Oficina de Tratamiento Digital del Dato: formalización para la administración adecuada del dato digital

Lía Molinari[1], Sandra D'Agostino[2]

[1]Dirección de Gobierno en Línea, Subsecretaría de Gobierno Digital, Ministerio de Jefatura de Gabinete, Gobierno de la Pcia de Bs. As., calle 48 # 343, La Plata, lia.molinari@gba.gob.ar
Universidad Nacional de La Plata, Facultad de Informática, calle 50 y 120, La Plata, lmolinari@info.unlp.edu.ar
[2]Subsecretaría de Gobierno Digital, Ministerio de Jefatura de Gabinete, Gobierno de la Pcia de Bs. As., calle 6 entre 51 y 53, La Plata, sandra.dagostino@gba.gob.ar

Resumen. Este trabajo expone la propuesta de creación de una Oficina de Tratamiento del Dato Digital desde la Subsecretaría de Gobierno Digital del Gobierno de la Provincia de Buenos Aires. El objetivo es promover el tratamiento adecuado de los datos en todas las dependencias del GPBA, considerando su criticidad y su sensibilidad, resguardando principalmente los datos personales de la ciudadanía. No obstante, la propuesta incluye otros datos de uso habitual (que no se incluyen dentro de la categoría de "personales") que son tratados sin considerar su grado de criticidad, cómo es el caso de aquéllos con carácter estratégico para la gestión o la interpretación correcta de los datos a ser usados con fines estadísticos. Esta impronta, dentro de la política digital del GPBA abre nuevos modelos en el desarrollo de sistemas informáticos y otros objetos, incluyendo el análisis de los datos a tratar desde el inicio del ciclo de vida de esos objetos.

Palabras claves: tratamiento de datos, protección de datos, datos personales

1 Introducción

La creación de una Oficina de Tratamiento del Dato Digital (OTDD) desde la Subsecretaría de Gobierno Digital (SGD) del Gobierno de la Provincia de Buenos Aires (GPBA) forma parte de la transformación propuesta por esa Subsecretaría mediante un conjunto de ejes estratégicos. El objetivo es promover el tratamiento adecuado de los datos en todas las dependencias del GPBA. La propuesta aplica al universo de datos que por su naturaleza exigen ser tratados obedeciendo una serie de principios inehrentes al riesgo de su exposición o el impacto de una mala interpretación. Ese universo incluye los datos personales, pero también otros de uso habitual que son tratados sin considerar su grado de criticidad, cómo es el caso de aquéllos con carácter estratégico para la gestión, o los que serán utilizados para estadísticas.

Actualmente, en el Gobierno de la Provincia de Buenos Aires hay 52 direcciones o áreas de TI distribuidas entre los diferentes Ministerios y otras entidades. Todos ellos tratan datos de diferente naturaleza. Por lo tanto, esta propuesta es relevante y se instala en un área de vacancia en el marco de los objetivos del gobierno abierto.

La SGD es responsable de intervenir en el diseño, formulación y coordinación de las políticas públicas de transformación, mejora administrativa y tecnológica del Gobierno Provincial. Interviene en los procesos de implementación, reforma o actualización de los servicios de atención ciudadana presencial, digital, telefónica, multiplataforma y cualquier otra que en el futuro concentre, dictando, en conjunto con las áreas competentes, las normas que se consideren pertinentes en el ámbito de su competencia[1].

Su misión de promover la transformación digital. La firme convicción de pensar, construir y promover una ciudadanía digital hace impostergable esa transformación.

El concepto de lo digital se vincula a la tecnología y la informática, mediante la representación que haga factible la interacción con dispositivos tecnológicos y que pueda ser transmitida por los distintos medios de comunicación y sus protocolos.

La ciudadanía digital puede definirse cómo las normas de comportamiento que conciernen al uso de la tecnología. Es el espacio digital que es mediado por las diferentes herramientas y dispositivos digitales para

[1] https://www.gba.gob.ar/jefatura/gobiernodigital/funciones_y_direcciones

el ejercicio de la ciudadanía. Esa ciudadanía se representa en la pertenencia a una comunidad, promovida por el uso de las tecnologías de la información y comunicación, acordando normas de comportamiento responsable entre quienes la componen [1].

El dato no vale por sí sólo. En su combinación con otros datos (uso, procesamiento) genera información. Es tan importante el dato como su procesamiento, sin dejar de lado la determinación temprana de los criterios de calidad o la preservación digital.

La propuesta de creación de una Oficina de Tratamiento del Dato Digital (OTDD) de la PBA tiene como objetivo la definición e implementación de políticas acerca del tratamiento de los datos digitales en todos los organismos del Gobierno de la PBA, garantizando razonablemente su confidencialidad, integridad y disponibilidad en todos los procesos que los incluya, entre ellos, los relacionados con la interoperabilidad de los sistemas.

La construcción de una cultura sobre el dato poniéndolo en valor y tratándolo adecuadamente impone una alianza, una colaboración entre las dependencias provinciales. Es un trabajo conjunto para que la solución sea viable, implementable en etapas, por parte de todos los organismos provinciales.

La SGD promueve una nueva cultura acerca de los trámites digitales que facilite su concreción reduciendo tiempo y costos. Para ello, se hace imprescindible la disposición y fluidez de la información con pautas claras de protección, orientada al postergado concepto de ventanilla única: un equilibrio entre accesibilidad y protección.

La importancia que el GPBA da a los datos queda evidenciado en la creación de la Infraestructura de Datos Espaciales de la Provincia de Buenos Aires (IDEBA), mediante el Decreto N° 609/20, cuyo objetivo principal es propiciar la cooperación entre diferentes instituciones públicas y privadas para garantizar el acceso a la información geoespacial.

La creación de esta Oficina no requiere inicialmente más hardware y software que el necesario para tareas administrativas. Pero en las definiciones de estándares y buenas prácticas se promoverá el uso de herramientas libres para el tratamiento de los datos y, si no fuera posible, la definición de acuerdos adecuados para preservar la confidencialidad, la integridad y la disponibilidad en el marco de la protección de los datos.

2 Situación-Problema u Oportunidad

El actual contexto de pandemia por COVID-19 y las consecuentes modalidades de DISPO (Distanciamiento Social, Preventivo y Obligatorio) y ASPO (Aislamiento Social Preventivo y Obligatorio), promovieron un mayor uso de las herramientas para la interacción y comunicación remota entre todos los actores, tanto internos y externos, de la Provincia de Buenos Aires.

Desde trámites de la ciudadanía a procedimientos internos y con terceros, el intercambio de datos es imprescindible para cumplir con los diferentes procesos en la administración pública provincial.

El Gobierno de la Provincia de Buenos Aires, mediante sus diferentes organismos y dependencias, genera, usa, procesa, transmite y elimina datos. Estos datos son obtenidos mediante diferentes fuentes (formularios, sistemas, redes sociales, etc.) y están en diferentes formatos (papel, digital, audios, etc.).

Gran parte de ellos son datos personales de la ciudadanía que deberían resguardarse adecuadamente. Pero también hay datos que son estratégicos en el marco de la gobernabilidad y que también deber accedidos y tratados sólo por el personal autorizado.

En un enfoque realista, la dificultad reside en dos miradas que se suponen opuestas: protección y accesibilidad. Hacer una propuesta sin analizar esta relación de fuerzas conduce al acceso dificultoso al dato o su vulnerabilidad.

En este contexto de dar valor al dato, es imprescindible comenzar por tomar conocimiento acerca de qué datos trata una organización, qué operaciones se realizan, su naturaleza, si existen roles relacionados con ellos. Algunos organismos del GPBA son grandes estructuras, con dependencias distribuidas en el territorio provincial. Se pierde referencia de los datos que se tratan, su criticidad y sensibilidad.

Es habitual compartir datos sin descripción, que en algunos casos participan en estadísticas, siendo interpretados erróneamente, y por lo tanto llegando a conclusiones equivocadas.

Para poner en contexto los escenarios existentes y la vulnerabilidad de los datos, se analizan a continuación tres tipos de datos: personales, estratégicos y estadísticos

2.1 Datos Personales

La SGD reconoce la importancia y por lo tanto la necesidad de la administración de los datos personales de la ciudadanía.

De acuerdo con la Ley 25326 [2], de Protección de los Datos Personales, se considera dato personal a la información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

En los documentos internacionales, los datos personales son referidos como PII, Personally Identified Information.

Según la Regulación General de Datos Personales europea (RGDP; en inglés General Data Protection Regulation, GDPR) dato personal es cualquier dato que puede ser usado para identificar a una persona (GDPR) [3].

En la ISO/IEC 29151 (o su gemela, la recomendación ITU X.1058) se considera PII cualquier información que a) pueda ser usada para identificar a una persona que está relacionada con esa información o b) pueda directa o indirectamente relacionarse con una persona [4].

En la Publicación Especial NIST 800-122, PII es cualquier información sobre una persona que posea una organización, incluyendo: a) cualquier información que pueda ser usada para distinguir o rastrear la identidad de una persona, tales como nombre, número de seguridad social, fecha y lugar de nacimiento, nombre de soltera de su madre, o registros biométricos; b) cualquier información que esté vinculada pueda vincularse con un individuo, por ejemplo, información de salud, financiera o de empleo [5].

En la que podemos considerar como el estándar más reconocido acerca de los sistemas de gestión de la seguridad de la información, la ISO:IEC 27001: 2013, se define un control indicando la recomendación sobre asegurar la privacidad y protección de PII mediante legislaciones y regulaciones donde sea aplicable [6].

Las distintas dependencias del Gobierno de la PBA obtienen estos datos de la ciudadanía, y su tratamiento debe ser el adecuado para su protección, garantizando razonablemente la confidencialidad, la integridad y la disponibilidad.

Las herramientas de identificación/autenticación deben lograr el equilibrio ya planteado de accesibilidad y protección. Deben elegirse un conjunto de elementos (número de trámite presente en el DNI, CUIT, dato biométrico u otro medio) que garanticen que toda persona residente en el territorio bonaerense puede concretar ese proceso con un enfoque realista, incluyendo situaciones tales como personas sin DNI, extranjeros residentes, etc.

La replicación del dato personal en diferentes bases de datos puede generar copias desactualizadas y necesitar la intervención repetida de las personas para su ratificación o rectificación, lo que genera pérdida de oportunidades, retrasos en trámites, o la posibilidad de acciones ilegales ante la falta de control acerca de los datos.

El riesgo inherente a no realizar un tratamiento adecuado de esos datos es su exposición ante personas/entidades no autorizadas a su acceso, o una mala interpretación en su contexto.

GDPR considera una violación de la seguridad de los datos personales a:

> *"Toda violación de 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".*

El decreto de la Nación Argentina nro. 1558/2001 [7] plantea que lo adecuado en cuanto al nivel de protección se define considerando la transferencia. Considera "…*la naturaleza de los datos, la finalidad y la duración de tratamiento o de los tratamientos previstos, el lugar de destino final, las normas de derecho, generales o sectoriales, vigentes en el país de que se trate, así como las normas profesionales, códigos de conducta y las medidas de seguridad en vigor en dichos lugares, o que resulten aplicables a los organismos internacionales o supranacionales*…".

Las ciencias de datos, con conceptos de Big data, perfilado (profiling), etc., evidencian que desde el 2001, cuando fue promulgado ese decreto, el contexto ha cambiado y que la protección adecuada transciende la transferencia.

2.1.1 Disociación de datos personales

Se llama disociación de datos a todo tratamiento de datos personales donde la información obtenida no pueda asociarse a persona determinada o determinable. De esta manera se puede trabajar los datos sin exponer la identidad de su titular.

GDPR define la seudomización como el "*...tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable...*" Permite la re-identificación.

La des-identificación es el proceso por el cual no permito volver a identificar el titular del dato. Por ejemplo, si destruyo la información adicional que mantiene la seudomización destruyo la posibilidad de re-identificación

La anonimización es el proceso donde se aplican operaciones adicionales sobre los datos para no re-identificarlos (funciones criptográficas, perturbación de datos, reducción de datos, etc.). Es irreversible.

2.1.2 Privacidad por diseño

La privacidad por diseño (Privacy by design, PBD) trata sobre incorporar los principios de privacidad dentro del diseño, operación y gestión de un objeto (hardware, software, sistema, servicio o proceso) involucrado en los sistemas de la organización. Ese ciclo de vida el objeto son todas las etapas por las que atraviesa el objeto desde su concepción hasta su retirada, pasando por las fases de desarrollo, puesta en producción, operación, mantenimiento y retirada.

Este concepto fue expuesto por Ann Cavoukian, y luego aceptado en la "Resolución sobre la Privacidad por Diseño", en la 32ª Conferencia Internacional de Comisionados de Privacidad y Protección de Datos en Jerusalén, Israel, en octubre de 2010.

PBD se sostiene en un conjunto de principios como la proactividad, la privacidad incorporada en la fase de diseño, tener un enfoque centrado en el sujeto de datos, el aseguramiento de la privacidad en todo el ciclo de vida, entre otros.

Proponer PBD es cambiar el paradigma habitual en el desarrollo de los sistemas informáticos o un hardware, o la configuración de un nuevo sistema de comunicaciones. Debe estar presente desde el principio, no ser una capa que se agrega al final.

Un análisis acerca de privacidad de los datos que se verán involucrados en un sistema informático o de comunicaciones, debe estar presente desde las primeras fases de desarrollo y no ser una capa añadida a un producto o sistema. Esta forma temprana de detección de las características de lo datos, permite planificar e implementar una protección adecuada.

2.2 Datos estadísticos

La interpretación del dato es decisiva en su participación en las estadísticas. La falta de claridad o acuerdo acerca de su significancia puede llevar a conclusiones erróneas.

La aplicación de métodos cuantitativos o cualitativos no adecuados a la naturaleza del dato pueden ser un factor de degradación en la calidad de los resultados del proceso de tratamiento.

Tipo de dato, método, herramienta para su procesamiento, son elementos que deben considerarse para obtener resultados de calidad y que habiliten la representación de la realidad y la posibilidad de inferencia o proyección.

2.3 Datos estratégicos

La información estratégica es un componente de la gobernabilidad que se sostiene sobre datos de calidad. La información debe ser oportuna, relevante, verificable, proveniente de diversas fuentes.

El primer paso es definir qué criterios definen a la información como estratégica, qué datos o combinación de ellos aportan a esa información y cómo se obtiene, se procesa y se protege.

Esta información estratégica es el elemento fundamental del proceso de toma de decisiones.

3 Solución

La solución que se propone es coherente con una política digital del GPBA, que se inicia con la definición de ejes estratégicos dentro de la SGD. Si bien la situación de pandemia atrasó la concreción de los objetivos que es ese momento se plantearon a corto plazo, este período fue un intenso aprendizaje en cuanto a la realidad de la provincia de Buenos Aires y su inserción en el mundo digital.

Con respecto al tratamiento de los datos, este aprendizaje puso en evidencia una falta de cuidado en su valor, recomendaciones de uso y control.

Para definir el concepto de tratamiento del dato nos referiremos a la Ley 25.326, de protección de los datos personales:

> *"Operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias".*

Habitualmente, cuando se refiere al tratamiento del dato, se reitera un enfoque desde lo jurídico, imprescindible, pero insuficiente en el marco de los objetivos de la OTDD: cómo la tecnología aporta a ese tratamiento adecuado de manera asequible, dinámica, inclusiva.

3.1 Funciones de la OTTD

En este contexto se atribuirán a la OTTD un conjunto de funciones, principalmente orientadas a establecer un marco de uso adecuado de los datos, a ser elaborado en conjunto con los organismos provinciales y promoviendo la creación de entidades propias en cada uno de ellos para fortalecer una cultura de protección del dato.

Se proponen el siguiente conjunto de funciones:

- Definir y promover políticas acerca del tratamiento digital del dato en el contexto del gobierno provincial por parte por parte de los sistemas informáticos
- Definir y promover los criterios y su evaluación, por ejemplo, la criticidad, la sensibilidad
- Definir tipos de datos, e identificar qué datos son críticos en el contexto de los procesos
- Establecer recomendaciones basadas en estándares y buenas prácticas para el tratamiento de datos
- Establecer especificaciones y funcionalidades de las herramientas para el tratamiento del dato que garanticen su preservación digital y faciliten la interoperabilidad
- Promover el análisis y la aplicación efectiva de nuevas tecnologías que hagan un aporte significativo en el tratamiento del dato. Big data, herramientas de machine learning, Distributed Ledger Technologies (DLT), sovereign identity, entre otros, son tecnologías que deben ser analizadas en el marco de una innovación responsable.
- Acordar con los organismos pautas claras de preservación digital que incluya formato, almacenamiento, destrucción efectiva de la información en dispositivos de descarte.
- Establecer pautas acerca de la disociación de datos para los procesos que lo precisen

- Promover un tratamiento adecuado de los datos personales respetando los principios de privacidad, como finalidad, uso legítimo, consentimiento, etc.

3.2 Interacción con los organismos provinciales

Se propone que esta oficina esté dentro del ámbito de la SGD, lo que permite trabajar los objetivos en conjunto con las cuatro direcciones de su área: DPSIT, DPT, DPMA y DPGEL.

Cada organismo provincial designa un representante del organismo que tendrá contacto activo con la Oficina. Como representante debe transmitir propuestas y necesidades del organismo para que la labor de la Oficina tengo una impronta realista, de los problemas o vulnerabilidades sobre los datos. Debe trasladar propuestas e inquietudes de la Oficina al organismo. El rol de este representante es fundamental para lograr buenas prácticas o definir estándares que realmente sean útiles para la administración adecuada de los datos.

3.4 Actividades

En el contexto de las funciones enunciadas, se plantean a continuación un conjunto de actividades a cumplir, sostenidas por jornadas de capacitación y concientización con los organismos provinciales:

- Desarrollar una política de protección de datos personales
- Definición de normativa para el tratamiento de los datos (incluyendo datos personales)
- Definición de tipos de datos y categorías
- Definición de roles en el tratamiento del dato
- Creación del inventario provincial de datos
- Elaboración un código de conducta sobre los datos
- Definición de principios sobre los datos

A continuación, se desarrollan algunos de estas propuestas específicas.

3.5 Inventario Provincial de Datos

Una de las propuestas en el contexto de la OTTD es la creación y mantenimiento de un inventario provincial de datos, para saber dónde están los datos, con qué finalidad, acceso, su naturaleza y trazabilidad, actualización, etc.

Actualmente el GPBA. no tiene un registro de datos. Cada organismo administra sus propios repositorios de datos y los intercambia mediante diferentes herramientas. En algunos casos se utilizan servicios que, definen y formalizan, en cierto modo, la dinámica por sí mismos. En otros casos se comparten bases de datos o se transfiere información, sin existir ningún instrumento formal acerca de ese intercambio.

Habitualmente, un organismo pierde la trazabilidad del dato que transfirió. La actualización del repositorio original no genera un efecto de modificación en todos los repositorios. Por lo tanto, esos datos no actualizados conducen a situaciones no deseadas que se evidencian en forma tardía, atrasando un trámite, generando estadísticas poco fiables, desconfianza y falta de credibilidad.

3.6 Código de conducta sobre los datos

Los códigos de conducta son un mecanismo para la autorregulación por parte de los responsables y encargados (controller y processor, en GDPR) para el cumplimiento de la normativa que hayan adoptado para la protección de datos personales.

El artículo 30 del Decreto 1558/2001 [7] que reglamenta la Ley N.º 25.326 alienta a elaborar códigos de conducta destinados a contribuir, en función de las particularidades de cada sector.

3.7 Definición de Principios aplicables al tratamiento de datos personales

SI bien la OTTD abarcará el tratamiento de todo tipo de dato, la necesidad de proteger adecuadamente los datos personales de la ciudadanía le da a éstos un lugar preferencial.

La norma ISO/IEC 29100 [7] establece 11 principios relacionados con la protección de datos personales:

- Consentimiento y opción
- Legitimidad de propósito y especificación
- Limitación en la recolección
- Minimización de datos
- Limitación de uso, retención y divulgación
- Exactitud y calidad
- Apertura, transparencia y notificación
- Participación individual y acceso
- Rendición de cuentas
- Seguridad de la información
- Cumplimiento de la privacidad

GDPR también establece sus principios, como así también la Organización para la Cooperación y el Desarrollo Económicos (OCDE). No obstante, los principios indicados en la ISO 29100:2011 [8] cubren la totalidad de las características de todos los anteriores.

En la figura 1, y a modo de ejemplo, se detalla el cumplimiento de acuerdo con el tipo de dato con respecto a estos principios.

Principio	Dato personal	Dato estratégico (*)	Dato estadístico (*)
Consentimiento y opción	x		
Legitimidad de propósito y especificación	x		
Limitación en la recolección	x		
Minimización de datos	x		
Limitación de uso, retención y divulgación	x	x	x
Exactitud y calidad	x	x	x
Apertura, transparencia y notificación	x		
Participación individual y acceso	x		
Rendición de cuentas	x	x	X
Seguridad de la información	x	x	X
Cumplimiento de la privacidad	x	x	
Responsabilidad de Interpretación			X

(*) usando técnicas de pseudoanomización o anomización

Figura 1 – Principios aplicables sobre los datos, ISO/IEC 29100:2011

La importancia del consentimiento para el uso de los datos personales merece un párrafo. La ISO/IEC 29184:2020 [9], no sólo estandariza la terminología relacionada, si no que da importantes pautas para el manejo del consentimiento en línea. Está norma define el consentimiento explícito como el acuerdo dado libremente, en forma específica y no ambigua para el procesamiento de los datos personales mediante un acto afirmativo del titular de esos datos. Lo de acto afirmativo tiene que ver con lo que se llama modalidad OPT-IN, donde la persona debe indicar expresamente el consentimiento. Lo más común es implementarlo mediante un checkbox, donde al marcarlo, indica su consentimiento.

Las solicitudes de consentimiento deben ser "claramente distinguibles de los demás asuntos" y presentadas en "lenguaje claro y claro". Los interesados pueden retirar el consentimiento otorgado previamente cuando lo deseen (renovación de consentimiento).

4 Conclusiones

La protección adecuada de los datos de acuerdo con principios establecidos tales como la exactitud, definición de propósito, de plazo de conservación, responsabilidad, confidencialidad, integridad beneficia a:

- cualquier persona del mundo que habite definitiva o temporariamente en la Provincia de Buenos Aires y realice trámites con el Gobierno Provincial, y si además esa persona es ciudadana de la Unión Europea se debe garantizar que el tratamiento de sus datos es adecuado de acuerdo con las exigencias de GDPR;
- cualquier entidad con o sin fines de lucro, regionales, provinciales o internacionales, privadas o públicas, que realizan trámites con el Gobierno Provincial;
- cualquier entidad que desee realizar estadísticas sobre datos de la Provincia;
- cualquier entidad que use, procese, almacene, transfiera o pretenda destruir datos inicialmente generados en dependencias provinciales.

Si bien contar con un área de datos es habitual en las organizaciones, es la primera vez en el Gobierno de la Provincia de Buenos Aires, donde se establecerá una oficina que promueva y acompañe a las dependencias en el camino de la puesta en valor del dato mediante su tratamiento adecuado de acuerdo con un conjunto de principios, definición de buenas prácticas y acciones. Esta propuesta es innovadora en cuanto a su creación en la Provincia y el alcance de sus objetivos.

La creación de la OTDD pone el valor el dato promoviendo una cultura para su tratamiento adecuado. Las acciones derivadas de la creación de esta oficina garantizan la confiabilidad no sólo en el tratamiento de los datos dentro del GPBA sino por parte de aquellas entidades que realizan estadísticas, pues el dato está interpretado previamente para minimizar la posibilidad

Los ejes estratégicos de la SGD y su política digital, como así también las misiones y funciones de sus Direcciones Provinciales que constituyen el núcleo directo y consultor de la Oficina dan plena viabilidad a esta propuesta.

El interés de los agentes provinciales en ser parte de una jerarquización profesional se puso en evidencia en la alta participación en actividades llevadas a cabo por la SGD, por ejemplo, en las charlas previas a la presentación del Plan de Ciberseguridad.

Se promoverá que cada organismo provincial tenga su propia oficina del dato donde canalizar propuestas y registrar situaciones tales como vulnerabilidades (posibles o detectadas) o amenazas.

Referencias

[1] Ribble Mike S., Bailey Gerald D., y Ross Tweed W.. “Digital Citizenship, addressing appropriate technology behavior". https://files.eric.ed.gov/fulltext/EJ695788.pdf. Septiembre 2004

[2] Ley 25236, Protección de datos personales. Sancionada: Octubre 4 de 2000. Promulgada Parcialmente: Octubre 30 de 2000. http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

[3] Regulación General de Datos Personales europea (RGDP; en inglés General Data Protection Regulation, GDPR). Información en https://gdpr-info.eu/

[4] ISO/IEC 29151 :2017. Information technology — Security techniques — Code of practice for personally identifiable information protection. Gemela a Recomendación ITU X.1058

[5] National Institute of Standards and Technology (NIST). Special Publication 800-122

[6] ISO/IEC 27001: 2013. Information technology — Security techniques — Information security management systems — Requirements

[7] Decreto 1558/2001. PROTECCION DE LOS DATOS PERSONALES

[8] ISO/IEC 29100 :2011. Information technology — Security techniques — Privacy framework

[9] ISO/IEC 29184 :2020. Information technology — Online privacy notices and consent