GOBERNANZA DE DATOS PARA EL SECTOR PÚBLICO COSTARRICENSE

Costa Rica, 2022

Contenido

Autoridades

Ministerio de Comunicación	Agustín Castro Solano
Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones	Paola Vega Castillo

Comisión Nacional de Datos Abiertos

Ministerio de Comunicación	Sigrid Segura Artavia
Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones	Diego Vargas Pérez Vivian Aguilar Aguilar
Ministerio de Planificación Nacional y Política Económica	Sylvia Retana Rodríguez Iván Acuña Chaverri
Dirección General de Archivo Nacional	Ivannia Valverde Guevara Denise Calvo López
Instituto Nacional de Estadística y Censos	Ronny Umaña Palma Pilar Ramos Vargas
Organización Abriendo Datos Costa Rica	Susana Soto González Ignacio Alfaro Marín
Cooperativa Sulá Batsú	Kemly Camacho Jiménez Christian Hidalgo García
Conare - Universidad Nacional	Dennis Víquez Ruíz
Sector Privado	David Zamora Barrantes Jorge Umaña Cubillo Guillermo Rodríguez

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones

Dirección de Gobernanza Digital	Jorge Mora Flores
Dirección de Gobernanza Digital	Dayanna Mejía García
Dirección de Gobernanza Digital	Roberto Lemaitre Picado

Acompañamiento Técnico y Compilación

Comisión Económica para América Latina y el Caribe	Francisco Mendez Sanhueza
Ministerio de Comunicación	Sigrid Segura Artavia

Revisión y Aportes

Comisión Nacional de Datos Abiertos	Christian Hidalgo García
Dirección de Gobernanza Digital	Dayanna Mejía García
Comisión Nacional de Datos Abiertos	Dennis Víquez Ruíz
Comisión Nacional de Datos Abiertos	Diego Vargas Perez
Comisión Nacional de Datos Abiertos	Ignacio Alfaro Marín
Comisión Nacional de Datos Abiertos	Ivannia Valverde Guevara
Comisión Nacional de Datos Abiertos	Jorge Umaña Cubillo
Dirección de Gobernanza Digital	Jorge Mora Flores
Comisión Nacional de Datos Abiertos	Pilar Ramos Vargas
Dirección de Gobernanza Digital	Roberto Lemaitre Picado
Comisión Nacional de Datos Abiertos	Ronny Umaña Palma
Comisión Nacional de Datos Abiertos	Sigrid Segura Artavia
Comisión Nacional de Datos Abiertos	Susana Soto González
Comisión Nacional de Datos Abiertos	Sylvia Retana Rodríguez

Glosario

Accesibilidad de los datos. Grado en el que los datos pueden ser accedidos en un contexto específico, particularmente por personas que necesiten tecnologías de apoyo o una configuración especial por algún tipo de discapacidad.

Actualidad de los datos. Grado en el que los datos tienen atributos que tienen la edad correcta en un contexto de uso específico.

Credibilidad. Grado en el que los datos tienen atributos que se consideran ciertos y creíbles en un contexto de uso específico. La credibilidad incluye el concepto de autenticidad (la veracidad de los orígenes de datos, la calidad y atribuciones, compromisos).

Completitud. Grado en el que los datos asociados con una entidad tienen valores para todos los atributos esperados e instancias de entidades relacionadas en un contexto de uso específico.

Comprensibilidad. Grado en el que los datos tienen atributos que permiten ser leídos e interpretados por los usuarios y son expresados utilizando lenguajes, símbolos y unidades apropiados en un contexto de uso específico. Cierta información sobre la comprensibilidad puede ser expresada mediante metadatos.

Confidencialidad. Grado en el que los datos tienen atributos que aseguran que mismos son sólo accedidos e interpretados por usuarios autorizados en un contexto de uso específico. La confidencialidad es un aspecto de la seguridad de la información (junto con la disponibilidad y la integridad).

Conformidad. Grado en el que los datos tienen atributos que se adhieren a estándares, convenciones o normativas vigentes y reglas similares referentes a la calidad de datos en un contexto de uso específico.

Consistencia. Grado en el que los datos están libres de contradicción y son coherentes con otros datos en un contexto de uso específico. Puede ser analizada en datos que se refiere tanto a una como a varias entidades comparables.

Disponibilidad. Grado en el que los datos tienen atributos que permiten ser obtenidos por usuarios y/o aplicaciones autorizados en un contexto de uso específico.

Eficiencia. Grado en el que los datos tienen atributos que pueden ser procesados y proporcionados con los niveles de rendimiento esperados mediante el uso de cantidades y tipos adecuados de recursos en un contexto de uso específico.

Exactitud. Grado en el que los datos representan correctamente el verdadero valor del atributo deseado de un concepto o evento en un contexto de uso específico.

Tiene dos principales aspectos:

a. Exactitud Sintáctica: cercanía de los valores de los datos a un conjunto de valores definidos en un dominio considerado sintácticamente correcto.
b. Exactitud Semántica: cercanía de los valores de los datos a un conjunto de valores definidos en un dominio considerado semánticamente correcto.

Portabilidad. Grado en el que los datos tienen atributos que les permiten ser instalados, reemplazados o eliminados de un sistema a otro, preservando el nivel de calidad en un contexto de uso específico.

Precisión. Grado en el que los datos tienen atributos que son exactos o proporcionan discernimiento en un contexto de uso específico.

Recuperabilidad. Grado en el que los datos tienen atributos que permiten mantener y preservar un nivel específico de operaciones y calidad, incluso en caso de fallos, en un contexto de uso específico.

Trazabilidad. Grado en el que los datos tienen atributos que proporcionan un camino de acceso auditado a los datos o cualquier otro cambio realizado sobre los datos en un contexto de uso específico.

Nota. Los conceptos utilizados en el presente Glosario han sido transcritos de la propuesta de asesoría técnica[1].

[1] Méndez, F. (2021).

Presentación

Conscientes de la necesidad de contar con un marco inicial para la gestión y gobernanza de datos en el Sector Público Costarricense, en 2021 (atendiendo la disposición 4.8 del informe N° DFOE-CAP-IF-00012-2021) la Comisión Nacional de Datos Abiertos decidió asumir el reto de trabajar y apoyar los esfuerzos en materia de datos desde su experiencia e interés.

Construir un instrumento de gobernanza sobre cualquier temática no es tarea menor, y en materia de datos el reto es aún mayor, dado no solo por la complejidad y relevancia que adquiere el tema en la actualidad y los pocos instrumentos de referencia regionales que existen en la materia, sino también por los carentes recursos disponibles y la coyuntura nacional atravesada por la pandemia por COVID-19 y transición de gobierno.

En ese sentido, reconociendo la responsabilidad de avanzar pero también la seriedad y rigor con la que se debe asumir el tema, se ha plasmado en el presente documento algunos puntos de partida y recomendaciones para la construcción e implementación de un Modelo Nacional de Gobernanza de Datos para el Sector Público Costarricense (MGD-CR).

Capítulo I. Introducción

Los datos y la información son activos que tienen valor para cualquier entidad. Ese valor se encuentra implícito y transversal a todo el ciclo de vida del dato, por tanto en su gestión se deben considerar sus distintas etapas, principios, estándares, legislación, roles y mecanismos de interacción de los diversos actores involucrados y su ecosistema.

Es decir, su ciclo de vida debe abordar el dato desde su creación, almacenamiento, extracción, importación y exportación, migración, validación, edición, actualización, transformación, conversión, revisión, integración, restauración, segregación, recuperación, archivo y eliminación.

Por tanto, es importante tener en cuenta su arquitectura institucional, cuestiones de organización y de cultura distintivas, así como los retos y oportunidades para su gestión, que varían en cada país. Toda propuesta de gobernanza de datos debería ser única y para su construcción se requiere conocer el estado, cultura y dinámica de la administración pública de cada país. Y en ese sentido, el presente abordaje inicialmente da un acercamiento conceptual y principios rectores propuestos, así como un repaso por el marco normativo actual, para seguidamente introducir una serie de procesos sugeridos en la propuesta presentada por la asesoría técnica[2], para llegar a su implementación.

[2] Méndez, F. (2021).

Capítulo II. Sobre el proceso

Para el diseño de este esquema inicial se procedió, en primera instancia con la revisión bibliográfica de documentos de referencia técnica y política a nivel internacional, tanto global como local. Asimismo se realizaron sesiones de intercambio con la asesoría técnica recibida desde la Comisión Económica para América Latina y el Caribe (CEPAL) y sesiones de trabajo en las que participaron miembros de la Comisión Nacional de Datos Abiertos (CNDA) y representantes del Ministerio de Comunicación y la Dirección de Gobernanza Digital (DGD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.

La Comisión Nacional de Datos Abiertos

Constituye un foro permanente multiactor presidido y coordinado por el Ministerio de Comunicación, encargado de asesorar los procesos en materia de apertura de datos públicos, y que en este proceso ha asumido el rol de coordinación y liderazgo. Se encuentra conformado por representaciones de:

- Ministerio de Comunicación.
- Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones.
- Ministerio de Planificación Nacional y Política Económica.
- Instituto Nacional de Estadísticas y Censos.
- Dirección General de Archivo Nacional.
- Dos representantes de organizaciones sociales.
- Dos representantes del sector privado.
- Un representante del sector académico.

Dirección de Gobernanza Digital

La Dirección de Gobernanza Digital (DGD) del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), tiene por objetivo “brindar los insumos para emitir las políticas públicas, estándares, normas, procedimientos y lineamientos en materia de Gobernanza Digital, así como brindar acompañamiento a las instituciones públicas en la implementación de proyectos

en materia de Gobernanza". Sus funciones son: coordinar, promover, fomentar y desarrollar la Gobernanza Digital en Costa Rica, transformando a este sector en motor para el desarrollo económico y social del país. La DGD ha dado apoyo durante el proceso y realizado alianzas para el acompañamiento técnico por parte de la CEPAL.

Comisión Económica para América Latina y el Caribe

La Comisión Económica para América Latina y el Caribe (CEPAL) es un organismo dependiente de la Organización de las Naciones Unidas, creado para promover el desarrollo económico y social de la región.

La CEPAL ha venido dando apoyo técnico y acompañamiento al MICITT en la construcción e implementación de otras acciones e instrumentos de transformación digital e interoperabilidad. De esta manera, y dada la relación en la materia, para el diseño del MGD-CR se recibió el apoyo técnico del organismo por medio de un apoyo técnico, la cual se presenta como parte de este documento.

Capítulo III. Marco conceptual

Entre la multiplicidad de acepciones que aporta la literatura, Weber ...[et al] (2009) y Khatri y Brown (2010) definen la gobernanza de datos en términos de marco que establece derechos y responsabilidades en la toma de decisiones en el uso de datos. Otros aportes plantean entender el concepto como la confluencia de varias áreas relacionadas con los datos como la gestión de calidad de datos, los sistemas de gestión de datos, la seguridad de datos y la administración de datos.

En el monográfico de la revista Information Systems Frontiers dedicado a Big and Open Linked Data en el sector público, se destacan diferentes factores que propician e influyen en los procesos de innovación basados en datos (data-driven innovation) (Janssen ...[et al], 2017). Entre los mismos sobresale precisamente la

gobernanza de datos asociada a su acceso y calidad, a la posibilidad de reutilización, a las capacidades para procesarlos y compartirlos y, finalmente, a la normativa de acceso, seguridad y privacidad. Pero tanto la propia gobernanza de datos como los procesos de innovación asociados a los datos también vienen condicionados por factores políticos y estratégicos, organizativos y tecnológicos, a los que hay que añadir cuestiones de seguridad y privacidad en su uso.

En esa misma línea, el libro *Definitive guide to Data Governance* expone que el proceso permite fijar una serie de procesos y responsabilidades que aseguran la calidad y la seguridad de los datos que se emplean en una sociedad u organización, definiendo quién puede emprender cuáles acciones, sobre qué datos, en qué situaciones y mediante qué métodos. Mientras que de acuerdo a la definición del Data Governance Institute, “la gobernanza de datos es un sistema de derechos de decisión y responsabilidades para los procesos relacionados con la información, ejecutado de acuerdo con modelos acordados que describen quién puede tomar qué acciones con qué información, y cuándo, bajo qué circunstancias, usando qué métodos. “

Para efectos de esta propuesta, partiremos de que la gobernanza de datos es un conjunto de procesos, funciones, mediciones, normas, políticas y procedimientos que garantizan el uso seguro, eficaz y eficiente de los datos para apoyar y fortalecer la toma de decisiones .

Capítulo IV. Principios rectores

En este apartado se proponen una serie de principios rectores transversales a la integralidad que debería tener el MGD-CR, los cuales parten del marco conceptual de la Guía de Fundamentos para la Gestión de Datos[3]:

Los datos son un activo. Los datos tienen un valor real, tangible y medible, por lo que deben reconocerse como un valioso activo en las instituciones públicas. Los datos son el activo clave para la toma de decisiones, por lo que debe asegurarse que sean definidos, controlados y accesibles. Además, es importante señalar que, como activos públicos, deben contemplarse como parte de la materia de las normativas de acceso a la información pública.

Los datos son un recurso valioso; tienen un valor real y medible. En términos simples, el propósito de los datos es ayudar a la toma de decisiones, y los datos precisos y oportunos son fundamentales para ello. Los activos institucionales se administran cuidadosamente y los datos no son una excepción, siendo estos la base de nuestra toma de decisiones, por lo que también debemos gestionar cuidadosamente los datos para asegurarnos de que sabemos dónde están, podemos confiar en su exactitud y podemos obtenerlos cuando y donde los necesitemos.

Los datos se comparten. La toma de decisiones compartida es un eje distintivo en un Gobierno de Datos. Los usuarios tienen acceso a los datos necesarios para realizar sus tareas; por lo tanto, los datos se comparten entre las funciones y áreas interinstitucionales.

El acceso oportuno a datos precisos es esencial para mejorar la calidad y la eficiencia de la toma de decisiones institucionales, y por tanto es menos costoso

[3] DAMA-DMBOK

mantener datos oportunos y precisos en una sola aplicación y, a continuación, compartirlos, que mantener datos duplicados en varias aplicaciones. Así, los datos compartidos darán lugar a decisiones basadas en evidencia más ágiles, oportunas y precisas utilizando menos fuentes y mejorando la calidad de las mismas.
Asimismo, el compartirlos es necesario, tanto para la toma de decisiones, como para la generación de conocimiento, como parte del derecho a una democratización de los datos.

Los datos son accesibles. Los datos son accesibles para que los usuarios realicen sus funciones. El amplio acceso a los datos conduce a la eficiencia y eficacia en la toma de decisiones, y ofrece una respuesta oportuna a las solicitudes de información y a la prestación de servicios. El uso de la información debe tenerse en cuenta desde una perspectiva institucional para permitir el acceso de una amplia variedad de usuarios. Se ahorra tiempo de personal y se mejora la coherencia de los datos

Los datos son administrados. Cada elemento de datos tiene una entidad y persona administradora responsable de la calidad de los datos. Una de las ventajas de un entorno de arquitectura es la capacidad de compartir datos de diverso tipo y formato (texto, número, imagen, video, sonido, etc.) entre instituciones. A medida que crece el grado de intercambio de datos y las unidades institucionales se basan en información común, se vuelve esencial que solo el administrador de datos tome decisiones sobre el contenido de los mismos. Dado que los datos pueden perder su integridad cuando se ingresan varias veces, la entidad administradora será la única responsable de la entrada de datos, lo que elimina el esfuerzo humano redundante y los recursos de almacenamiento de datos.

Los datos son protegidos. Los datos están protegidos contra el uso y la divulgación ilegal y no autorizada. Además de los aspectos tradicionales de la clasificación de seguridad nacional, lo que incluye, pero no se limita a la protección de la información previa a la toma de decisiones, sensible, sensible al origen, y propietario.

El intercambio abierto de información y la divulgación de información con el sustento legal pertinente, deben equilibrarse con la necesidad de restringir la disponibilidad de información. Las leyes y reglamentos existentes requieren la salvaguardia de la seguridad nacional y la privacidad de los datos, al tiempo que permiten el acceso libre.

Los datos tienen una semántica. Los datos se definen de forma coherente en todo el sector y las definiciones son comprensibles y están disponibles para todas las personas usuarias. Los datos que se utilizarán en el desarrollo y/o implementación de aplicaciones deben tener una definición común en todas las áreas institucionales para permitir su intercambio. Un vocabulario común facilitará las comunicaciones y permitirá que el diálogo sea eficaz. Además, es necesario para interconectar sistemas e intercambiar datos.

Capítulo V. Objetivo

Implementar un modelo de gobernanza por medio del alineamiento estratégico de la gestión estatal de datos, que genere valor público mediante un conjunto de procesos, funciones, mediciones, normas, políticas y procedimientos que garanticen el uso seguro, eficaz, transparente y eficiente de los datos para apoyar y fortalecer la toma de decisiones y la generación de conocimiento, con ética y respeto de los derechos humanos.

Capítulo VI. Marco regulatorio

Costa Rica cuenta con diversos instrumentos reguladores y orientadores en materia de gobernanza y transformación digital, apertura de datos públicos y protección de datos personales y empresariales. Se señala a continuación un recuento de las principales normas, con la recomendación de que puede ser ampliado con cualquier otro instrumento normativo que haya sido omitido o que se genere a futuro.

Ley General de la Administración Pública N° 6227

Regula la Administración Pública constituida por el Estado y los demás entes públicos, cada uno con personalidad jurídica y capacidad de derecho público y privado.

Ley Protección de la Persona frente al tratamiento de sus datos personales N° 8968

Tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa con relación a su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes.

Ley General de Telecomunicaciones N° 8642

Establece el ámbito y los mecanismos de regulación de las telecomunicaciones, que comprende el uso y la explotación de las redes y la prestación de los servicios de telecomunicaciones. Están sometidas a la presente Ley y a la jurisdicción costarricense, las personas, físicas o jurídicas, públicas o privadas, nacionales o extranjeras, que operen redes o presten servicios de telecomunicaciones que se originen, terminen o transiten por el territorio nacional.

Ley Sistema de Estadística Nacional N° 9694

Regula el Sistema de Estadística Nacional, las instituciones que lo componen, fija las normas básicas para su adecuada coordinación y la obtención de información que permita el desarrollo estadístico de manera veraz y oportuna.

Ley del Sistema Nacional de Archivos N° 7202

Regula el funcionamiento de los órganos del Sistema Nacional de Archivos y de los archivos de los Poderes Legislativo, Judicial y Ejecutivo, y de los demás entes públicos, cada uno con personalidad jurídica y capacidad de derecho público y privado, así como de los archivos privados y particulares que deseen someterse a estas regulaciones.

Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454

Establece por firma digital cualquier conjunto de datos adjunto o lógicamente asociado a un documento electrónico, que permita verificar su integridad, así como identificar en forma unívoca y vincular jurídicamente al autor con el documento electrónico. Así mismo indica que una firma digital se considerará certificada cuando sea emitida al amparo de un certificado digital vigente, expedido por un certificador registrado.

Ley de Protección al ciudadano del exceso de requisitos y trámites administrativos N° 8220

Esta ley es aplicable a toda la Administración Pública, central y descentralizada, incluso instituciones autónomas y semiautónomas, órganos con personalidad jurídica instrumental, entes públicos no estatales, municipalidades y empresas públicas. Se exceptúan de su aplicación los trámites y procedimientos en materia de defensa del Estado y seguridad nacional. Para los efectos de esta Ley, se entenderá por administrado a toda persona física o jurídica que, en el ejercicio de su derecho de petición, información y/o derecho o acceso a la justicia administrativa, se dirija a la Administración Pública.

Decreto Ejecutivo N° 40199-MP " Establece la apertura de los datos públicos"

Establece la forma mediante la cual, los datos de carácter público, se ponen a disposición de la población como datos abiertos, con el propósito de facilitar su acceso, uso, reutilización y redistribución para cualquier fin lícito. El Decreto es de

aplicación obligatoria a la Administración Pública Central, sin perjuicio del principio de separación de poderes consagrado en la Constitución política y el régimen de autonomía que corresponda de conformidad con las disposiciones legales y constitucionales pertinentes, los Poderes Legislativo y Judicial, el Tribunal Supremo de Elecciones, sus dependencias y órganos auxiliares, municipalidades, universidades estatales, instituciones autónomas, semiautónomas, empresas públicas, así como las empresas privadas que administran bienes públicos o ejecutan potestades públicas, podrán aplicar la presente normativa como marco de referencia para el fomento de la Apertura de Datos Públicos.

Directriz Ejecutiva N° 074-MP "Apertura de Datos Abiertos"

Establece la forma mediante la cual, los datos de carácter público, se ponen a disposición de la población como datos abiertos, con el propósito de facilitar su acceso, uso, reutilización y redistribución para cualquier fin lícito. Esta directriz va dirigida a las instituciones que conforman la Administración Pública Descentralizada.

Decreto Ejecutivo N° 40200-MP-MEIC-MC "Transparencia y Acceso a la Información Pública"

Tiene por objeto que el Estado garantice el cumplimiento efectivo del derecho humano de acceso a la información pública, de forma proactiva, oportuna, oficiosa, completa y accesible.

Directriz Ejecutiva N° 073-MP-MEIC-MC "Transparencia y Acceso a la Información Pública"

Tiene por objeto que el Estado garantice el cumplimiento efectivo del derecho humano de acceso a la información pública, de forma proactiva, oportuna, oficiosa, completa y accesible. Esta directriz va dirigida a las instituciones que conforman la Administración Pública Descentralizada.

Directriz N° 019-MP-MICITT "Desarrollo del Gobierno Digital del Bicentenario"

Ordena a la Administración Central y se instruye a la Administración Descentralizada a tomar las medidas administrativas, técnicas y financieras

necesarias para la consecución de los objetivos del Gobierno Digital del Bicentenario.

Directriz N° 133- MP-MICITT "Mejoras en Materia de Ciberseguridad para el Sector Público del Estado"

Se instruye a la Administración Pública Central y se insta a la Administración Pública Descentralizada a cumplir las recomendaciones y medidas técnicas que emanen del Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones, por medio de la Dirección de Gobernanza Digital y el Centro de Respuesta de Incidentes de Seguridad Informática, como ente coordinador de la ciberseguridad nacional, referentes a ciberseguridad y seguridad de la información, con el fin de mejorar las capacidades técnicas, de atención y de gestión de la ciberseguridad y seguridad de la información en las instituciones.

Capítulo VI. Alineamiento Estratégico

Para que el modelo de gobernanza sea eficiente y cumpla sus objetivos, se considera indispensable la alineación estratégica con cada uno de los instrumentos de política pública y de planificación nacional que se relacionen con la materia, tales como: la Política Nacional de Sociedad y Economía basadas en el Conocimiento (PNSEBC), el Plan Nacional de Ciencia, Tecnología e Innovación (PNCTI), Plan Nacional de Desarrollo y de Inversiones Públicas (PNDIP 2019-2022), Plan Nacional de Estado Abierto, entre otros incluidos en el siguiente listado que se recomienda revisar y mejorar.

Instrumento	Linea clave
Objetivos de Desarrollo Sostenible	Objetivo 8. Trabajo decente y crecimiento económico. Objetivo 9. Industria, innovación, infraestructura. Objetivo 16. Paz, justicia e instituciones fuertes.

	Objetivo 17. Alianzas para los objetivos.
Carta Internacional de Datos Abiertos	Principios de los Datos Abiertos.
Política Nacional de Sociedad y Economía basadas en el Conocimiento (2022-2050)	Quinto Pilar Tecnología Digital: Fomento de las Tecnologías Digitales como catalizador del conocimiento. Línea de acción 14.
Plan Nacional de Ciencia, Tecnología e Innovación PNCTI (2022-2027)	Temática Transversal: Tecnologías Digitales
Plan Nacional de Desarrollo y de Inversión Pública del Bicentenario PND IP (2019-2022)	Área estratégica: Innovación y Competitividad Meta Nacional: PIB Real
Estrategia de Transformación Digital hacia la Costa Rica del Bicentenario 4.0 (2018-2022)*	Eje Buena Gobernanza. Líneas de Acción: 1. Promover la ciencia de datos para la toma de decisiones y gestión de riesgos 2. Estado Abierto para la participación ciudadana digital 3. Política Nacional de Preservación de Datos e Información 4. Adaptación del marco normativo nacional a las nuevas tecnologías
Plan Nacional de Estado Abierto	Compromisos de: Educación, Empleo, Descarbonización, Inclusión Social, Integridad y Anticorrupción, Reactivación Económica, Seguridad Ciudadana, Justicia Abierta, Parlamento Abierto.

Estrategia Nacional de Ciberseguridad (2017-2021)*	Línea Estratégica 2.2. Sector público Línea estratégica 6.3. Adopción de medidas de seguridad de referencia
Código Nacional de Tecnologías Digitales	Capítulos: 1. Accesibilidad, Usabilidad y Experiencia de Usuario. 2. Identificación y Autentificación Ciudadana. 3. Seguridad Tecnológica. 4. Infraestructura y Tecnología en la Nube. 5. Interoperabilidad. 6. Neutralidad Tecnológica.

*A la fecha de este documento ambas Estrategias se encuentran en proceso de construcción de su próxima versión.

Capítulo VII. Proceso de Implementación

Para la eventual implementación del MGD-CR, desde la asesoría técnica recibida de CEPAL[4] se proponen cuatro fases de avance, las cuales se mencionan y describen a continuación:

Fase 0. Adherencia a estándares

La adherencia a estándares implica revisión, estudio, análisis y adhesión a estándares sobre la Arquitectura Institucional, el Gobierno de Datos, y la Calidad de Datos. De estos últimos se resaltan características inherentes al dato, inherentes al sistemas e híbridas.

En ese sentido, como parte de la Fase 0 propuesta, se recomienda[5] considerar una serie de prácticas en cuanto la seguridad de datos, debido a que el nivel de protección de la información de la organización puede aumentar cuando en el plan de seguridad se tienen en cuenta mejores acciones como las siguientes:

1. Definir una estrategia global de seguridad y actualizarla.

2. Monitorizar todas las aplicaciones con acceso a datos para detectar las menos seguras y trabajar sobre esos puntos débiles, evitando que se conviertan en una puerta de acceso para ataques.

[4] Los textos incluidos en esta sección, se integran con fidelidad a la propuesta recibida.
[5] Méndez, F. (2021)

3. Crear controles de acceso específicos para todos los usuarios, limitando su acceso a los sistemas que necesitan para sus tareas exclusivamente y reduciendo así la exposición de los datos sensibles.

4. Obtener un registro completo y detallado de lo que ocurre en los sistemas corporativos. Una decisión que, además de reforzar la seguridad, facilitará la resolución de problemas.

5. Asegurarse de que la seguridad del software y del hardware están actualizadas con las nuevas tecnologías antimalware.

6. Nombrar a una persona oficial de seguridad de la información para que se haga cargo de la seguridad.

7. Formar a los usuarios en mejores prácticas de seguridad cibernética para que sepan crear contraseñas seguras, reconocer emails sospechosos de amenaza, evitar aplicaciones peligrosas y prevenir cualquier otro riesgo relevante para la seguridad de la información.

8. Definir claramente los requisitos y las expectativas de la organización en materia de seguridad, especialmente al practicar contrataciones o al iniciar relaciones con socios y proveedores.

9. Determinar una línea de base que incluya los estándares de seguridad aplicables a terceros.

10. Monitorizar la actividad usuaria para verificar que sus acciones cumplen con las recomendaciones de seguridad.

11. Crear un plan de respuesta a la violación de datos que permita cerrar cualquier vulnerabilidad y limitar el daño que la brecha puede hacer.

12. Garantizar el cumplimiento normativo en toda la organización y estar al tanto de los cambios que pudieran producirse en la legislación.

13. Realizar evaluaciones de las amenazas y estudiarlas mediante técnicas de análisis que permitan estar mejor protegido.

14. No usar diccionarios ni algoritmos de descifrado, que se podrían hackear, sino usar reglas de enmascaramiento fijas o aleatorias.

15. Sustituir los encriptados por enmascaramiento o hacer una encriptación centralizada y llevada a cabo por el propio producto.

Fase 1. Nivel de madurez

Evaluar el nivel de madurez de la organización en el gobierno de datos es necesario para conocer nuestra ubicación en el espectro del ciclo y de esa manera orientar mejor los esfuerzos. Algunas de las sugerencias en este proceso van desde aplicar un cuestionario de madurez, e identificar el nivel actual de madurez de gobierno de datos, hasta definir el siguiente nivel al que se desea llegar. De acuerdo con la asesoría técnica brindada desde CEPAL, se puede implementar un esquema basado en algunas prácticas del gobierno de datos, diagnosticando el nivel de madurez y así orientar la ruta a seguir, tal como se indica en la tabla 1.

Nivel de Madurez	Procesos
2	DM.1. Gestión de Requisitos de Datos DM.2. Gestión de la Infraestructura Tecnológica DM.3. Gestión de Datos Históricos DM.4. Gestión de la Seguridad de Datos DM.5. Gestión de la Configuración de Datos DQM.2. Monitorización y Control de Calidad de Datos DG.4. Establecimiento de Estándares, Políticas y Buenas Prácticas
3	DM.6. Gestión de Datos Maestros y de Referencia DM.7. Arquitectura y Diseño de Datos DM.8. Establecimiento de Fuentes y Destinos de Datos DM.9. Integración de Datos DQM.1. Planificación de Calidad de Datos DG.1. Establecimiento de Estrategias de Datos DG.2. Gestión del Ciclo de Vida de los Datos DG.5. Gestión de Recursos Humanos
4	DQM.3. Aseguramiento de Calidad de datos DG.3. Gestión del Valor de los Datos DG.6. Gestión de Recursos Financieros DG.7. Monitorización de las Estrategias Organizacionales de Datos
5	DQM.4. Mejora de Calidad de Datos DG.8. Gestión de Cambios en las Estrategias de Datos

Tabla 1. Diagnóstico de Nivel de Madurez

Fase 2. Priorizar el gobierno de datos

Mediante la fase 2 se propone priorizar el gobierno de datos con base a las necesidades de la institución. De esta manera y con base en las principales recomendaciones internacionales[6], se sugieren algunas actividades y proyectos a implementar:

1. Definir las prioridades de la Institución y sus respectivos modelos de dominio para el gobierno de datos.
2. Definición del mapa de interdependencias de datos, en función de las fuentes de datos existentes, priorizados de las necesidades institucionales.
3. Identificar aplicaciones impactadas en la interdependencia de datos.
4. Creación del listado de datos y aplicaciones impactadas con otros dominios de información.

[6] DAMA-DMBOK

5. Creación de los grupos de datos/aplicaciones de menor a mayor impacto con otros dominios (autocontenido).
6. Definir el grupo de datos priorizados, partiendo por el de menor impacto, que se debe gobernar y crear backlog con los grupos restantes.
7. Generación de Roadmap de implementación de cada grupo de datos a gobernar.

Fase 3. Gestión de datos priorizados

Como parte de la gestión de datos priorizados se sugiere abordar tres aspectos centrales como: gestión de calidad del dato y gestión de la seguridad del dato.

Gestión de la Calidad del Dato

Perfilado de Datos

Intenta obtener las reglas de negocio, para el perfilado de datos estructurante por medio de cuestionantes como: ¿Cuáles son las reglas de servicio estructurante de los datos del grupo priorizado?, así como del perfilado de datos de contenido respondiendo a ¿Cuáles son las reglas de servicio para el contenido de cada dato del grupo priorizado?

Asimismo, complementar las reglas de servicio en una herramienta de software, para conocer:
Completitud: ¿Qué dato falta o no se usa en el grupo priorizado?.
Consistencia: ¿Qué datos presentan información conflictiva?
Duplicación: ¿Qué datos están duplicados?
Precisión: ¿Qué datos son incorrectos u obsoletos?
Integridad: ¿Qué datos no están correctamente referenciados?
Relaciones y Dependencias: ¿Cómo están relacionados los datos, del grupo priorizado, con el resto de fuentes de datos existentes?.

Ineficiencias / Redundancias: ¿Qué datos son redundantes, están huérfanos, son inconsistentes?.
Conformidad: ¿Qué datos tienen un formato o un contenido no acorde al estándar definido?.
Ratios: ¿Qué cálculos, valores, resultados se salen de los rangos de validez?

Es decir, aplicar la herramienta de software y realizar una validación por el responsable institucional en las fuentes de datos existentes y generar informes permite conocer e intervenir aspectos importantes como la eventual falta de completitud, falta de consistencia, datos duplicados, datos incorrectos u obsoletos, falta de Integridad referencial, falta de relaciones y dependencias, datos que son redundantes, están huérfanos, o son inconsistente, datos que tienen un formato o un contenido no acorde al estándar definido, así como datos fuera de los rangos y valores definidos.

Limpieza y Estandarización/Normalización de Datos

En materia de limpieza se podría aplicar *parsing* al dato, donde se requiera, el cual permite la descomposición de los distintos elementos que lo componen. Existen múltiples modos de separar los datos, desde métodos simples por medio de sub cadenas (usado para referencias de productos, números de cuenta, separación del prefijo del teléfono), hasta métodos más complejos que usan diccionarios de valores y componentes que tienen en cuenta los patrones, la posición de un elemento o el tipo de dato. En ese sentido se sugieren algunas prácticas como:

Aplicar la estandarización del dato, como la adecuación de un dato a un formato esperado. Por ejemplo, el reemplazo de caracteres o la sustitución de elementos a partir de diccionarios de traslación y componentes de tratamiento de mayúsculas y minúsculas

Aplicar normalización del dato, consiste en el reemplazo/enriquecimiento de un elemento erróneo o la no existencia del mismo por uno correcto. Esto generalmente se realiza a través del enfrentamiento de los datos originales contra los existentes en una fuente de datos de referencia o con diccionarios. La relación con fuentes externas o diccionarios se realiza a través de la relación directa con otros campos o a través de un proceso de *matching*).

Aplicar enriquecimiento al dato donde se requiera, consiste en añadir datos que no existían originalmente en la fuente de origen. Técnicamente, es muy similar al proceso de corrección sólo que, en lugar de un dato incorrecto, lo que se reemplaza es un dato vacío.

Matching

Aplicar *matching* al dato, donde se requiera, consiste en buscar registros que tengan una coincidencia, dependiendo de una serie de atributos, los cuales servirán para identificar los duplicados.

Gestión de la Seguridad del Dato

Con relación a las necesidades de seguridad, regulaciones en general y la regulación de datos, es importante abordar algunas cuestiones como: ¿Cuáles son los requisitos institucionales para la seguridad del dato? ¿Auditable? ¿Restringido a un perfil de usuarios? ¿Sin restricción? ¿Qué es privado? ¿Qué es confidencial? ¿Qué es público? ¿Cuáles son los requisitos reglamentarios, regulatorios o legales para el dato?

Por otro lado, definir la Política de Seguridad de Datos además de dar mayor fortaleza jurídica al proceso, permite adelantar, actualizar y definir una gestión más robusta de los mismos, considerando aspectos como: ¿Cuáles son las políticas de seguridad del dato definidas por el gobierno? ¿Cuáles son las políticas de seguridad del dato definidas por el área de tecnología? ¿Se requiere una política de seguridad estricta y con el máximo de obstáculos para que el dato no se visualice de forma fácil? ¿Se requiere una política de seguridad basada en la confianza y con trazabilidad del acceso a este dato? ¿Se requiere definir ninguna política de seguridad para el dato?

En caso de definir los Controles y Procedimientos de Seguridad de Datos, cabe valorar cuáles son los controles de seguridad a ser aplicados a los datos, según el

criterio institucional, así como los procedimientos a ser aplicados en el control de los datos, de acuerdo al criterio institucional.

Asimismo, como parte de los aspectos a definir como Usuarios, Contraseñas y Definiciones de Grupos a ser Administrados, cabe identificar cuáles son los usuarios que la institución identifica, para que tengan acceso a los datos, así como los grupos de usuarios definidos y que deben tener acceso a los datos.

Y finalmente, definir el acceso de vistas y permisos de accesos a ser administrados, permite monitorear de manera más segura la autenticación del usuario y comportamiento de acceso, la clasificación de la confidencialidad del dato, y definir auditorías.

Capítulo VIII. Estructura

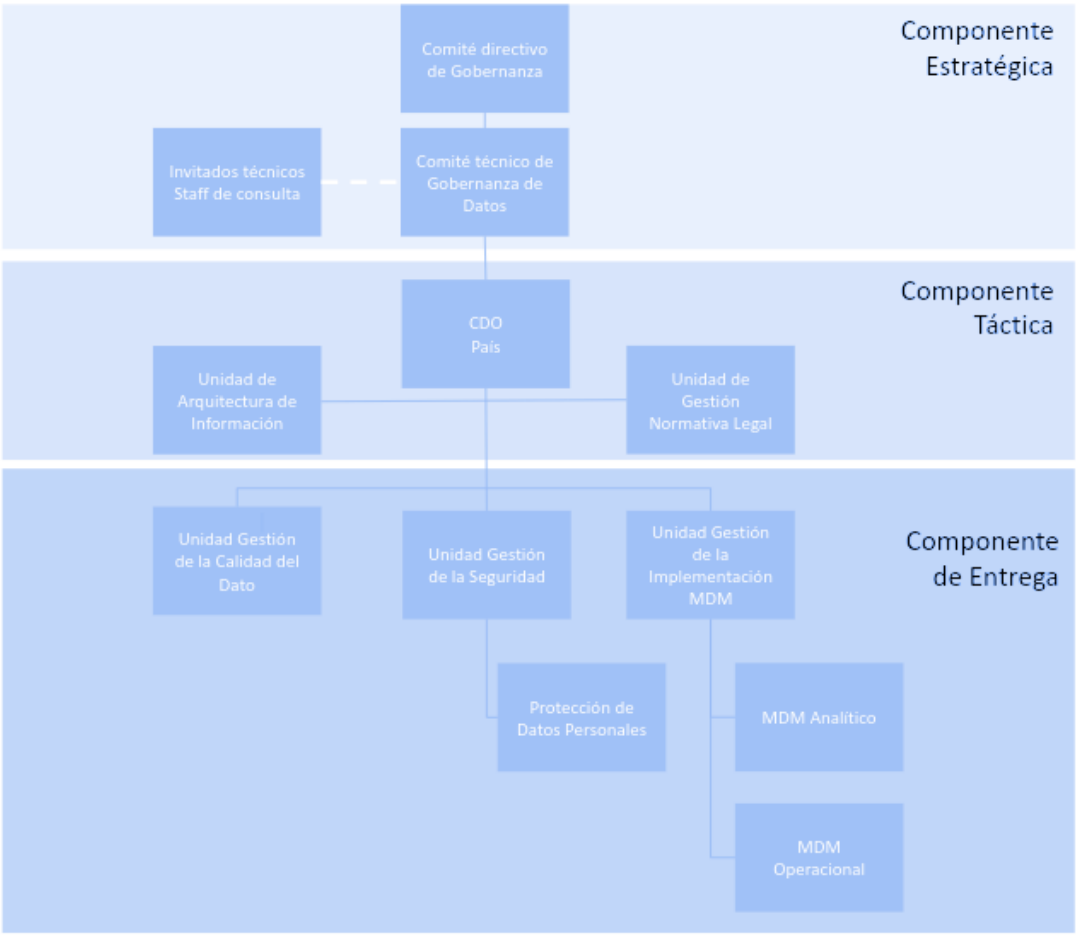

Tabla 2. Estructura de Gobernanza

Capítulo IX. Roles y Responsabilidades

De acuerdo con algunos criterios internacionales[7], en muchas organizaciones, la estrategia de datos es coordinada por el Consejo de Gobierno de Datos, con la orientación del Director General de Información (CIO) y el Director Ejecutivo de Gestión de Datos. En otras organizaciones, estos ejecutivos pueden conservar la propiedad y el control de la estrategia de datos; sin embargo, compartir la propiedad construye una asociación de gestión de datos con interinstitucional. A menudo, el Ejecutivo de Gestión de Datos elabora una estrategia inicial de datos,

[7] DAMA-DMBOK - DAMA Data Management Knowledge System Guide, https://www.dama.org/cpages/body-of-knowledge

incluso antes de que se forme un Consejo de Gobierno de Datos, con el fin de lograr el compromiso de la alta dirección para el establecimiento de la administración de datos y la gobernanza.

En este capítulo se propone[8] la valoración de roles claves en el diseño e implementación de un MGD, algunos de los cuales se mencionan a continuación:

Comité directivo de Gobernanza.

Articular y concretar las políticas y estrategias de Gobierno de datos con los diversos actores involucrados (Estado, Sociedad Civil y Sector Privado), con la finalidad de alcanzar competencias y cooperación para crear valor público mediante el tratamiento de datos y la optimización de los recursos de los involucrados, mediante el uso de tecnologías digitales.

Comité técnico de Gobernanza de Datos

Proponer, diseñar, consensuar los aspectos de detalle de las políticas de Gobierno de datos en colaboración con los actores involucrados, y contribuir en la identificación de las competencias específicas y necesidades de cooperación entre actores involucrados para crear valor público mediante el tratamiento de datos y la optimización de los recursos de los involucrados, mediante la definición y propuestas de tecnologías digitales para el Gobierno de Datos a nivel País.

Invitados técnicos

Contribuir en el diseño de las políticas de Gobierno de datos en aspectos específicos de sus dominios como representantes de instituciones invitadas, en colaboración con los otros actores involucrados. Así como contribuir en la identificación de las competencias específicas propias de su dominio institucional para crear valor público mediante el tratamiento de datos y la optimización de los recursos de los involucrados.

Gestión Normativa Legal

Proponer, diseñar, consensuar e integrar las reglas, lineamientos y normativas existentes o, que se requieran para fortalecer y hacer aplicables las políticas de

[8] Los textos incluidos en esta sección, se integran con fidelidad a la propuesta recibida.

Gobierno de datos que se definan a nivel país. Así como establecer y promover los principios que establecerán los límites éticos en el tratamiento de datos gubernamentales.

Chief Data Officer (CDO) país

Establecer la estrategia de uso de los datos país con la finalidad de alcanzar competencias y cooperación para crear valor público mediante el tratamiento de datos y la optimización de los recursos de los involucrados. Así como establecer las políticas y procedimientos para la gestión de los datos, trabajando de forma transversal con las instituciones del Estado para obtener, preparar, organizar, proteger y analizar los datos, de manera que se puedan utilizar para alcanzar el valor público esperado.

Unidad Arquitectura de Información

Diseñar, consensuar e integrar los modelos de dominio de información y datos desde las distintas instituciones públicas involucradas, velando por identificar y asignar responsabilidades con respecto a la identificación, resguardo y compartición de información propia de cada institución en sus dominios propios y en los dominios utilizados por/desde las otras instituciones.

Velar por una arquitectura de Información/Datos pública que en su diseño, resguarde la protección de datos personales, la transformación de datos públicos en datos abiertos, la mantención de la integridad, disponibilidad, privacidad, control y autenticidad de los datos públicos.

Unidad Gestión de Calidad del Dato

Establecer las políticas y procedimientos a nivel país y/o por dominios institucionales para la limpieza y estandarización/normalización de los datos velando por resolver la falta de completitud, falta de consistencia, datos duplicados, datos incorrectos u obsoletos, falta de integridad referencial, falta de relaciones y dependencias, datos que son redundantes, están huérfanos, o son inconsistente, datos que tienen un formato o un contenido no acorde al estándar definido, datos fueras de los rangos y valores definidos. Esto en coordinación con los respectivos encargados de datos por institución.

Unidad de Gestión de Apertura del Dato

Acompañar a las instituciones en la implementación de los procesos de apertura de datos; y asesorar técnicamente a las distintas instituciones estatales para el diseño de los planes de publicación de datos abiertos y su implementación; Procurar la ejecución de la política, los planes de acción y demás instrumentos que lleven a la disponibilidad y uso de los datos abiertos de carácter público; Monitorear las acciones necesarias para la ejecución de los anteriores; Coordinar con los distintos actores del ecosistema, tanto de la sociedad civil, el sector privado, la academia y el sector público, para la publicación y uso de los datos abiertos; Promover la construcción, publicación, mantenimiento, y ampliación del catálogo de datos abiertos de carácter público; Estudiar, desarrollar o proponer adaptación de estándares para la publicación de datos abiertos de carácter público; Promoción y desarrollo de actividades de capacitación dirigidas a las personas funcionarias y ciudadanía en general, con el fin de transmitir conocimientos, técnicas y metodologías que permitan y faciliten los procesos de la apertura de datos, su uso y reuso.

Unidad Gestión de Seguridad del Dato

Establecer las políticas y procedimientos a nivel país o por dominios institucionales para contribuir mediante normativa, procedimientos y tecnología de ciberseguridad, a mantener la integridad, disponibilidad, privacidad, control y autenticidad de los datos manejados computacionalmente por los servicios públicos, velando por contar con:

- Una estrategia global de seguridad y actualizarla.
- Monitorizar todas las aplicaciones con acceso a datos para detectar las menos seguras y trabajar sobre esos puntos débiles, evitando que se conviertan en una puerta de acceso para los *hackers*.
- Crear controles de acceso específicos para todos los usuarios, limitando su acceso a los sistemas que necesitan para sus tareas exclusivamente y reduciendo así la exposición de los datos sensibles.
- Obtener un registro completo y detallado de lo que ocurre en los sistemas corporativos. Una

decisión que, además de reforzar la seguridad, facilitará la resolución de problemas.

- Asegurarse de que la seguridad del software y del hardware están actualizadas con las nuevas tecnologías antimalware.
- Nombrar a un oficial de seguridad de la información (CISO) para que se haga cargo de la seguridad.
- Formar a las personas usuarias en mejores prácticas de seguridad cibernética para que sepan crear contraseñas seguras, reconocer emails sospechosos de amenaza, evitar aplicaciones peligrosas y prevenir cualquier otro riesgo relevante para la seguridad de la información siguiendo las pautas de la Estrategia Nacional de Ciberseguridad.
- Definir claramente los requisitos y las expectativas de la organización en materia de seguridad, especialmente al practicar contrataciones o al iniciar relaciones con socios y proveedores.
- Determinar una línea de base que incluya los estándares de seguridad aplicables a terceros.
- Monitorizar la actividad usuaria para verificar que sus acciones cumplen con las recomendaciones de seguridad.
- Crear un plan de respuesta a la violación de datos que permita cerrar cualquier vulnerabilidad y limitar el daño que la brecha puede hacer.
- Garantizar el cumplimiento normativo en toda la organización y estar al tanto de los cambios que pudieran producirse en la legislación.
- Realizar evaluaciones de las amenazas y estudiarlas mediante técnicas de análisis que permitan estar mejor protegido.
- No usar diccionarios ni algoritmos de descifrado, que se podrían hackear, sino usar reglas de enmascaramiento fijas o aleatorias.
- Sustituir los encriptados por enmascaramiento o hacer una encriptación centralizada y llevada a cabo por el propio producto.

  Esto en coordinación con los respectivos encargados de seguridad de datos por institución.

- **Protección de Datos Personales**

  Establecer las medidas básicas que garanticen de manera eficiente los niveles de seguridad y privacidad para el tratamiento y Protección de Datos Personales, de tal forma que se eviten posibles adulteraciones, pérdidas, consultas y usos o accesos no autorizados por el propietario de los datos; Velar por el establecimiento de procedimientos que resguarden a las instituciones a la exposición al riesgo legal y reputacional como consecuencia del tratamiento ilegal o inadecuado de información personal; Proteger los derechos del ciudadano respecto del acceso, rectificación, limitación, oposición, supresión (“derecho al olvido”), portabilidad y oposición al tratamiento de decisiones automatizadas con el uso de sus datos personales.

Unidad Gestión Implementación MDM

Proveer un enfoque país, que contribuya a aumentar el valor de la infraestructura de datos institucionales y el análisis de sus datos, así como contribuir a conectar la información, las personas y los procesos para fortalecer el cumplimiento de los objetivos de las instituciones y mejorar la calidad de los datos del Estado.

MDM Analítico: relacionar los datos críticos de cada institución en archivos maestros por dominio (bases de datos federadas), en la búsqueda de obtener puntos de referencia común para los datos más importantes, simplificando el intercambio de datos entre instituciones en el marco de las políticas de interoperabilidad del país.

MDM Operacional: contribuir, a nivel de cada institución, a mantener control sobre cada registro relevante de información en sus sistemas, con la finalidad de contar con una fuente vigente, consistente y completa de los datos relevantes para el normal funcionamiento de la institución y la interoperabilidad de ésta con otras instituciones, manteniendo la consistencia con los sistemas operacionales que son fuente de los datos usados.

Capítulo X. Mecanismos de interacción

El proceso de Gobernanza de Datos debe incluir en sus prácticas, algunas acciones y actividades en distintas áreas de planificación, desarrollo, operación y control. En esa línea se pueden valorar algunos procesos para su integración de la siguiente manera:

Proceso	Tipo
Identificar necesidades del sector	Planificación
Diseño e implementación de Estrategia de datos	Planificación
Articulación de gestión de datos multiactor	Planificación
Identificar y nombrar los actores clave en la administración	Planificación
Diseñar, revisar y recomendar las políticas de datos y procedimientos	Planificación
Revisión y aprobación de arquitectura de datos	Planificación
Planificar y promover proyectos en materia de datos	Planificación
Estimación de datos de valor de activos y costos asociados	Planificación
Soportar y resolver problemas en materia de datos	Control y Seguimiento

Supervisar y garantizar el cumplimiento normativo	Control
Vigilar el cumplimiento de las políticas de datos	Control
Supervisar los proyectos y servicios de gestión de datos	Control
Comunicar y promover el valor, uso y reuso de los datos	Operación

Capítulo XI. Conclusiones y Recomendaciones

De acuerdo con el Barómetro de Datos Abiertos (Web Foundation, 2018) existen tres áreas de política pública que requieren resolverse para habilitar los datos como un activo en el ciclo de política pública y construir una gobernanza alrededor de la política de datos abiertos.

La primera de ellas tiene que ver con la apertura por defecto, a partir de procedimientos claros y estándares que permitan compartir los datos de manera automática y proactiva, es decir sin que medie necesariamente una petición ciudadana de acceso a la información.

La segunda tiene que ver con la infraestructura de datos a partir de la mejora en la calidad e integridad de los datos, así como de su interoperabilidad y vinculación mediante sistemas de gestión adecuados para administrar datos abiertos. La interoperabilidad se relaciona con el uso de estándares para representar datos, lo que significa que los datos relacionados con las mismas cosas pueden reunirse fácilmente.

Y la tercera, supone datos con un propósito, trabajando en estrecha colaboración con las entidades usuarias finales y grupos cívicos para identificar *ex*-ante los desafíos más urgentes que los datos abiertos puedan ayudar a resolver.

En ese sentido, y a fin de fortalecer el texto presentado, sugerimos una serie de recomendaciones desde la experiencia, para un mejor abordaje y así avanzar en el diseño de un MGD-CR más robusto y a la vanguardia de las mejores prácticas en la materia.

1. Resaltar al órgano contralor la necesidad e importancia de contar con mayores tiempos para el diseño e implementación del modelo, acordes con la realidad nacional.

2. El proceso de diseño del modelo de gobernanza de datos, debe partir de la elaboración de un estado de la cuestión en Costa Rica: esta supone una etapa fundamental en la construcción de cualquier instrumento, no obstante dados los tiempos establecidos y los recursos con que se ha contado, resulta necesario someterlo como recomendación inherente a la construcción del modelo.
3. Como país adherido a estándares internacionales de gobierno abierto y con una normativa que privilegia la participación de sectores involucrados, se debe continuar con una construcción que contemple más canales de participación, co-diseño y consulta multisectorial: si bien la CNDA ha convenido sobre la necesidad de avanzar en la apertura de tales canales, la pandemia por la COVID- 19 entre el 2020 y el 2021, seguida por el inicio del período electoral y transición de administración, afectaron en gran medida cualquier acción en esa línea.
4. Someter a revisión de pares expertos: como cualquier instrumento que contenga aspectos técnicos, resulta una buena práctica someter el texto a revisión de actores internos y externos especializados a fin de obtener realimentación de la propuesta.
5. Consultar con más organismos internacionales que desarrollan procesos de gobernanza de datos y brindan asesoría técnica en esta área: existen algunos organismos internacionales identificados que han realizado importantes aportes para la generación de un marco regional de gobernanza de datos, por lo que una vez teniendo un margen de maniobra mayor, se sugiere contrastar la propuesta recibida, generar la consulta sobre lo realizado y obtener las recomendaciones al caso.
6. Fortalecer la implementación mediante mesas de trabajo: para el proceso de diseño y construcción, la CNDA ha identificado actores clave que deberían participar en el proceso, por lo que una vez inicie la administración 2022-2026 se sugiere retomar la ruta propuesta con tales actores de manera progresiva.
7. Contemplar el hecho de que, siendo el modelo de gobernanza de datos del país, un instrumento que requiere amplios conocimientos técnicos, un proceso de investigación, actividades de co-diseño y consulta y otros que aseguren su confiabilidad y solidez, debe preverse la asignación de recursos económicos y humanos, así como los espacios en la planificación

de las instituciones o entes que asuman el proceso de diseño y su posterior implementación.

Bibliografía

Cetina, C. (2021, July 22). Gobernanza de datos y capacidades estatales para la post pandemia. Caracas: CAF. Recuperado desde: http://scioteca.caf.com/handle/123456789/1765

DAMA-DMBOK. (2009). Guía de Fundamentos para la Gestión de Datos. DAMA International. ISBN 9780977140084.

Fumega, Silvana; Scrollini, Fabrizio; Zapata, Enrique (2021) ¿Cuán abiertos están los datos públicos? El barómetro de datos abiertos de América Latina y el Caribe 2020. Caracas: CAF. Recuperado desde: https://scioteca.caf.com/handle/123456789/1710

GPAI (2020). Data Governance Working Group A Framework Paper for GPAI's work on Data Governance. Disponible en: https://gpai.ai/projects/data-governance/gpai-data-governance-wg-report-november-2020.pdf

Méndez, S. F. (2021). Marco Metodológico y cómo implementar un gobierno de datos. Acompañamiento técnico, Comisión Económica para América Latina y el Caribe. Santiago, Chile.

OECD (2019), The Path to Becoming a Data-Driven Public Sector, OECD Digital Government Studies, OECD Publishing, Paris, https://doi.org/10.1787/059814a7-en.

OECD. (2020). Open, Useful and Re-usable data (OURdata) Index: 2019 - Policy Paper, March 2020 - Jacob Arturo Rivera Perez, Cecilia Emilsson & Barbara Ubaldi, OECD Digital Government Studies, OECD Publishing, Paris. http://www.oecd.org/governance/digital-government/our-data-index-policy-paper-2020.pdf

Web Foundation (2018). Barómetro de los Datos Abiertos - Edición de los Líderes. Washington DC: World Wide Web Foundation