruiz, F. (2007). *La utilización de software libre y estándares abiertos en la Construcción del Gobierno Electrónico*, Tesis para optar al Grado de Magíster en Derecho de la Informática y de las Telecomunicaciones. Santiago, Chile, Facultad de Derecho, Universidad de Chile.
- Sánchez García, Alfonso (2022). La gestión del dato en la contratación pública. *Revista Sarteca*, 182. Editorial La Ley.
- Santos, Ernani Marques dos (2008), “Implementing Interoperability Standards for Electronic Government: an Exploratory Case Study of the E-PING Brazilian Framework”, en *International Journal of Electronic Government Research*, Vol. 4 N° 3, Hershey, pp. 103-112.

- Simborg, D. W. (1988). Network Application Architecture. Proceedings of the Annual Symposium on Computer Application in Medical Care, 648.
- Tarrés Vives, Marc (2003). Normas Técnicas y Ordenamiento Jurídico. Valencia, España: Tirant Lo Blanch.
- Valero Torrijos, J. (2018). “La necesaria reconfiguración de las garantías jurídicas en el contexto de la transformación digital del Sector Público”, en DE LA QUADRASALCEDO FERNÁNDEZ DEL CASTILLO, Tomás, y PIÑAR MAÑAS, José Luis (Coord.), Sociedad digital y derecho, Madrid: Ministerio de Industria, Comercio y Turismo.
- Vivas, Hector Luis; Colectivo de Autores (s.a). Diseño de un ecosistema de interoperabilidad en la Provincia de Río Negro. Universidad Nacional de Río Negro (UNRN), Laboratorio de de Informática Aplicada LIA, Sede Atlántica, Viedma, Río Negro SIE, Simposio de Informática en el Estado.
- Whittingham Munévar, M. V. (2010). “¿Qué es la gobernanza y para qué sirve?”, Revista Análisis Internacional RAI, N° 2, Bogotá, Editorial Utadeo.
- Winner, L. (1980). Do Artifacts Have Politics? Daedalus, 109(1), 121– 136.
- Wolpes Álvarez, Antonio (2022). Retos en el Gobierno electrónico en la transformación digital de la administración pública en Cuba. Disponible en [Http://www.scielo.sld.cu](http://www.scielo.sld.cu).