XXXIV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos.
Colegio de Graduados en Ciencias Económicas, Buenos Aires, 2022.

Clasificación de la información contable dispuesta por la Ley de Habeas Data en la República Argentina.

Diego Sebastian Escobar.

XXXIV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos

Título: Clasificación de la información contable dispuesta por la Ley de Habeas Data en la República Argentina

Área: Contabilidad y Auditoría

1.9. Medidas preventivas para la seguridad informática dentro del marco de las organizaciones

Autor: ***Diego Sebastián Escobar***

Maipú 429, Piso 5 Depto. 3, CP 1006, CABA.

Tabla de contenido

Clasificación de la información contable dispuesta por la Ley de Habeas Data en la República Argentina

1.1. Introducción

En el marco de las XXXIV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos organizadas por el Colegio de Graduados en Ciencias Económicas someto a la consideración de todos los participantes el análisis de la clasificación de la información contable establecida por el plexo normativo vigente en la Argentina.

El objetivo del presente trabajo es identificar las bases de datos existentes en el sistema de información contable, relacionarlas con la clasificación establecida en la ley de Habeas Data y por último enumenrar las medidas de seguridad dispuestas por el organismo de control.

En el año 2000, en la República Argentina se promulgó la Ley N°25.326 de Protección de Datos Personales, en donde se estableció el marco legal para el

tratamiento de los datos de las personas físicas y jurídicas resguardados en entornos de procesamiento digitalizados o en soporte de papel.

El principal objetivo de esta ley es la "*protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean estos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como el acceso a la información que sobre las mismas se registre*." (Escobar, 2010).

Asimismo, la Ley y las disposiciones dictadas por el organismo de control (actualmente la AAIP), establecen que las bases de datos o archivos públicos y privados destinados a proporcionar informes o procesen información personalizada deben estar inscriptos en un registro especial y cumplir con las medidas de seguridad dispuestas por el organismo.

1.2. Clasificación de datos personales

En la citada Ley N°25.328 y las Disposiciones de la ex - Dirección Nacional de Protección de Datos Personales (exDNPDP) o Agencia de Acceso a la Información Pública (AAIP), se ha establecido que la información personalizada (o sea, aquella que identifica a las personas) puede clasificarse en datos básicos, intermedios y sensibles.

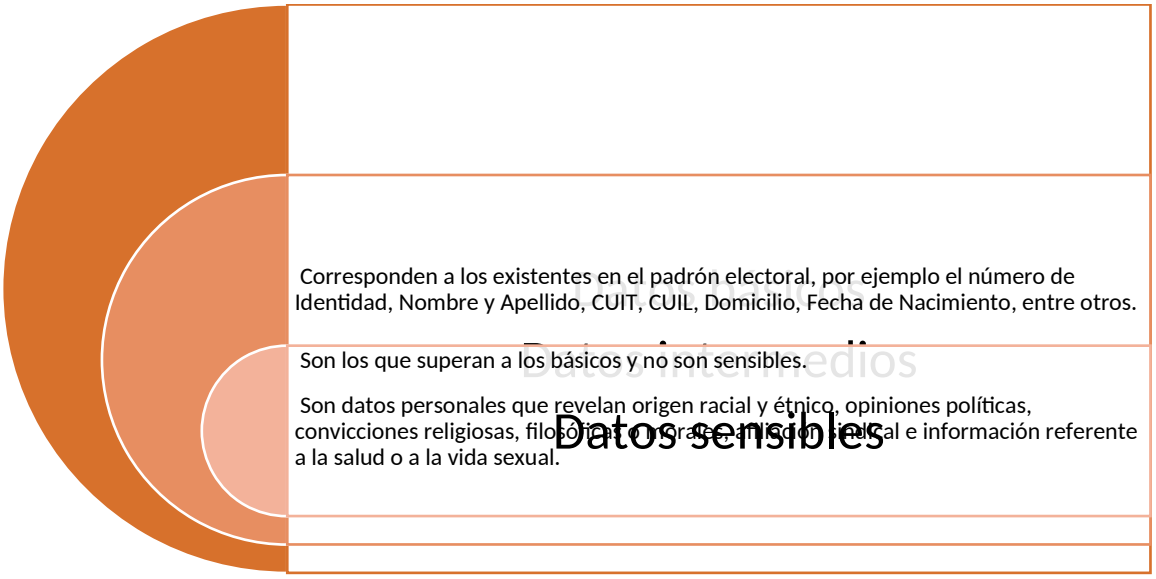
Los datos considerados básicos, corresponden a los existentes en el padrón electoral. Entre ellos encontramos al número de identidad, nombre y apellido, número de CUIT o CUIL, domicilio, fecha de nacimiento, entre otros.

Los datos intermedios son los que superan a los básicos y no son sensibles. Por ejemplo, estado civil, ingresos y egresos, etc.

Los datos sensibles son 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.

En el siguiente cuadro se resumen la clasificación de los datos dispuesto por la normativa vigente:

Esquema N°1: Niveles en la clasificación de los datos



Fuente: Elaboración propia.

Considerando la presente normativa, la documentación contable analizada por el Contador Público en las organizaciones deberá ser clasificada considerando sus datos contenidos, como también se debe cumplir con las medidas de seguridad dispuestas por la AAIP. Con respecto a la categoría de datos, el artículo N°7 de la Ley establece que:

Fuente: (Congreso de la República Argentina, 2020)

A continuación, se presenta la documentación presente en las empresas, en donde se incluyen datos personales, con la clasificación de la información contenida.

Esquema N°2: Comprobantes y documentación contable

Tipo de Comprobante	Características	Tipo de Dato
Facturas	Si determina el cliente	Datos Intermedios
Notas de Débito / Crédito	Si determina el cliente	Datos Intermedios
Remitos	Si determina el cliente	Datos Intermedios
Cupones de Tarjeta de Crédito / Debito	Si determina el cliente	Datos Intermedios

Fuente: Elaboración propia.

Generalmente, la información contenida en los comprobantes y documentación de comercio con la identificación de los clientes o proveedores es considerada intermedia porque con los datos contenidos en los mismos se pueden determinar el ingreso y el consumo de estos, sus gustos y preferencias por productos o marcas, entre otras cosas.

ESQUEMA N°3: Comprobantes internos contables

Tipo de Comprobante	Características	Tipo de Dato

Legajos de Clientes	Si determina el Cliente	Datos Intermedios
Asientos Diarios	-	Datos Intermedios

Fuente: Elaboración propia.

La información contenida en los comprobantes y documentación bancaria con "*la identificación de los clientes o proveedores es considerada intermedia porque con los datos contenidos en los mismos se pueden determinar el ingreso y el consumo de estos, su capacidad de pago y su disponibilidad, entre otras cosas*" (Suarez Kimura & Escobar, 2017).

ESQUEMA N°4: Relacionados con los empleados

Tipo de Comprobante	Tipo de Dato
Legajos Personales	Datos Sensibles
Recibos de Sueldos y Jornales	Datos Intermedios
Declaraciones Juradas	Datos Intermedios
Formularios de Contribuciones Sociales	Datos Sensibles

Fuente: Elaboración propia.

En el caso de las bases de datos con información de sus empleados, están conformados por datos intermedios y sensibles, que son utilizados para confeccionar declaraciones juradas, aportes y contribuciones, asignaciones familiares, entre otros.

ESQUEMA N°5: Relacionados con clientes y proveedores

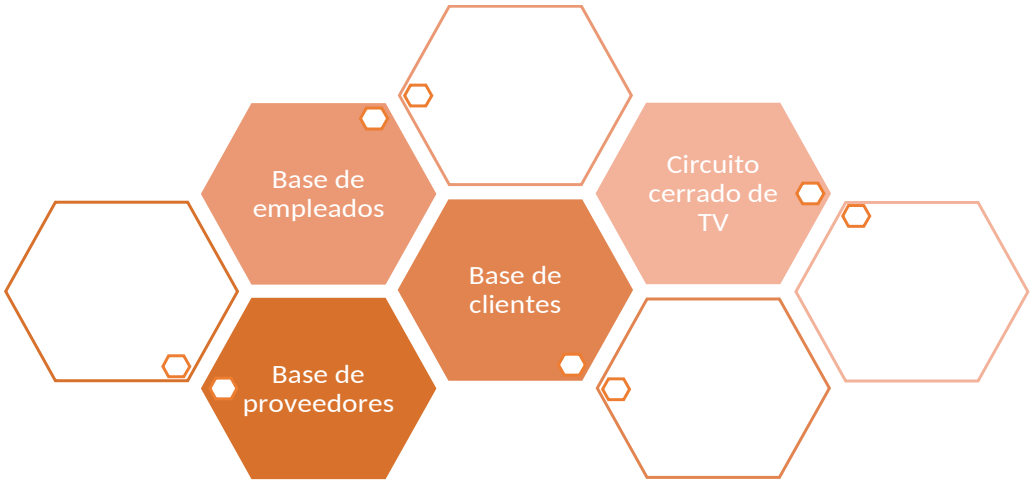
Tipo de Comprobante	Características	Tipo de Dato
Legajos de proveedores	Si determina el cliente	Datos Intermedios
Facturas, Nota debito / Crédito, Remitos, etc.	Si determina el cliente	Datos Intermedios

Fuente: Elaboración propia.

En el caso de las bases de datos con información de sus empleados, están conformadas por datos intermedios y sensibles, que son utilizados para confeccionar declaraciones juradas, realizar aportes y contribuciones, asignaciones familiares, entre otros.

Por lo tanto, en el sistema contable se pueden identificar las siguientes bases de datos:

ESQUEMA N°6: Bases de datos existentes en el sistema contable



Fuente: Elaboración propia.

Como se aclaró precedentemente, en las organizaciones existen numerosas bases de datos con la información personal para confeccionar diversos informes, que tendrían que estar registradas en la AAIP. No se debería considerar únicamente como una obligación, sino también como una ventaja competitiva en el manejo de la información.

1.3. Seguridad de los datos

El responsable o usuario del archivo de datos debe adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos personales, de modo de evitar su adulteración, pérdida, consulta o tratamiento no autorizado, y que permitan detectar

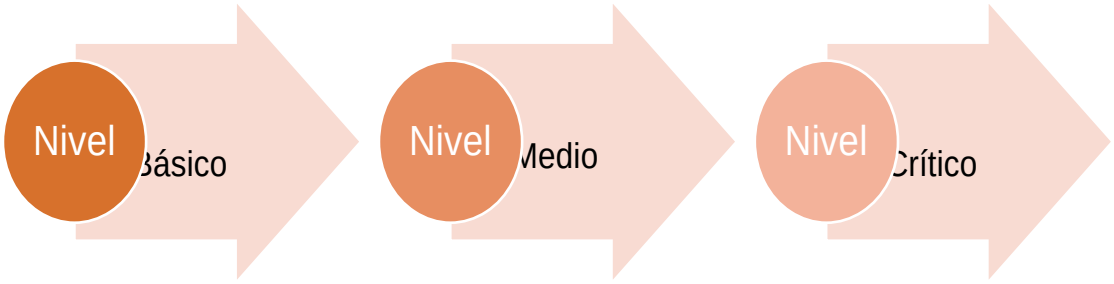
desviaciones, intencionales o no de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad, seguridad, como también los que no garanticen el cumplimiento de los términos de la presente ley.

En la disposición N°11/2006, la AAIP, establece diferentes niveles de seguridad, para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos públicas no estatales y privadas. Dichos niveles de seguridad dependen del tipo de datos que contengan.

A continuación, se enunciarán las características más importantes de cada nivel de seguridad. (AAIP, 2020).

ESQUEMA N°7: Niveles de Seguridad



Fuente: Elaboración propia.

1.3.1. Medidas de seguridad del nivel básico

Para los archivos, registros, bases y bancos de datos que contengan datos de carácter personal, deberán adoptarse las medidas de seguridad calificadas como de nivel básico en la disposición N°11/2006 (AAIP, 2020) que a continuación se detallan:

Disponer del documento de seguridad de datos personales en el que se especifiquen, entre otros, los procedimientos y las medidas de seguridad a observar sobre los archivos, registros, bases y bancos con contenidos de estas características. Deberá mantenerse en todo momento actualizado y ser revisado cuando se produzcan cambios en el sistema de información.

Contendrá, entre otras, las siguientes medidas:

ESQUEMA N°8: Medidas de seguridad del nivel básico

1. "Funciones y obligaciones del personal".

2. "Descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan".

3. "Descripción de las rutinas de control de datos de los programas de ingreso de datos y las acciones a seguir ante los errores detectados a efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de

control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes".

4. "Registros de incidentes de seguridad".

5. "Procedimientos para efectuar las copias de respaldo y de recuperación de datos".

6. "Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso".

7. "Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información".

8. "Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados".

9. "Medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal".

Fuente: Disposición N°11/2006 – (AAIP, 2020)

1.3.2. Medidas de seguridad del nivel medio

Además de las medidas de seguridad de nivel básico, deberán adoptarse las que se detallan a continuación sobre los archivos, registros, bases y bancos de datos

de las empresas privadas que desarrollen actividades de prestación de servicios públicos, así como los pertenecientes a entidades que cumplan una función pública y/o privada que, más allá de lo dispuesto por el artículo N°10 de la Ley N°25.326, deban guardar secreto de la información personal por expresa disposición legal (como el secreto bancario):

ESQUEMA N°9: Medidas de Seguridad del Nivel Medio

1. "El Instructivo de seguridad deberá identificar al responsable (u órgano específico) de Seguridad".

2. "Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales".

3. "Limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información".

4. "Establecer un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal".

5. "Gestión de Soportes e información contenida en ellos".

6. "Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo

informatizado".

7. "Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa, no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados".

Fuente: Disposición N°11/2006 – (AAIP, 2020)

1.3.3. Medidas de seguridad del nivel crítico

Los archivos, registros, bases y bancos de datos que contengan datos personales, definidos como "datos sensibles", además de las medidas de seguridad de nivel básico y medio, deberán adoptar las que a continuación se detallan:

ESQUEMA N°10: Medidas de Seguridad de Nivel Crítico

*1. "**Distribución de soportes**: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte."*

*2. "**Registro de accesos**: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuándo lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso*

haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como mínimo por el término de un TRES (3) años."

*3. "**Copias de respaldo**: además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en una caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales."*

*4. "**Transmisión de datos**: los datos de carácter personal que se transmitan a través de redes de comunicación deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas."*

Fuente: Disposición N°11/2006 – (AAIP, 2020)

Juntamente con la registración de las bases de datos con información personal, las entidades deben implementar el nivel de seguridad acorde con el tipo de datos

que manejen, cabe destacar que el incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en la ley.

1.4. Reflexiones finales

En los sistemas contables de los entes existen bases de datos en donde se almacena información relacionada con clientes, proveedores y empleados. La Ley N°25.326 establece que las destinadas a proporcionar informes o procesen información con datos personalizados deben inscribirse en el registro establecido por la Agencia de Acceso la Información Pública.

La información contenida en los sistemas contables puede clasificarse en datos básicos, intermedios y sensibles dependiendo de la criticidad de la misma. Los datos considerados básicos, corresponden a los existentes en el padrón electoral. Los datos intermedios son los que superan a los básicos y no son sensibles. Los datos sensibles son 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.

Juntamente con la registración de las bases de datos con información personal, los entes deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad y confidencialidad de los datos

personales, a fin de evitar su adulteración, pérdida, consulta o tratamiento no autorizado.

1.5. Bibliografía

Escobar, D. S. (2010). Ley de Protección de Datos Personales. *Revista Imagen Profesional de La Federación Argentina de Consejos Profesionales en Ciencias Económicas*, 22-24.

Suarez Kimura, E. B., & Escobar, D. S. (2010). Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público. *Foro Nacional de Simposios de Profesores de Práctica Profesional*, Publicación contínua.

Congreso de la República Argentina. (19 de abril de 2020). *Ley N°25.326*. Obtenido de Infoleg: http://servicios.infoleg.gob.ar/infolegInternet/anexos/60000-64999/64790/norma.htm

Suarez Kimura, E. B., & Escobar, D. E. (2017). Identificación de conceptos básicos de la ley de habeas data en los sistemas contables: perspectivas a considerar por parte de los pequeños estudios. *Enfoques*, 40-56.

AAIP. (19 de abril de 2020). *Agencia de Acceso a la Información Pública.* Obtenido de Disposición N° 11/2006: http://www.jus.gob.ar/datos-personales.aspx