Propuesta de marco regulatorio y de gobernanza

Red Ciudadana

GUATEMALA
GUATEMALA NO SE DETIENE

Resumen Ejecutivo

La protección de datos personales es una prioridad global en la era de la digitalización. Este documento proporciona un análisis exhaustivo de la propuesta de marco normativo para la protección de datos en Guatemala, comparándola con estándares internacionales como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Se destacan los principios fundamentales, derechos de los titulares de datos, responsabilidades de los procesadores de datos, y se examinan las medidas disciplinarias y los procedimientos administrativos para la resolución de conflictos.

El marco propuesto establece principios de tratamiento de datos que incluyen legalidad, transparencia, limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, y responsabilidad. Estos principios son esenciales para garantizar que el tratamiento de los datos personales se realice de forma justa y legal, proporcionando una base sólida para la protección de datos personales.

Se refuerzan los derechos de los individuos sobre sus datos personales, garantizando su derecho al acceso, rectificación, supresión, limitación del tratamiento, portabilidad de datos, y oposición. Estos derechos permiten a los individuos tener un control significativo sobre sus datos personales, asegurando su capacidad para proteger su privacidad y autonomía en la gestión de su información personal.

Las entidades que manejan datos personales están obligadas a adoptar medidas técnicas y organizativas adecuadas para asegurar y proteger los datos personales. Esto incluye la implementación de políticas de seguridad, la realización de evaluaciones de impacto en la protección de datos y el mantenimiento de registros detallados de las actividades de tratamiento de datos.

El marco normativo establece un sistema de sanciones para el incumplimiento, que incluye multas económicas, sanciones administrativas, e incluso sanciones penales para delitos graves relacionados con el tratamiento indebido de datos personales. Este sistema busca disuadir el incumplimiento y promover el cumplimiento de las normas de protección de datos.

Este resumen ejecutivo enfatiza la importancia de un marco normativo robusto para la protección de datos personales en Guatemala. La propuesta refleja un esfuerzo serio por alinear la legislación local con estándares internacionales, promoviendo así un entorno seguro y confiable para el tratamiento de datos personales en la era digital.

Tabla de contenidos

Resumen Ejecutivo **2**

Tabla de contenidos **3**
Objetivos de la Consultoría **5**
Contexto de la consultoría 5
Productos de la consultoría 5
Producto 2. Propuesta de Marco Regulatorio y de Gobernanza 5
Marco Regulatorio y de Gobernanza de datos **5**
Modelo Ideal de Gobernanza de Datos **6**
Alineación y diferencias **10**
Ámbito de Aplicación 10
Enfoque en la Protección de Datos desde el Diseño y por Defecto 11
Transferencias Internacionales de Datos 11
Régimen de Sanciones 11
Participación Pública y Conciencia 11
Enfoque Regulatorio 11
Propuesta de marco regulatorio y de gobernanza **12**
1. Preceptos Fundamentales 12
Capítulo I: Disposiciones Generales 12
Capítulo II: Principios Rectores 12
Principios Clave: 12
Capítulo III: Generalidades del Tratamiento de Datos Personales 13
Directrices Generales: 13
2. Titulares de Datos Personales 13
Capítulo 1: Derechos de los Titulares de Datos Personales 13
Derechos Específicos de los Titulares de Datos Personales 13
Mecanismos de Ejercicio y Protección de los Derechos 15
3. Obligaciones del Responsable y del Encargado de Tratamiento de Datos Personales 15
Obligaciones Generales 15
Obligaciones Específicas 16
Responsabilidades Adicionales 16
4. Autoridades 17
Capítulo I: Consejo Nacional de Protección de Datos Personales 17
Funciones del CNPDP 17
Capítulo II: Instituto Guatemalteco de Protección de Datos Personales 18
Sección I: Creación, Funciones, Presupuesto y Recursos Financieros 18
Funciones del Instituto Guatemalteco de Protección de Datos Personales 18
Sección II: Dirección General 18
Responsabilidades y Supervisión 19
5. Presupuesto y recursos financieros 19
Asignación de Presupuesto 19

Recursos Financieros 20
Gestión de Recursos 20
6. Procedimiento de verificacion 20
Objetivo del Procedimiento de Verificación 21
Procesos y Etapas del Procedimiento de Verificación 21
Transparencia y Participación Pública 22
Capacitación y Recursos 22
7. Infracciones y sanciones 22
Definición de Infracciones 22
Sanciones Aplicables 23
Procedimientos para la Imposición de Sanciones 24
8. Procedimientos administrativos para solucion de conflictos 24
Sección I: Disposiciones Generales 24
Sección II: Conciliación entre las Partes 25
Sección III: Procedimiento de Protección de Datos Personales 25
Sección IV: Aplicación de las Resoluciones 25
Sección V: Impugnación de las Resoluciones 26
9. Delitos en materia de tratamiento de datos personales 26
Delitos Específicos 26
Penalizaciones 27
10. Disposiciones transitorias, finales y derogatorias 27
Disposiciones Transitorias 28
Disposiciones Finales 28
Disposiciones Derogatorias 28
Conclusiones y Modelos Recomendados 29
Bibliografía 30
Anexos 30

Objetivos de la Consultoría

Contexto de la consultoría

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

Productos de la consultoría

Producto 2. Propuesta de Marco Regulatorio y de Gobernanza

- La consultoría se propone desarrollar un marco regulatorio específico que estandarice las prácticas digitales en el sector público. Este marco incluirá directrices sobre seguridad de datos, privacidad, accesibilidad y uso ético de la tecnología, asegurando que la digitalización de los servicios públicos se realice de manera responsable y beneficiosa para la ciudadanía.

Marco Regulatorio y de Gobernanza de datos

La teoría de la protección de datos se fundamenta en principios universales que garantizan que el tratamiento de los datos personales se realice de manera justa, legal y transparente. Estos principios incluyen la limitación de la finalidad, minimización de datos, exactitud, limitación del almacenamiento, integridad y confidencialidad, y responsabilidad (European Commission, 2020).

El enfoque en los derechos de los individuos es central en la teoría de la protección de datos. Estos derechos incluyen el acceso, rectificación, supresión, y la objeción al procesamiento de datos personales, así como el derecho a la portabilidad de los datos (European Commission, 2020). Estos derechos aseguran que los individuos puedan controlar sus datos personales y desafiar el tratamiento cuando se infringen sus derechos de privacidad.

Desde una perspectiva teórica, la responsabilidad de los procesadores de datos es asegurar que los principios de protección de datos se apliquen efectivamente. Esto implica implementar medidas técnicas y organizativas adecuadas para proteger los datos personales y garantizar la transparencia en el tratamiento de los datos (Kuner et al., 2017).

El análisis comparativo de legislaciones como el GDPR y las propuestas legislativas en países como Guatemala revela cómo se adaptan los principios y directrices a diferentes contextos socio-legales. A pesar de las similitudes en los principios básicos, las diferencias en el alcance de aplicación, sanciones, y procedimientos de implementación reflejan adaptaciones necesarias a las realidades locales (Bygrave, 2017).

El rápido avance de la tecnología digital plantea nuevos desafíos y oportunidades para la protección de datos. La teoría debe considerar cómo la inteligencia artificial, el big data y las tecnologías emergentes afectan la privacidad y el tratamiento de datos personales (Zarsky, 2016).

Modelo Ideal de Gobernanza de Datos

Definición y Componentes Clave del Modelo

La gobernanza de datos se refiere al conjunto de procesos, responsabilidades, políticas y métricas que aseguran el uso efectivo y eficiente de la información en una organización. En el contexto de un gobierno, esto implica una estructura que no solo gestiona los datos, sino que también los transforma en un activo estratégico. Un modelo ideal de gobernanza de datos debe incluir varios componentes clave:

- **Políticas y Estándares:** Establecer políticas claras y coherentes es fundamental. Estas políticas deben definir cómo se deben manejar y proteger los datos, establecer normas para la calidad de datos, privacidad, seguridad y uso compartido de datos. Deben ser flexibles para adaptarse a los cambios en el entorno y al avance de la tecnología, pero también lo suficientemente robustas para garantizar la integridad y confidencialidad de los datos.

- **Estructura Organizativa:** Es importante contar con una estructura organizativa clara y bien definida para la gestión de datos. Esto incluye la creación de roles y responsabilidades específicos, como un comité de gobernanza de datos, administradores de datos y propietarios de datos. Estos roles deben tener autoridad y recursos suficientes para cumplir con sus responsabilidades.

- **Procesos de Gestión de Datos:** Desarrollar procesos estandarizados para la recopilación, almacenamiento, procesamiento, distribución y eliminación de datos es esencial. Estos procesos deben ser eficientes y eficaces, minimizando el riesgo de errores y asegurando la integridad y disponibilidad de los datos cuando sea necesario.

- **Cultura y Capacitación:** Fomentar una cultura organizativa que valore los datos como un activo crítico es fundamental. Esto implica crear conciencia sobre la importancia de los datos y proporcionar capacitación continua en gestión y protección de datos para todo el personal. La cultura organizativa debe promover la transparencia y la colaboración en el manejo de los datos.

- **Tecnología y Herramientas:**Implementar las herramientas y tecnologías adecuadas es crucial. Esto incluye sistemas de almacenamiento seguro, herramientas de análisis y visualización de datos, así como soluciones de seguridad de la información. Estas herramientas deben ser compatibles con las políticas y estándares establecidos y permitir la gestión efectiva de los datos en toda la organización.

- **Métricas y Monitoreo:**Establecer métricas para evaluar la calidad y eficacia de la gestión de datos es fundamental. Esto permite realizar un seguimiento del cumplimiento de las políticas y estándares establecidos y realizar mejoras continuas en la gestión de datos. El monitoreo continuo es clave para identificar y abordar de manera proactiva cualquier problema que pueda surgir en la gestión de datos.

- **Participación Ciudadana y Transparencia:** Asegurar la transparencia en el manejo de los datos y fomentar la participación ciudadana en la toma de decisiones relacionadas con datos son aspectos clave. Esto implica proporcionar acceso público a los datos cuando sea apropiado y permitir que los ciudadanos participen en la formulación de políticas de datos abiertos y en la evaluación de su impacto en la sociedad.

Directrices y principios recomendados:

El marco regulatorio para la digitalización de los servicios públicos en Guatemala debe considerar las siguientes directrices y principios:

1. Seguridad de Datos:

a. **Evaluaciones de Riesgo y Auditorías Regulares:** Implementar evaluaciones de riesgo obligatorias antes de iniciar cualquier proyecto que involucre datos personales, seguidas de auditorías regulares para asegurar el cumplimiento continuo con las normativas de seguridad.

b. **Cifrado y Protección de Datos:** Todos los datos personales deben ser cifrados tanto en reposo como en tránsito para protegerlos contra accesos no autorizados, pérdidas o filtraciones.

c. **Control de Acceso y Autenticación:** Definir e implementar políticas de control de acceso basadas en el principio de mínimo privilegio, junto con sistemas de autenticación robustos que aseguren que solo personal autorizado pueda acceder a la información sensible.

d. **Respuesta a Incidentes y Recuperación de Datos:** Establecer un plan de respuesta a incidentes de seguridad que incluya procedimientos para la notificación a las partes afectadas y autoridades reguladoras. Asimismo, desarrollar estrategias de recuperación de datos para minimizar la pérdida de información en caso de un incidente de seguridad.

2. Privacidad

a. Consentimiento Informado y Gestión de Preferencias: Asegurar que todos los ciudadanos tengan la capacidad de proporcionar un consentimiento informado para el procesamiento de sus datos personales, con facilidades para gestionar y retirar este consentimiento en cualquier momento.

b. Transparencia y Comunicación: Proveer a los ciudadanos información clara sobre cómo se utilizan sus datos, quién tiene acceso a ellos y cuáles son sus derechos respecto a esos datos.

c. Limitación de Propósito y Retención de Datos: Los datos recopilados deben ser usados exclusivamente para los fines especificados y no deben ser retenidos por más tiempo del necesario para cumplir con esos propósitos.

d. Derechos de Acceso y Rectificación: Facilitar mecanismos para que los ciudadanos accedan a sus datos personales almacenados por entidades gubernamentales y soliciten su corrección o eliminación cuando sea apropiado.

3. Accesibilidad

a. Diseño Universal: Desarrollar servicios digitales con un enfoque de diseño universal, asegurando que sean accesibles para todos los ciudadanos, incluyendo aquellos con discapacidades.

b. Facilidad de Uso: Los servicios digitales deben ser fáciles de usar y entender, con interfaces intuitivas que no requieran conocimientos técnicos avanzados.

c. **Soporte y Formación:** Proveer soporte continuo y oportunidades de formación para los usuarios de los servicios digitales, asegurando que todos los ciudadanos puedan beneficiarse de la digitalización de los servicios públicos.

4. Uso Ético de la Tecnología

a. **Principios Éticos en IA y Automatización**: Establecer directrices éticas para el desarrollo y uso de tecnologías como la inteligencia artificial en servicios públicos, incluyendo la transparencia, la equidad y la responsabilidad.

b. **Protección contra el Sesgo y la Discriminación:** Implementar medidas para detectar y mitigar el sesgo en algoritmos y bases de datos para evitar la discriminación.

c. **Supervisión y Evaluación Continua:** Crear un comité ético para supervisar la implementación y el funcionamiento de tecnologías emergentes en el sector público, asegurando que estas tecnologías se utilizan de manera que respeten los derechos y libertades de todos los ciudadanos.

Implementando estas directrices, Guatemala puede garantizar que la transformación digital de sus servicios públicos no solo mejore la eficiencia y accesibilidad de estos servicios, sino que también proteja y respete los derechos de sus ciudadanos en el proceso.

Importancia de un Modelo de Gobernanza de Datos para la Transformación Digital

La transformación digital en el sector público implica la integración de tecnologías digitales en todos los aspectos de las operaciones gubernamentales para mejorar la prestación de servicios, aumentar la eficiencia y fomentar la participación ciudadana. En este contexto, los datos juegan un papel fundamental, ya que son la base sobre la cual se construyen las soluciones digitales. Por lo tanto, la implementación de un modelo de gobernanza de datos eficaz es crucial para el éxito de la transformación digital en el sector público por varias razones:

- **Mejora de la Toma de Decisiones:** Un modelo de gobernanza de datos bien establecido garantiza que los datos utilizados para la toma de decisiones sean precisos, confiables y oportunos. Esto permite a los líderes gubernamentales tomar decisiones más informadas y basadas en evidencia, lo que conduce a políticas más efectivas y eficientes.

- **Optimización de Servicios:** La transformación digital busca mejorar la prestación de servicios públicos a través de la tecnología. Un modelo de gobernanza de datos eficaz garantiza que los datos necesarios para optimizar los servicios estén disponibles, lo que puede llevar a una mayor eficiencia y satisfacción del ciudadano.

- **Promoción de la Innovación:** Una buena gobernanza de datos fomenta la innovación al facilitar el acceso a datos para el desarrollo de nuevas soluciones y servicios. Esto puede impulsar la creación de aplicaciones y herramientas innovadoras que mejoren la calidad de vida de los ciudadanos.

- **Protección de la Privacidad:** La transformación digital puede plantear desafíos en términos de protección de la privacidad de los ciudadanos. Un modelo de gobernanza de datos sólido incluye políticas y prácticas para garantizar que los datos personales se manejen de manera segura y se protejan de posibles infracciones de seguridad.

- **Aumento de la Transparencia y la Confianza:** La transparencia en el manejo de datos es esencial para construir la confianza de los ciudadanos en las iniciativas digitales del gobierno. Un modelo de gobernanza de datos que promueva la transparencia ayuda a garantizar que los ciudadanos comprendan cómo se utilizan sus datos y por qué, lo que puede aumentar su confianza en el gobierno.

En resumen, un modelo de gobernanza de datos efectivo es fundamental para la transformación digital en el sector público, ya que garantiza que los datos se utilicen de manera responsable, eficiente y segura. Esto no solo mejora la prestación de servicios y la toma de decisiones, sino que también construye la confianza de los ciudadanos en las iniciativas digitales del gobierno.

Aplicabilidad en el Contexto Guatemalteco

La implementación de un modelo de gobernanza de datos en Guatemala presenta desafíos únicos, pero también oportunidades significativas. El país, con sus particularidades culturales, económicas y tecnológicas, requiere un enfoque personalizado que considere estas variables.

- **Alineación con el Contexto Local:** Es crucial que el modelo de gobernanza de datos se alinee con las realidades sociopolíticas y económicas de Guatemala. Esto incluye considerar los niveles de alfabetización digital, la infraestructura tecnológica existente y las particularidades culturales en la percepción y uso de los datos.

- **Foco en la Inclusión Digital:** La gobernanza de datos debe promover la inclusión digital, asegurando que los beneficios de la transformación digital lleguen a todos los sectores de la sociedad guatemalteca, incluyendo las áreas rurales y las comunidades indígenas.

- **Desarrollo de Capacidades Locales:** Es esencial el desarrollo de capacidades locales en materia de gestión de datos. Esto implica no solo la formación de personal especializado sino también la sensibilización y capacitación a nivel de usuarios y ciudadanos.

- **Colaboración Público-Privada:** La colaboración entre el sector público, el sector privado y las organizaciones no gubernamentales puede ser un motor clave para el desarrollo de un modelo de gobernanza de datos eficaz. Esta colaboración puede facilitar la transferencia de conocimientos, la innovación tecnológica y la inversión en infraestructura.

- **Adaptabilidad y Escalabilidad:** El modelo debe ser lo suficientemente flexible para adaptarse a los cambios rápidos en la tecnología y en el entorno socioeconómico, y escalable para acomodar el crecimiento y la evolución de las necesidades de gestión de datos.

Implementar un modelo de gobernanza de datos en Guatemala requerirá un enfoque integral, considerando factores locales y globales, y promoviendo una colaboración efectiva entre

diferentes actores. Este esfuerzo no solo mejorará la eficiencia y eficacia del sector público, sino que también será un paso importante hacia la construcción de una sociedad más informada, participativa y digitalmente empoderada.

Alineación y diferencias

Aunque la propuesta de marco normativo para la protección de datos en Guatemala se inspira en el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y comparte muchas similitudes, también existen diferencias significativas entre ambos, que reflejan adaptaciones a las realidades legales, culturales y administrativas específicas de Guatemala. Aquí algunas de las principales diferencias:

Ámbito de Aplicación

- **GDPR**: Tiene un alcance extraterritorial muy amplio, aplicándose no solo a las entidades dentro de la UE, sino también a organizaciones fuera de la UE que procesan datos de residentes de la UE.
- **Propuesta guatemalteca:** Su aplicación probablemente se limite a las entidades que operan dentro de Guatemala, sin extender su alcance a entidades fuera de las fronteras nacionales que procesen datos de ciudadanos guatemaltecos.

Enfoque en la Protección de Datos desde el Diseño y por Defecto

- **GDPR:** Exige que la protección de datos desde el diseño y por defecto sea incorporada en todas las operaciones de tratamiento de datos desde las primeras etapas.
- **Propuesta guatemalteca:** Aunque promueve la adopción de medidas técnicas y organizativas para garantizar la seguridad de los datos, puede no especificar con la misma fuerza el requisito de integrar la protección de datos desde el diseño.

Transferencias Internacionales de Datos

- **GDPR**: Establece reglas estrictas sobre la transferencia de datos personales fuera de la UE, permitiendo transferencias solo a países que proporcionen un nivel adecuado de protección de datos o mediante la implementación de salvaguardias adecuadas.
- **Propuesta guatemalteca:** Puede tener reglas menos detalladas o rigurosas sobre las transferencias internacionales de datos, reflejando las necesidades y capacidades regulatorias locales.

Régimen de Sanciones

- **GDPR:** Las sanciones son extremadamente altas, pudiendo llegar hasta 20 millones de euros o el 4% del volumen de negocio global anual.
- **Propuesta guatemalteca:** Aunque las sanciones pueden ser severas, es probable que no alcancen el nivel máximo establecido por el GDPR, ajustándose a la realidad económica y empresarial del país.

Participación Pública y Conciencia

- **GDPR:** Parte de un entorno donde la conciencia pública y empresarial sobre la protección de datos ya es relativamente alta.
- **Propuesta guatemalteca:** Podría requerir un esfuerzo significativo en educación y sensibilización sobre la importancia de la protección de datos, dado que este puede ser un concepto relativamente nuevo para muchos sectores de la sociedad y la economía en Guatemala.

Enfoque Regulatorio

- **GDPR:** Funciona en un sistema donde múltiples autoridades nacionales de protección de datos colaboran y coexisten dentro del marco del Comité Europeo de Protección de Datos.
- **Propuesta guatemalteca:** Es probable que funcione bajo una única autoridad nacional de protección de datos, reflejando una estructura gubernamental y administrativa más centralizada.

Propuesta de marco regulatorio y de gobernanza

1. Preceptos Fundamentales

Capítulo I: Disposiciones Generales

- **Objeto del marco regulatorio:** El objetivo es promover una administración pública más eficiente, transparente y accesible, mejorando así la calidad de los servicios ofrecidos a los ciudadanos, que incluye la protección de datos personales, la regulación del uso de la tecnología en la prestación de servicios públicos y la promoción del acceso universal a los servicios digitales.
- Garantizar la protecci6n de los datos personales en poder de terceros, su tratamiento legitimo, adecuado, proporcional, seguro, controlado e informado, a efecto de salvaguardar la privacidad y el derecho a la autodeterminacion informativa de las personas.
- **Ámbito de Aplicación:** Las agencias y departamentos del gobierno que manejen datos personales deben cumplir con estas normativas.
- **Definiciones Clave:** Establecer definiciones claras de términos técnicos y legales tales como "datos personales", "tratamiento de datos", "consentimiento informado", y "acceso digital" para asegurar un entendimiento uniforme de la ley.

Capítulo II: Principios Rectores

Este capítulo introduce los principios rectores que deben guiar la implementación y gestión de la digitalización de los servicios públicos, asegurando que todos los procesos respeten los

derechos fundamentales de los ciudadanos y las normativas internacionales de protección de datos.

Principios Clave:

- **Legalidad:** Asegurar que todo el tratamiento de datos personales se realice en un marco legal claro y justo.
- **Finalidad:** Limitar la recopilación de datos a fines específicos, legítimos y explícitos, los cuales deben ser informados al ciudadano al momento de la recolección.
- **Minimización de Datos:** Recolectar solo los datos que son estrictamente necesarios para cumplir con los propósitos declarados.
- **Precisión y Calidad de los Datos:** Mantener los datos personales exactos, actualizados y completos.
- **Transparencia:** Proporcionar a los ciudadanos información clara sobre cómo se recogen, usan y protegen sus datos.
- **Seguridad de los Datos:** Implementar medidas técnicas y organizativas avanzadas para proteger los datos personales contra el acceso no autorizado o ilegal y contra su pérdida, destrucción o daño accidental.
- **Responsabilidad:** Obligar a los responsables del tratamiento de datos a demostrar el cumplimiento de todos los principios de protección de datos y privacidad.

Capítulo III: Generalidades del Tratamiento de Datos Personales

Este capítulo detalla las normas generales para el tratamiento de datos personales, estableciendo un marco sólido que las entidades gubernamentales deben seguir al manejar información personal en el contexto de servicios digitales.

Directrices Generales:

- **Base Legal para el Tratamiento:** Definir las bases legales específicas que justifican el tratamiento de datos personales, incluyendo el consentimiento explícito, el cumplimiento de una obligación legal o la protección del interés público.
- **Derechos del Interesado:** Garantizar que los ciudadanos tengan derecho a acceder a sus datos personales, a solicitar la rectificación o eliminación de sus datos, y a oponerse o restringir su tratamiento.
- **Evaluaciones de Impacto sobre la Protección de Datos:** Exigir que se realicen evaluaciones para cualquier nuevo proyecto o tecnología que pueda tener un impacto significativo en la privacidad de los datos personales.
- **Procedimientos de Consentimiento:** Desarrollar y mantener procedimientos para obtener, verificar y documentar el consentimiento de los titulares de datos de manera que este consentimiento sea libre, informado, específico e inequívoco.

2. Titulares de Datos Personales

Capítulo 1: Derechos de los Titulares de Datos Personales

Este capítulo centraliza su atención en los derechos fundamentales de los ciudadanos en el contexto de la digitalización de los servicios públicos en Guatemala.

Derechos Específicos de los Titulares de Datos Personales

- **Derecho de Acceso:** Cada ciudadano tiene el derecho de acceder a los datos personales que sobre él se hayan recogido y están siendo tratados por entidades públicas. Este acceso debe ser fácil, directo y sin costos prohibitivos, permitiendo al individuo obtener una copia de sus datos en un formato comprensible.
- **Derecho de Rectificación:** Los titulares de datos tienen el derecho a solicitar la corrección de datos incorrectos o incompletos que les conciernan. Esto es crucial para garantizar la precisión de la información en bases de datos gubernamentales, especialmente en áreas sensibles como la salud, educación y servicios legales.
- **Derecho de Supresión ("Derecho al Olvido"):** Este derecho permite a los individuos solicitar la eliminación de sus datos personales cuando ya no sean necesarios para los fines para los que fueron recogidos, o cuando el titular retire su consentimiento. Este derecho es particularmente importante en el contexto de la protección contra el procesamiento prolongado e innecesario de datos personales.
- **Derecho a la Limitación del Tratamiento:** Los ciudadanos pueden solicitar la limitación del tratamiento de sus datos personales, lo cual es relevante en situaciones donde la exactitud de los datos es impugnada o el tratamiento es ilegal, pero el titular se opone a su eliminación y en su lugar solicita la restricción de su uso.
- **Derecho a la Portabilidad de los Datos:** Este derecho facilita a los ciudadanos la capacidad de mover, copiar o transferir datos personales fácilmente de un entorno de TI a otro de manera segura, sin impedimentos. Esto es esencial para fomentar la competencia y la eficiencia de los servicios, permitiendo a los individuos beneficiarse de aplicaciones y servicios que pueden ofrecer un mejor uso de sus datos.
- **Derecho de Oposición:** Los titulares de datos pueden oponerse en cualquier momento, por motivos relacionados con su situación particular, al tratamiento de datos personales que les conciernan, incluido el perfilado. Este derecho es crucial para garantizar que los individuos puedan evitar participar en procesos de toma de decisiones automatizados y sin intervención humana que podrían afectarlos significativamente.
- **Derecho a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado, incluida la elaboración de perfiles:** Este derecho garantiza que se tome ninguna decisión significativa basada solo en el procesamiento automatizado de datos, incluidos el perfilado, que produzca efectos jurídicos o afecte significativamente al individuo.

Mecanismos de Ejercicio y Protección de los Derechos

El gobierno debe establecer procedimientos claros y accesibles para que los ciudadanos ejerzan estos derechos. Esto incluye:

- **Puntos de contacto accesibles:** Proporcionar oficinas y plataformas en línea donde los ciudadanos puedan realizar consultas y ejercer sus derechos relacionados con sus datos personales.
- **Respuestas oportunas:** Garantizar que todas las solicitudes relacionadas con datos personales sean atendidas de manera eficiente y dentro de los marcos temporales establecidos por la ley.
- **Soporte y asistencia:** Ofrecer asistencia para educar a los ciudadanos sobre cómo gestionar sus datos personales y cómo ejercer sus derechos efectivamente.

Al garantizar estos derechos, Guatemala se alinea con estándares internacionales de protección de datos y refuerza su compromiso con la gobernanza digital ética y responsable.

3. Obligaciones del Responsable y del Encargado de Tratamiento de Datos Personales

Se establece un marco claro que garantiza la protección de la información personal contra el acceso indebido, la manipulación, la pérdida o el uso inapropiado, fortaleciendo así la confianza del público en los sistemas digitales del gobierno.

Obligaciones Generales

- **Adoptar Medidas de Seguridad Apropiadas:** Los responsables y encargados del tratamiento de datos deben implementar medidas de seguridad técnicas y organizativas adecuadas para proteger los datos personales contra la destrucción accidental o ilícita, pérdida, alteración, divulgación o acceso no autorizado. Esto incluye la utilización de cifrado, controles de acceso, auditorías de seguridad y protocolos de respuesta a incidentes.
- **Garantizar la Confidencialidad, Integridad y Disponibilidad:** Deben asegurar que los datos personales se manejan con confidencialidad, integridad y disponibilidad en todo momento, especialmente en el procesamiento y almacenamiento de datos.
- **Verificación y Validación de Datos:** Es fundamental verificar la exactitud de los datos personales al momento de su recolección y actualizarlos según sea necesario. Los responsables deben validar la fuente de los datos y asegurarse de que los datos recopilados son pertinentes y no excesivos para los fines para los que se procesan.

- **Consentimiento Informado:** Deben obtener el consentimiento expreso de los titulares de los datos para el tratamiento de sus datos personales, excepto en los casos que la ley permita otro tipo de tratamiento. El consentimiento debe ser libre, informado, específico e inequívoco.
- **Transparencia en el Tratamiento:** Proporcionar información clara y accesible a los titulares de los datos sobre quién está tratando sus datos, con qué propósito, cuáles son sus derechos y cómo pueden ejercerlos.

Obligaciones Específicas

- **Notificación de Brechas de Seguridad:** En caso de una violación de seguridad que pueda poner en riesgo los derechos y libertades de los individuos, los responsables y encargados deben notificarlo a la autoridad competente y, cuando sea necesario, a los afectados, en un plazo no mayor a 72 horas después de haber tenido conocimiento de la brecha.
- **Realización de Evaluaciones de Impacto sobre la Protección de Datos (DPIAs):** Antes de implementar tecnologías o procesos que puedan resultar en un alto riesgo para los derechos y libertades de los individuos, deben llevar a cabo evaluaciones de impacto que identifiquen y mitiguen estos riesgos.
- **Designación de un Delegado de Protección de Datos (DPD):** En casos donde el volumen y tipo de tratamiento de datos lo requieran, designar un DPD que supervise el cumplimiento de las normativas de protección de datos, actúe como punto de contacto con los titulares de los datos y coopere con la autoridad supervisora.
- **Capacitación y Concienciación:** Deben asegurar que el personal involucrado en el tratamiento de datos personales esté adecuadamente capacitado y consciente de sus obligaciones bajo esta ley.

Responsabilidades Adicionales

- **Cooperación con Autoridades Reguladoras:** Los responsables y encargados están obligados a cooperar con las autoridades de protección de datos en cualquier investigación o solicitud de información relativa al tratamiento de datos personales.
- **Registro de Actividades de Tratamiento:** Mantener un registro detallado de las actividades de tratamiento de datos personales, especificando el propósito del tratamiento, las categorías de datos tratados, y los destinatarios de los datos.

4. Autoridades

Capítulo I: Consejo Nacional de Protección de Datos Personales

- Este capítulo establece la creación y funcionamiento del Consejo Nacional de Protección de Datos Personales (CNPDP), una entidad dedicada a supervisar y asegurar la implementación adecuada de las políticas y normativas de protección de datos en el sector público.
- El Consejo actúa como el máximo órgano de gobernanza en cuestiones de privacidad y protección de datos en Guatemala, asegurando que las actividades de tratamiento de datos personales se realicen en conformidad con la ley.

Funciones del CNPDP

- **Establecer Políticas y Directrices:** El Consejo es responsable de desarrollar políticas y directrices estratégicas para la protección de datos personales. Esto incluye la elaboración de normativas que aborden los desafíos emergentes en la digitalización de servicios públicos y el uso de nuevas tecnologías.
- **Supervisión y Auditoría:** Supervisar y realizar auditorías periódicas de las actividades de tratamiento de datos personales llevadas a cabo por las entidades públicas. Esto asegura que todas las operaciones cumplen con las normas establecidas y respetan los derechos de los ciudadanos.
- **Asesoramiento y Apoyo:** Proporcionar asesoramiento técnico y apoyo a las entidades del gobierno en la implementación de prácticas adecuadas de gestión de datos. Esto incluye la ayuda en la realización de Evaluaciones de Impacto sobre la Protección de Datos (DPIA) y en la formación del personal en cuestiones de privacidad.
- **Gestión de Quejas y Disputas:** Recibir y gestionar quejas y disputas relacionadas con el tratamiento indebido de datos personales. El Consejo tiene la autoridad para imponer sanciones o exigir cambios en las prácticas de tratamiento de datos si se determina que una entidad ha violado la legislación.
- **Promoción de la comunicación Pública:** Llevar a cabo campañas de educación y concienciación pública sobre los derechos relacionados con la protección de datos y las responsabilidades de las entidades públicas. Esto es fundamental para fortalecer la cultura de protección de datos en el país.
- **Cooperación Internacional:** Representar a Guatemala en foros internacionales relacionados con la protección de datos y privacidad, y colaborar con organismos de protección de datos de otros países para compartir mejores prácticas y fortalecer las capacidades regulatorias.

Capítulo II: Instituto Guatemalteco de Protección de Datos Personales

Sección I: Creación, Funciones, Presupuesto y Recursos Financieros

- Este capítulo y sección detallan la creación del Instituto Guatemalteco de Protección de Datos Personales (IGPDP), una entidad operativa responsable de la ejecución de las políticas establecidas por el CNPDP.
- El Instituto tiene autonomía administrativa y técnica, y está equipado con los recursos financieros necesarios para llevar a cabo su misión.

Funciones del Instituto Guatemalteco de Protección de Datos Personales

- **Monitoreo y Cumplimiento:** Monitorear el cumplimiento de la ley de protección de datos por parte de las entidades públicas y privadas que manejan datos personales. Esto incluye realizar inspecciones y evaluaciones regulares.
- **Registro de Actividades de Tratamiento de Datos:** Mantener un registro público de todas las entidades que realizan tratamiento de datos personales, incluyendo detalles sobre el tipo de datos tratados y los fines del tratamiento.
- **Resolución de Conflictos:** Actuar como mediador en los conflictos entre ciudadanos y entidades públicas relacionados con el tratamiento de datos personales, asegurando una resolución justa y eficiente de las disputas.
- **Desarrollo de Capacidades:** Organizar y proporcionar programas de capacitación para entidades y individuos sobre cómo gestionar la protección de datos de manera efectiva.

Sección II: Dirección General

- La Dirección General del IGPDP es responsable de la gestión diaria y la implementación de las decisiones del Consejo. El Director General es nombrado por un periodo fijo y es responsable ante el Consejo y el público por la administración del Instituto.

Responsabilidades y Supervisión

- Ambas entidades, el CNPDP y el IGPDP, trabajan conjuntamente para asegurar que Guatemala avance hacia una sociedad digital más segura y transparente, donde los derechos a la privacidad y la protección de datos personales de todos los ciudadanos sean respetados y protegidos efectivamente.

5. Presupuesto y recursos financieros

- Se centra en la asignación de presupuesto y recursos financieros necesarios para implementar efectivamente las políticas de protección de datos y garantizar la gestión eficiente y ética de la información personal en el entorno digital del sector público.
- Es crucial para asegurar que las entidades encargadas de la protección de datos personales tengan los medios necesarios para cumplir sus objetivos de manera sostenible y efectiva.

Asignación de Presupuesto

- **Fondos Suficientes:** El Ministerio de Finanzas Publicas asignara anualmente en el Presupuesto General de Ingresos y Egresos del Estado, fondos suficientes para cubrir todas las operaciones del Consejo Nacional de Protección de Datos Personales (CNPDP) y del Instituto Guatemalteco de Protección de Datos Personales (IGPDP). Esto incluye, pero no se limita a, la supervisión y regulación del tratamiento de datos personales, la formación y capacitación de personal, y la investigación y desarrollo de nuevas tecnologías y metodologías para mejorar la protección de datos.
- **Presupuesto Anual:** El presupuesto para la protección de datos personales será revisado y aprobado anualmente por el Congreso. Esta revisión debe considerar las necesidades cambiantes y los desafíos emergentes en el sector de protección de datos para adaptar y escalar los recursos de acuerdo con las demandas.
- **Transparencia en la Gestión de Fondos:** Se establecerán mecanismos de transparencia y rendición de cuentas para asegurar que todos los fondos asignados se utilicen exclusivamente para las actividades relacionadas con la protección de datos personales. Esto incluirá informes periódicos sobre el gasto y los resultados obtenidos, accesibles al público y a otras entidades gubernamentales.

Recursos Financieros

- **Diversificación de Fuentes de Financiamiento:** Además de los fondos gubernamentales, el CNPDP y el IGPDP podrán recibir financiamiento de otras fuentes, incluidos fondos internacionales, donaciones y contribuciones voluntarias de entidades privadas, siempre y cuando no comprometan su independencia o el cumplimiento de sus misiones.
- **Inversión en Tecnología y Infraestructura:** Una parte significativa del presupuesto debe destinarse a la inversión en tecnología avanzada y en la infraestructura necesaria para proteger y gestionar los datos personales de manera segura. Esto incluye sistemas de seguridad cibernética, plataformas de gestión de datos y herramientas de monitoreo y análisis.
- **Capacitación Continua:** Se asignarán recursos para programas continuos de formación y capacitación para todo el personal involucrado en el tratamiento de datos personales. Esto es

esencial para mantener al personal actualizado sobre las mejores prácticas, las leyes vigentes y las tecnologías emergentes en el campo de la protección de datos.

Gestión de Recursos

- **Establecimiento de Prioridades:** El CNPDP y el IGPDP deberán trabajar juntos para establecer prioridades claras sobre cómo se deben asignar los recursos, asegurando que los aspectos más críticos de la protección de datos reciban la financiación adecuada.
- **Fondo de Reserva para Emergencias**: Crear un fondo de reserva específico para ser utilizado en situaciones de emergencia, como brechas de datos o ataques cibernéticos, que requieran una respuesta rápida y recursos adicionales para mitigar los daños.
- **Incentivos para la Innovación:** Destinar recursos para fomentar la investigación y el desarrollo de nuevas tecnologías y prácticas que puedan mejorar la protección de datos personales. Esto podría incluir subvenciones o premios para proyectos innovadores en el sector público o colaboraciones con entidades académicas y privadas.
- **Evaluación de Efectividad:** Implementar sistemas de evaluación para medir la efectividad del uso de los recursos en la protección de datos personales y ajustar las estrategias y asignaciones presupuestarias según sea necesario para mejorar la eficiencia y eficacia.
-

6. Procedimiento de verificacion

- Se describe el marco y las metodologías que deben seguirse para realizar auditorías y controles periódicos que aseguren el cumplimiento de las normativas de protección de datos personales y la seguridad de la información.

Objetivo del Procedimiento de Verificación

- El principal objetivo del Procedimiento de Verificación es asegurar que todas las entidades que manejan datos personales en el ámbito público cumplan con las leyes establecidas.
- Este procedimiento busca identificar y rectificar cualquier irregularidad o brecha en la protección de datos personales, así como mejorar continuamente las prácticas de manejo de datos a través de revisiones sistemáticas y retroalimentación constructiva.

Procesos y Etapas del Procedimiento de Verificación

- **Planificación de la Verificación:** La planificación es el primer paso y uno de los más importantes en el proceso de verificación. Durante esta fase, se define el alcance de la auditoría, se seleccionan las entidades a ser examinadas y se establecen los criterios específicos de verificación basados en la legislación vigente y las mejores prácticas internacionales. Esta planificación debe ser exhaustiva y adaptada a las particularidades de cada entidad y los datos que maneja.

- **Realización de Auditorías:** Las auditorías pueden ser tanto internas como externas y deben llevarse a cabo de forma regular y ad hoc cuando se identifiquen posibles riesgos o infracciones. Estas auditorías incluyen la revisión de sistemas tecnológicos, procesos administrativos y prácticas operativas relacionadas con el manejo de datos personales. Los auditores deben tener acceso total a los sistemas y registros, garantizando una evaluación completa y sin restricciones.
- **Informe de Auditoría:** Al concluir cada auditoría, se debe elaborar un informe detallado que incluya los hallazgos, las áreas de riesgo identificadas y las recomendaciones para mitigar estos riesgos. Este informe debe ser presentado a la dirección de la entidad auditada y al Instituto Guatemalteco de Protección de Datos Personales, para su revisión y seguimiento.
- **Seguimiento de Recomendaciones:** Una vez entregado el informe, la entidad auditada tiene la responsabilidad de implementar las recomendaciones en un plazo determinado. El seguimiento de estas acciones correctivas es crucial y debe ser parte integral del proceso de verificación, asegurando que todas las medidas sean efectivamente implementadas y resulten en mejoras tangibles en la protección de datos personales.
- **Retroalimentación y Mejora Continua:** El proceso de verificación no termina con la implementación de medidas correctivas; es un ciclo continuo de evaluación y mejora. Las entidades deben utilizar la retroalimentación de las auditorías para realizar ajustes proactivos y preventivos en sus sistemas y procesos, fomentando una cultura de mejora continua en la gestión de datos personales.

Transparencia y Participación Pública

- El procedimiento de verificación debe ser transparente y abierto a la participación pública. Las entidades deben publicar los resultados de las auditorías de manera regular, excepto en aquellos aspectos que puedan comprometer la seguridad de la información o la privacidad de los individuos.
- Además, debe fomentarse la participación ciudadana permitiendo que los individuos presenten quejas o preocupaciones relacionadas con el tratamiento de sus datos personales, las cuales deben ser consideradas durante las auditorías.

Capacitación y Recursos

- Para garantizar la efectividad de este procedimiento, es esencial que el personal involucrado en la realización de las auditorías esté adecuadamente capacitado y cuente con los recursos necesarios para realizar su trabajo de manera eficiente. Esto incluye formación continua en las últimas tecnologías y métodos de protección de datos, así como en las leyes y regulaciones aplicables.

7. Infracciones y sanciones

- Se establece un marco robusto para la imposición de infracciones y sanciones relacionadas con el tratamiento indebido de datos personales en el contexto de la digitalización de servicios públicos en Guatemala.
- Asegura que existan consecuencias claras y efectivas para el incumplimiento de las normativas establecidas en la ley, incentivando así el cumplimiento y la protección efectiva de los derechos de los ciudadanos.

Definición de Infracciones

- Las infracciones en el contexto de protección de datos personales se clasifican según su gravedad y el impacto en los derechos de los individuos:
  - **Infracciones Leves:** Estas incluyen errores no intencionales que no resultan en un daño significativo para los sujetos de datos pero que constituyen una violación de las normativas. Ejemplos podrían ser la falta de reporte de una brecha de datos en el plazo establecido, siempre que no se derive en un riesgo para los derechos y libertades de los individuos.
  - **Infracciones Graves:** Estas son violaciones que pueden tener un impacto negativo directo sobre la privacidad y la seguridad de los datos personales. Incluyen la falta de medidas de seguridad adecuadas que resulten en acceso no autorizado o pérdida de datos personales.
  - **Infracciones Muy Graves:** Estas infracciones ocurren cuando hay una violación deliberada de la ley que implica el uso indebido de datos personales para fines no autorizados, como la venta o explotación de información sin consentimiento adecuado de los titulares de los datos.

Sanciones Aplicables

- Las sanciones están diseñadas para ser proporcionales a la gravedad de la infracción y tienen como objetivo disuadir la repetición de violaciones, compensar a los afectados y, si es necesario, castigar a los responsables:
  - **Multas Económicas:** Estas son la forma más común de sanción y pueden variar desde montos menores para infracciones leves hasta sumas significativas para infracciones muy graves. Las multas están diseñadas para reflejar la gravedad del incumplimiento y el beneficio económico que el infractor pudo haber obtenido de la acción ilegal.
  - **Advertencias y Amonestaciones:** Para infracciones menores o cuando es la primera vez que se comete la infracción, se pueden emitir advertencias o amonestaciones que exigen la corrección del incumplimiento y advierten sobre sanciones más severas en caso de reincidencia.
  - **Suspensión o Revocación de Licencias:** En casos de infracciones graves o muy graves, se puede ordenar la suspensión o revocación de las licencias o permisos que permiten a las entidades operar en el ámbito de los servicios públicos.

- **Indemnizaciones a Afectados:** Cuando las infracciones resulten en daños a los individuos, se puede requerir que el responsable compense a los afectados. Esto asegura que las víctimas de violaciones de datos reciban una reparación justa.
- **Prohibiciones de Operación:** En los casos más extremos, donde las infracciones ponen en riesgo significativo la seguridad pública o los derechos fundamentales, se puede prohibir permanentemente a las entidades responsables operar en ciertos ámbitos o manejar datos personales.

Procedimientos para la Imposición de Sanciones

- Para garantizar la justicia y el debido proceso, el procedimiento para la imposición de sanciones incluye varias etapas:
- **Investigación Preliminar:** Al recibir una denuncia o detectar una posible infracción, se realiza una investigación preliminar para determinar si existen méritos para proceder.
- **Notificación al Infractor:** Si se considera que hay suficiente evidencia de una infracción, se notifica al presunto infractor, dándole la oportunidad de responder y presentar su defensa.
- **Decisión:** Basándose en la evidencia y la defensa presentada, se toma una decisión sobre la infracción y la sanción correspondiente.
- **Apelación:** Se permite la apelación de la decisión ante un tribunal o un cuerpo superior para garantizar el derecho a un juicio justo.

8. Procedimientos administrativos para solucion de conflictos

- Se dedica a establecer un marco formal y efectivo para la solución de conflictos relacionados con el tratamiento de datos personales. Es importante para garantizar que existan mecanismos claros y accesibles para resolver disputas entre los ciudadanos y las entidades gubernamentales o privadas que manejan datos personales.
- A través de este marco, se busca preservar los derechos de los individuos y mantener la confianza en el sistema de protección de datos.
- **Objetivos**: El principal objetivo es proporcionar un proceso estructurado y eficiente para la resolución de conflictos, asegurando que todos los ciudadanos tengan acceso a remedios administrativos y legales en caso de violación de sus derechos de privacidad. Este proceso está diseñado para ser rápido, transparente y justo, reduciendo la necesidad de litigios prolongados y costosos.

Sección I: Disposiciones Generales

- Establece que todos los procedimientos deben ser manejados de manera que se respeten los derechos de todas las partes involucradas y que se proporcione una solución justa y equitativa. Además, se enfatiza la importancia de la conciliación como un medio para resolver disputas de manera amistosa antes de proceder a instancias más formales.

- El Instituto Guatemalteco de Proteccion de Datos Personales actuara de oficio por medio de la presentacion de queja por parte de aquellas personas que se consideren agraviados por el tratamiento de sus datos personales, y asegurarse que las infracciones a esta ley sean debidamente sancionadas.
- Resolucion de conflictos. Para la resolucion de los conflictos y controversias que surjan en el manejo de datos personales entre los responsables o encargados de archivos, registros, bases banco de datos personas y los titulares de los mismos, que puedan constituir infraccion a la presente ley, se establecen los siguientes procedimientos: a) Conciliacion entre las partes; b) Procedimiento de proteccion de datos personales.

Sección II: Conciliación entre las Partes

- **Inicio del Proceso de Conciliación:** Cualquier parte afectada por el tratamiento de sus datos personales puede iniciar un procedimiento de conciliación presentando una solicitud ante el Instituto Guatemalteco de Protección de Datos Personales (IGPDP). La solicitud debe detallar la naturaleza del conflicto y las razones por las cuales se busca una solución conciliatoria.
- **Procedimiento de Conciliación:** El IGPDP facilitará el proceso de conciliación, nombrando a un conciliador neutral que trabajará con las partes para alcanzar un acuerdo. El conciliador deberá asegurarse de que todas las partes comprendan sus derechos y las implicaciones de cualquier acuerdo alcanzado.
- **Acuerdo de Conciliación:** Si las partes llegan a un acuerdo, este será puesto por escrito y firmado por ambas partes y el conciliador. Este acuerdo tendrá efecto vinculante y será ejecutable legalmente.

Sección III: Procedimiento de Protección de Datos Personales

- **Presentación de Reclamaciones:** Si la conciliación no resuelve el conflicto, los individuos tienen el derecho de presentar una reclamación formal ante el IGPDP. La reclamación debe incluir pruebas del daño sufrido y de cómo se han violado las normativas de protección de datos.
- **Investigación y Resolución:** El IGPDP investigará la reclamación, lo que puede incluir inspecciones y la solicitud de información adicional a las partes. Basándose en la evidencia, el IGPDP emitirá una resolución que puede incluir medidas correctivas, sanciones contra la entidad infractora y, si corresponde, compensaciones para la parte afectada.

Sección IV: Aplicación de las Resoluciones

- La aplicacion de sanciones establecidas en esta ley corresponde al Instituto, salvo los casos que constituyan delitos, cuyo conocimiento y sancion corresponde a los organos jurisdiccionales correspondientes.

- Si durante la tramitacion del procedimiento de proteccion de datos personales, se determine la probable comision de delito, el Instituto se abstendra de imponer sancion alguna y pondra de oficio, el hecho en conocimiento del Ministerio Publico.

Sección V: Impugnación de las Resoluciones

- **Derecho de Apelación:** Las partes tienen derecho a apelar las decisiones del IGPDP ante un tribunal administrativo. La apelación debe basarse en argumentos legales sólidos y presentarse dentro de un plazo específico desde la notificación de la decisión.
- **Revisión Judicial:** Finalmente, si las partes no están satisfechas con la decisión del tribunal administrativo, pueden buscar una revisión judicial, garantizando así el derecho a un juicio justo.

9. Delitos en materia de tratamiento de datos personales

- Al establecer claramente los delitos y sus correspondientes sanciones, se refuerza la seriedad con la que el estado guatemalteco trata la protección de la información personal.
- **Objetivos**: El principal objetivo es proporcionar un entorno seguro y protegido donde los datos personales de los individuos no sean sujetos a abuso, manipulación ilegal, o explotación.
- Se busca también restaurar la confianza pública en los sistemas de información y servicios digitales del gobierno, asegurando que haya consecuencias legales claras para aquellos que violen las normas establecidas.

Delitos Específicos

- **Acceso Ilegal a Datos Personales:** Este delito ocurre cuando una persona accede sin autorización a sistemas de información que contienen datos personales. La penalización de este delito refleja la gravedad de la intrusión en la privacidad del individuo y la potencial exposición a riesgos.
- **Alteración de Datos Personales:** Consiste en modificar, sin permiso o de manera fraudulenta, datos personales almacenados en cualquier sistema informático. Este delito puede tener consecuencias graves, incluyendo la pérdida de la integridad de los datos y potenciales daños a la reputación o derechos de los individuos afectados.
- **Destrucción de Datos Personales:** Este delito se refiere a la eliminación o destrucción intencionada de datos personales sin autorización o en contravención de las normativas legales. La destrucción de datos puede impedir que los individuos ejerzan derechos esenciales como el acceso a la información o la rectificación de sus datos personales.
- **Divulgación Indebida de Datos Personales:** Involucra la revelación de información personal sin consentimiento del titular de los datos o sin otra justificación legal. Este delito es especialmente grave cuando implica la divulgación de datos sensibles que pueden afectar la privacidad y seguridad de una persona.
- **Uso Indebido de Datos Personales:** Este delito ocurre cuando los datos personales se utilizan para fines diferentes a aquellos para los que fueron recopilados, especialmente en casos donde el uso indebido conlleva beneficios económicos o perjuicios a terceros.

Penalizaciones

- Las sanciones por los delitos mencionados varían dependiendo de la gravedad del acto y sus consecuencias. Pueden incluir:
  - **Multas:** Establecidas de acuerdo a la gravedad del delito y el daño causado. Las multas buscan ser disuasorias y proporcionalmente significativas para desincentivar la conducta delictiva.
  - **Prisión:** Para los delitos más graves, especialmente aquellos que involucren daño significativo a los individuos o beneficios económicos ilícitos, se pueden imponer penas de prisión.
  - **Prohibiciones de Futuro Manejo de Datos:** En algunos casos, se puede prohibir a los infractores volver a manejar datos personales, especialmente cuando han demostrado un desprecio flagrante por las leyes de protección de datos.
  - **Compensación a Víctimas:** Los delincuentes pueden ser obligados a compensar a las víctimas por cualquier daño que hayan sufrido como resultado del delito. Esto incluye compensación económica y medidas para restaurar la dignidad y privacidad de la persona afectada.

10. Disposiciones transitorias, finales y derogatorias

- Establece los lineamientos necesarios para modificar, adaptar o eliminar las normativas existentes que puedan entrar en conflicto con la nueva ley, y proporciona un marco temporal dentro del cual todas las partes involucradas deben ajustarse a los nuevos requisitos.
- Además, delinea las disposiciones finales que consolidan la ley, asegurando su efectividad y coherencia con el marco legal general del país.

Disposiciones Transitorias

- **Período de Adaptación:** Se establece un período de adaptación de dos años a partir de la promulgación de la ley, durante el cual todas las entidades públicas y privadas que manejen datos personales deben ajustar sus procesos, sistemas y políticas para cumplir con las nuevas normativas. Este período permite que las organizaciones realicen las inversiones necesarias en tecnología y capacitación sin perturbar sus operaciones diarias.
- **Auditorías Iniciales:** Durante el primer año después de la entrada en vigor de la ley, se realizarán auditorías iniciales para evaluar el estado actual del manejo de datos personales por parte de las entidades. Estas auditorías ayudarán a identificar las áreas críticas que requieren mejoras urgentes y servirán como base para las acciones correctivas.
- **Registro de Actividades de Tratamiento:** Las entidades deberán registrar todas sus actividades de tratamiento de datos ante el Instituto Guatemalteco de Protección de Datos Personales dentro de los primeros seis meses tras la promulgación de la ley. Este registro es crucial para la transparencia y la supervisión reguladora.
- **Plan de Implementación:** Cada entidad deberá desarrollar y presentar un plan de implementación detallado que muestre cómo se ajustará a las nuevas disposiciones legales.

Este plan debe ser aprobado por el Instituto y actualizado anualmente hasta que finalice el período de adaptación.

Disposiciones Finales

- **Entrada en Vigor:** La ley entrará en vigor inmediatamente después de su publicación en el diario oficial, excepto para aquellos artículos o secciones que requieran reglamentación secundaria, los cuales entrarán en vigor una vez que dicha reglamentación sea emitida.
- **Obligación Continua de Cumplimiento:** Aunque el período de adaptación permita ciertas flexibilidades temporales, las entidades deben cumplir con los principios fundamentales de la ley desde el primer día. Esto incluye el respeto a los derechos de los titulares de datos y la aplicación de medidas básicas de seguridad.
- **Publicación y Difusión:** La ley completa, junto con cualquier reglamento asociado, deberá ser publicada en el portal web del Instituto Guatemalteco de Protección de Datos Personales y otros medios públicos para garantizar su amplio conocimiento y comprensión por parte de todos los sectores afectados.

Disposiciones Derogatorias

- **Derogación de Normativas Anteriores:** Todas las disposiciones legales, reglamentos y normativas que entren en conflicto con lo establecido en la nueva ley serán derogadas. Se incluirá una lista detallada de las disposiciones afectadas en un anexo a la ley.
- **Revisión y Actualización de la Legislación Relacionada:** Se establece un mandato para que todas las leyes y reglamentos relacionados con la protección de datos personales sean revisados y, si es necesario, actualizados dentro de los cinco años siguientes a la implementación de la nueva ley para garantizar la coherencia y eficacia del marco legal.
- **Cláusula de Salvaguardia:** En caso de que cualquier parte de la ley sea anulada o invalidada por un tribunal, las demás disposiciones seguirán en vigor, asegurando que la protección integral de los datos personales no se vea comprometida.

Conclusiones y Modelos Recomendados

La transformación digital en Guatemala, guiada por un marco de gobernanza de datos robusto y bien definido, es fundamental para el avance y la modernización del sector público. Las conclusiones clave de este reporte enfatizan la necesidad de un modelo de gobernanza que sea inclusivo, seguro, y adaptativo, con un enfoque centrado en:

- **Respeto a los Derechos Fundamentales:** La protección de la privacidad y los datos personales es crucial en un mundo digitalmente interconectado, y es un pilar para construir la confianza del público.

- **Adaptabilidad y Escalabilidad:** La capacidad de adaptarse a cambios tecnológicos y escalar para satisfacer las crecientes demandas de gestión de datos es esencial para una gobernanza de datos exitosa y sostenible.

- **Participación Ciudadana:** La integración activa de los ciudadanos en la gobernanza de datos asegura transparencia y responsabilidad, fomentando políticas que reflejen las necesidades y expectativas de la sociedad.

Implicaciones para el Futuro Digital de Guatemala

El establecimiento de un modelo de gobernanza de datos robusto y efectivo tiene profundas implicaciones para el futuro digital de Guatemala:

- **Creación de un Marco de Confianza Digital:** La implementación de prácticas de gobernanza de datos sólidas y transparentes ayuda a construir un entorno digital de confianza, esencial para la aceptación y adopción de tecnologías emergentes por parte de los ciudadanos y las empresas.

- **Impulso a la Innovación y el Desarrollo Económico**: Al garantizar el acceso a datos de alta calidad y promover la seguridad y privacidad, se crea un entorno propicio para la innovación y el desarrollo económico. Las empresas y los emprendedores pueden utilizar los datos abiertos para desarrollar nuevas soluciones y servicios.

- **Mejora en la Prestación de Servicios Públicos:** Con una gestión de datos más eficiente y una participación ciudadana efectiva, los servicios públicos pueden ser más responsivos a las necesidades de la población, mejorando la calidad de vida de los ciudadanos.

- **Adaptabilidad a Futuros Desafíos Tecnológicos:** Un sistema de gobernanza adaptable y escalable posiciona a Guatemala para responder con eficacia a los rápidos cambios tecnológicos, asegurando que el país no se quede atrás en la evolución digital global.

Un marco de gobernanza de datos bien estructurado y enfocado en los principios de participación ciudadana, respeto a los derechos fundamentales, y adaptabilidad y escalabilidad, no solo mejorará la gestión y uso de datos en el sector público, sino que también jugará un papel crucial en moldear un futuro digital seguro, inclusivo y próspero para Guatemala.

Bibliografía

- Bygrave, L. A. (2017). Data privacy law: An international perspective. Oxford University Press.
- European Commission. (2020). Data protection in the EU. Retrieved from https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en
- Kuner, C., Cate, F. H., Millard, C., & Svantesson, D. J. B. (Eds.). (2017). The EU General Data Protection Regulation (GDPR): A commentary. Oxford University Press.
- Zarsky, T. Z. (2016). The trouble with algorithmic decisions: An analytic road map to examine efficiency and fairness in automated and opaque decision making. Science, Technology, & Human Values, 41(1), 118-132. https://doi.org/10.1177/0162243915605575

Anexos

Anexo 1. Presentación de informe: Propuesta de marco regulatorio y de gobernanza

Anexo 2. Propuesta de Marco Regulatorio de protección de datos personales.

Red Ciudadana

GUATEMALA
GUATEMALA NO SE DETIENE

Propuesta de marco regulatorio y de gobernanza

Red Ciudadana

GUATEMALA
GUATEMALA NO SE DETIENE

PROPUESTA DE MARCO REGULATORIO DE PROTECCIÓN DE DATOS PERSONALES

Considerando:

- Que la Constitución de la República de Guatemala consagra el derecho a la intimidad y la privacidad de cada individuo, y es imperativo desarrollar legislación que proteja estos derechos en el contexto de un mundo digitalizado.

- Que el desarrollo tecnológico y la globalización han transformado la manera en que los datos personales se recopilan, almacenan, utilizan y transmiten, presentando nuevos desafíos que requieren una regulación específica para garantizar la protección efectiva de los datos personales.

- Que la falta de una legislación específica sobre la protección de datos personales en Guatemala ha creado un vacío legal que pone en riesgo la privacidad de los ciudadanos, especialmente en lo que respecta al acceso y uso de sus datos personales por parte de entidades tanto públicas como privadas.

- Que numerosos países alrededor del mundo, incluyendo los miembros de la Unión Europea con su Reglamento General de Protección de Datos (GDPR), han implementado regulaciones robustas que pueden servir de modelo para el desarrollo de normativas adecuadas en el contexto nacional.

- Es fundamental establecer un marco normativo que no sólo proteja los datos personales de los ciudadanos sino que también fomente la confianza en el uso de servicios digitales, promoviendo así el desarrollo económico y tecnológico del país.

- Se reconoce la importancia de alinear las prácticas de protección de datos personales con estándares internacionales para facilitar el intercambio de información y la cooperación internacional en un mundo cada vez más interconectado.

- Que la protección eficaz de los datos personales y la garantía de los derechos digitales son fundamentales para el fortalecimiento de la democracia y el respeto de los derechos humanos en la era digital.

Por tanto:

Se somete a consideración del honorable Congreso de la República de Guatemala la siguiente propuesta de ley, con el objetivo de establecer un marco legal claro y efectivo que

regule el tratamiento de los datos personales, garantice la protección de la privacidad de los individuos y promueva el uso ético de la tecnología en todos los sectores de la sociedad. Esta legislación busca asegurar que Guatemala se mantenga a la vanguardia en la protección de los derechos fundamentales en el contexto de la revolución digital, proporcionando las herramientas necesarias para una gestión segura y responsable de los datos personales.

PROPUESTA DE MARCO REGULATORIO DE PROTECCIÓN DE DATOS PERSONALES

Artículo 1. Objeto de la ley

Esta ley tiene como objeto la protección de los datos personales tratados por entidades públicas y privadas en Guatemala, asegurando el respeto a la privacidad y los derechos fundamentales de los individuos.

Artículo 2. Ámbito de aplicación

La presente ley es aplicable a cualquier tratamiento de datos personales realizado en territorio guatemalteco, así como al tratamiento de datos de ciudadanos guatemaltecos por parte de entidades fuera del país.

Capítulo I: Disposiciones Generales

Artículo 3. Definiciones

Se establecen las definiciones clave como "datos personales", "tratamiento", "responsable del tratamiento", "encargado del tratamiento", y otras necesarias para la correcta interpretación y aplicación de la ley.

Capítulo II: Principios Rectores

Artículo 4. Legalidad y transparencia

Todo tratamiento de datos personales se realizará de manera lícita, leal y transparente en relación con el titular del dato.

Artículo 5. Limitación de la finalidad

Los datos personales serán recopilados para fines específicos, explícitos y legítimos, y no se tratarán de manera incompatible con esos fines.

Artículo 6. Minimización de datos

Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.

Artículo 7. Precisión

Los datos personales serán exactos y, si fuera necesario, actualizados; se tomarán todas las medidas razonables para asegurar que los datos personales que sean inexactos se eliminen o rectifiquen sin demora.

Artículo 8. Limitación del almacenamiento

Los datos personales se mantendrán en una forma que permita la identificación de los titulares durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

Artículo 9. Integridad y confidencialidad

Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, utilizando medidas técnicas o administrativas apropiadas.

Artículo 10. Responsabilidad

El responsable del tratamiento será responsable de cumplir y demostrar el cumplimiento de los principios mencionados.

Capítulo III: Generalidades del Tratamiento de Datos Personales

Artículo 11. Consentimiento del titular

El tratamiento de datos personales sólo se llevará a cabo con el consentimiento expreso y verificable del titular, salvo que la ley disponga otra cosa.

Artículo 12. Medidas de seguridad

Las entidades responsables deberán implementar medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad apropiado al riesgo que presenta el tratamiento.

Artículo 13. Evaluación de impacto sobre la protección de datos

Será obligatorio realizar una evaluación de impacto sobre la protección de datos personales para tratamientos que supongan un alto riesgo para los derechos y libertades de los individuos.

Título II: Titulares de Datos Personales

Artículo 14. Derecho de acceso

El titular de los datos tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen, y en su caso, acceso a los datos personales.

Artículo 15. Derecho de rectificación y supresión

El titular de los datos podrá solicitar la rectificación de datos inexactos que le concierne, así como la supresión de los datos cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos.

Artículo 16. Derecho a la limitación del tratamiento

El titular de los datos podrá solicitar la limitación del tratamiento de sus datos, lo cual implica que los datos podrán ser tratados, aparte de su almacenamiento, solo con el consentimiento del titular, para la formulación, el ejercicio o la defensa de reclamaciones o con vistas a la protección de los derechos de otra persona natural o jurídica o por razones de interés público importante.

Artículo 17. Derecho a la portabilidad

El titular de los datos tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable sin que lo impida el responsable al que se los hubiera facilitado.

Artículo 18. Derecho de oposición

El titular de los datos tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a qué datos personales que le conciernen sean objeto de un tratamiento.

Artículo 19. Decisiones automatizadas, incluida la elaboración de perfiles

El titular de los datos tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Título III: Obligaciones del Responsable y del Encargado de Tratamiento de Datos Personales

Artículo 20. Implementación de principios

El responsable y el encargado del tratamiento estarán obligados a aplicar efectivamente los principios de protección de datos personales y a integrar las garantías necesarias en el tratamiento para cumplir los requisitos de esta ley y proteger los derechos de los titulares de los datos.

Artículo 21. Mantenimiento del registro de actividades

El responsable y el encargado del tratamiento deberán mantener un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Este registro deberá contener toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en esta ley.

Artículo 22. Cooperación con la autoridad de control

El responsable y el encargado del tratamiento cooperarán con la autoridad de control competente en el desempeño de sus tareas.

Título IV: Autoridades

Artículo 23. Creación del Consejo Nacional de Protección de Datos Personales

Se crea el Consejo Nacional de Protección de Datos Personales como órgano colegiado de carácter técnico y especializado, adscrito al Ministerio de Gobernación, con autonomía técnica y funcional y con competencia en todo el territorio nacional.

Artículo 24. Funciones del Consejo

El Consejo tendrá las siguientes funciones:

a) Velar por el cumplimiento de las legislaciones de protección de datos personales y garantizar la aplicación de los principios de protección de datos.
b) Emitir directrices y recomendaciones sobre procedimientos y normas técnicas de seguridad adecuadas para el tratamiento de los datos personales.
c) Atender las consultas que le sean formuladas en materia de su competencia.
d) Informar de oficio o a petición de parte, los asuntos de su competencia.
e) Promover la formación y la sensibilización de los responsables y encargados del tratamiento de datos personales.
f) Colaborar con autoridades de protección de datos de otros países y participar en foros internacionales y reuniones vinculadas con la protección de datos personales.
g) Elaborar su reglamento interno y cuantas otras funciones sean necesarias para el cumplimiento de sus objetivos.

Artículo 25. Creación del Instituto Guatemalteco de Protección de Datos Personales

Se crea el Instituto Guatemalteco de Protección de Datos Personales como órgano desconcentrado del Consejo Nacional de Protección de Datos Personales, con personalidad jurídica y patrimonio propio, con autonomía de gestión administrativa, técnica y financiera, con competencia en todo el territorio nacional.

Artículo 26. Funciones del Instituto

El Instituto tendrá las siguientes funciones:

a) Ejercer la potestad administrativa sancionadora en materia de protección de datos personales.
b) Atender y resolver las reclamaciones y denuncias que le sean presentadas por los titulares de los datos.
c) Ordenar la adopción de medidas cautelares cuando existan indicios racionales de que un tratamiento de datos personales puede estar vulnerando las disposiciones establecidas en la legislación de protección de datos personales.
d) Promover la adopción de códigos de conducta ajustados a las disposiciones previstas en la legislación de protección de datos personales, que ayuden a las entidades responsables y encargadas del tratamiento a aplicar efectivamente los principios de protección de datos.
e) Realizar investigaciones y estudios sobre la protección de datos personales.
f) Fomentar la formación y la sensibilización de los responsables y encargados del tratamiento de datos personales.
g) Cualquier otra función que le sea encomendada por ley o reglamento.

Título V: Presupuesto y Recursos Financieros

Artículo 27. Presupuesto del Consejo y del Instituto

El Consejo y el Instituto contarán con un presupuesto anual asignado por el Estado, que será parte del presupuesto general de la nación. Los recursos asignados estarán destinados a cubrir los gastos de funcionamiento e inversión y a la realización de las actividades propias de su competencia.

Artículo 28. Recursos propios del Instituto

El Instituto podrá obtener recursos propios por la prestación de servicios, tales como la emisión de informes, certificaciones y realización de auditorías y cualesquiera otros servicios que pueda prestar en ejercicio de sus funciones. Los recursos que obtenga por estas vías no podrán destinarse a fines distintos de los previstos en esta ley.

Título VI: Procedimiento de Verificación

Artículo 29. Procedimientos de inspección

El Instituto realizará inspecciones y auditorías periódicas a las entidades responsables y encargadas del tratamiento de datos personales, para verificar el cumplimiento de la legislación aplicable en materia de protección de datos personales. Para ello, podrá acceder a sus instalaciones y solicitar la exhibición de los documentos y la información que considere necesarios.

Artículo 30. Inicio de procedimiento de inspección

El procedimiento de inspección podrá iniciarse de oficio o a petición de parte. El Instituto deberá notificar al responsable o encargado del tratamiento la realización de la inspección, con una antelación mínima de diez días, salvo que por la urgencia del caso deba actuar de inmediato.

Título VII: Infracciones y Sanciones

Artículo 31. Tipos de infracciones

Las infracciones se calificarán en leves, graves y muy graves, según el grado de incumplimiento de las disposiciones establecidas en la legislación de protección de datos personales, el tipo de derechos afectados, la cantidad de titulares de datos afectados, y la repetición en la comisión de infracciones.

Artículo 32. Sanciones

A quienes resulten responsables de la comisión de infracciones de protección de datos personales se les impondrán sanciones que podrán consistir en amonestaciones, multas, suspensión de actividades, clausura de instalaciones y otras que la ley determine. Las multas se graduará según la gravedad de la infracción, pudiendo llegar hasta el equivalente a cien veces el salario mínimo.

Artículo 33. Procedimiento para la imposición de sanciones

El procedimiento para la imposición de sanciones se iniciará de oficio o a petición de parte, y garantizará el derecho de audiencia del presunto infractor, quien podrá presentar las pruebas y alegatos que considere pertinentes.

Título VIII: Procedimientos Administrativos para la Solución de Conflictos

Artículo 34. Procedimientos de reclamación

Los titulares de datos personales que consideren que sus derechos han sido vulnerados por el tratamiento de sus datos personales podrán presentar una reclamación ante el Instituto. El procedimiento de reclamación deberá resolverse en un plazo máximo de noventa días, pudiendo ampliarse por un período igual en casos debidamente justificados.

Artículo 35. Medidas cautelares

En cualquier fase del procedimiento de reclamación, el Instituto podrá adoptar las medidas cautelares que estime necesarias para asegurar la efectividad de la resolución que pudiera recaer, incluida la orden de cese provisional del tratamiento de datos personales.

Título IX: Delitos en Materia de Tratamiento de Datos Personales

Artículo 36. Delitos y penas

Constituirán delitos en materia de tratamiento de datos personales los actos u omisiones que vulneren los derechos de los titulares de los datos, que sean realizados por quienes tengan el deber de respetar y garantizar esos derechos. Quienes cometan estos delitos serán sancionados con pena de prisión de dos a cinco años y multa de cincuenta a cien días multa.

Artículo 37. Agravantes

La pena prevista en el artículo anterior se aumentará en un tercio cuando los delitos sean cometidos por funcionarios públicos en el ejercicio de sus funciones, o cuando los datos afectados sean especialmente protegidos.

Título X: Disposiciones Transitorias, Finales y Derogatorias

Artículo 38. Implementación progresiva

Las disposiciones de esta ley se implementarán de manera progresiva, según un calendario que el Instituto establecerá y publicará dentro de los noventa días siguientes a la entrada en vigor de esta ley. Durante el período de implementación, el Instituto proporcionará la asistencia técnica necesaria a las entidades obligadas a cumplir con la ley, para facilitar una adecuada adaptación a sus disposiciones.

Artículo 39. Derogación de normativas anteriores

Quedan derogadas todas las disposiciones que se opongan a lo establecido en esta ley o que regulen de manera menos favorable la protección de los datos personales.

Artículo 40. Entrada en vigor

Esta ley entrará en vigor noventa días después de su publicación en el Diario Oficial.

Red Ciudadana

GUATEMALA
GUATEMALA NO SE DETIENE