Protocolo de Interoperabilidad de Bases de Datos y Metadatos

GOBIERNO NACIONAL
CON PASO FIRME

MINISTERIO
DE CULTURA

ISBN 978-9968-56-111-8

Protocolo de Interoperabilidad de Base de Datos y Metadatos.
Cuenta Satélite de Cultura de Panamá (CSCP)
600-Tecnología (Ciencias Aplicadas)

Primera Versión

Co Edición: Organización del Convenio Andrés Bello (CAB)
Especialistas temáticos:
Angela del Rosario Ardines Ortega y Frank Abel Góndola

Autoridades del Ministerio de Cultura:
María Eugenia Herrera – Ministra de Cultura
Arianne Benedetti – Viceministra
Ivis V. Moreno - Secretaria General
Beatriz Castañet – Directora de Oficina de Asesoría Legal
Maidys Chen – Directora Nacional de Derecho de Autor
Fernando Bolívar – Director de Administración y Finanzas

Equipo de Cuenta Satélite de Cultura:
Jeannette Jacqueline Chenier Ortega -Jefa Encargada de Oficina de Planificación Dhavinia De Mares -Directora Encargada de la Dirección Nacional de Artesanías

Edición y Corrección de estilo:
Diana Rey Vásquez
Marisa Montesano de Talavera

Protocolo de Interoperabilidad de Bases de Datos y Metadatos

PRESENTACIÓN

Cuenta Satélite de Cultura de Panamá (CSCP)

El Ministerio de Cultura de Panamá ha asumido, con determinación, el reto de implementar la Cuenta Satélite de Cultura de Panamá (CSCP), una iniciativa estratégica destinada a medir y visibilizar el impacto económico y social del ecosistema cultural y creativo del país. Esta herramienta permitirá contar, por primera vez, con información continua, estructurada y comparativa sobre el valor que genera la cultura en el desarrollo sostenible de la nación.

Para asegurar el éxito de este ambicioso proyecto, MiCultura ha confiado en la experiencia de la Organización del Convenio Andrés Bello (CAB), pionera en la creación de la metodología de Cuenta Satélite de Cultura (CSC) desde 2009. La colaboración se formalizó mediante el Acuerdo Específico de Colaboración No.001-2023, que sienta las bases de una alianza técnica de gran alcance entre ambas instituciones.

La implementación de la CSCP también incluye el desarrollo del “Protocolo de Interoperabilidad de Bases de Datos y Metadatos”, un marco técnico que garantiza altos estándares de confidencialidad, seguridad y calidad en el manejo de datos personales, monetarios y no monetarios, de acuerdo con la normativa vigente en la República de Panamá. Este protocolo es clave para facilitar la cooperación entre instituciones involucradas y asegurar la integridad de los procesos estadísticos que acompañarán la ejecución de la cuenta.

Con esta acción, Panamá da un paso firme hacia la consolidación de políticas culturales basadas en evidencia, fortaleciendo el vínculo entre cultura, economía y desarrollo. La Cuenta Satélite de Cultura de Panamá permitirá visibilizar y respaldar con datos la creatividad, diversidad y productividad artística del país, aportando al diseño de estrategias más eficaces para el bienestar de las comunidades y la economía cultural panameña.

María Eugenia Herrera
Ministra de Cultura

ÍNDICE

INTRODUCCIÓN

El Protocolo de interoperabilidad de bases de datos y metadatos tiene como objetivo orientar todas las acciones de generación, procesamiento, análisis y divulgación de información recopilada por el proyecto de la Cuenta Satélite de Cultura de Panamá (CSCP), con mira a garantizar el correcto manejo de los datos personales, su seguridad y secreto estadístico.

Para estos efectos, este Protocolo define los lineamientos normativos que deben seguir los procesos de investigación sobre el manejo de da datos personales, bases de datos estadísticos e información no monetaria; así como, los criterios técnicos que deberá tener en cuenta la construcción e implementación del Sistema Interactivo de las Estadísticas Culturales de Panamá.

Las recomendaciones incluidas en este Protocolo facilitan la identificación de los criterios legales para los acuerdos de confidencialidad y cooperación técnica entre el Ministerio de Cultura, el Instituto Nacional de Estadísticas y Censos (INEC) y organizaciones públicas y privadas del país que deseen ofrecer información monetaria y no monetaria sobre establecimientos (culturales y no culturales) dentro del territorio nacional para la estimación de la CSCP. Dichas recomendaciones están incluidas en el Anexo 1.

Este Protocolo está estructurado, por lo tanto, en tres grandes apartados. El primer apartado se refiere a los lineamientos normativos que deben seguir los procesos de investigación. El segundo apartado se refiere a los criterios para el Sistema de Interactivo de las Estadísticas Culturales. Finalmente, y el tercer apartado, corresponde a un análisis detallado de la legislación de la República de Panamá sobre protección de tratamiento de datos personales, encaminados a garantizar que los convenios que van a celebrarse en torno a la Cuenta Satélite de Cultura cumplan a cabalidad las mismas

A. LINEAMIENTOS PARA EL MANEJO DE DATOS PERSONALES POR PARTE DE LA CSCP

En Panamá existen diversas leyes y normas que regulan el registro de accesos y auditoría a los datos. La más importante es la Ley 81 de 2019 sobre Protección de Datos Personales, la cual establece que los responsables del tratamiento de datos personales deben implementar medidas técnicas y organizativas adecuadas para garantizar la seguridad de los datos personales, incluyendo la auditoría de los accesos a los datos.

Antes de precisar los criterios técnicos para el tratamiento de datos por parte de las diversas investigaciones en el marco de la Cuenta Satélite de Cultura en Panamá, es fundamental resumir los principales lineamientos contenidos en las normas panameñas de protección de datos. Si bien, los detalles de la normatividad panameña están contenidos en el apartado de Anexos, el siguiente subtítulo presenta un marco introductorio al respecto.

1. Normas Rectoras

La Ley 81 de marzo de 2019, tal como se incorpora en el Anexo B, establece los principios denominados ARCO (Acceso, Rectificación, Cancelación y Oposición) reconocidos como derechos irrenunciables básicos que tienen los titulares de datos personales y que pueden ser ejercidos en todo momento por este). (ANEXO B, artículo 15). En este sentido, también como un derecho ARCO, se incluye el Derecho de Potabilidad: derecho a obtener una copia de los datos personales (ANEXO B, Artículo 15 ordinal 5).

La principal condición que se debe tener en cuenta al momento del tratamiento de dato es el consentimiento (ANEXO A, artículo 6, ordinal 1), y la persona que consiente debe ser informada del propósito del uso de sus datos personales. Bajo estos términos, corresponde al responsable del tratamiento de datos personales contenidos en base de datos crear los protocolos, procesos y procedimientos de gestión y transferencia segura, protegiendo los derechos de los titulares (ANEXO B artículo 7).

Esta labor será fiscalizada y supervisada por la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI). La Ley (ANEXO B) crea un ente consultivo: Consejo de Protección de Datos Personales, conformado por diferentes instituciones del Estado y organismos (ANEXO B artículo 34 y 35), que tiene entre sus funciones asesorar a la ANTAI, en materia de protección de datos, recomendar acciones y reglamentaciones.

a. Sanciones administrativas

La ANTAI, a través del Oficial de Protección de Datos creado en la Ley 33 de 2013 (que crea la autoridad), es la facultada para sancionar a la persona natural o jurídica responsable del tratamiento de los datos personales (ANEXO B artículo 36), así como el custodio de la base datos (ANEXO C, Artículos 46 y 47).

De acuerdo con la normatividad, existen diversas categorías de infracciones y sanciones están contenidas en la Ley 81 de 26 de marzo de 2019 artículo 38 y siguientes (ANEXO B artículos 38 y siguientes). Se consideran infracciones leves aquellas relativas a:

- No remitir y/o informar a la Autoridad Nacional de Transparencia y Acceso a la Información dentro de los plazos requeridos la información de lo ordenado en esta Ley, su reglamentación o cualquier otra disposición normativa. (ANEXO B Artículo 39)

Se consideran infracciones graves:

- Efectuar el tratamiento de datos personales sin haber obtenido el consentimiento de su titular, según el procedimiento indicado por esta Ley, su reglamentación o cualquier otra disposición normativa que se refiera a la presente Ley.
- Infringir los principios y garantías establecidos en la presente Ley o en su reglamentación.
- Infringir el compromiso de confidencialidad relacionado al tratamiento de los datos personales.
- Restringir o entorpecer la aplicación de los derechos de acceso, rectificación, cancelación y oposición.
- Incumplir el deber de informar al titular afectado acerca del tratamiento de sus datos personales, cuando los datos no hayan sido obtenidos del propio titular.

- Almacenar o archivar datos personales sin contar con las adecuadas condiciones de seguridad que esta Ley o su reglamento disponga.
- No atender la reiteración de los requerimientos u observaciones formalmente notificados, o no proporcionar la documentación o información formalmente solicitada por la Autoridad Nacional de Transparencia y Acceso a la Información.
- Entorpecer o no cooperar con la Autoridad Nacional de Transparencia y Acceso a la Información al momento en que esta ejerza su función de inspección. (ANEXO B, Artículo 40). Se consideran infracciones muy graves.
- Recopilar de datos personales en forma dolosa.
- No observar de las regulaciones establecidas respecto al tratamiento de los datos sensibles.
- No suspender el tratamiento de datos personales cuando existiera un previo requerimiento de la Autoridad Nacional de Transparencia y Acceso a la Información para ello.
- Almacenar o transferir internacionalmente datos personales, violentando lo establecido en esta Ley.
- Reincidir en las faltas graves. (ANEXO B Artículo 41).

Las sanciones que imponga la Autoridad Nacional de Transparencia y Acceso a la Información a los responsables de las bases de datos y demás sujetos alcanzados por el régimen de la presente ley y sus reglamentos, se graduarán dependiendo de la gravedad de la infracción cometida. (ANEXO B Artículo 42).

Las infracciones a la Ley son sancionadas de conformidad a lo que establece el artículo 43. De acuerdo a este, la falta leve se da por citación ante la Autoridad Nacional de Transparencia y Acceso a la Información con relación a registros o atender faltas. Las faltas graves dan lugar a multas según su proporcionalidad; mientras que, las faltas muy graves conducen a la clausura de los registros de la base de datos, sin perjuicio de la multa correspondiente. Para ejecutar esta acción, la Autoridad Nacional de Transparencia y Acceso a la Información deberá contar con la opinión formal del Consejo de Protección de Datos Personales, sin perjuicio de los recursos que esta Ley le concede al afectado

Así mismo, esta categoría de faltas da lugar a la suspensión e inhabilitación de la actividad de almacenamiento y/o tratamiento de datos personales de forma temporal permanente, sin perjuicio de la multa correspondiente.

Se considerará reincidencia cuando la misma falta se repita dentro de un periodo de tres años. Para hacer cumplir la sanción de suspensión o clausura, la Autoridad Nacional de Transparencia y Acceso a la Información podrá requerir el auxilio de la Fuerza Pública. Los hechos que acarreen una sanción serán documentados de acuerdo con las formalidades legales y se realizarán informes estadísticos que permitan a la Autoridad Nacional de Transparencia y Acceso a la Información establecer la gravedad, reiteración o reincidencia de la infracción cometida. (ANEXO B Artículo 43).

b. Sanciones Penales

El Código Penal de la República de Panamá establece en su Título VIII, los "Delitos contra la seguridad jurídica de los medios electrónicos" y en su Capítulo I, regula los "Delitos contra la seguridad informática", los cuales suponen según el: "Artículo 289. Quien indebidamente ingrese o utilice una base de datos, red o sistema informático será sancionado con dos a cuatro años de prisión.

Artículo 290. Quien indebidamente se apodere, copie, utilice o modifique los datos en tránsito o contenidos en una base de datos o sistema informático, o interfiera, intercepte, obstaculice o impida su transmisión será sancionado con dos a cuatro años de prisión.

Estas sanciones se aplicarán sin perjuicio de las sanciones aplicables si los datos de que trata el presente capítulo consisten en información confidencial de acceso restringido, referente a la seguridad del Estado, según lo dispuesto en el Capítulo I, Título XIV, del Libro Segundo de este Código. Artículo 292. Si las conductas descritas en el presente Capítulo las comete la persona encargada o responsable de la base o del sistema informático, o la persona autorizada para acceder a este, o las cometió utilizando información privilegiada, la sanción se agravará entre una sexta y una tercera parte.

2. Auditoría y registro de accesos a los datos

Existen diversos beneficios de la auditoría y el registro de accesos a los datos, entre los que se destacan:

- Mejora la seguridad de la información: La auditoría y el registro de accesos a los datos pueden ayudar a detectar actividades sospechosas y prevenir fraudes o filtraciones de datos.
- Demuestra el cumplimiento de las leyes y normas: La auditoría y el registro de accesos a los datos pueden ayudar a las organizaciones a demostrar que cumplen con las leyes y normas relacionadas con la protección de datos personales.
- Mejora la responsabilidad: La auditoría y el registro de accesos a los datos pueden ayudar a las organizaciones a identificar a los responsables de accesos no autorizados a los datos.

Existen diversas herramientas disponibles para la auditoría y el registro de accesos a los datos. Algunas de las herramientas más comunes incluyen:

- Registros de auditoría: Los registros de auditoría registran toda la actividad que se realiza en un sistema, como los inicios de sesión, los accesos a archivos y las modificaciones a los datos.
- Herramientas de monitoreo: Las herramientas de monitoreo permiten a las organizaciones monitorear la actividad en tiempo real y detectar actividades sospechosas.
- Herramientas de análisis de registros: Las herramientas de análisis de registros permiten a las organizaciones analizar los registros de auditoría y detectar patrones o tendencias que pueden indicar actividades sospechosas.

Las siguientes son algunas recomendaciones para la implementación de la auditoría y el registro de accesos a los datos en Panamá:

- Definir una política de auditoría y registro de accesos a los datos: La política debe definir qué datos se deben auditar y registrar, quién debe tener acceso a los registros de auditoría y cómo se deben almacenar y proteger los registros de auditoría.
- Implementar herramientas de auditoría y registro de accesos a los

datos: Las herramientas deben ser adecuadas para el tamaño y la complejidad de la organización.

- Privacidad de los datos: Obtención del consentimiento informado de los titulares de los datos personales para su recolección y tratamiento.

a. Elementos del consentimiento informado

El consentimiento informado debe reunir los siguientes elementos: (i) Capacidad: El titular de los datos personales debe tener la capacidad legal para otorgar su consentimiento; (ii) Información: El responsable del tratamiento de datos personales debe proporcionar al titular información clara, precisa y completa sobre los siguientes aspectos:

- la identidad y datos de contacto del responsable del tratamiento
- la finalidad del tratamiento de los datos personales,
- los datos personales que se van a recolectar y tratar,
- el plazo previsto para la conservación de los datos personales;
- los derechos del titular de los datos personales, incluyendo el derecho de acceso, rectificación, supresión, limitación del tratamiento, oposición al tratamiento y portabilidad de los datos.
- Los riesgos que pueden derivarse del tratamiento de los datos personales.

Importante considerar que el consentimiento debe ser otorgado libremente, sin coacción ni presión. El consentimiento debe ser específico para cada tratamiento de datos personales. El consentimiento debe ser inequívoco, es decir, el titular de los datos personales debe saber claramente a qué está consintiendo. El consentimiento debe ser otorgado de forma expresa o mediante un acto afirmativo.

Medios para obtener el consentimiento informado.
El consentimiento informado puede obtenerse de diversas formas, como, por ejemplo:

- Formulario escrito: El responsable del tratamiento puede proporcionar al titular un formulario escrito en el que se explique la información sobre el tratamiento de datos personales y se solicite su consentimiento.
- Casilla de verificación en línea: El responsable del tratamiento puede incluir una casilla de verificación en su sitio web o aplicación en la que el titular pueda marcar su consentimiento para el tratamiento de sus datos personales.
- Llamada telefónica: El responsable del tratamiento puede obtener el consentimiento del titular por teléfono, siempre que se grabe la conversación y se proporcione al titular una copia de la grabación.

Conservación del consentimiento informado: El responsable del tratamiento de datos personales debe conservar una prueba del consentimiento informado durante todo el período de tratamiento de los datos personales. Las siguientes son algunas recomendaciones para obtener el consentimiento informado de los titulares de los datos personales en Panamá:

- Desarrollar una política de obtención del consentimiento informado: La política debe definir los procedimientos para obtener el consentimiento informado de los titulares de los datos personales, de acuerdo con los requisitos de la Ley 81 de 2019.
- Proporcionar información clara y precisa al titular: El responsable del tratamiento debe proporcionar al titular información clara, precisa y completa sobre el tratamiento de sus datos personales.
- Obtener el consentimiento de forma libre y específica: El consentimiento debe ser otorgado libremente y de forma específica para cada tratamiento de datos personales.
- Conservar una prueba del consentimiento informado: El responsable del tratamiento debe conservar una prueba

del consentimiento informado durante todo el período de tratamiento de los datos personales.

Limitación del uso de los datos a los fines específicos para los que fueron recolectados. El responsable del tratamiento de datos personales debe adoptar las medidas necesarias para garantizar el cumplimiento del principio de limitación del tratamiento de datos personales. Estas medidas incluyen:

- Definir claramente las finalidades para las que se recolectan los datos personales.
- Informar al titular de los datos sobre las finalidades del tratamiento.
- Obtener el consentimiento expreso del titular de los datos cuando sea necesario.
- Implementar medidas de seguridad para proteger los datos personales.
- Limitar el acceso a los datos personales a las personas que necesiten conocerlos para las finalidades del tratamiento.

Las siguientes son algunas recomendaciones para el responsable del tratamiento de datos personales para garantizar el cumplimiento del principio de limitación del tratamiento de datos personales:

- Desarrollar una política de tratamiento de datos personales que defina las finalidades para las que se recolectan los datos personales y los procedimientos para obtener el consentimiento del titular de los datos.
- Capacitar al personal del responsable del tratamiento sobre el principio de limitación del tratamiento de datos personales.
- Implementar medidas de seguridad para proteger los datos personales.
- Realizar auditorías periódicas para verificar el cumplimiento del principio de limitación del tratamiento de datos personales.
- Permitir a los titulares de los datos personales el acceso, rectificación, cancelación y oposición al tratamiento de sus datos.

b. Derechos de los titulares de datos personales

La Ley 81 de 2019 sobre Protección de Datos Personales en Panamá establece el derecho de los titulares de datos personales a acceder a sus datos, rectificarlos, cancelarlos y oponerse a su tratamiento. Estos derechos, conocidos como derechos ARCO, son fundamentales para garantizar el control de los individuos sobre sus datos personales y proteger su privacidad.

- Obtener información sobre el tratamiento de sus datos personales: Esto incluye saber quién es el responsable del tratamiento, para qué fines se tratan los datos, qué datos se tratan, a quién se comunican los datos, y durante cuánto tiempo se conservarán los datos.
- Acceder a sus datos personales: El titular tiene derecho a obtener una copia de sus datos personales.
- Derecho de rectificación: El titular de los datos personales tiene derecho a solicitar la rectificación de sus datos personales: Esto significa que el titular puede pedir que se corrijan los datos personales que sean inexactos o incompletos.
- Obtener la rectificación de sus datos personales sin demora indebida: El responsable del tratamiento debe actuar sobre la solicitud de rectificación sin demora indebida.
- Derecho de cancelación: El titular de los datos personales tiene derecho a solicitar la cancelación de sus datos personales. Esto significa que el titular puede pedir que se eliminen sus datos personales. Obtener la cancelación de sus datos personales sin demora indebida: El responsable del tratamiento debe actuar sobre la solicitud de cancelación sin demora indebida.
- Derecho de oposición al tratamiento: El titular de los datos personales tiene derecho a oponerse al tratamiento de sus datos personales. Esto significa que el titular puede pedir que se deje de tratar sus datos personales.
- Obtener que se deje de tratar sus datos personales sin demora indebida: El responsable del tratamiento debe dejar de tratar los datos personales del titular cuando este se oponga a dicho tratamiento.
- Ejercicio de los derechos ARCO: El titular de los datos personales

puede ejercer sus derechos ARCO mediante la presentación de una solicitud al responsable del tratamiento. La solicitud debe ser por escrito y debe incluir la siguiente información:

- Nombre y apellidos del titular.
- Documento de identidad del titular.
- Domicilio del titular.
- Datos de contacto del titular (correo electrónico y/o teléfono).
- Solicitud concreta que se realiza (acceso, rectificación, cancelación u oposición).
- Motivos de la solicitud (en caso de rectificación, cancelación u oposición)

El responsable del tratamiento debe responder a la solicitud del titular en el plazo de un mes a partir de su recepción. La respuesta debe ser por escrito y debe informar al titular sobre si se ha estimado o no su solicitud.

c. Medidas para garantizar la confidencialidad de los datos

Existen diversas medidas que el responsable del tratamiento de datos personales puede implementar para garantizar la confidencialidad de los datos, como, por ejemplo:

- Control de acceso: Limitar el acceso a los datos personales a las personas que necesiten conocerlos para las finalidades del tratamiento.
- Seguridad de la información: Implementar medidas de seguridad física y lógica para proteger los datos personales, por ejemplo, el uso de contraseñas seguras, el cifrado de datos y el control de accesos físicos a los lugares donde se almacenan los datos.
- Sensibilización y formación: Capacitar al personal del responsable del tratamiento sobre la importancia de la confidencialidad de los datos y las medidas que se deben tomar para protegerla.
- Procedimientos de seguridad: Establecer procedimientos de seguridad para el tratamiento de datos personales, por ejemplo, los procedimientos para la gestión de incidencias de seguridad.
- Evaluación y auditoría: Evaluar periódicamente la eficacia de las

medidas de seguridad implementadas y realizar auditorías para verificar el cumplimiento de la normativa de protección de datos personales.

Las siguientes son algunas recomendaciones para el responsable del tratamiento de datos personales para garantizar la confidencialidad de los datos:

- Realizar un análisis de riesgos para identificar los riesgos potenciales para la confidencialidad de los datos.
- Implementar las medidas de seguridad necesarias para mitigar los riesgos identificados.
- Documentar las medidas de seguridad implementadas. • Capacitar al personal del responsable del tratamiento sobre la importancia de la confidencialidad de los datos y las medidas que se deben tomar para protegerla.
- Realizar auditorías periódicas para verificar el cumplimiento de la normativa de protección de datos personales.

d. Medidas para garantizar la calidad de los datos

Para asegurar la exactitud, integridad y consistencia de los datos, las organizaciones pueden implementar las siguientes medidas:

- Establecer procedimientos para la recolección de datos: (i) Definir claramente qué datos se van a recolectar y cómo se van a recolectar; (ii) Implementar medidas de control para garantizar que los datos recolectados sean exactos y completos.

- Implementar mecanismos para la validación de datos: (i) Utilizar herramientas de validación de datos para identificar y corregir errores en los datos. (ii) Realizar revisiones manuales de los datos para verificar su exactitud.

- Establecer procedimientos para la actualización de datos: (i) Definir cuándo y cómo se deben actualizar los datos. (ii) Implementar mecanismos para automatizar la actualización de datos.

- Implementar mecanismos para la corrección de errores en los datos: (i) Definir un proceso para la identificación y corrección de errores en los datos. (ii) Permitir a los titulares de datos solicitar la corrección de sus datos personales.

- Establecer procedimientos para la eliminación de datos: (i) Definir cuándo y cómo se deben eliminar los datos. (ii) Implementar mecanismos para garantizar que los datos eliminados no sean recuperables.

Las siguientes son algunas recomendaciones para las organizaciones en Panamá para asegurar la calidad de los datos:

- Desarrollar una política de calidad de datos que defina los principios y las responsabilidades para la gestión de la calidad de los datos.
- Capacitar al personal de la organización sobre la importancia de la calidad de los datos y las medidas que se deben tomar para garantizarla.
- Implementar herramientas de gestión de calidad de datos.
- Realizar auditorías periódicas para verificar la calidad de los datos.

e. Medidas para garantizar la Accesibilidad de la información

El acceso a la información es un derecho fundamental consagrado en la Constitución Política de la República de Panamá y en diversas leyes, incluyendo la Ley 6 de 2002 de Transparencia y Acceso a la Información Pública. Este derecho implica que las personas tienen derecho a acceder a la información pública que generan las entidades del Estado.

La Ley 6 de 2002 de Transparencia y Acceso a la Información Pública establece que las entidades del Estado deben facilitar el acceso a la información pública de forma clara, transparente y oportuna. Esto significa que la información debe ser:

- Clara: Fácil de entender para cualquier persona,

independientemente de su conocimiento técnico o jurídico.
• Transparente: Disponible de forma abierta y sin restricciones innecesarias.
• Oportuna: Entregada en un plazo razonable.
• Facilitar el acceso a la información de forma clara, transparente y oportuna.

Las entidades del Estado pueden facilitar el acceso a la información de forma clara, transparente y oportuna mediante la implementación de las siguientes medidas:

• Publicación de información en un sitio web:
  · Publicar la información pública en un sitio web de fácil acceso y navegación.
  · Mantener el sitio web actualizado con la información más reciente.
  · Utilizar un lenguaje claro y sencillo en la redacción de la información.

• Implementación de mecanismos para la solicitud de información: · Establecer mecanismos claros y sencillos para la solicitud de información pública.
  · Responder a las solicitudes de información en un plazo razonable.
  · Proporcionar la información solicitada en un formato adecuado para el solicitante.

• Implementación de mecanismos para la consulta y descarga de datos:
  · Permitir la consulta y descarga de datos públicos en formatos abiertos y accesibles.
  · Implementar mecanismos para la búsqueda y filtrado de datos.
  · Proporcionar documentación sobre los datos públicos disponibles.

• Garantía de la compatibilidad de los datos con diferentes formatos y estándares:
  · Utilizar formatos de datos abiertos y estándares para la

publicación de información pública.
· Proporcionar herramientas para la conversión de datos a diferentes formatos.
· Facilitar la interoperabilidad de los datos públicos con otros sistemas de información.

3. Criterios técnicos para Manejo de los Datos

Este título abarca la definición del tipo de datos a compartir, los mecanismos para su intercambio, los formatos de los datos, las medidas de seguridad, así como el Protocolo en Caso de Fuga de Información y el Plan de Contingencia.

Capítulo I. Mecanismos de Intercambio de Datos

Este Protocolo de Interoperabilidad define las siguientes tres opciones para el intercambio de datos:

- Plataforma de intercambio de datos: El Sistema Interactivo de las Estadísticas Culturales constituirá la principal herramienta para el intercambio de datos entre las entidades involucradas.
- Intercambio de archivos: El intercambio de datos podría realizarse mediante el intercambio de archivos en formatos estandarizados. • APIs: Se podrían desarrollar APIs que permitan a las entidades acceder a los datos de otras entidades de manera automatizada.

Independientemente de las opciones que se utilicen, será fundamental precisar la frecuencia de intercambio de datos, considerando la naturaleza de los datos y las necesidades de los usuarios. Así mismo, las partes que acuerden el intercambio deberán gestionar las versiones de datos a través del establecimiento de mecanismos claros que aseguren la trazabilidad y la coherencia de la información. De igual forma, entre las partes deberán estar claras las medidas de seguridad para proteger los datos durante su intercambio y almacenamiento, y finalmente, los procedimientos para garantizar la calidad de los datos intercambiados, incluyendo su precisión, integridad y consistencia.

Capítulo II. Formatos de Datos

Se utilizarán formatos de datos abiertos y estandarizados para facilitar

la interoperabilidad y reutilización de la información.

Algunos formatos de datos recomendados incluyen:

• CSV (Comma Separated Values): Un formato de archivo simple y ampliamente utilizado para almacenar datos tabulares. • JSON (JavaScript Object Notation): Un formato de intercambio de datos ligero y basado en texto que es fácil de leer y procesar por máquinas.

- XML (Extensible Markup Language): Un lenguaje de marcado basado en texto que permite estructurar y codificar datos de manera flexible.
- SDMX (Statistical Data and Metadata eXchange): Un estándar internacional para el intercambio de datos estadísticos y metadatos.

Se utilizarán protocolos de comunicación seguros y confiables para el intercambio de datos. Algunos protocolos recomendados incluyen:

- HTTP (Hypertext Transfer Protocol): Un protocolo de red sin estado que se utiliza para transferir datos entre servidores y clientes web.
- HTTPS (Hypertext Transfer Protocol Secure): Una versión segura de HTTP que utiliza cifrado para proteger la confidencialidad e integridad de los datos.
- FTP (File Transfer Protocol): Un protocolo de red para la transferencia de archivos entre computadoras.
- SFTP (Secure FTP): Una versión segura de FTP que utiliza cifrado para proteger la confidencialidad e integridad de los archivos transferidos.

El manejo de este tipo de datos requiere que se cuente con una infraestructura de servidores que permita cuatro condiciones a saber:

- Escalabilidad: La infraestructura debe ser capaz de soportar el crecimiento futuro del sistema en términos de usuarios, datos y procesamiento.
- Rendimiento: El sistema debe ser capaz de responder a las solicitudes de los usuarios de manera rápida y eficiente.

• Disponibilidad: El sistema debe estar disponible para los usuarios la mayor cantidad de tiempo posible.
• Seguridad: El sistema debe proteger los datos contra accesos no autorizados, modificaciones o destrucciones.

Capítulo III. Formato de Datos Institucionales

Las entidades participantes podrán solicitar datos a otras entidades a través de un mecanismo establecido, como un portal web o una API. La solicitud de datos deberá incluir la siguiente información:

• Identificador de la entidad solicitante: Identifica a la entidad que solicita los datos.
• Identificador de la entidad proveedora: Identifica a la entidad que posee los datos solicitados.
• Descripción de los datos solicitados: Especifica los tipos de datos que se solicitan, incluyendo variables, indicadores y periodos de tiempo.
• Formato de los datos solicitados: Indica el formato en que se desean recibir los datos (CSV, JSON, XML, etc.).
• Propósito de la solicitud de datos: Explica el uso que se dará a los datos solicitados.

La entidad proveedora de datos entregará los datos solicitados a la entidad solicitante a través del mecanismo establecido. La entrega de datos deberá cumplir con los siguientes requisitos:

• Oportunidad: Los datos se entregarán en un plazo de tiempo razonable, de acuerdo con la complejidad de la solicitud.
• Completitud: Los datos entregados incluirán toda la información solicitada por la entidad solicitante.
• Precisión: Los datos entregados serán precisos y confiables.
• Consistencia: Los datos entregados serán consistentes con otras fuentes de información.
• Formato: Los datos se entregarán en el formato solicitado por la entidad solicitante.

En caso de que surjan problemas durante el intercambio de datos, se implementará un mecanismo de resolución de problemas que permita:

- Identificar el problema: Determinar la causa del problema, ya sea un error en la solicitud de datos, un problema en la entrega de datos o un error en la interpretación de los datos.
- Comunicar el problema: Informar a las entidades involucradas sobre el problema identificado.
- Analizar el problema: Investigar las causas del problema y determinar las soluciones posibles.
- Implementar la solución: Aplicar la solución elegida para resolver el problema.
- Monitorear la solución: Verificar que la solución implementada haya resuelto el problema de manera efectiva.

Capítulo IV. Mecanismos de Seguridad

Se implementarán mecanismos de seguridad robustos para proteger la información durante su intercambio y almacenamiento. Algunos mecanismos de seguridad recomendados incluyen:

- Cifrado de datos: Se utilizarán algoritmos de cifrado para proteger la confidencialidad de los datos durante su transmisión y almacenamiento.
- Autentificación y autorización: Se implementarán mecanismos para verificar la identidad de las entidades que participan en el intercambio de datos y para controlar el acceso a la información.
- Firmas digitales: Se utilizarán firmas digitales para garantizar la integridad y autenticidad de los datos intercambiados.
- Auditorías de seguridad: Se realizarán auditorías de seguridad periódicas para detectar y prevenir vulnerabilidades en el sistema de intercambio de datos.

La adopción de estas medidas debe efectuarse garantizando que sea posible la compatibilidad con versiones anteriores de los formatos de datos y protocolos de comunicación para facilitar la migración de sistemas existentes. Así mismo, el proceso debe estar plenamente

documentado y claro en función de los estándares técnicos utilizados, incluyendo especificaciones técnicas, guías de implementación y ejemplos de código. Y finalmente, debe brindarse capacitación a las entidades participantes sobre el uso de los estándares técnicos establecidos.

Capítulo V. Encriptación de Datos en Reposo y en Tránsito en Panamá

La encriptación es una técnica fundamental para proteger la información confidencial, tanto cuando se almacena en dispositivos (en reposo) como cuando se transmite a través de redes (en tránsito). En Panamá, existen diversas leyes y normas que regulan la encriptación de datos y establecen los requisitos para su implementación. La encriptación de datos es importante por las siguientes razones:

- Confidencialidad: Protege los datos de accesos no autorizados, asegurando que solo las personas autorizadas puedan leerlos.
- Integridad: Protege los datos de modificaciones no autorizadas, garantizando que no se alteren durante su almacenamiento o transmisión.
- No repudio: Permite verificar la identidad del origen de los datos y evitar que se niegue su envío o recepción.

Tipos de encriptación: Existen dos tipos principales de encriptación. La simétrica que utiliza una misma clave para cifrar y descifrar los datos. Así como, la encriptación asimétrica que utiliza dos claves diferentes, una pública para cifrar y una privada para descifrar.

Igualmente, puede haber una encriptación de datos en reposo que se utiliza para proteger los datos que se almacenan en dispositivos como discos duros, unidades USB y servidores. Existen diversos algoritmos de encriptación que se pueden utilizar para cifrar datos en reposo, como AES, RSA y Blowfish. También está la encriptación de datos en tránsito que se transmiten a través de redes, como Internet o redes privadas. El protocolo más común para la encriptación de datos en tránsito es TLS/SSL (Transport Layer Security/Secure Sockets Layer).

Capítulo VI. Protocolo en Caso de Fuga de Información y Plan de Contingencia

Una fuga de información de la base de datos puede tener un impacto significativo en una organización, tanto en términos financieros como de reputación. Es importante contar con un protocolo para responder a este tipo de incidente de manera rápida y efectiva. El plan de contingencia debe incluir los siguientes elementos:

- Equipo de respuesta a incidentes: El equipo de respuesta a incidentes debe estar integrado por representantes de diferentes áreas de la organización, como TI, legal, recursos humanos y comunicaciones.
- Procedimientos de respuesta: Los procedimientos de respuesta deben describir los pasos que se deben seguir para identificar, contener, erradicar y recuperarse de un incidente cibernético.
- Comunicaciones: El plan de contingencia debe incluir un plan de comunicaciones para informar a los empleados, clientes y otras partes interesadas sobre un incidente cibernético.
- Pruebas y ejercicios: El plan de contingencia debe probarse y actualizarse regularmente para asegurarse de que sea efectivo.

Entre los procedimientos a considerar debe estipularse los siguientes:

a. Detección: Monitoreo continuo de la actividad de la base de datos: Es importante monitorear la actividad de la base de datos de manera continua para detectar actividades inusuales que podrían indicar una fuga de información.
b. Análisis de registros: Los registros de la base de datos deben analizarse regularmente para identificar posibles accesos no autorizados o intentos de fuga de información.
c. Alertas de sistemas de detección de intrusiones: Se deben implementar sistemas de detección de intrusiones para detectar y alertar sobre posibles fugas de información.
d. Contención: Aislar la base de datos afectada: Si se detecta una fuga de información, es importante aislar la base de datos afectada para evitar que el malware se propague.
e. Restringir el acceso a la base de datos: Se debe restringir el acceso a la base de datos afectada para evitar que más

personas accedan a la información comprometida.

f. Cambiar las contraseñas: Se deben cambiar las contraseñas de acceso a la base de datos afectada.

g. Investigación: Determinar el alcance de la fuga: Es importante determinar qué información se ha fugado y cómo se ha producido la fuga.

h. Identificar a los responsables: Se debe intentar identificar a los responsables de la fuga.

i. Preservar la evidencia: Se debe preservar toda la evidencia relacionada con la fuga para fines de investigación.

j. Comunicación: Notificar a las personas afectadas: Si la fuga de información ha comprometido datos personales, se debe notificar a las personas afectadas de acuerdo con las leyes de protección de datos aplicables. Ello implica comunicar el incidente a las autoridades: Si la fuga de información ha comprometido información confidencial o sensible, se debe comunicar el incidente a las autoridades. Así mismo, comunicar el incidente a los medios de comunicación: Si la fuga de información ha tenido un impacto significativo en la organización, se debe comunicar el incidente a los medios de comunicación de manera transparente y responsable.

k. Recuperación: Restaurar la base de datos: Una vez que se haya contenido la fuga, se debe restaurar la base de datos afectada.

l. Mejorar las medidas de seguridad:
Se deben implementar medidas de seguridad adicionales para evitar que se produzcan futuras fugas de información.

m. Prevención. Mantener las medidas de seguridad actualizadas: Las medidas de seguridad deben actualizarse regularmente para protegerse contra las últimas amenazas.

n. Capacitar a los empleados: Los empleados deben recibir capacitación continua sobre seguridad de la información.

o. Realizar pruebas de penetración: Se deben realizar pruebas de penetración regularmente para identificar y corregir vulnerabilidades en los sistemas de la organización.

B. CRITERIOS PARA LA IMPLEMENTACIÓN DEL SISTEMA INTERACTIVO DE LAS ESTADÍSTICAS CULTURALES DE PANAMÁ.

Para la construcción del software del Sistema Interactivo de las Estadísticas Culturales, es necesario definir un conjunto de criterios claros que guíen su desarrollo. El principal antecedente legal en este contexto es el Decreto Ejecutivo 285 del 28 de mayo de 2021, que reglamenta la Ley 81 del 2019 de Protección de Datos Personales, estableciendo los principios, derechos, obligaciones y procedimientos para la protección de datos personales en Panamá[1].

Este capítulo define los criterios técnicos que deberá cumplir el software para el Sistema Interactivo de las Estadísticas Culturales, así como los mecanismos de intercambio de datos, mecanismos de seguridad, mecanismos de intercambio de datos, el formato de los datos.

Capitulo VII. Marco Legal con referencia a los criterios legales para la construcción del Sistema

Ley No. 81 de 26 de marzo de 2019 “Sobre protección de datos personales”, publicada en la Gaceta Oficial Digital 28743-A de 29 de marzo de 2019, Artículo 1, Artículo 2, Numerales 1, 2, 3, 4, 5, 6,7, 8, 9, Artículo 3, 4, Numeral 1 y 3, Artículo 5, Numerales 1, 2, 3, 4, 5, Artículos 36, 38 y 63.

[1] La publicación en Gaceta Oficial de esta reglamentación proporciona a todos los sectores que manejan bases de datos las herramientas necesarias para implementar protocolos y procedimientos adecuados para el tratamiento de datos y el cumplimiento de la ley. El decreto establece disposiciones generales, requisitos para recabar información, funciones del Oficial de Protección de Datos Personales y criterios para la aplicación de sanciones, entre otros aspectos. Esta ley otorga al ciudadano control sobre el uso de su información personal. La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI) cuenta ahora con la Dirección de Protección de Datos Personales para gestionar consultas y denuncias relacionadas.

Capítulo VIII. Criterios Técnicos para el Sistema Interactivo de las Estadísticas Culturales

Este Protocolo establece cuatro tipos de criterios a saber: (i) funcionalidad; (ii) calidad; (iii) gestión y (iv) éxito.

Funcionalidad: El software debe cumplir con todos los requisitos funcionales especificados en el Documento de Requisitos del Sistema (DRS). Los cuales incluyen:

- Rendimiento: El software debe manejar eficientemente el volumen de datos y usuarios esperados, sin degradación en su desempeño.
- Escalabilidad: El software debe ser escalable para adaptarse al crecimiento futuro de la CSCP.
- Seguridad: El software debe ser seguro y proteger los datos de la CSCP contra accesos no autorizados, modificaciones o destrucciones.
- Usabilidad: El software debe ser fácil de usar y comprender para los usuarios finales.
- Mantenimiento: El software debe ser fácil de mantener y actualizar.
- Compatibilidad: El software debe ser compatible con los sistemas operativos y hardware existentes de la CSCP.

Calidad:

- Precisión: El software debe proporcionar información precisa y confiable.
- Completitud: El software debe proporcionar toda la información necesaria para los usuarios finales.
- Consistencia: El software debe ser consistente en su comportamiento y apariencia.
- Integridad: El software debe estar libre de errores y defectos.
- Verificabilidad: El software debe ser fácil de verificar y validar.
- Documentación: El software debe estar bien documentado para

facilitar su uso, mantenimiento y actualización.

Gestión del proyecto:

- Planificación: El proyecto debe estar bien planificado y tener un cronograma definido.
- Presupuesto: El proyecto debe tener un presupuesto definido y realista.
- Gestión de riesgos: El proyecto debe identificar y gestionar los riesgos potenciales.
- Comunicación: El proyecto debe tener un plan de comunicación efectivo para mantener informadas a todas las partes interesadas.
- Monitoreo y control: El proyecto debe ser monitoreado y controlado para garantizar que se cumpla con el plan y el presupuesto.

Criterios de éxito:

- Satisfacción del usuario: El software debe satisfacer las necesidades y expectativas de los usuarios finales.
- Cumplimiento de objetivos: El software debe cumplir con los objetivos de la CSCP.
- Retorno de la inversión (ROI): El software debe generar un retorno de la inversión positivo para la CSCP.
- Mejora de la eficiencia: El software debe mejorar la eficiencia de los procesos de la CSCP.
- Reducción de costos: El software debe ayudar a reducir los costos de la CSCP.

Los criterios descritos en este documento proporcionan una base sólida para la construcción del software del sistema de información de la CSCP.

Al considerar estos criterios cuidadosamente durante el proceso de desarrollo, se puede garantizar que el software sea de alta calidad, satisfaga las necesidades de la CSCP y tenga éxito en el logro de sus objetivos.

Capítulo IX. Infraestructura de Servidores

El Protocolo establece la posibilidad de almacenar los datos en dos tipos de servidores locales o en la nube. En el caso de los servidores locales estos pueden ser:

a. Servidores Web: Deben ser de alta capacidad y rendimiento para manejar el tráfico de usuarios.
b. Servidores de Bases de Datos: Necesitan ser de alta capacidad y rendimiento para gestionar las consultas de los usuarios. c. Servidores de Aplicaciones: Serán utilizados para ejecutar la lógica de negocio del sistema, requiriendo alta capacidad y rendimiento para manejar la carga de trabajo.

Adicionalmente, se puede aprovechar la nube mediante: a. Infraestructura como Servicio (IaaS): Para provisionar recursos de computación y almacenamiento de forma rápida y escalable. b. Plataforma como Servicio (PaaS): Para desarrollar, implementar y administrar aplicaciones web sin preocuparse por la infraestructura subyacente.

Para garantizar la seguridad, independientemente del tipo de servidor, será importante que se estipulen los principios de redundancia, así como se formule un Plan de contigencia. En el caso de la redundancia se refiere a la replicación de datos para replicarse en varios servidores para garantizar su disponibilidad en caso de que un servidor falle. Así como, el sistema debe tener la capacidad de conmutar por error a un servidor secundario en caso de que un servidor principal falle.

En el caso del Plan de contingencia se refiere a las medidas de recuperación ante desastres para restaurar el sistema en caso de un desastre. Este debe incluir un plan de continuidad para describir cómo la organización continuará operando en caso de una interrupción del sistema. Dicho plan además implica tener claro que la infraestructura debe cumplir con todos los requisitos de seguridad aplicables. Debe ser constantemente monitoreada para detectar y resolver problemas de manera proactiva.

Capítulo X. Estrategias de Protección contra Malware y Otras Amenazas Cibernéticas

Las amenazas cibernéticas son cada vez más sofisticadas y representan un riesgo significativo para las organizaciones de todos los sectores. La Cuenta Satélite de Cultura de Panamá no es una excepción. Es importante implementar medidas de seguridad adecuadas para proteger los sistemas y datos de la organización contra estas amenazas. Entre estas:

a. Implementar un antivirus y un anti-malware: Es esencial contar con un antivirus y un anti-malware actualizado para detectar y eliminar malware de los sistemas.
b. Mantener el software actualizado: Es importante instalar las actualizaciones de software y seguridad de manera regular para corregir vulnerabilidades que podrían ser explotadas por los ciberdelincuentes.
c. Utilizar contraseñas seguras: Se deben utilizar contraseñas seguras y únicas para todas las cuentas. Se recomienda utilizar una combinación de letras mayúsculas y minúsculas, números y símbolos.
d. Habilitar la autenticación de dos factores: La autenticación de dos factores agrega una capa adicional de seguridad al requerir que los usuarios proporcionen dos formas de identificación para acceder a una cuenta.
e. Capacitar a los empleados: Los empleados deben ser capacitados sobre cómo reconocer y evitar ataques cibernéticos. f. Realizar copias de seguridad de los datos: Es importante realizar copias de seguridad de los datos de manera regular para poder restaurarlos en caso de un ataque cibernético.
g. Implementar un plan de respuesta a incidentes: Se debe tener un plan para responder a incidentes cibernéticos de manera rápida y efectiva.

Igualmente, será fundamental desarrollar un Plan de contingencia para describir los pasos que se deben seguir en caso de un incidente cibernético.

Capítulo XI. Bitácora General del Proyecto

En esta bitácora se pueden registrar los eventos más importantes del proyecto, como las reuniones, las decisiones tomadas, los avances logrados y los problemas encontrados.

Es útil para tener una visión general del proyecto y para realizar un seguimiento del progreso. Dicha bitácora debe tener varias secciones. La primera bitácora referente a las incidencias para registrar los problemas o incidencias que se encuentren durante el desarrollo del proyecto.

Para cada incidencia, se debe registrar una descripción del problema, la fecha en que se encontró, el responsable de solucionarlo y la solución aplicada. Es útil para identificar y solucionar problemas de manera oportuna.

Bitácora de cambios: En esta bitácora se pueden registrar los cambios que se realizan al software del sistema. Para cada cambio, se debe registrar una descripción del cambio, la fecha en que se realizó, el responsable de realizarlo y el motivo del cambio.

Es útil para realizar un seguimiento de los cambios realizados al software y para identificar posibles problemas de compatibilidad.

Bitácora de pruebas:
En esta bitácora se pueden registrar los resultados de las pruebas que se realizan al software del sistema. Para cada prueba, se debe registrar una descripción de la prueba, la fecha en que se realizó, el responsable de realizarla y los resultados obtenidos. Es útil para identificar y corregir errores en el software antes de que sea implementado en producción.

Bitácora de reuniones. En esta bitácora se pueden registrar los detalles de las reuniones que se llevan a cabo durante el desarrollo del proyecto. Para cada reunión, se debe registrar la fecha, la hora, los asistentes, los temas tratados, las decisiones tomadas y los siguientes pasos.

Es útil para tener un registro de las decisiones tomadas en las reuniones y para realizar un seguimiento de las acciones pendientes.

Tipos de controles de acceso
Existen diversos tipos de controles de acceso que se pueden implementar, como:

- Control de acceso basado en roles (RBAC): Este tipo de control de acceso asigna permisos a los usuarios en función de su rol dentro de la organización.
- Control de acceso basado en atributos (ABAC): Este tipo de control de acceso permite definir permisos más granulares en función de una serie de atributos, como la ubicación del usuario, la hora del día o el dispositivo que se utiliza para acceder a la información.
- Control de acceso basado en la autenticación (ABA): Este tipo de control de acceso requiere que los usuarios se autentiquen antes de poder acceder a la información. La autenticación puede realizarse mediante el uso de contraseñas, tokens de seguridad o biometría.

C. ANÁLISIS MARCO REGULATORIO

Iniciamos con las normas contenidas en la Constitución Política de la República de Panamá, que hablan de la protección de datos, tomando en consideración que estás se encuentra dentro de las garantías fundamentales que tienen todos los ciudadanos panameños.

En ese orden continuamos con el análisis de La Ley 81 de 26 de marzo de 2019, Sobre protección de datos personales", publicada en la Gaceta Oficial Digital 28743-A de 29 de marzo de 2019, la que fue reglamentada mediante el Decreto Ejecutivo No. 285 de 28 de mayo de 2021. Con referencias a estos documentos legales, consideramos que los mismos contienen los requisitos especiales que reglamentan dicha materia.

Dentro del Protocolo consideramos importante revisar y analizar la Resolución No. 23-2022-INEC de 12 de enero de 2022, por la que se

aprueba el Código Nacional de Buenas Prácticas para las actividades estadísticas, de la Contraloría General de la República, que indica el camino normativo que se debe de seguir, en este aspecto.

No hemos dejado de mencionar el Código Penal de Panamá, que señala en su Título VI, Capítulo IV, las penas correspondientes a los delitos contra la seguridad informática. Determinando que existen sanciones administrativas que encontramos en la Ley No. 81 de 26 de marzo de 2019 y penas por la infracción de delitos contra la seguridad informática.

Finalmente, a raíz de esta revisión se ofrecen recomendaciones.

1. Constitución Política de la República de Panamá

El derecho fundamental a la protección de datos de carácter personal de los ciudadanos es una garantía fundamental contenida en la Constitución Política de la República de Panamá, específicamente en el Título III, Derechos y Deberes Individuales, Capítulo I-Garantías fundamentales, en sus artículos 42, 43 y 44.

“Artículo 42: toda persona tiene derecho acceder a la información personal contenido en bases de datos o registros públicos y privados y a requerir su rectificación y protección, así como su supresión, de conformidad con lo previsto en la Ley.

Esta información solo podrá ser recogida para fines específicos, mediante consentimiento de su titular o por disposición de autoridad competente…”

La norma transcrita implica la obligación de obtener el consentimiento del titular, o sea la manifestación de voluntad de este para obtener los datos y ser informado del fin específico para el cual se requiere recopilar los datos.

El artículo 43 de la Constitución Política de Panamá, establece las garantías constitucionales, en las que toda persona tiene derecho a

solicitar información de acceso público o de interés colectivo y solicitar su rectificación.

Finalmente, en la esfera constitucional, encontramos el artículo 44 que señala que toda persona puede promover una acción de habeas data para garantizar el derecho de acceso a su información personal recabada en bancos de datos o registros oficiales.

2. **Ley no. 81 de 26 de marzo de 2019 "sobre protección de datos personales"** publicada en la gaceta oficial digital 28743-a de 29 de marzo de 2019.

Iniciamos señalando que esta Ley tiene como propósito principal busca salvaguardar y garantizar el derecho fundamental a la protección de los datos de carácter personal de los ciudadanos, estableciendo regulaciones al tratamiento, automatizado o no, de datos personales, el cual será de orden público y de observancia general en toda la República.

Los sujetos regulados en esta Ley son las personas naturales y jurídicas de carácter público o privado, con o sin fines de lucro, que lleven a cabo el tratamiento y/o custodia de datos personales. La misma entró en vigor, dos (2) años después de su promulgación o sea 29 de marzo de 2021.

Derechos de los titulares de datos personales.

Se reconocen como derechos irrenunciables básicos los derechos que tienen los titulares de datos personales, sin perjuicio de cualquier otro derecho reconocido en esta Ley:

- Derecho de acceso: permite al titular obtener sus datos personales que se encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados.

- Derecho de rectificación: permite al titular solicitar la

corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

- Derecho de cancelación: permite al titular solicitar la eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

4. Derecho de oposición: permite al titular, por motivos fundados y legítimos relacionados con una situación en particular, negarse a proporcionar sus datos personales o a que sean objeto de determinado tratamiento, así como a revocar su consentimiento.

5. Derecho de portabilidad: derecho a obtener una copia de los datos personales de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable, cuando:

- El titular haya entregado sus datos directamente al responsable.
- Sea un volumen relevante de datos, tratados de forma automatizada.
- El titular haya dado su consentimiento para el tratamiento o se requiera para la ejecución o el cumplimiento de un contrato.

En todo momento, el titular de los datos personales podrá ejercer estos derechos, los cuales son irrenunciables, salvo las excepciones establecidas en leyes especiales.

Principios generales en los que se inspiran y rigen la protección de datos de carácter personal.

Los principios generales en los cuales está inspirada la Ley 81 de 2019 sobre la protección de datos personales, se encuentran contenidos en el artículo 2, cuando se establecen los siguientes:

- Principio de lealtad: los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos.

- Principio de finalidad: los datos personales deben ser recolectados con fines determinados y no ser tratados posteriormente para fines incompatibles o distintos para los cuales se solicitaron, ni conservarse por tiempo mayor del necesario para los fines de tratamiento.
- Principio de proporcionalidad: solo deberán ser solicitados aquellos datos adecuados, pertinentes y limitados al mínimo necesario en relación con la finalidad para la que son requeridos.
- Principio de veracidad y exactitud: los datos de carácter personal serán exactos y puestos al día de manera que respondan con veracidad a la situación actual del propietario del dato.
- Principio de seguridad de los datos: los responsables del tratamiento de los datos personales deberán adoptar las medidas de índole técnica y organizativa necesarias para garantizar la seguridad de los datos bajo su custodia, principalmente cuando se trate de datos considerados sensibles, e informar al titular, lo más pronto posible, cuando los datos hayan sido sustraídos sin autorización o haya indicios suficientes de que su seguridad ha sido vulnerada.
- Principio de transparencia: toda información o comunicación al titular de los datos personales relativa al tratamiento de estos deberá ser en lenguaje sencillo y claro, y mantenerlo informado de todos los derechos que le amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO.
- Principio de confidencialidad: todas las personas que intervengan en el tratamiento de datos personales están obligadas a guardar secreto o confidencialidad respecto de estos, incluso cuando hayan finalizado su relación con el titular o responsable del tratamiento de datos, impidiendo el acceso o uso no autorizado.
- Principio de licitud: para que el tratamiento de un dato personal sea lícito, deberá ser recolectado y tratado con el consentimiento previo, informado e inequívoco del titular del dato o por fundamento legal.
- Principio de portabilidad: el titular de los datos tiene derecho a obtener de parte del responsable del tratamiento una copia de los datos personales de manera estructurada en un formato genérico y de uso común.

Ámbito De Aplicación De La Ley 81 De 2019.

Los artículos 3 y 5 de la Ley 81 de 2019, establecen su ámbito de aplicación, en primer lugar “aquellos tratamientos que expresamente se encuentren regulados por leyes especiales o por las normativas que las desarrollen” (que trataremos más adelante); además de los tratamientos de datos personales siguientes:

1. Los que realice una persona natural para actividades exclusivamente personales o domésticas.
2. Los que realicen autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales.
3. Los que se efectúen para el análisis de inteligencia financiera y relativos a la seguridad nacional de conformidad con las legislaciones, tratados o convenios internacionales que regulen estas materias.
4. Cuando se trate de tratamiento de datos relacionados con organismos internacionales, en cumplimiento de lo dispuesto en los tratados y convenios vigentes ratificados por la República de Panamá.
5. Los resultantes de información obtenida mediante un procedimiento previo de disociación o anonimización, de manera que el resultado no pueda asociarse al titular de los datos personales.

El artículo 5 de la Ley 81 de 2019, establece de igual manera, que su ámbito de aplicación y reglamentación se aplican a todas las bases de datos que se encuentren en el territorio de la República de Panamá, que almacenen o contengan datos personales de nacionales o extranjeros o que el responsable del tratamiento de los datos esté domiciliado en el país.

La norma excluye de esta normativa la base de datos de sujetos regulados por leyes especiales, siempre que estas leyes que lo regulan o su normativa que las desarrollan establezcan estándares técnicos mínimos necesarios para la correcta protección y tratamiento de datos personales, conforme a lo establecido en esta Ley.

El artículo 5 de la Ley 81 de 2019, establece de igual manera, con referencia al almacenamiento o transferencia de datos personales originados o almacenados dentro de la República de Panamá que sean confidenciales, sensibles o restringidos, que reciban un tratamiento transfronterizo, será permitido siempre que el responsable del almacenamiento de esos datos o el custodio de estos cumpla con los estándares de protección de datos personales exigidos por esta Ley, o pueda demostrar que cumple con los estándares y normas de protección de datos personales iguales o superiores a los exigidos en esta.

Se exceptúan para efectos del requerimiento que trata el párrafo anterior, los casos siguientes:

- Cuando el titular haya otorgado su consentimiento para la transferencia.
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar por el interesado o en interés de este.
- Cuando se trate de transferencias bancarias, dinerarias y bursátiles del mercado de valores.
- Cuando se trate de información cuya transmisión sea requerida por ello en cumplimiento de tratados internacionales ratificados por la República de Panamá.

En cualquiera de los casos, el tratamiento o transferencia de datos personales que se realice a través de Internet o cualquier otro medio de comunicación electrónica, digital o física, el custodio de la base de datos y/o el responsable por el tratamiento deberá cumplir con los estándares, normas, certificaciones, protocolos, medidas técnicas y de gestión informática adecuados para preservar la seguridad en sus sistemas o redes, o en la prestación de sus servicios, con el fin de garantizar los niveles de protección de los datos personales tal cual lo establece esta Ley y su reglamentación, así como las certificaciones, protocolos, estándares y otras medidas que se establezcan.

Definiciones Contenidas En La Ley.

Toda Ley requiere en su elaboración una serie de definiciones específicas para evitar ambigüedades en su interpretación. El artículo 4 de la Ley 81 contiene las definiciones que corresponden a la materia, las que pasamos a señalar:

- Almacenamiento de datos. Conservación o custodia de datos en una base de datos establecida en cualquier medio provisto, incluido el de las Tecnologías de la Información y la Comunicación (TICs).
- Base de datos. Conjunto ordenado de datos de cualquier naturaleza, cualquiera que sea la forma o modalidad de su creación, organización o almacenamiento, que permite relacionar los datos entre sí, así como realizar cualquier tipo de tratamiento o transmisión de estos por parte de su custodio.
- Bloqueo de datos. Restricción temporal de cualquier acceso o tratamiento de los datos almacenados.
- Consentimiento. Manifestación de la voluntad del titular de los datos, mediante la cual se efectúa el tratamiento de estos. Consideramos este término fundamental, ya que para el tratamiento de un dato personal sea lícito, debe ser recolectado y tratado con el consentimiento previo del titular, quien además tiene el derecho a saber cuál es el uso que se le dará a su información. El consentimiento deberá ir precedido de la información y prevista en el.
- Custodio de la base de datos. Persona natural o jurídica, de derecho público o privado, lucrativa o no, que actúa a nombre y por cuenta del responsable del tratamiento y le compete la custodia y conservación de la base de datos.
- Datos confidenciales. Aquellos datos que por su naturaleza no deben ser de conocimiento público o de terceros no autorizados, incluyendo aquellos que estén protegidos por ley, por acuerdos de confidencialidad o no divulgación, a fin de salvaguardar información. En los casos de la Administración Pública, son aquellos datos cuyo tratamiento está limitado para fines de esta

Administración o si se cuenta con el consentimiento expreso del titular, sin perjuicio de lo dispuesto por leyes especiales o por las normativas que las desarrollen. Los datos confidenciales siempre serán de acceso restringido.

- Dato anónimo. Aquel dato cuya identidad no puede ser establecida por medios razonables o el nexo entre este y la persona natural a la que se refiere.
- Dato caduco. Aquel dato que ha perdido actualidad por disposición de la ley, por el cumplimiento de la condición o la expiración del plazo señalado para su vigencia o, si no hubiera norma expresa, por el cambio de los hechos o circunstancias que consigna.
- Dato personal. Cualquier información concerniente a personas naturales, que las identifica o las hace identificables.
- Dato disociado. Aquel dato que no puede asociarse al titular ni permitir por su estructura, contenido o grado de desagregación la identificación de la persona, sea esta natural.
- Dato sensible. Aquel que se refiera a la esfera íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para este. De manera enunciativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico; creencias o convicciones religiosas, filosóficas y morales; afiliación sindical; opiniones políticas; datos relativos a la salud, a la vida, a la preferencia u orientación sexual, datos genéticos o datos biométricos, entre otros, sujetos a regulación y dirigidos a identificar de manera unívoca a una persona natural.
- Eliminación o cancelación de datos. Suprimir o borrar de forma permanente los datos almacenados en bases de datos, cualquiera que sea el procedimiento empleado para ello.
- Ficha técnica. Documento que contiene los registros, protocolos y reglas, relacionados al almacenamiento y tratamiento de los datos personales.
- Fuente accesible. Bases de datos que no sean de acceso restringido o contengan reserva alguna a consultas, o que sean de acceso público, como las publicaciones estatales de carácter oficial,los medios de comunicación, los directorios telefónicos y la

lista de personas que pertenecen a un grupo de profesionales que contengan únicamente nombre, título o profesión, actividad, dirección laboral o comercial, al igual que información que indique su pertenencia a organismos.

- Modificación de datos. Todo cambio en el contenido de los datos almacenados en bases de datos.
- Procedimiento de disociación o anonimización. Todo tratamiento de datos que impide que la información disponible en la base de datos pueda asociarse a persona natural determinada o determinable.
- Responsable del tratamiento de los datos. Persona natural o jurídica, de derecho público o privado, lucrativa o no, que le corresponde las decisiones relacionadas con el tratamiento de los datos y que determina los fines, medios y alcance, así como cuestiones relacionadas a estos.
- Titular de los datos. Persona natural a la que se refieren los datos.
- Transferencia de datos. Dar a conocer, divulgar, comunicar, intercambiar y/o transmitir, de cualquier forma y por cualquier medio, de un punto a otro, intra o extra fronterizo, los datos a personas naturales o jurídicas distintas del titular, ya sean determinadas o indeterminadas.
- Tratamiento de datos. Cualquier operación o complejo de operaciones o procedimientos técnicos, de carácter automatizado o no, que permita recolectar, almacenar, grabar, organizar, elaborar, seleccionar, extraer, confrontar, interconectar, asociar, disociar, comunicar, ceder, intercambiar, transferir, transmitir o cancelar datos, o utilizarlos en cualquier otra forma.

Condiciones Para El Tratamiento De Datos Personales.

El artículo 6 de la Ley 81, especifica que el tratamiento de datos personales solo podrá realizarse cuando se cumplan al menos una de las condiciones siguientes:

- Que se obtenga el consentimiento del titular de los datos.
- Que el tratamiento de los datos sea necesario para la ejecución de una obligación contractual, siempre que el titular de los datos sea parte.

- Que el tratamiento sea necesario para el cumplimiento de una obligación legal para la cual el responsable de los datos esté sujeto.
- Que el tratamiento de los datos personales esté autorizado por una ley especial o las normativas que las desarrollan.

La persona que acepte dicho tratamiento debe ser debidamente informada respecto del propósito del uso de sus datos personales.

El consentimiento podrá obtenerse de forma que permita su trazabilidad mediante documentación, ya sea electrónica o mediante cualquier otro mecanismo que resulte adecuado al medio de que se trate el caso y podrá ser revocado, sin efecto retroactivo.

El artículo 8 de la Ley, establece por su parte, los casos cuando no se requiere autorización para el tratamiento de datos personales:

- Los que provengan o que se recolecten de fuentes de dominio público o accesible en medios públicos.
- Los que se recolecten dentro del ejercicio de las funciones propias de la Administración Pública en el ámbito de sus competencias.
- Los de carácter económico, financiero, bancario o comercial que cuenten con el consentimiento previo.
- Los que se contengan en listas relativas a una categoría de personas que se limiten a indicar antecedentes, como la pertenencia de la persona natural a una organización, su profesión o actividad, sus títulos educativos, dirección o fecha de nacimiento.
- Los que son necesarios dentro de una relación comercial establecida, ya sea para la atención directa, comercialización o venta de los bienes o servicios pactados.

El tratamiento de datos personales que realicen organizaciones privadas para el uso exclusivo de sus asociados y de las entidades a que están afiliadas, con fines estadísticos, de tarificación u otros de beneficio general de aquellos.

Los casos de urgencia médica o sanitaria.

El tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

El tratamiento que sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un menor de edad o una persona con discapacidad.

Cuando el consentimiento se refiera a datos personales sensibles de salud, el consentimiento será previo, irrefutable y expreso. En los supuestos previstos en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso a sus datos personales sin cargo alguno. El titular podrá, en cualquier momento, solicitar la modificación, eliminación o bloqueo de sus datos.

En los supuestos previstos en el presente artículo, el titular de los datos podrá ejercer el derecho de acceso a sus datos personales sin cargo alguno. El titular podrá, en cualquier momento, solicitar la modificación, eliminación o bloqueo de sus datos personales de las bases de datos a los que se refiere este artículo. Lo anterior se entiende, sin perjuicio de lo que dispongan leyes especiales.

Responsabilidad Del Tratamiento De Datos.

El artículo 7 de la Ley específica que “El responsable del tratamiento de datos personales contenidos en bases de datos establecerá los protocolos, procesos y procedimientos de gestión y transferencia segura, protegiendo los derechos de los titulares sobre sus datos bajo los preceptos de esta Ley”...

De igual manera, la norma establece que el responsable de los tratamientos de datos será fiscalizado y supervisado por la Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), con el

apoyo de la Autoridad Nacional para la Innovación Gubernamental (AIG), cuando se trate de aspectos relacionados a las Tecnologías de la Información y la Comunicación (TICs).

Los requerimientos mínimos que deben contener las políticas de privacidad, los protocolos, los procesos y los procedimientos de tratamiento y transferencia segura que deberá cumplir el responsable del tratamiento de datos serán emitidos por el regulador del tratamiento de acuerdo con la Ley.

Derechos De Los Titulares De Datos Personales.
El artículo 15 de la Ley 81 reconocen como derechos irrenunciables básicos que tienen los titulares de datos personales, sin perjuicio de cualquier otro derecho reconocido en esta Ley, los llamados ARCO :

Derecho de acceso: permite al titular obtener sus datos personales que se encuentren almacenados o sujetos a tratamiento en bases de datos de instituciones públicas o privadas, además de conocer el origen y la finalidad para los cuales han sido recabados.

Derecho de rectificación: permite al titular solicitar la corrección de sus datos personales que sean incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

Derecho de cancelación: permite al titular solicitar la eliminación de sus datos personales incorrectos, irrelevantes, incompletos, desfasados, inexactos, falsos o impertinentes.

Derecho de oposición: permite al titular, por motivos fundados y legítimos relacionados con una situación en particular, negarse a proporcionar sus datos personales o a que sean objeto de determinado tratamiento, así como a revocar su consentimiento.

Derecho de portabilidad: derecho a obtener una copia de los datos personales de manera estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable, cuando:

a. El titular haya entregado sus datos directamente al responsable.

b. Sea un volumen relevante de datos, tratados de forma automatizada.

c. El titular haya dado su consentimiento para el tratamiento o se requiera para la ejecución o el cumplimiento de un contrato. En todo momento, el titular de los datos personales podrá ejercer estos derechos, los cuales son irrenunciables, salvo las excepciones establecidas en leyes especiales.

Responsabilidad Por Las Infracciones Art. 36.

La Autoridad Nacional de Transparencia y Acceso a la Información, a través de la Dirección creada para conocer esta materia, está facultada para sancionar a la persona natural o jurídica responsable del tratamiento de los datos personales, así como al custodio de la base de datos, que por razón de la investigación de las quejas o denuncias que se les presenten y se les compruebe que han infringido los derechos del titular de los datos personales.

Las decisiones de la Dirección competente para esta materia dentro de la Autoridad Nacional de Transparencia y Acceso a la Información serán impugnables mediante recurso de reconsideración ante esta Dirección y de apelación que se interpondrá ante el director general de la Autoridad Nacional de Transparencia y Acceso a la Información como segunda instancia, los cuales se sustentarán en un término de cinco días, a partir del día siguiente hábil después de su notificación.

Aquellos casos de queja que se presenten ante los entes reguladores, en los que se realicen tratamientos de datos que se encuentren regulados por leyes especiales y que no se encuentren las sanciones a las faltas cometidas en dichas leyes expresamente tipificadas, el regulador a quien se le interponga la queja deberá aplicar supletoriamente las sanciones establecidas en esta Ley.

La Autoridad Nacional de Transparencia y Acceso a la Información fijará los montos de las sanciones aplicables a las respectivas faltas,

acordes a la gravedad de las faltas, que se establecerán desde mil balboas (B/.1,000.00) hasta diez mil balboas (B/.10,000.00), así como reglamentará el procedimiento correspondiente.

Las sanciones pecuniarias que imponga la Autoridad Nacional de Transparencia y Acceso a la Información en el ejercicio de las facultades establecidas en esta Ley que no hayan sido pagadas en el término concedido, se remitirán para su cobro a la Dirección General de Ingresos del Ministerio de Economía y Finanzas.

El responsable del tratamiento de los datos personales deberá indemnizar el daño patrimonial y/o moral que causará por el tratamiento indebido de estos, de conformidad con lo establecido en esta Ley o en el ordenamiento legal vigente.

Los tribunales de justicia conocerán de las demandas que se presenten contra los responsables del tratamiento de los datos personales, así como sobre las reclamaciones por daños y perjuicios causados.

Infracciones Y Sanciones

Artículo 38.
Las infracciones a esta Ley se califican en leves, graves o muy graves.
SE CONSIDERA INFRACCIÓN LEVE:

No remitir y/o informar a la Autoridad Nacional de Transparencia y Acceso a la Información dentro de los plazos requeridos la información de lo ordenado en esta Ley, su reglamentación o cualquier otra disposición normativa.

Se Consideran Infracciones Graves:

- Efectuar el tratamiento de datos personales sin haber obtenido el consentimiento de su titular, según el procedimiento indicado por esta Ley, su reglamentación o cualquier otra disposición normativa que se refiera a la presente Ley.

- Infringir los principios y garantías establecidos en la presente Ley o en su reglamentación.

- Infringir el compromiso de confidencialidad relacionado al tratamiento de los datos personales.

- Restringir o entorpecer la aplicación de los derechos de acceso, rectificación, cancelación y oposición.

- Incumplir el deber de informar al titular afectado acerca del tratamiento de sus datos personales, cuando los datos no hayan sido obtenidos del propio titular.

- Almacenar o archivar datos personales sin contar con las adecuadas condiciones de seguridad que esta Ley o su reglamento disponga.

- No atender la reiteración de los requerimientos u observaciones formalmente notificados, o no proporcionar la documentación o información formalmente solicitada por la Autoridad Nacional de Transparencia y Acceso a la Información.
- Entorpecer o no cooperar con la Autoridad Nacional de Transparencia y Acceso a la Información al momento en que esta ejerza su función de inspección.

Se Consideran Infracciones Muy Graves:

- Recopilar datos personales en forma dolosa.

- No observar de las regulaciones establecidas respecto al tratamiento de los datos sensibles.

- No suspender el tratamiento de datos personales cuando existiera un previo requerimiento de la Autoridad Nacional de Transparencia y Acceso a la Información para ello.

- Almacenar o transferir internacionalmente datos personales, violentando lo establecido en esta Ley.

- Reincidir en las faltas graves.

Las sanciones que imponga la Autoridad Nacional de Transparencia y Acceso a la Información a los responsables de las bases de datos y demás sujetos alcanzados por el régimen de la presente ley y sus reglamentos, se graduarán dependiendo de la gravedad de la infracción cometida.

Los criterios de graduación de las sanciones al igual que la prescripción tipificada en esta Ley se encuentran desarrolladas en el Decreto Ejecutivo 285 de 28 de mayo de 2021.

3. Decreto Ejecutivo 285 del 28 de mayo de 2021.

La Ley 81 de 26 de marzo de 2019, fue reglamentada a través del Decreto Ejecutivo 285 del 28 de mayo de 2021.

Como ya hemos visto la Ley 81 de 26 de marzo de 2019, sobre protección de datos personales, contiene principios, derechos y obligaciones que regulan la protección de datos personales en la República de Panamá. Esta reglamentación fue publicada en la Gaceta Oficial Digital 28743-A de 29 de marzo de 2021, ofrece a todos los sectores que manejan base de datos, las herramientas necesarias para que pongan en práctica los protocolos y procedimientos para el tratamiento de los datos y cumplimiento de la ley.

En el artículo 1 del Decreto Ejecutivo 285, se establece su objeto “desarrollar las disposiciones que regulan el régimen general de protección de datos personales para la República de Panamá previstos en la Ley 81 de 26 de marzo de 2019.”

El artículo establece que “las disposiciones y postulados sobre protección de datos personales contenidos en la Ley 81 de 2019 y el

presente decreto, son mínimas y no excluyentes de otras leyes especiales sobre la materia, especialmente en lo relativo al tratamiento y custodia de datos. Este decreto constituye el régimen de aplicación general a cualquier tratamiento de datos personales sin perjuicio de tener que observar, además, los requisitos añadidos que puedan establecerse en leyes especiales que resulten aplicables al tratamiento de datos que se llevan a cabo por el responsable del tratamiento o por el custodio de la base de datos y especialmente en el caso de actividades reguladas.

En el caso de sujetos regulados por la ley especial, siempre que esta ley contenga reglas relativas al tratamiento de datos personales, se tendrá la Ley 81 de 2019 y el presente decreto como régimen general y estándar mínimo de cumplimiento para garantizar la correcta protección de los datos personales. La ley especial debe regular aquellos requisitos especiales que exijan los tratamientos de datos que en ella se señalan y de esta forma complementar y ampliar las previsiones de la Ley 81 de 2019, con la finalidad de que los datos personales que sean objeto de tratamiento de esa actividad queden debidamente protegidos.

Cuando así lo exija el sector regulado, los requerimientos de las políticas de privacidad, protocolos, procesos y procedimientos de tratamiento y transferencia segura establecidos por la Ley 81 de 2019 y este decreto, deberán ser completados para adaptarse a las exigencias de sus tratamientos de datos.

En el artículo 2 del Decreto Ejecutivo se encuentra el ámbito de aplicación de la Ley 81 de 2019 y el presente decreto, señalando que esta se aplica en los siguientes casos:

1. Las bases de datos se encuentren en el territorio de la República de Panamá y almacenen o conserven datos personales de nacionales o extranjeros;

2. El responsable del tratamiento de los datos personales esté domiciliado en la República de Panamá.

3. Los tratamientos de datos cuyo origen o almacenamiento sea el territorio de la República de Panamá, con las excepciones previstas en la Ley 81 de 2019; y

4. Los tratamientos de datos realizados en el marco de una actividad comercial, por Internet o cualquier otro medio de comunicación electrónica o digital, conforme a la Ley 51 de 2008, para organizar la protección de los datos personales en las actividades dirigidas al mercado panameño.
Sujetos protegidos que se encuentran protegidos en la Ley. (Artículo 3 del Decreto Ejecutivo).

El artículo 3 señala que “quedan sujetos a protección los tratamientos de datos personales

Las personas naturales, siempre que estos datos los identifiquen o los hagan identificables.

Los derechos de las personas fallecidas en relación con sus datos personales se rigen por las reglas generales del Código Civil.

En el caso de tratamiento de datos personales de menores de edad, se dará prioridad al interés superior del menor conforme a las normas de la República de Panamá y a los tratados internacionales existentes en la materia.

Como señalamos en el punto 3 de la Ley encontramos las definiciones que han seguir los lineamientos correspondientes.
Para los efectos del decreto que reglamenta la Ley, encontramos también los siguientes:

Autoridad de control. La Autoridad Nacional de Transparencia y Acceso a la Información (ANTAI), es el organismo de la administración pública responsable de supervisar, implementar y controlar el cumplimiento de la Ley 81 de 2019 y el presente decreto, en todo el territorio nacional.

Datos biométricos. Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona natural que permitan o confirmen la identificación única de dicha persona.

Datos genéticos. Datos personales relativos a las características genéticas heredadas o adquiridas de una persona natural que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.

Datos relativos a la salud. Datos personales relativos a la condición física o mental de una persona natural, que revelen información sobre su estado de salud.

Derechos ARCO. Derechos irrenunciables básicos de los titulares de datos personales, e identificados como: derechos de acceso, rectificación, cancelación y oposición. Estos derechos ARCO, están contenidos en el artículo 15 de la Ley 81 de 2019.

Destinatario: La persona natural o jurídica, autoridad pública, servicio u organismo al que se transfieran datos personales.

Elaboración de perfiles. Toda forma de tratamiento automatizado que utilice datos personales para evaluar determinados aspectos de una persona natural, y en particular para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos.

Exportador. Persona natural o jurídica de carácter público o privado, domiciliado en el país, que efectúe transferencias de datos personales extrafronterizos, conforme a lo dispuesto en la Ley 81 de 2019 y el presente decreto.

Evaluación de impacto en protección de datos. Documentación del responsable del tratamiento que contiene la descripción de los

procesos con datos personales que pueden generar riesgos para los derechos y deberes individuales y sociales, así como medidas, salvaguardas y mecanismos de mitigación de riesgos.

Oficial de Protección de Datos Personales. Funcionario designado para atender la unidad de enlace.

Regulador: Entidad del Estado encargada de fiscalizar a los sujetos de sectores regulados por leyes especiales.

Violación de la seguridad de los datos personales. Toda infracción a la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

En la Sección Primera del Decreto Ejecutivo se encuentran los principios generales para el tratamiento de los datos, los que se consagran en el artículo 2 de la Ley 81 de 2019.

El artículo 5 del Decreto Ejecutivo establece que la protección de datos personales se rige por los principios de lealtad, finalidad, proporcionalidad, veracidad y exactitud, seguridad de los datos, transparencia, confidencialidad, licitud y portabilidad.

Principio de lealtad (artículo 6). Los datos personales deberán recabarse sin engaño o falsedad y sin utilizar medios fraudulentos, desleales o ilícitos.

Principio de finalidad (artículo 7). Los responsables del tratamiento deberán recolectar datos con fines determinados y legítimos. Los datos no podrán utilizarse posteriormente de manera incompatible o diferente con dichos fines. El tratamiento ulterior de los datos personales con fines de investigación, estudios, encuestas o conocimientos de interés público, no se considerará incompatible con los fines que motivaron la recogida. Los fines del tratamiento de los datos determinarán el plazo de conservación de estos, transcurrido el cual el responsable del tratamiento los suprimirá o eliminará de sus archivos, registros, bases

de datos, expedientes o sistemas de información, o en su caso, los someterá a un procedimiento de anonimización.

Para determinar el plazo de conservación de los datos se acudirá a las leyes aplicables en cada caso y a las responsabilidades de todo orden que deban ser atendidas por el responsable del tratamiento o custodio de la base de datos. En el caso de datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias se atenderá a lo dispuesto en el artículo 30 de la Ley 81 de 2019.

Principio de proporcionalidad (artículo 8). Para conocer qué datos son adecuados, pertinentes y mínimos necesarios para la finalidad perseguida con el tratamiento de los datos, los responsables del tratamiento y, en su caso, los custodios de la base de datos tomarán en cuenta el estado de la tecnología, la naturaleza, ámbito, contexto y fines de tratamiento. Con este fin podrán realizar y documentar evaluaciones de impacto en protección de datos personales con el objeto de minimizar los datos objeto de tratamiento, conocer los riesgos que impliquen los tratamientos y adoptar las medidas y garantías necesarias para mitigarlos. La autoridad de control podrá definir aquellos supuestos en los que es recomendable realizar una evaluación de impacto y establecer las pautas o estándares a seguir en su desarrollo. Los responsables del tratamiento y los custodios de las bases de datos adoptarán medidas organizativas que regulen el acceso a los datos personales en su entidad, conforme a este principio permitiendo el acceso a ellos únicamente a los empleados o funcionarios públicos que lo necesiten para el desarrollo de sus funciones y limitando el mismo a la cantidad de datos y al tiempo necesario para ello.

Principio de veracidad y exactitud (Artículo 9). Los responsables del tratamiento adoptarán las medidas necesarias para mantener exactos y puestos al día los datos personales en su posesión, de tal manera que no se altere la realidad de éstos conforme se requiera para el cumplimiento de las finalidades que motivaron su tratamiento.

Principio de transparencia (Artículo 10). Toda información o comunicación al titular de los datos personales relativa al tratamiento de éstos deberá ser en lenguaje sencillo y claro, y mantenerlo

informado de todos los derechos que le amparan como titular del dato, así como la posibilidad de ejercer los derechos ARCO.

Principio de confidencialidad (Artículo 11). Todas las personas que intervengan en el tratamiento de datos personales están obligadas a guardar secreto o reserva respecto de estos, incluso cuando hayan finalizado su relación con el titular o responsables del tratamiento de los datos, impidiendo el acceso o uso no autorizado.

Principio de licitud (Artículo 12). Para que el tratamiento de un dato personal sea lícito, deberá ser recolectado y tratado con base en algunas de las condiciones de licitud que reconoce la Ley 81 de 2019 y conforme a lo que se describe en la Sección tercera de este Capítulo.

Principio de portabilidad (Artículo 13). El titular de los datos tiene derecho a obtener de parte del responsable del tratamiento una copia de los datos personales de manera estructurada en un formato genérico de uso común.

Sección Segunda. Requisitos de la Información.

Contenido de la información. (Artículo 14) Cuando los datos se obtengan directamente del titular, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

1. La identidad y datos de contacto del responsable del tratamiento.

2. La finalidad o finalidades del tratamiento a que se destinarán los datos personales; cuando el responsable del tratamiento proyecte el tratamiento posterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento posterior, información sobre ese otro fin y cualquier información adicional pertinente.

3. La condición que legitima el tratamiento conforme a los artículos 6, 8

y 33 de la Ley 81 de 2019. Cuando el tratamiento esté basado en el consentimiento del interesado, se le debe informar de su derecho a revocar el consentimiento en cualquier momento, sin que ello tenga efectos retroactivos; cuando el tratamiento de datos personales sea un requisito legal o un requisito necesario para suscribir un contrato, así se indicará y cuando el tratamiento se base en los intereses legítimos del responsable del tratamiento o de un tercero, conforme al artículo 8 de la Ley 81 de 2019, se detallará cuáles son estos intereses.

4. Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.

5. La intención del responsable del tratamiento de transferir datos personales a un tercer país, así como la condición prevista en el artículo 33 de la Ley 81 de 2019 que resulta aplicable.

6. El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

7. La existencia, forma y mecanismos o procedimientos a través de los cuales podrá ejercer los derechos de acceso, rectificación, cancelación, oposición y portabilidad.

8. La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 19 de la Ley 81 de 2019, y, al menos en tales casos, la información significativa sobre la lógica aplicada, como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

9. Los datos de contacto del oficial de protección de datos personales. Cuando los datos personales no se hayan obtenido de su titular, el responsable del tratamiento le facilitará, además de la información a que se refiere este artículo, la referente a la categoría de los datos de que se trate y la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

Plazos Para Facilitar La Información (Artículo 15).

Cuando los datos sean proporcionados por el titular, la información se facilitará en el momento de la recogida de los datos. Cuando los datos se obtengan de otra fuente, la información se facilitará:

1. Si los datos personales se utilizan para comunicarse con el titular, a más tardar en el momento de la primera comunicación.

2. Si se comunica a otro destinatario, éste deberá informar al titular en la primera comunicación que le dirija.

Forma Para Facilitar La Información (Artículo 16).

El responsable del tratamiento podrá elegir la forma en la que va a proporcionar la información al titular de los datos siempre que ésta le permita demostrar que cumplió con la obligación de informar. La información proporcionada al titular tendrá que ser suficiente y fácilmente accesible, así como redactarse y estructurarse en un lenguaje claro, sencillo y de fácil comprensión para los titulares a quienes va dirigida, especialmente si se trata de menores de edad. Podrá utilizarse recursos audiovisuales, cuando sea apropiado, con el fin de proporcionar la información necesaria.

Cuando la información vaya a facilitarse a través de Internet o a través de dispositivos de pantalla reducida, y siempre que así lo considere el responsable del tratamiento, se podrá dar cumplimiento al deber de información mediante un sistema de información dividida en capas.

De esta forma la política de privacidad y/o las condiciones de servicios accesibles, a las que se refiere la Ley 81 de 2019, se podrán dividir en capas. En la primera capa se facilitará al afectado la información básica referente a la identidad del responsable del tratamiento, finalidad del tratamiento y posibilidad de ejercer los derechos que le reconoce la Ley 81 de 2019 y se le indicará una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.

Sección Tercera. Condiciones De Licitud Para El Tratamiento

Condiciones de licitud para el tratamiento (Artículo 17). Se podrá proceder el tratamiento de los datos cuando se cumplan, al menos, una de las condiciones siguientes:

Cuando el titular de los datos haya otorgado su consentimiento previo, inequívoco e informado por un medio que permita al responsable del tratamiento probar la trazabilidad de dicho consentimiento. Cuando el tratamiento tenga lugar en el marco de una relación contractual en la que el titular de datos sea parte o se celebre en su interés.
Cuando el tratamiento sea necesario para el cumplimiento de una obligación legal por parte del responsable del tratamiento.

En estos casos, la ley que recoja la obligación debe disponer:

a. La finalidad del tratamiento.
b. La determinación del responsable o responsables del tratamiento. c. Las limitaciones que rigen la licitud del tratamiento por parte del responsable.
d. Las categorías de datos objeto de tratamiento.
e. Los titulares de los datos afectados.
f. Las entidades a las que se pueden comunicar los datos y los fines de la comunicación;
g. Los plazos de conservación de los datos.

Cuando el tratamiento este autorizado en una ley especial o las normativas que las desarrollen. Estas leyes podrán imponer condiciones especiales al tratamiento respetando lo previsto en la Ley 81 de 2019 y el presente decreto.

Cuando el tratamiento sea necesario para proteger intereses vitales del titular de los datos o de otra persona natural.
Cuando sea requerido por una entidad pública en el ejercicio de sus funciones legales, para la salvaguarda de un interés público o por orden judicial.

Cuando el tratamiento sea necesario para satisfacer el interés legítimo perseguido por el responsable del tratamiento o por un tercero, siempre que prevalezcan los intereses o los derechos y libertades fundamentales del titular de los datos, en especial cuando sea un menor de edad.

Para justificar el interés legítimo el responsable del tratamiento deberá demostrar que evaluó y ponderó los intereses o derechos involucrados y que adoptó las medidas necesarias para mitigar los riesgos derivados del tratamiento. Esta condición de licitud no será aplicable al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.

Cuando se trate de datos sensibles, se atenderá a las condiciones previstas en el artículo 13 de la Ley 81 de 2019 para proceder a su transferencia a terceros.

El artículo 18 del Decreto Ejecutivo establece las condiciones para el Consentimiento. Como ya hemos señalado el consentimiento es el requisito indispensable en el tratamiento de datos personales, tal como aparece en el artículo 6 de la Ley 81 de 2019. En este sentido el consentimiento debe cumplir con requisitos contenidos en el presente Decreto Ejecutivo.

Condiciones para el Consentimiento.
El consentimiento deberá ir precedido de la información prevista en el artículo 10 del presente decreto, para cumplir las exigencias de ser informado e inequívoco.

En este sentido el consentimiento debe estar revestido del principio de transparencia: deberá constar en lenguaje sencillo y claro y mantener al titular informado de todos los derechos que le amparan como titular del dato , así como la posibilidad de ejercer los derechos ARCO.

El consentimiento deberá obtenerse de forma que permita su trazabilidad. Esto es, cuando el tratamiento se base en el consentimiento del interesado, el responsable del tratamiento deberá

ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.

Se considera válida la documentación del consentimiento, incluso por vía electrónica o por cualquier otro mecanismo, conforme al medio que se utilice en cada caso para la recogida de los datos, siempre que éste permita demostrar al responsable del tratamiento que el consentimiento fue otorgado.

Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos.

El consentimiento para el tratamiento de datos de salud, así como otros datos sensibles, cuando la ley que los regule lo exija, deberá ser irrefutable y expreso. En el caso de tratamiento de datos de menores de edad e incapaces, el tratamiento deberá llevarse a cabo con la autorización previa del acudiente, tutor o quien ejerza la guardia y crianza o tutela del menor o incapaz.

En estos casos, el responsable del tratamiento deberá demostrar que hizo todos los esfuerzos razonables para verificar esta autorización, teniendo en cuenta el estado de la tecnología disponible en cada momento. Los datos personales de los menores de edad e incapaces se pueden recopilar sin consentimiento cuando el tratamiento sea necesario para contactar con los padres, acudiente, tutor o quien ejerza la guarda y crianza o tutela del menor o incapaz y únicamente con esta finalidad.

El artículo 19 establece que el consentimiento podrá ser revocado en cualquier momento. El retiro del consentimiento no afectará la licitud del tratamiento basada en el consentimiento previo a su revocación, salvo las excepciones contenidas en la ley 81 de 2019 y cualquier otra disposición legal aplicable. Antes de dar su consentimiento, el interesado será informado de ello. Deberá ser tan fácil retirar el consentimiento como otorgarlo.

Derechos De Los Titulares De Datos Personales (Capítulo II). El artículo 21 del Decreto Ejecutivo 285, contiene las disposiciones generales sobre el ejercicio de los derechos de los titulares de datos personales, que pueden ser ejercidos por el titular personalmente o a través de representante legal.

Es nulo o cualquier acto o convenio entre los responsables del tratamiento o custodios de la base de datos y los titulares de los datos que limiten esos derechos.

El responsable del tratamiento establecerá protocolos sencillos, accesibles y gratuitos que permitan al titular de los datos ejercer sus derechos y al responsable del tratamiento dar respuesta en tiempo y forma.

El responsable del tratamiento informará al titular de los datos sobre los medios a su disposición para ejercer los derechos que le correspondan. Los medios deberán ser fácilmente accesibles y el responsable del tratamiento no podrá denegar el derecho por el solo motivo de optar el titular de los datos por otro medio, siempre que no suponga un coste desproporcionado para el responsable del tratamiento. El solicitante deberá acreditar su identidad en el momento de la solicitud, así como los datos de contacto necesarios para enviarle la respuesta al ejercicio de su derecho.

En el caso de ejercicio por medio de representante legal, deberá acompañarse a la solicitud la documentación que acredite la misma conforme al ordenamiento jurídico vigente.

El custodio de la base de datos podrá tramitar, por cuenta del responsable del tratamiento, las solicitudes de ejercicio a los derechos formuladas por los afectados, si así se establece en el contrato o acto jurídico que les vincule.

El responsable del tratamiento deberá dar respuesta al ejercicio de los derechos, incluso cuando no obrasen datos en sus bases de datos relacionados con el solicitante.

La prueba del cumplimiento del deber de responder a la solicitud de ejercicio de los derechos formulado por el afectado recaerá sobre el responsable del tratamiento. Cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos, se atenderá lo dispuesto en aquellas, siempre que respeten los requisitos que se establecen en la Ley 81 de 2019 y en este decreto.

Cada derecho deberá ejercitarse separadamente sin que el ejercicio de uno excluya a los demás.

Ejercicio De Derechos De Menores E Incapaces. (Artículo 22 De La Ley).
Los padres, madres, acudientes, tutores o quienes ejerzan la guarda y crianza de menores o incapaces podrán ejercitar en su nombre y representación los derechos de acceso, rectificación, cancelación, oposición, portabilidad o cualesquiera otros que pudieran corresponderles en el contexto de la Ley 81 de 2019 y el presente decreto.

Gratuidad De Las Actuaciones. (Artículo 23 Del Decreto Ejecutivo).
Serán gratuitas las actuaciones llevadas a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de estos derechos, con las limitaciones que este decreto establece y las que dispongan leyes especiales en su caso.

Derechos De Los Titulares De Los Datos Personales.
Se denominan Derechos ARCO, y se encuentran regulados en la Ley 81 en Capítulo II artículos 15 al 24, son derechos irrenunciables básicos que tienen los titulares de datos personales, específicamente:

Derecho de ACCESO, Derecho de RECTIFICACIÓN, Derecho de CANCELACIÓN, Derecho de OPOSICIÓN.

Es importante señalar que la Ley contiene el Derecho de PORTABILIDAD, el que permite obtener una copia de los datos personales de manera

estructurada, en un formato genérico y de uso común, que permita ser operado por distintos sistemas y/o transmitirlos a otro responsable, cuando:

a. El titular haya entregado sus datos directamente al responsable.

b. Sea un volumen relevante de datos, tratados de forma automatizada.

c. El titular haya dado su consentimiento para el tratamiento o se requiera para la ejecución o el cumplimiento de un contrato.

Autoridad De Control (Capítulo IV).

El artículo 54 del Decreto señala que la autoridad de control para el tratamiento de datos es la AUTORIDAD NACIONAL DE TRANSPARENCIA Y DE ACCESO A LA INFORMACIÓN (ANTAI), a través de la Dirección de Protección de Datos Personales, es el organismo rector en materia de protección de datos personales. Contará con el apoyo de la AUTORIDAD NACIONAL PARA LA INNOVACIÓN GUBERNAMENTAL (AIG), cuando se trate de aspectos relacionados con las Tecnologías de la Información y las Comunicaciones. La Dirección de Protección de Datos Personales, resolverá, las quejas y peticiones presentadas a la Autoridad de Control.

Sus decisiones pueden ser impugnadas mediante recurso de reconsideración ante la misma o de apelación que se interpondrá ante el Director General de la Autoridad Nacional de Transparencia y Acceso a la Información.

Composición De La Dirección De Protección De Datos Personales. (Artículo 55 Del Decreto).

La Dirección de Protección de Datos Personales deberá estar dotada de perfiles de nivel asesor y de nivel técnico para el desempeño de sus funciones.

Formarán parte de la Dirección de Protección de Datos Personales los servidores públicos que la Dirección General de autoridad de control designe.

El Decreto crea el Consejo de Protección de Datos Personales como ente consultivo en la materia que regula la presente Ley, que estará conformado por:

1. El ministro de Comercio e Industrias o quien este delegue, quien la presidirá.
2. El administrador general de la Autoridad de Protección al Consumidor y Defensa de la Competencia o quien este delegue.
3. El director general de Autoridad Nacional de Transparencia y Acceso a la Información o quien este delegue, quien ejercerá la Secretaría de esta.
4. El defensor del pueblo o quien este delegue.
5. Un representante del Consejo Nacional de la Empresa Privada.
6. Un representante del Colegio Nacional de Abogados.
7. Un representante de la Asociación Bancaria de Panamá.
8. Un representante del Tribunal Electoral.
9. Un representante de la Cámara de Comercio, Industrias y Agricultura de Panamá.

El Consejo de Protección de Datos Personales tendrá las facultades siguientes:

1. Asesorar a la Autoridad Nacional de Transparencia y Acceso a la Información en materia de protección de datos personales, recomendar acciones y reglamentos.
2. Recomendar políticas públicas relacionadas con esta materia.
3. Evaluar casos que le sean presentados para consulta y brindar sus recomendaciones.
4. Desarrollar su reglamento interno.

Responsabilidad Por Las Infracciones A La Ley 81. Finalmente, con referencia a la responsabilidad por las Infracciones, contenidas en el

Capítulo VI del Decreto Ejecutivo, estas infracciones están contenidas en el Capítulo V de la Ley .

La Autoridad Nacional de Transparencia y Acceso a la Información, a través de la Dirección creada para conocer esta materia, está facultada para sancionar a la persona natural o jurídica responsable del tratamiento de los datos personales, así como al custodio de la base de datos, que por razón de la investigación de las quejas o denuncias que se les presenten y se les compruebe que han infringido los derechos del titular de los datos personales.

Las decisiones de la Dirección competente para esta materia dentro de la Autoridad Nacional de Transparencia y Acceso a la Información serán impugnables mediante recurso de reconsideración ante esta Dirección y de apelación que se interpondrá ante el director general de la Autoridad Nacional de Transparencia y Acceso a la Información como segunda instancia, los cuales se sustentarán en un término de cinco días, a partir del día siguiente hábil después de su notificación.

Aquellos casos de queja que se presenten ante los entes reguladores, en los que se realicen tratamientos de datos que se encuentren regulados por leyes especiales y que no se encuentren las sanciones a las faltas cometidas en dichas leyes expresamente tipificadas, el regulador a quien se le interponga la queja deberá aplicar supletoriamente las sanciones establecidas en esta Ley.

La Autoridad Nacional de Transparencia y Acceso a la Información fijará los montos de las sanciones aplicables a las respectivas faltas, acordes a la gravedad de las faltas, que se establecerán desde mil balboas (B/.1,000.00) hasta diez mil balboas (B/.10,000.00), así como reglamentará el procedimiento correspondiente.

Las sanciones pecuniarias que imponga la Autoridad Nacional de Transparencia y Acceso a la Información en el ejercicio de las facultades establecidas en esta Ley que no hayan sido pagadas en el término concedido, se remitirán para su cobro a la Dirección General de Ingresos del Ministerio de Economía y Finanzas.

Deber De Indemnizar Al Responsable Del Tratamiento De Los Datos Personales.
El responsable del tratamiento de los datos personales deberá indemnizar el daño patrimonial y/o moral que causará por el tratamiento indebido de estos, de conformidad con lo establecido en esta Ley o en el ordenamiento legal vigente.

Los tribunales de justicia conocerán de las demandas que se presenten contra los responsables del tratamiento de los datos personales, así como sobre las reclamaciones por daños y perjuicios causados.

CAPÍTULO VI INFRACCIONES Y SANCIONES ART. 38.

Las infracciones a esta Ley se califican en leves, graves o muy graves.
Se considera infracción leve:
No remitir y/o informar a la Autoridad Nacional de Transparencia y Acceso a la Información dentro de los plazos requeridos la información de lo ordenado en esta Ley, su reglamentación o cualquier otra disposición normativa.

Se consideran infracciones graves:
Efectuar el tratamiento de datos personales sin haber obtenido el consentimiento de su titular, según el procedimiento indicado por esta Ley, su reglamentación o cualquier otra disposición normativa que se refiera a la presente Ley.

Infringir los principios y garantías establecidos en la presente Ley o en su reglamentación.

Infringir el compromiso de confidencialidad relacionado al tratamiento de los datos personales.

Restringir o entorpecer la aplicación de los derechos de acceso, rectificación, cancelación y oposición.

Incumplir el deber de informar al titular afectado acerca del tratamiento de sus datos personales, cuando los datos no hayan sido obtenidos del propio titular.

Almacenar o archivar datos personales sin contar con las adecuadas condiciones de seguridad que esta Ley o su reglamento disponga.

No atender la reiteración de los requerimientos u observaciones formalmente notificados, o no proporcionar la documentación o información formalmente solicitada por la Autoridad Nacional de Transparencia y Acceso a la Información.

Entorpecer o no cooperar con la Autoridad Nacional de Transparencia y Acceso a la Información al momento en que esta ejerza su función de inspección.

Se consideran infracciones muy graves:

1. Recopilar de datos personales en forma dolosa.
2. No observar de las regulaciones establecidas respecto al tratamiento de los datos sensibles.
3. No suspender el tratamiento de datos personales cuando existiera un previo requerimiento de la Autoridad Nacional de Transparencia y Acceso a la Información para ello.
4. Almacenar o transferir internacionalmente datos personales, violentando lo establecido en esta Ley.
5. Reincidir en las faltas graves.

Las sanciones que imponga la Autoridad Nacional de Transparencia y Acceso a la Información a los responsables de las bases de datos y demás sujetos alcanzados por el régimen de la presente ley y sus reglamentos, se graduarán dependiendo de la gravedad de la infracción cometida.

CRITERIOS DE GRADUACIÓN DE LAS SANCIONES. Las sanciones previstas en los numerales 2 y 3 del artículo 43 de la Ley 81 de 2019 se aplicarán teniendo en cuenta los criterios de graduación siguientes:

1. La intencionalidad.
2. La reincidencia, por comisión de infracciones de la misma

naturaleza, sancionadas mediante resolución en firme.
3. La naturaleza y cuantía de los perjuicios causados.
4. En plazo de tiempo durante el que se haya estado cometiendo la infracción.
5. El beneficio que haya reportado al infractor la comisión de la infracción.
6. El volumen de la facturación a que afecte la infracción cometida. 7. La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
8. La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
9. La afectación a los derechos de los menores de edad.
10. El haber designado un oficial de protección de datos personales.
11. La adopción reiterada y demostrada de mecanismos y procedimientos internos capaces de minimizar el daño, dirigidos al tratamiento seguro y adecuado de los datos, como, por ejemplo: la adopción de una política de buenas prácticas y gobernanza.
12. La pronta adopción de medidas correctivas.
13. La proporcionalidad entre la gravedad de la falta y la intensidad de la sanción.

Prescripciones. (Artículo 63 de la Ley 81).

Prescripción De La Acción.
La acción de las infracciones tipificadas en la Ley 81 de 2019 prescriben en los siguientes plazos:
Las infracciones leves, prescriben en el plazo de un año. 2. Las infracciones graves prescriben en el plazo de tres años. 3. Las infracciones muy graves prescriben en el plazo de cinco años.

El plazo de prescripción de las infracciones comenzará a correr el día siguiente al que se haya cometido la acción que motiva la infracción. Se interrumpe la prescripción de la infracción por el inicio de la investigación o del procedimiento sancionador.

Prescripción de la sanción.
Las sanciones impuestas con arreglo a la Ley 81 de 2019 prescriben en los siguientes plazos:

1. Las sanciones leves prescriben en un plazo de tres años.
2. Las sanciones graves prescriben en un plazo de cinco años.
3. Las sanciones muy graves son imprescriptibles.

El plazo de prescripción de las sanciones comenzará a correr el día siguiente al que se haya impuesto. Se interrumpe la prescripción de la sanción por cualquier acto que tienda a la ejecución de la resolución que la impuso.

4. Resolución No. 23-2022 – INEC de 12 de enero 2022.

El Código Nacional de Buenas prácticas para las actividades estadísticas fue aprobado por el Instituto Nacional de Estadísticas y Censo (INEC) de la Contraloría General de la República por la gaceta oficial digital no. 29611 de 31 de agosto de 2022, con la finalidad establecer requisitos en la aplicación y cumplimiento del marco legal regulatorio que conforma el Sistema Estadístico Nacional (SEN), y de esta forma garantizar la eficiencia y calidad del proceso de producción estadística, evitando la duplicidad de esfuerzos y optimizando los recursos, para que se cuente con una data estadística de país, confiable y segura.

El Código Nacional de Buenas Prácticas Estadísticas está conformado por once 11 principios y fue elaborado tomando en cuenta el Código Regional de Buenas Prácticas adoptado por los países miembros de la Conferencia Estadística de las Américas (CEA), así como la Declaración sobre Ética Profesional del Instituto Internacional de Estadísticas (ISI) y los Principios Fundamentales de las Estadísticas Oficiales de la Comisión de Estadísticas de las Naciones Unidas, en cuya adaptación se tuvieron presente las particularidades nacionales, en materia de estadística. Este Código fue aprobado mediante la Resolución No. 23-2022-INEC de 12 de enero de 2022.

Su marco legal establece dos tipos de principios que rigen la actividad estadística:

A. Entorno institucional: Independencia, Secreto estadístico, Imparcialidad, Transparencia, Accesibilidad

B. Producción estadística: Coherencia, Comparabilidad, Oportunidad Puntualidad

Secreto Estadístico:

Obligación de las entidades públicas que integran el SEN, de tratar los datos individuales proporcionados por la fuente de información con absoluta confidencialidad, de tal manera, que no se revele su identidad y sean utilizados exclusivamente para fines estadísticos.

Se dispone de protocolos, estructuras físicas, tecnológicas y organizativas para proteger la seguridad y la integridad de las bases de datos.

El acceso a microdatos o bases de datos debe estar sujeto a protocolos de confidencialidad, establecidos para usuarios externos que acceden con fines de análisis e investigación estadística.

Se debe informar a las fuentes acerca de los principales usos y limitaciones de acceso que se aplican a la información que ellas proporcionan.

Se debe archivar la información de acuerdo con los protocolos de seguridad y

Confidencialidad establecidos, y con las normas vigentes.

5. Ley 64 de 10 de octubre de 2012 sobre Derechos de Autor y Derechos Conexos.

La ley 64 de 10 de octubre de 2012, sobre Derechos de Autor y Derechos Conexos de la República de Panamá, protege las obras originarias: literarias, musicales, teatrales, audiovisuales, programas de ordenadores (software) y artísticas (arquitectura, escritura, dibujo, pintura, fotografía y artes aplicadas).

De igual manera, se protegen las obras derivadas como: adaptaciones, traducciones, compilaciones y bases de datos, antologías, anotaciones

y comentarios, actualizaciones, resúmenes, extractos, parodias, arreglos y orquestaciones.

La protección de los Derechos de Autor surge con la creación de la obra y en términos generales, la protección de los derechos patrimoniales se hace efectiva durante la vida del autor y 70 años después de su muerte.

Dentro de nuestro estudio identificamos en la Ley 64 sobre Derechos de Autor y Derechos Conexos, el Capítulo III, denominado “Bases y compilaciones de datos”.

“Capítulo III Bases y compilaciones de datos
Artículo 33.
Las bases o compilaciones de datos o de otros materiales, legibles por máquina o en cualquier otra forma, están protegidas siempre que por la selección o disposición de las materias constituyan creaciones intelectuales.
La protección así reconocida no se hace extensiva a los hechos, datos, informaciones o material compilados en sí mismos, pero no afecta los derechos intelectuales que pudieran subsistir sobre las obras o materiales que conforman la compilación.

6. Código Penal de la República de Panamá

El artículo 262 del Título VII del Código Penal de la República de Panamá, denominado “De los delitos contra la propiedad intelectual” regulan los derechos de autor y derechos conexos.

En ese sentido el artículo 262 ordinales 6, 7 y 8 establece: “Artículo 262. Se impondrá pena de uno a tres años de prisión o de doscientos a cuatrocientos días multa a quien, sin la correspondiente autorización del titular o fuera de los límites permitidos por las normas sobre los Derechos de Autor y Derechos Conexos, realice cualesquiera de las siguientes conductas:

Emplee indebidamente el título de una obra, sin el consentimiento del autor, para identificar otra del mismo género, cuando exista peligro de

confusión entre ambas.

Se atribuya falsamente la calidad de titular originario o derivado de los derechos morales y patrimoniales del autor.

Comunique públicamente, por cualquier forma o procedimiento, una obra debidamente protegida, en forma original o transformada, íntegra o parcialmente, en violación a los derechos morales y patrimoniales del autor.

Comunique, reproduzca o distribuya la obra después de vencido el plazo de autorización que se haya convenido o en número mayor de ejemplares que el permitido por contrato.

Retransmita, por cualquier medio alámbrico o inalámbrico, reproducción y retransmisión de las emisiones de los organismos de radiodifusión de cable o satélite.

Modifique total o parcialmente una obra protegida por el Derecho de

Autor y Derechos Conexos.

Ponga a disposición del público transmisiones de interpretaciones o ejecuciones artísticas o de producciones fonográficas.

Incurra en infracción dolosa de piratería lesiva de derecho de autor o derechos conexos, que no tenga una motivación directa o indirecta de ganancia económica y cauce un daño económico mayor a una infracción de poco valor

Se impondrá pena de uno a tres años de prisión o de doscientos a cuatrocientos días multa a quien, sin la correspondiente autorización del titular o fuera de los límites permitidos por las normas sobre los Derechos de Autor y Derechos Conexos, realice cualesquiera de las siguientes conductas:

Modifique total o parcialmente una obra protegida por el Derecho de Autor y Derechos Conexos.

Ponga a disposición del público transmisiones de interpretaciones o ejecuciones artísticas o de producciones fonográficas.

Incurra en infracción dolosa de piratería lesiva de derecho de autor o derechos conexos, que no tenga una motivación directa o indirecta de ganancia económica y cauce un daño económico mayor a una infracción de poco valor.

Por otro lado, el artículo 263, señala que: “Se impondrá pena de dos a cuatro años de prisión a quien, sin la correspondiente autorización del titular o fuera de los límites permitidos por las normas sobre los Derechos de Autor y Derechos Conexos, realice cualesquiera de las siguientes conductas:

Inscriba en el Registro de Derecho de Autor y Derechos Conexos una obra, interpretación o producción ajena, como si fuera propia o de persona distinta del verdadero autor, artista o productor.

Utilice ejemplares de la obra, sin autorización y los ponga a disposición del público, inclusive la distribución de fonogramas.

Presente declaraciones falsas de certificaciones de ingresos, repertorio utilizando identificación de los autores; autorización obtenida, número de ejemplares o cualquier otra adulteración de datos susceptibles de causar perjuicio a cualquiera de los titulares de derechos protegidos.

Realice actividades propias de una entidad de gestión colectiva, sin contar con la resolución emitida al efecto por la autoridad competente.

Usurpe la paternidad de una obra protegida por el Derecho de Autor y Derechos Conexos.

Reproduzca, copie o modifique íntegra o parcialmente una obra protegida por el Derecho de Autor y Derechos Conexos, fijada de manera provisional o permanente, de una obra protegida por el

Derecho de Autor y Derechos Conexos.

Los artículos 266 A y 266 B, establecen:
Artículo 266-A. Quien, con el fin de lograr una ventaja comercial o ganancia financiera privada, evada sin autorización cualquier medida tecnológica que controle el acceso a una obra,
interpretación, ejecución o fonograma protegido, será sancionado con prisión de uno a tres años.

Artículo 266-B. Se impondrá la pena de dos a cuatro años de prisión a quien fabrique, importe, distribuya, ofrezca al público, proporcione o de otra manera trafique dispositivos, productos, o componentes, u ofrezca al público o proporcione servicio, los cuales:

Son promocionados, publicitados, o comercializados con el propósito de evadir una medida tecnológica efectiva; o

Únicamente tienen un limitado propósito o uso de importancia comercial diferente al de evadir una medida tecnológica efectiva; o

Son diseñados, producidos o ejecutados principalmente con el fin de permitir o facilitar la evasión de cualquier medida tecnológica efectiva.

Quedan excluidos del alcance de lo dispuesto en el Artículo 266-A y este artículo las bibliotecas, archivos, instituciones educativas u organismos públicos de radiodifusión no comercial sin fines de lucro.
Artículo 266-C. Se impondrá la pena de dos a cuatro años a quien realice sin autorización y de manera dolosa, con el fin de lograr una ventaja comercial o ganancia financiera privada, respecto a la información sobre gestión del Derecho de Autor o Derechos Conexos, alguna de las siguientes acciones:

1. Suprima o altere cualquier información sobre gestión de derechos;

2. Distribuya o importe para su distribución, información sobre gestión de derechos sabiendo que esa información sobre gestión de derechos ha sido suprimida o alterada sin autoridad;

3. Distribuya, importe para su distribución, transmita, comunique o ponga a disposición del público copias de obras, interpretaciones o ejecuciones o fonogramas, sabiendo que la información sobre gestión de derechos ha sido suprimida o alterada sin autoridad.

Quedan excluidos del alcance de lo dispuesto en el presente artículo las bibliotecas, archivos, instituciones educativas u organismos públicos de radiodifusión no comercial sin fines de lucro.
Preparación:

1. Conocer a fondo la audiencia:
Investigar las funciones y responsabilidades de las autoridades involucradas en el proyecto CSCP.
Identificar a los tomadores de decisiones clave.
Adaptar el lenguaje y el nivel de detalle de la propuesta a la audiencia.

2. Dominar la propuesta jurídica:
Asegurarse de comprender completamente todos los aspectos de la propuesta jurídica.
Anticipar posibles preguntas y objeciones de las autoridades.
Practicar la presentación para garantizar una entrega clara y concisa.

3. Recopilar materiales de apoyo:
Preparar presentaciones visuales que complementen la información verbal.
Redactar folletos o resúmenes de la propuesta jurídica. Anticipar la necesidad de cualquier material adicional, como datos estadísticos o informes legales.
Presentación:

4. Estructura clara y organizada:
Comenzar con una introducción sólida que resuma los objetivos de la propuesta.
Desarrollar los puntos clave de la propuesta de manera lógica y ordenada.
Concluir con una llamada a la acción que solicite la aprobación e implementación de la propuesta.

5. Comunicación efectiva:
Utilizar un lenguaje claro, conciso y profesional.
Evitar tecnicismos legales innecesarios.
Enfatizar los beneficios de la propuesta para el proyecto
CSCP. Hablar con confianza y entusiasmo.

6. Responder preguntas y objeciones:
Escuchar atentamente las preguntas y objeciones de las
autoridades. Responder de manera completa, precisa y educada.
Estar preparado para defender los argumentos de la propuesta jurídica.

7. Seguimiento:
Agradecer a las autoridades por su tiempo y
atención. Reiterar los puntos clave de la propuesta.
Proporcionar información de contacto para futuras
consultas. Recomendaciones adicionales:
Considerar la posibilidad de involucrar a un experto legal externo en la presentación.

Adaptar la propuesta jurídica a las necesidades y requisitos específicos del Cuenta Satélite de Cultura de Panamá.
Enfatizar cómo la propuesta jurídica se alinea con los objetivos estratégicos del proyecto CSCP.
Demostrar el compromiso de implementar la propuesta de manera efectiva y eficiente.

7. Decreto Ejecutivo No. 52 de 30 de abril de 2008.

El Decreto No. 52 de 30 de abril de 2008, es la Ley Bancaria de Panamá, crea la Superintendencia Bancos de Panamá, contiene normas aplicables al suministro de información:

“ARTÍCULO 200. SUMINISTRO DE INFORMACIÓN. Del contenido del artículo 36 de la Ley 45 de 2007, sólo le será aplicable a los bancos lo establecido en los numerales 1, 2, 7, 9, 12 y 13, los cuales establecen la obligación de suministrar información a su consumidor bancario.

Para los efectos de lo establecido en dichos numerales, y siempre que los contratos bancarios se ajusten a las exigencias de ley, se entenderá que los proveedores cumplen con la obligación de suministrar información al consumidor bancario, con la entrega del documento que contenga el contrato o los términos y condiciones del servicio o producto de que se trate."

Esta norma se encuentra relacionada como podemos ver, con el artículo 36 de la Ley No. 45 de 31 de octubre de 2007, que establece el deber de informar a los consumidores.

ANEXO 1.

Criterios legales para los acuerdos de confidencialidad entre las instituciones aliadas a la CSCP

Los siguientes son los criterios legales que deben tomarse en cuenta preparar acuerdos o convenios de confidencialidad técnica entre el Ministerio de Cultura, Instituto Nacional de Estadísticas y Censos y organizaciones pública y privadas de la República de Panamá, tomando en consideración las normativas legales existentes que se encuentra detalladas en el ANEXO de este documento:

- Finalidad. Consideramos en primer lugar que cada acuerdo de confidencialidad y cooperación técnica debe ser específico para el proyecto o acuerdo que se va a realizar. En otras palabras, debe especificar con claridad la finalidad de este, estableciendo la información de las responsabilidades de cada parte, para que no se presente ambigüedades en el documento a firmar. Especificar el alcance del convenio, incluyendo las instituciones participantes, los tipos de datos culturales que se compartirán y las actividades de colaboración previstas.
- Objeto y alcance. Definir claramente el objetivo principal del convenio, que es la implementación del Protocolo de Interoperabilidad de los Datos de la CSCP.
- Obligaciones de las partes. Establecer las obligaciones específicas de cada parte involucrada, tales como la provisión de datos, la implementación de las medidas técnicas y
- organizativas necesarias para garantizar la seguridad de los datos, la participación en actividades de capacitación y sensibilización, etc.
- Intercambio de datos. Definir los mecanismos y procedimientos para el intercambio de datos culturales, incluyendo la frecuencia, el formato y los estándares de calidad de los datos.
- Período de duración. Debe contener el período de duración del acuerdo; esto es que el tiempo que va a durar el mismo se determine específicamente y en caso de que el mismo sea a perpetuidad señalar esta situación.

- Consideramos esta cláusula importante, tomando en consideración que en el Protocolo se van a realizar acuerdos para la realización de un objetivo específico y deben de especificarse tiempos para su cumplimiento.

- Ámbito de aplicación. El protocolo tiene como base legal la Ley 81 de 26 de marzo de 2019, que señala cual es el ámbito de aplicación de esta. En este sentido debemos referirnos específicamente en el ANEXO B, a los artículos 3 que contiene las excepciones de su ámbito de aplicación y el artículo 5 ibidem , que señala que bases de datos están sujetas a las normas establecidas en la Ley.

- Clausula lingüística/Idioma. Si bien es cierto el idioma oficial de la República de Panamá, consideramos que se debe especificar el nombre del idioma rector, su influencia en la interpretación y ejecución del contrato, y la situación de cualquier traducción o versión del contrato en otros idiomas. Además, también debe establecer quién es responsable de proporcionar traducciones o versiones del contrato en otros idiomas, así como quién asumirá el costo. De igual manera realizamos recomendación en caso de realizarse convenios internacionales que incluyan países del área cuyo idioma oficial no sea el español.

- Principios del convenio. La Ley 81 de 26 de marzo de 2019, recoge una serie de principios en los que se inspira y rige la protección de datos de carácter personal (Anexo B artículo 2). Señalando específicamente que deben reconocerse los derechos irrenunciables básicos que tienen los titulares de datos personales, llamados ARCOS: ACCESO, RECTIFICACIÓN, CANCELACIÓN, OPOSICIÓN (ANEXO B Artículo 15), incluyéndose en nuestra legislación el de PORTABILIDAD)ANEXO B, Artículo 15, ordinal 5).

- Principios que rigen la actividad estadística en el entorno institucional, con especial énfasis en el Secreto Estadístico y sus criterios de cumplimiento (ANEXO D, artículo A, ordinal 12).

- Ley aplicable. La ley aplicable en los acuerdos de confidencialidad: Ley No. 19 de 26 de marzo de 2019, el Decreto Ejecutivo No. 285 de 28 de mayo de 2021, que reglamenta la Ley anterior, Ley 64 de 10 de octubre de 2012, Capítulo III, sobre Bases y compilaciones de datos, Resolución No. 23-2022-INEC de 12 de enero de 2022, por el cual se aprueba el Código Nacional de Buenas Prácticas para las actividades estadísticas, el Código Penal de la República de Panamá.
- Resolución de controversias. Establecer un mecanismo para la resolución de controversias que puedan surgir entre las partes involucradas. Considerar la posibilidad de incluir una cláusula de arbitraje para la resolución de disputas.
- Medidas de seguridad. Establecer medidas de seguridad para garantizar la confidencialidad, integridad y disponibilidad de los datos durante el proceso de intercambio.
- Propiedad intelectual. Clarificar la propiedad intelectual de los datos culturales compartidos, asegurando el respeto a los derechos de los titulares de los datos.
- Sanciones aplicables. Tanto la Ley 81 de 26 de marzo de 2019, (ANEXO A, artículo 43) como el Código Penal de la República de Panamá, (ANEXO E, Título VIII, Capítulo I), contienen sanciones a las personas naturales o jurídicas responsable del tratamiento de datos.
- Autoridad facultada. La Autoridad Nacional de Transparencia y Acceso a la información a través de la Dirección correspondiente, cuando se traten de faltas leves, graves o muy graves (ANEXO B Artículo 38). Y EL órgano Judicial cuando se traten de delitos tipificados en el Código Penal de la República de Panamá.

Recomendaciones adicionales.

Establecer mecanismos para la gestión de licencias y permisos de uso de los datos.

Involucrar a las instituciones relevantes en el proceso de elaboración de los convenios de cooperación para garantizar su aceptación y compromiso.

Realizar talleres de capacitación y sensibilización para el personal de las instituciones involucradas sobre los términos y condiciones de los convenios de cooperación.

Establecer mecanismos de seguimiento y evaluación para monitorear el cumplimiento de los convenios de cooperación y su impacto en la implementación del Protocolo de Interoperabilidad de los Datos de la CSCP.

REFERENCIAS BIBLIOGRÁFICAS

Constitución Política de la República de Panamá, Edición actualizada según la reforma del año 2004. Editorial Cultural Portobelo. Panamá 2005.

Código Penal de la República de Panamá, Editorial Mizrachi y Pujol, S. A. Junio 2004.

https//asesorapyme.org/2023/05/12/7-criterios-de-evaluación-de software.

Ley No. 81 de 26 de marzo de 2019 Sobre protección de datos personales.

Ley 64 de 10 de octubre de 2012 sobre derechos de autor y derechos conexos, gaceta oficial digital no. 27139-b de 10 de octubre de 2012. Decreto ejecutivo no. 52 de 30 de abril de 2008.

ISBN: 978-9962-56-111-8