Vinculación e Identificación de Conceptos Básicos de la Ley de Habeas Data en Los Sistemas Contables: El Caso Práctico En Entidades Hospitalarias.[66] - Cra. Elsa Beatriz Suarez Kimura - Universidad De Buenos Aires – Dr. Diego Sebastián Escobar - Universidad Del Salvador.

Área: Metodología de la enseñanza
Sub-área: Contable

Autores:
Elsa Beatriz Suarez Kimura
Profesora Asociada Regular Contabilidad Patrimonial. Tutora de tesis de Grado, Posgrado y Doctorado. Facultad de Ciencias Económicas. Universidad de Buenos Aires

Diego Sebastián Escobar
Profesor de Tecnología de la Información y Tutor de Trabajo Final de Grado. Facultad de Ciencias Económicas. Universidad del Salvador.

1. INTRODUCCIÓN

En el 2012, el Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales (CODECE) en su documento base para la acreditación de la carrera de Contador Público, ha definido que "*el objeto de su profesión es la "información" en todas sus formas, sea la misma generada dentro de las organizaciones, interactuando éstas entre sí o en su vinculación con el contexto*".

Si analizamos criteriosamente los sistemas contables microsociales, independientemente del segmento observado: financiero, de gestión, ambiental y/o social, la información es el input para cada uno de ellos. Y como un activo intangible clave del ente, los contadores deberían conocer los conceptos básicos que le permitan protegerla.

En la República Argentina se encuentra vigente la ley de Habeas Data, en donde se establecen los lineamientos principales para el tratamiento de información personal y el organismo de control pertinente, impactando en los sistemas contables.

En marco del trigésimo séptimo Simposio de Profesores de Práctica Profesional, sometemos al debate de todos los asistentes la inclusión de la Ley de protección de datos personales y normas complementarias en el manejo de información contable, destacando el caso particular de la asociación de los citados conceptos con los indicadores de gestión hospitalarios, dictado a un grupo de alumnos en la Facultad de Ciencias Económicas de la Universidad del Salvador.

2. IMPLICANCIAS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA DE INFORMACIÓN CONTABLE MICROSOCIAL EN HOSPITALES.

[66] Trabajo financiado por el Proyecto de Investigación Trienal 2014 / 2017 - UBACyT – 20020130100340. "Los sistemas de información contable en contextos tecnológicos: abordajes concurrentes para su diagramación, seguimiento y control para el ejercicio profesional de los Contadores Públicos." Directora: ELSA BEATRIZ SUAREZ KIMURA

Con la promulgación de la ley 25.326 de Protección de Datos Personales en la República Argentina en el año 2000, se estableció entre otras obligaciones, que las bases de datos o archivos públicos y privados que contengan información personal, destinados a proporcionar informes deben estar inscriptos y cumplir con los requisitos que establezca el registro especial.

Al analizar el caso de los sistemas contables microsociales en hospitales, se destaca la existencia de numerosas bases de datos que contienen y analizan información personal, emitiendo diferentes tipos de informes, desde médicos, técnicos, de gestión y de control; cuya información debería ser tratada bajos los estándares establecidos y cuyas bases registradas para cumplir con el marco legal vigente.

A continuación se analiza la ley de Protección de Datos personales y su vinculación con la información contenida en los sistemas de información contable.

2.1. Reconocimiento de las Bases de Datos presentes en los hospitales.

- *Conceptos y objetivos de la Ley 25.326.*

El principal objetivo de la citada 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 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."*[16]

La ley toma en cuenta tanto los datos de las personas de físicas como los de las de existencia ideal. En una interpretación de la misma en un sistema contable hospitalario, podemos identificar información de pacientes, empleados y proveedores, en donde se utiliza esa información para brindar diferentes tipos de informes.

A continuación se analizan las secciones más relevantes de la ley, prestando mayor interés en la información hospitalaria.

- *Tipo de Datos Personales.*

La ley 25.328 y las Disposiciones de la Dirección Nacional de Protección de Datos Personales, "han establecido una clasificación a los datos personales, en Datos Básicos, Intermedios y Sensibles"[67].

Esquema Nº 1: Tipos de Datos Personales.

[67]Suarez Kimura E. y Escobar, D. S., Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público, en el XXXII Simposio Nacional de Profesores de Práctica Profesional del Contador. FACULTAD DE HUMANIDADES, CIENCIAS SOCIALES Y DE LA SALUD UNIVERSIDAD NACIONAL DE SANTIAGO DEL ESTERO, Septiembre, 2010.

Fuente: Elaboración propia.

1. Los datos considerados básicos, corresponden a los presentes en el padrón electoral. Entre ellos encontramos al Número de Identidad, Nombre y Apellido, CUIT, CUIL, Domicilio, Fecha de Nacimiento, entre otros.

2. Los datos Intermedios son los que superan a los básicos y no son sensibles. Por ejemplo, estado civil, Ingresos y egresos, etc.

3. 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 caso particular del sistema de indicadores en hospitales se maneja información básica, intermedia y sensible. Con respecto a la categoría de datos, el artículo 7 de la Ley establece que:

"1. Ninguna persona puede ser obligada a proporcionar datos sensibles.

2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.

3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.

4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas."[68]

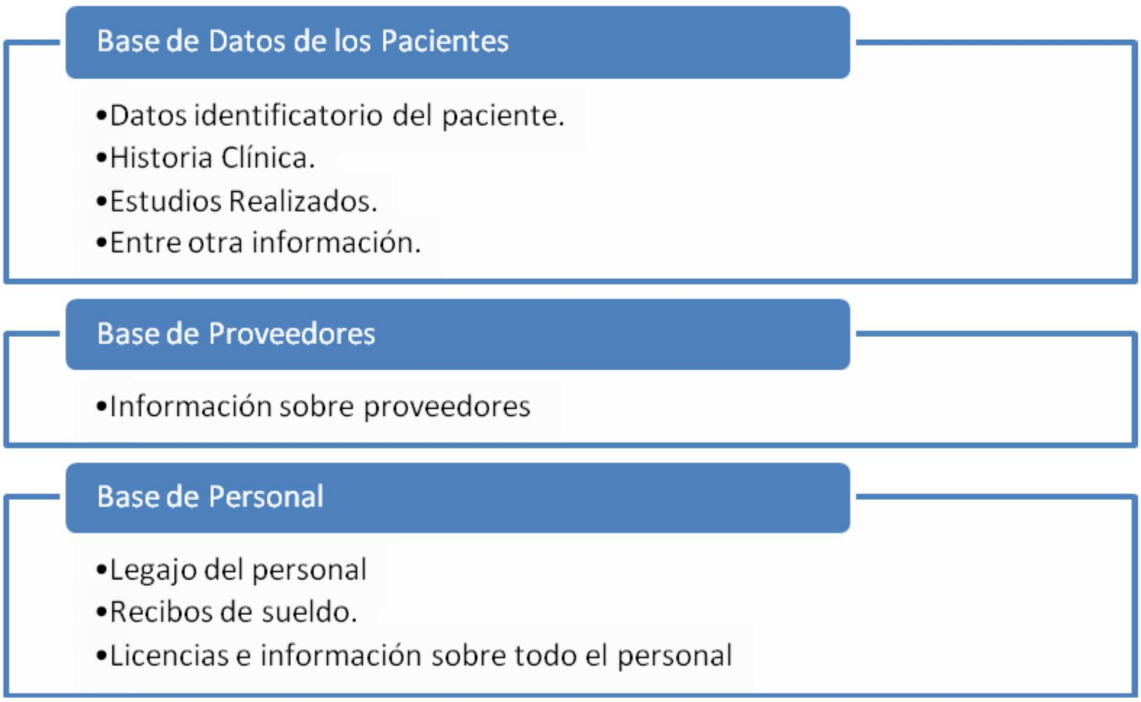
A continuación se presenta la documentación presente en hospitales, en donde se incluyen datos personales, con la clasificación de la información contenida.

- ***Bases de datos hospitalarias***
-

En el sistema de información contable microsocial hospitalario contienen mínimamente información de pacientes, proveedores y del personal de la institución. En el siguiente gráfico se presentan las bases de datos que una institución hospitalaria podría contener.

Esquema Nº 2: Tipos de Bases de datos existente en hospitales.

[68]Ley 25326, Ley de Habeas Data, Artículo 7, Boletín oficial de la República Argentina, Buenos Aires. 30 de Octubre de 2000.

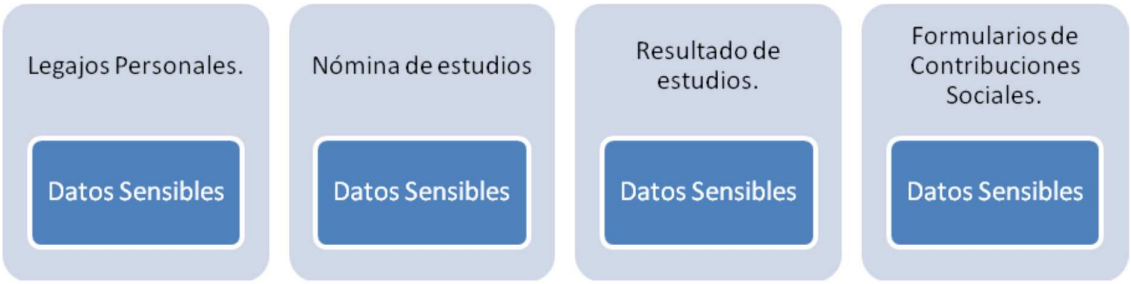


Fuente: Elaboración propia.

En el análisis de la información de la Base de los pacientes(si determinan al paciente), la mayoría de la información es considerada sensible. A continuación se pueden identificar los siguientes datos:

Esquema Nº 3: Datos relacionados con los pacientes (Si determinan los usuarios).

Tipo de documentación / Tipo de Dato

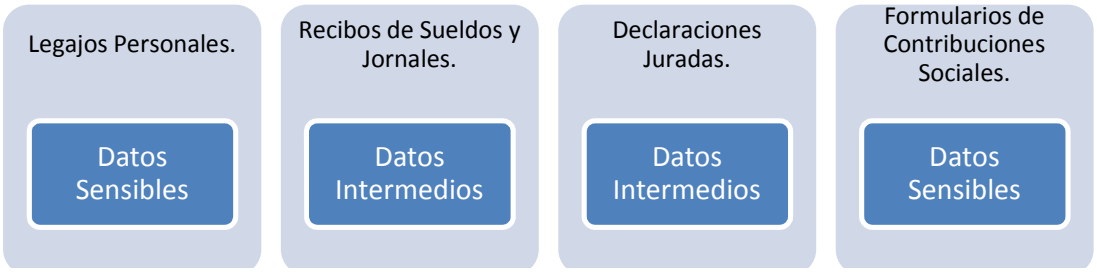


Fuente: Elaboración propia.

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 Nº 4: Relacionados con los empleados (Si determinan los usuarios).

Tipo de Comprobante / Tipo de Dato



Fuente: Elaboración propia.

Como se aclaró precedentemente, en las organizaciones hospitalarias existen numerosas bases de datos con la información personal para confeccionar diversos informes, estadísticas e indicadores, que tendrían que estar registrados en el organismo correspondiente, que en este caso es la Dirección Nacional de Protección de Datos Personales.

3.1. Responsabilidad del responsable de la información

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 no garanticen el cumplimiento de los términos de la presente ley.

En la disposición 11/2006, la Dirección Nacional de Protección de Datos Personales, establece diferentes niveles de seguridad, para el tratamiento y conservación de los datos personales contenidos en archivos, registros, bancos y bases de datos publicas no estatales y privadas. Dichos niveles de seguridad dependen del tipo de datos que contengan.[69]

Esquema Nº 5:Niveles de Seguridad.

[69] A los interesados en ampliar la información l sobre el tema, podrán consultar en página web indicada en la bibliografía del presente trabajo la resolución completa Nº 11/2006 de la DNPDP. Dirección Nacional de Protección de Datos Personales. Disposición 11/2006, Medidas de Seguridad. Buenos Aires, Argentina. 2015, accedido desde http://www.jus.gob.ar/datos-personales.aspx

Fuente: Elaboración propia.

Dependiendo de la información existente en la base, se clasifica la criticidad de la misma y del procesamiento de los datos. Y en base a esa criticidad, de deben adoptar las medidas se seguridad para cada caso. A los interesados en analizar las medidas a implementar, en el anexo 1 del presente trabajo, se exponen los conceptos más relevantes.

4. CONCLUSIONES

Como se indicó precedentemente, el objetivo principal del trabajo es difundir como se analizó la inclusión de la Ley de protección de datos personales en el manejo de la información en un sistema contable microsocial, dictado en la Facultad de Ciencias Económicas de la Universidad del Salvador.

Luego de vincular los conceptos expuestos, se pueden identificar en los sistemas hospitalarios numerosas bases de datos en donde se almacenan datos personales, comerciales, de uso interno y legajos, entre otros. La ley 25.326 establece que las citadas bases destinadas a proporcionar informes deben inscribirse en el Registro que al efecto habilite el organismo de control, ya que esa información contenida en los sistemas es utilizada para realizar diversos reportes como: Indicadores de Servicios, Índices de Salud, Estados Contables, Informes de Responsabilidad Social Empresaria, etc.

En esta línea, además de registrar las bases en el organismo competente, que en el caso de las entidades hospitalarias privadas corresponde a la Dirección Nacional de Protección de Datos Personales, 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, 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.

5. BIBLIOGRAFÍA

Dirección Nacional de Protección de Datos Personales. Disposición 11/2006, Medidas de Seguridad. Buenos Aires, Argentina. 2015, accedido desde http://www.jus.gob.ar/datos-personales.aspx

Escobar, D. S., Ley de Protección de Datos Personales, Revista Imagen Profesional, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas, 2010.

Ley 25326, Ley de Habeas Data, Artículo 7, Boletín oficial de la República Argentina, Buenos Aires. 30 de Octubre de 2000.

Suarez Kimura E. y Escobar, D. S., Repercusiones de La Ley De Protección de Datos Personales en el Ejercicio Profesional del Contador Público, en el XXXII Simposio Nacional de Profesores de Práctica Profesional del Contador. FACULTAD DE HUMANIDADES, CIENCIAS SOCIALES Y DE LA SALUD UNIVERSIDAD NACIONAL DE SANTIAGO DEL ESTERO, Septiembre, 2010.

Suarez Kimura, E. B., Escobar, D. S. y De Franceschi, R. L.; (2014) “El rol del profesional en Ciencias Económicas en la planificación estratégica de las tecnologías de información.”. XXXVI Simposio Nacional de Profesores de Práctica Profesional. FACULTAD DE CIENCIAS ECONÓMICAS UNIVERSIDAD ARGENTINA DE LA EMPRESA (UADE). PINAMAR, BUENOS AIRES, 18, 19 Y 20 DE SEPTIEMBRE DE 2014.

Suarez Kimura, Elsa B. (2004) Auditoría y Sistema de Control Interno: Particularidades a considerar en los contextos tecnológicamente mediados. XXVI Simposio de Profesores de Práctica Profesional. Universidad del Museo Social Argentino. Buenos Aires. Argentina.

Suarez Kimura, Elsa Beatriz, (2008), “Tesis Doctoral, Posibles mejoras teórico-tecnológicas aportadas por la contabilidad a los Sistemas de información de los entes”. Investigación y Doctorado, FCE UBA.

- **ANEXO N°1: TIPOS DE MEDIDAS SOBRE LA INFORMACIÓN**

MEDIDAS DE SEGURIDAD DEL NIVEL BASICO:[70]

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 11/2006 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:

Tabla Nº 4: 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 11/2006 –DNPDP.

MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:[71]

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 10 de la Ley Nº 25.326, deban guardar secreto de la información personal por expresa disposición legal (como el secreto bancario):

Tabla Nº 5: 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 11/2006 – DNPDP.

[70]Dirección Nacional de Protección de Datos Personales. Disposición 11/2006, Medidas de Seguridad. Buenos Aires, Argentina. 2003, accedido desde http://www.jus.gob.ar/datos-personales.aspx
[71]Ídem Nota N°5.

MEDIDAS DE SEGURIDAD DEL NIVEL CRÍTICO[72]:

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:

Tabla Nº 6: 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, cuando 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 minino 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 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 11/2006 - DNPDP.

Conjuntamente con la registración de las bases de datos con información personal, las empresas 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.

[72] Ídem Nota N°5.