ESPECIALIZACIÓN EN AUDITORÍA INTERNA GUBERNAMENTAL

FACULTAD DE CIENCIAS ECONÓMICAS UNIVERSIDAD NACIONAL DE LA PLATA

TRABAJO INTEGRADOR FINAL (TIF)

NOVIEMBRE 2021

"Propuesta Metodológica para la evaluación y tratamiento de los datos personales incluidos en los Informes de Auditoría"

AUTOR: DABUSTI MARIA CECILIA

DIRECTORES: SOLARI, ESTEFANÍA

MARTIRES, LORENA

1. RESUMEN

La Ley Nacional N° 24.156 establece en su art. 102 que *"La auditoría interna es un servicio a toda la organización y consiste en un examen posterior de las actividades financieras y administrativas de las entidades a que hace referencia esta ley, realizada por los auditores integrantes de las unidades de auditoría interna…"*

En el mismo orden de ideas, es el Instituto de Auditores Internos de Argentina quien incorpora en su definición que, la "*Auditoría Interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno."*

Existen diversas Leyes y/o disposiciones y buenas prácticas que impulsan a las Auditorías para que estén en constante actualización de sus metodologías de su trabajo, a saber: la Ley Nacional N° 25.326 de Habeas Data, las normas emanadas por el Instituto Argentino de Normalización y Certificación como por ejemplo la norma ISO-IRAM 31.000 sobre la Administración y Gestión de Riesgos, las resoluciones emitidas por la propia Sindicatura General de la Nación, como por ejemplo la Resolución N° 172/2014 sobre el informe COSO, Referencial IRAM N° 13 sobre la Gestión de Calidad de las Unidad de Auditoría Interna, y particularmente la Ley Nacional N° 27.275 sobre el Derecho de Acceso a la Información Pública.

Conforme lo publicado en la página web de "Argentina.gob.ar", quienes tienen la obligación de brindar el acceso a la información pública son: la Administración Pública Nacional, las instituciones de la seguridad social, el Poder Legislativo de la Nación, el Ministerio Público Fiscal de la Nación, el Ministerio Público de Defensa, el Consejo de la Magistratura, las empresas y sociedades del Estado, las empresas y sociedades en las que el Estado es socio, las empresas que dan servicios públicos, Instituciones o fondos administrados por el Estado, empresas partidos políticos, sindicatos, universidades y cualquier entidad privada a la que se la hayan dado fondos públicos, personas públicas no

estatales, fideicomisos formados con bienes del Estado, el Banco Central de la República Argentina, entes que cooperan con organismos estatales, entes formados por varias provincias en los que interviene el Estado Nacional y empresas que tienen la concesión sobre juegos de azar.

Debe tenerse en cuenta que existe una amplia diversidad de temas que son materia auditable en una Organización, y es por ello que en el presente trabajo se desarrollará una metodología sobre la Protección datos, entendiendo como uno de los procedimientos más críticos, aquel relacionado a la evaluación de los datos personales/sensibles que son incluidos en un informe de Auditoría, los cuales son susceptibles de ser requeridos por invocación del ejercicio de la Ley de Información Pública, y no se encuentran con el tratamiento adecuado para evitar su identificación.

Para abordar la metodología, resultó necesario integrar tanto el análisis de la legislación y normativa vigente, los procesos en las UAI, la necesidad de la protección de los datos de los ciudadanos en los informes emitidos por las mismas y por último brindar una herramienta a los procedimientos existentes en el desarrollo de las auditorías.

TABLA DE CONTENIDO

2. INTRODUCCIÓN

El presente trabajo surge como una propuesta metodológica para las Unidades de Auditoría Interna (UAI), que poseen en sus informes datos personales y/o sensibles, a fin que permita el cumplimiento legislativo, en relación a la protección de datos personales y el acceso a la información pública, ya sea por la publicación de la información o por requerimientos de terceros interesados.

Conforme lo establece el Manual de Auditoría Interno Gubernamental, elaborado por la Sindicatura General de la Nación (SIGEN) y emitido por la Resolución SGN N°3/11, el "*Informe de Auditoría es el producto último del auditor, por medio del cual expone sus observaciones, conclusiones y recomendaciones por escrito…"*

Asimismo, en el mencionado manual, se establecen las características del informe final, siendo éstas la importancia del contenido, su completitud, suficiencia, utilidad, oportunidad, objetividad, que posea equidad, de calidad convincente, claro y simple, conciso y que sea elaborado con un tono constructivo.

En la realización del informe final de Auditoría, al igual que en el informe preliminar, el auditor suele incluir, como evidencia en la redacción de las observaciones o en cuadros adjuntos, datos personales y/o sensibles de las personas.

Es la Ley Nacional N° 25.326 sobre la Protección de los datos Personales Habeas Data, que establece como su objetivo principal, la protección integral de los datos personales asentados en archivos, registros, bancos de datos u otros medios técnicos de tratamiento de datos, sean éstos 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 establecidos en el artículo 43, párrafo tercero de la Constitución Nacional.

En correlación a la protección de los datos personales, durante el año 2016 el Senado y la Cámara de Diputados promulgaron la Ley Nacional N° 27.275 sobre el Derecho de Acceso a la Información Pública. Su finalidad es garantizar el efectivo ejercicio del derecho de acceso a la información pública, promoviendo la participación ciudadana y la transparencia de la gestión pública fundada en principios tales como presunción de publicidad, transparencia y máxima divulgación, informalismo, máximo acceso, apertura, disociación de aquella información que se encuadre taxativamente en las excepciones, no discriminación, máxima premura, gratuidad, control, responsabilidad, alcance limitado de las excepciones, In dubio pro petitor[1], facilitación y por último buena fe para poder garantizar el efectivo ejercicio del acceso a la información.

Esta información, que refiere a toda aquella que se encuentre en poder del Estado, se presume pública, salvo las excepciones, y dando cuenta de la transparencia en la gestión pública, dentro de la cual se encuentran los informes emitidos por las UAI.

Esta Ley de Acceso a la Información Pública, es el punto de confluencia de los procesos dirigidos a preservar los derechos de los ciudadanos en relación a su acceso a la información de interés público, en base a una adecuada protección de los datos personales en custodia del Estado Nacional.

Se debe tener presente que en la actualidad ha cobrado especial interés toda información que es utilizada y administrada por el Estado Nacional, en cualquiera de sus intervenciones, la cual puede ser utilizada en beneficio de los ciudadanos, en relación a las herramientas que brindan la apertura de datos, pero al mismo tiempo sin el debido resguardo de seguridad puede vulnerar el derecho de su información privada y/o sensible.

Es finalidad del presente trabajo aportar a las distintas UAI, una metodología que les permita optimizar el tratamiento de los datos personales/sensibles, contenidos en los

[1] Refiere a que en caso de duda siempre será a favor de la mayor vigencia y alcance del derecho de la información

informes, limitando la exposición a reclamos o quejas por divulgación de información privada.

La optimización de las UAI impactará positivamente en la protección de los ciudadanos y sus derechos a que sus datos personales/sensibles se encuentren asegurados de una incorrecta publicación.

3. PLANTEAMIENTO DEL TEMA / PROBLEMA

En el devenir de las mencionadas legislaciones, el creciente interés legítimo del derecho de acceso a la información pública por parte de los ciudadanos, ha impulsado a las tecnologías que su avance y adaptación para el cumplimiento legislativo sea vertiginoso, como por ejemplo en los tiempos de pandemia donde la relación con la sociedad y el Organismo se basó en la virtualidad.

En el ámbito del acceso a la información pública, las UAI se ven alcanzadas con la publicación de sus informes, siempre considerando aquellos que en su totalidad o parcialidad no están contemplados en el art. 17 de la Ley de Habeas Data (Excepciones).

Dicha publicación se encuadra en el cumplimiento del Art. 32 inc i) en relación a la Transparencia Activa y la publicación en forma completa y actualizada por medios digitales y en formatos abiertos de la Ley Nacional 27.275 sobre el Derecho de Acceso a la Información Pública.

Las UAI aún deben optimizar sus procesos, a fin de incorporar una metodología de trabajo, que permita evaluar el impacto y el tratamiento que debe darse a los datos personales incluidos en sus informes. Esto tiene relevancia, cuando se considera que los Informes deben ser publicados y susceptibles de ser requeridos por terceros interesados.

Actualmente y ante situaciones de publicación y/o requerimiento por parte de terceros interesados, ante la ausencia de procedimientos, debe realizarse una evaluación presurosa

del contenido del informe y un trabajo manual o artesanal que implica tachar u ocultar los datos que debieron haber sido disociados o anonimizados.

Considerando el tiempo transcurrido desde la aplicabilidad de la legislación y a pesar que "tachar u ocultar" el dato personal/sensible a los fines de su protección, se encuentra contemplado en la misma, dicho método puede resultar ineficiente y exponer a la Organización a riesgo de alto impacto ante errores humanos.

Tal como lo establece SIGEN en sus normativas, las UAI deben orientar sus procesos para que les permita asesorar a la Organización y cumplir sus funciones desde una actitud proactiva y alineada a los avances tecnológicos. Es por ello, que se considera valorable una metodología de protección de aquellos datos incluidos en los informes de las UAI, que se encuentre en línea con los avances tecnológicos y minimice los riesgos.

En el caso de dichos informes, en ocasiones resulta necesaria la incorporación de datos personales en las observaciones, dado que constituyen el input para las áreas responsables de la falencia detectada. Es ante esta situación que las UAI deben arbitrar mecanismos innovadores y optimizar los existentes, que permitan asegurar que los informes emitidos cumplan con todos los requisitos del resguardo los derechos de los ciudadanos en la sociedad, en relación a su privacidad.

Por lo expuesto, la finalidad del presente trabajo es brindar una metodología para la evaluación, tratamiento, protección de los datos y mejora continua para los informes emitidos por las UAI.

Por último, se menciona que, no conforman el desarrollo del presente la funcionalidad de las técnicas de protección de datos, que se mencionarán.

4. OBJETIVOS

4.1. Objetivos General

Brindar una metodología que permita optimizar la protección de los datos personales/sensibles, que se encuentran incluidos en los informes emitido por las UAI, a fin que los mismos cuenten con los tratamientos adecuados para el cumplimiento legal y el resguardo de los derechos de los ciudadanos.

4.2. Objetivos Específicos

- Analizar las Leyes Nacionales relacionadas con la protección de datos personales, aquella relativa al Derecho de Acceso a la Información Pública, normativa sobre evaluación de riesgos y mejores prácticas internacionales.
- Identificar las técnicas de tratamiento de datos.
- Determinar los pasos que debe contemplar la metodología de protección datos personales que son incluidos en los informes de Auditoría.
- Desarrollar una propuesta para publicar, de manera segura, la información contenida en los informes de Auditoría.

Palabras Claves: Informes de Auditoría, Protección de Datos Personales, Derecho de Acceso a la Información Pública, Riesgos, Evaluación Impacto, Tratamiento de datos, Anonimización / Disociación de datos.

5. MARCO TEÓRICO

Por imperio de la Ley Nacional 24.156, las UAI poseen la responsabilidad del Control Interno de los Organismos en los cuales ejecutan sus actividades, bajo la dependencia funcional de la Sindicatura General de la Nación.

Es en post de dicho cumplimiento que las UAI emiten informes por distintos motivos, como por ejemplo, cumplimiento legislativo, a solicitud de la Sindicatura General de la Nación, por cumplimiento del Plan Anual de Trabajo y excepcionalmente, a pedido de la Alta Dirección del Organismo donde desarrollan sus tareas.

A título de ejemplo pueden mencionarse los siguientes Organismos, los cuales se encuadran en dicha características en relación a los datos personales/sensibles: Desarrollo Social, Administración Federal de Ingresos Públicos (AFIP), Administración Nacional de la Seguridad Social (ANSES), Instituto Nacional contra la Discriminación, la Xenofobia y el Racismo (INADI), Agencia Nacional de Discapacidad, Banco Nacional de Datos Genéticos, Instituto de Ayuda Financiera para Pago de Retiros y Pensiones Militares (IAF).

Es por ello~~,~~ que, de acuerdo a la finalidad que posea el Organismo~~,~~ donde esta actividad se realiza, las UAI, podrían incluir en sus informes datos personales/sensibles, ya sea para identificar donde se detectó la ausencia de la efectividad del control o para que las áreas responsables puedan, a partir de dicho dato, revertir la falencia detectada considerando sus consecuencias.

Tanto el Organismo de Control Interno como Externo, también han realizado auditorías, bajo su órbita, a fin de verificar el cumplimiento de la Ley de Protección de Datos Personales. Ello se vio reflejado por ejemplo en el informe realizado por la SIGEN al

Registro Único de Aspirantes a Guarda, cuyo tema fue la Fiscalización de Bases de Organismos Registrales[2].

Por su parte, la Auditoría General de la Nación (AGN), emitió el informe sobre Dirección Nacional de Protección de datos personales – Registro Nacional No Llame, realizado al Ministerio de Justicia y Derechos Humanos.[3]

Pero sin perjuicio del desarrollo de la labor de las UAI y sus Órganos de Control en relación a las áreas que auditan, existen a la fecha, procesos internos que deben optimizarse en el marco de la innovación tecnológica y la minimización de riesgos y errores al momento de que deba exponerse la información sobre los datos personales y/o sensibles.

Lo mencionado, se encuadra a la concepción que un régimen apropiado de protección de datos personales, es una condición necesaria para la adecuada implementación de nuevas tecnologías que modernicen el Estado y, más concretamente, al quehacer de los Entes Públicos. La protección de la esfera de la privacidad, también es un elemento fundamental en la implementación de herramientas de gobierno abierto y en la participación de los sujetos, en el diseño, implementación y evaluación que identifique o permita identificar al titular de dichos datos. Prácticas de protección de datos que adopten estándares y principios reconocidos internacionalmente en la materia, resultan un incentivo adicional para la mejora continua. (*Manual Operativo de protección de datos en el Salvador – Alfredo Chirino Febrero 2015*).

Es en ese sentido, que los Organismos deben cumplir con un control mandatorio que, en base al cumplimiento legislativo y la aplicación de buenas prácticas internacionales, aseguren que los datos personales sean protegidos con adecuados procedimientos de seguridad y privacidad.

[2] Informe 26/2017 - Gestión de Protección de Datos Personales
[3] Informe 221/18 – Registro Nacional No Llame

Por otra parte, la Ley Nacional N° 27.275 de Acceso a la Información Pública expone a los Organismos y sus procesos de seguridad sobre la protección de dichos datos personales al momento de determinar la obligatoriedad de disponibilidad pública sobre la información. Esto último considerando las excepciones que la misma Ley establece.

Cuando se traten datos de las personas humanas y los Organismos no tengan la obligación de pedir el consentimiento del titular, la responsabilidad de los mismos debiera traducirse en una actitud proactiva, generando de esta manera un crecimiento y fortalecimiento del ambiente de control interno en lo que respecta a la seguridad y privacidad de dichos datos.

La importancia que tiene el derecho a la protección de los datos personales, la condición para garantizar el derecho a la autodeterminación informativa de los ciudadanos y sobre todo la obligación de la disponibilidad de la información pública, contemplados en los apartados no exceptuados, requieren que las UAI incorporen u optimicen procesos internos en cuanto a los datos que son utilizados y expuestos en sus informes de Auditoría.

En dicho papel, el Estado cuenta con Organismos dependientes que poseen la responsabilidad de la protección de los datos personales/sensibles de los ciudadanos, como así también que el derecho de acceso a la información pública se encuentre disponible, asegurándose que los datos que serán brindados no incurran en incumplimientos y expongan la privacidad de las personas.

En el mismo orden de ideas, resulta oportuno citar la norma IRAM-ISO/IEC ISO 27001 sobre “Sistemas de Gestión de Seguridad de la Información”, la cual es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. Esta norma que, en consideración con el objetivo planteado resulta complementaria, debe estar integrada y considerada en su aplicación cuando se trabaje sobre la protección de los datos personales.

Es en su Anexo A Objetivos de Control y Controles (ítem A15.1.4), que dicha norma incorpora la Protección de los Datos y Privacidad de la información personal, donde se establece como aspecto de control que la protección y privacidad de los datos debe ser

garantizada según requiera en las legislaciones y regulaciones relevantes, y si es aplicable, en las cláusulas contractuales.[4]

Posterior a dicha norma, surge la extensión de la misma, la norma ISO/IEC 27701, cuyo objetivo es proporcionar orientación sobre la protección de la privacidad, incluida la forma en que las organizaciones deben gestionar la información personal, además de ayudar a demostrar el cumplimiento de la normativa en privacidad, como el Reglamento General de Protección de Datos, en todo el mundo.

La SIGEN ha plasmado en el Instructivo De Trabajo Nº 7/2015 - GNyPE. PROTECCIÓN DE DATOS PERSONALES, dicha protección en responsabilidad de los Organismos, cuyo objetivo constituye una herramienta para guiar y organizar las actividades de control en base a la Ley Nº 25.326 y la "Guía de Buenas Prácticas en Políticas de Privacidad para las Bases de Datos del Ámbito Público"

Para una mejor exposición, se incorporan al presente las normativas, marcos de referencia y buenas prácticas nacionales e internacionales, relacionados con el objeto del presente trabajo.

A. Informe COSO – Sistema de Control Interno y su relación con la información y el cumplimiento.
B. Interrelación de las tres líneas de defensa y los principios del informe COSO
C. Informe de Auditoría – Manual de Control Interno Gubernamental
D. Legislación Nacional – Protección de Datos Personales
E. Legislación Nacional – Derecho de Acceso a la Información Pública y su relación con los informes de Auditoría
F. Agencia de Acceso a la Información Pública y su relación con los datos personales

[4] Esquema 1 IRAM-ISO/IEC 27001:2007

G. Concepto de Evaluación de Impacto

H. Concepto de Disociación de datos

A. Informe COSO – Sistema de Control Interno y su relación con la información y el cumplimiento.

La SIGEN, como órgano rector del Sistema de Control Interno del Poder Ejecutivo Nacional, normativo, de supervisión y coordinación, emitió la Resolución N° 107/98, por medio de la cual se aprobaron las *"Normas de Control Interno"*, de aplicación en todo el ámbito del Poder Ejecutivo Nacional, como base de la responsabilidad que la Ley Nacional N° 24.156 impone a la administración superior de cada jurisdicción o entidad del Sector Público Nacional.

La mencionada resolución recoge el denominado Informe COSO[5], el cual define al Control Interno como un proceso integrado a los procesos, efectuado por el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos de las siguientes categorías:

- Eficacia y eficiencia de las operaciones
- Confiabilidad de la información financiera y no financiera
- Cumplimiento de las leyes reglamentos y políticas.

Asimismo, el marco integrado de control que plantea, consta de cinco componentes interrelacionados, a saber:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control

[5] Committee of Sponsoring Organizations of the Treadway

- Información y comunicación
- Supervisión

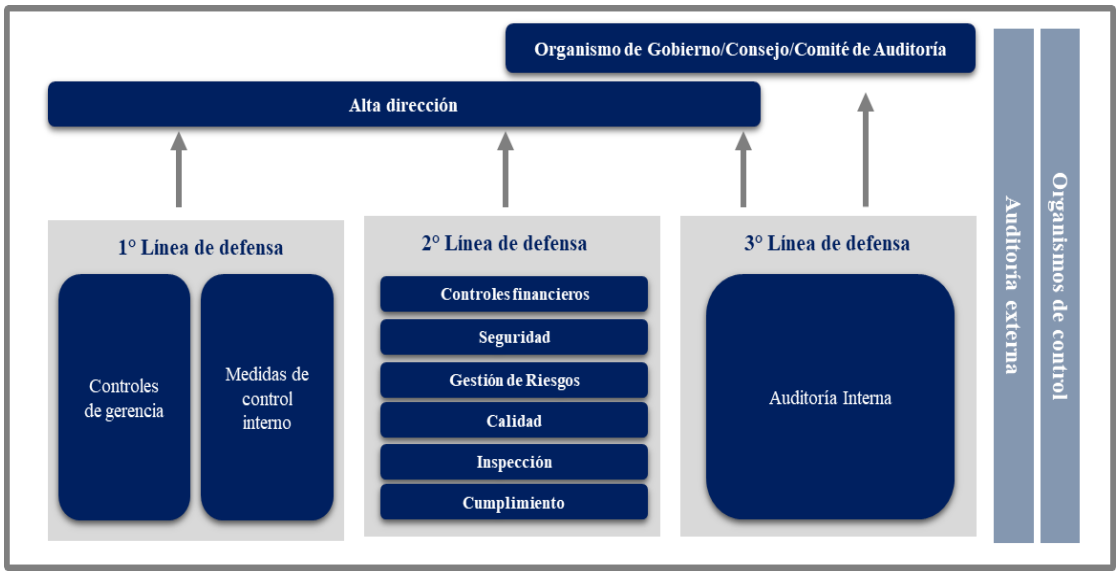
Siendo la UAI la responsable de la evaluación independiente del Sistema de Control Interno del Organismo, sus procesos deben estar actualizados y alineados a los cambios tecnológicos, ya que su evaluación impactará en las acciones llevadas a cabo por el Organismo.

B. Interrelación de las tres líneas de defensa y los principios del informe COSO

En las organizaciones del siglo XXI, no es raro encontrar diversos equipos de auditores internos, especialistas en gestión de riesgos corporativos, oficiales de cumplimiento, especialistas en control interno, inspectores de calidad, investigadores de fraude y otros profesionales del riesgo y del control, trabajando juntos para ayudar a sus organizaciones a gestionar el riesgo.

En el modelo de las Tres Líneas de Defensa, el control de la gerencia es la primera línea de defensa en la gestión de riesgos; las varias funciones de supervisión de riesgos, controles y cumplimiento establecidas por la administración, son la segunda línea de defensa; y el aseguramiento independiente es la tercera. Cada una de estas "líneas" juega un papel distinto dentro del marco amplio de gobernabilidad de la organización.

PRIMER MODELO DE LAS TRES LINEAS DE DEFENSA



Adaptado de la Guía emitida por ECIIA/FERMA
sobre la 8va Directiva de Derecho de Sociedades de la Unión Europea, artículo 41

Particularmente la tercera línea de defensa es la que, por medio de los auditores internos, proporcionan a los organismos de gobierno corporativo y a la alta dirección un aseguramiento comprensivo basado en el más alto nivel de independencia y objetividad dentro de la organización.

Ahora bien, este esquema de las tres líneas de defensa, fue actualizado por el Instituto de Auditores, ofreciendo una mayor integración de las funciones de aseguramiento que pueden aportar eficacia y eficiencia en cuanto a la gestión de los riesgos y mayor confort a los órganos de gobierno. Pero, por otra parte, exigirá el establecimiento de mayores mecanismos de coordinación y de salvaguarda para preservar la independencia de las distintas líneas.

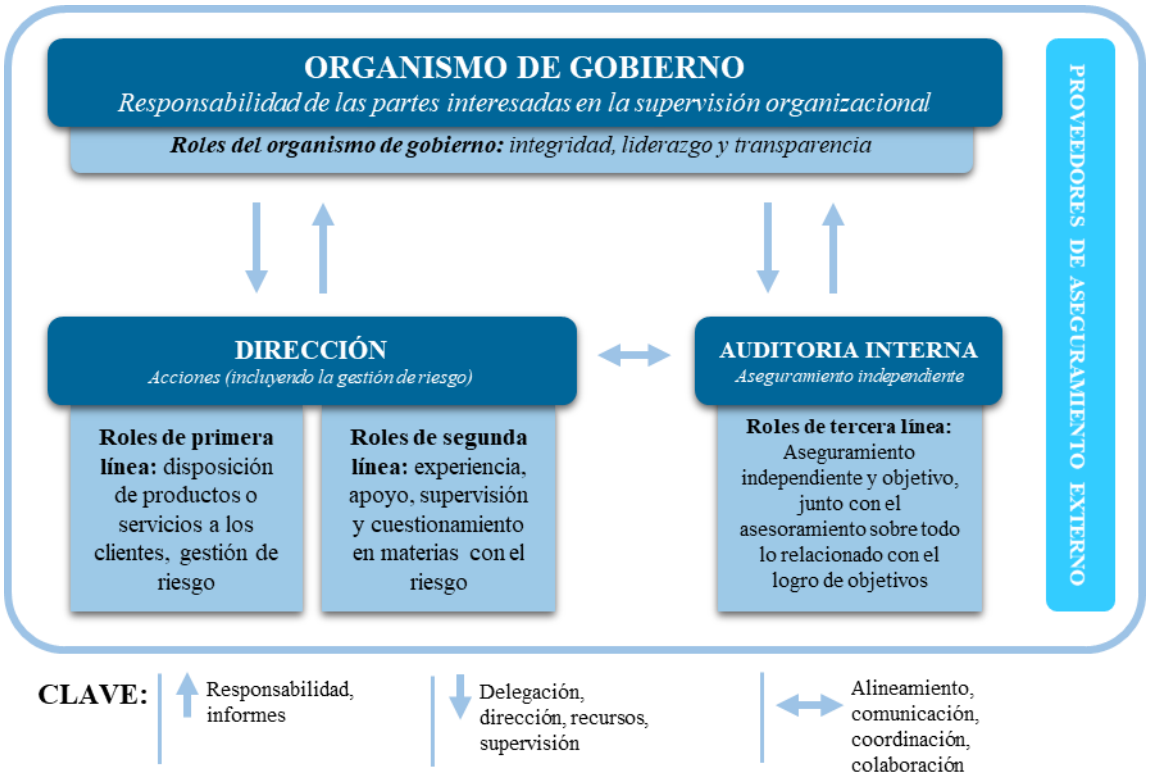
La aparición del nuevo marco de referencia (COSO – Principios), recogidos también por la SIGEN en su Resolución SIGEN 172/14, llevó a la redefinición de las 3 líneas de defensa orientada a la aplicación de 17 principios de control, repartidos en cinco elementos que estructuran el sistema de control interno, sobre tres componentes claves:

eficiencia operacional; reportes internos y externos y cumplimiento de leyes y regulaciones; lo cual implicó la revisión, en algunas organizaciones, de temas diversos tales como: el enfoque de gestión de riesgos, la estructura de gobierno corporativo, la calidad de la rendición de cuentas, la efectividad de los sistemas de prevención de fraude y de lavado de activos, la cobertura de los planes de capacitación, entre muchos otros elementos.

Sus objetivos refieren a: asegurar la consistencia y factibilidad de un marco de referencia institucional, cambiar comportamientos de forma sostenible, implantar un modelo de líneas de defensa eficiente y lo menos costoso posible, integrar la visión de riesgos, procesos y controles, justificar la inversión con análisis sustentados.

El nuevo modelo de las tres líneas de defensa realza el entendimiento del manejo de riesgos y controles mediante la asignación o clarificación de roles y responsabilidades a través de toda la organización.

MODELO DE LAS TRES LÍNEAS DE DEFENSA - IIA 2020 -



La primera línea debe gestionar los riesgos y controles: la cultura de control debe enfocarse a que las Unidades de Negocio u organizacionales internalicen que ellas tienen la principal responsabilidad en materia de control.

La segunda línea monitorea los riesgos y controles que soportan el manejo de las funciones de las Unidades de Prevención y Control.

La tercera línea de defensa tiene como misión proveer aseguramiento independiente a la Junta Directiva y a la Alta Administración con respecto a la efectividad del manejo de riesgos y controles. En este sentido, la visión de la auditoría interna y sus capacidades actuales, deben servir para el análisis de aquellas áreas, subsidiarias, productos y servicios, infraestructura de TI relevantes y que inciden en la definición de una cobertura amplia del plan anual de la unidad que sirva a las expectativas de las partes interesadas y se alinee con la estrategia del negocio. (Instituto de Auditores Internos - Artículo de Bismark Rodríguez 2016).

Es en este nuevo contexto, donde la Auditoría tiene una relación bidireccional directa tanto con el Organismo de Gobierno como con la Dirección, es evidente una mayor responsabilidad, tanto hacia la Organización bajo su evaluación como en la responsabilidad de mantener optimizados los procesos internos e incorporación de nuevas metodologías y tecnologías para asegurar el cumplimiento y la transparencia.

Por último, debe destacarse que el nuevo modelo se incorpora el concepto de Proveedores de Aseguramiento Externo.

C. Informe de Auditoría – Manual de Control Interno Gubernamental

Conforme lo establece el Manual de Control Interno Gubernamental, emitido por la SIGEN, el Informe Final de Auditoría es el producto último del auditor, por medio del cual expone sus observaciones, conclusiones y recomendaciones por escrito y que es remitido a distintos funcionarios según corresponda.

El mismo debe contener juicios fundamentados en las evidencias obtenidas a lo largo del examen con el objeto de brindar suficiente información acerca de los desvíos o deficiencias más importantes, así como recomendar mejoras en la conducción de las actividades y ejecución de las operaciones.

Este informe brinda una buena oportunidad para captar la atención de los niveles administrativos de la institución auditada y para mostrar los beneficios que le ofrece este tipo de examen.

Cubre dos funciones básicas:

- Comunica los resultados de la evaluación del sistema de control interno, de la auditoría de gestión y del cumplimiento de la normativa vigente; y
- Persuade a la Dirección del Organismo para adoptar determinadas acciones y, cuando es necesario llama su atención, respecto de algunos problemas que podrían afectar adversamente sus actividades y operaciones.

Es necesario tener en cuenta determinadas características en el momento de elaborar los informes, con el objeto de mantener un suficiente nivel de calidad. Por lo tanto, se recomienda considerar las siguientes características: importancia del contenido, completo y suficiente, útil, oportuno, objetivo, que posea equidad, de calidad convincente, claro, simple, conciso y con un tono constructivo.

En el marco de dichas características, el informe puede contener información que identifique datos personales o sensibles de los ciudadanos. En algunas ocasiones dichos datos resultan necesarios en el detalle de la observación, como evidencia de la evaluación detectada por la UAI. Cabe mencionar, que de acuerdo a la temática que se encuentre bajo evaluación, dichos datos resultan indispensables para la corrección por parte de las áreas auditadas, con el fin de revertir el desvío detectado.

D. Legislación Nacional - Ley Nacional de Protección de Datos Personales Habeas Data

La Ley Nacional N° 25.326, denominada Habeas Data, tiene como objeto la protección de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos 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 art. 43, párrafo tercero de la Constitución Nacional.

En su art. 2, la Ley Nacional define a los datos personales como aquella información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinables.

En este aspecto es destacable mencionar lo establecido por la Ley Orgánica de Protección de Datos Personales de España[6], la cual en su art. 3 inc a) define el dato personal como "cualquier información concerniente a personas físicas identificadas o identificables". Asimismo, en su art. 5.1.f) del Reglamento de dicha ley, indica que el dato personal es "cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables"

Refiriendo nuevamente a la Ley Nacional, y en relación a los Datos Sensibles, la misma los define como aquellos datos que revelan origen racial o étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.

En relación al tratamiento de los datos, la misma refiere a aquellas operaciones y procedimientos sistemáticos, electrónicos o no que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo,

[6] Ley Orgánica 15/1999.

destrucción, y en general el procesamiento de datos personales, como así también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

En dicho encuadre, los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación al ámbito y finalidad para los que se hubieren obtenido. Por cuanto los datos deber ser exactos y actualizarse en el caso de que ello fuera necesario.

Es en su Capítulo II sobre Principios generales relativos a la protección de datos, que se establecen los relativos a los Archivos de datos y su Licitud, la calidad de los datos, el consentimiento para el tratamiento de los datos, la información sobre la finalidad para lo cual se recaban los datos, la categoría de datos, los datos relativos a la salud, la seguridad de los datos, el deber de confidencialidad, los criterios para la cesión de los datos y la transferencia internacional de los datos personales.

Sin perjuicio de lo establecido por la ley en sus diversos capítulos, la misma contempla en su art. 17 las correspondientes excepciones en tres incisos referidos a:

1. Los responsables o usuarios de bancos de datos públicos pueden, mediante decisión fundada, 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.

2. La información sobre datos personales también puede ser denegada por los responsables o usuarios de bancos de datos públicos, cuando de tal modo se pudieran obstaculizar actuaciones judiciales o administrativas en curso vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones de control de la salud y de medio ambiente, la investigación de delitos penales y la verificación de infracciones administrativas. La resolución que así lo disponga debe ser fundada y notificada al afectado.

3. Sin perjuicio de lo establecido en los incisos anteriores, se deberá brindar acceso a los registros en cuestión en la oportunidad que el afectado tenga que ejercer su derecho a defensa.

En Organismos donde se administran, gestionan y tratan datos personales y/o sensibles, de acuerdo al objeto que la Auditoría haya determinado evaluar en su planificación, existe la posibilidad que, de acuerdo a la evaluación de riesgos realizada previamente, deban incluirse datos sensibles como por ejemplo aquellos relacionados con salud, elección de sexualidad o datos personales nombre y apellidos, domicilio, dirección de correo electrónico, número de documento nacional de identidad u otros datos.

E. Legislación Nacional – Derecho de Acceso a la Información Pública y su relación con los informes de Auditoría

La Ley Nacional 27.275 tiene como objeto garantizar el efectivo ejercicio del derecho de acceso a la información pública, promover la participación ciudadana y la transparencia de la gestión pública, y se funda en los siguientes principios: presunción de publicidad, transparencia y máxima divulgación, informalismo, máximo acceso, apertura, disociación, no discriminación, máxima premura, gratuidad, control, responsabilidad, alcance limitado de las excepciones, In dubio pro petitor (a favor de la mayor vigencia y alcance del derecho a la información), facilitación y por último buena fe.

Por régimen general, la Ley establece que el derecho de acceso a la información pública comprende la posibilidad de buscar, acceder, solicitar, recibir, copiar, analizar, reprocesar, reutilizar y redistribuir libremente la información bajo custodia de los sujetos obligados enumerados en el art. 7°, como así con las únicas limitaciones y excepciones de la Ley.

Lo mencionado, en el párrafo precedente, establece el Ámbito de Aplicación, es decir los sujetos obligados a brindar información pública:

a) La administración pública nacional, conformada por la administración central y los organismos descentralizados, comprendiendo en estos últimos a las instituciones de seguridad social.

b) El Poder Judicial de la Nación

c) El Poder Legislativo y los órganos que funcionan en su ámbito

d) El Ministerio Público Fiscal de la Nación

e) El Ministerio Público de la Defensa

f) El consejo de la Magistratura

g) Las empresas y sociedades del Estado que abarcan a las empresas del Estado, las sociedades del Estado, las sociedades anónimas con participación estatal mayoritaria, las sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el Estado Nacional tenga participación mayoritaria en el capital o en la formación de las decisiones societarias.

h) Las empresas y sociedades en las cuales el Estado Nacional tenga una participación minoritaria, pero sólo en lo referido a la participación estatal.

i) Concesionarios, permisionarios y licenciatarios de servicios públicos o concesionarios permisionarios de uso del dominio público, en la medida en que cumplan servicios públicos y en todo aquello que corresponda al ejercicio de la función administrativa delegada; y contratistas, prestadores y prestatarios bajo cualquier otra forma o modalidad contractual;

j) Organizaciones empresariales, partidos políticos, sindicatos, universidades y cualquier entidad privada a la que se le hayan otorgado fondos públicos, en lo que se refiera, únicamente, a la información producida total o parcialmente o relacionada con los fondos públicos recibidos.

k) Instituciones o fondos cuya administración, guarda o conservación esté a cargo del Estado Nacional

l) Personas jurídicas públicas no estatales en todo aquello que estuviese regulado por el derecho público, y en lo que se refiera a la información producida o relacionada con los fondos públicos recibidos;

m) Fideicomisos que se constituyeren total o parcialmente con recurso o bienes del Estado Nacional;

n) Los entes cooperadores con los que la administración pública nacional hubiera celebrado o celebre convenios que tengan por objeto la cooperación técnica o financiera con organismos estatales;

o) El Banco Central de la República Argentina

p) Los entes interjurisdiccionales en los que el Estado Nacional tenga participación o presentación;

q) Los concesionarios, explotadores, administradores y operadores de juegos de azar, destreza y apuesta, debidamente autorizados por autoridad competente.

En su art. 8° se determinan las excepciones por medio de las cuales los sujetos obligados sólo podrán exceptuarse de proveer la información cuando se configure alguno en los supuestos determinados en dicho artículo.

Particularmente para el objetivo a lograr, es de resaltar que dentro de las excepciones que la Ley establece en su art. 8° inc. i) se encuentra aquella relacionada con la "*excepción de brindar información aquella que contenga datos personales y no puede brindarse aplicando procedimientos de disociación, salvo que se cumpla con las condiciones de licitud previstas en la Ley 25.326 de protección de datos personales y sus modificatorias.*"

En cuanto a las responsabilidades (art. 18), la Ley de Derecho de Acceso a la Información Pública, establece que el funcionario público o agente responsable que en forma arbitraria obstruya el acceso del solicitante a la información pública requerida, o la suministre en forma incompleta u obstaculice de cualquier modo el cumplimento de la ley, incurre en

falta grave sin perjuicio de las responsabilidades administrativas, patrimoniales y penales que pudieran caberle conforme lo previsto en las normas vigentes.

Por último, es dable destacar, que el Titulo II que establece la Transparencia Activa por medio de la cual los sujetos obligados enumerados en el art. 7°, con excepción de los indicados en sus incisos i) y q), deberán facilitar la búsqueda y el acceso a la información pública a través de su página oficial de la red informática, de una manera clara, estructurada y entendible para los interesados y procurando remover toda barrera que obstaculice o dificulte su reutilización por parte de terceros. Asimismo, los sujetos obligados deberán publicar en forma completa actualizada, por medios digitales y en formatos abiertos.

De los incisos mencionados por la Ley, es importante mencionar el inc. i) referido a los informes de auditoría, evaluaciones, internas y externas, realizadas previamente, durante o posteriormente, referidas al propio organismo, sus programas, proyectos y actividades.

F. Agencia de Acceso a la Información Pública y su relación con los datos personales

El derecho de acceso a la información pública se encuentra consagrado en los principales instrumentos internacionales de Derechos Humanos, tales como la Declaración Universal de Derechos Humanos, el Pacto Internacional de Derechos Civiles y Políticos y la Convención Americana de Derechos Humanos, los que tienen recepción en nuestro ordenamiento constitucional a través del artículo 75 inciso 22 C.N.

En el ámbito del Ministerio Público Fiscal de la Nación -mediante Resolución PGN N° 914/13- se creó el “Plan de Transparencia Institucional” estableciendo, además de plantear la necesidad de mejorar los mecanismos de acceso a la información y participación ciudadana, el portal de datos abiertos del Organismo, hoy conocido como Portal de Transparencia.

En septiembre de 2016 se sancionó la Ley 27.275 de Derecho de Acceso a la Información Pública con el objeto de garantizar el efectivo ejercicio del acceso a la información, promover la participación ciudadana y la transparencia de la gestión pública de todos los poderes y organismos del Estado Argentino.

La norma prevé la creación de diversas Agencias de Acceso a la Información Pública y específicamente, en la órbita del sistema de administración de Justicia, identifica al Ministerio Público Fiscal como uno de los sujetos obligados.

En función de ello, en septiembre de 2017 la Resolución PGN N° 2757/17 creó, en la órbita del MPF, la Agencia de Acceso a la Información Pública (AAIP) y dispuso la implementación de un proceso de selección abierto, público y transparente de su director, nominación que –según se estableció- debe recaer en un fiscal general de la institución.

Entre las funciones de la Agencia de Acceso a la Información Pública se encuentran: implementar una plataforma tecnológica para la gestión de las solicitudes de información y sus correspondientes respuestas, requerir a los sujetos obligados que modifiquen o adecuen su organización, procedimientos, sistemas de atención al público y recepción de correspondencia a la normativa aplicable a los fines de cumplir con el objeto de la presente ley, proveer un canal de comunicación con la ciudadanía con el objeto de prestar asesoramiento sobre las solicitudes de información pública y, en particular, colaborando en el direccionamiento del pedido y refinamiento de la búsqueda, elaborar y publicar estadísticas periódicas sobre requirentes, información pública solicitada, cantidad de denegatorias y cualquier otra cuestión que permita el control ciudadano a lo establecido por la presente ley, publicar periódicamente un índice y listado de la información pública frecuentemente requerida que permita atender consultas y solicitudes de información por vía de la página oficial de la red informática de la Agencia de Acceso a la Información Pública, publicar un informe anual de rendición de cuentas de gestión, elaborar criterios orientadores e indicadores de mejores prácticas destinados a los sujetos obligados, elaborar y presentar ante el Honorable Congreso de la Nación propuestas de reforma legislativa respecto de su área de competencia.

Un dato importante, surge de la estructura de la mencionada la Agencia, la cual posee la Dirección Nacional de Protección de Datos Personales. En relación a ésta última, es por RESOL-2018-47-APN-AAIP que se establecen las medidas de seguridad recomendadas para el tratamiento y conservación de los datos personales en medios informatizados y medios no informatizados. Dichas medidas, tal cual refiere la normativa, son a modo referencial y tienen como objetivo facilitar el cumplimiento de la Ley N° 25.326 de Protección de los Datos Personales.

En relación a los informes de Auditoría, las mismas se encuentran incorporadas en dichos cumplimientos, de manera eficaz y efectiva.

G. Concepto de Evaluación de Impacto

Fruto del trabajo conjunto entre la Agencia de Acceso a la Información Pública de la República Argentina y la Unidad Reguladora y de Control de Datos Personales de Uruguay, se publicó la guía "Evaluación de Impacto en la Protección de Datos" (EIPD), documento que orienta a las empresas y organismos públicos para que, desde una etapa temprana, las prácticas y proyectos que puedan afectar los derechos de las personas sean evaluados y constituidos de acuerdo a ciertos criterios de seguridad e integridad.

El manual de evaluación de impacto reúne las legislaciones y guías más recientes, particularmente las leyes de los Estados miembro de la Unión Europea y de los Estados parte del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal. Dicho convenio ha sido suscripto y ratificado por Argentina en el año 2019.

Conforme la Guía mencionada, 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 actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales. Ello considerando que, el tratamiento de datos personales puede provocar impactos en los derechos de las

personas que deben ser de algún modo identificados, gestionados, minimizados o eliminados para cumplir con la normativa vigente.

Para que este proceso resulte exitoso, es necesario involucrar a las personas que integran la organización, a consultores expertos e incluso a los sectores o grupos de titulares de datos que posiblemente puedan ser afectados. (Guía de Evaluación de Impacto en la Protección de Datos EIPD).

Dicha metodología establece que se debe asegurar la homogeneidad y comparabilidad de los resultados, mediante un proceso sistemático y repetible, garantizando así la objetividad del proceso.

En tal sentido se desarrollan los pasos a seguir para la determinación de participantes y documentación de los procesos de elaboración de la EIPD, el análisis normativo aplicables, el análisis preliminar, el contexto del tratamiento, las etapas del ciclo de vida de los datos, la gestión de riesgos, la identificación del riesgo, su evaluación y el plan de tratamiento de los mismos.

Esta metodología, que tiene la finalidad de dar un marco de referencia, una guía, a las organizaciones que deben tratar datos personales, es también, en el marco de las tareas de las UAI, un "input" sumamente importante, al momento de evaluar los datos contenidos en sus informes, como se analizará en el desarrollo del presente trabajo.

H. Concepto de Disociación de datos

Conforme la Guía emitida por la Agencia de Acceso a la Información Pública y Uruguay, previamente indicada, la Disociación de Datos es una operación que permite que la información obtenida no pueda asociarse a persona determinada o determinable.

Por su parte la Ley de Acceso a la Información Pública (Ley Nacional N° 27.275) en su Art. 1 establece: "*en aquel caso en el que parte de la información se encuadre dentro de las excepciones taxativamente establecidas por esta Ley, la información no exceptuada*

debe ser publicada en una versión del documento que tache, oculte o disocie aquellas partes sujetas a la excepción."

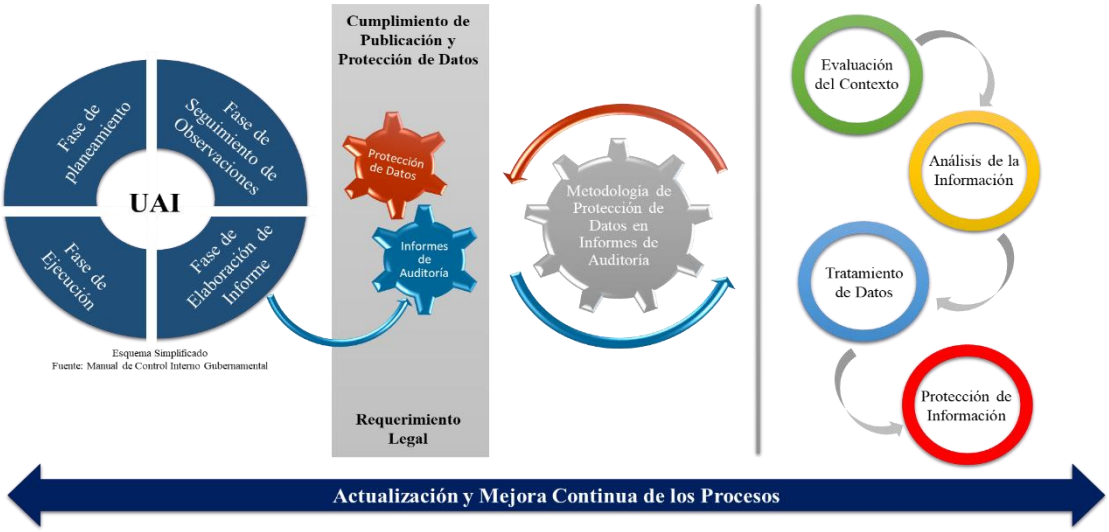
Lo mencionado ut supra, resulta importante en consideración a la Transparencia y a la Máxima divulgación en relación a que la información en poder, custodia o bajo control del sujeto obligado debe ser accesible para todas las personas. Por ello sólo será limitado dicho acceso, cuando concurra alguna de las excepciones previstas en la Ley.

6. DESARROLLO

El presente trabajo surge del análisis y evaluación de las normativas, legislación y buenas prácticas relacionadas con el cumplimiento, los procesos y de la detección temprana de optimizar los procedimientos de las UAI, en relación al tratamiento que debe darse a los datos personales/sensibles contenidos en los informes, los cuales son de publicación obligatoria o factibles de requerimiento por parte de terceros interesados.

A partir del análisis del marco teórico y contexto, se elaboró una propuesta metodológica, para el presente trabajo, que permite integrar los informes de Auditoría y la protección de datos personales, cuyo esquema se expone a continuación:

ESQUEMA DE INTEGRACIÓN METODOLÓGICA



Esquema y gráfico de elaboración propia.

6.1 Introducción y conceptos

Para abordar la metodología, resultó necesario integrar tanto el análisis de la legislación y normativa, los procesos existentes en la UAI, la necesidad de la protección de los datos de los ciudadanos en los informes emitidos por las mismas y por último identificar los pasos necesarios para formalizar una metodología de protección de datos para informes de Auditoría.

La determinación de las etapas fue considerada desde el análisis del marco teórico pero particularmente poniendo foco en las normas ISO/IRAM 31000 (Gestión de Riesgo), ISO/IEC 27000 (Seguridad de la Información) y específicamente la Norma ISO/IEC 27701 (Sistema de Gestión de Información de Privacidad).

Teniendo en cuenta que la labor de la auditoría no contemplaba, hasta la publicación de la legislación mencionada, la exposición pública de sus informes, se consideró necesario, partiendo de informes de auditoría ya emitidos como aquellos contenidos en futuros planes anuales de las UAI, incorporar en sus procesos la protección de los datos personales a fin que la metodología resulte efectiva y eficiente.

Complementariamente, se consideró la Guía de Evaluación de Impacto sobre la protección de datos personales (EIDP), cuyo análisis permitió, a partir de la herramienta brindada por la guía, adecuar la estructura de la misma a fin de obtener una herramienta de autoevaluación del contexto, etapa integrante de la metodología.

Sin perjuicio que no resulta materia del presente trabajo específicamente el tratamiento de disociación, sino la determinación de los datos que sí deben ser disociados, la Auditoría debería asegurar el cumplimiento y la ejecución de dicho tratamiento.

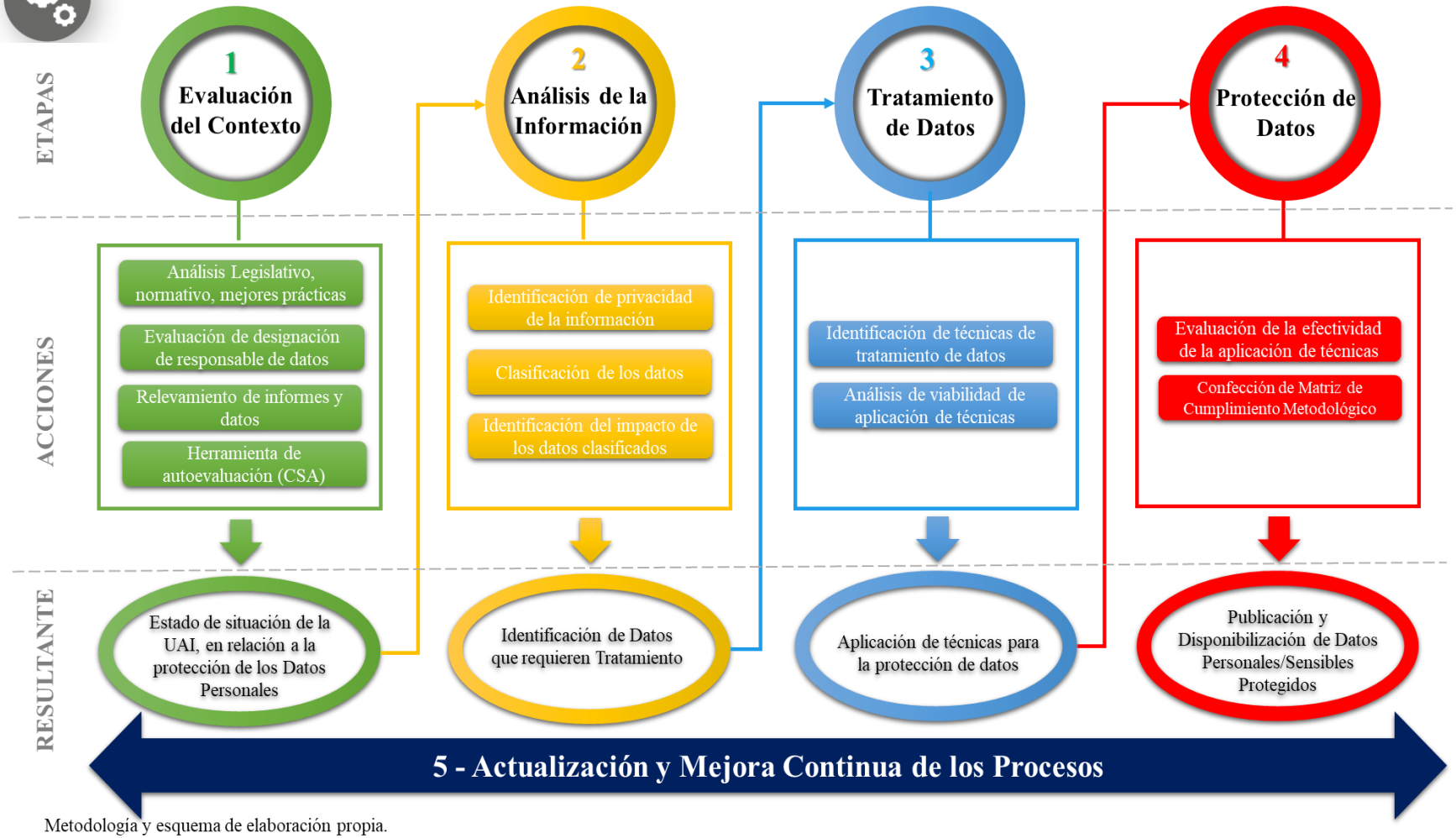
Por último, no resulta menor volver a destacar que cada etapa de la metodología fue conceptualizada desde el requisito de integridad, es decir, que cada resultante de cada etapa sea un suministro de la etapa siguiente y a su vez retroalimente la actualización y mejora continua de los procesos.

Las etapas que componen la metodología son 4 y refieren a:

1- Evaluación del Contexto.
2- Análisis de la Información.
3- Tratamiento de Datos.
4- Protección de Datos.
5- Actualización y Mejora Continua de los procesos.

Se adjunta seguidamente el gráfico de la metodología y la interacción entre las etapas.

ESQUEMA DE LA METODOLOGÍA



Metodología y esquema de elaboración propia.

6.1 Etapa 1 - Evaluación del Contexto

La Norma ISO/IEC 31000 define el establecimiento del contexto como aquellos parámetros básicos para gestionar el riesgo y establece el alcance y los criterios para el resto del proceso. Esto incluye tanto parámetros internos como externos pertinentes a la Organización.

Considerando dicho proceso, las UAI debieran realizar el análisis legislativo, normativo y de mejores prácticas, la evaluación de la pertinencia de una designación de responsable del análisis de los datos susceptibles de tratamiento, relevamiento de informes y datos, y por último realizar una autoevaluación (Control Self Assesment - CSA) con dicha información, además incorporar mejores prácticas para optimizar este procedimiento, como ser el "Benchmarking".

Los aspectos que se desarrollarán no conforman una lista ni definiciones taxativas, pudiendo ser ampliadas o profundizadas por las UAI, de acuerdo a las misiones y funciones que posea el Organismo donde desarrolla su función.

Como resultante de esta etapa, la UAI debiera obtener un estado de situación, en relación a la protección de los Datos Personales, contenidos en sus informes de Auditoría.

Es importante tener presente que esta etapa, como consecuencia de la aplicación de la actualización y mejora continua, estará en constante monitoreo y revisión a fin de retroalimentar las etapas subsiguientes.

El contexto externo es el más influyente tanto para la Organización como para la UAI y resulta el más impredecible para la implementación de actividades preventivas, por lo cual requiere mayor monitoreo y actualización.

En relación a la reglamentación sobre la Protección de los Datos Personales y al Derecho de Acceso a la Información Pública, las UAI deben estar en continua actualización por dos principales propósitos, por un lado, porque en el caso particular requiere de acciones

inmediatas por parte de la UAI para no incurrir en un incumplimiento que podría traer hasta consecuencias legales, pero por otro lado, la mencionada actualización debiera ser parte integrante de la mejora continua que todas las UAI deben perseguir.

6.1.1 Análisis de la legislación, normativa y mejores prácticas

Tanto la Ley de Habeas Data cuanto la Ley de Derecho de Acceso a la Información Pública, constituyen elementos fundamentales para entender por qué la facultad de decidir sobre el manejo, control y exposición de la información revierte para el Estado un papel fundamental e indelegable ante la Sociedad.

El art. 11 de la Ley Nº 25.326 (Habeas Data), establece como principio general de protección de datos personales la obligación de requerir el consentimiento previo del titular para la cesión de datos personales. A este principio se le aplican las excepciones reguladas en el inc. 3 del mismo artículo, cuyo apartado "c" dispone que no será exigido el consentimiento cuando "se realice entre dependencias de los órganos del Estado en forma directa, en la medida del cumplimiento de sus respectivas competencias".

Es por ello que, en lo referente a dicha excepcionalidad, la responsabilidad de los Organismos sobre la protección de los datos personales y/o sensibles revierte mayor importancia, dado que no requerirán el consentimiento del titular de los datos para su tratamiento, uso y exposición.

Esta responsabilidad, que solamente refería al tratamiento de los datos, actualmente con la promulgación de la Ley Nacional 27.275 Derecho de Acceso a la Información Pública, impacta también en la responsabilidad que le cabe a la Auditoría, en relación a la publicación de dichos datos, en las páginas institucionales o ante un requerimiento de terceros interesados.

Sumado a lo expuesto, la UAI deberá considerar también su rol en la actualización de las "Tres Líneas de Defensa", las cuales posicionan a las UAI en una relación bidireccional con la Dirección (Gestión), que incluye acciones de gestión de riesgos, como con el

Organismo de Gobierno (Gobernabilidad), el cual contempla en sus roles de gobierno conceptos como integridad, liderazgo y transparencia.

En esta bidireccionalidad entre el Organismo de Gobierno y las UAI, adquieren relevancia y mayor responsabilidad en la manera en que éstas últimas ejecutan y actualizan sus procesos y procedimientos.

Por otra parte, es importante delimitar, como es de conocimiento, que las UAI, por independencia y transparencia, no intervienen ni participan de la gestión de riesgos y la definición de sus tratamientos de la Organización, ya que resulta una tarea incompatible con su función, pero no la exime de desarrollar procedimientos de gestión de riesgos de sus propios procesos.

Cuando las tecnologías avanzan abruptamente, como fue el caso de los últimos dos años donde fue decretada la pandemia, con la finalidad de continuar la operatividad, los Organismos debieron modificar sus procesos, procedimientos y tecnología hacia la virtualidad y poder reemplazar, en algunos casos, la atención presencial sin discontinuar los servicios, información y atención que brindaba a los ciudadanos.

Esta situación no menor, requiere de una actualización continua por parte de la UAI, dado los cambios emergentes y las posibles vulneraciones de controles en los procesos ante los cambios, máxime si se tiene en cuenta que en relación a la disponibilidad de los datos, el reconocimiento de la intimidad de las personas es crítico al momento de proteger y permitir a los ciudadanos ejercer otros derechos que se derivan de su privacidad.

Es en este punto, donde las UAI, a fin de brindar valor agregado a la Organización, debieran contemplar las mejores prácticas que llevan al trabajo de los auditores a una mejora continua, que asegure que la información que se publicará o expondrá no posee errores de revelación inadecuada o no correspondiente conforme la legislación, ya que ello lleva, además de un incumplimiento a una vulneración de los derechos de los ciudadanos a su privacidad.

Las UAI deben contar con auditores especialistas en protección de datos que integren tanto los conocimientos legislativos/normativos como aquellos aspectos relacionados con los procesos de EIPD. Asimismo, resulta valorable el auditor de sistemas especialista en seguridad informática, lo que permitirá aconsejar sobre las medidas de seguridad, así como para detectar riesgos informáticos potenciales.

En resumen, en esta sub etapa, las UAI debieran monitorear y evaluar el impacto ante la detección de:

- Nueva legislación que impacte en la administración, gestión y protección de los datos personales.
- Mejores prácticas emitidas por Organismos de Contralor / Institutos de Auditores.
- Modificación de legislación vigente.
- Desactualización normativa interna.
- Nuevas normas de procedimiento interna.

Esta enumeración no debe considerarse de manera taxativa, sino orientativa.

Adicionalmente, las UAI debieran asegurarse que los auditores posean capacitaciones específicas relacionadas a la privacidad de los datos personales, a través de cursos o talleres.

6.1.2. Evaluación de designación de responsabilidad sobre los datos

Las UAI pueden contar con distintas estructuras orgánicas, por lo cual, adicionalmente a la cantidad de recursos humanos con los que cuente, impactará en este ítem la existencia de un área legal y/o de sistemas.

Por otro lado, la cultura que posea cada UAI, en cuanto a competencias, influirá en la definición de la/s persona/s a la cual/es se les asigne la responsabilidad de identificar en los informes aquellos datos que requerirán tratamiento para su protección.

Puede existir la posibilidad que el responsable de la emisión del informe, quien conoce la especialidad auditada, sea el responsable de dicha acción.

Sin perjuicio de cualquiera de las situaciones con que cada UAI se identifique, resulta imprescindible, para lograr un control e identificación efectivo de los datos personales / sensibles que requieren tratamiento para su protección, que la/s persona/s responsable/s cuenten como mínimo con las siguientes características, lo que permitirá asegurar el derecho de la privacidad.

- Conocimiento y actualización continua de la legislación sobre Protección de Datos Personales y Derecho a la Información Pública.
- Conocimiento y actualización continua de las distintas técnicas que pueden aplicarse a los datos personales/sensibles.
- Sólidos conocimientos y actualización continua sobre las técnicas de auditoría.

6.1.3 Identificación de informes y datos

Entre las tareas que deben desarrollar las UAI, se encuentran aquellas relacionadas con el relevamiento de los informes emitidos, a fin de poder determinar la existencia de la totalidad de los informes. Esto obedece a que la legislación permite la solicitud de informes emitidos en años anteriores y las UAI debieran tener acceso a los mismos.

De detectarse la ausencia de algún informe, la UAI deberá arbitrar las medidas necesarias para obtener los mismos, a fin de no incurrir en un incumplimiento relacionados con su publicación y disponibilidad conforme la legislación.

En relación a la guarda de los informes, la UAI debe evaluar qué medidas de seguridad posee el ambiente donde se encuentran alojados los informes y si los accesos a la base de informes, se encuentran correctamente administrados y restringidos exclusivamente a personal de la UAI. Este relevamiento refiere a la confidencialidad de la información que posee la UAI, ya que estos informes pueden contener datos personales que aún no han sido identificados como sensibles y por ende no protegidos.

En otra instancia del relevamiento, debe considerarse el contenido de los informes, identificando la existencia de datos personales/sensibles, y si los mismos se encuentran en el cuerpo principal o anexos del informe, dado que aquellos datos que se encuentren en un Anexo, permitirán a las UAI evaluar su tratamiento.

Las UAI deben analizar la factibilidad de anonimización de los datos personales de acuerdo al formato en que se encuentren los informes, considerando como iniciales aquellas técnicas con procedimientos automáticos y como última alternativa la opción de anonimizar los datos por medio de ocultar los mismos ("Tachar el dato").

Asimismo, deben identificar correctamente aquellos datos que son considerados personales sensibles los cuales no deben ser omitidos para su tratamiento a fin de evitar la exposición de la privacidad de los ciudadanos.

6.1.4 Herramienta de Autoevaluación

La norma SIGEN IRAM Referencial N° 13, sobre la calidad de las UAI, incorpora en su ítem 9 la autoevaluación cuyo propósito es la realización de una revisión sistemática de las actividades de la UAI y de su desempeño verificando el cumplimiento de los requisitos, la implementación y el mantenimiento eficaz del sistema y el enfoque de mejora continua.

La autoevaluación de control (CSA por sus siglas en inglés) se constituye como un proceso a través del cual se examina y evalúa la efectividad del control interno con el objetivo de proporcionar seguridad razonable de que todos los objetivos de negocio serán alcanzados.

En ese sentido, dentro de la autoevaluación pueden incorporarse mejores prácticas que sirven de comparación para determinar la situación en que se encuentra la Auditoría.

Una de las prácticas más comunes la constituye el Benchmarking, la cual obedece a un *"proceso de comparación y medición de las operaciones o procesos internos de una organización versus los de un representante mejor de su clase y de su sector"*. Al evaluar

y recomendar esas mejores prácticas que se aplican de manera eficiente y eficaz contribuya al objetivo primordial de la auditoría, como es el mejoramiento continuo de la organización, que sin duda se considerará como aporte valioso o valor agregado de su labor de auditoría y control.

En muchos casos, las UAI desarrollan sus tareas en Organismos cuyas misiones, funciones y objetivos lo constituyen como únicos en el país como puede citarse las tareas desarrolladas por ANSES, AFIP, Migraciones, Ministerio de Salud, etc. Particularmente en lo que refiere a la protección de los datos personales y el derecho al acceso a la información pública o requerimientos de terceros interesados, la situación cambia exponencialmente, dado que las técnicas de protección de datos son generales, independientemente de las misiones y funciones que poseen los distintos Organismos.

En tal sentido, para la Auditoría que aún no se encuentra preparada o no ha optimizado sus procesos de protección de datos personales contenidos en sus informes, encarar acciones de Benchmarking con otras UAI, puede permitirles evaluar sus fortalezas y debilidades. Se recomienda realizarlo con aquellas UAI que se encuentran certificadas en procedimientos de calidad.

Como fuera expuesto con anterioridad, las UAI deben estar en permanente retroalimentación y adquisición de mejores prácticas, por lo cual el Benchmarking le permitirá:

- La mejora continua.
- Es un medio para alcanzar objetivos nuevos.
- Legitimar los objetivos basándose en la orientación externa.
- Ayuda a descubrir lo que se espera de la UAI.
- Es un aporte a la planificación estratégica.

Para esta etapa, se confeccionó un formulario, desde el concepto de herramienta de Autoevaluación (CSA) para las UAI, conformada a partir de una adecuación de la grilla contenida en la Guía de Evaluación de Impacto en la Protección de Datos.

Por último, las distintas UAI debieran, luego de la evaluación de los distintos contextos, poder determinar, de acuerdo a la disponibilidad de recursos calificados y la tecnología existente, la conveniencia de quien realizará el tratamiento para la protección de los datos personales.

En relación al formulario de autoevaluación, al no poseer un puntaje de asignación de cada factor, se apelará a la razonabilidad y la responsabilidad proactiva de la UAI para su completitud.

El objetivo de la herramienta, al igual que la propuesta planteada es, desde una etapa temprana, identificar los procedimientos que deben reverse a fin de preservar los datos personales/sensibles incluidos en los informes de Auditoría y que los mismos no sean expuestos y como consecuencia afecten los derechos de los ciudadanos.

Las preguntas incluidas en la siguiente grilla no deben considerarse de manera taxativa, sino orientativas para determinar, en base a una autoevaluación, en qué situación se encuentra la UAI en relación a la protección de los datos en sus informes.

PREGUNTA	ACTIVIDAD DE LA UAI	FACTORES	IMPACTO DE NO DETECCION
¿La Unidad de Auditoría Interna (UAI) posee una base de datos de los informes emitidos durante los últimos 10 años?	La UAI identificará los informes emitidos y en caso de ausencia, se solicitará la remisión de los faltantes informes a la SIGEN	Disponibilidad de la Información	Cumplimiento Legislativo. Observaciones por parte de los Organismos de Control. Sanciones Reclamos por vía judicial al Organismo.
¿La UAI tiene publicados sus informes en la página institucional?	La UAI identificará los informes publicados y los no publicados	Derecho acceso a la Información Pública	Cumplimiento Legislativo. Observaciones por parte de los Organismos de Control.

PREGUNTA	ACTIVIDAD DE LA UAI	FACTORES	IMPACTO DE NO DETECCION
			Sanciones Reclamos por vía judicial al Organismo.
La UAI puede identificar los informes que poseen datos personales/sensibles ?	La UAI identificará y apartará todos los informes que contengan datos personales.	Tratamiento de datos personales	Cumplimiento Legislativo. Sanciones
La UAI posee auditores capacitados para identificar los datos personales/Sensibles ?	La UAI realizará un relevamiento de sus auditores a fin de determinar la necesidad de capacitación.	Identificación de los datos que requieren tratamiento.	Sobre de no identificación de datos sensibles.
¿Los informes contienen los datos personales/sensibles en el cuerpo principal o en Anexos?	La UAI identificará y seleccionará dos grupos de informes, los que contengan los datos en el cuerpo principal y los que se encuentran en Anexos.	Priorización de tratamiento considerando que los Anexos pueden desglosarse y darse tratamiento posterior o distinto.	Cumplimiento Legislativo. Sanciones
¿Los datos que se encuentran en los informes de Auditoría provienen de personas en alguna situación de vulnerabilidad?	La UAI trata los datos de personas que, por razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales, se encuentran expuestos a sufrir vulneración en sus derechos fundamentales.	Titulares de datos en situación de especial vulnerabilidad.	Cumplimiento Legislativo. Exposición de situaciones de vulnerabilidad de los titulares datos. Observaciones por parte de los Organismos de Control. Sanciones

PREGUNTA	ACTIVIDAD DE LA UAI	FACTORES	IMPACTO DE NO DETECCION
			Reclamos por vía judicial al Organismo.
¿La UAI posee actualmente un procedimiento normado y sistematizado de tratamiento de los datos existentes en sus informes?	La UAI no posee procedimientos normatizados para la protección de los datos.	Implementación de normas de tratamiento de datos personales/sensibles.	Falta de homogeneidad de aplicación ante la ausencia de normas sobre tratamiento de datos.
¿La UAI realizó un análisis de factibilidad sobre el tratamiento que puede aplicarse a los informes con el objeto de proteger los datos?	La UAI analizará las alternativas que, conforme los formatos de los informes pueden realizarse, tratando de evitar "tachar" los datos de manera manual	Aplicabilidad de tratamiento sobre los datos a proteger.	Continuar con tratamiento de datos de manera manual. Esto expondría tanto a la UAI y como consecuencia al Organismo a incumplimiento legislativo y posibles reclamos judiciales.
Los informes de Auditoría que poseen datos personales/sensibles que aún no han sido protegidos, se encuentran bajo medidas de seguridad de acceso a los mismos?	La UAI analizará la base de informes y sus accesos.	Seguridad y Protección de los datos personales/Sensibles	Posible exposición de la información, por inadecuado análisis de accesos a la información. Intrusión externa a los datos.

PREGUNTA	ACTIVIDAD DE LA UAI	FACTORES	IMPACTO DE NO DETECCION
¿La UAI analizó si el área responsable de la reversión de la observación, requiere la identificación de los casos incluyendo todos sus datos personales en el informe?	LA UAI analizará las distintas situaciones a fin de normar a futuro la razonabilidad de incorporación de los datos.	Protección de los datos personales/sensibles y su relación con las observaciones y acciones de reversión de lo detectado.	Incorporación de datos que no resultan necesarios incorporar en el informe. Esto derivara en un dispendio de recursos.
¿La incorporación de los datos en el informe respeta los criterios de Relevancia del informe? Esto refiere a la relación existente entre la evidencia obtenida y el uso que se le puede dar. La información utilizada para demostrar o refutar un hecho será relevante si guarda una relación lógica y directa con ese hecho, y es importante para poder demostrarlo.	La UAI no siempre considera este criterio para la inclusión de información relevante y/o pertinente pudiendo incorporarse datos personales/sensibles innecesarios.	Relevancia y pertinencia de la información	Cumplimiento de pautas de Órganos de Control. Sanciones

PREGUNTA	ACTIVIDAD DE LA UAI	FACTORES	IMPACTO DE NO DETECCION
¿La Organización cuenta con canales claros y accesibles para la visualización o requerimiento de la información referida a Informes de Auditoría?	La UAI analizará los canales de acceso de la ciudadanía, a fin que permita libremente y gratuitamente la obtención de la información.	Derecho de Acceso a la Información Pública. Oportunidad del Tratamiento de los datos en los informes.	Cumplimiento Legislativo. Observaciones por parte de los Organismos de Control. Sanciones Reclamos por vía judicial al Organismo.
La UAI ha asegurado que los informes de Auditoria que se brindan ante requerimientos de terceros posean la seguridad adecuada para que los datos personales/sensibles no permitan identificar al ciudadano?	La UAI evaluará la consistencia del tratamiento sobre los datos incluidos en el informe.	Protección de Datos Personales Control sobre los resultados del tratamiento de los datos.	Cumplimiento Legislativo. Sanciones El tratamiento permite identificar a las personas. Exposición de los datos por evaluación incorrecta.
La UAI se encuentra actualizada sobre la legislación/normativa/mejores prácticas?	La UAI evaluará el conocimiento de sus áreas/auditores a fin de determinar su actualización.	Protección de Datos Personales Disponibilidad de la información Pública	Cumplimiento legislativo. Sanciones Errores ante falta de actualización.

6.2 Etapa 2 - Análisis de la Información

Identificadas las diferentes variables que pueden surgir de la incorporación de los datos personales/sensibles en un informe de Auditoría, se debe evaluar el riesgo que existe en la incorporación de dichos datos en sus informes, es decir debe analizar la información.

Inicialmente este análisis se realizará sobre informes ya emitidos, permitiendo en futuros informes optimizar las etapas de tratamiento de datos.

El tratamiento que se determine realizar a los datos incluidos en los informes, puede provocar impactos en los derechos de las personas que deben ser de algún modo, identificados, gestionados minimizados o eliminados para cumplir con la normativa vigente, si el mismo se realiza de manera incorrecta o los datos no fueron identificados como personales/sensibles.

Es importante considerar que, sin perjuicio que es la Organización quien debe arbitrar los medios necesarios para la protección de la información sobre los datos personales/sensibles, los cuales utiliza para el cumplimiento de su misión y función, existe el riesgo que el incumplimiento o exposición indebida no sea ocasionado por la propia Organización, sino que sea resultado de procesos no homogéneos, o desactualizados por parte de la UAI.

Lo referido podría ser consecuencias, por ejemplo, de los siguientes riesgos no identificados o no tratados por las UAI en sus procesos:

- Inexistentes y/o inadecuados procedimientos para la identificación de datos personales o sensibles que requieran protección.
- Diferencias de criterios en la identificación de los datos que deben ser protegidos, por falta de capacitación.

- Ausencia de metodologías para la identificación y tratamiento de los datos contenidos en los informes de Auditoría.
- Tratamientos manuales ("tachar el dato") con mayor probabilidad de error, como todo proceso manual vs proceso sistematizado. Resulta necesario reiterar que la Ley de Derecho de Acceso a la Información Pública, en su art. 1 permite tachar u ocultar.

El análisis de la información no debe realizarse de manera individual, sino en el contexto en que se encuentran los mismos, dado que el tratamiento que se le dará a los datos que la componen no posee el mismo impacto, pudiendo derivar en un riesgo significativo sobre los derechos y garantías fundamentales de los ciudadanos en relación a su privacidad.

Por otra parte, y en virtud que la información, en este caso los informes de la UAI, deben estar disponibles en la página institucional del Organismo para ser consultado o en su defecto requeridos por terceros interesados, esta sub etapa de análisis de información requerirá que la identificación de informes y datos se realice sin omisiones o errores, ya que todo informe/dato no identificado no será susceptible de análisis en esta etapa.

6.2.1 Identificación de la privacidad en la Información

Uno de los factores claves para la seguridad de la información es identificar y proteger los activos de información, evitando la divulgación inadecuada. La seguridad de la información se determina como la preservación de su confidencialidad, integridad y disponibilidad.

En este punto, la privacidad se constituye como el componente fundamental, por medio del cual se reconocen los derechos de los ciudadanos respecto de su información personal, es decir toda aquella información que pueda ser usada para distinguir o que permita la del titular, como puede ser su nombre, número de seguro social, fecha y lugar de nacimiento, apellido de la madre o registros biométricos; y cualquier otra información que vincule o

asocie a un individuo, como puede ser información médica, educacional, financiera y laboral (Norma ISO/IEC 27701:2019)

Esta definición establece con claridad la exigencia a la que cualquier Organización se obliga respecto al manejo y uso de la información, respecto de los datos de los ciudadanos. En esta exigencia, se contempla claramente el accionar de la UAI en cuanto a la publicación de sus informes y la disponibilidad de los mismos ante requerimientos efectuados por terceros interesados.

Es en este punto donde deben integrarse en los procesos, los conceptos y cumplimiento de privacidad y la protección de los datos personales conforme la legislación.

Las UAI deben considerar que, a excepción de lo establecido por la Ley, la exposición de la privacidad de la información de las personas, a quienes no son titulares de las mismas, vulnera el derecho fundamental de su privacidad.

Las UAI deben considerar, al momento de identificar la privacidad en la información, que un adecuado procedimiento mediante el aprovechamiento de las TIC fortalece la seguridad de la información con el fin de garantizar la protección de la misma y la privacidad de los datos personales.

Esta sub etapa se complementa con la identificación de los datos personales/sensibles existentes en los informes, dado que la UAI utilizará dicha información para evaluar lo relativo a la privacidad y en consecuencia la protección de los datos personales.

El análisis que deben realizar las UAI, debe considerar, particularmente el aspecto de privacidad de los datos que, conforme legislación, no deben ser divulgados a terceros no autorizados o disponibles sin tratamiento y por ende sin protección, exponiendo, conforme lo menciona la Ley de Protección de Datos Personales, la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

Las UAI deben tener presente que la privacidad se encuentra íntimamente ligada a la clasificación de los datos y su protección, y las falencias detectadas en las distintas etapas previas y sucesivas pueden conllevar a riesgos reputacionales, por lo cual las UAI deben siempre considerar las dinámicas de los riesgos de la privacidad. Éstos impactan directamente sobre el cumplimiento de la Ley.

6.2.2. Clasificación de los datos

La Ley 25326 sobre Protección de los datos Personales – Habeas Data establece la siguiente clasificación (definición) de los datos

- Datos personales: Información de cualquier tipo referida a personas físicas o de existencia idean determinadas o determinables.
- Datos sensibles: Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.
- Titular del dato: persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la presente ley.

A partir de dicha clasificación, y considerando los datos que no podrán ser públicos, las UIA deben clasificar los datos contenidos en los informes, evaluando aquellos datos que requerirán tratamiento para asegurar su debida protección.

En la clasificación de dichos datos, las UAI deben tener presente lo establecido en el Art. 32 de la Ley sobre Derecho de Acceso a la Información Pública, el cual establece en su inc. i) que los informes de auditorías o evaluaciones, internas o externas, realizadas previamente, durante o posteriormente, referidas al propio organismo, sus programas, proyectos y actividades.

Debe considerarse también, el riesgo residual derivado de la posible reindentificación de datos y la seguridad de la confidencialidad de la información que no fue tratada, lo que podría permitir la identificación del titular.

6.2.3 Identificación del impacto de los casos clasificados

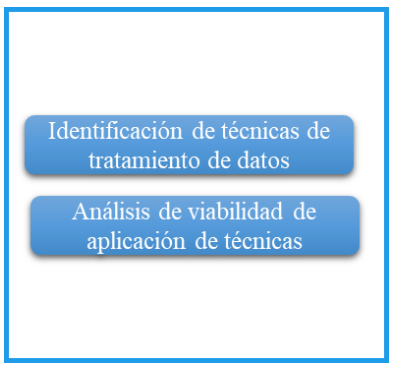
Una vez que las UAI identifiquen y clasifiquen los datos que requieran tratamiento para su protección, debe evaluar el impacto que tienen los mismos, esto refiere a si requerirán tratamiento para su protección a con el fin de asegurar que no sea posible la identificación del titular.

Como las anteriores etapas, adicionalmente a tomar como información etapas anteriores, esta etapa determinará aquellos casos que tendrán un impacto ante la no protección de los datos personales, determinando sus consecuencias.

Esta etapa es una de las más importantes de la metodología, junto con la identificación de los datos, dado que su efectividad permitirá identificar los datos que requerirán tratamiento para su protección.

Es por ello que las UAI deben asegurar la correcta ejecución de cada etapa, dado que todo dato no identificado, no evaluado y no tratado expondrá, tanto a la Organización como a la UAI, en un incumplimiento y sus consecuencias.

6.3. Etapa 3 - Tratamiento de datos



Por último, es importante destacar que, sin perjuicio de identificarse las distintas técnicas que podrían aplicarse para la protección de los datos, las mismas sólo serán definidas teóricamente y no desarrolladas en su aspecto técnico funcional. Esto último obedece a que la aplicación de dichas técnicas no está sujetas a ser

realizadas exclusivamente por las UAI, sino que, el objetivo es la identificación de los datos que deben protegerse.

Para el tratamiento de los datos personales, las UAI deben identificar y evaluar cuál de las herramientas de disociación de datos es la más efectiva y viable para proteger los datos de las personas, y de no poseer la capacitación/área pertinente, deberá contar con asesoramiento para tal fin.

En tal sentido, la disociación de datos permite brindar herramientas y coordinar el avance tecnológico con la protección y tutela de los derechos. Las UAI deben evaluar y asegurarse que las técnicas que se seleccionen permitan el cumplimiento efectivo de la legislación, considerando al mínimo la posibilidad de reidentificación del titular del dato.

La disociación de datos, también llamada anonimización, incorporan conceptos como "cadena de confidencialidad" cuya finalidad es el enmascaramiento o disociación de los datos. La ruptura de dichas cadenas puede permitir la materialización de riesgos de reidentificación de los titulares de los datos que se pretenden proteger.

Como responsable de la evaluación del control interno, una correcta implementación de un proceso de protección de datos personales permite a los organismos desarrollar tareas en un ambiente controlado, evitando riesgos como exposición, sanción, reclamos judiciales, entre otros.

Llevar a cabo un proceso de disociación permite que la información personal que maneja/administra y gestiona el Organismo y la UAI, no pueda asociarse a una persona concreta (identificada o identificable). Un dato disociado tiene la finalidad de "hacer" anónima la información, a fin de proteger la información crítica.

En este punto, es importante considerar que la técnica que se seleccione sobre anonimización de los datos, posee diversas características que deben ser tenidas en cuenta cada vez que se va a materializar, para que los datos puedan ser utilizados en forma abierta:

- No puede establecerse un vínculo alguno entre el dato su titular sin un esfuerzo desproporcionado.
- No puede ser reversible, es decir que es el resultado de un tratamiento de datos personales realizados para impedir que se vuelva atrás y se identifique al interesado.
- Que en la práctica sea equivalente al de un borrado permanente.
- Que lleve implícito un factor de riesgo que se debe tener en cuenta a valorar las técnicas de anonimización.

Todo proceso de anonimización persigue el objetivo de proveer los datos desagregados para que el público en general pueda utilizarlos, sin generar conflictos con los titulares de los datos. Ello también implica la realización de controles periódicos por parte de la UAI o responsable designado, para prevenir y evitar los posibles riesgos de reidentificación.

Una vez que se verificaron los controles, se deben dar de baja los datos que permiten la reidentificación, a fin que no sean publicados o expuestos ante solicitudes de terceros interesados. Esto lleva también a la necesidad de no aplicar las teorías del derecho al olvido, lo que evitará la reparación de datos y perjuicios al titular del dato que, sin perjuicio que pudiera haber sido generado por la UAI, serán afrontados por los Organismos a los cuales pertenecen.

Las UAI también deben considerar que puede existir la posibilidad que el titular del dato se sienta identificado por un conjunto de datos expuestos, por lo cual, ante la comunicación del mismo, deben reverse nuevamente la identificación de dichos datos y su tratamiento.

Por último, las UAI deben estar en continua actualización tanto normativa como tecnológica, dado que un cambio en cualquiera de ellas puede generar un nuevo riesgo que permita la identificación de los titulares.

6.3.1 Identificación de técnicas de tratamiento de datos

La anonimización o disociación de datos cuenta con un conjunto de técnicas que se dividen en aleatorización y generalización, que a su vez poseen las siguientes subdivisiones.

Exposición gráfica de elaboración propia

Las definiciones fueron adecuadas conforme son expuestas en https://www.gub.uy/unidad-reguladora-control-datos-personales/comunicacion/publicaciones/guia-criterios-disociacion-datos-personales

1. **Aleatorización**

La aleatorización es un conjunto de técnicas que modifican la veracidad de los datos con el fin de eliminar el vínculo existente entre los datos y el titular. Si los datos se vuelven lo suficientemente ambiguos, no se podrá identificar a una persona en concreto.

Este conjunto de técnicas por sí sola no reduce la particularidad de cada uno de los registros, puesto que estos pueden obtenerse a partir de un único interesado. Puede proteger contra ataques o riesgos de inferencia. Estos últimos se basan en información deducida lógicamente a partir de piezas aparentemente inconexas. (https://www.ccn-

cert.cni.es/publico/seriesCCN-STIC/series/400-Guias_Generales/401-glosario_abreviaturas/index.html?n=98.html).

1.1 Adicción de ruido

Esta técnica es una modificación de los atributos del conjunto de datos para que sean menos exactos, conservando no obstante su distribución general.

Si trata un conjunto de datos, cualquier persona que posee acceso a ellos, puede suponer que son exactos, pero no es totalmente exacto.

Si se utiliza esta técnica de manera eficiente, un tercero no podrá identificar a una persona a partir de los datos que visualiza, ni tampoco podría restaurar dichos datos u obtener información de cómo fueron modificados.

Esta técnica debe combinarse con otras como de eliminación de atributos obvios y de cuasi identificadores.

El nivel de ruido depende de la cantidad y el tipo de información que se requiera, así como del impacto que tenga la revelación de los atributos protegidos en la privacidad de las personas.

Esta técnica puede tener errores como, por ejemplo: añadir ruido inconsistente, pensar que la adición de ruido es una medida suficiente.

1.2 Permutación

Esta técnica consiste en mezclar los valores de los atributos en una tabla para que algunos de ellos puedan vincularse artificialmente a distintos interesados. Es una estrategia útil en el caso que sea importante conservar la distribución exacta de cada atributo en el conjunto de datos. La permutación podrá considerarse como una forma de adición de ruido.

En esta técnica se intercambian los valores contenidos en el conjunto de datos, trasladándose de un registro a otro, lo que garantiza que el rango y la distribución de valores sean idénticos, no así las correlaciones entre los valores y las personas.

Si dos o más atributos tienen una relación lógica o una correlación estadística y se permitan independientemente del resto, dicha relación queda destruida, por ello es importante permutar un conjunto de atributos que estén relacionados entre sí a fin de no romper la relación lógica. De no suceder esto, un atacante podría identificar los atributos permutados y revertir la técnica, pudiendo acceder a la identificación de las personas.

1.3 Privacidad diferencial

Esta técnica puede realizarse cuando el responsable del tratamiento de datos genera visitas anonimizadas de un conjunto de datos, al mismo tiempo que almacena una copia de los originales.

Esta técnica requiere de una supervisión continua para evaluar cualquier tipo de identificación de las personas en el conjunto de resultados de las consultas.

Es importante destacar que las técnicas de privacidad diferencial no modifican los datos originales, por ende, el responsable del tratamiento puede identificar los titulares de los datos a partir de los resultados de las consultas de privacidad diferencial.

Una de las ventajas de esta técnica, consiste en el hecho de que los conjuntos de datos se entregan a terceros autorizados como respuesta a una consulta concreta y no simplemente como consecuencia de la publicación de un único conjunto de datos.

Desde el punto de vista de la protección de los datos personales, la mayor dificultad que existe es poseer la capacidad de generar la cantidad adecuada de ruido, es necesario hacer bastante ruido, ya que no hacerlo es un error frecuente, y trae como consecuencia el riesgo de exposición o identificación del titular de los datos.

2. Generalización

Este grupo de técnicas generaliza o diluye los atributos de los interesados modificando las respectivas escalas u órdenes de magnitud, por ejemplo, sustituyendo una ciudad por una región, por una semana o mes.

La Generalización puede ser efectiva para descartar la singularización, pero no permite obtener una anonimización eficaz en todos los casos.

2.1 Agregación y Anonimato k

Estas técnicas tienen como objetivo el impedir que un interesado sea singularizado, cuando se le agrupa junto con, al menos, un número k de personas.

Estos métodos son aplicables cuando la correlación de valores puntuales de atributos puede crear cuasi identificadores.

La carencia principal de esta técnica es que no impide los ataques por inferencia.

2.2 Diversidad I y Proximidad t

La diversidad I extiende el anonimato k para garantizar que ya no se puedan realizar ataques por inferencia determinadas. Para ello se debe prevenir que, en cada clase de equivalencia, todos los atributos tienen al menos I valores diferentes.

Uno de los objetivos de esta técnica, consiste en limitar la ocurrencia de clases de equivalencias que tengan una variabilidad de atributos escasa.

La diversidad I es útil para proteger los datos ante ataques por inferencia. Por otro lado, la proximidad t consiste en crear clases equivalentes que se parezcan a la distribución inicial de los atributos en la tabla. Esta técnica es útil cuando haya que conservar los datos lo más próximo posible a los originales. Por ello es necesario que cada valor deba representarse tantas veces como sea necesario a fin de reflejar la distribución inicial de cada atributo.

Ambas técnicas garantizan que los registros relativo a una persona no se puedan distinguir o destacar de las otras personas en base de datos con cien por ciento de confianza.

6.3.2 Análisis de viabilidad de aplicación de técnicas

En esta etapa de la metodología, la UAI o quien se determine como responsable, deberá analizar la viabilidad de aplicación de técnicas, que le permitan optimizar los procesos que actualmente puedan llevarse a cabo.

Este análisis no solamente debe contemplar las técnicas de anonimización, sino también los formatos y procedimientos que realiza la UAI para la emisión de los informes de auditoría.

Conforme lo establece la guía de la Agencia Española de Protección de Datos Personales[7], cuando se pretenda anonimizar datos pertenecientes a las categorías especiales a las que se refiere el artículo 9 del RGPD, en nuestro caso la Ley de Protección de Datos Personales, se podría tener en cuenta la existencia de un equipo para el estudio de la viabilidad del proceso de anonimización. La labor de este equipo tendrá especial relevancia y su tarea principal sería la realización de un informe de viabilidad que reflejará detalladamente los motivos y condiciones específicas para la anonimización de los datos especialmente protegidos. En dicho informe podrían incluirse entre otros, por ejemplo, fundamentos o vinculaciones éticas del proceso de anonimización.

Las UAI debieran considerar los especialistas en seguridad, ya que ejercerán como órgano consultivo con el fin de aportar viabilidad técnica a los fundamentos que habiliten la utilización de la información anonimizada y el proceso de anonimización.

[7] (https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf#page=14&zoom=99,0,754)

6.4. Etapa 4 - Protección de Datos

La protección de datos es una disciplina jurídica para evitar el empleo indiscriminado de datos personales, es decir toda aquella información que es parte integrante de la esfera privada de los ciudadanos. Es la Ley de Protección de Datos Personales la cual reconoce y protege dicho derecho.

Hasta la promulgación de dicha ley, este derecho se circunscribía a la esfera privada y relacional entre el ciudadano y quien administraba y protegía sus datos dentro del Organismo.

Como marco genérico, en dicho ámbito la UAI, solo tenía la responsabilidad de evaluar el tratamiento que realizaba el Organismo sobre los datos personales, cómo se gestionaban y qué medidas de seguridad estaban implementadas y su eficacia. Asimismo, el objetivo podía considerar la evaluación del cumplimiento de las funciones de quienes eran los responsables de los datos y la evaluación de la finalidad para lo cual fueron recogidos los datos personales.

Con la promulgación de la Ley de Derecho de Acceso a la Información Pública, el rol de la UAI en la Organización, comenzó a jugar un rol que requiere sea proactivo e introspectivo. Esta nueva Ley implicó para las UAI la publicación, en las páginas institucionales, de los informes emitidos, antes y después de la Ley.

A esta nueva situación se suma la alta velocidad con que la virtualidad obligó a las Organizaciones a transformar sus procesos y en muchos casos alinearlos a las Tecnologías de la Información y la Comunicación (TIC) para continuar su operatividad.

Inevitablemente a lo expuesto, las UAI debieron considerar la protección de los datos personales y toda excepción contenida en la Ley en sus propios informes, a fin de dar cumplimiento a la legislación y evitar riesgos de exposición a la Organización y a la propia UAI.

6.4.1 Evaluación de la efectividad de la aplicación de técnicas

Esta etapa contempla las evaluaciones periódicas que deben realizar las UAI o el responsable designado, sobre los datos publicados y se encuentran disociados/anonimizados, a fin de detectar que las técnicas continúan protegiendo los datos personales.

Dentro de las responsabilidades de las UAI/responsable estará la actualización continua de la legislación o cambio tecnológico en la Organización, dado que pueden impactar en el procedimiento, en los cambios y en la eficacia de las técnicas utilizadas para la protección de los datos.

Las UAI deben identificar aquellos elementos tecnológicos que intervienen en las actividades de tratamiento de los datos de carácter personal, sin llegar a un análisis tecnológico pormenorizado.

En el mismo orden de ideas, deben evaluar si las medidas técnicas permiten conservar la integridad, confidencialidad y disponibilidad de la información de forma de garantizar la seguridad de los datos personales.

Para ello se deben realizar dos instancias de pruebas. En una primera instancia, sobre la técnica identificada como la más eficaz para la protección de los datos y en segundo lugar, y quizás una de las más importantes, un control periódico, a fin de asegurar que dichas técnicas continúan siendo eficaces para proteger los datos personales.

Esta última instancia se complementa con la mejora continua como se explicará en la etapa correspondiente.

Conforme lo menciona la Guía de Orientaciones y garantías en los procedimientos de anonimización de datos, emitida por la Agencia Española de Protección de Datos Personales, el proceso de anonimización/disociación no puede asegurar la imposibilidad de reidentificación de las personas en términos absolutos, motivo por el cual se deben de

tener en cuenta las garantías jurídicas necesarias para preservar los derechos de los interesados.

Las pruebas que se realicen deben considerar:

- Verificación que la disociación no puede revertirse.
- Verificación que los informes publicados posean los datos personales/sensibles protegidos conforme lo indicado.
- Valoración y reporte de los resultados.

6.4.3. Confección de Matriz de Cumplimiento Metodológico

Conforme lo establece el Manual de Control Interno Gubernamental, emitido por la Sindicatura General de la Nación, los papeles de trabajo de las UAI constituyen las evidencias respaldatorias de todo trabajo de auditoría. Estos son necesarios para el adecuado y eficiente desempeño del auditor, teniendo en cuenta la importancia que reviste la registración de las pruebas de auditoría realizadas, así como el conocimiento y comprensión del universo a auditar, sobre el cual se basan sus conclusiones.

Por ello, las normas de auditoria (gubernamental y profesionales) indican que el auditor deberá confeccionar un archivo completo y detallado que incorpore los papeles de trabajo de la labor efectuada y de las conclusiones alcanzadas, los cuales serán reservados en legajos preparados para tal fin.

Uno de los objetivos de la presente metodología es la confección de una matriz, donde se registren las acciones y evaluaciones llevadas a cabo y que a misma constituya un respaldo documental.

En tal sentido la matriz constituye, al igual que los papeles de trabajo, un respaldo documental sobre los procedimientos llevados a cabo para el cumplimiento legislativo, tanto en la protección de los datos personales como la disponibilidad de la información o requerimientos de terceros interesados, como así también la evidencia de dicho control.

La matriz que se desarrolla seguidamente no resulta taxativa, ni tiene como intención agregar una actividad que devengue en un dispendio de recursos, por lo cual las distintas UAI podrán tomar la misma como base para su beneficio, pero siempre considerando la evidencia que el responsable rendirá cuenta de su completitud.

MATRIZ DE CUMPLIMIENTO METODOLÓGICO

Informe N°	
Año de Emisión	

Identificación de la Observación (Nro de la Observación)	Tema tratado en la observación (Título o falencia detectada)	Incluye datos personales/sensibles (SI/NO)	Que clasificación posee: 0. No Aplica 1. Personal 2. Sensible	De existir Datos personales/sensibles los mismos se encuentran en un Anexo del Informe? (SI/NO)	¿Requiere tratamiento?	¿Qué técnica corresponde? (Mencionar la Técnica)	¿Se realizaron las pruebas de efectividad de las técnicas de disociación sobre los datos? (SI/NO)

Publicación del Informe en Página Institucional (SI/NO)	
Fecha de Control Metodológico	
Responsable del Control	

Matriz de elaboración propia

Como resultante de la Etapa de Protección de Datos se obtendrá la publicación y disponibilización de datos personales/sensibles protegidos.

6.5. Etapa 5 – Actualización y Mejora Continua de los Procesos

El proceso de mejora continua es un proceso continuo para mejorar los procesos. Las mejoras buscadas pueden ser incrementales con el tiempo o lograrse con un momento decisivo.

Las principales reglas para medir los cambios son la eficiencia, efectividad y flexibilidad de estos procesos.

Tanto la mejora continua cuanto la innovación, facilitan el desarrollo de nuevos procesos, así como su racionalización, simplificación y normalización. La mejora continua sólo es posible con una perspectiva correctiva y orientada al futuro, alentando a las personas a identificar y reconocer errores propios y ajenos, y proponer mejoras para superarlos.

Conforme el Referencial IRAM 13, publicada por SIGEN, el propósito es alinear la gestión de las UAI al enfoque en la mejora continua. Asimismo, establece como requisito que las UAI deben considerar los resultados del análisis y de la evaluación (satisfacción de las partes interesadas, seguimiento de indicadores, revisiones por la Dirección, informes de auditorías, resultados de la formación, acciones correctivas implementadas), para determinar si hay necesidades u oportunidades que deben considerarse como parte de la mejora. Debe conservarse información documentada del análisis, de la evaluación y de la decisión de la adopción o no de oportunidades de mejora.

En este contexto y enmarcado a la protección de los datos personales, las resultantes de cada una de las etapas que componen la metodología y el análisis de cada una de sus subetapas, son la información más relevante de la mejora continua.

Debe tenerse presente que la aplicación de la metodología por sí sola no determina el éxito de la mejora continua, sino que dependerá de la capacitación, especialización y actualización profesional que posean las personas que apliquen la misma. En virtud de ello, será la relevancia de la información que surja de cada una de las etapas y sus resultantes.

La actualización y mejora continua debe constituir en sí misma un proceso continuo y no estático, por lo cual las UAI pueden determinar que esta etapa requiera mayor detalle para profundizar en cada análisis de cada etapa.

A título de ejemplo, se mencionan para cada una de las etapas, posibles riesgos que puede considerar el profesional, al momento de rever el proceso y los procedimientos, dado que la inadecuada evaluación puede exponer los datos personales, incumpliendo la legislación sobre los derechos de las personas.

ETAPA	RIESGO DE SUB ETAPAS	RIESGO DE LA RESULTANTE
Evaluación del Contexto	- Cambios en la normativa o legislación no detectados. - Nueva legislación/normativa no detectada. - Legislación/normativa dada de baja sin detectarse. - Ausencia de responsable de datos incluidos en los informes de auditoría. - Ausencia de informes emitidos con anterioridad. - Ausencia de detección de la necesidad de reformular las estructuras de los informes / redacción de las observaciones, de acuerdo a la protección de los datos.	- Inadecuado estado de situación de la UAI en relación a la Protección de Datos Personales. - Información insuficiente o deficiente para el análisis de la información.

ETAPA	RIESGO DE SUB ETAPAS	RIESGO DE LA RESULTANTE
	- Inadecuada autoevaluación. - Falta de capacitación de los responsables.	
Análisis de Información	- Desconocimiento del dato privado. - Inadecuada/Errónea clasificación de datos - Desconocimiento de los procesos para poder determinar el impacto de los datos clasificados. - Falta de capacitación de los responsables.	- Datos personales/sensibles que no son identificados. - Datos que no tendrán tratamiento de protección.
Tratamiento de Datos	- Desconocimiento de las técnicas de tratamiento de datos. - Ausencia de recursos que puedan identificar las técnicas - Ausencia de profesionales de Sistemas de Información para la realización de pruebas sobre la viabilidad de aplicación. - Ausencia de identificación de amenazas que pudieran producir un daño o una violación de los derechos de los titulares de los datos.	- Imposibilidad de aplicación de técnicas. - Utilización de la técnica de "tachado" para no incurrir en el incumplimiento legislativo.
Protección de Datos	- Ausencia de pruebas sobre la aplicación de la técnica - Falta de capacitación para la realización de las pruebas	- Desconocimiento si los datos serán protegidos de manera eficaz. - Publicación de datos que debieran estar protegidos.

ETAPA	RIESGO DE SUB ETAPAS	RIESGO DE LA RESULTANTE
	- Ausencia de responsable de la matriz de cumplimiento metodológico. - Ausencia de documentación que respalde el control de las etapas.	- Identificación de titulares por ausencia de protección de sus datos. - Utilización indiscriminada de los datos obtenidos,

Tabla de contenido de elaboración propia

En tal sentido, y particularmente para el alcance del presente trabajo, las UAI deben considerar, como mínimo, la evaluación de los siguientes aspectos, a fin de ejecutar la etapa de actualización y mejora continua de manera eficiente, efectiva y profesional:

- Estrategias de la UAI ante modificaciones de procedimientos internos.
- Flexibilidad para afrontar cambios.
- Integración de la UAI (Estructura Orgánica Funcional).
- Recursos humanos disponibles.
- Capacitación de los auditores.
- Detección de necesidades de capacitación relacionadas con la protección de datos personales/sensibles.
- Rotación de los recursos.
- Identificación de nuevas, cambios o bajas legislativa o de normativa que impacta sobre la protección de datos.
- Evaluación del impacto de los cambios o ausencia de las TIC que soportan la protección de los datos.
- Identificación de ajustes que requieren las etapas para ser más efectivas y óptimas.
- Información a el/los responsables datos ante la detección de datos que pueden ser identificables.

- Formatos de los informes emitidos.
- Aspectos operativos.
- Aspectos funcionales.
- Publicación de los informes.
- Procedimiento de respuesta ante requerimientos de terceros interesados.

6 CONCLUSIONES

El derecho a la protección de los datos personales/sensibles, que refieren al derecho de la vida privada e intimidad de sus titulares requirió una atención particular por la aparición de nuevas tecnologías y por la aparición de la virtualidad operativa que tuvieron que asumir las Organizaciones para no discontinuar su operatividad.

Al mismo tiempo, la promulgación de la Ley sobre el Derecho de Acceso a la Información Pública, ya sea por la publicación en las páginas institucionales o por terceros interesados, impulso a las UAI activar la modificación de sus procesos en la realización de sus auditorías como en el control de la protección de los datos personales que incluye en sus informes.

En este punto, las mismas deben encarar sus operatorias y procedimientos hacia una actitud proactiva y de cara a la actualización y la mejora continua, teniendo en cuenta su responsabilidad en la evaluación del sistema de control interno imperante en la Organización.

En tal sentido, esa mejora continua debe, principalmente, estar orientada a lograr el cumplimiento efectivo de la protección de datos personales, y de manera consecuente ello impactará en la optimización de los procesos de Auditoría.

Los procesos de disociación resultan una herramienta válida tanto para alinearse a los avances tecnológicos como para garantizar la protección de los datos personales.

Si las UAI sólo desarrollan sus actividades de protección de los datos personales/sensibles existentes en sus informes, sobre procedimientos no formalizados, manuales o desactualizados, no lograrán asegurar el cumplimiento legislativo, pero sobre todo no resguardarán los derechos de los ciudadanos a su intimidad.

Es importarte destacar, que los procesos de disociación de datos, no garantizan que exista la posibilidad que se puedan reidentificar a los titulares de dichos datos, pero si los mismos se sustentan en procesos y metodologías que tienden a mejoras continuas y poseen monitoreos sistemáticos, se minimiza el error humano, lográndose minimizar los riesgos de exposición o divulgación de los datos de los titulares y las consecuencias que ello conlleva.

El análisis y evaluación realizado para el presente Trabajo Final Integral, permitió alcanzar los objetivos planteados por medio de la exposición de una metodología de elaboración propia, que permita asegurar que los datos personales expuestos en los informes de Auditoría se encuentren debidamente protegidos.

7 BIBLIOGRAFIA

Instituto de Auditores Internos (2004):(siglas en inglés IIA). *Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna.* Normas Internacionales de Auditoría.

Organización Internacional de Normalización (2018):(siglas en inglés ISO). Directrices para la auditoría de los sistemas de gestión (Norma núm. 19011). Disponible en: https://www.isotools.org/2019/02/13/iso-19011-2018-7-principios-de-auditoria/

Comisión Electrotécnica Internacional (siglas en inglés IEC) - Organización Internacional de Normalización (2005) (siglas en inglés ISO). Seguridad de la Información.

Comisión Electrotécnica Internacional (siglas en inglés IEC) - Organización Internacional de Normalización (2019) (siglas en inglés ISO). Gestión de la Privacidad de la Información.

Organización Internacional de Normalización (2015):(siglas en inglés ISO). Gestión del Riesgo (Norma núm. 31000).

Chirino Alfredo (2015). Manual Operativo de protección de datos en el Salvador.

Fassio, A & Pascual, L (2016). Apuntes para desarrollar una investigación en el campo de la Administración y el Análisis Organizacional. Buenos Aires: EUDEBA

Resolución SIGEN Nº3 (2011). Manual de Control Interno Gubernamental. Sindicatura General de la Nación.

Resolución SIGEN Nº152 (2002). Normas de Auditoría Interna Gubernamental. Sindicatura General de la Nación.

Resolución SIGEN N° 107 (1998). Normas Generales de Control Interno.

Agencia Española de Protección de Datos "Orientaciones y garantías en los procedimientos de Anonimizacón de datos". Disponible en https://www.aepd.es/sites/default/files/2019-12/guia-orientaciones-procedimientos-anonimizacion.pdf#page=14&zoom=99,0,754.

Instructivo de Trabajo 7/15-GNYE, provistos por la SIGEN – Protección de Datos Personales.

Martires, L. (2020). Asesoramiento y Gestión de Riesgo. [Material de clase]. Auditoría Interna Gubernamental II. Universidad Nacional de La Plata e Instituto Superior de Control de la Gestión Pública, Ciudad de Buenos Aires, Argentina.

Bismark Rodriguez (2016). Instituto de Auditores Internos. Artículo "El marco de referencia COSO de Control Interno y el modelo de tres líneas de defensa". Disponible en https://iaia.org.ar/

Agencia de Acceso a la Información Pública de Argentina y la Unidad Reguladora y de Control de Datos Personales de Uruguay (2020) "Guía de Evaluación de Impacto en la Protección de Datos Personales". Disponible en https://www.argentina.gob.ar/noticias/argentina-y-uruguay-lanzan-la-guia-evaluacion-de-impacto-en-la-proteccion-de-datos.

Malvicino G. (2020). La gestión de la calidad en el ámbito la gestión de la calidad en el ámbito de la administración pública. Potencialidades para un Potencialidades para un cambio gerencial. [Material de clase]. Auditoría Interna Gubernamental II. Universidad Nacional de La Plata e Instituto Superior de Control de la Gestión Pública, Ciudad de Buenos Aires, Argentina.

Miner, W. (2019). Auditoría del Sistema Gestión de Calidad. [Material de clase]. Universidad Nacional de La Plata e Instituto Superior de Control de la Gestión Pública, Ciudad de Buenos Aires, Argentina.

SIGEN IRAM Referencial N° 13 (2017). Unidades de Auditoría Interna del Sector Público Nacional. Requisitos de gestión de la calidad.

8 ANEXOS

ANEXO 1 – Grilla de Preguntas Guía EIDP

	PREGUNTAS	ALCANCE	FACTORES
TIPOS DE DATOS	¿Se recolecta un gran volumen de datos personales? ¿Podría establecer aproximadamente el número de personas que se encuentran en sus bases de datos? ¿Es este número superior al 1% de la población del país?	La organización trata o planea tratar datos de gran cantidad de personas	Tratamiento de datos personales a gran escala
	¿El proyecto implica la recolección de datos considerados sensibles?	La organización trata o planea tratar datos de carácter sensible. Por ejemplo, datos referidos a la salud de las personas, a sus opiniones políticas, sus preferencias sexuales o sus convicciones religiosas.	Sensibilidad de los datos tratados.
	¿Los datos que trata provienen de personas en alguna situación de vulnerabilidad?	La organización trata o planea tratar datos de personas que, por razón de su edad, género, estado físico o mental, o por circunstancias sociales, económicas, étnicas y/o culturales, se encuentran expuestos a sufrir menoscabos en sus derechos fundamentales.	Titulares de datos en situación de especial vulnerabilidad.
	¿Los datos son recogidos con consentimiento? ¿Ese consentimiento es expreso? ¿Se le informa al ciudadano para que se utilizarán sus datos antes de que consienta? Si trata los datos sin consentimiento, ¿bajo cuál excepción?	La organización trata o planea tratar datos sin requerir el consentimiento de los titulares de datos.	Recolección de los datos amparada en una base legal distinta del consentimiento.

	PREGUNTAS	ALCANCE	FACTORES
TRATAMIENTO	¿Por cuánto tiempo se preservan los datos personales en su sistema? ¿Existe un mecanismo de minimización o destrucción periódica de los datos? ¿Guarda alguna clase de datos personales por lapsos prolongados de tiempo? ¿Guarda datos personales por razones estadísticas, científicas o históricas? ¿Realiza procesos de anonimización o disociación previa al guardado?	La organización almacena o planea almacenar datos personales por tiempo indeterminado o por lapsos prolongados	Retención prolongada de los datos y mecanismo de almacenamiento.
FINALIDAD	¿Se utilizarán los datos para elaborar perfiles predictivos? ¿Con qué finalidad se usan esos perfiles? ¿Se toman decisiones mediante operaciones automatizadas de tratamiento de datos	La organización usa o planea utilizar los datos que recolecta para elaborar perfiles predictivos y tomar decisiones en base a esos perfiles. La organización toma decisiones a través de operaciones automatizadas de tratamiento de datos	Uso de los datos con el fin de elaborar perfiles predictivos. Decisiones a partir del tratamiento automatizado de datos
	¿El proyecto involucra el uso de tecnologías que, en principio, entrañarían riesgos para la privacidad o los derechos de las personas debido a su naturaleza o extensión?	La organización utiliza sistemas de reconocimiento biométrico, videovigilancia extendida, uso de VANT's o técnicas de tratamiento automatizado.	Utilización de tecnologías invasivas que, por sí mismas, importen riesgos para la privacidad
INTER	¿Se contratan a terceros ajenos a la organización para que realicen actividades de tratamiento de datos?	El procesamiento de los datos se realiza por cuenta de un tercero	Contratación de encargados de tratamiento de datos.

	PREGUNTAS	ALCANCE	FACTORES
COMUNICACIÓN DE DATOS	¿Los empleados suscriben contratos de confidencialidad? ¿Qué consecuencias acarrea el incumplimiento de tales contratos? ¿Qué medidas de orden manual e informático se implementan para afianzar la seguridad de los datos? ¿La organización cuenta con una política de privacidad o de protección de los datos personales?	La organización no cuenta con una política de privacidad, no suscribe pactos de confidencialidad con sus integrantes y no tiene una política en materia de seguridad de la información	Implementación de medidas de seguridad y confidencialidad inadecuadas.
	¿Se realizan transferencias de datos a terceros países? ¿Esos países tienen legislación considerada adecuada? ¿Las transferencias de datos se hacen conforme a alguna otra base legal que no sea una decisión de adecuación?	La organización transfiere o planea transferir los datos que recaba a terceros países. Este criterio se vuelve especialmente relevante cuando esos países no fueron reconocidos como adecuados por las autoridades de control uruguaya o argentina	Recurrente transferencia de los datos a terceros países.
	¿Se realizan frecuentemente cesiones de datos a terceros ajenos a la organización? ¿Esas cesiones se instrumentan mediante un contrato escrito?	La organización cede o planea ceder los datos que recaba a terceros en numerosas ocasiones dentro del propio país.	Recurrencia de las cesiones a terceros.