GUATEMALA
GUATEMALA NO SE DETIENE

Red Ciudadana

INTRODUCCIÓN A MODELOS DE GOBERNANZA DE DATOS

Resumen Ejecutivo

En la era digital actual, la gobernanza de datos se ha convertido en un elemento fundamental para garantizar la protección de la privacidad, la seguridad de la información y el uso ético y efectivo de los datos. Este documento examina las políticas y leyes de protección de datos a nivel internacional, destacando las mejores prácticas y los desafíos en la implementación de regulaciones efectivas.

En el desarrollo del producto se mencionan países con mayores prácticas de gobernanza, se menciona Singapur, Austria, Alemania, Finlandia, Japón, Reino Unido y Estonia. La Unión Europea se destaca por su enfoque integral hacia la protección de datos personales, establecido en el Reglamento General de Protección de Datos (GDPR). El GDPR ha establecido un nuevo estándar en la protección de datos, enfatizando el consentimiento explícito, los derechos de los individuos y la responsabilidad de las organizaciones en el tratamiento de datos personales. Este enfoque ha inspirado a otras jurisdicciones a revisar y fortalecer sus propias legislaciones de protección de datos.

En contraste, Estados Unidos adopta un enfoque más sectorial, con leyes específicas como la HealthInsurancePortability and AccountabilityAct (HIPAA) y la Children's Online PrivacyProtectionAct (COPPA). A nivel estatal, la California ConsumerPrivacyAct (CCPA) se destaca por otorgar a los consumidores derechos comparables a los del GDPR, como el derecho a saber qué información personal se recopila y a optar por no participar en la venta de esa información.

En América Latina, el manejo de la gobernanza de datos ha tomado distintos enfoques en países como Uruguay, Chile, Colombia, Brasil y México, reflejando un creciente reconocimiento de la importancia de la protección de datos personales y la promoción de la transparencia. Uruguay, pionero en la región, cuenta con una legislación robusta desde 2008, la Ley de Protección de Datos Personales, que establece un marco sólido para el manejo de datos y la privacidad. Chile, por su parte, ha fortalecido su marco legislativo con la creación de una agencia de protección de datos y está en proceso de adecuar su legislación a estándares internacionales como el GDPR. Cada uno de estos países, a pesar de sus distintos niveles de desarrollo económico y tecnológico, ha reconocido la necesidad crítica de regular la gobernanza de datos para proteger los derechos de los ciudadanos y fomentar un entorno digital seguro y confiable.

El análisis de estas legislaciones revela un panorama diverso en cuanto a la protección de datos personales. Aunque el GDPR ha influenciado significativamente el desarrollo de leyes en otras regiones, la implementación y el alcance de estas regulaciones varían ampliamente. Los desafíos incluyen la armonización de las leyes a nivel internacional, la adaptación a la evolución tecnológica y el equilibrio entre la protección de la privacidad y la promoción de la innovación.

Este documento subraya la importancia de una gobernanza de datos efectiva y responsable para proteger los derechos de los individuos y fomentar un entorno digital seguro y transparente. A medida que avanzamos hacia un futuro cada vez más orientado a los datos, la cooperación internacional y el intercambio de mejores prácticas serán esenciales para

desarrollar marcos regulatorios que protejan los derechos de los individuos y promuevan el crecimiento económico y la innovación.

Glosario de términos

A continuación, se presenta una lista de términos esenciales con sus definiciones:

- Gobernanza de Datos: Conjunto de procesos, políticas, normas y métricas que aseguran el uso efectivo y eficiente de la información en una organización para alcanzar sus objetivos.

- Calidad de Datos: Se refiere a la condición de los datos basada en factores como su precisión, consistencia, integridad y actualización.

- Estándares abiertos: son especificaciones técnicas diseñadas para ser utilizadas públicamente y accesibles sin restricciones. Facilitan la interoperabilidad y la compatibilidad entre diferentes sistemas y productos tecnológicos, permitiendo que trabajen juntos de manera eficiente y efectiva.

- Interoperabilidad: Capacidad de distintos sistemas, entornos, aplicaciones o productos de trabajar juntos sin interrupciones ni esfuerzos adicionales por parte del usuario.

- Privacidad de Datos: Derecho de los individuos a controlar o influir en qué información relacionada con ellos puede ser recopilada y almacenada y por quién, y a quién puede ser divulgada.

- Seguridad de Datos: Protección de datos contra accesos no autorizados, alteraciones, divulgación o destrucción para garantizar la integridad, confidencialidad y disponibilidad de los datos.

- Cumplimiento Regulatorio: Adecuación de una organización a las leyes y regulaciones relevantes en materia de protección y gestión de datos.

- Anonimización de Datos: Proceso por el cual los datos personales se modifican de tal manera que ya no se pueden asociar con un individuo específico sin el uso de información adicional.

- Datos Abiertos: Datos que están disponibles para el público de manera gratuita, para ser utilizados y compartidos por cualquiera.

- Chief Data Officer (CDO): Ejecutivo responsable de la gestión de datos y la política de datos en una organización. El CDO supervisa la estrategia de datos, la calidad de los datos, la protección de datos y el ciclo de vida de los datos.

- Consentimiento Informado: Acuerdo explícito de un individuo, basado en el conocimiento de qué datos personales serán recopilados y cómo se utilizarán, para permitir el tratamiento de sus datos personales.

Abreviaturas y Siglas sobre Gobernanza de Datos

- GDPR: General Data ProtectionRegulation (Reglamento General de Protección de Datos) - Legislación de la Unión Europea que regula la protección de datos personales.
- DPO: Data ProtectionOfficer (Delegado de Protección de Datos) - Persona designada para supervisar el cumplimiento del GDPR y otras leyes de protección de datos en una organización.
- CDO: Chief Data Officer (Director de Datos) - Ejecutivo responsable de la gestión de datos y políticas de datos en una organización.
- CCPA: California ConsumerPrivacyAct (Ley de Privacidad del Consumidor de California) - Ley estatal de EE.UU. que regula la privacidad de datos personales de los residentes de California.
- PII: PersonallyIdentifiableInformation (Información Personal Identificable) - Cualquier dato que pueda usarse para identificar a una persona específica.
- LGPD: LeiGeral de Proteção de Dados (Ley General de Protección de Datos Personales) - Ley brasileña similar al GDPR que regula la protección de datos personales.
- FOIA: FreedomofInformationAct (Ley de Libertad de Información) - Ley de EE.UU. que proporciona acceso público a la información del gobierno federal.
- ISO: International OrganizationforStandardization (Organización Internacional de Normalización) - Organismo internacional que desarrolla y publica estándares internacionales, incluidos los relacionados con la seguridad y gestión de datos.
- NIST: NationalInstituteofStandards and Technology (Instituto Nacional de Estándares y Tecnología) - Agencia del Departamento de Comercio de EE.UU. que desarrolla estándares y guías relacionadas con la tecnología y la seguridad de datos.
- HIPAA: HealthInsurancePortability and AccountabilityAct (Ley de Portabilidad y Responsabilidad del Seguro Médico) - Legislación de EE.UU. que protege la privacidad y seguridad de la información de salud.
- AI: Artificial Intelligence (Inteligencia Artificial) - Tecnología y disciplina que se enfoca en crear sistemas capaces de realizar tareas que normalmente requieren inteligencia humana.
- API: ApplicationProgrammingInterface (Interfaz de Programación de Aplicaciones) - Conjunto de definiciones y protocolos para construir e integrar software de aplicaciones.

Tabla de contenido

Contenido

Marco de Referencia de la Consultoría

1.1 Contexto de la consultoría

La iniciativa "Guatemala no se Detiene" representa un ambicioso esfuerzo colaborativo entre el sector público y el privado, orientado a impulsar el desarrollo económico y social de Guatemala a través de la generación de empleo y la atracción de inversión extranjera. Este proyecto se basa en un entendimiento compartido de los desafíos y oportunidades que enfrenta el país en el contexto global actual, donde la competitividad y la innovación son fundamentales para el crecimiento sostenible.

1.2 Objeto y alcances

A continuación, se detallan los objetivos y alcances de la consultoría, delineando las metas específicas y el marco de acción propuesto para alcanzar estos ambiciosos objetivos.

1. Generación de un Sector Público Atento y Eficiente: El primer objetivo específico de la consultoría implica la transformación del sector público para que este se vuelva más receptivo a las necesidades de la población y del entorno empresarial.
2. Creación de un Ambiente de Negocios Atractivo: En estrecha relación con el primer objetivo, la consultoría busca promover un ambiente de negocios más atractivo para inversores tanto nacionales como internacionales.

1.3 Productos de la consultoría

1.3.1 Desarrollo de Modelos de Gobernanza de Datos

Un componente crucial para lograr los objetivos mencionados es el desarrollo de modelos avanzados de gobernanza de datos. Esto implica la creación de políticas y marcos regulatorios que aseguren la gestión eficaz, segura y ética de los datos, facilitando la interoperabilidad entre distintas plataformas y entidades gubernamentales. La gobernanza de datos efectiva es fundamental para la digitalización de servicios y la creación de un gobierno más abierto y transparente.

Introducción

En un mundo cada vez más impulsado por datos, la gobernanza de estos se ha convertido en una cuestión fundamental. Los datos, abarcando desde la información personal hasta grandes conjuntos de datos económicos y medioambientales, son ahora una fuente crítica de poder y conocimiento. Este documentoexamina los modelos de gobernanza de datos, con un enfoque particular en las mejores prácticas internacionales y cómo estos pueden ser adaptados y aplicados en el contexto de Guatemala.

La gobernanza de datos se refiere a los procesos y políticas mediante los cuales los datos son adquiridos, gestionados, compartidos y utilizados. Es un campo que se extiende más allá del mero manejo de datos; implica considerar aspectos éticos, legales y sociales relacionados con los datos. En una era donde los datos son omnipresentes y su impacto en la sociedad es profundo, una gobernanza de datos efectiva es crucial para garantizar que se maximicen sus beneficios mientras se minimizan los riesgos asociados, como la violación de la privacidad o el mal uso de la información.

En la última década, la importancia de los datos ha escalado a las cimas de las agendas políticas globales. Esto se debe a la creciente conciencia de que los datos son un recurso clave para el desarrollo económico, la gestión de crisis como la pandemia de COVID-19, y la respuesta a los desafíos sociales y ambientales. Sin embargo, el progreso hacia una gobernanza efectiva de los datos y la realización de su valor público sigue siendo desigual entre países y regiones. Mientras que algunos países han avanzado significativamente, implementando leyes de protección de datos y políticas de datos abiertos, otros aún se encuentran en las etapas iniciales de desarrollo de estas capacidades.

En este contexto, el Barómetro Global de Datos emerge como una herramienta valiosa, proporcionando comparaciones críticas y análisis que pueden ayudar a los países a impulsar acciones para aprovechar las oportunidades que ofrece la "revolución de los datos" y mitigar sus riesgos. El Barómetro no solo evalúa a los países según el estado de sus datos sino que también apoya el aprendizaje colectivo sobre qué funciona y cómo intervenir efectivamente en la gestión de datos.

A pesar de los avances significativos en algunas áreas,existen desafios globales que persisten. Por ejemplo, muchas leyes de protección de datos carecen de mecanismos de rectificación eficaces, dejando a las personas y comunidades con limitado control sobre sus propios datos. Además, las políticas y prácticas de datos a menudo no abordan completamente problemas emergentes como la toma de decisiones algorítmica o los datos de ubicación. En áreas críticas como la acción climática, las brechas de datos pueden frustrar los esfuerzos locales para proteger los ecosistemas y responder a la vulnerabilidad climática.

Este documento busca proporcionar una base de conocimiento y recomendaciones para Guatemala, aprovechando las lecciones aprendidas y las mejores prácticas a nivel global. El objetivo es explorar cómo Guatemala puede desarrollar un marco de gobernanza de datos robusto y adaptado a sus necesidades específicas, que permita capitalizar los beneficios de los datos mientras se protegen los derechos y se promueve el bienestar general.

Marco Conceptual de la Introducción a Modelos de Gobernanza de Datos

La gobernanza de datos ha emergido como un campo crítico en la era de la información, donde la gestión eficaz de los datos es fundamental para el éxito organizacional y la integridad de la información. La adopción de modelos de gobernanza de datos efectivos permite a las organizaciones maximizar el valor de sus datos, asegurando al mismo tiempo su uso ético y la protección de la privacidad de los usuarios (DAMA International, 2017). En este contexto, la gobernanza de datos se define como el ejercicio de autoridad, control y toma de decisiones compartida (gobierno) sobre la gestión de los recursos de datos (Weber, Otto, &Österle, 2009).

Imagen 1. Recuperado de https://pensertrust.com/diseno-de-modelo-de-gobierno-de-datos/

El principio fundamental de la gobernanza de datos es garantizar que los datos, considerados un activo estratégico, sean gestionados de manera efectiva a lo largo de toda la organización. Esto incluye la calidad de los datos, la metadata, la seguridad, la privacidad, y el cumplimiento normativo, así como el manejo de los datos a lo largo de su ciclo de vida (Khatri& Brown, 2010). La transparencia en la toma de decisiones, la integridad y la precisión de los datos, y el cumplimiento con las regulaciones vigentes son piedras angulares en la gobernanza de datos.

Para implementar una gobernanza de datos efectiva, las organizaciones deben establecer estructuras específicas que involucren la creación de un consejo de gobernanza de datos, la designación de administradores de datos (data stewards), y la definición clara de los roles y responsabilidades de los propietarios de los datos (Otto, 2011). Estas estructuras son esenciales para desarrollar y mantener políticas, procedimientos, estándares, y guías que aseguren la gestión adecuada de los datos a lo largo de la organización.

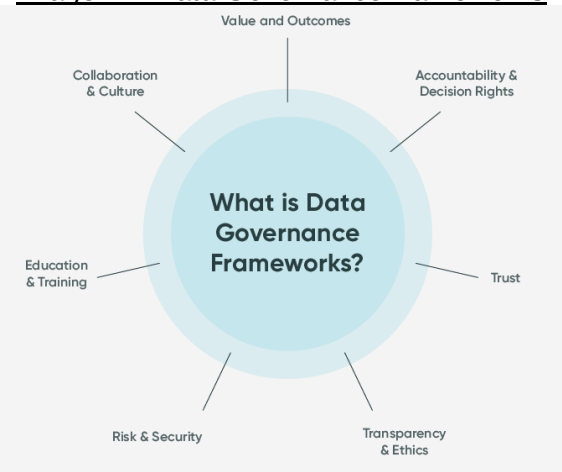
Sin embargo, implementar un modelo de gobernanza de datos efectivo presenta varios desafíos. La resistencia al cambio, las complejidades regulatorias, la garantía de la calidad de los datos en sistemas dispersos y la protección de los datos contra amenazas de seguridad son obstáculos comunes (Tallon, 2013). Además, en un contexto globalizado, la variabilidad de las legislaciones sobre la protección de datos y privacidad entre países añade una capa adicional de complejidad a la gobernanza de datos, especialmente para organizaciones que operan en múltiples jurisdicciones.

La relevancia de una gobernanza de datos efectiva no se limita a las corporaciones o al sector tecnológico; también es crítica para los gobiernos y las organizaciones internacionales. En países en desarrollo como Guatemala, la implementación de modelos de gobernanza de datos puede ofrecer una oportunidad significativa para mejorar la transparencia gubernamental, fomentar la participación ciudadana eimpulsar el desarrollo económico y social (Bertot, Jaeger,

&Grimes, 2010 Mediantela adopción de mejores prácticas internacionales y la colaboración con países y organizaciones que han establecido marcos de gobernanza de datos exitosos, Guatemala podría acelerar su proceso de transformación digital y fortalecer su capacidad para gestionar datos de manera efectiva y ética.

La colaboración internacional y el aprendizaje de modelos de gobernanza de datos exitosos en otros países son esenciales para adaptar y aplicar prácticas de gobernanza de datos en el contexto específico de Guatemala. La experiencia de la Unión Europea con el Reglamento General de Protección de Datos (GDPR) ofrece valiosas lecciones sobre la protección de la privacidad de los datos y el cumplimiento normativo (Voigt&VondemBussche, 2017). Asimismo, la iniciativa de datos abiertos de Singapur proporciona un ejemplo de cómo la transparencia y la accesibilidad de los datos pueden fomentar la innovación y el desarrollo económico (Kankanhalli, Charalabidis, &Mellouli, 2019).

Imagen 2. Data GovernanceFrameworks



En conclusión, la gobernanza de datos es un campo crítico que requiere atención cuidadosa y estratégica para maximizar el valor de los datos y asegurar su uso ético y seguro. A medida que Guatemala busca implementar modelos de gobernanza de datos, es esencial considerar las lecciones aprendidas de otras jurisdicciones, adaptándolas a sus necesidades específicas y desafíos. La colaboración con organizaciones internacionales y países con marcos de gobernanza de datos establecidos puede proporcionar guías valiosas y apoyo en este esfuerzo. Al comprometerse con estos principios y desafíos, Guatemala puede avanzar hacia una gestión de datos más efectiva, transparente y segura, lo que a su vez puede impulsar el desarrollo económico y social del país.

La gobernanza de datos es un aspecto crucial de la gestión moderna, que implica no sólo la eficiencia en el manejo de la información sino también consideraciones éticas, legales y de privacidad. A nivel global, hay una creciente tendencia hacia la adopción de prácticas robustas en la gobernanza de datos, impulsada por la necesidad de manejar efectivamente los enormes volúmenes de datos generados en la era digital. Este segmento analiza las mejores prácticas internacionales en la gobernanza de datos, ofreciendo un panorama de cómo diferentes países han abordado este desafío.

Tabla 1. Síntesis de las Mejores Prácticas Internacionales en Gobernanza de Datos. Elaboración propia.

País/ Región	Mejores Prácticas en Gobernanza de Datos	Aplicación/Descripción
Unión Europea (UE)	Protección de Datos y Privacidad	ZGDPR - Regulación integral para proteger datos personales y la privacidad.
Estonia	Gobierno Digital y Transparencia	Sistema de gobierno electrónico que facilita la transparencia y eficiencia.
Australia	Datos Abiertos y Accesibilidad	Políticas de datos abiertos para mejorar la transparencia y participación.
Reino Unido	Ética en la Gestión de Datos	Creación de comités y marcos para abordar cuestiones éticas en datos.
Israel	Seguridad de Datos y Gestión de Riesgos	Medidas de seguridad avanzadas y estrategias de gestión de riesgos de datos.
Alemania	Capacitación en Datos y Desarrollo de Habilidades	Programas de educación y capacitación en análisis y ética de datos.
OCDE	Directrices y Marcos Globales	Proporciona marcos y directrices para prácticas éticas y seguras de datos.
Japón	Innovación en Gobernanza de Datos	Enfoque en la integración de IA y tecnologías avanzadas en la gestión de datos.
Finlandia	Interoperabilidad y Estándares Abiertos	Sistemas y prácticas que promueven la interoperabilidad de los datos.

Transparencia y Protección de la Privacidad

En el contexto de la era digital, dos conceptos que frecuentemente se encuentran en una delicada balanza son la transparencia y la protección de la privacidad. La transparencia, en el ámbito de la gestión de datos y la gobernanza, se refiere a la apertura y accesibilidad de la información, permitiendo a los usuarios entender cómo se recolectan, procesan y utilizan sus

datos. Por otro lado, la protección de la privacidad se concentra en garantizar la seguridad de los datos personales de los usuarios, asegurando que su información se maneje de manera confidencial y con el debido respeto a su autonomía personal.

La transparencia es fundamental para construir la confianza entre las entidades que manejan datos (ya sean empresas, gobiernos o instituciones) y los individuos cuyos datos se están procesando. Al ser transparentes sobre las políticas de datos, los procedimientos de recolección de datos, y los mecanismos de seguridad implementados para proteger esos datos, las organizaciones pueden demostrar su compromiso con la ética y la responsabilidad. Este nivel de apertura es crucial para empoderar a los usuarios, dándoles la capacidad de tomar decisiones informadas sobre si desean interactuar con ciertos servicios, cómo desean que se manejen sus datos y qué información están dispuestos a compartir (Birkinshaw, 2010).

Sin embargo, la transparencia no debe comprometer la privacidad. La protección de la privacidad es un derecho fundamental que se ha vuelto cada vez más prominente a medida que nuestras vidas se digitalizan. Las leyes de protección de datos, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, han establecido un precedente global, enfatizando la importancia de manejar los datos personales de manera que respete la privacidad y la autonomía de los individuos (Albrecht, 2016). Estas regulaciones requieren que las organizaciones no solo protejan la información personal contra el acceso no autorizado y las violaciones de datos, sino que también aseguren que la recolección y el uso de datos se realicen con el consentimiento explícito de los usuarios.

El equilibrio entre transparencia y protección de la privacidad implica una cuidadosa consideración de cómo se comunican y se implementan las prácticas de manejo de datos. Por un lado, debe haber una clara divulgación de las prácticas de recolección y uso de datos. Por otro lado, debe haber garantías sólidas que protejan esa información contra el mal uso. Implementar prácticas como la minimización de datos, donde solo se recolecta la información estrictamente necesaria para el propósito declarado, y la pseudonimización, que oculta la identidad de los usuarios, puede ayudar a lograr este equilibrio[1] (Cavoukian, 2009).

Además, el derecho a ser olvidado, que permite a los individuos solicitar la eliminación de sus datos personales de los registros de una organización, es otro ejemplo de cómo se puede proteger la privacidad en un marco de transparencia. Esta medida no solo refuerza el control de los usuarios sobre sus datos, sino que también promueve una cultura de responsabilidad y respeto por la privacidad dentro de las organizaciones (Rosen, 2012).

En resumen, la transparencia y la protección de la privacidad son dos pilares fundamentales en la era de la información. Su coexistencia armoniosa es esencial para fomentar un entorno digital que respete y proteja los derechos de los usuarios mientras promueve la apertura y la accesibilidad de la información. Las organizaciones deben esforzarse por mantener este equilibrio, implementando políticas y prácticas que aseguren la transparencia en sus operaciones de manejo de datos y adoptando medidas robustas para proteger la privacidad de los individuos. Al hacerlo, pueden construir una relación de confianza con los usuarios, lo cual es indispensableen el panorama digital actual.

El marco de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) para la gobernanza de datos se centra en establecer principios y directrices para manejar eficientemente los datos, especialmente en el contexto de las políticas públicas. Este marco aborda varios aspectos clave:

Transparencia y Accesibilidad:
- Promoción de la transparencia en el uso y gestión de datos.
- Facilitar el acceso a datos para ciudadanos y partes interesadas.

Integridad y Calidad de los Datos:
- Asegurar la integridad y precisión de los datos recopilados y utilizados.
- Implementar procesos para mantener la calidad y fiabilidad de los datos.

Protección de Datos y Privacidad:
- Establecer normas para la protección de datos personales y la privacidad.
- Balancear el acceso a datos y la protección de información sensible.

Uso Responsable de los Datos:
- Fomentar un uso ético y responsable de los datos.
- Implementar políticas para evitar el uso indebido de datos.

Gobernanza y Marco Institucional:
- Desarrollo de un marco institucional claro para la gobernanza de datos.
- Definir roles y responsabilidades en la gestión de datos.

Participación de Stakeholders:
- Involucrar a todas las partes interesadas en el proceso de gobernanza de datos.
- Promover la colaboración entre sectores públicos, privados y la sociedad civil.

Innovación y Apertura:
- Estimular la innovación a través del uso abierto y compartido de datos.
- Apoyar la investigación y el desarrollo basados en datos.

Capacitación y Competencias:
- Desarrollar habilidades y competencias en gestión de datos en el sector público.
- Capacitar a los empleados en aspectos relacionados con la protección de datos y la analítica de datos.

Este modelo de gobernanza de datos propuesto por la OCDE enfatiza la importancia de una gestión de datos equilibrada que sirva tanto a los objetivos de políticas públicas como a los derechos e intereses de los individuos. La implementación de este marco puede ayudar a los países a mejorar su manejo de datos, fomentando la eficiencia, la transparencia y la confianza pública.

Oficina de Datos (Chief Data Officer, CDO)

El papel del Director de Datos (Chief Data Officer, CDO) se ha vuelto cada vez más crucial en los gobiernos de los países de la OCDE como un medio para dirigir y coordinar políticas nacionales de datos. El CDO es una figura política clave que impulsa esfuerzos significativos en el avance de la gestión de datos, jugando un rol esencial en la mejora de las políticas públicas y los servicios para la ciudadanía. A continuación, se detallan las tareas y el ámbito de la gobernanza de datos asociados a este rol.

Tareas del CDO

1. Fortalecer la Capacidad de Proceso y Análisis de Datos:
    a. Mejorar el conocimiento de la relación entre el Estado y la ciudadanía.
    b. Contribuir a un Estado más inteligente, transparente y amigable.
2. Identificación de Brechas de Datos en el Sector Público:
    a. Trabajar con diversas entidades para identificar y abordar carencias en la recopilación y uso de datos.
3. Impulsar la Interoperabilidad de Datos:
    a. Fomentar la cooperación en el manejo de datos entre servicios públicos, y entre el sector público y privado (incluyendo la academia).
    b. Promover la interoperabilidad de datos a nivel nacional e internacional.
4. Desarrollo de Estrategias para la Recolección de Datos Estratégicos:
    a. Crear y ejecutar planes para la recopilación eficaz de datos clave para políticas públicas.
5. Implementación de Estrategias para la Gobernanza e Interoperabilidad de Datos Públicos:
    a. Desarrollar y aplicar políticas para mejorar la gestión y el acceso a datos públicos.

Ámbito de la Gobernanza de Datos

1. Datos para Fines Públicos (Leyes y Trámites):
    a. Asegurar que los datos se utilicen para mejorar la formulación y aplicación de leyes y trámites.
2. Disponibilidad de Datos Abiertos:
    a. Facilitar el acceso a datos gubernamentales de manera abierta y transparente.
3. Uso de Algoritmos (IA) para Fines Públicos:
    a. Integrar la inteligencia artificial en la gestión de datos para mejorar los servicios y políticas públicas.
4. Generación de Guías Generales para la Gobernanza y Gestión de Datos:
    a. Crear directrices para orientar la recolección, análisis y uso de datos en el sector público.
5. Soporte Tecnológico para la Generación de Datos del Sector Público:
    a. Brindar asistencia tecnológica para mejorar la capacidad de generación de datos del gobierno.
6. Colaboración en la Articulación y Uso Compartido de Datos:
    a. Promover la colaboración entre diferentes sectores para el intercambio y análisis conjunto de datos.

El CDO juega un papel transformador en la manera en que los gobiernos manejan y utilizan los datos. Al liderar estas iniciativas, el CDO no solo mejora la eficiencia del gobierno, sino que también impulsa la innovación, la transparencia y una mayor eficacia en la prestación de servicios públicos.

Instrumentos legales para la Gobernanza de Datos

En un mundo cada vez más digitalizado, la gobernanza de datos se ha convertido en un pilar fundamental para asegurar la efectividad, eficiencia y ética en el manejo de la información. Los instrumentos de política para la gobernanza de datos se diseñan no sólo para proteger la privacidad de los individuos y asegurar la seguridad de los datos, sino también para fomentar la innovación y el crecimiento económico mediante el uso estratégico de los datos. Este documento explora diversos instrumentos de política a nivel internacional, destacando tipos de legislación, aspectos relevantes y proporcionando referencias para una exploración más profunda.

Tabla 2. Leyes relacionadas a la Gobernanza de Datos. Elaboración propia

País/Región	Nombre de la Ley	Aspectos Clave	Enlace Oficial
Unión Europea	Reglamento General de Protección de Datos (GDPR)	Consentimiento explícito Derechos de los sujetos de datos Transferencias internacionales	GDPR
Estados Unidos	Ley de Privacidad del Consumidor de California (CCPA)	Derecho a saber Derecho a optar por no participar Protecciones para menores	CCPA
Brasil	Ley General de Protección de Datos (LGPD)	Principios similares al GDPR Consentimiento Derechos de acceso y eliminación	LGPD
Costa Rica	Ley de Protección de la Vida Privada de las Personas frente al Tratamiento de sus Datos Personales, Ley N° 8968	principios clave como el consentimiento informado, la finalidad específica del uso de datos y medidas de seguridad obligatorias, además de la creación de la Agencia de Protección de Datos de los Habitantes (PRODHAB) como ente regulador.	LPVP
Singapur	Ley de Protección de Datos Personales (PDPA)	Consentimiento para el procesamiento Protección de datos Políticas de privacidad	PDPA

La Unión Europea ha liderado el camino con el Reglamento General de Protección de Datos (GDPR), que se ha convertido en un referente global en materia de privacidad y protección de

datos. El GDPR establece requisitos rigurosos para el tratamiento de datos personales, incluyendo el consentimiento explícito, la protección de datos desde el diseño, el derecho al olvido, y sanciones significativas para el incumplimiento. Este reglamento ha inspirado a países fuera de la UE a revisar y fortalecer sus propias legislaciones de protección de datos (EuropeanParliament and Council, 2016).

En la implementación de marcos normativos como el GDPR, países como España y Alemania adaptan directrices de la UE a contextos nacionales, enfrentando retos únicos en sus procesos de ajuste. España, por ejemplo, está trabajando activamente para superar desafíos en su iniciativa de Datos Abiertos, según el INE, lo que incluye mejorar la interoperabilidad y la calidad de los datos para cumplir con las expectativas de transparencia y accesibilidad.

En contraste, en Estados Unidos, la protección de datos se maneja a través de un enfoque sectorial, con leyes como la HealthInsurancePortability and AccountabilityAct (HIPAA) para la protección de datos de salud y la Children's Online PrivacyProtectionAct (COPPA) para la protección de la privacidad de los niños en línea. A nivel estatal, la California ConsumerPrivacyAct (CCPA) se destaca por otorgar a los consumidores derechos comparables a los del GDPR, como el derecho a solicitar la eliminación de sus datos personales y a optar por no participar en la venta de sus datos (Stateof California DepartmentofJustice, n.d.).

Brasil ha seguido un camino similar al de la UE con la promulgación de la LeiGeral de Proteção de Dados (LGPD), que comparte muchas similitudes con el GDPR, pero está adaptada al contexto brasileño. La LGPD refleja un compromiso creciente en América Latina hacia la protección de datos y la privacidad, marcando un paso importante hacia la armonización de las normas de protección de datos en la región (Presidência da República, 2018).

Más allá de la protección de datos personales, la gobernanza de datos también abarca la interoperabilidad y el intercambio de datos entre entidades. La Unión Europea ha implementado el Marco Europeo de Interoperabilidad (EIF) para facilitar la cooperación transfronteriza entre servicios públicos, promoviendo el uso de estándares abiertos y fomentando la disponibilidad de datos abiertos (EuropeanCommission, n.d.).

Estos instrumentos de política subrayan la importancia de una gobernanza de datos efectiva y responsable, equilibrando la necesidad de proteger la privacidad y seguridad de los datos con el potencial de los datos para impulsar la innovación y el desarrollo económico. A medida que la digitalización continúa avanzando, la adaptación y actualización constantes de estas políticas serán cruciales para abordar nuevos desafíos y aprovechar nuevas oportunidades.

La gobernanza de datos representa un campo dinámico en el que legisladores, empresas y la sociedad civil deben colaborar para crear un entorno que promueva tanto la seguridad como la libertad de información. A medida que avanzamos hacia un futuro cada vez más orientado a los datos, la construcción de marcos normativos sólidos y flexibles será esencial para garantizar que la revolución de los datos beneficie a todos.

Análisis de Políticas y Leyes de Protección de Datos a Nivel Internacional

Este documento explora las políticas y leyes de protección de datos a nivel internacional, destacando los tipos de legislación y sus aspectos más relevantes. A través de un análisis

comparativo, se examinan las diferentes aproximaciones adoptadas por jurisdicciones clave para abordar los desafíos en la protección de datos personales.

Al comparar las políticas y leyes de protección de datos a nivel internacional, es evidente que existen variaciones significativas en la comprehensividad y enfoque. Por ejemplo, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea es considerado uno de los marcos más completos y rigurosos. El GDPR destaca por su enfoque exhaustivo en los derechos de los sujetos de datos, incluyendo derechos avanzados como el de acceso, rectificación, supresión (el derecho al olvido), y la portabilidad de datos.

Por contraste, Estados Unidos adopta un enfoque más sectorial y menos uniforme. Aunque la California ConsumerPrivacyAct (CCPA) introdujo derechos comparables a los del GDPR, como el derecho a saber qué información personal se recopila y a optar por no participar en la venta de esa información, no abarca el mismo espectro de derechos ni la misma profundidad en el consentimiento explícito que caracteriza al GDPR.

En Asia, Singapur con su Ley de Protección de Datos Personales (PDPA) ofrece un enfoque equilibrado que fomenta tanto la protección de datos personales como la libertad económica, pero ha enfrentado críticas por no ofrecer suficientes mecanismos de aplicación y rectificación comparables a los de la UE.

Un caso notable de problemas generados por regulaciones de protección de datos es el del Safe Harbor Agreement entre EE.UU. y la UE, que fue invalidado por el Tribunal de Justicia de la Unión Europea debido a preocupaciones sobre la vigilancia masiva por parte de los EE.UU., lo que llevó a la creación del Escudo de Privacidad UE-EE.UU., que también enfrenta críticas y desafíos legales continuos.

Estos ejemplos muestran la importancia de un análisis profundo de las leyes de protección de datos para entender no solo su contenido y alcance, sino también su eficacia, áreas de fortaleza, y sus potenciales debilidades en la implementación y cumplimiento.

La Unión Europea (UE) se ha establecido como líder en la protección de datos personales con la implementación del Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) en mayo de 2018. El GDPR se destaca por su enfoque exhaustivo hacia la privacidad y protección de datos, aplicando no solo a entidades dentro de la UE, sino también a aquellas fuera de la región que procesan datos de ciudadanos de la UE. Este reglamento enfatiza principios fundamentales como el consentimiento explícito de los individuos para el procesamiento de sus datos, el derecho al olvido, y la portabilidad de datos, estableciendo un nuevo estándar global en la protección de datos (EuropeanParliament and Council, 2016).

En contraste, Estados Unidos adopta un enfoque más fragmentado hacia la protección de datos, sin una ley federal integral equivalente al GDPR. Sin embargo, la Ley de Privacidad del Consumidor de California (CCPA), que entró en vigor en enero de 2020, marca un hito importante en la legislación estadounidense, ofreciendo a los residentes de California derechos comparables a los del GDPR, como el derecho a saber qué información personal se recopila sobre ellos y a optar por no participar en la venta de esa información (Stateof California DepartmentofJustice, n.d.).

Brasil, por su parte, promulgó la LeiGeral de Proteção de Dados (LGPD)en agosto de 2018, reflejando muchos de los principios y disposiciones del GDPR. La LGPD representa un paso significativo hacia la armonización de las leyes de protección de datos en América Latina, proporcionando un marco detallado para el procesamiento de datos personales y reforzando los derechos de privacidad de los individuos en Brasil (Presidência da República, 2018).

Mientras tanto, en Asia, la Ley de Protección de Datos Personales (PDPA) de Singapur, implementada en fases a partir de 2013, establece normas de gobernanza para la recopilación, uso y divulgación de datos personales. La PDPA destaca por su enfoque pragmático y equilibrado, que busca proteger los datos personales de los individuos al mismo tiempo que apoya las necesidades de las organizaciones para procesar datos con fines legítimos (Personal Data ProtectionCommissionSingapore, n.d.).

Este análisis revela un panorama global diverso en lo que respecta a la protección de datos personales. Aunque el GDPR ha influenciado significativamente el desarrollo de legislaciones en otras jurisdicciones, la implementación y el alcance de estas leyes varían ampliamente. Esta diversidad plantea desafíos particulares para las empresas globales, que deben navegar por un mosaico de regulaciones para asegurar el cumplimiento a nivel internacional.

La evolución continua de las tecnologías digitales, junto con la creciente conciencia sobre la importancia de la privacidad de datos, sugiere que la protección de datos personales seguirá siendo un tema crítico en la agenda global. A medida que las jurisdicciones buscan equilibrar la protección de la privacidad con las demandas de la economía digital, la cooperación internacional y el intercambio de mejores prácticas serán esenciales para desarrollar marcos regulatorios que no solo protejan los derechos de los individuos, sino que también faciliten la innovación y el crecimiento económico.
A continuación, se destacan algunos de los articulados más importantes de leyes de protección de datos a nivel internacional, narrando su significado y relevancia.

Reglamento General de Protección de Datos (GDPR) - Unión Europea

El Artículo 15 - Derecho de acceso del interesado, es uno de los pilares del GDPR. Este artículo otorga a los individuos el derecho a obtener del responsable del tratamiento confirmación sobre si se están tratando datos personales que les conciernen y, en tal caso, derecho de acceso a dichos datos. Este derecho subraya la transparencia y empodera a los ciudadanos en el manejo de su información personal (EuropeanParliament and Council, 2016).

Ley de Privacidad del Consumidor de California (CCPA) - Estados Unidos

El Artículo 1798.120 - Derecho a optar por no participar en la venta de datos personales, representa un avance significativo en la protección de la privacidad. Este artículo permite a los consumidores de California decir "no" a la venta de sus datos personales, otorgándoles un control directo sobre su información personal y cómo se comparte (Stateof California DepartmentofJustice, n.d.).

Ley General de Protección de Datos (LGPD) - Brasil

El Artículo 7 - Condiciones para el procesamiento de datos personales, es crucial en la LGPD. Este artículo establece las condiciones bajo las cuales el procesamiento de datos personales es legal, incluyendo el consentimiento del titular de los datos, el cumplimiento de una obligación legal por parte del responsable del tratamiento, y la protección de la vida o de la integridad física del titular de los datos, entre otros. Este artículo es fundamental para entender el marco

legal bajo el cual se pueden procesar los datos personales en Brasil (Presidência da República, 2018).

Ley de Protección de Datos Personales (PDPA) - Singapur

El Artículo 14 - Consentimiento, es clave en la PDPA. Este artículo destaca la importancia del consentimiento de los individuos antes de que sus datos personales sean recopilados, usados o divulgados por las organizaciones. Este consentimiento debe ser informado y dado voluntariamente, lo cual es esencial para la autonomía de los individuos en el manejo de su información personal (Personal Data ProtectionCommissionSingapore, n.d.).

Estos artículos representan solo una muestra de las disposiciones fundamentales presentes en las leyes de protección de datos a nivel internacional. Cada uno refleja un aspecto crucial de la protección de datos: el derecho a la información y acceso, el control sobre la venta de datos personales, las condiciones legales para el procesamiento de datos y la importancia del consentimiento. Juntos, forman una base sobre la cual se construye la protección de la privacidad en la era digital.

Mejores Prácticas para el Cumplimiento

Para cumplir con la legislación de protección de datos, las organizaciones deben adoptar una serie de mejores prácticas, incluyendo:

- **Evaluaciones de Impacto de Protección de Datos (DPIAs):** Realizar evaluaciones regulares para identificar y mitigar riesgos en el procesamiento de datos personales.
- **Designación de un Oficial de Protección de Datos (DPO):** Nombrar a un experto en protección de datos para supervisar el cumplimiento de las políticas de privacidad y servir como punto de contacto con las autoridades reguladoras.
- **Capacitación**: Asegurar que todo el personal esté informado sobre las obligaciones de protección de datos y cómo estas afectan sus roles específicos.
- **Implementación de Medidas de Seguridad de Datos**: Adoptar medidas técnicas y organizativas para proteger los datos personales contra el acceso no autorizado, la pérdida o el daño.
- **Transparencia y Comunicación con los Interesados:** Mantener una comunicación clara y transparente con los individuos sobre cómo se recopilan, usan y protegen sus datos.

La legislación de protección de datos y el cumplimiento no son solo obligaciones legales, sino también componentes críticos de la ética empresarial y la responsabilidad social corporativa en la era digital. A medida que la cantidad de datos personales recolectados y procesados continúa creciendo, también lo hace la importancia de proteger esos datos. Las organizaciones deben considerar el cumplimiento no como una carga, sino como una oportunidad para fortalecer la confianza y la lealtad de los clientes, asegurando al mismo tiempo que operan de manera ética y responsable. Navegar por el complejo panorama de la protección de datos requiere un compromiso constante con la mejora y adaptación, pero los beneficios de hacerlo correctamente son inmensurables, tanto para los individuos como para las organizaciones.

Interoperabilidad y Estándares Abiertos

La interoperabilidad y los estándares abiertos son conceptos fundamentales en el ámbito de la tecnología de la información y comunicación (TIC), esenciales para el desarrollo, implementación y operación efectiva de sistemas digitales en una amplia gama de sectores. La interoperabilidad se refiere a la capacidad de diferentes sistemas, dispositivos o aplicaciones para trabajar juntos, compartir y utilizar datos de manera efectiva, independientemente de sus diferencias en diseño o tecnología. Los estándares abiertos, por otro lado, son especificaciones técnicas disponibles públicamente que se utilizan para facilitar la interoperabilidad entre productos y servicios tecnológicos, asegurando que estos puedan comunicarse y operar juntos sin restricciones.

Importancia de la Interoperabilidad

La interoperabilidad es crucial en el mundo digital moderno, donde la necesidad de sistemas y dispositivos para interactuar y compartir datos es omnipresente. Desde la atención médica hasta la banca, la educación y el gobierno, la capacidad de diferentes sistemas para trabajar juntos de manera eficiente tiene un impacto significativo en la eficiencia operativa, la innovación y la entrega de servicios. En el sector de la salud, por ejemplo, la interoperabilidad entre sistemas de información hospitalaria, registros electrónicos de salud y dispositivos médicos puede mejorar significativamente la calidad del cuidado al permitir una gestión más efectiva y un acceso más fácil a los datos del paciente. En el contexto gubernamental, facilita la provisión de servicios públicos de manera más integrada y accesible para los ciudadanos.

A pesar de su importancia, lograr la interoperabilidad presenta varios desafíos. La diversidad de estándares tecnológicos, la variabilidad en las implementaciones de sistemas y la presencia de sistemas heredados pueden obstaculizar la capacidad de los sistemas para interactuar. Además, las preocupaciones sobre la seguridad de los datos y la privacidad se magnifican cuando los datos se comparten entre sistemas y fronteras organizacionales. Por lo tanto, lograr un equilibrio entre interoperabilidad, seguridad y privacidad es un desafío constante.

Los estándares abiertos juegan un papel crucial en la superación de estos desafíos. Al proporcionar un conjunto común de normas y protocolos, facilitan la compatibilidad y la funcionalidad entre diferentes sistemas y dispositivos. Los estándares abiertos no solo promueven la interoperabilidad sino que también fomentan la innovación, permitiendo a los desarrolladores y fabricantes construir sobre una base común de tecnología. Esto reduce la duplicación de esfuerzos y permite una mayor concentración en la innovación y la mejora de servicios y productos.

La adopción de estándares abiertos tiene el potencial de reducir significativamente los costos asociados con el desarrollo de tecnologías interoperables, ya que permite la reutilización de soluciones existentes en lugar de requerir el desarrollo de soluciones propietarias desde cero. Además, los estándares abiertos pueden contribuir a un mercado más competitivo y diverso, reduciendo el riesgo de dependencia de proveedores únicos y promoviendo una mayor elección para los consumidores.

Para un gobierno que busca implementar estándares abiertos, es crucial considerar aquellos que faciliten la interoperabilidad entre diferentes sistemas gubernamentales y mejoren la

accesibilidad y transparencia de los servicios públicos. Algunos estándares a considerar incluyen por ejemplo:

- Open DocumentFormat (ODF): Para la documentación gubernamental, garantizando que los documentos sean accesibles con cualquier software de oficina, evitando la dependencia de proveedores específicos.
- Open311: Facilita la comunicación entre ciudadanos y servicios municipales para reportes de problemas urbanos, mejorando la gestión y respuesta ciudadana.
- GTFS (General TransitFeedSpecification): Estándar para compartir información sobre transporte público, permitiendo la integración de diferentes servicios de transporte en aplicaciones de mapeo y planificación de rutas.

Existen numerosos ejemplos de estándares abiertos que han facilitado la interoperabilidad en diferentes campos. En la web, tecnologías como HTML, CSS y JavaScript, todas basadas en estándares abiertos definidos por el World Wide Web Consortium (W3C), han permitido el desarrollo de una internet accesible y universal. En el intercambio de datos, formatos como XML y JSON facilitan la interoperabilidad de datos entre sistemas dispares. En la atención médica, estándares como HL7 y FHIR están diseñados para permitir el intercambio seguro y eficiente de datos de salud electrónicos.

La interoperabilidad y los estándares abiertos son fundamentales para el éxito y la sostenibilidad de los ecosistemas digitales en nuestra sociedad interconectada. Facilitan la comunicación y colaboración entre diferentes sistemas y tecnologías, promoviendo la innovación y mejorando la eficiencia y calidad de los servicios. A medida que avanzamos hacia un futuro cada vez más digitalizado, la importancia de fomentar la interoperabilidad y adoptar estándares abiertos solo seguirá creciendo, planteando desafíos y oportunidades para desarrolladores, empresas, gobiernos y usuarios finales por igual.

Calidad y Consistencia de Datos

La calidad y consistencia de los datos son aspectos cruciales en la gestión de la información dentro de cualquier organización, afectando directamente la toma de decisiones, la eficiencia operativa y la capacidad de innovación. La calidad de los datos se refiere a la precisión, completitud, fiabilidad y relevancia de los datos, mientras que la consistencia se ocupa de la uniformidad de estos datos a lo largo del tiempo y a través de diferentes sistemas y procesos. Juntos, estos factores aseguran que la información sea confiable y válida para su uso en análisis, reportes y otras aplicaciones críticas para el negocio.

Los datos de alta calidad y consistentes son fundamentales para cualquier entidad que busque tomar decisiones basadas en información sólida y realizar operaciones sin interrupciones. La calidad de los datos impacta directamente en la confianza que los usuarios y gestores pueden depositar en los sistemas de información para la toma de decisiones estratégicas. Datos inexactos o incompletos pueden llevar a conclusiones erróneas, decisiones mal informadas y, en última instancia, a pérdidas financieras significativas. Por otro lado, la consistencia de los datos asegura que independientemente del punto de acceso o el momento, la información recuperada es uniforme y comparable, lo cual es esencial para el análisis de tendencias a lo largo del tiempo y la integración de sistemas.

Asegurar la calidad y consistencia de los datos presenta varios desafíos, especialmente en organizaciones grandes y complejas donde los datos se generan y recolectan a través de múltiples canales y sistemas. Entre estos desafíos se incluyen:

- **Diversidad de Fuentes de Datos:** La integración de datos de diversas fuentes aumenta el riesgo de inconsistencias y errores.
- **Datos Desactualizados:** La rapidez con la que la información puede volverse obsoleta requiere procesos constantes de actualización y verificación.
- **Errores Humanos y de Procesamiento:** Los errores en la entrada de datos o en los algoritmos de procesamiento pueden comprometer la calidad de los datos.
- **Falta de Estándares Uniformes:** La ausencia de estándares de datos coherentes a lo largo de una organización puede llevar a discrepancias y fragmentación de la información.

Estrategias para Mejorar la Calidad y Consistencia de Datos

Para superar estos desafíos y asegurar la calidad y consistencia de los datos, las organizaciones pueden adoptar varias estrategias y prácticas:

- Implementación de Estándares de Datos: Establecer y aplicar estándares uniformes para la entrada, procesamiento y almacenamiento de datos ayuda a asegurar su consistencia.
- Sistemas de Gestión de Calidad de Datos: Utilizar software especializado que automáticamente verifica, limpia y enriquece los datos puede reducir significativamente los errores y las inconsistencias.
- Capacitación y Concienciación: Educar al personal sobre la importancia de la calidad de los datos y entrenarlos en prácticas adecuadas de manejo de datos es esencial para minimizar los errores humanos.
- Procesos de Revisión y Auditoría de Datos: Establecer revisiones periódicas y auditorías de datos para identificar y corregir problemas de calidad y consistencia.
- Gobernanza de Datos: Crear un marco de gobernanza de datos que defina claramente las responsabilidades y procesos para el manejo de datos en toda la organización.

El Instituto Nacional de Estadística (INE) juega un rol crucial en la consolidación y diseminación de datos fiables y precisos que son fundamentales para la formulación de políticas públicas, planificación gubernamental y evaluación de programas. La capacidad del INE para recolectar, analizar y distribuir estadísticas sobre diversos aspectos socioeconómicos y demográficos proporciona una base sólida para decisiones informadas a todos los niveles del gobierno y el sector privado. El intercambio de experiencias y el apoyo mutuo entre países pueden mitigar las vulnerabilidades políticas de los institutos estadísticos al proporcionar un marco de trabajo que respalde su autonomía y destaque la importancia de estadísticas confiables y objetivas. En este sentido, los convenios se vuelven esenciales para asegurar que los INEs puedan ejercer sus funciones de manera efectiva, libre de influencias indebidas y con el respaldo de una comunidad internacional que valora y depende de la precisión de sus datos para la formulación de políticas efectivas y el desarrollo sostenible.

La tecnología juega un papel crucial en la mejora de la calidad y consistencia de los datos. Las soluciones tecnológicas modernas, como la inteligencia artificial (IA) y el aprendizaje automático (ML), pueden automatizar la detección y corrección de errores en los datos, así

como la identificación de inconsistencias. Además, los sistemas de gestión de datos maestros (MDM) permiten a las organizaciones mantener una fuente única de verdad para datos críticos, asegurando su consistencia a través de diferentes aplicaciones y sistemas.

La calidad y consistencia de los datos son pilares fundamentales para el éxito de las organizaciones en la era digital. Asegurar que los datos sean precisos, completos, confiables y consistentes es esencial para tomar decisiones informadas, mejorar la eficiencia operativa y fomentar la innovación. Mediante la implementación de estrategias efectivas de gestión de la calidad de los datos, la adopción de tecnologías avanzadas y el establecimiento de una cultura organizacional que valore la integridad de los datos, las organizaciones pueden superar los desafíos asociados y aprovechar al máximo su activo más valioso: sus datos.

Gobernanza Colaborativa y Participación

La gobernanza colaborativa y la participación representan un paradigma emergente en la administración de organizaciones y sistemas, enfatizando la importancia de la inclusión, la colaboración y el compromiso entre diversos grupos de interés para lograr resultados efectivos y sostenibles. Este enfoque se extiende más allá de las estructuras tradicionales de toma de decisiones, promoviendo un modelo más abierto y participativo que aprovecha la diversidad de perspectivas y conocimientos.

La gobernanza colaborativa se basa en el principio de que los desafíos complejos y multifacéticos que enfrentan las sociedades y organizaciones contemporáneas requieren soluciones igualmente complejas, las cuales son mejor desarrolladas e implementadas a través de la colaboración entre una amplia gama de actores. Estos actores pueden incluir entidades gubernamentales, organizaciones no gubernamentales, el sector privado, comunidades y ciudadanos individuales.

Este enfoque reconoce que ningún sector tiene todas las respuestas o recursos necesarios para abordar los problemas de manera efectiva por sí solo. Por lo tanto, la gobernanza colaborativa busca construir puentes entre diferentes sectores, facilitando espacios donde se puedan compartir ideas, recursos y responsabilidades para el bien común (Ansell&Gash, 2008).

La participación es un componente esencial de la gobernanza colaborativa, enfatizando el derecho y la capacidad de todos los interesados relevantes para contribuir al proceso de toma de decisiones. La participación efectiva asegura que las decisiones reflejen un amplio rango de intereses y conocimientos, aumentando la legitimidad, la aceptación y la efectividad de las políticas y acciones resultantes.

La participación va más allá de la mera consulta, buscando activamente involucrar a los interesados en el diseño, la implementación y la evaluación de las políticas y programas. Este enfoque participativo puede ayudar a identificar soluciones innovadoras, mitigar conflictos y construir un sentido de propiedad y compromiso entre los participantes (Fung, 2006).

Implementar la gobernanza colaborativa y fomentar la participación efectiva presenta varios desafíos. Entre estos, destacan la necesidad de equilibrar intereses divergentes, superar barreras de comunicación y construir confianza entre los participantes. Además, es fundamental asegurar que la participación sea genuina y representativa, evitando la inclusión superficial o el dominio de grupos de interés particulares.

Otro desafío significativo es el diseño de estructuras y procesos que faciliten la colaboración efectiva y la participación sin crear sistemas excesivamente complejos o burocráticos que puedan obstaculizar la toma de decisiones y la acción (Emerson, Nabatchi, &Balogh, 2012).

Estrategias para Promover la Gobernanza Colaborativa y la Participación

Para superar estos desafíos y promover una gobernanza colaborativa efectiva, las organizaciones y gobiernos pueden adoptar varias estrategias, incluyendo:

- **Desarrollo de Plataformas de Colaboración:** Crear espacios físicos y digitales que faciliten el intercambio de ideas y recursos entre diferentes actores.
- **Capacitación y Fortalecimiento de Capacidades:** Invertir en el desarrollo de habilidades de liderazgo colaborativo, negociación y resolución de conflictos entre los participantes.
- **Mecanismos de Retroalimentación y Evaluación:** Implementar sistemas para monitorear y evaluar la efectividad de la colaboración y la participación, permitiendo ajustes continuos.
- **Transparencia y Comunicación Efectiva:** Asegurar que todos los participantes tengan acceso a información relevante y utilizar medios de comunicación que faciliten el entendimiento mutuo.

La gobernanza colaborativa y la participación representan enfoques vitales para abordar los complejos desafíos de nuestro tiempo. Al promover la inclusión, la colaboración y el compromiso entre una amplia gama de actores, estos enfoques pueden aumentar la efectividad, legitimidad y sostenibilidad de las decisiones y acciones. Sin embargo, para que sean efectivos, es esencial superar los desafíos inherentes a la colaboración y participación, diseñando procesos y estructuras que faciliten la interacción productiva entre los diversos grupos de interés. Al hacerlo, organizaciones y gobiernos pueden aprovechar el poder de la diversidad y la colaboración para crear soluciones innovadoras y efectivas a los problemas que enfrentamos colectivamente.

Enfoque en la Ética de los Datos

los datos se han convertido en uno de los activos más valiosos para organizaciones y sociedades. Sin embargo, la recolección, el análisis y el uso de datos masivos plantean importantes cuestiones éticas que deben abordarse con cuidado para proteger los derechos individuales y promover el bienestar colectivo. Un enfoque ético en la gestión de datos no solo es crucial para mantener la confianza del público y la legitimidad de las entidades que manejan datos, sino también para asegurar que la innovación y el progreso tecnológico se realicen de manera responsable y justa.

La ética de los datos se basa en principios fundamentales destinados a guiar el comportamiento responsable en la recolección, el procesamiento y el uso de datos. Estos principios incluyen:

- Respeto por la Autonomía: Reconocer y respetar el derecho de las personas a controlar sus datos personales, incluyendo el derecho a dar o retirar el consentimiento para su uso.

- No Maleficencia: Evitar causar daño a las personas a través del mal uso de sus datos, protegiendo su privacidad y seguridad.
- Beneficencia: Asegurar que los datos se utilicen de manera que promuevan el bienestar de las personas y la sociedad, contribuyendo a la mejora de servicios, productos y políticas.
- Justicia: Garantizar que los beneficios y las cargas derivadas del uso de datos se distribuyan de manera equitativa entre todos los grupos sociales, evitando la discriminación y promoviendo la equidad.
- Transparencia: Ser abierto y honesto acerca de cómo se recolectan, procesan y utilizan los datos, permitiendo el escrutinio público y la rendición de cuentas.

Desafíos Éticos en la Gestión de Datos

La gestión de datos presenta varios desafíos éticos, incluyendo la protección de la privacidad, el consentimiento informado, la discriminación y el sesgo algorítmico, y el acceso equitativo a los beneficios de la tecnología. Por ejemplo, la recolección masiva de datos personales, a menudo sin el conocimiento o consentimiento explícito de los individuos, plantea serias preocupaciones sobre la privacidad y la autonomía personal. Del mismo modo, el uso de algoritmos de inteligencia artificial y aprendizaje automático puede perpetuar o incluso exacerbar la discriminación y el sesgo si los datos utilizados para entrenar estos sistemas no son representativos o están sesgados.

Para abordar estos desafíos y asegurar un enfoque ético en la gestión de datos, las organizaciones pueden adoptar varias estrategias y prácticas, incluyendo:

- Desarrollo de Políticas Éticas de Datos: Crear y implementar políticas claras que reflejen los principios éticos y guíen la recolección, el procesamiento y el uso de datos.
- Evaluaciones de Impacto Ético: Realizar evaluaciones regulares del impacto ético de las actividades de manejo de datos para identificar y mitigar posibles riesgos éticos.
- Educación y Capacitación: Fomentar una cultura ética mediante la educación y capacitación de empleados y partes interesadas sobre la importancia de la ética de los datos y las prácticas responsables.
- Diseño Centrado en el Humano: Incorporar consideraciones éticas en el diseño de sistemas de datos y algoritmos, asegurando que sean justos, transparentes y respetuosos con la privacidad.
- Participación de Grupos de Interés: Involucrar a una amplia gama de partes interesadas, incluyendo a usuarios y grupos afectados, en el proceso de toma de decisiones relacionado con los datos.

El enfoque en la ética de los datos es esencial para navegar el complejo paisaje de la era digital de manera responsable. Al adherirse a principios éticos fundamentales y enfrentar proactivamente los desafíos éticos, las organizaciones pueden asegurar que la gestión de datos no solo cumpla con las obligaciones legales y regulatorias, sino que también promueva el respeto por los derechos individuales y contribuya al bienestar colectivo. La ética de los datos, por lo tanto, no solo es una cuestión de cumplimiento, sino un imperativo moral y estratégico que sustenta la confianza pública y la sostenibilidad a largo plazo en la era de la información.

Iniciativas de Datos Abiertos

Las iniciativas de datos abiertos se han convertido en un componente crucial de la gobernanza moderna y la estrategia de datos de muchas organizaciones, tanto en el sector público como en el privado. Estas iniciativas se centran en la publicación y compartición de datos en formatos accesibles y reutilizables, sin restricciones que impidan su uso o distribución. Su objetivo es promover la transparencia, fomentar la innovación, mejorar la eficiencia de los servicios públicos y estimular el crecimiento económico a través del uso estratégico de los datos.

Las iniciativas de datos abiertos son fundamentales por varias razones. Primero, aumentan la transparencia gubernamental al permitir a los ciudadanos acceder a información sobre las actividades gubernamentales, decisiones y políticas. Esto, a su vez, mejora la rendición de cuentas y la confianza pública. En el ámbito económico, los datos abiertos ofrecen oportunidades para el desarrollo de nuevos productos y servicios, impulsando la innovación y el emprendimiento. Además, facilitan la investigación y el desarrollo al proporcionar a los académicos y científicos acceso a conjuntos de datos valiosos.

El gran desafío de transformar los registros en datos útiles y accesibles es fundamental para mejorar la gestión de información en un contexto gubernamental. En este proceso, el Instituto Nacional de Estadística (INE) juega un papel esencial, dado que cada vez más extrae información valiosa de registros administrativos para elaborar estadísticas que soporten la toma de decisiones informadas y políticas públicas eficaces.

La digitalización, observada en instituciones como el Ministerio de Economía (MinEco) y la Superintendencia de Administración Tributaria (SAT), está revolucionando la generación y manejo de datos al facilitar el acceso y análisis de grandes volúmenes de información en tiempo real. Esta transformación digital no solo optimiza los recursos y procesos, sino que también mejora la transparencia y la eficiencia del servicio público.

Imagen 3. Barometro regional de Datos Abiertos. ILDA

Posición	País	Puntuación SOBRE 100	Evolución SOBRE EDICIONES ANTERIORES	Preparación SOBRE 100	Implementación SOBRE 100	Impacto SOBRE 100
1	Uruguay	64		73.32	82.33	35.00
2	Argentina	63		69.10	75.33	45.00
3	Colombia	60		74.08	75.67	31.67
4	Brasil	60		61.61	87.33	31.67
5	México	58		62.12	73.33	40.00
6	Chile	54		61.00	75.67	26.67
7	Costa Rica	45		58.00	66.67	11.67
8	República Dominicana	45		55.31	58.33	21.67
9	Perú	45		59.44	68.33	6.67
10	Paraguay	44		45.72	60.33	26.67
11	Panamá	43		59.65	67.67	1.67
12	Ecuador	42		61.61	60.33	5.00
13	Bolivia	41		46.51	58.67	18.33
14	Jamaica	41		41.94	54.67	26.67

A pesar de sus beneficios, las iniciativas de datos abiertos enfrentan varios desafíos. Uno de los principales es garantizar la calidad y la relevancia de los datos publicados. Los datos deben ser precisos, actualizados y presentados en formatos estandarizados para ser útiles. Otro desafío es proteger la privacidad y la seguridad de la información personal, lo que requiere un cuidadoso equilibrio entre la apertura y la protección de datos sensibles. Además, es fundamental superar las barreras técnicas y culturales que impiden la adopción y el uso efectivo de los datos abiertos, como la falta de capacidad técnica en algunos usuarios potenciales o la resistencia al cambio dentro de las organizaciones.

Ejemplos de Iniciativas de Datos Abiertos Exitosas

- Portal de Datos Abiertos de la Unión Europea: Proporciona acceso a un amplio rango de datos generados por las instituciones y otros órganos de la UE, abarcando temas como el medio ambiente, la educación, la salud y el transporte.
- Data.gov en Estados Unidos: Ofrece más de 200,000 conjuntos de datos de diversas agencias gubernamentales, disponibles para el público con el objetivo de mejorar la transparencia gubernamental y fomentar la innovación.
- Open Data Institute: Fundado en el Reino Unido por Sir Tim Berners-Lee y Sir Nigel Shadbolt, trabaja para promover las iniciativas de datos abiertos a nivel global, ofreciendo asesoramiento, investigación y formación

Estrategias para Implementar Iniciativas de Datos Abiertos

Para que las iniciativas de datos abiertos sean efectivas, las organizaciones y las instituciones públicas deben adoptar varias estrategias clave:

- **Desarrollar una Política de Datos Abiertos**: Establecer un marco legal y normativo que defina claramente los objetivos, responsabilidades y procesos para la publicación de datos abiertos.
- **Asegurar la Calidad y la Estándarización de los Datos:** Implementar procesos para garantizar que los datos sean precisos, relevantes y accesibles en formatos estandarizados y fáciles de usar.
- **Fomentar la Participación y Colaboración**: Involucrar a una amplia gama de actores, incluyendo el gobierno, el sector privado, la academia y la sociedad civil, para aprovechar al máximo el potencial de los datos abiertos.
- **Proporcionar Capacitación y Recursos**: Ofrecer recursos educativos y técnicos para ayudar a los usuarios a entender y utilizar los datos abiertos de manera efectiva.
- **Promover Casos de Uso Innovadores:** Destacar y apoyar ejemplos exitosos de cómo los datos abiertos están siendo utilizados para crear valor, incentivando así una mayor adopción y experimentación.

Las iniciativas de datos abiertos representan una oportunidad significativa para transformar la manera en que interactuamos con los datos, abriendo nuevas vías para la transparencia, la colaboración y la innovación. Al superar los desafíos relacionados con la calidad de los datos, la privacidad y la usabilidad, y al implementar estrategias efectivas para promover su adopción, las organizaciones y gobiernos pueden maximizar el impacto positivo de los datos abiertos en la sociedad y la economía. En última instancia, las iniciativas de datos abiertos tienen el potencial de empoderar a los ciudadanos, impulsar el desarrollo sostenible y fomentar una cultura de apertura y colaboración que beneficie a todos.

Seguridad de Datos y Gestión de Riesgos

La seguridad de datos y la gestión de riesgos son aspectos críticos en la administración de la información en la era digital. A medida que las organizaciones dependen cada vez más de sistemas digitales para operar, la cantidad y el valor de los datos almacenados y procesados crecen exponencialmente. Esto no solo aumenta las oportunidades para la innovación y la eficiencia sino que también eleva los riesgos asociados con la pérdida, el robo o el mal uso de datos. La seguridad de datos se enfoca en proteger los activos de información contra amenazas internas y externas, mientras que la gestión de riesgos implica identificar, evaluar y mitigar los riesgos asociados con la operación y el uso de sistemas de información.

La seguridad de datos es esencial para proteger la privacidad de los individuos, mantener la confianza del cliente, cumplir con regulaciones y leyes de protección de datos, y proteger los activos intelectuales y financieros de una organización. Las violaciones de datos pueden resultar en pérdidas financieras significativas, daño a la reputación, pérdida de confianza del cliente y sanciones legales. Por lo tanto, implementar medidas de seguridad de datos robustas es fundamental para prevenir accesos no autorizados, filtraciones de datos, y otros tipos de incidentes de seguridad.

Los desafíos en la seguridad de datos son multifacéticos y en constante evolución. Las amenazas cibernéticas, como el malware, el ransomware, el phishing y los ataques de denegación de servicio (DDoS), son cada vez más sofisticadas y difíciles de prevenir. Además, la complejidad de las infraestructuras tecnológicas y la adopción de tecnologías emergentes, como la nube y el Internet de las Cosas (IoT), introducen nuevas vulnerabilidades. Otro desafío importante es el factor humano, ya que los errores de los empleados o la falta de conciencia sobre seguridad pueden comprometer los sistemas de datos.

Principios de la Gestión de Riesgos

La gestión de riesgos implica un proceso sistemático de identificar, evaluar y tratar los riesgos que podrían afectar negativamente la información y los activos de una organización. Los principios clave de la gestión de riesgos incluyen:

- Identificación de Riesgos: Reconocer las amenazas potenciales y las vulnerabilidades dentro de la organización que podrían facilitar un ataque o pérdida de datos.
- Evaluación de Riesgos: Determinar la probabilidad y el impacto potencial de los riesgos identificados.
- Mitigación de Riesgos: Implementar medidas de control adecuadas para reducir la probabilidad o el impacto de los riesgos.
- Monitoreo y Revisión: Supervisar continuamente el entorno de riesgo y ajustar las medidas de control según sea necesario.

Estrategias para Mejorar la Seguridad de Datos y la Gestión de Riesgos

Para enfrentar los desafíos en seguridad de datos y gestión de riesgos, las organizaciones pueden adoptar varias estrategias:

- Capacitación: Educar a los empleados sobre las mejores prácticas de seguridad de datos y concienciarlos sobre los riesgos potenciales.

- Implementación de Políticas de Seguridad de Datos: Desarrollar y aplicar políticas de seguridad que aborden aspectos como el acceso a datos, la gestión de contraseñas y la seguridad física.
- Uso de Tecnología de Seguridad Avanzada: Aplicar soluciones tecnológicas como el cifrado de datos, firewalls, sistemas de detección de intrusiones y autenticación multifactor para proteger los sistemas y datos.
- Gestión de Acceso: Limitar el acceso a datos y sistemas solo a los usuarios autorizados que necesiten acceso para realizar sus funciones.
- Planificación de Respuesta a Incidentes: Preparar un plan de respuesta a incidentes de seguridad para garantizar una respuesta rápida y efectiva ante violaciones de datos o ataques cibernéticos.
- Evaluaciones de Seguridad Regular y Auditorías: Realizar evaluaciones de seguridad y auditorías regularmente para identificar y remediar vulnerabilidades.

La seguridad de datos y la gestión de riesgos son fundamentales para proteger los activos de información en el mundo digital de hoy. Al comprender los desafíos y aplicar estrategias efectivas, las organizaciones pueden mitigar los riesgos asociados con la seguridad de datos y garantizar que sus operaciones y la información sensible estén protegidas contra amenazas internas y externas. Un enfoque proactivo en la seguridad de datos y la gestión de riesgos no solo salvaguarda la información crítica sino que también refuerza la confianza de los stakeholders en la capacidad de la organización para manejar de manera responsable y segura sus datos.

Formación y Desarrollo de Capacidades

La formación y el desarrollo de capacidades representan pilares fundamentales para el crecimiento y la sostenibilidad de cualquier organización en el contexto actual, caracterizado por la rápida evolución tecnológica y los constantes cambios en el mercado laboral. Estas prácticas no solo están dirigidas a mejorar las habilidades y conocimientos de los empleados, sino también a fomentar un ambiente de aprendizaje continuo que pueda adaptarse a los desafíos futuros. En este sentido, la formación y el desarrollo de capacidades se convierten en estrategias clave para potenciar la innovación, mejorar la competitividad y asegurar la retención del talento dentro de las organizaciones.

En un mundo donde el conocimiento se actualiza constantemente y las nuevas tecnologías transforman los modos de trabajar, la formación y el desarrollo de capacidades se hacen esenciales para que tanto individuos como organizaciones mantengan su relevancia y eficacia. Para los empleados, adquirir nuevas habilidades y competencias es crucial para su crecimiento profesional y satisfacción laboral. Para las organizaciones, contar con un equipo bien capacitado es vital para la innovación, la eficiencia operativa y la capacidad de responder a las demandas del mercado.

Implementar programas efectivos de formación y desarrollo de capacidades presenta varios desafíos. Primero, está el reto de identificar las necesidades de capacitación que están en constante cambio. Esto requiere un entendimiento profundo de las tendencias del mercado, las tecnologías emergentes y las competencias futuras necesarias. Segundo, adaptar los métodos de capacitación para satisfacer las preferencias de aprendizaje de una fuerza laboral diversa, que incluye múltiples generaciones con diferentes estilos de aprendizaje, es otro desafío significativo. Además, medir el impacto de estos programas en el rendimiento organizacional y en el desarrollo profesional individual puede ser complejo.

Estrategias Efectivas para la Formación y Desarrollo de Capacidades

Para superar estos desafíos y maximizar los beneficios de la formación y el desarrollo de capacidades, las organizaciones pueden adoptar varias estrategias:

- Evaluación de Necesidades de Capacitación: Realizar evaluaciones periódicas para identificar las brechas de competencias y diseñar programas de capacitación que se alineen con los objetivos estratégicos de la organización.
- Aprendizaje Personalizado y Flexible: Implementar métodos de capacitación que permitan la personalización y ofrezcan flexibilidad en términos de tiempo y lugar, como el e-learning y el aprendizaje móvil.
- Capacitación Basada en Competencias: Centrar los programas de formación en el desarrollo de competencias específicas que agreguen valor inmediato a las funciones y responsabilidades del empleado.
- Fomentar el Aprendizaje Continuo: Crear una cultura organizacional que valore y promueva el aprendizaje continuo, ofreciendo tiempo y recursos para la capacitación personal y profesional.
- Utilizar Tecnologías Emergentes: Aprovechar las tecnologías emergentes, como la realidad virtual y la inteligencia artificial, para crear experiencias de aprendizaje inmersivas y efectivas.
- Seguimiento y Evaluación: Establecer indicadores de rendimiento claros para evaluar la efectividad de los programas de capacitación y ajustarlos según sea necesario.

Los beneficios de invertir en formación y desarrollo de capacidades son numerosos y significativos. Desde el punto de vista del empleado, aumenta la motivación, el compromiso y la satisfacción laboral, al sentir que la organización invierte en su crecimiento personal y profesional. Para la organización, los resultados incluyen una mayor innovación, productividad y adaptabilidad, así como una mejora en la calidad del trabajo y en la capacidad de atraer y retener talento.

La formación y el desarrollo de capacidades son esenciales para preparar tanto a empleados como a organizaciones para el futuro, permitiéndoles adaptarse y prosperar en un entorno cambiante. Al implementar estrategias efectivas que aborden las necesidades de capacitación y promuevan un ambiente de aprendizaje continuo, las organizaciones pueden asegurar que su fuerza laboral esté bien equipada para enfrentar los desafíos actuales y futuros. En última instancia, la inversión en formación y desarrollo de capacidades es una inversión en el activo más valioso de cualquier organización: su gente.

Ejercicio comparado para identificar la gobernanza, estructura, funciones, buenas prácticas y lecciones aprendidas

Realizaremos un ejercicio comparativo para identificar aspectos clave en la gobernanza de datos, estructura, funciones, buenas prácticas y lecciones aprendidas en cinco países de América Latina: Uruguay, Chile, Colombia, Brasil y México. Esta comparación nos permitirá entender cómo cada país aborda la gobernanza de datos y cuáles son sus prácticas destacadas.

Tabla 3. Ejercicio comparado para identificar la gobernanza

País	Entidad Responsable	Naturaleza de la Gobernanza	Funciones Principales	Buenas Prácticas	Lecciones Aprendidas
Uruguay	AGESIC (Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento)	Centralizada	Implementación de políticas de TI y datos abiertos.	Avanzado en gobierno digital y datos abiertos. Políticas enfocadas en la transparencia y la accesibilidad de los datos.	La centralización en una entidad puede facilitar la implementación uniforme de políticas de datos y TI.
Chile	División de Gobierno Digital - SEGPRES	Autónomo	Promueve la transparencia y el acceso a la información pública.	Fuerte enfoque en la transparencia y la protección de datos personales. Estrategias para mejorar la gobernanza y la infraestructura de datos.	La autonomía de las entidades responsables puede promover un enfoque específico y especializado en transparencia y protección de datos.

Colombia	Ministerio de Tecnologías de la Información y las Comunicaciones - MINTIC	Centralizado	Lidera las iniciativas de gobierno digital y datos abiertos.	Esfuerzos significativos en la digitalización de servicios gubernamentales. Políticas de datos abiertos y transparencia en desarrollo.	La importancia de la digitalización como base para una gobernanza de datos efectiva y la necesidad de políticas en desarrollo constante.
Brasil	Autoridad Nacional de Protección de Datos (ANPD)	Autónoma	Supervisa y aplica la LGPD y políticas de datos.	Implementación de la LGPD, alineada con el GDPR. Enfoque en la mejora de la transparencia y la protección de datos.	La adaptación de marcos internacionales como el GDPR puede facilitar el desarrollo de políticas de protección de datos robustas.

México	INAI (Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales)	Autónomo	Garantizar el derecho a la información y protección de datos.	Desarrollo progresivo en la gobernanza de datos y políticas de privacidad. Iniciativas de datos abiertos y gobierno electrónico.	La creación de entidades específicas para la transparencia y protección de datos promueve la importancia de estos temas a nivel nacional.

La tabla compara la gobernanza de datos en cinco países latinoamericanos, destacando cómo cada uno ha abordado la implementación de políticas y estructuras para la gestión de datos. A través de esta comparación, se pueden identificar varias lecciones importantes: la centralización frente a la autonomía de las entidades responsables tiene diferentes ventajas, desde la implementación uniforme hasta la promoción de enfoques especializados.

La distinción entre protección de datos y datos abiertos presenta un dilema fundamental en la gestión de la información pública. La protección de datos se enfoca en salvaguardar la privacidad individual y asegurar que la información personal no sea mal utilizada ni expuesta sin consentimiento. Por otro lado, la iniciativa de datos abiertos busca hacer la información gubernamental accesible y utilizable por el público en general para fomentar la transparencia, innovación y colaboración.

En el contexto de Guatemala, el desafío de generar datos abiertos es significativo debido a varias razones, como limitaciones en la infraestructura tecnológica, falta de marcos normativos específicos para datos abiertos, y posiblemente una cultura de compartición de información no tan desarrollada dentro de las entidades gubernamentales.

El enfoque de Brasil hacia la protección de datos, especialmente con la implementación de la LeiGeral de Proteção de Dados (LGPD), refleja un compromiso fuerte con la privacidad que, a primera vista, podría parecer que limita la capacidad de generar y compartir datos abiertos. Sin embargo, este enfoque también establece un marco legal claro y robusto que, si se implementa adecuadamente, puede proporcionar la seguridad y la confianza necesarias para que los datos se compartan de manera más abierta y transparente, siempre que se respeten las normas de privacidad.

La adaptación de marcos internacionales y la creación de entidades específicas para la transparencia y protección de datos son estrategias efectivas para mejorar la gobernanza de datos. Además, estas comparaciones resaltan la importancia de las iniciativas de gobierno digital y datos abiertos como medios para promover la transparencia, la accesibilidad y la protección de la privacidad. La experiencia de estos países ofrece valiosos insights sobre cómo desarrollar e implementar políticas de gobernanza de datos efectivas, equilibrando las necesidades de seguridad y accesibilidad.

Tabla 4. Ejercicio comparado para identificar la estructura

País	Descripción de la Estructura	Características Principales	Buenas Prácticas	Lecciones Aprendidas
Uruguay	Estructura centralizada y eficiente en la gestión de datos.	Infraestructura digital avanzada Centralización de la gestión de datos.	Inversión en infraestructura digital. Coordinación efectiva entre agencias.	La centralización puede facilitar la eficiencia y uniformidad en la implementación de políticas de datos.
Chile	Estructura integrada con colaboración entre diferentes sectores.	Inversiones en tecnología e infraestructura para datos. Colaboración multisectorial.	Fomento de la colaboración entre el gobierno, el sector privado y la academia. Inversiones estratégicas en infraestructura.	La colaboración entre sectores es clave para el desarrollo y la implementación efectiva de iniciativas de datos.

Colombia	Estructura en proceso de modernización y digitalización.	Diversidad regional en la implementación de políticas de datos. Esfuerzos de modernización digital.	Adaptación de políticas a contextos regionales. Inversión en digitalización.	La consideración de la diversidad regional es crucial en la formulación de políticas de datos efectivas.
Brasil	Estructura federal compleja con variabilidad en la implementación.	Progresos en la integración de sistemas de datos a nivel nacional. Desafíos en la coordinación entre estados y el gobierno federal.	Esfuerzos para integrar sistemas de datos a nivel nacional. Políticas dirigidas a superar la fragmentación.	La necesidad de coordinación y integración en sistemas federales complejos es fundamental para la coherencia de las políticas de datos.
México	Estructura diversificada con avances en digitalización.	Avances significativos en digitalización. Desafíos en la integración y coordinación a nivel federal y estatal.	Iniciativas para promover la digitalización. Estrategias para mejorar la coordinación entre niveles de gobierno.	La digitalización es un proceso clave para la modernización, pero requiere esfuerzos coordinados para su implementación efectiva.

Al considerar la estructura organizacional de una autoridad de protección de datos, ya sea en un contexto federal o regional, es crucial comprender cómo se compone la junta directiva, cómo se nombra a la autoridad, y cuáles son los principales departamentos que la componen. Estos factores son fundamentales para garantizar una administración eficaz y transparente que pueda equilibrar adecuadamente la protección de datos personales con la promoción de datos abiertos.

Esta tabla compara las estructuras de gestión de datos de cinco países, resaltando cómo cada uno enfrenta y aborda los desafíos de la digitalización y la gobernanza de datos. A través de este ejercicio comparado, se identifican buenas prácticas y lecciones aprendidas, tales como la importancia de la centralización para la eficiencia, la colaboración multisectorial para el desarrollo integral de iniciativas de datos, la adaptabilidad de las políticas a la diversidad regional, la necesidad de integración en sistemas federales para evitar la fragmentación, y la importancia de la coordinación entre diferentes niveles de gobierno para la implementación efectiva de la digitalización. Cada país presenta un enfoque único según su contexto político, económico y social, proporcionando valiosos insights sobre los diversos caminos hacia la modernización y la eficacia en la gestión de datos.

Tabla 5. Ejercicio comparado para identificar funciones

País	Funciones Principales	Buenas Prácticas	Lecciones Aprendidas
Uruguay	Líder en servicios de gobierno electrónico y datos abiertos. Uso de datos para mejorar la eficiencia y la transparencia gubernamental.	Implementación efectiva de plataformas de gobierno electrónico que facilitan el acceso y uso de datos abiertos.	La centralización y el liderazgo claro en la estrategia de datos pueden acelerar la adopción de servicios de gobierno electrónico y mejorar la transparencia.

Chile	Uso de datos para fomentar la transparencia y mejorar servicios públicos. Implementación de políticas para proteger la privacidad de los ciudadanos.	Estrategias integradas que promueven la colaboración entre diferentes sectores para el uso de datos en la mejora de servicios.	La colaboración intersectorial y la inversión en tecnología son clave para el éxito en la implementación de servicios públicos eficientes y transparentes.
Colombia	Uso de datos en la mejora de la transparencia y la toma de decisiones. Iniciativas para integrar datos en la planificación y desarrollo.	Esfuerzos para modernizar la infraestructura de datos y promover la digitalización a nivel nacional.	La diversidad del país representa desafíos y oportunidades para la implementación de políticas de datos, subrayando la importancia de estrategias adaptativas.
Brasil	Enfoque en la protección de datos y cumplimiento de la LGPD. Uso de datos para mejorar la gobernanza y la participación ciudadana.	Políticas específicas para la protección de datos personales y fomento de la participación ciudadana a través de plataformas de datos abiertos.	La legislación específica de protección de datos, como la LGPD, es fundamental para asegurar la privacidad de los ciudadanos y fomentar un entorno de confianza.

México	Uso de datos abiertos para fomentar la transparencia y la innovación. Desarrollo de políticas para mejorar la gestión y seguridad de datos.	Iniciativas dirigidas a la digitalización y el uso estratégico de datos abiertos para innovar y mejorar la transparencia.	La diversificación y el avance en la digitalización presentan oportunidades para mejorar la gestión de datos, aunque es necesario superar desafíos de integración y coordinación.

A continuación, se presenta una tabla comparativa que identifica las buenas prácticas en la gobernanza de datos de Uruguay, Chile, Colombia, Brasil y México. Esta tabla se enfoca en destacar los modelos ejemplares, avances legislativos, progresos en digitalización, y la implementación de políticas de protección de datos y gobierno electrónico entre estos países.

Tabla 6. Ejercicio comparado para identificar buenas practicas

País	Buenas Prácticas
Uruguay	Modelo ejemplar en la implementación de gobierno electrónico. Políticas efectivas de datos abiertos y accesibilidad. Enfoque integral en la transparencia gubernamental y la participación ciudadana.
Chile	Avances significativos en legislación de protección de datos personales, con enfoque en la transparencia. Iniciativas para mejorar la gobernanza de datos y fomentar la colaboración entre diferentes sectores.
Colombia	Progresos notables en la digitalización y acceso a servicios públicos mediante el uso de tecnologías de información. Enfoque en la transparencia y mejora de la infraestructura de datos para facilitar el acceso ciudadano.

Brasil	Implementación efectiva de la Ley General de Protección de Datos (LGPD), alineada con estándares internacionales como el GDPR. Esfuerzos dirigidos hacia la mejora de la transparencia y la protección de datos personales.
México	Avances en la implementación de políticas de datos abiertos y el desarrollo del gobierno digital. Iniciativas para integrar y proteger los datos a nivel nacional, promoviendo la innovación y la participación ciudadana.

Lecciones Aprendidas

- **Integración y Accesibilidad:** Uruguay demuestra la importancia de una estrategia integrada y accesible en gobierno electrónico, donde la facilidad de acceso a los datos promueve una mayor transparencia y participación ciudadana.
- **Legislación Específica:** Chile resalta la necesidad de avanzar en la legislación específica de protección de datos para asegurar los derechos de los ciudadanos y establecer un marco claro para la gobernanza de datos.
- **Digitalización de Servicios:** La experiencia de Colombia subraya el valor de la digitalización de servicios públicos para mejorar la eficiencia gubernamental y la accesibilidad para los ciudadanos.
- **Protección de Datos:** Brasil ilustra la importancia de adoptar leyes de protección de datos alineadas con estándares internacionales para garantizar la seguridad de la información personal y fortalecer la confianza pública.
- **Datos Abiertos y Gobierno Digital:** México muestra cómo los avances en datos abiertos y gobierno digital pueden fomentar la transparencia y la innovación, destacando la necesidad de políticas que integren y protejan los datos a nivel nacional.

Estas buenas prácticas y lecciones aprendidas reflejan la diversidad de enfoques y desafíos en la gobernanza de datos en América Latina. La colaboración entre países, el intercambio de conocimientos y experiencias, y la adaptación de estrategias exitosas a contextos locales pueden contribuir significativamente al avance de la gobernanza de datos en la región.

En resumen, este ejercicio comparativo revela que, aunque cada país tiene su propio enfoque y desafíos en la gobernanza de datos, hay lecciones comunes y mejores prácticas que pueden ser compartidas y adaptadas a nivel regional. La protección de la privacidad, la transparencia,

la accesibilidad y la calidad de los datos son aspectos clave que todos estos países están abordando de diversas maneras.

Aliados Internacionales y Modelos a Seguir

En el ámbito de la gobernanza de datos, varios países e instituciones internacionales se destacan como modelos a seguir. Estos modelos ofrecen valiosos aprendizajes que pueden ser adaptados y aplicados en contextos como el de Guatemala. En esta sección, se identifican algunos de estos modelos y se analiza cómo pueden ser adaptados a Guatemala, junto con ejemplos de colaboraciones internacionales exitosas.

Países e Instituciones Modelo

La Unión Europea y el GDPR: La Unión Europea ha establecido un estándar global con el Reglamento General de Protección de Datos (GDPR). Este marco se centra en la protección de la privacidad y los derechos de los ciudadanos sobre sus datos personales. Proporciona un ejemplo de cómo un enfoque equilibrado y centrado en el individuo puede mejorar la confianza en el manejo de datos.

Estonia y su Gobierno Digital: Estonia es conocida por su gobierno electrónico avanzado y su enfoque holístico en la gobernanza de datos. El país ha implementado sistemas que permiten a los ciudadanos controlar el acceso a sus datos personales, ofreciendo un modelo de transparencia y participación ciudadana.

Organización para la Cooperación y el Desarrollo Económicos (OCDE): La OCDE ofrece marcos y directrices en la gobernanza de datos, centrados en promover prácticas éticas, seguras y eficientes. Sus recursos y estudios pueden ser una guía valiosa para los países en desarrollo.

Adaptación de Modelos a Guatemala

- **Implementación de Protecciones de Privacidad al Estilo GDPR:** Guatemala podría considerar la implementación de leyes de protección de datos inspiradas en el GDPR, adaptadas a su contexto legal y cultural. Esto implicaría fortalecer las regulaciones existentes sobre datos personales y mejorar los mecanismos de control y cumplimiento.

- **Colaboración con la OCDE y OEA para Desarrollar Políticas de Datos:** Guatemala podría buscar asesoramiento y colaboración con la OCDE y OEA para desarrollar y mejorar sus políticas de gobernanza de datos, aprendiendo de las mejores prácticas y directrices de esta organización.

Casos de Estudio de Colaboraciones Internacionales Exitosas

- **Colaboración UE-América Latina en Datos Abiertos:** Un ejemplo notable es la colaboración entre la Unión Europea y países de América Latina en iniciativas de datos abiertos. Estos proyectos han ayudado a mejorar la transparencia y la participación ciudadana en la región.

- **Cooperación Estonia-Georgia en Gobierno Electrónico:** La colaboración entre Estonia y Georgia en el desarrollo de gobierno electrónico es otro ejemplo exitoso. Estonia ha compartido su experiencia y asesoramiento en la digitalización de servicios públicos, lo que ha llevado a avances significativos en Georgia.

- **Participación de Países en Desarrollo en Foros de la OCDE:** Países en desarrollo, incluyendo varios en América Latina, han participado en foros y talleres de la OCDE, beneficiándose del intercambio de conocimientos y experiencias en políticas de datos y gobernanza.

La adaptación de estos modelos y colaboraciones internacionales a la realidad de Guatemala requiere un enfoque personalizado que considere las especificidades culturales, económicas y políticas del país. Sin embargo, la adopción de estas mejores prácticas y la colaboración con instituciones y países líderes en gobernanza de datos puede proporcionar un camino claro hacia el desarrollo de un sistema de gobernanza de datos robusto y eficiente en Guatemala. Este enfoque no solo mejorará la gestión de los datos, sino que también fomentará la transparencia, la innovación y la participación ciudadana, contribuyendo al desarrollo sostenible y a una sociedad más informada y conectada.

Recomendaciones y Modelos para Guatemala

Para mejorar la gobernanza de datos en Guatemala, es esencial considerar un enfoque holístico que incluya la adopción de mejores prácticas internacionales, la adaptación a las necesidades locales y la implementación de un plan de acción concreto. A continuación, se presentan propuestas específicas, seguidas de una comparación con modelos internacionales y un esquema del plan de acción para su implementación.

Tabla 7. Modelos para Guatemala

Modelo Recomendado	Descripción del Modelo	Aplicabilidad para Guatemala
GDPR de la Unión Europea	Reglamento que establece directrices para la protección de datos personales.	Implementar leyes de protección de datos personales alineadas con estándares internacionales.
Ciudad Inteligente de Singapur	Uso de datos e innovación tecnológica para mejorar la eficiencia urbana.	Desarrollar proyectos de ciudad inteligente en centros urbanos.
Datos Abiertos de Australia	Políticas para hacer los datos gubernamentales accesibles al público.	Promover la apertura y transparencia de datos gubernamentales.
Programas de Alfabetización Digital de Alemania	Iniciativas para mejorar habilidades en análisis y gestión de datos.	Fomentar programas educativos en alfabetización y ética de datos.
Estrategia de Datos de Japón	Enfoque en la innovación y ética en la gestión y uso de datos con IA.	Integrar tecnologías avanzadas en la gestión de datos.
Directrices de la OCDE	Recomendaciones para políticas de datos eficaces a nivel internacional.	Adoptar mejores prácticas globales en la formulación de políticas de datos.
Modelo de Ciberseguridad de Israel	Medidas avanzadas para la protección de datos y gestión de riesgos.	Fortalecer la seguridad de los datos y desarrollar capacidades en ciberseguridad.
Colaboración con Red GEALC	Red de intercambio de conocimientos en gobierno electrónico.	Participar en iniciativas regionales y aprender de las experiencias de otros países de América Latina.

Cooperación con el BID	Asistencia en proyectos de desarrollo y transformación digital.	Buscar financiamiento y asesoramiento técnico para proyectos de gobernanza de datos.

Propuestas Específicas

- **Establecimiento de un Marco Legal Robusto:** Inspirándose en el GDPR de la Unión Europea, Guatemala debe desarrollar y fortalecer su marco legal en torno a la protección de datos. Esto incluiría leyes que regulen la recopilación, uso, divulgación y protección de datos personales.

- **Implementación de Políticas de Datos Abiertos:** Siguiendo el ejemplo de países como Australia, Guatemala debería promover políticas de datos abiertos, haciendo que los datos gubernamentales sean accesibles y utilizables por el público y las empresas.

- **Desarrollo de Infraestructura de Ciudad Inteligente:** Inspirándose en Singapur, se propone el desarrollo de proyectos de ciudad inteligente en áreas urbanas, utilizando datos para mejorar servicios como transporte, salud y seguridad.

- **Fortalecimiento de la Seguridad de Datos y Gestión de Riesgos:** Inspirándose en Israel, Guatemala debe mejorar sus medidas de seguridad de datos y desarrollar estrategias de gestión de riesgos para proteger contra violaciones de datos y ciberataques.

- **Fomento de la Alfabetización en Datos y Capacitación:** Siguiendo el modelo de Alemania, se debe invertir en programas de educación y capacitación para desarrollar habilidades en análisis de datos, gestión de privacidad y ética de datos.

Comparación y Adaptación a las Necesidades Locales

- **Marco Legal:** A diferencia del GDPR, el marco legal en Guatemala debe adaptarse a su contexto específico, considerando factores como el nivel de desarrollo tecnológico y las particularidades culturales.

- **Datos Abiertos:** Mientras que Australia tiene un ecosistema de datos maduro, en Guatemala se debe comenzar con pasos básicos, como la publicación de datos gubernamentales clave y la educación sobre su uso.

- **Ciudad Inteligente:** A diferencia de Singapur, un enfoque gradual sería apropiado para Guatemala, comenzando con proyectos piloto en ciudades específicas.

- **Ética de Datos:** La estructura ética en Guatemala debe considerar los desafíos locales, como la brecha digital y las disparidades socioeconómicas.

- **Seguridad de Datos:** Mientras Israel tiene una avanzada industria de ciberseguridad, Guatemala necesitará inicialmente centrarse en establecer protocolos básicos de seguridad y colaborar con expertos internacionales.

- **Alfabetización en Datos:** A diferencia de Alemania, donde hay un fuerte enfoque en la digitalización, Guatemala debería primero desarrollar programas básicos de alfabetización en datos para funcionarios públicos, educadores y estudiantes.

Plan de Acción para la Implementación

Fase 1: Evaluación y Planificación

- Realizar un diagnóstico de la situación actual de la gobernanza de datos en Guatemala.
- Establecer un comité de expertos para desarrollar un plan estratégico, incluyendo objetivos a corto, mediano y largo plazo.

Fase 2: Desarrollo Legal y Político

- Redactar y promulgar leyes de protección de datos basándose en el marco legal propuesto.
- Iniciar programas de datos abiertos, comenzando con sectores clave como salud y educación.

Fase 3: Implementación y Desarrollo de Infraestructura

- Establecer protocolos de seguridad de datos y comenzar la formación en gestión de riesgos.

Fase 4: Capacitación y Concienciación

- Lanzar programas de alfabetización en datos para funcionarios públicos, educadores y estudiantes.
- Organizar talleres y seminarios sobre ética en la gestión de datos.

Fase 5: Evaluación y Escalado

- Monitorear y evaluar los proyectos implementados, ajustando estrategias según sea necesario.
- Ampliar los programas exitosos a nivel nacional.

Fase 6: Colaboración Internacional y Mejora Continua (Continua)

- Buscar colaboraciones con países y organizaciones internacionales para el intercambio de conocimientos y mejores prácticas. Implementar un ciclo de mejora continua para adaptar y actualizar las estrategias de gobernanza de datos.

La adopción de un modelo de gobernanza de datos eficaz y la implementación de un plan de acción sólido pueden marcar una diferencia significativa en el manejo de la información en Guatemala. A través de la adaptación de las mejores prácticas internacionales a las necesidades locales y la colaboración continua con aliados internacionales, Guatemala puede establecer un marco de gobernanza de datos que no solo mejore la eficiencia y la transparencia, sino que también fomente la innovación y el desarrollo sostenible.

Conclusiones

El análisis de las prácticas de gobernanza de datos a nivel internacional y la exploración de cómo pueden ser adaptadas y aplicadas en Guatemala revelan varios hallazgos clave y ofrecen perspectivas prometedoras para el futuro.

- Importancia de un Marco Legal Robusto: La protección y regulación de datos personales, inspirada en modelos como el GDPR de la UE, es fundamental. Un marco legal sólido es el cimiento sobre el cual se construyen todas las demás prácticas de gobernanza de datos.

- Datos Abiertos y Transparencia: La implementación de políticas de datos abiertos, similar a las de Australia y los Países Bajos, puede mejorar significativamente la transparencia y fomentar la innovación y la participación ciudadana.

- Inversión en Infraestructura Digital y Ciudad Inteligente: Inspirándose en el modelo de Singapur, la inversión en infraestructuras digitales y proyectos de ciudad inteligente puede potenciar la eficiencia de los servicios públicos y mejorar la calidad de vida.

- Ética y Seguridad en la Gestión de Datos: Es esencial establecer marcos éticos y protocolos de seguridad robustos para la gestión de datos, siguiendo ejemplos como los del Reino Unido e Israel.

- Capacitación y Desarrollo de Habilidades: La alfabetización en datos y la capacitación en análisis y ética de datos, basada en el modelo alemán, son cruciales para el desarrollo de un ecosistema de datos sólido.

Perspectivas Futuras para Guatemala

Mirando hacia el futuro, Guatemala tiene la oportunidad de transformar su enfoque de gobernanza de datos, lo cual es esencial para su desarrollo integral. La implementación de un marco legal fuerte y políticas de datos abiertos puede ser el primer paso hacia una sociedad más informada y participativa. El desarrollo de ciudades inteligentes y la inversión en infraestructura digital pueden mejorar la calidad y eficiencia de los servicios públicos. Además, al fomentar una cultura de seguridad de datos y ética, Guatemala puede asegurar un manejo responsable de la información.

Es fundamental que Guatemala no solo adopte estas prácticas, sino que también las adapte a su contexto único. Esto implica considerar factores como la brecha digital, la diversidad cultural y las necesidades específicas de sus ciudadanos. La colaboración internacional y el aprendizaje continuo serán aspectos clave en este proceso.

En conclusión, la gobernanza de datos representa una oportunidad significativa para Guatemala. A través de su implementación cuidadosa y adaptada, Guatemala puede esperar no solo mejoras en la gestión de datos, sino también un avance significativo en su camino hacia el desarrollo sostenible y la inclusión digital. Con el enfoque correcto, la gobernanza de datos puede ser un catalizador para un cambio positivo, mejorando la vida de los ciudadanos y fortaleciendo las instituciones del país.

Bibliografía

- Albrecht, J. P. (2016). How the GDPR will change the world. European Data Protection Law Review, 2(3), 287-289.

- Bertot, J. C., Jaeger, P. T., & Grimes, J. M. (2010). Using ICTs to create a culture of transparency: E-government and social media as openness and anti-corruption tools for societies. GovernmentInformationQuarterly, 27(3), 264-271.

- Centro Internacional de Investigaciones para el Desarrollo (IDRC) de Canadá. (s.f.). Data for Development (D4D). Recuperado de https://www.idrc.ca/en/project/data-for-development-d4d
- DAMA International. (2017). DAMA-DMBOK: Data Management Body of Knowledge (2ª ed.). TechnicsPublications.

- Gobierno de Estonia. (s.f.). Estrategia Digital Nacional de Estonia. Recuperado de https://www.valitsus.ee/en
-
- Gobierno de México. (s.f.). Ley de Protección de Datos Personales en Posesión de los Particulares. Recuperado de https://www.gob.mx/mexico
- Kankanhalli, A., Charalabidis, Y., &Mellouli, S. (2019). Open government data: Towards empirical analysis of open government data initiatives. Government Information Quarterly, 36(4), 101384.

- Khatri, V., & Brown, C. V. (2010). Designing data governance. Communications of the ACM.

- Naciones Unidas. (2019). Informe Mundial sobre la Ciencia de Datos 2019. Recuperado de https://www.un.org/en/sections/issues-depth/data-science/index.html
- Presidência da República. (2018). Lei No 13.709, de 14 de Agosto de 2018, Lei Geral de Protección de Datos Pessoais (LGPD). Recuperado de http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm

- Rosen, J. (2012). The right to be forgotten. Stanford Law Review Online, 64(88), 88-92.

- Unión Europea. (s.f.). Reglamento General de Protección de Datos (GDPR). Recuperado de https://europa.eu/european-union/index_es

- Unión Internacional de Telecomunicaciones (UIT) & UNESCO. (2020). Informe del Estado de la Banda Ancha 2020. Recuperado de https://www.itu.int/en/ITU-D/Statistics/Pages/publications/broadband-report-2020.aspx

- Voigt, P., & Von demBussche, A. (2017). The EU General Data Protection Regulation (GDPR). Springer.

- Weber, K., Otto, B., &Österle, H. (2009). One size does not fit all—a contingency approach to data governance. ACM Journal of Data and Information Quality.

- World Wide Web Foundation. (s.f.). Open Data Barometer. Recuperado de https://opendatabarometer.org/

Anexos

Anexo 1. Presentación de informe: Introducción a modelos de gobernanza de datos v1.2

Anexo 2. Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Unión Europea.

Anexo 3. Ley General de Protección de Datos Personales (LGPD) de Brasil. Gobierno de Brasil.

GUATEMALA
GUATEMALA NO SE DETIENE

Red Ciudadana