UNIVERSIDAD NACIONAL DE LA PLATA

FACULTAD DE INFORMÁTICA

TESINA DE LICENCIATURA

TÍTULO: MODELO DE PREVENCIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES.

AUTORES: Sebastián María Alejandra – Vazquez Nadia Estefanía

DIRECTOR: Molinari Lía

CODIRECTOR:

ASESOR PROFESIONAL:

CARRERA: Licenciatura en Sistemas

Resumen

El tema sobre los datos personales fue elegido porque reconocemos, que con el avance tecnológico la información está más expuesta a distintos ataques y estos datos necesitan una seguridad y un manejo correcto adicional, que trabajando con buenas prácticas una organización puede alcanzar los niveles de confianza para no exponer información indebida y trabajar con procesos seguros y circuitos de mejora continua.

Palabras Clave

Datos Personales – Datos Sensibles – Protección de Datos Personales

Conclusiones

Debido a que los datos personales pertenecen a su titular y no a las entidades que utilizan las bases de datos, se han puesto en marcha iniciativas alrededor del mundo, que buscan proteger los datos personales que se encuentran en posesión de particulares o de gobiernos, haciendo de la tarea de protección de la información, una responsabilidad compartida entre los usuarios, las organizaciones que tienen acceso a los datos y gobiernos que deben legislar al respecto, así como crear las instituciones encargadas de regular y hacer cumplir las leyes.

Trabajos Realizados

Entre los antecedentes de investigación se encuentran:
1. Congreso CACIC 2018: Caso de estudio sobre GDPR aplicado en Sistemas de Gestión Académica.
2. Contribución en la ITU Septiembre 2019: REVISIÓN OF ITU-T X.1058.
3. Contribución en la ITU Mazo 2020: The Open Consultation on the draft Guidelines for utilization of the GCA.
4. Contribución en la ITU en Junio 2020: Recommendations for the ITU Guidelines for Child Online Protection, in relation to Cookies and Consent.

Trabajos Futuros

- *Revisar el impacto que tiene el tratamiento de datos personales utilizando tecnologías distribuidas o DLT.*
- *Realizar una guía que sirva de entrada para realizar auditorías en Bases de datos personales.*
- *Cómo influye el Modelo de Alineamiento (SAM) dentro de las organizaciones, teniendo en cuenta los datos personales.*
- *Cómo una organización puede realizar el ciclo de vida de sus procesos utilizando el modelo de referencia (COBIT 5) con la perspectiva en datos personales.*
- *Un tablero de control con las estadísticas/métricas de estos, para saber a dónde debería apuntar la organización para mejorar sus procesos.*
- *Guía para la Construcción del consentimiento.*

Fecha de la presentación: Septiembre 2021

FACULTAD DE INFORMATICA

UNIVERSIDAD NACIONAL DE LA PLATA

MODELO DE PREVENCIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES UN ENFOQUE TECNOLÓGICO

Autores: Sebastián, María Alejandra

Vázquez, Nadia Estefanía

Directora de Tesina: Dra. Lía Molinari

Año de Presentación: 2021

La Plata, Argentina

Agradecimientos

A mi hija Ainara

En primer lugar quiero agradecer a mi compañero de vida que siempre estuvo presente ayudándome, acompañándome y respetando mis espacios de estudios pero dando aliento con un “Dale María” para seguir.

A mi amiga y compañera de tesina, Nadia. Siempre estaré agradecida por su paciencia y apoyo; fue una hermosa experiencia escribir juntas.

A todas mis amigas, que siempre me apoyaron y brindaron amor, con mensajitos, cartelitos y chocolates para estudiar.

A nuestra directora de tesina que desde el inicio nos apoyó en todos los proyectos que queríamos hacer y que nos dio la oportunidad de crecer en este tema que desde el inicio supimos que no sólo era importante para nosotros sino para todas las personas.

Y a mis padres y mi familia, ya que sin su apoyo nunca hubiera podido estudiar esta hermosa carrera.

A Dios y a mis padres Elsa y Eduardo, por darme la oportunidad de estudiar, por sostenerme para llegar y estar incondicionalmente a mi lado.

Ale es quién dedico muchas horas de su vida, para hacer reuniones, tirar ideas, escribir, leer, pensar, analizar, revisar y soñar que después de rendir concurrente, nos recibíamos. Amiga y compañera de todos estos años, a vos gracias Mamasa.

A Fer mi leal compañero quién compartió este proceso conmigo, ayudándome en todo siempre con buen humor, palabras y gestos que me alentaron a seguir.

A Lía, por tener la visión de que lo podíamos hacer y siempre nos empujó a más.

A mis hermanas/o Ana, Sami y Milo por acompañarme y estar en cada momento. A mis amigos y amigas, los de siempre y los hechos en este camino.

A la Universidad Pública y en especial al grupo educativo de la Facultad de Informática.

ÍNDICE

Palabras clave

Consentimiento - Datos Personales – Datos Sensibles – Protección de Datos Personales – Seguridad de los datos – Política de privacidad

Nómina de abreviaturas

AMNT: Asamblea Mundial de Normalización de las Telecomunicaciones.

ARCO: Derechos de Acceso, Rectificación, Cancelación y Oposición.

COP: Child Online Protection (Protección infantil en línea).

DP: Datos Personales.

DPD: Oficiales de Protección de Datos.

DPO: Data Protection Officer.

GDPR: General Data Privacy Regulation.

ICT: Information and Communication Technology.

IP: Protocolo de Internet.

ITU: Telecommunication Union (Unión Internacional de Telecomunicaciones).

PIA: Privacy Impact Assestment o una Evaluación de Impacto en la Protección de Datos Personales.

PII: Personally Identifiable Information.

PBD: Privacy by Design (Privacidad por Diseño).

SAM: Modelo de Alineación Estratégica de Henderson y Venkatraman.

SI: Sistemas de Información.

SSL: Secure Socket Layer o Capa de conexión segura.

UE: Unión Europea.

UIT: Unión Internacional de Telecomunicaciones.

Glosario

Acceso no autorizado: El acceso no autorizado a un sistema informático, consiste en acceder de manera indebida, sin autorización o contra derecho a un sistema de tratamiento de la información.

Activo: Cualquier recurso que tenga valor para la organización.

Anonimización: Técnica que se aplica a los datos personales con el objetivo de eliminar las posibilidades de identificación de las personas de manera irreversible, pero manteniendo la veracidad de los resultados del tratamiento de los datos.

Buenas Prácticas: una práctica que se ha demostrado que funciona bien y produce buenos resultados, y, por lo tanto, se recomienda como modelo.

Data leak: Fuga de datos. Acceso por partes no autorizadas a datos de acceso restringido.

Encriptación de datos: La encriptación de datos o cifrado de archivos es un procedimiento mediante el cual los archivos, o cualquier tipo de documento, se vuelven completamente ilegibles gracias a un algoritmo que desordena sus componentes.

Gestión de claves: La gestión de claves de cifrado es administrar el ciclo de vida completo de las claves criptográficas. Esto incluye: generar, usar, almacenar, archivar y eliminar claves. La protección de las claves de cifrado incluye limitar el acceso a las claves física, lógica y mediante el acceso de usuario / rol.

IP: Conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo), que corresponde al nivel de red del modelo TCP/IP.

NIST Privacy Framework: Es una herramienta voluntaria desarrollada en colaboración con las partes interesadas con la intención de ayudar a las organizaciones a identificar y administrar los riesgos de privacidad para crear productos y servicios innovadores mientras se protege la privacidad de las personas.

Organización: Una organización es una asociación de personas que se relacionan entre sí y utilizan recursos de diversa índole con el fin de lograr determinados objetivos o metas. Esta estructura ordenada coexiste e interactúa con personas con diversos roles, responsabilidades o cargos, donde usualmente cuenta con normas (formales o informales) que especifican la posición de cada persona en la estructura y las tareas que debería llevar a cabo.

Pseudo Anonimización: Corresponde al 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 atribuyen a una persona física identificada o identificable.

Segregación de tareas: Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

SSL: Una tecnología que se utiliza para securizar la transmisión de datos en internet: cifra y protege los datos transmitidos utilizando el protocolo HTTPS.

Tokenización: proceso que permite proteger datos sensibles, sustituyéndolos por equivalentes no-sensibles, conocidos como tokens.

Resumen

El camino que recorrimos para llegar hasta aquí, comenzó con un artículo que se presentó en el congreso CACIC 2018, donde se analizó y trabajó sobre el impacto de GDPR en los sistemas académicos. Luego nos adentramos en un tema en particular: los datos personales. Si bien, nos encontramos con un abanico de artículos científicos, checklist, guías de buenas prácticas, recomendaciones para las organizaciones, tomamos el camino de los estándares, ya que los mismos tienen reconocimiento internacional. El tema sobre los datos personales fue elegido porque reconocemos, que con el avance tecnológico la información está más expuesta a distintos ataques y estos datos necesitan una seguridad y un manejo correcto adicional, que trabajando sobre un conjunto de ISO, una organización puede alcanzar los niveles de confianza y gestión de las buenas prácticas para no exponer información indebida y trabajar con procesos seguros y circuitos de mejora continua. Como resultado de trabajar sobre los estándares ISO, tuvimos la oportunidad de presentar propuestas de mejora en la ITU sobre la X.1058, basada en la ISO/CEI 29151:2017 durante los años 2019 y 2020.

La tesina se presenta en capítulos bien diferenciados, pero con el mismo lineamiento. El Capítulo 2 trata de cómo las organizaciones utilizan los datos para alimentar sus sistemas de información, y de esta manera, conseguir mayor competencia en el mercado. En los últimos años se han adoptado medidas de seguridad con respecto a esta información, para que no haya fuga de datos y la organización no pierda competitividad y/o reputación.

En el Capítulo 3 se desarrollaron definiciones en donde se resalta la importancia que tienen los datos personales y los datos sensibles; y cuál es el rol de la organización cuando se debe ejecutar un tratamiento, por ejemplo: otorgando información de una transferencia y/o una cesión. También se trabajó el consentimiento como pieza fundamental que tiene el titular de los datos, para demostrar que permite la utilización de sus datos, para las acciones que el consentimiento refleje, dejando de lado cualquier otra utilización.

Luego, en el capítulo 4 se dispone de las distintas bases de información que se tuvieron en cuenta para el desarrollo de la guía, se estudió y profundizó la ley Argentina, donde residimos, el GDPR y los estándares internacionales sobre temas IT y seguridad de datos, reconocidos a nivel mundial. Se analizó la Ley Argentina 25326, ya que es importante conocer la situación en la cual se encuentra, destacar su avance pero también plasmar los artículos que hoy esta ley reconoce como defensa del titular de los datos personales. El Reglamento general de datos personales se estudió como reflejo de la Unión Europea y lo que reconoce como datos personales, los derechos y obligaciones que el titular del mismo recibe; pero además fue una reglamentación de estudio ya que la República Argentina es reconocida por

parte de la Unión Europea como país seguro para realizar transferencia de datos. Se tomó el estándar ISO/IEC 27701:2019 (ISO, 2019), que posee amplia experiencia en brindar puntos de seguridad, y este apartado hace mayor foco en seguridad de datos personales. Estas sugerencias abarcan el contexto de la organización, roles y responsabilidades y brinda lineamientos para la seguridad a través de distintas políticas. Por último se incorporó la ISO/IEC 29134:2017 (ISO, 2017) que habla de la Evaluación de Impacto. Este tema es muy importante para que la organización evalúe el impacto de realizar el tratamiento de datos personales, obtener resultados y verificar si con los controles necesarios la organización puede afrontar el riesgo que existe por su tratamiento. Este tipo de evaluación se realiza antes de cualquier tratamiento por lo cual la organización puede tener un panorama y decidir si seguir por el camino del tratamiento o desistir.

En el capítulo 5 como parte de la etapa de mitigación de los distintos tipos de ataques donde el principal perjudicado es el titular de los datos y es la organización quién tiene que velar por la seguridad de estos, se pensó una herramienta que le permita a la organización hacer una retrospectiva de los procesos internos y el manejo del conjunto de datos personales, para que pueda a futuro planificar mejoras y tomar buenas prácticas, para no solo cumplir con las regulaciones vigentes si no con estándares internacionales como son las ISO sobre datos personales. Esta guía posee puntos para que la organización pueda tener un relevamiento de lo que posee, y lo que le falta. La misma está dividida en etapa, esto es porque al agruparlas no solo facilita su lectura, sino que a medida que avanza en la etapa, se procede en el camino natural del ciclo de vida del dato. Pero no se pensó como reemplazo de ningún estándar, sino como complemento de mejores prácticas para llevar a la organización a mejorar su desempeño garantizando que los datos personales están seguros y brindando confianza al titular de los mismos.

A través de los distintos trabajos que fuimos realizando notamos que los datos personales son importantes, pero no siempre la organización tiene una noción del impacto que puede tener sin su apropiada seguridad. Esta guía ayuda a las organizaciones a comenzar a tener en cuenta los datos personales como los activos más importantes, como clasificarlos y qué políticas comenzar tener en cuenta. Brinda Sirve como apoyo si se quiere tener una certificación, ya que ofrece los primeros pasos que se necesitan, no brindando una metodología, sino nombrando los puntos más relevantes. Pero además le brinda facilita a las organizaciones, que ya están maduras en este tema, una perspectiva desde el riesgo; ya que tomando los puntos de la evaluación de riesgo, las mismas pueden tener desde mucho antes del tratamiento que impacto tiene sobre la organización y así, tomar medidas, y/o controles para mitigar ese riesgo.

CAPÍTULO I: Introducción y Motivación

1.1 Introducción

Este trabajo de grado explora la temática de la protección de los datos personales mediante una mirada orientada a facilitar su tratamiento en las áreas de tecnología informática de una organización.

Mediante el análisis de normativa internacional, nacional, estándares y marcos referenciales identifica un conjunto de buenas prácticas hacia una cultura de la protección de datos, estableciendo un equilibrio entre el tratamiento adecuado y la disponibilidad orientada a la finalidad acerca del tratamiento de este tipo de información.

Las autoras de este trabajo han tenido la posibilidad de participar en el grupo de estudio 17 (SG17), “Cybersecurity” de la International Telecommunication Union ((ITU, 2020)) en propuestas de mejoras de recomendaciones relacionadas, y en la iniciativa Child Online Protection (COP, 2020) de la misma dependencia de Naciones Unidas, lo que les permitió identificar la protección de datos como un área de vacancia sobre la que investigar y proponer en el marco de la tecnología. Estas experiencias constituyen la motivación de este trabajo.

1.2 Objetivo general y específico

El objetivo general de la tesina es proveer un modelo para el tratamiento adecuado de los datos personales (DP) de una organización por parte de su área de tecnología informática, identificando buenas prácticas basadas en normativas internacionales, nacionales y marcos referenciales.

Este modelo constituye un modelo de prevención y tratamiento, pues acompañará a las organizaciones en asumir su responsabilidad en el resguardo de los datos personales en forma consciente y alineada al negocio.

El tratamiento de los DP Incluye el reconocimiento de los activos de información relacionados (localización e identificación), clasificación de la información (pública, privada, grado de sensibilidad, impacto ante su pérdida/borrado, robo, exposición no deseada), procesos que involucran acciones con datos personales con pautas que se adapten cumplimiento de leyes/normativas o buenas prácticas.

Los objetivos específicos en el marco de ese objetivo general, son:

- desarrollar una herramienta para la implementación de controles efectivos sobre los DP en las áreas de tecnología;
- elaborar un conjunto de recomendaciones que guíen al establecimiento de una cultura de la protección de los DP, difundiendo conceptos claves para la identificación de los DP y su tratamiento adecuado;
- identificar normativa, estándares y marcos referenciales para determinar un marco teórico a seguir en la construcción de buenas prácticas;
- promover el análisis de riesgo mediante la determinación del impacto en el tratamiento de la privacidad;
- establecer conceptos claves para el análisis de la incidencia de las nuevas tecnologías en la protección de los DP.

La herramienta habilita el análisis de los DP desde una etapa temprana, promoviendo la Privacidad por Diseño (Privacy by Design, PBD) y que el tratamiento de sus datos personales sea evaluado por responsables con una mirada práctica que garantice la disponibilidad, resguardando la confidencialidad y la integridad en el contexto de la privacidad.

1.3 Fuentes de análisis de información y análisis

En el contexto de esta temática, las autoras han identificado y analizado las siguientes fuentes, todas ellas reconocidas internacionalmente:

- GDPR
- Recomendación X.1058 de ITU/ISO/IEC 29151
- ISO/IEC 29100:2011
- ISO/IEC 27701:2019
- Protección de datos personales Ley Argentina 25.326

1.4 Participación en congresos y ámbitos de discusión

Entre los antecedentes de investigación se encuentran:

1. Congreso CACIC 2018: Caso de estudio sobre GDPR aplicado en Sistemas de Gestión Académica, donde se expuso sobre el reglamento europeo para la protección de los datos (General Data Privacy Regulation, GDPR), y cómo se

aplica en el ámbito académico nacional argentino poniendo en evidencia cómo una regulación europea tiene incidencia en repositorios locales.

2. Contribución en la ITU Septiembre 2019: REVISIÓN OF ITU-T X.1058, donde se expuso que para la revisión se tenga en cuenta, con colaboración de ADC.
3. Contribución en la ITU Mazo 2020: The Open Consultation on the draft Guidelines for utilization of the GCA, donde se contribuyó en la Agenda sobre Ciberseguridad Global.
4. Contribución en la ITU en Junio 2020: Recommendations for the ITU Guidelines for Child Online Protection, in relation to Cookies and Consent, donde se realizó un trabajo de investigación sobre el consentimiento en menores.

1.5 Publicaciones vinculadas a esta tesina

Título: Caso de estudio sobre GDPR aplicado en Sistemas de Gestión Académica

Autores: Nadia Vázquez, M. Alejandra Sebastián, Lía Molinari

Año: 2018

Evento: CACIC 2018

Lugar de realización: Tandil, Buenos Aires, Argentina

Contribuciones en ITU

- ITU-T X.1058; Revision of ITU-T Recommendation X.1058 incorporating relevant concepts

- Recommendations for the ITU Guidelines for Child Online Protection, in relation to Cookies and Consent

- Draft baseline text for a new work item on draft Recommendation ITU-T Y.Data.Sec.IoT-Dev “Requirements of data security for the heterogeneous IoT devices”

1.6 Organización de la Tesina

La presente tesina fue planteada y planificada en dos etapas, una fase de investigación y análisis, y otra de desarrollo de la guía.

En la primera etapa, se realizó una investigación referente al área de datos personales y los diferentes marcos legales que.

- Capítulo 1: Introducción y Motivación.
- Capítulo 2: Las Organizaciones basadas en los Sistemas de Información.
- Capítulo 3: Datos Personales y su protección.
- Capítulo 4: Regulaciones Sobre Datos Personales.
- Capítulo 5: Guía de buenas prácticas.

CAPÍTULO II – Las Organizaciones basadas en los Sistemas de información

2.1 Introducción

La información es clave para la competitividad en las organizaciones. Por ello es importante entender la diferencia entre datos, información y conocimiento. En una conversación informal, los tres términos suelen utilizarse indistintamente y esto puede llevar a una interpretación libre del concepto de conocimiento. En este capítulo se abordarán los conceptos sobre los tres términos y se relacionarán con la importancia dentro del contexto de una organización; y cómo un sistema de información (SI) crea valor a partir del conocimiento, que es utilizado para la toma de decisiones y el cumplimiento de las metas pautadas por la organización.

2.2 El dato

Según Davenport y Prusak (1999) (Autor, s.f.), un dato es un conjunto discreto, de factores objetivos sobre un hecho real. Es decir, un dato es una representación simbólica de alguna situación o suceso, sin ningún sentido semántico, describiendo un hecho concreto.

Algunas organizaciones relacionan el concepto de datos en el marco de los registros de transacciones. Las mismas realizan el tratamiento de datos utilizando diversas tecnologías, siendo hoy en día el activo más importante y valioso de estas; y la buena gestión de estos datos es esencial para su funcionamiento, ya que generan millones de transacciones diarias. Las organizaciones, por lo tanto, necesitan datos y son totalmente dependientes de ellos como, por ejemplo: Bancos, compañías de seguros, agencias gubernamentales y la Seguridad Social. Este hecho se reafirmó durante el año 2020 ante la situación de pandemia por COVID-19 que incrementó notablemente el acceso remoto a los sistemas de información.

Pero en general, la mayoría de las organizaciones, relevan y almacenan muchos datos. Este volumen de datos almacenado sin relación a un tratamiento, no le sirve a la organización por dos razones. La primera es que demasiados datos hacen más complicado identificar aquellos que son relevantes y, la segunda razón, es que los datos no tienen significado en sí mismos. Los datos describen únicamente una parte de lo que pasa en la realidad y no proporcionan juicios de valor o interpretaciones, y por lo tanto no son orientativos para accionar.

Es por esto que uno de los desafíos que tienen las organizaciones a la hora de relevar datos, es que los mismos se encuentren en un contexto acotado, directamente relacionado con el fin del tratamiento; y no se guarden datos que no sólo no sirven a la organización y consumen recursos como almacenamiento, si no que la falta de tratamiento adecuado sobre ese volumen puede concluir en una fuga de datos (data leak).

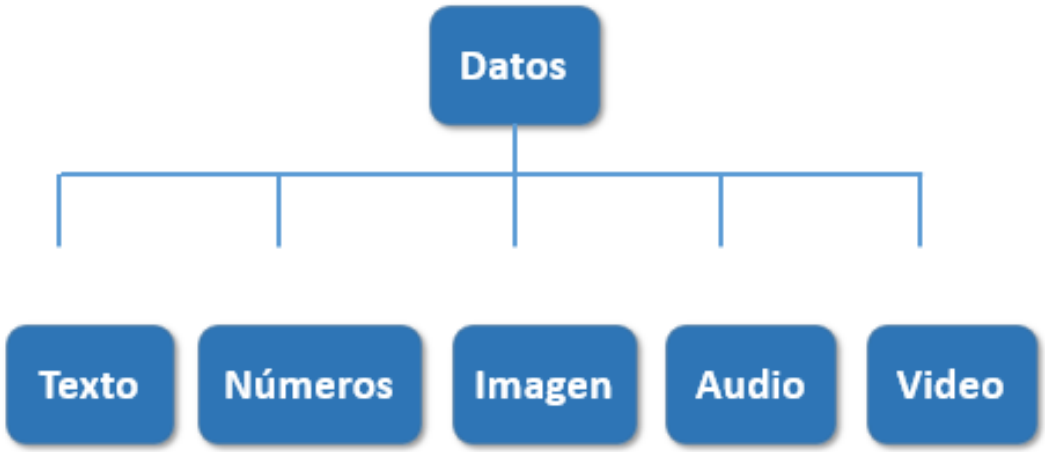

FIGURA 1: DATO

UNIDAD MÍNIMA DE INFORMACIÓN

2.3 La información

En algunos casos, la información se describe como un mensaje, normalmente bajo la forma de un documento o algún tipo de comunicación audible o visible. A diferencia de los datos, la información tiene significado (relevancia y propósito). No sólo puede formar potencialmente al que la recibe, sino que está organizada para un propósito. Es por esto, que los datos se convierten o transforman en información cuando se les provee significado, añadiéndoles valor de las siguientes maneras:

- Contextualizando: saber para qué propósito se generaron los datos.
- Categorizando: conocer las unidades de análisis de los componentes principales de los datos.
- Calculando: los datos pueden haber sido analizados matemática o estadísticamente.
- Corrigiendo: los errores se han eliminado de los datos.
- Condensando: los datos se han podido resumir de forma más concisa.

Las computadoras facilitan el añadir valor y transformar datos en información, pero un problema muy común es confundir la información con la tecnología que la soporta. Desde la televisión a Internet, es importante tener en cuenta que el medio no es el mensaje. Lo que se intercambia aporta el valor al medio que se usa para hacerlo. En definitiva, que actualmente tengamos acceso a más tecnologías de la información no implica que hayamos mejorado nuestro nivel de información.

Para la organización entonces, la información, es un conjunto de datos adecuadamente procesados, para proveer un mensaje que contribuya a la toma de decisiones a la hora de resolver un problema o afrontar una situación cualquiera.

FIGURA 2: INFORMACIÓN

AGRUPACIÓN DE LOS DATOS PARA TRANSMITIR UN MENSAJE DEL CONJUNTO

2.4 El conocimiento

Es la combinación de información, contexto y experiencia. La gran cantidad de información generada sólo será útil si puede aplicarse a la creación de conocimiento dentro de la organización. Para que la información se convierta en conocimiento es necesario realizar la comparación con otros elementos, predicción de consecuencias, búsquedas de conexiones y conversación con otros portadores de conocimiento. Entonces, una vez que el conocimiento es validado y orientado hacia un objetivo genera inteligencia (sabiduría).

Hace más de tres décadas que Russell Ackoff (Russell L.Ackoff, s.f.) desarrolló lo que hoy conocemos como “pirámide del conocimiento”. Esta pirámide es tomada como base para la Gestión del Conocimiento, tanto desde un punto de vista teórico como de aplicación a las organizaciones, donde se puede representar las relaciones entre Datos, Información, Conocimiento, y en algunos casos Sabiduría.

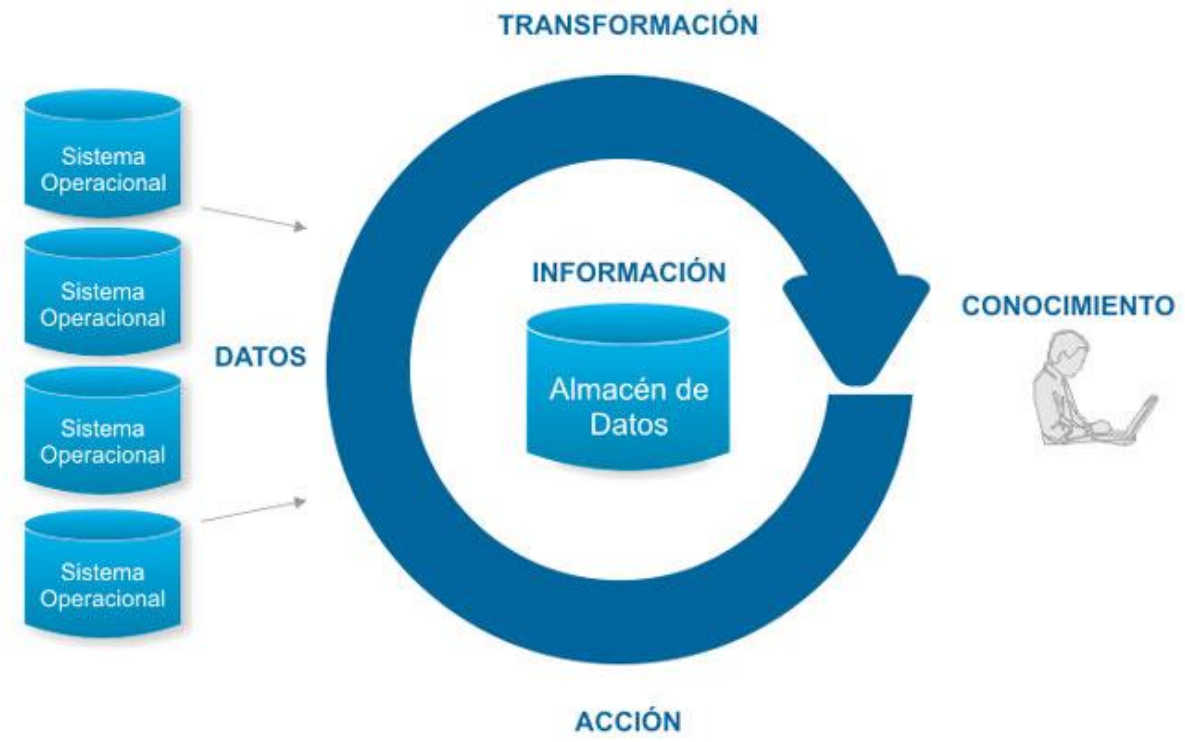

FIGURA 3: CONOCIMIENTO

INFORMACIÓN + EXPERIENCIA

2.5 Sabiduría

La sabiduría es la suma del conocimiento y la optimización. La optimización es un proceso creativo que se encarga de intentar modificaciones en la gestión de la información que realiza el Sistema de Información para cubrir las necesidades del negocio. La sabiduría supone poder modificar el sistema para mejorarlo con la garantía que dichas modificaciones lo mejoraran, gestionando todo el conocimiento para la toma de decisiones.

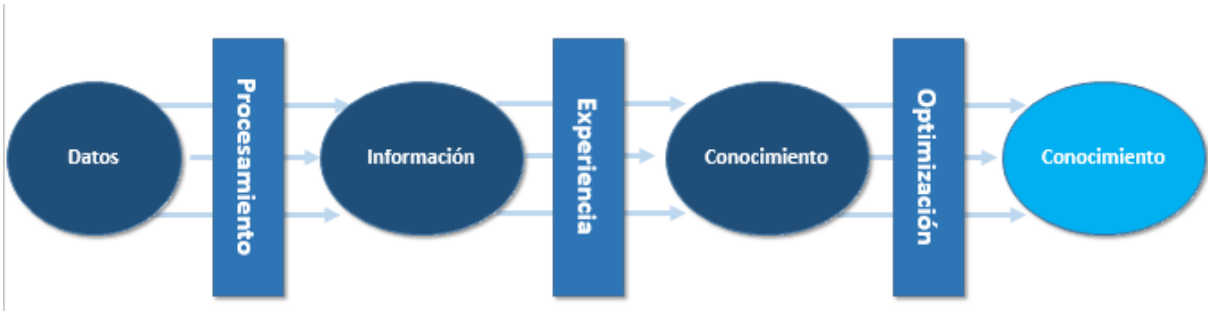

FIGURA 4: SABIDURÍA

CONOCIMIENTO + OPTIMIZACIÓN

Básicamente, la Pirámide del Conocimiento establece una jerarquía entre estos conceptos, colocando los datos en su parte más baja y la sabiduría en la más alta, o de más valor.

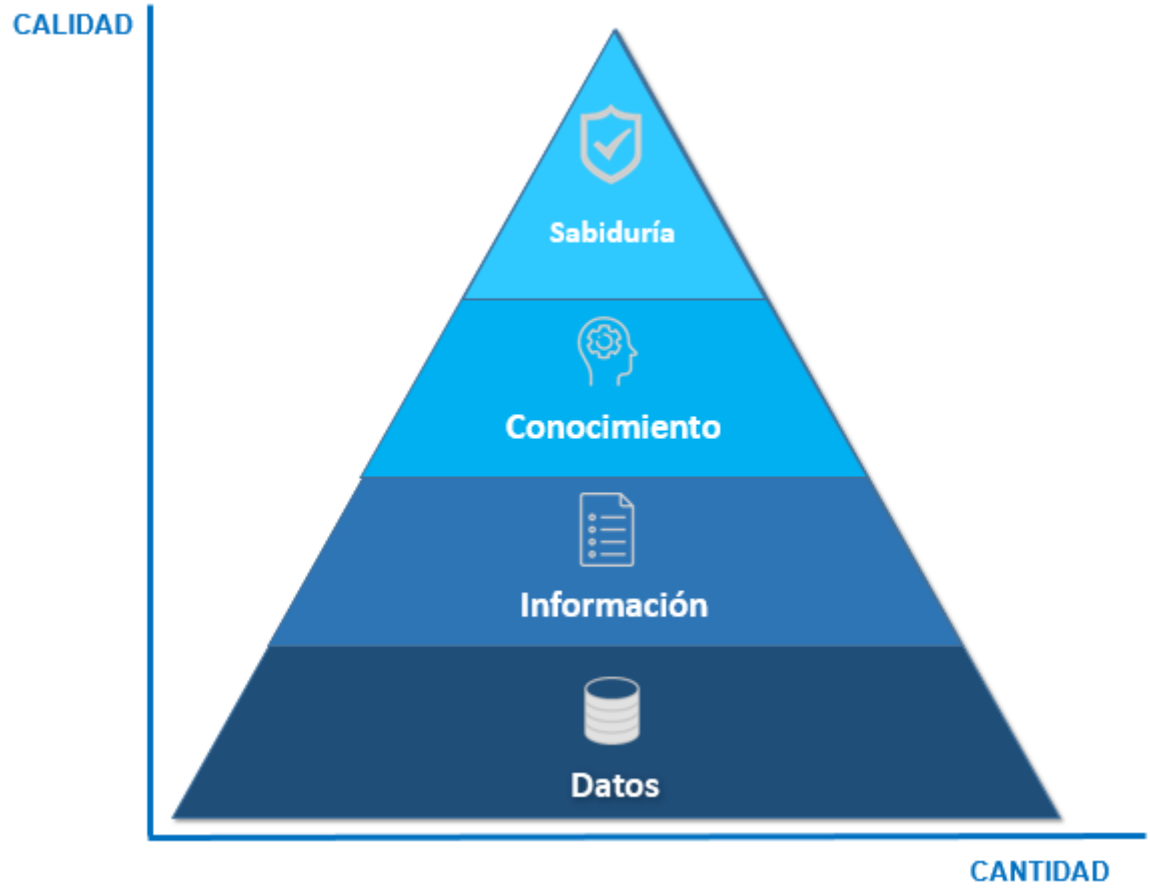

FIGURA 5: PIRÁMIDE DE CONOCIMIENTO

Así mismo, si aplicamos los criterios de calidad y cantidad, en los escalones superiores de la pirámide los datos serán pocos, pero con más calidad, mientras que en los escalones inferiores se encuentran más cantidad de datos y con poca o escasa calidad.

Esta información que fluye a través de la organización de forma diferentes a medida que sube los escalones de la pirámide, se asocia a políticas de innovación permanente, marketing estratégico, dirección por objetivos, calidad total y reingeniería de procesos, en el que se prioriza la productividad, la competitividad, el incremento de oportunidades, y la capacidad de liderazgo de las organizaciones.

Además, esta estrategia nos brinda beneficios como por ejemplo:

- Mejorar la calidad de sus productos y servicios
- Crea condiciones para mejorar el ambiente de trabajo.
- Mejora la comunicación interpersonal.
- Mejorando la información y la comunicación, estimula la participación de los trabajadores.
- Reducción del número de procesos de gestión/producción.
- Simplificación de los procesos de gestión/producción.
- Permite una mayor eficiencia en el uso de los recursos.
- Proporciona mejores herramientas para la gestión de la dirección.

2.6 Estado de los datos

El estado de un dato muestra un comportamiento cuando se encuentra con una característica en particular. Los datos se pueden encontrar en estados diferentes (sealpath.com, s.f.):

En reposo (WhatIs.com, Datos en reposo, s.f.): Es un término IT referido a datos inactivos que se almacenan físicamente en cualquier formato digital (ej.: bases de datos, almacenes de datos, hojas de cálculo, archivos, cintas, backups remotos, dispositivos móviles, etc.). Cualquier dato que no se mueva activamente de un lugar a otro, como un dispositivo a otro o una red a otra, se considera información en reposo a nivel físico, en nuestro caso podría ser el fichero .mdf, .ldf o los Backups que se realizan de la base de datos.

En uso (WhatIs.com, Datos en uso, s.f.): Es un término IT referido a datos activos que se almacenan en un estado no-persistentes digital, típicamente en una computadora, memoria de acceso aleatorio (RAM), Cachés de la CPU, o Registros de la CPU. A nivel lógico, son los datos que encontramos en las tablas de una base de datos.

En movimiento (sealpath, s.f.): Los datos en tránsito, o datos en movimiento, son datos que se mueven de una ubicación a otra, ya sea de un dispositivo a otro, a través de una red privada o de Internet, es decir cuando nuestros datos viajan en forma de paquetes por la red.

FIGURA 6: LOS ESTADOS DEL DATO

2.7 Sistemas de información como parte de la infraestructura de la Organización

Como lo definen, Laudon & Laudon y Piccoli (Laudon, 2012); un Sistema de Información (SI) es un sistema organizacional formalizado definido como un conjunto de componentes interrelacionados que incluyen elementos sociales y técnicos organizados para recolectar, procesar, ordenar, almacenar y convertir los datos en información.

Estos elementos formarán parte de alguna de las siguientes clases:

- Personas
- Datos
- Actividades o técnicas de trabajo
- Recursos materiales en general

Estos sistemas de información generan y gestionan información sobre datos de componentes relevantes para la organización como: clientes, empleados, compras, ventas, etc. Estos datos deben ser procesados previamente para generar información útil mediante cuatro actividades básicas:

- Entrada de información: proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, DVD, pendrives, código de barras, etc.
- Almacenamiento de información: es una de las actividades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sesión o proceso anterior.
- Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos, fuente de información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, por ejemplo que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

- Salida de información: es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, graficadores, la voz, etc.

FIGURA 7: SISTEMAS DE INFORMACIÓN Y ORGANIZACIÓN

Fuente: Laudon & Laudon (2012)

Esta información se distribuye en la organización para apoyar los procesos de toma de decisiones correcta y eficaz, relacionados con la coordinación, control de recursos, análisis de problemas y temas complejos así como en la creación de nuevos productos. Esta información fluye, como en la pirámide de gestión del conocimiento, de forma similar que en los niveles de una organización.

2.7.1 Niveles organizacionales

Los niveles organizacionales o pirámide organizacional (HelmutSy, 2019) corresponden a los tres niveles de gestión en la mayoría de las organizaciones, que son la gerencia de nivel inferior, nivel medio y nivel superior.

El objetivo en la parte superior de la jerarquía es considerar la estrategia a mediano y largo plazo de la organización. Los interesados en la parte intermedia toman un aspecto más específico de esta estrategia amplia y aseguran una implementación más detallada. En el nivel inferior se centran en la ejecución efectiva con objetivos a corto plazo.

Nivel superior o estratégico

Los gerentes de alto nivel toman decisiones que afectan a la totalidad de la organización, establecen objetivos y la dirigen para lograrlos. El papel principal del equipo ejecutivo, o gerentes de nivel superior, es mirar a la organización como un todo y planificar planes estratégicos.

Nivel medio o táctico

Este nivel es responsable ante la alta gerencia y responsable por los líderes del nivel inferior. Dedican más tiempo a las funciones organizacionales y supervisoras, realizando distintas actividades como:

- Ejecutar planes organizacionales de conformidad con las políticas de la compañía y los objetivos de la alta dirección.
- Definir y discutir información y políticas desde la alta gerencia hasta la baja gerencia.
- Inspirar y brindar orientación a los gerentes de nivel inferior para ayudarlos a mejorar el desempeño y también lograr los objetivos del negocio.

Este nivel se encuentra más involucrado en el trabajo diario de una organización, por lo que puede brindar información valiosa a los gerentes superiores, que ayudará a mejorar el desempeño de la organización utilizando una visión más amplia y estratégica.

Nivel inferior u operativo

En este nivel las funciones abarcan tareas como contratar, evaluar el desempeño, brindar retroalimentación, delegar tareas funcionales, identificar vacíos, maximizar la eficiencia, programar y alinear equipos.

En los tres niveles debe fluir la información y la misma debe ser consistente, ya que de ella se deberán tomar decisiones que brinden una oportunidad de crecimiento a la organización. Tomando la pirámide de la organización y junto a la información tenemos como resultado una pirámide que muestra dependiendo el nivel que tipo de información necesita y que cantidad, como lo muestra la Figura. 8.

FIGURA 8: PIRÁMIDE DE GESTIÓN DE CONOCIMIENTO EN LA TOMA DE DECISIONES

Esta figura muestra cómo las organizaciones se apoyan en los sistemas de información y en la información, y que los mismos crean valor para que los niveles estratégicos o de alta gerencia tomen decisiones.

El conocimiento es un factor importante para alcanzar los objetivos y metas estratégicas como para elevar en nivel de productividad y rentabilidad, sin embargo se debe utilizar de forma correcta. Es por esto que los sistemas de información deben ser confiables ya que las tecnologías de información resultan una herramienta muy valiosa.

2.7.2 Información como valor

Una de las actividades de las organizaciones es satisfacer las necesidades de las partes interesadas y a la vez como objetivo de gobierno es crear valor. Para satisfacer estas necesidades la organización debe encontrar un equilibrio entre obtener beneficios, optimizar el riesgo y optimizar los recursos. De esta manera, la organización puede obtener los beneficios pero utilizando de una manera eficiente los recursos disponibles. Para optimizar el riesgo las organizaciones se apoyan en sus sistemas de información, obteniendo información de calidad y disminuyendo a través de procedimientos valores por encima del umbral que soporta la organización.

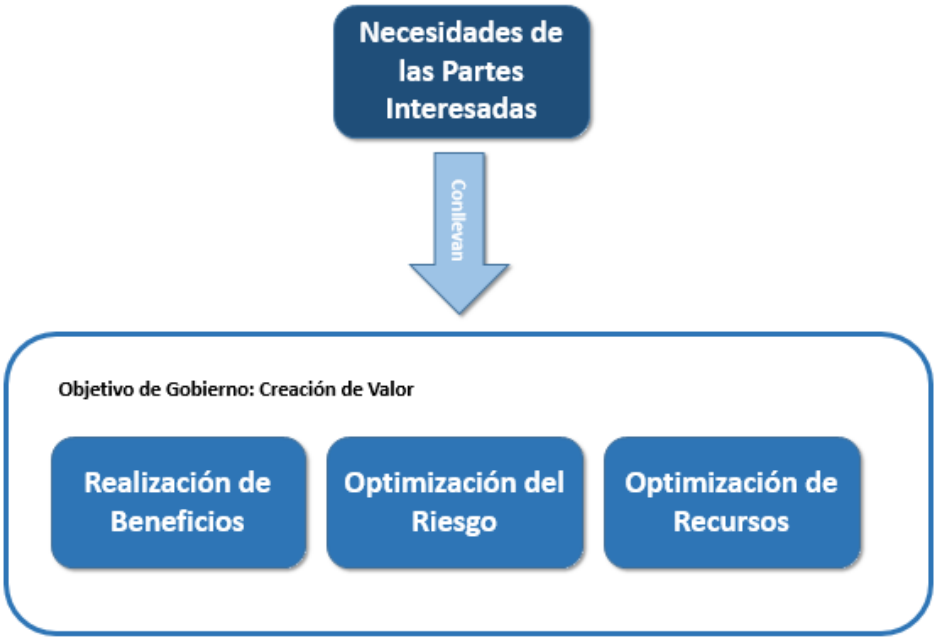

FIGURA 9: INFORMACIÓN COMO VALOR

Para que la información cree valor, la misma realiza un circuito de circulación. Este circuito comienza generando y procesando datos; para luego transformarse en información y en conocimiento. Después, crea valor para alimentar los procesos de Negocios. El conocimiento que llega a estos procesos de negocios tiene que ser de calidad para que la organización no tome decisiones basada en información errónea.

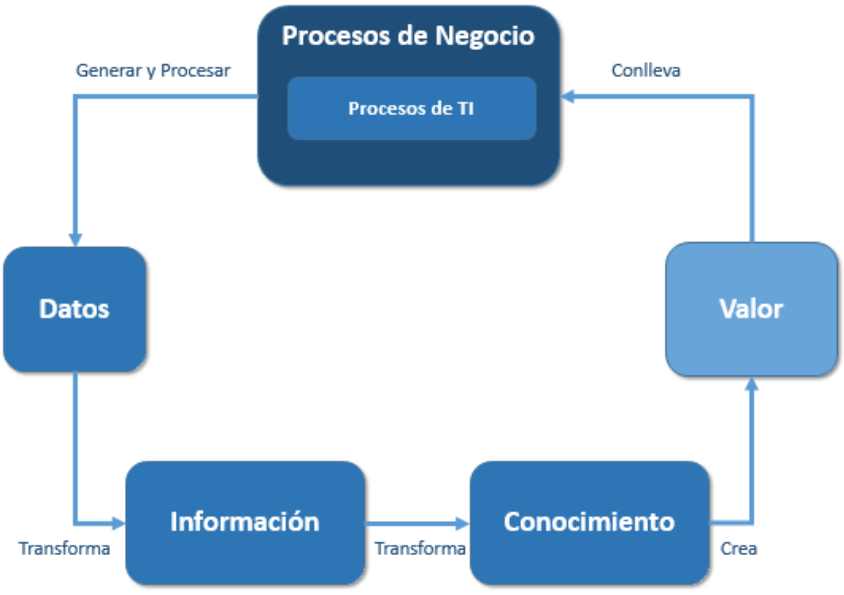

FIGURA 10: CIRCUITO DE LA INFORMACIÓN

Este circuito ayuda a la organización en sus tres pilares:

- En la optimización de recursos se debe tener un proceso con los recursos disponibles. Esta información ayuda a la organización a mantenerse actualizada de los recursos disponibles, en cómo ayudan y en los casos en los que no están siendo eficientes, cuales son lo que no están ayudando a crear valor.

  Cuando se detecta un recurso que no posee las condiciones necesarias o no aporta el beneficio que las organizaciones esperan, se debería proveer un mejoramiento, evaluando si se necesita de este recurso o se puede prescindir de él.

  Si se quiere optimizar recursos es necesario optimizar también los procesos, ya que se los utiliza para conseguir un fin determinado, lo que se traduce a más tiempo y por consecuencia más costos.
- En cuanto al riesgo la organización debe establecer procesos y procedimientos, para optimizar controles y función de monitoreo de los riesgos. Estos procesos pueden ser críticos si no se provee de información de calidad ya que de estos resultados la organización podría no optar por obtener un beneficio, si un proceso determinará un riesgo alto sobrepasando el umbral que la puede soportar.
- En todos los sistemas el simple hecho de tener un dato no implica la realización de beneficios. La organización debe contemplar cómo se invierten el tiempo y los recursos asignados. Si se quiere crear y mantener valor, los beneficios deben gestionarse a lo largo de todo el ciclo de vida.

Todos los procesos que las organizaciones poseen en sus circuitos contienen información. Los sistemas deben contemplar que no sólo sea válida, de calidad sino que además disminuya el riesgo que la misma le puede causar por sólo relevarla, o realizar cualquier tratamiento que se planee sobre ella.

CAPÍTULO III - Datos Personales y su protección

3.1 Introducción

Hay distintos datos de una persona que, relacionados, pueden crear perfiles o identificarla. Un número importante de organizaciones relevan estos tipos de datos o datos personales para sus sistemas de información, sin importar los derechos, la seguridad ni la privacidad que estos deben poseer. Este capítulo comienza con una breve descripción sobre los primeros derechos que obtuvieron las personas sobre sus datos; se describen definiciones sobre datos personales y sus clasificaciones, roles y responsabilidades que intervienen en un tratamiento y por último se menciona el riesgo que una organización puede llegar a tener por el tratamiento de los mismos si no se tiene en cuenta su seguridad.

3.2 Derechos ARCO

Los derechos ARCO surgen de la necesidad de que toda persona (física) tenga poder de control en relación con el uso de sus datos personales por parte de terceros; por lo tanto, regular los derechos al Acceso, Rectificación, Cancelación y Oposición. Se trata de derechos personalísimos, lo que significa que su titular puede hacer uso de los mismos ante la organización. El ejercicio de cualquiera de los derechos ARCO no es requisito previo, ni impide el ejercicio de otro; es por esto, que en cualquier momento el titular o su representante pueden solicitar a la organización, el acceso, rectificación, cancelación u oposición al tratamiento de los datos personales que le conciernen.

Los derechos ARCO, como se mencionó anteriormente, son cuatro principios:

- **Derecho de Acceso**: Todas las personas tienen derecho de acceder a su información personal que esté en posesión de la organización, a fin de conocer cuál es y la forma en que es utilizada.

FIGURA 11: DERECHO AL ACCESO

Además, se puede obtener la siguiente información:

- Copia de los datos personales que están siendo objeto del tratamiento
- Los fines del tratamiento
- La categoría de datos personales que están siendo tratados
- Los destinatarios o categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular los destinatarios en terceros países u organizaciones internacionales y, este caso, las garantías adecuadas en las que se realizan dichas transferencias
- El plazo previsto de conservación de los datos personales o en caso de no ser posible, los criterios para su determinación
- La existencia del derecho del interesado que solicita a la organización: la rectificación o supresión de sus datos personales, la limitación del tratamiento de sus datos personales u oponerse a ese tratamiento
- El derecho a presentar una reclamación ante una Autoridad de Control
- Cuando no hayan sido obtenidos directamente del interesado, la información disponible sobre su origen
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, y/o información significativa sobre la lógica aplicada, la importancia y las consecuencias previstas de ese tratamiento para el interesado

- **Derecho de Rectificación**: A través del derecho de rectificación es posible realizar la corrección de datos que sean inexactos, que cambiaron o permanezcan incompletos.

FIGURA 12: DERECHO A LA RECTIFICACIÓN

- **Derecho de Cancelación:** La cancelación se realiza cuando el titular considere que sus datos personales ya no se requieren, resulten inadecuados o excesivos, o cuando el tratamiento no se ajuste a las disposiciones legales.

FIGURA 13: DERECHO A LA CANCELACIÓN

- **Derecho de Oposición:** El titular podrá oponerse al tratamiento de sus datos para fines específicos, en caso de que hayan sido recabados sin su consentimiento, o cuando existan motivos fundados para ello, siempre que se ajuste a la Ley. Los datos serán bloqueados cuando la oposición resulte procedente, pero no eliminados.

FIGURA 14: DERECHO A LA OPOSICIÓN

3.3 Derechos ARCO en Argentina

En Argentina, en 1994 se realizó la reforma de la Constitución de la Nación Argentina1 donde se modificó esta carta magna e introdujo nuevos derechos e instituciones. Uno de los derechos nuevos que se otorgaron fueron los derechos ARCO.

Los derechos ARCO están contemplados amparados por la ley 25.3262 de Protección de Datos Personales. En el ARTÍCULO 16. — (Derecho de rectificación, actualización o supresión) — específica que: "El responsable o usuario del banco de datos, debe proceder a la rectificación, supresión o actualización de los datos personales del afectado, realizando las operaciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad."

También se menciona en el mismo artículo inciso 5 que:

"…*la supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros, o cuando existiera una obligación legal de conservar los datos*".

3.4 Los datos personales

En 1948, la Asamblea General de las Naciones Unidas publicó la "Declaración Universal de Derechos Humanos" lo que marcó un hecho histórico en lo que respecta a los derechos humanos. El artículo 12 de este documento establece lo siguiente:

"*Nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho*

[1] http://servicios.infoleg.gob.ar/infolegInternet/anexos/0-4999/804/norma.htm

[2] https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

a la protección de la ley contra tales injerencias o ataques". Declaración Universal de los Derechos Humanos, 1948.

De acuerdo con este artículo optamos por definir los datos personales como "toda información que nos identifica o nos puede hacer identificables".

Según la definición de la RAE un dato de carácter personal es: "*Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de otro tipo concerniente a personas físicas identificadas o identificables* (RAE, Dato de carácter personal, s.f.)", definiendo a persona identificable como "*Persona cuya identidad pueda determinarse directa o indirectamente mediante uno o varios elementos específicos característicos de su identidad física, fisiológica, psíquica, económica, cultural o social* (RAE, Persona Identificable, s.f.)".

De estas definiciones surgen distintos agrupamientos para clasificar los datos personales, por ejemplo:

- Datos de carácter identificativo: tipo y número de documento, dirección, imagen, voz, número de Seguridad Social/mutualidad, teléfono, marcas físicas, nombres y apellidos, firma, huella, firma electrónica.
- Datos relativos a las características personales: datos de estado civil, datos de familia, fecha de nacimiento, lugar de nacimiento, edad, sexo, nacionalidad, características físicas o antropométricas.
- Datos relativos a las circunstancias sociales: Características de alojamiento, vivienda, situación familiar, propiedades, posesiones, aficiones y estilos de vida, pertenencia a clubes y asociaciones, licencias, permisos y autorizaciones.
- Datos académicos y profesionales: Formación, titulaciones, historial del estudiante, experiencia profesional, pertenencia a colegios o asociaciones profesionales.
- Detalles laborales: Profesión, puestos de trabajo, justificativos médicos, sanciones, evaluaciones.
- Datos que aportan información comercial: Actividades y negocios, licencias comerciales, suscripciones a publicaciones o medios de comunicación, creaciones artísticas, literarias, científicas o técnicas.
- Datos económicos, financieros y de seguros: Ingresos, rentas, inversiones, bienes patrimoniales, créditos, préstamos, avales, datos bancarios, planes de pensiones, jubilación, datos económicos de nómina, datos deducciones impositivas/impuestos, seguros, hipotecas, subsidios, beneficios, historial de créditos, tarjetas de crédito.

- Datos relativos a transacciones de bienes y servicios: Bienes y servicios, transacciones financieras, compensaciones e indemnizaciones.

Estos datos reflejan la sensibilidad que poseen los mismos por su carácter personal. Las organizaciones deben tener en cuenta este agrupamiento y su sensibilidad a la hora de realizar el relevamiento y el tratamiento de estos datos, siempre teniendo en cuenta que el impacto no sólo es sobre la organización en sí, sino también sobre la persona titular de los datos, ante cualquier situación de inseguridad.

3.4.1 Datos Sensibles

Existe una clasificación que necesita más atención en las organizaciones, y es por su naturaleza en relación con los derechos y las libertades fundamentales. A estos datos se los conoce como *datos sensibles* y son datos que deben estar *especialmente protegidos*.

Según la RAE el dato sensible es un dato "*especialmente protegido* (RAE, Dato Sensible, s.f.)" y que por esta condición de dato que "*Por afectar a la raza, salud, vida sexual, ideología, afiliación sindical, religión o creencias de la persona, requiere para su tratamiento de un consentimiento reforzado de su titular, bien expreso o bien expreso y por escrito. Están legalmente protegidos los ficheros creados con la exclusiva finalidad de almacenar datos especialmente protegidos*" (RAE, Dato especialmente protegido, s.f.).

De la misma definición se desprende un agrupamiento de estos datos. Estos son:

1. **Datos genéticos**: Por datos genéticos se entienden los datos personales relacionados con características genéticas, heredadas o adquiridas, de una persona física, provenientes del análisis de una muestra biológica de la persona física en cuestión, en particular a través de un análisis cromosómico, un análisis del ácido desoxirribonucleico (ADN) o del ácido ribonucleico (ARN), o del análisis de cualquier otro elemento que permita obtener información equivalente.

2. **Biométricos**: Se consideran datos biométricos a los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos. Se reconocen dos tipos de datos biométricos, según si se refieren a características fisiológicas o de comportamiento.

    a. **Los identificadores fisiológicos** se relacionan con la composición de la persona e incluyen el reconocimiento facial, las huellas dactilares, la geometría de los dedos (el tamaño y la posición de los dedos), el reconocimiento del iris,

el reconocimiento de venas, el escaneo de retina, el reconocimiento de voz y la comparación de ADN.

b. **Los identificadores de comportamiento** incluyen las formas únicas en que actúan los individuos, incluido el reconocimiento de los patrones de escritura, la forma de caminar y otros gestos.

3. **Origen racial y étnico**: Este tipo de datos se refieren a la raza o etnia de las personas. La etnia es la creencia subjetiva en una procedencia común. Esa creencia puede basarse en semejanzas de aspecto exterior, costumbres, idioma, religión o memoria de eventos históricos como migraciones.

4. **Opiniones políticas y religiosas**: Son datos que reflejan las opiniones políticas convicciones religiosas, filosóficas o morales: Esto incluye todos aquellos datos referidos a la religión o creencia de una persona.

5. **Afiliación sindical**: Los datos sobre afiliación sindical son los que indican si una persona concreta está afiliada a un sindicato.

6. **Información referente a la salud**: Son datos personales relacionados con la salud física o mental de una persona física, incluida la prestación de servicios de atención médica, que revelan información sobre el estado de salud. Los datos de salud pueden referirse al estado pasado, actual o futuro de una persona. No solo cubre detalles específicos de condiciones médicas, pruebas o tratamientos, sino que incluye cualquier dato relacionado que revele algo sobre el estado de salud de una persona. Por tanto, los datos sanitarios pueden incluir una amplia gama de datos personales, por ejemplo:

a. Cualquier información sobre lesiones, enfermedades, discapacidades o riesgos de enfermedades, incluidos antecedentes médicos, opiniones médicas, diagnóstico y tratamiento clínico;

b. Datos de exámenes médicos, resultados de pruebas, datos de dispositivos médicos o datos de rastreadores de actividad física;

c. Información recopilada del individuo cuando se registra para los servicios de salud o accede al tratamiento; detalles de citas, recordatorios y facturas que le informan algo sobre la salud de la persona. Estos se incluyen en “la prestación de servicios de atención médica”, pero deben revelar algo sobre el estado de salud de una persona. Por ejemplo, una cita con el médico de cabecera o el hospital de forma aislada no le dirá nada sobre la salud de una persona, ya que puede ser una cita de control o evaluación. Sin embargo, podría inferir

razonablemente datos de salud de la lista de citas de una persona en una clínica de osteópata o de una factura por una serie de sesiones de fisioterapia.

7. **Orientación sexual**: Son los datos sobre la orientación sexual y el género.

8. **Penal**: Los datos personales sobre denuncias, procedimientos o condenas penales no son datos de categoría especial. Sin embargo, existen reglas y salvaguardas similares para procesar este tipo de datos, para hacer frente a los riesgos particulares asociados a ellos. Para procesar datos personales sobre condenas o delitos penales, debes tener una base legal y una autoridad legal o autoridad oficial para el procesamiento.

Se presume que estos tipos de datos deben tratarse con mayor cuidado en su recopilación. Para este tipo de datos las organizaciones deben de proveerse de un documento, firmado por el titular de los datos, a la hora de relevar o realizar el tratamiento de los mismos. Este documento se llama Consentimiento.

3.4.2 El consentimiento en los datos

Como se mostró anteriormente existen datos de naturaleza sensible a los que las organizaciones **deben proveer** un consentimiento. El objetivo es hacer que las personas sean participantes activos del proceso de decisión relativo al procesamiento de sus datos personales, excepto en los casos limitados por la legislación o la reglamentación.

Según la definición de la RAE el consentimiento es: "*Manifestación de voluntad, expresa o tácita, por la cual un sujeto se vincula jurídicamente* (RAE, Consentimiento, s.f.)", es decir, es la acción o efecto que tiene una persona de manifestarse, que puede ser expresa o tácita, sobre qué es lo que puede hacer la organización con respecto a sus datos; y además existe un vínculo Jurídico. Es decir que la organización asume responsabilidades y también reconoce derechos que la persona posee.

Este consentimiento, que la organización debe proveer, tiene que tener algunas características que sirva para que los titulares ejerzan derechos sobre sus datos. La construcción de este documento debe tener algunas características para que tenga validez:

- Otorgado libremente: Es decir que, el consentimiento tiene que ser prestado en un marco de libertad. La concesión del mismo no puede estar "condicionada a", por ejemplo, una rebaja en un servicio, consecución de un producto, o a cualquier otro tipo de condición.
- De manera consciente.

- Específico: Es decir que, cuando el tratamiento tenga varias finalidades, se recabe el consentimiento para cada uno de ellos.
- Informado: El consentimiento debe ser siempre informado, de manera que los textos legales informen al interesado de:
    - Finalidad del tratamiento para el que se quiere recabar el consentimiento
    - Información del responsable del tratamiento
    - Tratamiento de esos datos
    - Derechos del titular interesado
- Inequívoco. La información debe ser detallada de manera clara y sin ambigüedad. Es decir, la información debe presentarse por separado de otros aspectos.

Además en todo momento, el titular de los datos debe tener a su alcance el mecanismo para poder retirar el consentimiento otorgado previamente cuando lo desee.

3.4.2.1 Consentimiento en Menores y personas con discapacidad

A la hora de recabar los datos de menores, confeccionar perfiles u otras situaciones que impliquen la responsabilidad del tratamiento de datos personales de menores de edad, existen consideraciones que menciona la CONVENCIÓN SOBRE LOS DERECHOS DEL NIÑO y demás instrumentos internacionales que buscan su bienestar y protección integral.

Es importante que a la hora de trabajar con menores se tome conocimiento de la edad máxima que una persona se considera menor y cuál es dependiendo la legislación donde reside como menor de edad. En la construcción del consentimiento en este contexto, se identifican dos opciones:

1. Si la edad del menor es mayor a la que reconoce la legislación, el consentimiento del menor es suficiente si posee ciertos atributos, por ejemplo: debe estar adaptada a sus capacidades cognitivas.
2. Si la edad del menor está por debajo de lo que marca la legislación, la organización deberá obtener el consentimiento de los Padres y/o tutor, avalando que los datos son entregados según las características que se menciona anteriormente.

Las personas con discapacidad tienen menos capacidad para defender sus derechos. La organización debe proteger sus datos y, más aún, cuando una persona se encuentra en una situación de vulnerabilidad. En estos casos es el representante legal quien debe dar el

consentimiento. Otra especificación a tener en cuenta a la hora de elaborar un consentimiento, es que el mismo debe ser informado en lenguaje claro y estar claramente expresada: la finalidad, las consecuencias, los destinatarios y en caso que se almacenen en una base de datos, el nombre y los datos de contacto de la organización.

3.4.3 Roles y Responsabilidades de los datos personales

Con esta nueva información en las organizaciones surgen nuevas funciones y responsabilidades para asegurar que los datos sean relevados y tratados correctamente, pero además, que los titulares de los datos tengan la posibilidad de tener contacto con los responsables de que sus datos estén seguros.

3.4.3.1 Controladores de los datos

Los controladores son cualquier persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que, de manera individual o conjunta con otros, determina los propósitos y medios del procesamiento de datos personales. El controlador es quien asume la responsabilidad por todos los datos personales recopilados y debe garantizar que los derechos del titular de los datos y las obligaciones legales propias del controlador también estén cubiertos por el procesador. No sólo es el responsable del tratamiento de los datos personales sino también de su protección.

Esta figura es responsable de determinar los fines para los que se utilizan los datos personales y qué protección de privacidad debe implementarse, recopilarlos y determinar la base legal para hacerlo y por cuánto tiempo retener los datos.

El controlador de datos es el principal encargado de recabar los datos y entre sus responsabilidades se enumera:

- Responsabilidades que incluyen la obtención del consentimiento de la persona, clasificación de los datos, administración de consentimiento-revocación, autoridad del derecho de acceso, etc.
- Debe tener la capacidad para mostrar cumplimiento con los principios relacionados con el procesamiento de los datos personales. Estos principios son “legitimidad, justicia y transparencia, minimización de datos, exactitud, limitación de almacenamiento e integridad, además de confidencialidad de datos personales.”
- Implementar políticas adecuadas de protección de datos
- Llevar a cabo una evaluación de impacto de privacidad cuando sea necesario

- Implementare medidas técnicas y organizativas apropiadas para garantizar el procesamiento legal de datos personales
- Considerar la protección de datos por diseño y por defecto en las actividades de procesamiento.
- Implementar medidas técnicas y organizativas apropiadas para garantizar el procesamiento legal de datos personales
- Designar procesadores para diversas tareas.

3.4.3.2 Procesadores de los datos

El Procesador de datos es la persona física o jurídica, autoridad pública, agencia o cualquier otro organismo que procesa datos personales en nombre del controlador.

Los procesadores también deben implementar controles técnicos y organizacionales apropiados y cumplir con requisitos, por ejemplo:

- El procesamiento debe estar regido por un contrato u otras disposiciones legales que sean vinculantes para los procesadores.
- Adherirse a los códigos de conducta o mecanismos de certificación para demostrar el cumplimiento.
- No involucrar a otros procesadores sin autorización previa del controlador.
- Si el primer procesador designa a otros procesadores, se aplicarán las mismas obligaciones de protección de datos que se aplican al primer procesador.

3.4.3.3 Responsable de la Protección de los datos

Mientras no haya una normativa que lo exija, es una buena práctica que las organizaciones nombren a un responsable para la protección de datos. Su rol principal es asistir y asesorar al procesador con respecto al cumplimiento de las normativas vigentes y buenas prácticas recomendadas, y asegurarse de la aplicación de las mismas dentro de la organización.

Este responsable debe mantener un registro de todas las actividades de procesamiento que involucran datos personales, realizadas por la organización. Este registro debe incluir información explicativa sobre el propósito de las operaciones de procesamiento y debe ser accesible para cualquier persona. Sus actividades exigen un seguimiento periódico de los sujetos de datos y en gran escala, o cuando la información incluye datos sensibles.

Otras de las tareas son:

- La implementación y aplicación de las políticas de protección de datos.
- La asignación de responsabilidades, concienciación y formación del personal autorizado.
- La realización de la evaluación de impacto.
- Las auditorías realizadas.
- Gestionar la información de los interesados y las solicitudes presentadas en el ejercicio de sus derechos.
- Cooperar con la autoridad de control.

3.4.3.4 Autoridad de Control

Las autoridades de control son los organismos públicos e independientes que tienen como objetivo principal supervisar la aplicación de las regulaciones, para garantizar la protección de los derechos y libertades de las personas físicas.

Las autoridades de control tienen distintas responsabilidades, como por ejemplo:

- Supervisar e investigar la correcta aplicación de las regulaciones del país en donde se establece la organización;
- Asesorar al Gobierno y demás instituciones y organismos públicos sobre medidas legislativas y administrativas;
- Informar a los interesados sobre sus derechos;
- Tratar e informar de la investigación sobre reclamaciones presentadas por interesados y organismos;
- Evaluar cambios en tecnologías de la información y comunicación o prácticas comerciales con incidencia en protección de datos;
- Fomentar y gestionar todas las acciones encaminadas a establecer códigos de conducta y mecanismos de certificación;
- Registrar infracciones y medidas adoptadas.

Es importante que exista una autoridad de control principalmente para las organizaciones, ya que puede orientarlas, tanto en las regulaciones vigentes del país de procedencia como la de países terceros donde se quiere realizar transferencia de datos.

3.4.4 Transferencia y Cesión

En las últimas décadas, la transferencia y cesión de los datos personales se ha convertido en una cuestión sensible, sobre todo el modo en que determinados sujetos (las organizaciones) administran datos personales ajenos, un punto de alta relevancia si se tiene en cuenta la fuerza y rapidez de internet y las nuevas tecnologías como potenciadores de los eventuales daños que un incorrecto manejo de los mismos puede causar a los derechos e intereses legítimos de las personas titulares de esos datos.

El estado es quien garantiza un adecuado marco de protección de los datos, más aún en aquellas transferencias que tengan por destino países sin legislación calificable. A continuación, se nombran cada una de ellas.

3.4.4.1 Transferencia

Decimos que una transferencia internacional de datos se realiza cuando el responsable y/o encargado del tratamiento de los datos, envía información o bases de datos a un receptor, que a su vez es responsable del tratamiento y se encuentra fuera del país. Esto deja como resultado que los datos personales estén dispersos geográficamente. Uno de los requisitos que se debe contemplar es el “nivel adecuado” del país donde se va a transferir los datos. Es decir un nivel de protección de las libertades y derechos fundamentales equivalente del país origen al país receptor.

Cuando se realizan transferencias se debe tener en cuenta:

- Que el destinatario declarado posea nivel adecuado.
- Códigos de conducta, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.
- Mecanismos de certificación, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas las relativas a los derechos de las personas interesadas.
- Que la persona interesada haya dado explícitamente su consentimiento.
- Que la transferencia sea necesaria para la ejecución de un contrato entre la persona interesada y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona interesada.

- Que la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés de la persona interesada, entre quien es responsable del tratamiento y otra persona física o jurídica.
- Que la transferencia sea necesaria por razones importantes de interés público.
- Que la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones.
- Que la transferencia sea necesaria para proteger los intereses vitales de la persona interesada o de otras personas, cuando la persona interesada esté física o jurídicamente incapacitada para dar su consentimiento.

3.4.4.2 Cesión

Se puede definir a la cesión o comunicación de datos como “toda publicación de datos realizada a una persona distinta del titular o interesado”, este mecanismo implica no solo la recolección sino la entrega, comunicación, consulta, interconexión, transferencia, difusión o cualquier otra forma que facilite el acceso a los datos de un fichero a un tercero, distinto de la persona interesada Para poder realizar una cesión de datos se establecen dos requisitos iniciales que deben ejecutarse en toda cesión, con carácter general:

1. La cesión de datos debe cumplir los fines relacionados con las funciones de cedente y cesionario.
2. La organización debe tener el consentimiento informado del interesado.

Es una buena práctica realizar un contrato entre ambas partes con el siguiente contenido:

- Objeto de la prestación contratada.
- Mencionar que el acceso a los datos personales es necesario para el cumplimiento del objeto contractual.
- Obligaciones del encargado del tratamiento.

Los datos cedidos no pueden ser otros que los mencionados en el contrato. Al momento que se realice una transferencia o cesión se debe verificar el nivel de adecuación en el caso correspondiente, para proveer protección a los datos personales.

Cuando se habla de nivel de adecuación, tanto en la cesión como en la transferencia, se quiere reflejar que, el país donde se encuentran los datos, exige que el país destino

garantice, por su legislación interna o sus compromisos internacionales, un nivel de protección de las libertades y derechos fundamentales equivalente al que ya posee.

3.4.5 Seguridad de la información al tratar datos personales sensibles

El principio de seguridad de la información requiere que se analicen los datos personales teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información. Este principio es conocido como Triángulo CIA en donde los tres atributos que se aplican a la información de forma conjunta como lo muestra la figura. X.

FIGURA 15: TRIÁNGULO CIA

Toda la información que circule por la organización tiene que tener en cuenta los atributos antes mencionados y su relación con esta de la siguiente manera:

- **Confidencialidad**: está relacionada en cómo mantener la información y los sistemas seguros frente a los accesos no autorizados.
- **Integridad**: implica que la información esté protegida contra todo cambio no autorizado y accidental.
- **Disponibilidad**: asegura que la información esté accesible siempre que sea requerido.

Estas características se apoyan en procesos y prácticas que las organizaciones deben tener, que van desde encriptación de datos, tokenización y prácticas de gestión de claves, pero lo más importante son la implementación de políticas de seguridad robustas que abarquen todo el ciclo de vida de los datos.

Las políticas de seguridad o conjunto de reglas definen define qué es lo que desea proteger, proporcionar una base para la planificación de la seguridad, describir cómo se va a supervisar la efectividad de las medidas de seguridad y además deben contemplar:

- Asignación de responsabilidades relacionadas a la seguridad de la información.
- Segregación de tareas.
- Seguridad de la información en la gestión de proyectos.
- Control de acceso.
- Creación e implementación de políticas sobre el uso de controles de cifrado.
- Seguridad física y ambiental.
- Seguridad de las operaciones.
- Gestión de incidentes de seguridad de la información.

Todas las políticas que puedan crear las organizaciones siempre deben tener como objetivo la protección de los datos de las personas y que los recursos sean suficientes para brindar tal protección.

3.4.6 Riesgos en los datos personales

Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo. Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, con identificar los riesgos y siempre implica considerar la amenaza que los puede originar. En el caso de los datos personales se debe tener en cuenta los riesgos de privacidad y el impacto en la protección de los datos personales que puede generar un procesamiento.

Partiendo de la definición mencionada, la organización puede enfrentar varios riesgos, que influyen en los derechos y libertades de las personas físicas y es sobre estos en donde debe hacer un foco mayor. Estos mismos se pueden diferenciar en 2 dimensiones:

- **Riesgos asociados a la protección de la información** con foco en la integridad, disponibilidad y confidencialidad de los datos. Por ejemplo, acceso ilegítimo a los datos o pérdida de datos.
- **Riesgos asociados al cumplimiento de los requisitos regulatorios** relacionados con los derechos y libertades de los interesados. Por ejemplo, uso ilegítimo de datos personales.

Combinando dichas dimensiones y una evaluación de impacto sobre la privacidad, se obtiene como resultado una amplia identificación de los riesgos, lo cual permite a la organización posteriormente tomar las decisiones adecuadas para la protección de los datos.

Los criterios que a continuación se listan, son un indicativo de que la organización necesita realizar una evaluación de impacto:

- Datos sensibles o datos muy personales.
- Elaboración de perfiles y la predicción;
- Toma de decisiones automatizada con efecto jurídico significativo o similar;
- Observación sistemática;
- Tratamiento de datos a gran escala;
- Asociación o combinación de conjuntos de datos;
- Datos relativos a interesados vulnerables;
- Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas.

Una vez realizado un análisis de riesgo, la organización deberá evaluar los resultados de la misma y considerar los tratamientos necesarios en el caso de los riesgos altos. Este análisis además le brindará a la organización el nivel de riesgo que puede mitigar o aceptar en los casos de los riesgos bajos.

Es una buena práctica realizar una evaluación de impacto y así, la organización puede encontrar donde su seguridad es más vulnerable y realizar las políticas que se sugieran necesarias para mitigar los riesgos, asegurando a las personas el derecho a su privacidad y la protección de sus datos.

3.4.7 Política de privacidad

Es habitual encontrar situaciones donde se manifiesta la dificultad para que las personas u organizaciones conozcan o comprendan las potenciales amenazas de la exposición de los datos personales y sus consecuencias e impacto en la privacidad en su interacción con sistemas, productos o servicios.

La política de privacidad es un documento legal que tiene por objetivo poner en conocimiento de los titulares respecto a cuáles de los datos personales se está recabando, los tratamientos específicos de sus datos, las finalidades de los tratamientos, los datos de contacto para ejercer los derechos que le asisten, los plazos de conservación de la información y las medidas de seguridad entre otras cosas.

La adopción y difusión de una política de privacidad es un mecanismo efectivo para alertar, concientizar y poner en valor la privacidad y los riesgos de una protección inadecuada.

Cada política debe contemplar los objetivos de la organización, sus valores y su cultura. Debe equilibrar la necesidad del procesamiento de la información con el respeto por la privacidad de los individuos.

No hay una política general para todas las organizaciones. Si bien seguramente se abordarán puntos comunes, la definición de una política debe estar orientada fuertemente al contexto organizacional, sus misiones y funciones.

Existen marcos referenciales reconocidos, como el proporcionado por el NIST Privacy Framework, para que cada organización defina su propia política. Este tipo de herramientas alinean las políticas al negocio y las tendencias o prácticas tecnológicas. Facilitan la gestión de los riesgos mediante diferentes líneas de acción:

- Considerando la privacidad en los sistemas, productos y servicios que provee o utiliza la organización;
- Difundiendo sus prácticas orientadas a la protección de datos;
- Estableciendo un equipo integrado entre autoridades, área legal y de tecnología, para la definición de perfiles, establecer metas y lograr resultados.

Mediante un marco de privacidad se logra un lenguaje común para el entendimiento, la administración y la comunicación acerca de los riesgos de la privacidad tanto para todo el personal o tercero que interactúe con la organización. Se pueden identificar y priorizar acciones para la minimización del riesgo.

Sin llegar a la adopción de este tipo de marcos, la definición, adopción y difusión de una política de privacidad de la organización es fundamental para cualquier entidad que se plantee llevar a cabo y mantener la protección adecuada de los datos.

3.4.7.1 Pautas para la elaboración de una política de privacidad en una página web

Una política de privacidad (Proteccion, 2021) debe estar redactada en un lenguaje comprensible para cualquier persona que va a interactuar con la organización, explicando el propósito y tratamiento de los datos que solicite y administre. En su elaboración debe considerarse la normativa propia de ese país, la interacción con otras organizaciones o sucursales que estén en el extranjero, la adopción de estándares o marcos referenciales.

A continuación, se indican un conjunto de pautas para su elaboración:

- Indicar qué datos personales se recopilan, por qué se los solicita y cómo se van a procesar.
- Los datos serán recolectados en base al consentimiento otorgado libremente, específico, informado e inequívoco.
- Incluir frases que expliquen claramente acciones o restricciones sobre el tratamiento, por ejemplo:
    - No se solicitará información personal a menos que realmente sea necesaria para prestar los servicios que se ofrecen.
    - No se compartirá esa información con nadie, excepto para cumplir con la ley o si tengo la autorización del titular para hacerlo.
    - No se utilizarán los datos personales con una finalidad diferente a la expresada en esta política de privacidad.
    - Promover la lectura de la política antes de aceptarla
- Proponer la visita periódica de la política ante la posibilidad de cambios por nueva normativa o modificación de la existente.
- Asegurar que para el tratamiento de datos se implementen todas las medidas técnicas y organizativas de seguridad establecidas en la legislación vigente. Indicar normativa a cumplir o estándares, marcos o buenas prácticas adoptadas.
- Indicar información acerca del responsable del tratamiento de los datos personales: apellido y nombre, datos de contacto.
- Enunciar qué principios se aplicarán a los datos personales, por ejemplo:

- Licitud, lealtad y transparencia: siempre se requerirá consentimiento para el tratamiento de los datos personales para uno o varios fines específicos que se informarán previamente en forma transparente.
- Minimización de datos: sólo se solicitarán los datos estrictamente necesarios en relación con los fines para los que los que se requieren.
- Limitación del plazo de conservación: los datos serán mantenidos sólo el tiempo necesario para los fines del tratamiento. Se informará el plazo de conservación correspondiente. Transcurrido ese plazo, se eliminarán los datos. Si fuera necesario extender ese tiempo, se informará al titular y se solicitará nuevamente su consentimiento y opción. En el caso de suscripciones, periódicamente se revisarán las listas y se eliminarán los registros inactivos durante un tiempo considerable.
- Integridad y confidencialidad: los datos serán tratados de manera tal de garantizar su integridad y confidencialidad (sólo accesibles para personal autorizado).

- Enunciar los derechos que los titulares pueden ejercer sobre sus datos, por ejemplo:
  - Solicitar el acceso a sus datos personales
  - Solicitar su rectificación o supresión
  - Solicitar la limitación de su tratamiento
  - Oponerse al tratamiento
  - Solicitar la portabilidad de los datos.

3.4.7.2 Interacción con menores

- Indicar cómo se procede en caso de menores (según la normativa a cumplir) en cuanto al consentimiento de los padres o tutores para el tratamiento de sus datos personales.
- Aclarar acerca de que en ningún caso se recabarán datos relativos a la situación profesional, económica o a la intimidad de los otros miembros de la familia, sin el consentimiento de éstos.
- Avisar que si la persona es menor (según la normativa a cumplir) y ha accedido a ese sitio web sin avisar a tus padres no debe registrarse como usuario.

3.4.7.3 Otros párrafos aclaratorios

La política de privacidad puede incluir frases que ayuden a comprender el alcance del tratamiento de los datos.

A continuación se enuncian algunas.

- La organización no vende, alquila ni cede datos de carácter personal que puedan identificar al usuario, ni lo hará en el futuro, a terceros sin el consentimiento previo. Sin embargo, en algunos casos se pueden realizar colaboraciones con otras organizaciones. En esos casos, se requerirá consentimiento a los usuarios informando sobre la identidad del colaborador y la finalidad de la colaboración. Las organizaciones participantes cumplirán con las mismas pautas enunciadas en esta política.
- Los datos personales proporcionados se conservarán hasta que no se solicite su supresión por el interesado o la finalidad por la cual fueron recolectados haya llegado a su fin.
- Para prestar servicios estrictamente necesarios para el desarrollo de la actividad, la organización, comparte datos con los siguientes prestadores bajo sus correspondientes condiciones de privacidad. Por ejemplo, Google Analytics, Forms y otros.
- Al navegar por la web de la organización se pueden recolectar datos no identificables, que pueden incluir, direcciones IP, ubicación geográfica (aproximada), un registro de cómo se utilizan los servicios y sitios, y otros datos que no pueden ser utilizados para identificar al usuario. Entre los datos no identificativos están también los relacionados a los hábitos de navegación a través de servicios de terceros.
- Indicar si la web incluye un certificado SSL que permite que los datos viajen de manera íntegra y segura, es decir, la transmisión de los datos entre un servidor y usuario web, y en retroalimentación, es totalmente cifrada o encriptada.
- La organización no puede garantizar ser atacado por la red Internet y sufrir la violación de los datos mediante accesos fraudulentos a ellos por parte de terceros.
- La organización se asegurará de que cualquier persona que esté autorizada para procesar datos personales estará bajo la obligación apropiada de confidencialidad (ya sea un deber contractual o legal).
- Cuando se presente algún incidente de seguridad, la organización notificará al titular del dato sin demoras indebidas y deberá proporcionar información oportuna

relacionada con el Incidente de seguridad tal como se conozca o cuando el titular lo solicite.

- Sobre revocabilidad: el consentimiento prestado, tanto para el tratamiento como para la cesión de los datos de los interesados, es revocable en cualquier momento informando a la organización en los términos establecidos en esta política para el ejercicio de los derechos ARCO. Esta revocación en ningún caso tendrá carácter retroactivo.
- La organización se reserva el derecho a modificar la presente política para adaptarla a novedades legislativas o jurisprudenciales, así como a prácticas de la industria. Ante esta situación, se anunciarán en la página los cambios introducidos con razonable antelación a su puesta en práctica.

Además debe tener identificado los siguientes campos:

- Datos personales: Enunciar los datos personales que serán relevados.
- Datos personales sensibles: Enunciar de forma diferente si serán relevados datos sensibles.
- Derechos ARCO: Enunciar los derechos con los que cuenta el titular en relación a sus datos personales.
- Encargado: Enunciar los datos de la persona física que trate datos personales por cuenta del responsable.
- Ley: Enunciar la ley sobre los datos personales que rige donde se relevan los datos.
- Responsable: Enunciar los datos de quien decide sobre el tratamiento de datos personales.
- Tratamiento: Enunciar para que se realiza el relevamiento y qué acciones abarca.

3.4.7.4 Cookies

A la hora de implementar una política de privacidad se debe tener en cuenta las cookies. Las cookies se guardan en la computadora de forma local y muestran al propietario de las páginas, información sobre los hábitos de consumo de los usuarios como por ejemplo: que consultan en internet, qué páginas visitan, en cuáles navegan en primer o en segundo orden, en qué momentos del día y cuántas veces, entre otros datos.

Se debe identificar de manera clara cuáles son los datos que serán almacenados. De la misma manera deberá informarse los tipos de cookies y el uso que se le dará. Además la opción de que el usuario acepte el guardado de las mismas o cambie las preferencias y configurarlas según su uso.

3.4.7.5 Políticas de privacidad o Términos y Condiciones

Debe estar claramente diferenciadas las políticas de privacidad de los términos y condiciones. Las primeras, como se mencionó anteriormente, se refieren al tratamiento de los datos de los usuarios que tienen algún tipo de interacción con el sitio: cómo se recopilan, cómo se van a almacenar, para qué se van a usar y si se van a compartir. En cambio, los términos y condiciones se refieren al acuerdo básico entre el usuario del sitio web y la empresa en un ámbito global. Si es una tienda online, por ejemplo, se establecen los costos de envío, el tiempo de entrega de los productos, las tarifas y los impuestos, la prohibición del uso de imágenes del sitio, entre otros.

La política de privacidad debe estar visible o accesible cuando se vayan a recoger datos personales de los titulares. Debe estar separado el aviso legal (términos y condiciones) de la política de privacidad, es decir, presentarlos en dos textos diferentes en secciones separadas.

3.4.8 El derecho a la privacidad y la importancia de la protección de datos personales

Mediante los datos se individualiza a la persona. Nuestra existencia está registrada desde el nacimiento hasta la muerte, e incluso después de ella. Todos los datos que surgen de la vida cultural, social, profesional, laboral, económica, financiera, etc. se insertan dentro del mundo jurídico (BIANCHI, págs. 866, Tº 161) y son objeto de su pertinente tratamiento. Esta íntima e imprescindible relación entre los datos personales y la identidad de la persona, acredita su vital relevancia, como así también su obtención, conservación, almacenamiento, adaptación o modificación, extracción, consulta, cotejo o interconexión, limitación, evaluación, bloqueo, supresión, destrucción, difusión, y cesión a terceros.

Estas operaciones y procedimientos -denominado tratamiento de datos personales- no constituyen de ninguna manera un fenómeno reciente, pues la tenencia de información desde tiempos remotos permitió la generación de un poder que durante siglos fue canalizado con fines políticos, militares o económicos. Pero actualmente vivimos en un mundo gobernado, dirigido, influenciado y manipulado por quienes obtienen, almacenan, transmiten y comercializan información.

El progresivo desarrollo de las técnicas de recolección, almacenamiento y procesamiento de información y el desplazamiento de los registros manuales o mecánicos por las bases y bancos de datos, que trajo aparejada la aparición y avance de la informática, ha otorgado a los "datos personales" un rol notorio. A la rapidez en el acopio de la información, su capacidad inagotable y la diversificación de contenidos, se le suman la simultaneidad de su transmisión, sin restricciones de distancia, la perdurabilidad de los registros y la posibilidad de su alteración o su extinción, o bien de procesarla, vincularla y obtener de ello un nuevo producto.

La protección de datos personales cumple dos funciones: por un lado, regula la capacidad que tienen las personas para conocer, editar, gestionar o eliminar datos sobre ellas mismas y por el otro, mediante un conjunto de reglas específicas y principios generales, establece límites para el uso de datos por parte de entidades públicas y privadas (Argentina, s.f.).

La intercepción de telecomunicaciones, el monitoreo desproporcionado de los espacios públicos a través de sistemas de video vigilancia, la recolección o publicación de datos personales sin el consentimiento de sus titulares, así como el tratamiento automatizado de información mediante algoritmos o inteligencia artificial representan algunas situaciones problemáticas de las que se ocupa activamente esta rama del derecho.

CAPÍTULO IV - Regulaciones Sobre Datos Personales

4.1 Introducción

Una gran cantidad de datos personales son generados, almacenados, procesados y transferidos día a día, dejándolos expuestos a sufrir diferentes ataques informáticos si no son protegidos adecuadamente. Esto ha llevado a que varios países generen normativas, leyes, regulaciones y marcos que establezcan medidas para el manejo apropiado de los datos (sobre todo de aquellos definidos como datos personales) contenidos en los sistemas de información. En este capítulo se detalla los puntos más importantes que tomamos de leyes, normativas y marcos nacionales e internacionales sobre los cuales nos basamos para el desarrollo de la guía y su fundamentación.

4.2 Legislación en Argentina

La legislación argentina tiene como objetivo la protección integral de los datos personales a fin de garantizar el ejercicio pleno de los derechos de sus titulares. Posee fuertes estándares de privacidad, arraigados en la Constitución, y en legislaciones sobre protección de datos que se comparan a las de Europa. La ley N° 25326 (regulación de la protección de datos personales) sigue estándares internacionales, y se aplica al procesamiento por órganos públicos y privados.

La normativa nacional básica sobre tema de datos personales se compone de:

- Constitución Nacional. Artículo Nº 43.
- Leyes
    - Ley Nº 25.326. Ley de Protección de los Datos Personales.
    - Ley Nº 26.343. Incorporación del art. 47 a la Ley 25.326 de Protección de los Datos Personales.
    - Ley Nº 26.388. Reforma del Código Penal en materia de Delitos Informáticos. Deroga y modifica algunos incisos introducidos por el art. 32 de la Ley 25.326 al Código Penal.
- Decretos
    - Decreto Nº 995/2000. Veto y promulgación de la Ley Nº 25.326.
    - Decreto Nº 1.558/2001. Reglamentación de la Ley Nº 25.326. Principios generales relativos a la protección de datos. Derechos de los titulares de los

datos. Usuarios y responsables de archivos, registros y bancos de datos. Control. Sanciones.

- Resoluciones
    - Resolución Nº 98/2002. Modificación de la Resolución Nº 17/2002.

Además, cuenta con documentos relacionados con la legislación como los de la Unión Europea.

- Unión Europea. Dictamen 4/2002 del Grupo de Trabajo del Art. 29. Dictamen sobre el nivel de protección de datos personales en Argentina.
- Comisión de las Comunidades Europeas. Decisión C (2003) 1731. Decisión sobre la adecuación de la protección de los datos personales en Argentina.
- MERCOSUR/CMC/DEC. Nº 19/05. Norma relativa a los procedimientos y seguridad en el intercambio y consulta de datos obrantes en los sistemas informáticos aduaneros.

Documentos relacionados a los códigos éticos y de conducta en materia de protección de datos personales:

- Código de Ética de la AMDIA. Asociación de Marketing Directo e Interactivo de Argentina. Homologado por la Dirección Nacional de Protección de Datos Personales.
- Código de Conducta de la CEIC. Cámara de Empresas de Información Comercial.

Todas estas leyes, decretos y resoluciones fueron las bases para que los datos personales sean protegidos y seguros. Además asegura que las personas pueden ejercer los derechos que las mismas proveen sobre sus datos.

4.2.1 Ley de protección de la información personal en Argentina

La protección de los datos personales se encuentra explícitamente garantizada en nuestro país a través de la acción de hábeas data prevista en el artículo 43, tercer párrafo, de la Constitución Nacional (Argentina, Constitución Nacional, 1994), acción que fue incorporada en oportunidad de la reforma constitucional del año 1994, donde menciona que:

"*Toda persona podrá interponer esta acción para tomar conocimiento de los datos a ella referidos y de su finalidad, que consten en registros o bancos de datos públicos, o los privados destinados a proveer informes, y en caso de falsedad o discriminación, para exigir*

la supresión, rectificación, confidencialidad o actualización de aquéllos. No podrá afectarse el secreto de las fuentes de información periodística (Argentina, 1994)".

Posteriormente, se sancionó la Ley Nº 25.326 de Protección de Datos Personales (Argentina, 2000), norma de orden público que regula los principios aplicables en la materia, y el procedimiento de la acción de habeas data. La mencionada ley fue sancionada en octubre del 2000 y entró en vigencia al año siguiente.

Cabe destacar que se designa a la Agencia de Acceso a la Información Pública (AAIP), conforme los términos del artículo 19 de la Ley Nº 27.275, sustituido por el artículo 11 del Decreto Nº 746/17, como la autoridad de control de la ley de protección de datos personales, siendo la AAIP un ente autárquico con autonomía funcional en el ámbito de la Jefatura de Gabinete de Ministros.

4.2.2 Derechos que la ley reconoce sobre los datos personales

Según el artículo 1 de la ley N°. 25.326 tiene por objeto:

… *"la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre, de conformidad a lo establecido en el artículo 43, párrafo tercero de la Constitución Nacional."*

En el capítulo II detalla cuales son los principios generales relativos a la protección de datos que se tienen en cuenta, como son, por ejemplo:

i. Calidad de los datos

En el artículo 4 se menciona que atributos deben tener los datos. Los mismos deben ser ciertos, adecuados, pertinentes, además deben ser exactos y actualizarse en el caso de que fuera necesario. Cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados deben ser destruidos.

ii. Consentimiento

El titular tiene que prestar su consentimiento de manera libre, expresa e informada. Caso contrario el tratamiento de datos personales será considerado ilícito. Además, se menciona cuando no es necesario el mismo:

a) Los datos se obtengan de fuentes de acceso público irrestricto;

b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal;

c) Se trate de listados cuyos datos se limiten a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio;

d) Deriven de una relación contractual, científica o profesional del titular de los datos, y resulten necesarios para su desarrollo o cumplimiento;

e) Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526.

iii. Derecho de los titulares

En el capítulo 3 de la ley se detalla cuáles son los derechos que tienen los titulares. Estos derechos pueden ser ejercidos en cualquier momento. Algunos de ellos:

1. Derecho de Información (Artículo 13): Toda persona puede solicitar información al organismo de control y la identidad de sus responsables.
2. Derecho de acceso (Artículo 14): Este artículo menciona que el titular de los datos tiene derecho a solicitar y obtener información de sus datos personales incluidos en los bancos de datos públicos, o privados destinados a proveer informes.
3. Contenido de la información (Artículo 15): Este artículo está orientado a cómo debe ser suministrada la información según la opción de titular, si la misma es por escrito, por medios electrónicos, telefónicos, de imagen; y también de qué forma, si es clara, exenta de codificaciones y en su caso acompañada de una explicación.
4. Derecho de rectificación, actualización o supresión (Artículo 16): En este artículo se mencionan los derechos que tienen los titulares a que sus datos sean rectificados, actualizados y, cuando corresponda, suprimidos o sometidos a confidencialidad. Además, menciona que el responsable o usuario del banco de datos, debe proceder a realizar las acciones necesarias a tal fin en el plazo máximo de cinco días hábiles de recibido el reclamo del titular de los datos o advertido el error o falsedad.
5. Excepciones (Artículo 17): Este artículo menciona cuales son los casos o excepciones en el cual los responsables pueden denegar el acceso, rectificación o la supresión en función de la protección de la defensa de la Nación, del orden y la seguridad públicos, o de la protección de los derechos e intereses de terceros.

6. Gratuidad (Artículo 19): En el mismo se menciona que se debe proveer el mecanismo para que el titular pueda ejercer sus derechos sin cargo alguno para el interesado.

iv. Usuarios y responsables de archivos, registros y bancos de datos.

En el capítulo 4 se hace mención y se detalla sobre los usuarios y responsables de archivos, registros y bancos de datos.

1. Control

En el capítulo 5 En este apartado se hace mención de la necesidad de un Organismo de control y de las tareas que este debe llevar a cabo para el cumplimiento de los derechos de los titulares. Este órgano de control gozará de autonomía funcional y actuará como órgano descentralizado en el ámbito del Ministerio de Justicia y Derechos Humanos de la Nación. Será dirigido y administrado por un director designado por el término de 4 (cuatro) años, por el Poder Ejecutivo con acuerdo del Senado de la Nación, debiendo ser seleccionado entre personas con antecedentes en la materia.

2. Sanciones

En los artículos del Capítulo 6 se habla sobre las sanciones que la ley prevé en el caso del incumplimiento de algunos de los artículos mencionados anteriormente. Estas sanciones que el organismo de control aplica pueden ser de apercibimiento, suspensión, multa clausura o cancelación del archivo, registro o banco de datos. Además de sanciones penales en los casos en el que se inserte o hiciere insertar datos falsos en un archivo de datos personales.

3. Acción de protección de los datos personales

En el capítulo VII habla sobre la acción de protección de los datos personales, teniendo en cuenta la procedencia, legitimación activa, legitimación pasiva.

4.3 Reglamento general de protección de datos

El Reglamento General de Protección de Datos (GDPR) (gdpr, 2016), por sus siglas en inglés (General Data Protection Regulation), o RGPD por sus siglas en español (Reglamento General de Protección de Datos) es un reglamento por el que el Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea refuerzan y unifican la protección de datos para todos los individuos dentro de la Unión Europea (UE). También se ocupa de la exportación de datos personales fuera de la UE.

GDPR, es la normativa que regula la protección de los datos de los ciudadanos que viven en la Unión Europea. Entró en vigor en 2016 después de aprobar el Parlamento Europeo, y a partir del 25 de mayo de 2018, todas las organizaciones debían cumplirlo. Aunque fue redactado y aprobado por la Unión Europea (UE), impone obligaciones a las organizaciones en cualquier lugar, siempre y cuando apunten o recopilen datos relacionados con personas en la UE.

El objetivo principal del GDPR es dar control a los ciudadanos y residentes sobre sus datos personales y simplificar el entorno regulador de los negocios internacionales unificando la regulación dentro de la UE. El GDPR sustituye a la Directiva de protección de datos (oficialmente Directiva 95/46 / CE) de 1995. El Reglamento fue adoptado el 27 de abril de 2016. Se convierte en ejecutivo a partir del 25 de mayo de 2018 tras una transición de dos años y, a diferencia de una directiva, no obliga a los gobiernos nacionales a aprobar ninguna legislación habilitante, por lo que es directamente vinculante y aplicable.

El derecho a la privacidad forma parte de la Convención Europea de Derechos Humanos de 1950 (Europeo, 2010), que establece en el artículo 8 que "toda persona tiene derecho al respeto de su vida privada y familiar, su hogar y su correspondencia". Sobre esta base, la UE ha tratado de garantizar la protección de este derecho mediante legislación.

A medida que la tecnología progresó y surgió Internet, la UE reconoció la necesidad de protecciones modernas. Es así que, en 1995, aprobó la Directiva Europea de Protección de Datos, estableciendo estándares mínimos de privacidad y seguridad de datos, sobre los cuales cada estado miembro basó su propia ley de implementación.

4.3.1 Aplicación del GDPR

La aplicación hace referencia sobre a quién protege dicho reglamento, sus derechos y obligaciones. Es alcanzado por el GDPR cualquier persona que resida en la UE o trabaja con una organización que posee empleados o clientes en la UE. Aplica además a organizaciones con presencia física en al menos algún país miembro de la UE, que procesan o almacenan datos sobre individuos o que utilizan servicios de terceros que procesan o almacenan información sobre individuos que residen en la Unión Europea.

En cuanto a la aplicación territorial, el GDPR aplica a las operaciones realizadas sobre datos personales de ciudadanos residentes en la UE (interesados) efectuadas por un Responsable (RT) o un Encargado (ET) del tratamiento, ya sea que esté establecido en la UE, independientemente de que el tratamiento tenga lugar o no en la UE, o no esté

establecido pero es de aplicación la legislación de un Estado de la UE u otra condición es que las actividades del tratamiento estén relacionadas con:

- La oferta de bienes o servicios a personas residentes en la UE, se pague o no por ello.
- El control de la conducta de las personas, si tiene lugar en la UE.

4.3.2 Principios de protección de datos

Los principios se centran en la protección de los datos en el caso que los mismos sean tratados o procesados. Para que este tratamiento cumpla el GDPR, se debe realizar de acuerdo a los 7 (siete) principios de protección y responsabilidad descritos en el Artículo 5.1-2:

1. Legalidad, equidad y transparencia: el procesamiento debe ser legal, justo y transparente para el interesado.

   En donde el concepto de legalidad establece que todos los procesos que estén de alguna manera relacionados con datos personales deben cumplir los requisitos descritos en el GDPR. Esto incluye la recopilación, el almacenamiento y el procesamiento de datos. La legislación tiene instrucciones y normas para cada paso de su política de gestión de datos.

   La equidad significa que las acciones de marketing, ya sean realizadas por un controlador de datos o un procesador de datos, deben coincidir con la información que recibió el sujeto de los datos. Con el fin de que los datos personales sólo se utilicen para los fines establecidos en la base legal y sólo durante el período de tiempo que se indicó.

   El titular de los datos debe estar informado respecto a los propósitos, el uso y el período de tiempo durante el que se procesarán sus datos, es de lo que trata el concepto de transparencia.

2. Limitación del propósito: Los datos se pueden recopilar y usar sólo para aquellos fines que se han transmitido al interesado y sobre los cuales se recibió el consentimiento.
3. Minimización de datos: recopilar y procesar solo la cantidad de datos que sea absolutamente necesaria para los fines especificados. Así mismo justificar la cantidad de datos recopilados, por lo que el diseño de una política adecuada y la documentación es un punto importante.

4. Precisión o Exactitud: Los datos personales deben ser "precisos y, en caso necesario, mantenerse actualizados". De igual modo, no retener los contactos antiguos y desactualizados y garantizar el borrado de los datos personales inexactos sin demora.
5. Limitación de almacenamiento: solo almacenar datos de identificación personal durante el tiempo que sea necesario para el propósito especificado. Este principio se refiere a la ‘minimización de datos’ y establece que los datos personales deben "mantenerse en una forma que permita la identificación de los interesados por un período no superior al necesario". Por esta razón, hay que establecer cuál es el período de retención para los datos personales que se recopila y justificar que este período es necesario para los objetivos específicos.
6. Integridad y confidencialidad: El principio de integridad y confidencialidad requiere que los datos personales se manejen de una manera (que asegure) la apropiada seguridad de los datos, que incluyen “la protección contra el procesamiento ilegal o pérdida accidental, destrucción o daño". Para ello, implementar sistemas eficientes de anonimización o pseudónimo para proteger la identidad del titular
7. Responsabilidad: el controlador de datos es responsable de poder demostrar el cumplimiento de GDPR con todos los principios anteriormente mencionados. Cada paso de la administración de datos debe ser cuidadosamente formulado y justificado en el formulario oficial del documento. Todo se debe demostrar con los documentos que prueban el cumplimiento con el GDPR cuando lo soliciten las autoridades.

4.3.3 Derechos que establece el GDPR

El GDPR (gdpr, s.f.) otorga a los individuos el control sobre cómo las organizaciones pueden utilizar información que está directamente vinculada con ellos y les proporciona 8 (ocho) derechos específicos. Algunos de estos derechos fueron incorporados con la nueva Ley, y otros son versiones más rígidas de otros ya existentes con la Directiva de Protección de Datos. Estos derechos de GDPR adquieren el nombre de “Derechos de Sujetos de Datos”. Los derechos adquiridos son:

- Derecho a estar informado: Proporciona transparencia sobre cómo son utilizados sus datos personales.
- Derecho al acceso. Provee acceso a los datos del titular, cómo son utilizados, y a cualquier información suplementaria que pueda ser utilizada juntos con sus datos.
- Derecho a la rectificación: Otorga el derecho a que los datos personales sean rectificados en caso de ser incorrectos o incompletos.

- Derecho a ser borrado (o derecho a ser olvidado o derecho de supresión): Es el derecho a que los datos personales sean removidos de cualquier lugar si no existe una razón convincente para que estén almacenados.
- Derecho a limitación del procesamiento. Permite que los datos sean almacenados, pero no procesados. Por ejemplo, se puede recurrir a este derecho si el titular cree que sus datos almacenados son erróneos y está a la espera de que sean rectificados.
- Derecho a la portabilidad de datos: El titular puede solicitar copias de la información almacenada sobre sí mismo, para utilizar en cualquier otro lugar. Tal es el caso de si necesita esa información para otras organizaciones.
- Derecho a oposición: Otorga el derecho a objetar acerca del procesamiento de los datos. Un ejemplo podría ser la objeción de que sean utilizados por organizaciones de marketing directo.
- Derecho sobre la toma de decisiones y creación de perfiles automáticos: Permite objetar sobre la toma de decisiones automáticas que se hagan sobre los datos personales. “Automáticos” se refiere a sin intervención humana. Por ejemplo, la definición de determinados hábitos de compra online, en función a comportamientos previos.

4.3.4 Delegado de Protección de Datos

Una de las obligaciones incluidas en el GDPR es la designación de Oficiales de Protección de Datos o por sus siglas en inglés DPO, Data Protection Officer. El rol principal de un DPO es asistir y asesorar a quien procesa los datos con respecto al cumplimiento de GDPR, y asegurarse de la aplicación de las disposiciones dentro de la institución. Se le exige que mantenga un registro de todas las actividades de procesamiento que involucran datos personales, realizadas por la institución. Este registro debe incluir información explicativa sobre el propósito de las operaciones de procesamiento y debe ser accesible para cualquier persona.

Las actividades del DPO exigen un seguimiento periódico de los sujetos de datos y en gran escala, o cuando la información incluye datos sensibles. Tiene un cierto grado de independencia dentro de la organización y es el enlace entre ésta y el órgano de supervisión (en el caso de GDPR, el Supervisor Europeo de Protección de Datos) o los sujetos de datos.

Si se nombra a un DPO sus datos de contacto deben comunicarse a la autoridad de supervisión y estar públicos para que cualquier interesado realice consultas a la entidad, ya sea para cuestiones relativas al tratamiento de sus datos o para el ejercicio de sus derechos.

No todos los controladores o procesadores de datos deben designar un DPO, pero en el caso de que sí, hay tres condiciones bajo las cuales se debe designar un DPO:

1. La organización es una autoridad pública distinta de un tribunal que actúa a título judicial.
2. Sus actividades principales requieren que monitoree a las personas de manera sistemática y regular a gran escala. (por ejemplo, eres Google)
3. Sus actividades principales son el procesamiento a gran escala de categorías especiales de datos, enumerados en el Artículo 9 del RGPD, o datos relacionados con condenas penales y delitos mencionados en el Artículo 10 (por ejemplo, eres un consultorio médico).

4.4 X 1058 Tecnología de la información – Código de prácticas relativo a la protección de la información de identificación personal

La Unión Internacional de Telecomunicaciones (UIT) es el ente especializado de las Naciones Unidas en telecomunicaciones y tecnologías de la información y la comunicación. El Sector de Normalización de las Telecomunicaciones de la UIT (UIT-T) es el órgano que estudia los aspectos técnicos, de explotación y tarifarios; y posteriormente publica recomendaciones sobre los mismos, con la meta de la normalización de las telecomunicaciones a nivel mundial.

La Asamblea Mundial de Normalización de las Telecomunicaciones (AMNT), establece los temas que han de estudiar las Comisiones de Estudio del UIT-T, que a su vez producen recomendaciones sobre dichos temas.

La aprobación de recomendaciones por los miembros del UIT-T es el objeto del procedimiento establecido en la Resolución 1 (uno) de la AMNT. En algunos sectores de la tecnología de la información que corresponden a la esfera de competencia del UIT-T, es donde se desarrollan normas en colaboración con la ISO y la CEI.

4.4.1 Contexto

El número de organizaciones que llevan a cabo el procesamiento de la PII aumenta considerablemente, del mismo modo que la cantidad de PII que estas tratan. Por otra parte, las expectativas de la sociedad respecto de la protección de la PII y la seguridad de los datos personales también están aumentando. Un gran porcentaje de países incrementan su

legislación para hacer frente a las violaciones en la seguridad de los datos, con un número cada vez mayor de incidentes graves.

A medida que aumenta el número de violaciones de la PII, las organizaciones que llevan a cabo la recopilación o el procesamiento de la PII necesitarán, directrices más completas y robustas con objeto de reducir el riesgo de violación de la privacidad y disminuir la incidencia de las infracciones en la organización y en las personas afectadas. La especificación X.1058 describe ese tipo de directrices y ofrece orientaciones o directrices para los controladores de PII en una amplia gama de controles de la seguridad de la información y protección que se aplican de forma habitual en diferentes organizaciones encargadas de la protección de la PII. Esta especificación está conformada por la familia de normas internacionales de la familia ISO/CEI, que facilitan directrices o describen requisitos con respecto a otros aspectos del proceso general de protección de la PII:

- ISO/CEI 27001 describe un proceso de gestión de la seguridad de la información y requisitos asociados, que podrían servir de base para la protección de la PII.
- ISO/CEI 27002 facilita directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta uno o más entornos de riesgo para la seguridad de la información de una organización.
- ISO/CEI 27009, que describe los requisitos de utilización de ISO/CEI 27001 en un determinado sector (campo, zona de aplicación o sector de mercado), explica cómo incluir requisitos adicionales a los de ISO/CEI 27001, cómo reformular cualquiera de los requisitos de ISO/CEI 27001 y cómo incluir controles o conjuntos de controles, además de los indicados en Anexo A de ISO/CEI 27001.
- ISO/CEI 27018 da orientaciones a las organizaciones que cumplen la función de procesadores de PII cuando ofrecen capacidades de procesamiento como servicios en la nube.
- ISO/IEC 29134:2017 facilita directrices para la identificación, el análisis y la evaluación de los riesgos para la privacidad, si bien ISO/CEI 27001 e ISO/CEI 27005 describen una metodología destinada a identificar, analizar y evaluar dichos riesgos.

4.4.2 Anexo normativo

La Especificación X.1058 contiene un Anexo normativo en el cual se detalla un conjunto de controles específicos para la protección de la PII que complementan los indicados en ISO/CEI 27002. Estos controles, con sus directrices asociadas, se dividen en 12 (doce)

categorías, que corresponden a la política de privacidad y los 11 (once) principios de privacidad enumerados en ISO/CEI 29100:2011.

El anexo además describe las definiciones de nuevos objetivos, nuevos controles y nuevas directrices de implementación que forman un conjunto ampliado de controles para cumplir los requisitos específicos para la protección de la PII. Estos 11 (once) principios:

1. Consentimiento y Elección

    - Consentimiento

El objetivo es hacer de los titulares de la PII unos participantes activos del proceso de decisión relativo al procesamiento de su PII, excepto en los casos limitados por la legislación o la reglamentación, mediante el ejercicio de un consentimiento dado de manera consciente, informada y libre.

    - Elección

En el caso de elección el objetivo es ofrecer a los titulares de la PII, cuando sea adecuado y factible, la posibilidad de elegir no permitir el procesamiento de su PII, rechazar o cancelar el consentimiento, oponerse a un tipo de procesamiento específico y explicar al titular de la PII las implicaciones de dar o denegar el consentimiento.

2. Legitimidad y especificación de los fines

    - Legitimidad de los fines

El objetivo es asegurar que los fines del procesamiento de la PII se ajustan a las leyes aplicables y disponen de una base legal.

    - Especificación de los fines

El objetivo es especificar los fines para los cuales se recoge la PII antes del momento de la recopilación y limitar la utilización posterior al cumplimiento de los fines originales.

3. Limitación de la recopilación

El objetivo es limitar la recopilación de la PII a la que está dentro de los límites definidos por las leyes aplicables y es estrictamente necesaria para los fines especificados.

4. Minimización de datos

El objetivo es minimizar la PII procesada hasta lo estrictamente necesario para los intereses legítimos que persigue el controlador de la PII y limitar la divulgación de PII a un número mínimo de interesados en la privacidad.

5. Restricciones en materia de utilización, retención y divulgación

El objetivo es limitar la utilización y divulgación de PII a fines específicos, explícitos y legítimos, y retener la PII no más de lo necesario para alcanzar los fines indicados o para cumplir las leyes aplicables.

6. Exactitud y calidad

El objetivo es procurar que la PII procesada sea exacta, completa, actualizada, adecuada y pertinente a los efectos de su utilización

7. Apertura, transparencia y notificación

- Notificación de privacidad

El objetivo es procurar que las notificaciones de privacidad contengan el nivel adecuado de detalles, estén redactadas en un lenguaje sencillo y sean de fácil acceso.

- Apertura y transparencia

El objetivo es facilitar a los titulares de la PII una información clara y de fácil acceso sobre las políticas, los procedimientos y las prácticas del controlador de la PII con respecto al procesamiento de esa información.

8. Participación y acceso del titular de la PII

- Acceso del titular de la PII

El objetivo es ofrecer a los titulares de la PII la posibilidad de tener acceso a su información y revisarla, así como de controlar su exactitud y exhaustividad.

- Rectificación y participación

El objetivo es facilitar la modificación, corrección o eliminación de datos a los procesadores de la PII y a terceros cuyos datos personales han sido divulgados.

- Gestión de las reclamaciones

El objetivo es establecer un tratamiento eficaz de tratamiento de las reclamaciones y rectificar los procedimientos que deben ser utilizados por los titulares de la PII.

9. Rendición de cuentas

El objetivo es establecer una gobernanza eficaz del procesamiento de la PII.

10. Seguridad de la información

El objetivo es velar por la debida protección de la PII según los resultados de una evaluación de riesgos.

11. Cumplimiento de la privacidad

El objetivo es evitar infracciones de la política jurídica, normativa, reglamentaria, de la privacidad o el incumplimiento de obligaciones contractuales relacionadas con la privacidad o con cualquier requisito en la materia.

4.5 ISO/IEC 29100:2011 Marco de trabajo de privacidad para la protección de información de identificación personal

La ISO/IEC 29100:2011 es un estándar internacional cuyo foco se encuentra centrado en la privacidad de los datos; proporcionando un marco de alto nivel para la protección de datos personales dentro de los sistemas de tecnología de la información y la comunicación (TIC). Tiene como objetivo dar soporte a las organizaciones en la definición de los requerimientos para la privacidad de los datos en cualquier sistema en que se procese información complementándose con las leyes donde los mismos se encuentren.

4.5.1 Contexto histórico de las iniciativas de protección de la privacidad

Debido al desarrollo continuo de las tecnologías de información y comunicación (Information and Communication Technology – ICT) y la evidente confluencia entre los entornos físicos y digitales, la protección de la información de identificación personal (PII por sus siglas en inglés Personally Identifiable Information) se ha convertido en uno de los principales objetivos organizacionales desde la perspectiva de Seguridad de la Información debido a su valor legal y comercial en caso de un incidente.

A pesar de que la necesidad de protección de esta información era tangible desde los comienzos de la informática, no fue sino hasta 1980 cuando se desarrolló un modelo que permitió la implementación de una estrategia para la protección de la privacidad.

Más adelante, en 2005 se realizó la “27ª Conferencia Internacional de Protección de Datos” en Montreux (Suiza). En esta conferencia, más de 300 participantes de todo el mundo debatieron acerca del derecho a la protección de datos, cuyas conclusiones quedaron registradas en la declaración “*La protección de datos personales y de la intimidad en un mundo globalizado: un derecho universal que respeta diversidades*” (“The protection of personal data and privacy in a globalised world: a universal right respecting diversities”) en donde se establecen 11 (once) principios generales para la protección de datos personales:

11 Principios de protección de privacidad de la 27 Conferencia Internacional de Protección de datos (Montreux – Suiza)
1 – Principio de recopilación y procesamiento justo y legítimo de datos
2 – Principio de exactitud
3 – Principio de especificación y limitación de objetivo
4 – Principio de proporcionalidad
5 – Principio de transparencia
6 – Principio de participación individual y, en concreto la garantía del derecho de acceso de la persona en cuestión
7 – Principio de no discriminación
8 – Principio de la seguridad de los datos
9 – Principio de Responsabilidad
10 – Principio de supervisión independiente y sanción legal
11 – Principio de nivel adecuado de protección en caso de flujos transfronterizos de datos personales

TABLA 1: PRINCIPIOS DE PROTECCIÓN DE LA PRIVACIDAD

Iniciativas similares fueron desarrolladas de forma paralela por el Foro de Cooperación Económica Asia Pacífico (APEC), Federal CIO Council, la Red de Autoridades Francófonas, la Red Iberoamericana de Protección de Datos y la Red Global para hacer cumplir la ley de privacidad (Global Privacy Enforcement Network – GPEN). En 2007 como parte del WG5 de ISO/IEC/FIDIS/ITU-T de estándares de gestión de identidades se presentó el estándar ISO/IEC 29100:2011, enfocado al establecimiento de un marco de trabajo para la protección de la privacidad.

4.5.2 El marco de trabajo de protección

El objetivo de este estándar es soportar a las organizaciones en la definición de los requerimientos para preservar la privacidad en cualquier sistema en el que se procese información de identificación personal y servir como complemento en el caso que existan consideraciones legales relacionadas.

La PII tratada por el estándar debe coincidir con alguno de los siguientes identificadores:

- Si contiene o está asociada con un identificador que se refiera a una persona natural (por ejemplo, un número de obra social)
- Si contiene o está asociada con un identificador que pueda estar relacionado con una persona natural (por ejemplo, número de pasaporte o número de cuenta, etc.)
- Si contiene o está asociado con un identificador que pueda ser usado para establecer una comunicación con una persona natural identificada (por ejemplo, una ubicación geográfica precisa, un número de teléfono, etc.)
- Si contiene una referencia que esté enlazada con cualquiera de los identificadores anteriores.

Así mismo, también se contempla cualquier dato que distinga a una persona natural de otra (por ejemplo, datos biométricos).

Para la gestión de este tipo de datos se definen los siguientes actores:

- Titular de los datos (PII Principal / Data Subject): Persona física titular de la PII.
- Responsable de los datos (PII Controller): Parte interesada que determina el propósito y los medios para el procesamiento de información de identificación personal.
- Encargado del tratamiento (PII Processor): Parte interesada ajena al responsable que trata los datos como consecuencia de una relación jurídica que delimita su ámbito de actuación en la prestación de un servicio.
- Tercero (Third Party): Parte interesada diferente del titular, el responsable o el encargado.

La interacción de estos actores y la PII puede dar resultado a los siguientes flujos que definen las responsabilidades en el tratamiento de los datos:

Escenario	Titular	Responsable	Encargado	Tercero
A	Entrega PII	Recibe PII		
B		Entrega PII	Recibe PII	
C	Entrega PII		Recibe PII	
D	Recibe PII	Entrega PII		
E	Recibe PII		Entrega PII	
F		Recibe PII	Entrega PII	
G		Entrega PII		Recibe PII
H			Entrega PII	Recibe PII

TABLA 2: INTERACCIÓN ENTRE LOS ACTORES DEL TRATAMIENTO DE DATOS PERSONALES

Siendo así, el marco de trabajo para la protección de estos datos para la gestión de las anteriores interacciones está compuesto por 11(once) principios.

A continuación, se describen cada uno de estos principios:

1. Consentimiento y opción: El titular de los datos debe poder elegir el procesamiento o no de sus datos a través de un consentimiento y se le debe informar acerca de sus derechos de participación y acceso.
2. Legitimidad de propósito y especificación: El propósito de tratamiento de datos debe cumplir con las leyes aplicables y debe ser informado al titular antes de que la información sea recolectada a través de un lenguaje claro y adaptado a las circunstancias.
3. Limitación en la recolección: La recolección de datos personales deben ser limitada estrictamente a las necesidades del propósito especificado y bajo las consideraciones de las leyes aplicables.
4. Minimización de datos: Adoptar el principio de “necesidad de saber” (Need-to-know) para darle acceso a los datos únicamente al personal requerido y eliminar los datos cuyo propósito haya expirado o que no exista requerimiento legal para retenerlo.

5. Limitación de uso, retención y divulgación de los datos personales conforme con los propósitos específicos, explícitos y legítimos establecidos.
6. Exactitud y calidad: Garantizar que los datos procesados son exactos, completos, actualizados, adecuados y relevantes para el propósito de uso, validando su confiabilidad si son provistos por alguien diferente del titular, así como establecer procedimientos de control en la recolección y mecanismos periódicos para la validación de los datos recolectados y almacenados.
7. Apertura, transparencia y notificación: Proveer al titular de información de las políticas de procesamiento y de cualquier cambio en el procedimiento del tratamiento de datos.
8. Participación individual y acceso: Permitirle al titular acceder y revisar sus datos y definir procedimientos para que los titulares puedan ejercer sus derechos de forma rápida y eficiente.
9. Rendición de cuentas: Asignarle la responsabilidad de implementación de políticas de privacidad a un individuo en la organización, informarle al titular en caso de una brecha de seguridad que haya afectado sus datos, gestionar los terceros involucrados con los que se comparten los datos a través de consideraciones contractuales y efectuar formación al personal que tenga acceso a los datos.
10. Seguridad de la información: Implementar controles operativos, funcionales y estratégicos para garantizar la integridad, confidencialidad y disponibilidad de los datos personales y protegerlos contra riesgos como acceso no autorizado, destrucción, divulgación o pérdida a través del ciclo de vida, así como realizar análisis de riesgos para identificar el estado de controles físicos, técnicos y organizacionales.
11. Cumplimiento con la privacidad: Verificar y demostrar los niveles de protección de los controles de seguridad a través de auditorías periódicas con auditores internos o de terceros y monitorear el cumplimiento de los requerimientos de privacidad.

4.6 ISO/ IEC 27701:2019 - Seguridad de Datos Personales

La Norma ISO/ IEC 27701:2019 de Sistemas de Gestión de la Información de Privacidad (o en inglés Privacy Information Management System - PIMS), además de incluir el esquema común que comparten todas las Normas ISO sobre sistemas de gestión, incluye los controles de la Norma ISO/IEC 27001:2013 (ISO, 2013) y de la Guía de Buenas Prácticas de la ISO/IEC 27002:2013 enfocados a protección de datos, se almacenan directrices y requisitos específicos de protección de datos personales, teniendo en cuenta el RGPD y otras legislaciones vigentes en materia de Privacidad y de protección de datos personales.

En este estándar se describe cómo una norma que sirve para gestionar la seguridad de la información que contenga datos personales, en cualquier tipo de organización, ya sea pública o privada.

ISO/ IEC 27701:2019 se relaciona directamente con los requisitos que se encuentran en las regulaciones existentes de protección de datos, como por ejemplo el Reglamento general de protección de datos (GDPR). Este estándar recientemente publicado fue escrito con la intención de satisfacer los requisitos del RGPD y otras regulaciones de privacidad.

Dado que la ISO/IEC 27001:2013 es el estándar de referencia para implementar un sistema de gestión de seguridad de la información, la nueva ISO apunta a convertirse en el estándar de referencia para implementar un sistema de gestión de información de privacidad. Dado que ambos estándares comparten una superposición significativa en los requisitos técnicos optamos por analizar la ISO/ IEC 27701:2019, ya que implícitamente si una organización adopta la ISO/IEC 27001:2013, el cambio a la 27701 es menor.

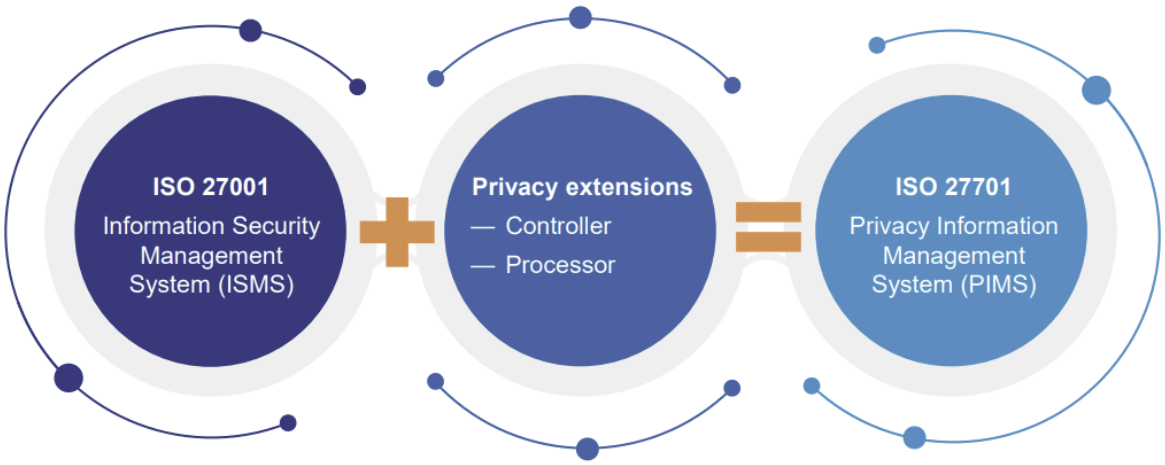

FIGURA 16: SISTEMA DE GESTIÓN DE PRIVACIDAD DE LA INFORMACIÓN

4.6.1 ISO/ IEC 27701:2019 y la organización

La ISO/ IEC 27701:2019 ayuda a las organizaciones a recopilar y procesar legalmente los datos personales. Lo que permitirá a la misma a crear y mantener un sistema de gestión de información de privacidad (PIMS). Este PIMS garantiza que las organizaciones dispongan de una gobernanza de datos completa. Similar a ISO/IEC 27001:2013, la extensión proporcionará objetivos de control y controles para que la organización considere implementarlos.

La ISO/ IEC 27701:2019 es aplicable a todos los tipos y tamaños de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro. Esta certificación actúa como un sello de aprobación y demuestra el compromiso de su organización con la privacidad y las mejores prácticas.

Aplicando este estándar en su estructura, las organizaciones podrán reducir sensiblemente los riesgos asociados a la vulneración de los derechos de privacidad de las personas. Está pensada para integrarse en el marco de un Sistema de Gestión de la Seguridad de la información (SGSI) existente en el cual se añade una línea adicional de principios y objetivos orientados a la privacidad, como por ejemplo:

- Controles específicos que aportan garantías de seguridad sobre los tratamientos de los datos personales.
- Incorporar la gestión de la privacidad en la gestión de riesgos de la empresa.
- Establecer roles y responsabilidades claras sobre los tratamientos.
- Mejorar la gestión de los contratos con los encargados del tratamiento.
- Requerir la incorporación de la privacidad por diseño y por defecto en los tratamientos.
- Garantizar que se permita a los propietarios de los datos personales el ejercicio de sus derechos sobre los mismos.

4.6.2 La importancia de la gestión de la información de privacidad

Tener un sistema de gestión de la información de privacidad asegura que la organización cumpla con regulaciones como el RGPD. Las sanciones por infringir las leyes de protección de datos pueden ser severas dependiendo del país.

La ISO/ IEC 27701:2019 tiene una estructura principal compuesta de 8 apartados y 6 anexos en la que se indica el camino para asegurar un PIMS, a continuación se detallan una descripción de que se encontrará la organización si trabaja sobre esta ISO:

- Cláusula 5: En esta cláusula se establece la correspondencia con los apartados 4 al 10 de la norma ISO/IEC 27001:2013, ampliando los requerimientos sobre protección de la información específicamente para el apartado 4 sobre el contexto organizacional y el apartado 6 relativo a la planificación de la gestión de riesgos, no aportando necesidades adicionales en el resto de los apartados.
- Cláusula 6: Este apartado amplía los requerimientos establecidos en la guía de buenas prácticas ISO/IEC 27002:2013 y los controles establecidos en el Anexo A de la ISO/IEC 27001:2013. Se amplían los requisitos sobre la protección de la información en algunos controles del 5 al 18, con excepción del control 17 (Seguridad de la información en la continuidad del negocio) donde no se establecen medidas adicionales a las ya existentes.
- Cláusula 7: Determina controles adicionales y la guía de implementación de estos para los propietarios de la Información de identificación personal (PII). En total con 4 objetivos de control y 31 controles.
- Cláusula 8: Este apartado establece controles adicionales y una recomendación de implantación para los encargados de tratar información personal de terceros contratados y la subcontratación de los servicios. En total con 4 objetivos de control y 18 controles.

Adicionalmente, se incluyen los Anexos A y B en los que se establecen los controles de privacidad para responsables y procesadores junto con el Anexo A de ISO/IEC 27001 que incluye los controles para seguridad de la información. Además, varios anexos como el Anexo C que hace referencia a los principios recogidos en ISO/IEC 29100:2011; Anexo D al RGPD, Anexo E a la ISO/IEC 27018; ISO/IEC 29151 y Anexo F con información sobre la ISO/IEC 27001:2013 e ISO/IEC 27002:2013.

En el Anexo D se presenta un mapeado de las cláusulas y los artículos del RGPD, haciendo referencia a los principios, el cumplimiento con las bases de legitimación, la obligación de transparencia e información, el ejercicio de los derechos ARSOPL, la evaluación de impacto, notificación a la autoridad de control, designación del Delegado de Protección de Datos (DPD) entre otros. Asimismo, como las exigencias de responsabilidad proactiva, materia de seguridad y las transferencias internacionales de datos personales.

En conclusión, este estándar es una buena herramienta para implementar e integrar los principios del RGPD en un sistema de gestión de seguridad de la información (SGSI), mejorando la reputación y las relaciones comerciales de la organización en la que se apliquen.

4.7 Evaluación de Impacto en la Protección de datos

Las evaluaciones de impacto son un tipo particular de evaluación que intenta ayudar a las organizaciones a obtener respuestas sobre causa y efecto. A diferencia de las evaluaciones generales, que pueden responder a muchos tipos de preguntas, las evaluaciones de impacto se preocupan por saber cuál es el impacto (o efecto causal) de un programa sobre un resultado de interés.

En el caso de la Evaluación de Impacto en la Protección de datos es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus tratamientos cuando involucran los datos personales.

Un informe PIA puede incluir documentación sobre las medidas tomadas para el tratamiento de riesgos, por ejemplo, las medidas que surgen del uso del sistema de gestión de seguridad de la información (SGSI) bajo ISO/IEC 27001 o un sistema de gestión de información sobre privacidad (PIMS) bajo ISO/IEC 27701. Un PIA es más que una herramienta: es un proceso que comienza en las etapas más tempranas posibles de una iniciativa, cuando todavía hay oportunidades para influir en su resultado y, por lo tanto, garantizar la privacidad por diseño. Es un proceso que continúa hasta que, e incluso después, de implementado el proyecto.

Por todo esto, consideramos que el PIA es un eslabón importante para garantizar que los recursos necesarios para establecer la protección de la privacidad o datos personales sean trabajados adecuadamente.

4.7.1 ISO/IEC 29134: 2017 - Tecnología de la información - Técnicas de seguridad - Directrices para la evaluación del impacto de la privacidad

La ISO/IEC 29134:2017 brinda pautas para realizar un proceso sobre evaluaciones de impacto en la privacidad, y permite armar una estructura y contenido de un informe PIA. Es aplicable a todo tipo y tamaño de organizaciones, incluidas empresas públicas, empresas privadas, entidades gubernamentales y organizaciones sin fines de lucro. Es relevante para aquellos involucrados en el diseño o implementación de proyectos, incluidas las partes que operan sistemas de procesamiento de datos y servicios que procesan los datos personales.

Un PIA se puede realizar con el propósito de:

- Identificar el impacto sobre la privacidad, riesgos y responsabilidades de la privacidad;
- Proporcionar información para diseñar para la protección de la privacidad (a veces llamada privacidad por diseño);
- Revisar los riesgos de privacidad de un nuevo sistema de información y evaluar su impacto y probabilidad;
- Proporcionar la base para el suministro de información de privacidad a los directores de datos personales sobre cualquier acción de mitigación recomendada;
- Mantener actualizaciones posteriores o actualizaciones con funcionalidad adicional que probablemente afecte los datos personales que se maneja;
- Compartir y mitigar los riesgos de privacidad con las partes interesadas, o proporcionar evidencia relacionada con el cumplimiento.

Esta evaluación de impacto proporciona una forma de detectar potenciales riesgos de privacidad que surgen del procesamiento de PII y, por lo tanto, informan a la organización que debe tomar precauciones y crear salvaguardas personalizadas antes, no después. En el caso de que se produzca un riesgo de privacidad o una infracción, el informe PIA puede proporcionar evidencia de que la organización actuó apropiadamente al intentar prevenir la ocurrencia.

4.7.1.1 Objetivos de los informes de PIA

El objetivo de los informes de PIA es comunicar los resultados de la evaluación a las partes interesadas. Para estos informes existen múltiples partes interesadas:

- PII principal - PIA es un instrumento que permite a los sujetos de PII tener la seguridad de que su privacidad es estar protegido.
- Gestión
    - Un PIA como instrumento para gestionar los riesgos de privacidad, crear conciencia y establecer la rendición de cuentas; visibilidad sobre el procesamiento de PII dentro de la organización, y los posibles riesgos e impactos de la mismo; insumos para la estrategia comercial o de productos;
    - La integración del PIA en las primeras etapas del proyecto garantiza que se cumplan los requisitos de privacidad, incluidos en los requisitos funcionales y

no funcionales, son alcanzables, viables y rastreados a través del cambio y la gestión de riesgos y puede resultar en que el proyecto no se lleve a cabo o se cancelado. El esfuerzo por clasificar y administrar la PII del proyecto debe financiarse como una inversión separada rubro y monto en un proyecto o presupuesto de programa, aceptable para todas las partes interesadas;

- Un PIA como una oportunidad para comprender mejor los requisitos de privacidad y evaluar las actividades contra estos requisitos; insumos para el diseño y la entrega de productos o servicios; revisado y modificado a través del proceso de gestión de cambios después de la entrega;
- Un PIA como instrumento para comprender los riesgos de privacidad a nivel de función / proyecto / unidad; consolidación de riesgos; aportes al diseño de políticas de privacidad y mecanismos de aplicación; entradas para rediseñar los procesos de privacidad.

- Regulador – Un PIA es un instrumento que aporta evidencia que respalda el cumplimiento de los requerimientos legales. Puede proporcionar evidencia de la debida diligencia tomada por la organización en caso de incumplimiento, incumplimiento, denuncia, etc.
- Cliente – Un PIA es un medio para evaluar cómo el procesador de PII o el controlador de PII está manejando PII y proporciona evidencia de que cumple con las obligaciones contractuales.

4.7.1.2 Proceso de realización de un PIA

El alcance de un PIA, los detalles específicos de lo que cubre y cómo se lleva a cabo deben adaptarse al tamaño de la organización, la jurisdicción local y el programa específico, sistema de información o proceso que es objeto del PIA.

El proceso debe contener el "Objetivo" es algo que debe lograrse, la "Entrada" que proporciona orientación sobre qué información puede ser necesaria para lograr el "Objetivo" y el "Resultado esperado" el cual es el objetivo recomendado para las "Acciones". Las "acciones", o sus equivalentes, son una guía sobre las actividades que pueden necesitar llevarse a cabo para lograr el "Objetivo" y crear el "Resultado esperado" recomendado, y la "Guía de implementación" proporciona más detalles de los asuntos que pueden necesitar ser considerados en realizando las “Acciones”.

Las "Acciones" en esta cláusula, o equivalentes, adaptadas al alcance y escala deseados de un PIA pueden ser implementadas de forma independiente por una

organización. Están destinados a formar una base razonable para la planificación, implementación y seguimiento de la PIA en una amplia gama de circunstancias.

CAPÍTULO V – Guía de buenas prácticas

5.1 Introducción

Toda la información mencionada en los capítulos 3 y 4, sobre todo aquellos centrado en la Ley 25.326, ITU-T X.1058, ISO/IEC 29100:2011, ISO/IEC 27701:2019 e ISO/IEC 29134:2017 al que llamaremos “Base de Información”, tienen el mismo objetivo, que es ofrecer al titular de los datos un marco de protección y seguridad, cuando los mismos son objeto de un tratamiento. Según en qué lugar de procedencia se encuentre el titular al momento de brindar datos, aplica una u otra normativa, y hasta un conjunto de ellas.

Este trabajo de tesina presenta una guía de buenas prácticas, que se encuentra alineada con los documentos de la “Base de información”, y cuyo enfoque se centra en los puntos que tienen mayor incidencia sobre el titular, pero también ayuda a las organizaciones a tomar puntos para no tener impactos negativos y consecuencias tanto en su imagen como legales. La guía se ha elaborado a modo de checklist, lo que facilita a una organización hacer una revisión introspectiva del manejo de los datos personales enfocado en su propósito y cumplimiento.

Esta guía acompaña puntos de política de privacidad de la organización y colabora con detectar o minimizar las potenciales consecuencias vinculadas con la negligencia en la protección de datos personales (multas, procesos legales, daños a la reputación, demandas, pérdida de la confianza de inversores, aumento en los costes de respuesta a incidentes, etc.). Por otra parte, la guía sirve para comprobar si la organización posee los puntos realizar una auditoría tanto de cumplimiento, como de información de técnicas y metodologías. De este modo se acompaña a la misma organización desde una etapa temprana, del ciclo de vida del dato, teniendo en cuenta el riesgo que conlleva los datos personales y su impacto en la organización.

Los estándares trabajados no se deben ver como un reemplazo de la legislación vigente de cada país o como orientación exclusiva para el cumplimiento legal. Al contrario, se asume como un marco holístico enmarcado dentro de una estrategia organizacional de alto nivel para la protección de la privacidad en cualquier ámbito que afecte a la empresa. La siguiente figura muestra como la guía toma los datos personales e incorpora las regulaciones.

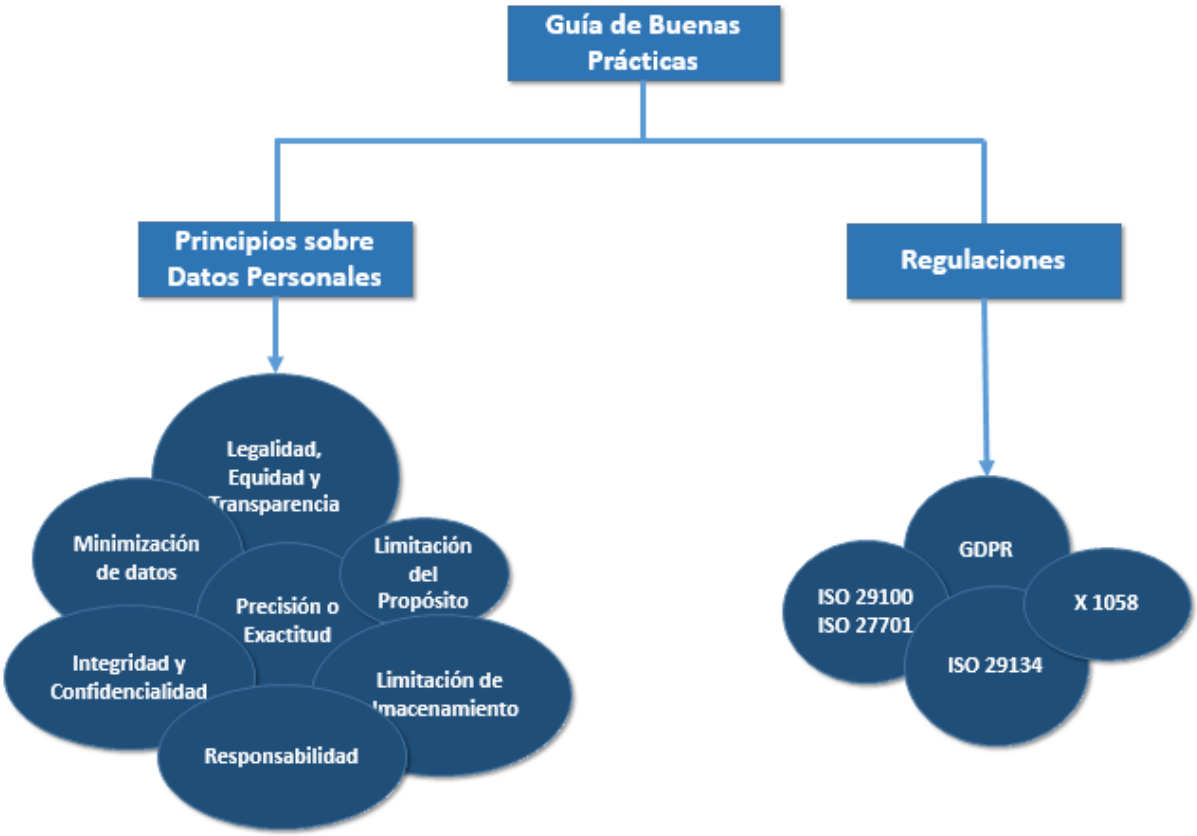

FIGURA 17: INTERSECCIÓN DE LA BASE DE INFORMACIÓN

5.5.1 Preparación de la Guía

Los datos personales son toda aquella información que permite identificarnos o nos hace identificables, como el nombre, el domicilio, la imagen u otros, por lo que tienen una directa e íntima relación con las distintas actividades que desarrollamos en nuestra vida diaria. Su protección deviene, por ello, en indispensable.

Cuando contratamos servicios de agua o luz, damos nuestro documento de identidad y señalamos nuestro domicilio; cuando adquirimos productos mediante el uso de tarjetas de crédito, firmamos para autorizar la transacción; cuando solicitamos un producto por delivery, brindamos el celular y la dirección de destino; incluso, cuando nos registramos en alguna red social o descargamos una app entregamos datos de identificación.

De allí y ante la preocupación que existe sobre el tratamiento de nuestra información personal, hemos desarrollado esta “Guía de verificación para el aseguramiento de la protección de datos personales” con el objetivo de que la organización o cualquier entidad, pueda conocer en forma clara, sencilla y didáctica qué datos trata, cuál es el tratamiento que les puede dar, cuáles son los derechos que garantiza frente a los bancos de datos, qué

instrumentos tiene para defenderlos, y la situación frente a la entidad encargada de protegerlos.

La recopilación y tratamiento permanente de esta información por parte de entidades públicas y privadas, requiere de mecanismos que permitan protegerlos adecuadamente y garanticen la posibilidad de efectuar un control sobre ellos, con la finalidad de evitar que un tratamiento indebido afecte directamente la intimidad personal y/o familiar, o sea utilizado para cometer actos ilícitos.

5.5.2 A quién va dirigida la guía

Esta Guía ofrece una lista de puntos de verificación de directrices y orientaciones de las diferentes normativas, con las que la organización, responsables de tratamiento, las personas delegadas de protección de datos, o aquellas unidades o departamentos que dentro de la entidad responsable tienen a su cargo el diseño, selección, desarrollo, despliegue, y explotación de aplicaciones y servicios podrán identificar as metodología para el cumplimiento de las mismas, sin embargo, no pretende ser la única manera en que puede llevarse a cabo para el cumplimiento. Las organizaciones que tengan ya implantados procesos y herramientas de análisis de datos personales pueden utilizarlas para evaluar los relativos a la privacidad y la protección de datos siempre que cubran los aspectos esenciales.

5.2 Etapas

La guía se presenta agrupada en 3 (tres) etapas. En cada etapa se incluyen los conjuntos de los puntos que consideran e integran las garantías para la protección de los derechos y libertad de la ciudadanía con relación a sus datos personales. En cada etapa se tuvo en cuenta los puntos y recomendaciones de la “Base de información” mencionados anteriormente. A continuación se menciona cada una de ellas y el agrupamiento que contiene.

5.2 Etapa 1

En esta etapa se encuentran agrupados los puntos que la organización realiza antes de realizar el tratamiento de los datos.

5.2.1 Privacidad desde el Diseño y Seguridad por defecto

Este conjunto de puntos está dirigido a relevar las medidas técnicas y organizativas que la organización posee. Las estrategias o medidas que haya adoptado la organización deben

incorporar la protección de la privacidad a lo largo de todo el ciclo de vida del objeto, en este caso el tratamiento de los datos; desde la etapa de su concepción, pasando por las fases de desarrollo, puesta en producción operación, mantenimiento y retirada. En este conjunto se hace foco en la privacidad desde el diseño orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias. Se tuvo en cuenta los “Principios fundacionales de la privacidad desde el diseño” definidos por Ann Cavoukian. Estos principios son:

1. Proactivo, no reactivo; Preventivo, no correctivo.
2. La privacidad como configuración predeterminada.
3. Privacidad incorporada en la fase de diseño.
4. Funcionalidad total: pensamiento “Todos ganan”.
5. Aseguramiento de la privacidad en todo el ciclo de vida.
6. Visibilidad y transparencia.
7. Enfoque centrado en el sujeto de los datos.

5.2.2 Políticas Generales

Este conjunto de puntos está dirigido a relevar acerca de las políticas generales que ayuden a la organización a alinear los objetivos de la misma. En cuanto a las políticas de seguridad sobre la información se tiene en cuenta los tres atributos más importantes llamado “triángulo CIA” y son: Confidencialidad (Confidentiality), Integridad (Integrity) y Disponibilidad (Availability).

La guía contempla todas las políticas sugeridas por los distintos estándares y cuáles son los atributos que las mismas deben contener con el fin de ayudar a la organización a mantener las cualidades de la información, cuando esté en tratamiento los datos personales.

5.2.3 Clasificación

Este conjunto está dirigido a la detección de los datos que necesita y clasifica la organización. La organización debería reafirmar que solo trabaja con los datos que necesita y que la clasificación le permite tomar medidas de seguridad para su resguardo y tratamiento.

5.2.4 Roles

Esta sección está dirigida para que la organización reconozca su rol dentro del tratamiento y proporcione una segregación de roles adecuada para la seguridad de los datos a través de todo su ciclo de vida.

5.3 Etapa 2

En esta etapa se encuentran agrupados los puntos que la organización tiene en cuenta a la hora de realizar el tratamiento de los datos

5.3.1 Consentimiento

Este conjunto de puntos no sólo está dirigido a identificar si la organización provee un mecanismo de consentimiento, sino también a identificar cuáles atributos posee. Algunos puntos están dirigidos al relevamiento de consentimientos de menores y personas con discapacidad.

5.3.2 Recopilación y Tratamiento

Esta sección contiene puntos sobre la especificación de los datos que se relevaron. Se reconocen los 7 (siete) principios de la protección de los datos y cómo la organización los tiene en cuenta.

5.3.3 Transferencia y cesión de datos

Este conjunto está dirigido a identificar, en el caso de transferencias o cesión de los datos personales, si la organización tiene en cuenta el nivel adecuado de seguridad del país destino o fuera de los dominios de la organización

5.4 Etapa 3

En esta etapa se encuentran todos los puntos que se debe tener en cuenta la organización a la hora de realizar una Evaluación de Impacto.

5.4.1 Evaluación de Impacto

La Evaluación de Impacto en la Protección de Datos Personales es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que está expuesto el tratamiento que realiza

La Evaluación de Impacto en la Protección de Datos Personales (en adelante, la EIPD) es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.

5.5 Guía de verificación para el aseguramiento de la protección de datos

El trabajo presenta una checklist para acompañar la implementación.

Marco inicial de protección

Marcar con una X la respuesta

Privacidad desde el diseño y por defecto	
	¿Se ha implementado un documento claro de política de protección de datos que establezca el espíritu de la organización y el enfoque general para la protección de datos y la privacidad?
	¿Se ha cubierto la protección de datos por diseño y por defecto en la capacitación del personal, para que las personas puedan comprender y abordar cualquier problema de manera proactiva, sistemática e innovadora?
	¿Se garantiza que la tecnología escogida para el desarrollo de productos habilita/facilita el ejercicio de los derechos relacionados con PDP (por ejemplo, derecho de borrado o al olvido)
	¿Se garantiza que la tecnología seleccionada para el desarrollo de productos no dé lugar a procesos o eventos que puedan ser inesperados, intrusivos o podrían presentar mayores riesgos de daño para las personas y sus datos personales?
	¿Se tiene fines relevantes, limitados y claramente definidos para la recolección de datos personales?
	¿Se comunica claramente a las personas/titulares cuáles son estos propósitos?
	¿Se recopila solo los datos personales que necesita para su propósito?
	¿Se garantiza que solo usa los datos que utilizarán para los fines enunciados?
	¿Se ha establecido el perfil predeterminado o la configuración de la cuenta de la manera más amigable para el usuario? Por ejemplo, cuando los usuarios pueden compartir perfiles o contenido.
	¿Necesita conservar los datos personales durante el tiempo previsto?
	¿Puede eliminarlo, archivarlo o agregarlo y, de ser así, cuál es la etapa más temprana en la que se puede hacer?
	¿Se han creado controles y / o documentación que permitan a los titulares revisar y modificar su configuración y preferencias de privacidad? Por ejemplo, una herramienta de auditoría para los usuarios para que puedan determinar cómo se almacenan, protegen y utilizan sus datos, y decidir si sus derechos están siendo protegidos adecuadamente.
	¿Se ha diseñado un proceso seguro para el borrado y / o destrucción de datos personales?

Anonimización

	¿Se ha establecido una modalidad de tratamiento de los datos personales que no permita la identificación de su titular, salvo mediante información adicional (seudonimización de los datos personales)?
	¿Se han establecido políticas de anonimización?
	En caso de que la respuesta anterior haya sido afirmativa: La política: [ ] ¿Cuenta con principios de protección de datos en el diseño de los procesos de anonimización? [ ] ¿Cuenta con los objetivos fijados en la gestión de riesgos? [ ] ¿Cuenta con la estructura y responsabilidades del equipo de trabajo implicado en los procesos de anonimización? [ ] ¿Cuenta con los objetivos y finalidad de la información anonimizada? [ ] ¿Cuenta con variables de anonimización, por ejemplo de identificación y clasificación? [ ] ¿Cuenta con técnicas de anonimización utilizadas
	¿Se han definido términos de uso y acceso a la información anonimizada?
	¿Se han definido medidas de control del personal con acceso a la información anonimizada (trazabilidad)?
	¿Se han identificado obligaciones y deberes en caso de ruptura de la cadena de anonimización que haga posible la Re identificación de los interesados?
	¿Se utilizan técnicas de anonimización?
	¿Se utilizan técnicas de seudo anonimización?
	¿Se ha definido un proceso de anonimización Planificación y asignación de tareas en la anonimización?
	¿Cuenta con un responsable del proceso de anonimización?
	¿Cuenta con personal con acceso a la información anonimizada?
	¿Han identificado las técnicas de anonimización?
	¿Se han determinado los recursos y equipo técnico necesarios para proceder a la anonimización de los datos?
	¿Han definido plazos de revisión periódica del proceso?
	¿Realizan capacitaciones e informan al personal implicado en los procesos de anonimización?
	¿Realizan capacitaciones e informan al personal que trabaja con datos anonimizados?

Técnicas y controles

	Durante el diseño del tratamiento ¿Se tiene en cuenta las medidas técnicas y organizativas apropiadas a los datos a relevar?
	¿Cuenta con la capacidad de garantizar la confidencialidad de los sistemas y servicios de tratamiento?
	¿Cuenta con la capacidad de garantizar la integridad de los sistemas y servicios de tratamiento?
	¿Cuenta con la capacidad de garantizar la disponibilidad de los sistemas y servicios de tratamiento?
	¿Cuenta con la capacidad de garantizar la resiliencia permanente de los sistemas y servicios de tratamiento?

	¿Se han creado controles para las preferencias de los usuarios de intercambio de datos (por ejemplo, inclusión / exclusión voluntaria), detallando los beneficios o consecuencias de hacerlo, incluido cualquier impacto potencial en las características o la funcionalidad del producto?
	¿Cuenta con los controles de acceso de usuario adecuados, incluidos los controles de acceso lógico?
	¿Cuenta con los procedimientos para eliminar las ID de usuario antiguas?
	¿Ha establecido controles robustos de acceso? Por ejemplo: uso de autenticación de dos factores, contraseñas de un solo uso, redes privadas virtuales
	¿Ha establecido controles adecuados para el acceso a las diferentes redes de comunicación? Por ejemplo a las redes inalámbricas, incluida la protección de diferentes redes y registros de acceso
	¿Cuentan con procesos para bloquear sitios web / plataformas de mayor riesgo que puedan representar un riesgo para los datos personales (por ejemplo, sitios para compartir archivos, correo electrónico personal)
	¿Se han asegurado de que existan procesos para marcar, poner en cuarentena o eliminar correos electrónicos sospechosos?
	¿Se han asegurado de que existan procesos para cifrar los datos cuando corresponda? Por ejemplo: discos duros y unidades de estado sólido en computadoras portátiles y de escritorio, cualquier tráfico de web a usuario, cualquier sitio web (desde el dispositivo al servicio backend) y conexiones bluetooth que transmiten información confidencial.
	¿Se ha creado un plan de respuesta a incidentes durante el proceso de diseño de un nuevo producto / servicio y hemos considerado qué medidas de seguridad pueden ser necesarias en caso de un incidente (por ejemplo, una brecha de acceso, un virus o daño físico al servidor)?
	¿Se han asegurado de contar con sistemas adecuados de respaldo y recuperación de datos (por ejemplo, si hay una filtración de datos o un desastre natural)?
	¿Siguen un plan de continuidad empresarial y lo probamos con regularidad?
	¿Se han implementado protocolos que evalúan y aseguran las garantías de nuestros procesadores de datos en cuanto a la suficiencia de las salvaguardias técnicas y organizativas que aplican cuando procesan datos personales en nuestro nombre?
	¿Dispone de programas antivirus / antimalware?
	¿Cuenta con procesos para las pruebas de penetración de la infraestructura de la empresa a intervalos regulares?
	¿Cuenta con procedimientos adecuados de actualización y parcheo, incluida la verificación de las fuentes de parches y la integridad de los paquetes?
	¿Se han asegurado de que los dispositivos y software estén sujetos a las pruebas del ciclo de vida del desarrollo de la seguridad (incluidas las pruebas de regresión y el modelado de amenazas)?
	¿Dispone protecciones para todos los sistemas para evitar que se copien datos personales en medios extraíbles (CD / DVD, discos duros externos, memorias USB, etc.)?
	¿Cuenta con la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico?
	¿Cuenta con un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento?
	¿Durante el tratamiento se comprueba la efectividad de las medidas aplicadas?
	¿Se aplican medidas técnicas y organizativas apropiadas para garantizar que, por defecto, solo se tratan datos necesarios para cada uno de los fines?
	¿Se aplican medidas técnicas y organizativas teniendo en cuenta la cantidad de datos personales recogidos, la extensión del tratamiento, el plazo de conservación y la accesibilidad?

	¿Las medidas garantizan que, por defecto, los datos no son accesibles a un número indeterminado de personas físicas, sin la intervención de personal?

Acceso y derechos

	¿Tienen una política / aviso de privacidad vigente que proporcione claramente toda la información requerida?
	¿Lo actualiza con regularidad o cuando hacen algo nuevo?
	¿Cuenta con un proceso para divulgar y explicar cambios significativos?
	¿Cuenta con un banner de cookies y un aviso / política de cookies en su lugar?
	¿Puede exportar personal en un formato legible por máquina de uso común?
	¿Cumple con los derechos de las personas a ser informados sobre los datos que tienen sobre ellos?
	¿El sistema facilita el derecho de las personas a solicitar acceso a los datos que la empresa tiene sobre ellos?
	¿El sistema facilita el derecho de las personas a corregir los datos que tienen sobre ellas?
	¿El sistema facilita el derecho de las personas a eliminar los datos que tienen sobre ellos?
	¿Se puede congelar / poner en cuarentena los datos que tienen sobre un individuo?
	¿Puede proporcionar a las personas sus datos en un formato de uso común y legible por máquina?
	¿Puede transmitir esa información a otra organización si es necesario?
	¿Cuenta con procedimientos para permitir que los interesados se opongan a la forma en que usan su información, en particular en relación con cualquier uso de marketing directo o de mayor riesgo?

Políticas generales

Marcar con una X la respuesta

Políticas generales para la utilización y protección de los datos personales

	¿Se cuenta con políticas de protección de los datos personales?
	Las políticas de protección de los datos personales ¿Son adecuadas a los fines de la organización?
	¿Son transparentes en lo relativo a la recopilación y procesamiento de los datos personales por la organización?
	¿Se cuenta con reglas para tomar decisiones en los temas de protección de los datos personales?
	¿Se cuenta con criterios sobre la aceptación de riesgos a la privacidad?
	¿Se cuenta con un compromiso de cumplimiento de los requisitos de protección de la privacidad aplicables?
	¿Se planifican y ejecutan capacitaciones para el personal de su organización sobre las políticas?
	¿Se le informa al personal que tratan datos personales?

Relevamiento de datos

Seleccione que políticas posee la organización

	¿Política de seguridad de la información?
	¿Política de control de acceso?
	¿Política de seguridad física y ambiental?
	¿Política de gestión de incidentes?
	¿Política de continuidad de negocio y recuperación ante desastres?
	¿Política de gestión de activos?
	¿Política de adquisición, desarrollo de software y mantenimiento de sistemas de información?
	¿Política de gestión de proveedores?
	¿Política de gestión de comunicaciones y operaciones?
	¿Política de cumplimiento?
	¿Política de gestión de riesgos?
	¿Se cuenta con reglas de comportamiento?

Brechas de seguridad

	¿Ha establecido un procedimiento para identificar y gestionar las brechas de seguridad?
	Los encargados del tratamiento ¿Han establecido un procedimiento para notificar las brechas de seguridad al responsable en el momento en que tomen conocimiento de ellas?
	¿Se cuenta con un procedimiento para notificar a la autoridad de control sobre la brecha y el grado de afectación de los datos?
	¿Se tiene un procedimiento para documentar los motivos por los que no se pudo notificar a la autoridad de control?
	¿Se ha definido un rango de días?
	¿Documentan todas las brechas de seguridad de los datos personales?
	La comunicación al interesado ¿Se le notifica en un lenguaje claro y sencillo, y describe la naturaleza de la brecha?

Atributos de las políticas	
	¿Se cuenta con un compromiso de mejora continua?
	¿Se han incluido medidas para asegurar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento?
	¿Se cuenta con medidas para asegurar la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico
	¿Se tienen medidas para garantizar que la/s persona/s autorizada/s a acceder a los datos sólo los tratan siguiendo instrucciones definidas por la organización?

Consecuencias	
	¿Se han tenido en cuenta los riesgos que presenta el tratamiento como consecuencia de su destrucción, pérdida o alteración accidental o ilícita que son transmitidos, conservados o tratados, o la comunicación o acceso no autorizados a dichos datos para evaluar el nivel de seguridad aplicado?

Bases de datos	
	¿Ha registrado la base de datos en donde se almacenan los datos personales?
	¿Se informa el responsable de la Base de datos?
	¿El responsable está inscripto en la Autoridad de control?
	¿Se cuenta con políticas de backups?
	¿Se cuenta con políticas de seguridad
	¿Se registra quién accede a los datos?
	¿Se registra cuándo se accedió a los datos??
	¿Se registra desde qué tipo de dispositivo/aplicación se accede?
	¿Se tiene en cuenta la segregación de funciones?
	¿Se registran logs?
	¿Se limita el acceso a los datos personales?
	¿La información se encuentra cifrada?
	¿Se posee el historial de transacciones?
	¿Se posee procedimientos de actualización?
	¿Cuenta con un proceso de auditoría para la base de datos?

Clasificación

Marcar con una X la respuesta

Relevamiento de datos

	¿Se relevan datos personales?
	¿Se relevan datos personales sensibles?
	¿Se conoce el número de personas que se encuentran en sus bases de datos?
	¿Es este número superior al 1% de la población del país?

Tipología de datos

	¿Se van a tratar datos personales?

Clasificación de los datos objeto del tratamiento

	Datos identificativos
	[ ] DNI [ ] Dirección postal o electrónica [ ] Imagen [ ] Voz [ ] Nº Seguridad Social o Mutualidad [ ] Teléfono [ ] Fax [ ] Marcas físicas [ ] Marcas físicas [ ] Nombre/s y Apellido/s [ ] Firma o huella [ ] Firma electrónica [ ] Tarjeta sanitaria

	Datos relativos a las características personales
	[ ] Datos de estado civil [ ] Datos de familia [ ] Fecha de nacimiento [ ] Lugar de nacimiento [ ] Edad [ ] Sexo [ ] Nacionalidad [ ] Lengua materna [ ] Características físicas [ ] Antropométricas

	Datos especialmente protegidos
	[ ] Datos de menores (herencia, seguros,) [ ] Datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad [ ] Datos relativos a salud Vida sexual u orientación sexual [ ] Religión u opiniones religiosas [ ] Origen étnico o racial [ ] Creencias o creencias filosóficas [ ] Datos ideológicos y políticos

[ ] Afiliación sindical
[ ] Datos biométricos
[ ] Datos genéticos que proporcionan una información única sobre la fisiología o la salud del identificado obtenidas del análisis de una muestra biológica.
[ ] Datos relativos a condenas y delitos penales.
[ ] Datos solicitados para fines policiales sin consentimiento de las personas afectadas.

	Datos académicos y profesionales
	[ ] Formación [ ] Titulaciones [ ] Historial del estudiante [ ] Experiencia profesional [ ] Pertenencia a colegios o asociaciones profesionales

	Datos relativos a las circunstancias sociales
	[ ] Datos de violencia de género y malos tratos

	Datos económicos, financieros y de seguros
	[ ] Cuenta bancaria [ ] Solvencia [ ] Ingresos [ ] Rentas [ ] Inversiones [ ] patrimoniales [ ] Créditos [ ] Préstamos [ ] Avales [ ] Datos bancarios [ ] Jubilación [ ] Datos económicos de nómina [ ] Seguros [ ] Hipotecas [ ] Subsidios [ ] Beneficios [ ] Historial de créditos [ ] Tarjetas de crédito [ ] Bienes [ ] Planes de pensiones [ ] Datos deducciones impositivas/impuestos

	Detalles de empleo o Profesionales
	[ ] Profesión [ ] Experiencia [ ] Puestos de trabajo [ ] Datos no económicos de nómina [ ] Historial del trabajador

	Datos especialmente protegidos
	[ ] Datos de salud (enfermedades, alergias, …) [ ] Otros tipos de datos: especificar qué datos

Categorías de personas físicas	
	¿Los datos que recolecta pertenecen a Clientes?
	¿Los datos que recolecta pertenecen a Empleados?
	¿Los datos que recolecta pertenecen a Proveedores?
	¿Los datos que recolecta pertenecen a Menores?
	¿Los datos que recolecta pertenecen a Personas discapacitadas?
	Otros tipos de datos que no han sido mencionados, especificar cual:

Roles

Marcar con una X la respuesta

Roles

	Responsable del tratamiento ¿La Organización es controladora?
	Encargados de tratamiento ¿La organización es procesadora?
	Terceras partes involucradas ¿Se informa terceras partes involucradas?
	Delegado de protección de datos ¿Se define una Persona a cargo de la privacidad de los datos?
	Autoridad de control ¿Se define una autoridad de Control?

Responsable

	¿Se identifica un responsable?
	¿Se involucra en las definiciones de las políticas de protección?
	¿Determina los fines para el tratamiento?
	¿Determina los medios para el tratamiento?
	¿Determina quién es el encargado?
	¿Lleva a cabo el registro de actividades de tratamiento?
	¿Ha designado a un DPD?

Encargado del tratamiento

	El tratamiento por el encargado ¿Se rige por un contrato u otro acto jurídico vinculante con arreglo a las normas de Derecho?
	¿Se accede a los datos únicamente siguiendo instrucciones del responsable?
	Las siguientes preguntas son sobre el contrato:
	¿Establece el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, así como las obligaciones y derechos del responsable?
	¿Establece que se tratan los datos personales únicamente siguiendo instrucciones documentadas del responsable?
	¿Garantiza que las personas autorizadas para tratar datos personales se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria?
	¿Establece que se tomarán las medidas de seguridad necesarias?
	¿Establece que se respetarán las condiciones indicadas para recurrir a otro encargado del tratamiento?
	¿Establece que el encargado asistirá para que se pueda responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados?
	¿Establece que se suprimen o devolverán los datos personales una vez finalice la prestación de los servicios, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales?
	¿Establece que pondrá a disposición toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas, así como para permitir y contribuir a la realización de auditorías e inspecciones, por parte del responsable o de otro auditor autorizado por el responsable?

	¿Establece que, si el encargado del tratamiento recurre a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se imponen a este otro encargado las mismas obligaciones de protección de datos que las estipuladas en el contrato, mediante contrato u otro acto jurídico establecido con arreglo a Derecho?
	¿Consta por escrito?

Delegado de protección de datos (DPD)

	¿Se ha designado un DPD atendiendo a sus cualidades de profesionalidad, conocimientos y competencias en la materia?
	¿Se han publicado los datos de contacto del DPD y se ha comunicado a la autoridad de control?
	¿Se garantiza que el DPD participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales?
	¿Se da respaldo en el desempeño sus funciones?
	¿Se le facilitan los recursos necesarios para el desempeño de sus funciones, el acceso a los datos personales y a las operaciones de tratamiento?
	¿Se le facilitan los recursos necesarios para mantener sus conocimientos?
	¿Se garantiza que el DPD no recibe ninguna instrucción en lo que respecta al desempeño de sus funciones?
	¿El DPD rinde cuentas directamente al más alto nivel jerárquico?
	¿El DPD atiende las solicitudes de los interesados?
	¿El DPD está obligado a mantener la confidencialidad en el desempeño de sus funciones?
	¿Se garantiza que no existe conflicto de intereses, si el DPD desempeña otras funciones?
	¿El DPD coopera y actúa como punto de contacto con la autoridad de control?

Consentimiento

Marcar con una X la respuesta

Consentimiento	
	¿Se ha verificado que, para el procesamiento, el consentimiento es la base legal más apropiada?
	La solicitud de consentimiento ¿Proporciona información clara sobre los detalles del procesamiento?
	La solicitud de consentimiento ¿Incluye el nombre y el cargo del procesador de datos?
	La solicitud de consentimiento ¿Incluye el propósito y el tipo de procesamiento?
	La solicitud de consentimiento ¿Incluye el tipo de datos que serán tratados?
	La solicitud de consentimiento ¿Incluye los derechos del interesado a acceder, borrar y retirar?
	¿Se obtiene un consentimiento para el caso de transferencia de los datos?
	¿Han definido los medios para obtener el consentimiento de los titulares de los datos personales?
	¿Se solicita el consentimiento de forma inteligible y de fácil acceso?
	¿El consentimiento es libre?
	¿El consentimiento es expreso?
	¿El consentimiento es de palabra o verbal?
	¿Se solicita usando lenguaje claro y sencillo?
	¿El consentimiento es dado a través de firma electrónica?
	¿El consentimiento dado a través de correo electrónico?
	¿Confirma la identidad del titular de los datos, o del representante legal del titular de los datos, que da el consentimiento para el procesamiento?
	¿El consentimiento es informado?
	¿Se puede demostrar que el titular dio su consentimiento para el tratamiento?
	¿Se solicita el consentimiento de forma clara e independiente de los demás asuntos?
	La solicitud de consentimiento ¿Proporciona una opción de participación y no incluye casillas previamente marcadas?
	¿Proporciona los medios, para que los titulares de los datos personales den su consentimiento, asegurando que se obtiene este consentimiento antes del inicio de cualquier procesamiento?
	¿Se mantienen registros de cuándo, dónde y cómo se otorgó el consentimiento?
	¿Se mantienen registros de los formularios de solicitud de consentimiento que un interesado acordó?
	¿Se almacena el registro del consentimiento cuando es facilitado por un representante legal? (por ejemplo, en nombre de un menor o de una persona legalmente incapacitada)
	¿Revisan periódicamente el propósito del consentimiento y realizan las actualizaciones necesarias?
	¿Cuentan con un sistema para gestionar el consentimiento y los retiros?
	¿Se permite retirar el consentimiento con la misma facilidad que se solicita?
	¿Proporciona un mecanismo para que los titulares puedan modificar el alcance de su consentimiento?
	¿Se ofrecen medios para retirar el consentimiento en cualquier momento?

	¿Se actúa rápidamente sobre las solicitudes de retiro sin demora?
	¿Penalizan a las personas que deseen retirar su consentimiento?

Menores

	¿Se recolecta el consentimiento de menores de 14 años al titular de la patria potestad o tutela sobre el niño?
	¿Se verifica que el consentimiento fue dado por el titular de la patria potestad o tutela sobre el niño?

Personas discapacitadas

	¿Se recolecta el consentimiento de personas discapacitadas?
	¿Se verifica que el consentimiento fue dado por el titular de la patria potestad o tutela sobre la persona?

Recopilación y Tratamiento

Marcar con una X la respuesta

Especificación

	¿Han identificado los datos personales que se utilizan para cada proceso de negocio?
	¿Separa los datos personales que utiliza para cada proceso de negocio de manera lógica?
	¿Gestiona los diferentes derechos de acceso de acuerdo con los procesos de negocio?
	¿Establece un entorno TI dedicado para los sistemas que procesan la información personal más sensible?
	¿Confirma regularmente que los datos personales están separados de manera eficaz y que no se ha agregado nuevos destinatarios o interconexiones?

Limitaciones

	¿Limita la recopilación de los datos personales a los mínimos elementos necesarios para los fines descritos en la notificación y para la cual el titular ha dado su consentimiento?
	¿Recopila datos personales sensibles sin un consentimiento?

Exactitud

	¿Establece procedimientos de recopilación de los datos personales que contribuyan a asegurar la exactitud y la calidad de los datos?
	¿Cómo se realiza la recopilación?
	[ ] Formularios en papel [ ] Entrevista telefónica [ ] Navegación o formularios Web [ ] Registro de aplicaciones móviles [ ] Datos de actividad personal [ ] Datos de sensores (IoT)
	¿Los datos personales son recolectados de tal forma que se detecte toda modificación una vez que se ha extraído de la fuente autorizada?
	¿Garantiza la fiabilidad de los datos personales recopilada de una fuente distinta a la de su titular antes de que sea procesada?
	¿Periódicamente, comprueba y corrige todos los datos personales inexactos o desactualizados que se utilizan en sus programas o sistemas?
	¿Formula directrices que aseguren y maximicen la exactitud, exhaustividad, conveniencia y pertinencia de la información divulgada?

Tratamiento

	¿Asegura que los titulares de los datos personales que eligen una opción respecto del procesamiento de sus datos, pueden hacerlo antes de que se inicie cualquier procesamiento?

Derechos individuales

	¿Se le informa al titular de los datos del Derecho a ser informado?
	¿Se le informa al titular de los datos del Derecho de acceso?
	¿Se le informa al titular de los datos del Derecho a rectificación?
	¿Se le informa al titular de los datos del Derecho a borrar?
	¿Se le informa al titular de los datos del Derecho a restringir el procesamiento?
	¿Se le informa al titular de los datos del Derecho a la portabilidad de datos?

	¿Se le informa al titular de los datos del Derecho a oponerse?
	¿Cuenta con un proceso de verificación, evaluación y valoración de la eficacia de las medidas técnicas y organizativas que utilizan para garantizar la seguridad del tratamiento?

Finalidad del tratamiento

	¿Se informa una descripción sencilla de los fines del tratamiento, incluso elaboración de perfiles?
	¿Se informa una descripción ampliada de los fines del tratamiento?
	¿Se informan los plazos o criterios de conservación de los datos?
	¿Se incorpora información sobre decisiones automatizadas, perfiles y lógica aplicada?

Legitimación jurídica del tratamiento

	¿Se incorpora la base jurídica o legitimación para el tratamiento?
	¿Se informa en detalle de la base jurídica del tratamiento, en los casos de obligación legal, interés público o interés legítimo?
	¿Se informa la obligación o no de facilitar datos y consecuencias de no hacerlo?
	¿Se incorpora la previsión de transferencias a Terceros Países?

Destinatarios

	¿Se incorpora destinatarios o categorías de destinatarios?
	¿Se incorpora decisiones de adecuación, garantías, normas corporativas vinculantes o situaciones específicas aplicables?
	¿Se incorpora como realizar derecho a retirar el consentimiento prestado?
	¿Se incorpora como ejercer el derecho a reclamar ante la Autoridad de Control?

Fuente de los datos

	¿Se incorpora información detallada del origen de los datos, incluso si proceden de fuentes de acceso público?

Fuente de los datos

	¿Se mantiene un registro de todos los tratamientos?
	¿Se informa el derecho a presentar una reclamación ante las Autoridades de Control?

Transferencia y cesión de datos

Marcar con una X la respuesta

Transferencia de datos

	¿Se utilizan procesadores de datos de terceros o empresas del grupo para procesar datos en su nombre?
	Si obtiene o recibe datos de Terceros, ¿El consentimiento se obtuvo / actualizó recientemente?
	¿Cuenta con un proceso para asegurarse de que el tercero pueda demostrar su consentimiento?
	¿Se ha asegurado de que la organización haya recibido un nombre específico cuando se recopilaron los datos?
	¿Registra el proceso para tener pruebas de que ha llevado a cabo una exhaustiva diligencia debida de sus proveedores de datos de terceros?
	La transferencia de datos personales cumple con alguna o más de las siguientes calificaciones:
	[ ] Hecho con el consentimiento informado de la persona [ ] Necesario para la ejecución de un contrato entre el individuo y la organización o para los pasos precontractuales tomados a solicitud del individuo [ ] Necesario para la ejecución de un contrato celebrado en interés de la persona entre el responsable del tratamiento y otra persona [ ] Necesario por razones importantes de interés público [ ] Necesario para el establecimiento, ejercicio o defensa de reclamaciones legales [ ] Necesario para proteger los intereses vitales del interesado u otras personas, cuando el interesado es física o legalmente incapaz de dar su consentimiento [ ] Elaborado a partir de un registro que está destinado a proporcionar información al público (y que está abierto a la consulta del público en general o de aquellos que puedan demostrar un interés legítimo en inspeccionar el registro)

Cesión de datos

	¿Cuenta con una lista de los destinatarios a quienes comunica o comunicó los datos personales?
	En la lista ¿Se han incluido los destinatarios a quienes comunica o comunicó los datos personales en terceros países u organizaciones internacionales?
	En caso de ceder datos de titulares o contactos a un tercero ¿Se ha formulado advertencias para los afectados y se ha recolectado su consentimiento?
	Cumple con los criterios siguientes:
	[ ] La transferencia de datos no la realiza una autoridad pública en ejercicio de sus poderes públicos [ ] La transferencia de datos no es repetitiva (no se realizan transferencias similares de forma regular) [ ] La transferencia de datos involucra datos relacionados solo con un número limitado de personas [ ] La transferencia de datos es necesaria para los fines de los intereses legítimos imperiosos de la organización (siempre que dichos intereses no sean anulados por los intereses de la persona) [ ] La transferencia de datos está sujeta a las garantías adecuadas establecidas por la organización (a la luz de una evaluación de todas las circunstancias que rodean la transferencia) para proteger los datos personales.

	La organización que recibe los datos personales ha proporcionado alguna de las salvaguardas siguientes:
	[ ] Un acuerdo legalmente vinculante entre autoridades u organismos públicos [ ] Normas corporativas vinculantes (acuerdos que rigen las transferencias realizadas entre organizaciones dentro de un grupo empresarial) [ ] Cláusulas estándar de protección de datos en forma de cláusulas de transferencia de plantilla [ ] Cláusulas estándar de protección de datos en forma de cláusulas de transferencia modelo adoptadas por una autoridad de control [ ] Cumplimiento de un código de conducta aprobado por una autoridad supervisora [ ] Certificación bajo un mecanismo de certificación aprobado según lo dispuesto en el GDPR [ ] Cláusulas contractuales acordadas y autorizadas por la autoridad supervisora competente [ ] Disposiciones incluidas en acuerdos administrativos entre autoridades públicas u organismos autorizados por la autoridad de control competente

Política de privacidad

Marcar con una X la respuesta

Políticas de privacidad

	¿Se ha definido una política de privacidad?
	¿Se encuentra de fácil acceso?
	¿Se ha redactado con lenguaje claro?
	¿Se ha redactado con lenguaje sencillo?
	¿Se informa los datos a relevar?
	¿Se informa si los datos a relevar son sensibles?
	¿Se informa los datos del encargado de tratamiento de los datos?
	¿Se informa los datos del responsable de los datos?
	¿Se informa los datos del responsable de la seguridad de los datos?
	¿Se detalla el propósito del relevamiento?
	¿Se enuncia el principio de Licitud?
	¿Se enuncia el principio de lealtad?
	¿Se enuncia el principio de transparencia?
	¿Se enuncia el principio de Minimización de datos?
	¿Se enuncia el principio de Limitación del plazo de conservación de los datos?
	¿Se enuncia el principio de Integridad y confidencialidad?
	¿Cuenta con el detalle de cómo el titular puede ejercer el Derecho al acceso?
	¿Cuenta con el detalle de cómo el titular puede ejercer el Derecho a la corrección ("Rectificación")?
	¿Cuenta con el detalle de cómo el titular puede ejercer el Derecho a la eliminación?
	¿Cuenta con el detalle de cómo el titular puede ejercer el Derecho a restringir el procesamiento?
	¿Cuenta con el detalle de cómo el titular puede ejercer el Derecho a la portabilidad de datos?
	¿Cuenta con el detalle de cómo el titular puede ejercer el Derecho a objetar el procesamiento?
	¿Se enuncia como el titular puede ejercer el Derecho a no ser sujeto de toma de decisiones automatizadas?
	¿Se informa como proceder en caso de datos de menores?
	¿Se informa como proceder en caso de datos de personas con discapacidad?
	¿Cuenta con el detalle de las leyes que debe cumplir?
	¿Se enuncia las acciones sobre el tratamiento?
	¿Se diferencia del aviso legal y/o Términos y Condiciones?
	¿Se informa plazos de conservación?

Cookies

	¿Se ha definido una política de cookies?
	¿Se diferencia de los términos y condiciones?

	¿Se informa cuáles son las cookies?
	¿Se diferencian las cookies de navegación?
	¿Se identifica cuáles son los datos almacenados?
	¿Se identifican los tipos de cookies?
	¿Se informa el proceso para configurarlas?
	¿Se informa el proceso para rechazarlas?
	¿Se informa el tiempo que persisten en el navegador?
	¿Se informa la finalidad para la cual son utilizadas?
	¿Sabe cómo se compiló la lista de Terceros a los cuáles se hace transferencia de datos personales?

Identidad del responsable del Tratamiento

	¿Se incorporan datos de Identidad del Responsable del Tratamiento?
	Datos de contacto del responsable
	Identidad y datos de contacto del representante
	Datos de contacto del delegado de Protección de Datos
	La información se presenta con las siguientes características:
	[ ] De forma concisa [ ] Un lenguaje claro y sencillo [ ] Transparente [ ] De fácil acceso [ ] Inteligible

Derecho

	¿Se incorpora la forma de cómo ejercer los derechos de acceso, rectificación, supresión y portabilidad de sus datos, y la limitación u oposición a su tratamiento?

Evaluación de impacto

Marcar con una X la respuesta

ETAPA 1 - Necesidad de realización de Evaluación de impacto

La organización releva alguno de estos puntos

	¿Se relevan datos sensibles o datos muy personales?
	¿Se realizan tratamientos de datos de menores de edad de forma significativa?
	¿Se elaboran perfiles y predicciones?
	¿Se realizan toma de decisiones con impacto regulatorio significativo o similar?
	¿Se realizan observaciones sistemáticas?
	¿Se realiza tratamiento de datos a gran escala?
	¿Se realiza asociación o combinación de conjuntos de datos?
	¿Se relevan datos relativos a interesados vulnerables?
	¿Se realiza un uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas?
	¿Se utilizan los datos obtenidos para una finalidad más intrusiva que la finalidad original para la que fueron recogidos?
	¿Se realiza transferencia de datos a países identificados como no-seguros?
	¿Se utilizan datos personales no disociados o no anonimizados de forma irreversible para fines estadísticos, históricos o de investigación científica?
	¿Se realiza cesión de datos a terceros?
	¿Se cuenta con riesgos específicos que puedan comprometer la confidencialidad, la integridad o la disponibilidad de los datos personales?
	En el caso que alguna respuesta fue si: ¿Se realiza una evaluación de impacto?

ETAPA 2 - Descripción del proyecto y los flujos de información

Descripción del proyecto y los flujos de información

	¿Se realiza una clasificación de los datos?
	¿Se informa a los usuarios de los datos a relevar?
	¿Se informa los flujos de información?
	¿Se discriminan las tecnologías utilizadas?

Identificación de responsables

	¿Se identifica al/los responsables/s del PIA?
	¿Se identifican stakeholders?
	¿Se identifica al responsable de cada flujo?
	¿Se identifica al procesador?
	¿Se identifican los roles y responsables en cada fase del ciclo de los datos?

Análisis del marco normativo aplicable

	¿Se identifican las normativas Nacionales?
	¿Se identifican las normativas Internacionales?

	¿Se identifican buenas prácticas aplicables?

Alcance

	¿Se define un perfil físico?
	¿Se define un perfil lógico?
	¿Se define una finalidad determinada para el procesamiento?
	¿Se define cual es el alcance? Cual:
	[ ] Un proceso [ ] Un sistema de información [ ] Un programa [ ] Otra iniciativa [ ] Un módulo de software o un dispositivo

Auditoría del proceso de anonimización

	¿Se realiza una auditoría del proceso de anonimización?
	¿Se define el alcance y objetivo de la auditoría?
	¿Se identifican el equipo auditor y recursos utilizados en la realización de la auditoría?
	¿Se identifican fases y planificación de la auditoría?
	¿Se identifican pruebas y verificaciones realizadas?
	¿Se identifica la valoración de los resultados?
	¿Se definen propuestas para la mejora del proceso de anonimización?
	¿Se define auditoría de la explotación de la información anonimizada?
	¿Se define periodo de revisión?

Contexto - Ciclo de vida de los datos

	¿Se identifica un procedimiento para la captura de datos?
	¿Se elabora un inventario de datos personales y de los sistemas de tratamiento?
	¿Se determinan las funciones y obligaciones de las personas que traten datos personales?
	¿Se realiza un registro de los medios de almacenamiento de los datos personales?
	¿Se define el plazo de Uso / Tratamiento?
	¿Se Cuenta con una política de destrucción y/o borrado seguro?

ETAPA 3 - Evaluación de impacto

Análisis de cumplimiento normativo

	¿Se identifica marco regulatorio?
	¿Se identifican buenas prácticas?
	¿Se identifican políticas aplicables sobre el tratamiento?
	¿Se identifican políticas de la organización aplicables?
	¿Se identifican los marcos aplicados sobre riesgos?

	Análisis de riesgo
	¿Se identifica de manera clara la metodología?
	¿Se identifican las etapas de los mismos?

	Identificar amenazas y riesgos
	¿Se identifican las amenazas?
	¿Se identifican los tipos de amenazas?
	¿Se identifican los riesgos sobre los principios?
	[ ] Licitud [ ] Lealtad y transparencia [ ] Limitación de la finalidad [ ] Minimización de los datos [ ] Exactitud [ ] Limitación del plazo de conservación [ ] Integridad y confidencialidad
	¿Se definen criterios de nivel de impacto?
	[ ] Insignificante [ ] Limitado [ ] Importante [ ] Máximo
	¿Se define el riesgo aceptable que soporta la organización?

	Evaluar los riesgos
	¿Se identifican valores para el cálculo de la probabilidad?
	¿Se identifican medidas de control?
	¿Se cuantifican el impacto de su materialización?

	Gestión del riesgo y privacidad
	¿Se identifican los controles?
	¿Se identifican los controles?
	Identifica por cada control:
	[ ] Responsable involucrado [ ] Tecnología involucrada [ ] Proceso involucrado

ETAPA 4 - Cumplimiento

	Medidas para el cumplimiento
	¿Se elabora un plan de acción?
	Se identifica por cada control:
	[ ] Responsable involucrado [ ] Tecnología involucrada [ ] Proceso involucrado

ETAPA 5 - Informe final

Informes

	¿Se informa el alcance de la evaluación?
	¿Se informan los requisitos de privacidad?
	¿Se informa la evaluación de riesgos?
	¿Se informa el plan de tratamiento de riesgos?
	¿Se informa la conclusión y las decisiones tomadas sobre la base de los resultados del PIA?
	¿Se informa un resumen público de PIA para informar a los directores de PII sobre el nivel de riesgo asociado con el programa, sistema de información, y el proceso implementado en el que participará su PII?

ETAPA 6 - Revisión

Revisión y retroalimentación

	¿Se definen planes de retroalimentación luego de aplicar el control?
	¿Se define periodo de revisión?
	¿Se define personal a cargo?
	¿Se identifica de manera clara el plan de acción?
	¿Se comunicó al personal involucrado sobre el control aplicado?

Responsable

	¿Se tienen en cuenta los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas?

Capítulo VI Conclusiones

Debido a que los datos personales pertenecen a su titular y no a las entidades que utilizan las bases de datos, se han puesto en marcha iniciativas alrededor del mundo, que buscan proteger los datos personales que se encuentran en posesión de particulares o de gobiernos, haciendo de la tarea de protección de la información, una responsabilidad compartida entre los usuarios, las organizaciones que tienen acceso a los datos y gobiernos que deben legislar al respecto, así como crear las instituciones encargadas de regular y hacer cumplir las leyes.

El punto de partida de la tesina fue identificar cual reglamentación o estándar, ayuda a la organización a cumplir con la protección adecuada de los datos. Uno de los inconvenientes fue no tener toda la información en un documento centralizado, en donde la solución encontrada fue generar una base de información donde se incluyen todos los documentos de apoyo que se tuvieron en cuenta.

A partir de los conocimientos que se adquirieron, en paralelo se presentó el caso de estudio de cómo el Reglamento General de Protección de Datos impacta en Sistemas de Gestión Académica en Argentina en CACIC 2018, reafirmando la importancia de los derechos que obtenían los titulares de los datos personales en cualquier sistema que realice un tratamiento de los mismos. Luego en 2019 y en 2020 se trabajó en las contribuciones para la Unión Internacional de Telecomunicaciones (ITU) para la ITU-T X.1058, The Open Consultation on the draft Guidelines for utilization of the GCA en relación a la Agenda de Ciberseguridad Global y en ITU Guidelines for Child Online Protection en la que se estudiaron entre otros puntos, el consentimiento, destacando el consentimiento cuando los datos de los titulares son de menores y/o personas discapacitadas, privacidad por diseño, roles, derecho al olvido y definiciones con el enfoque en datos personales y cookies.

Esta problemática, se destacó a finales del 2020 con la pandemia causada por el SARS-CoV-2 que dejó visible la brecha de seguridad sobre los datos personales y sensibles, más aún en aquellos referidos a datos de salud. Un ejemplo de ellos, los datos de las personas voluntarias que fueron inoculados en etapas tempranas de prueba de las vacunas, en donde se dejó asentado sus datos en aplicaciones para control o futuras dosis y cuyos registros no tuvieron la seguridad adecuada, ante el desconocimiento de buenas prácticas. Por otro lado, el aislamiento (provocado por la pandemia), las políticas de trabajo remoto desde el hogar (home office), las búsquedas de información sobre este virus, crearon una dependencia más fuerte en canales virtuales y electrónicos. Esto expuso la necesidad de las organizaciones de herramientas que mejoren sus procesos de una forma más eficiente. Al

mismo tiempo nos acercaba a alcanzar los objetivos generales planteados y a la construcción de la guía.

En la elaboración de la misma se pensó un diseño simple de comprobación de ítems, clasificados en temas y con un orden predeterminado, de diferentes acciones, medidas, directrices y buenas prácticas. Cada uno de los ítems en la guía son comunes, integrales y claves para la organización. Este mecanismo permite evitar errores y controlar con mayor profundidad el alcance de los distintos temas que son abordados. Además se agregaron otros puntos por fuera de los objetivos que son el consentimiento y las políticas de seguridad. Estos fueron incorporados por la relevancia que tienen ya que impacta directamente en los derechos de los titulares y la seguridad de sus datos.

Como conclusión personal, a raíz de todo el trabajo realizado nuestra mirada cambió en lo que respecta al uso de las tecnologías sobre el manejo de los datos personales y cómo estas deben seguir el lineamiento planteado para que el titular pueda ejercer sobre sus datos, derechos. Además, reafirmamos que las organizaciones deben comprometerse y realizar procesos más eficientes, a través del ciclo de mejora continua y en donde en cada ciclo incorpore técnicas y medidas para que los datos estén más seguros.

Capítulo VII Trabajo Futuro

Mientras escribíamos esta tesina pensamos que podría permitir disparar nuevas líneas de trabajo relacionadas. Las líneas que proponemos son:

- Revisar el impacto que tiene el tratamiento de datos personales utilizando tecnologías distribuidas o DLT, por su característica de bloques sin posibilidad de modificación. Esta característica debe contemplar el caso de que el titular ejerza el derecho de borrado y/o modificación y qué efecto tendría en la cadena.
- Realizar una guía que sirva de entrada para realizar auditorías en Bases de datos personales. Esta guía debería contemplar requerimientos legales, buenas prácticas y técnicas que ayuden al cumplimiento de la seguridad de los datos almacenados principalmente datos sensibles.
- Cómo influye el Modelo de Alineamiento (SAM) dentro de las organizaciones, teniendo en cuenta los datos personales.
- Cómo una organización puede realizar el ciclo de vida de sus procesos utilizando el modelo de referencia (COBIT 5) con la perspectiva en datos personales.
- A través de los resultados de la guía alimentar un tablero de control con las estadísticas/métricas de estos, para saber a dónde debería apuntar la organización para mejorar sus procesos.
- Con la guía y los puntos fundamentales, ayudar a la organización a la construcción del consentimiento de una forma puntual, tomando como entradas sus objetivos, tratamiento y reglas de negocio.

Índice de Figuras

Índice de Tablas

Bibliografía y Referencias

aepd. (2016). *Agencia Española de Protección de Datos*. Obtenido de https://www.boe.es/buscar/doc.php?id=DOUE-L-2016-80807

ADC; Vazquez, Nadia Estefanía; Sebastián, María Alejandra (2020) *The Open Consultation on the draft Guidelines for utilization of the GCA*

https://www.itu.int/en/action/cybersecurity/Pages/gca.aspx

Argentina, G. d. (1994). *Constitución Nacional*. Obtenido de https://www.congreso.gob.ar/constitucionNacional.php

Argentina, G. d. (2000). Obtenido de https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/texto

Argentino, G. (s.f.). *Evaluación de impacto*. Obtenido de https://www.argentina.gob.ar/sites/default/files/guia_final.pdf

Autor. (s.f.). Obtenido de iibi.unam.mx/voutssasmt/documentos/dato%20informacion%20conocimiento.pdf

BIANCHI, A. B. (s.f.). *"Hábeas data y derecho a la privacidad".* Revista El Derecho. Obtenido de Así como no hay personas sin nombre, patrimonio, ni estado civil, tampoco las hay sin datos.

COP. (2020). Obtenido de https://www.itu.int/en/ITU-D/Cybersecurity/Pages/COP.aspx

HelmutSy. (2019, 10 11). *Niveles organizacionales o pirámide organizacional.* From https://www.lifeder.com/niveles-organizacionales/

ISO. (2013). From https://www.iso.org/isoiec-27001-information-security.html

ISO. (2017). From https://www.iso.org/standard/62289.html

ISO. (2019). From https://www.iso.org/standard/71670.html

ITU. (2020). From https://www.itu.int/es/Pages/default.aspx

Molinari, Lía Hebe; Sebastián, María Alejandra; Vázquez, Nadia Estefanía (CACIC, 2018) *Caso de estudio sobre GDPR aplicado en Sistemas de Gestión* http://sedici.unlp.edu.ar/handle/10915/73652

Proteccion. (2021). *Ley de Protección de datos.* From https://ayudaleyprotecciondatos.es/aviso-legal-y-politica-privacidad/

RAE. (s.f.). *Consentimiento*. Obtenido de https://dle.rae.es/consentimiento

RAE. (s.f.). *Dato de carácter personal*. Obtenido de https://dpej.rae.es/lema/dato-de-car%C3%A1cter-personal

RAE. (s.f.). *Dato especialmente protegido*. Obtenido de https://dpej.rae.es/lema/dato-especialmente-protegido

RAE. (s.f.). *Dato Sensible*. Obtenido de https://dpej.rae.es/lema/dato-sensible

RAE. (s.f.). *Persona Identificable*. Obtenido de https://dpej.rae.es/lema/persona-identificable#:~:text=Persona%20cuya%20identidad%20pueda%20determinarse,%2C%20econ%C3%B3mica%2C%20cultural%20o%20social

Russell L.Ackoff. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Russell_L._Ackoff

sealpath.com. (s.f.). *Los tres estados*. Obtenido de https://www.sealpath.com/es/tres_estados_info/

WhatIs.com. (s.f.). *Datos en reposo*. Obtenido de https://copro.com.ar/Datos_en_reposo.html

WhatIs.com. (s.f.). *Datos en uso*. Obtenido de https://copro.com.ar/Datos_en_uso.html