

Universidad de Buenos Aires

**Facultad de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería**

Carrera de Especialización en Seguridad Informática

SEGURIDAD INFORMÁTICA EN LOS SISTEMAS CONTABLES

Un análisis de los aspectos legales, normativos y tecnológicos de la Seguridad de la Información en el almacenamiento, procesamiento, control y resguardo de los Registros Contables.

Autor:

Diego Sebastián Escobar

Tutor:

Ricardo Rivas

Abril de 2013

Cohorte 2010

- Declaración Jurada de origen de los contenidos:

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

Diego Sebastián Escobar
DNI: 31.782.894

- Resumen

El uso masivo de las tecnologías de la información y comunicación como medios para generar, almacenar, transferir y procesar información contable, se ha incrementado vertiginosamente en los últimos años convirtiéndose en un elemento indispensable en la mayoría de las organizaciones para el desarrollo de sus actividades y toma de decisiones, no importando su tamaño, la complejidad o extensión de su negocio.

En las organizaciones existen varios sistemas de información, pero en todas, por diversas obligaciones legales y reglamentarias, está presente como una cuestión ineludible el sistema de información contable.

Asegurar este tipo de información en una organización requiere instalar una cultura de seguridad e implementar una adecuada combinación de normas, tecnologías, metodologías y estándares.

En el presente trabajo se propone analizar los aspectos legales, normativos y tecnológicos de la Seguridad de la Información en el almacenamiento, procesamiento, control y resguardo de los Registros Contables aplicables a los entes que se organicen como Sociedades Comerciales en el ámbito de la Ciudad Autónoma de Buenos Aires.

- **Palabras Clave:** Seguridad de la Información, Sistemas de Información Contable.

- Índice de Contenidos

- Declaración Jurada de Contenidos.....	i
- Resumen	ii
- Índice de Contenidos	iii
- Nómima de abreviaturas.....	vii
- Introducción	1
- Capítulo I	3
1. REGISTROS Y SISTEMAS CONTABLES	3
1.1. Introducción	3
1.2. La Seguridad de la Información y la Contabilidad.....	3
1.3. Seguridad de la Información y su aporte a la contabilidad.....	5
1.4. Conclusiones particulares del Capítulo I.....	9
- Capítulo II	10
2. MARCO LEGAL DE LOS REGISTROS CONTABLES	10
2.1. Introducción	10
2.2. Obligación de Llevar Registros Contables	10
2.3. Los Registros Contables en formatos tecnológicos: Las características de la Ley de Sociedades Comerciales.....	11
2.4. Requisitos exigidos en los Sistemas de Registración Contable....	12
2.5. Los Riesgos identificados por la Doctrina y el Derecho Contable de Llevar una Contabilidad Informática.....	13

2.6. La legalidad de un sistema de registros contables en contextos informáticos.....	14
2.7. Conclusiones particulares del Capítulo II	14
- Capítulo III	16
3. REQUERIMIENTOS DE LA INSPECCIÓN GENERAL DE JUSTICIA	16
3.1. Introducción	16
3.2. Condiciones de los Sistemas de registraci3n contable resguardados en compact disc, otros discos 3pticos y microfilmes	17
3.3. Tr3mites y requisitos solicitados por la IGJ	20
3.4. Conclusiones Particulares del Cap3tulo III.....	22
- Cap3tulo IV	24
4. PROCEDIMIENTO GENERAL DE EMISI3N, CONVERSI3N Y CONSERVACI3N DE LA DOCUMENTACI3N RESPALDATORIA DE LOS REGISTROS CONTABLES....	24
4.1. Introducci3n	24
4.2. R3gimen de emisi3n de comprobantes y registraci3n de operaciones	25
4.2.1. Sistemas de emisi3n manual y mediante sistemas no manuales	25
4.2.2. R3gimen especial de emisi3n y almacenamiento de duplicados electr3nicos.....	26
4.3. Registraci3n de la Documentaci3n Respaldatoria	28
4.3.1. R3gimen de Almacenamiento Electr3nico de Comprobantes	29
4.3.2. Conservaci3n de comprobantes comerciales	31
4.3.3. Cuestiones espec3ficas de la emisi3n de comprobantes electr3nicos.....	32
4.4. Conclusiones particulares del Cap3tulo IV.....	33
- Cap3tulo V	35
5. IMPLICANCIAS DE LA LEY DE PROTECCI3N DE DATOS PERSONALES EN EL SISTEMA DE INFORMACI3N CONTABLE	35
5.1. Introducci3n	35
5.2. Reconocimiento de las Bases de Datos utilizadas y	

almacenadas en las Organizaciones. Conceptos y objetivos de la Ley 25.326	35
5.3. Tipo de Datos Personales	36
5.4. Seguridad de los Datos.....	39
5.5. Conclusiones particulares del Capítulo V.....	43
-Capítulo VI.....	45
6. PAUTAS MÍNIMAS DE AUDITORÍA INTERNA DE LA SEGURIDAD DE LA INFORMACIÓN EN SISTEMAS CONTABLES	45
6.1. Introducción	45
6.2. Pautas mínimas de auditoría interna para el cumplimiento de las normativas vigentes para entes organizados como Sociedades Comerciales en la Ciudad Autónoma de Buenos Aires.....	45
6.3. Normativas de cumplimiento optativo que contribuyen al cumplimiento de normas legales vigentes	49
-Capítulo VII.....	51
7. CONCLUSIONES FINALES DEL TRABAJO	51
- La Seguridad de la Información y la Teoría General Contable.....	51
- Garantías planteadas a nivel doctrinario para los Sistemas de Información Contable en soporte tecnológico	52
- Normas de las Seguridad de la Información contempladas en diferentes organismos de contralor en la Ciudad Autónoma de Buenos Aires.....	53
- Conclusiones Finales.....	54
- Anexo I: Características de los Sistemas de Registración Contable..	56
A. SISTEMAS DE REGISTROS CONTABLES.....	56
A.1. La contabilidad como un sistema.	56
A.2. Elementos del sistema contable	57
A.3. Teneduría de libros y utilización de software	59
- Bibliografía específica.....	60

- Bibliografía General	64
- Índices específicos	67
Índice de Tablas	67
Índice de Esquemas	67
Índice de Imágenes.....	68
Índice de Cuadros.....	68

- N6mina de abreviaturas

AFIP: Administraci6n Federal de Ingresos P6blicos.

CABA: Ciudad Aut6noma de Buenos Aires.

CPCECABA: Consejo Profesional de Ciencias Econ6micas de la Ciudad Aut6noma de Buenos Aires.

FACPCE: Federaci6n Argentina de Consejos Profesionales en Ciencias Econ6micas.

IGJ: Inspecci6n General de Justicia.

IRAM: Instituto Argentino de Normalizaci6n y Certificaci6n.

RT: Resoluci6n T6cnica.

- Introducción

En las organizaciones existen múltiples sistemas de información cuya interrelación conforma información útil para la toma de decisiones en los diferentes niveles jerárquicos de la misma. El sistema de información contable es uno de ellos, pero adquiere una importancia relevante y se diferencia de los demás al estar presente por obligaciones legales y reglamentarias vigentes en todo tipo de entes.

El presente Trabajo Final de la Carrera de Especialización en Seguridad Informática persigue como objetivo principal analizar los aspectos normativos y tecnológicos de la Seguridad de la Información en el almacenamiento, procesamiento, control y resguardo de los registros contables especificados por la normativa legal vigente en el ámbito de la Ciudad Autónoma de Buenos Aires para entes organizados como Sociedades Comerciales. Sobre esta base y con la intención de circunscribir el objeto de análisis conforme a las metodologías apropiadas al alcance del presente trabajo se ha escogido la citada jurisdicción.

En los diferentes capítulos se propone identificar aquellas normas legales y de control relacionadas con la Seguridad de la Información de cumplimiento obligatorio en los sistemas contables. Asimismo se plantea analizar el aporte de esta disciplina a la Teoría General Contable, la doctrina del Derecho Contable¹ y a diferentes fuentes normativas aplicables.

Se establecen los siguientes objetivos particulares:

- Determinar y puntualizar el aporte y la vinculación de la Seguridad de la Información a la Teoría General Contable.

¹ El Derecho Contable se define como la “ciencia cuyo objeto está constituido por las relaciones interdisciplinarias entre el Derecho, en cuanto Ciencia Jurídica, y la Contabilidad, en sus aspectos científicos y técnicos, comprendiendo tanto las áreas comunes como las recíprocas influencias entre ambas disciplinas y las nuevas interpretaciones que resultan de su armoniosa integración, superando asimetrías y dando coherencia a las regulaciones comunes” IADECO, Instituto Argentino de Derecho Contable. Véase referencia bibliográfica N° [31].

- Identificar las garantías exigidas por la doctrina del derecho contable al “Sistema de Información Contable en soportes tecnológicos”.
- Determinar la parte pertinente de las Normativas de la Inspección General de Justicia, la Administración Federal de Ingresos Públicos y la Dirección Nacional de Protección de Datos Personales relacionadas con la Seguridad de la Información contable.
- Identificar otras normas de implementación optativas que contribuyan al cumplimiento del plexo normativo vigente o que lo complementen.
- Proponer un esbozo de programa de auditoría interna sobre la Seguridad de la Información para cumplir con los requisitos solicitados por los organismos de control a los entes organizados como Sociedades Comerciales en la Ciudad Autónoma de Buenos Aires.

- Capítulo I

1. REGISTROS Y SISTEMAS CONTABLES.

1.1. Introducción.

El presente capítulo persigue el objetivo de desarrollar brevemente cuestiones básicas de la Seguridad de la Información y su aporte a la Teoría General Contable. Los interesados en ampliar los contenidos conceptuales de los registros y sistemas contables, son invitados al Anexo A en donde encontrarán desarrollados dichos conceptos.

El autor considera necesario el citado análisis ya que plantea las bases teóricas de los Sistemas de Registración Contable que luego son nombrados en los capítulos siguientes.

1.2. La Seguridad de la Información y la Contabilidad.

- Concepto de Seguridad de la Información.

La Real Academia Española establece que seguridad es la cualidad de Seguro, es decir “estar libre y exento de todo daño peligro o riesgo”². En tecnología de la información, la seguridad entendida según la citada definición es prácticamente imposible de conseguir, “por lo que se tiende más al concepto de fiabilidad; entendiéndose a un sistema seguro como aquel que se comporta como se espera de él.”³

En los sistemas informáticos, ya sean sistemas operativos, de servicios o aplicaciones, se dice que son seguros si cumplen con las siguientes características:

² Definición extraída de la Real Academia Española; Véase referencia bibliográfica N° [31].

³ Véase referencia bibliográfica N° [22].

- Confidencialidad: Requiere que la información sea accesible (usarla, leerla o escucharla) sólo para las personas autorizadas.
- Integridad: Requiere que la información sólo pueda ser modificada por las entidades autorizadas, asegurando que la información con la que se trabaja sea completa y precisa y poniéndole énfasis en la exactitud tanto en su contenido como en los procesos involucrados en su procesamiento.
- Disponibilidad: Requiere que los recursos del sistema informático estén disponibles para los usuarios y las entidades autorizadas cuando se los necesiten.

Estos tres requisitos son los básicos, pero según Gustavo Aldegani, el paradigma actual de la seguridad de la información incluye además de los citados principios a la “Verificación de la Identidad Digital y Registro de sus acciones, Confiabilidad de Navegación, y Prevención de pérdidas de datos.”⁴

- **Concepto de Contabilidad.**

La contabilidad como disciplina, fue conceptualizada por el Profesor Emérito Dr. Carlos Luís García Casella, el cual establece que “La contabilidad es una ciencia aplicada factual cultural que se ocupa de la descripción cuantitativa y de la proyección de la existencia y circulación de los objetos diversos en cada ente u organización social, en vista al cumplimiento de sus metas a través de un método basado en un conjunto de supuestos básicos [...]”⁵.

La contabilidad es considerada por muchos investigadores un sistema de información o sub-sistema de información en las organizaciones persiguiendo los siguientes objetivos:

- Captar y procesar datos sobre el Patrimonio del ente y su evolución en el tiempo.
- Proporcionar información para la Toma de Decisiones, Vigilancia y Control sobre recursos, obligaciones y cumplimiento de requisitos legales.

⁴ Véase referencia bibliográfica N° [23].

⁵ Informe presentado en el I Encuentro Universitario de Investigaciones del Área Contable. Véase referencia bibliográfica N° [21].

- Requisitos de la Información contenida en los Estados Contables.

En la Resolución Técnica N° 16⁶, denominada Marco Conceptual de la Información Contable de la FACPCE (Federación Argentina de Consejos Profesionales en Ciencias Económicas), se establece que para cumplir con su finalidad, la información contenida en los estados contables debe reunir los requisitos enunciados a continuación:

Tabla N° 1: Requisitos de la Información contenida en los Estados Contables.	
Pertinencia (atingencia)	
Confiabilidad (credibilidad)	- Aproximación a la realidad
	- Esencialidad (sustancia sobre forma)
	- Neutralidad (objetividad o ausencia de sesgos)
	- Integridad
Verificabilidad	
Sistematicidad	
Comparabilidad	
Claridad (comprensibilidad)	
Consideraciones sobre las restricciones que condicionan el logro de las cualidades recién indicadas:	
Oportunidad	
Equilibrio entre costos y beneficios	
Fuente: FACPCE ⁶ - Véase referencia bibliográfica N° [17].	

Estos atributos componen los requisitos que debe cumplir la información contable contenida en los estados contables emitidos.

1.3. Seguridad de la Información y su aporte a la contabilidad.

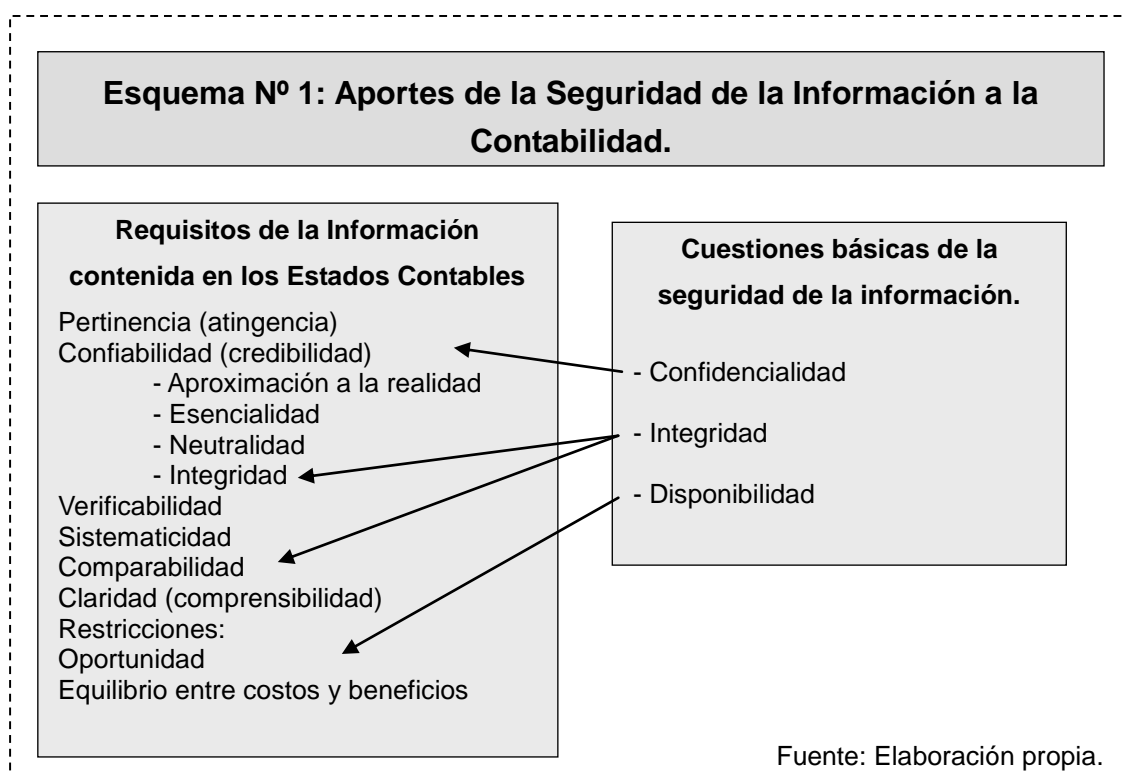
La contabilidad como campo de conocimiento toma conceptos de otras disciplinas, como la Administración, el Derecho y la Matemática entre otras. El autor del presente trabajo considera que la Seguridad de la

⁶ Extraído de la FACPCE. Véase referencia bibliográfica N° [17].

Información debería contemplarse como una de ellas, al contribuir con el cumplimiento de los requisitos de la información contable.

Teniendo en cuenta los principios básicos elementales de la seguridad de la información (integridad, confidencialidad y disponibilidad), se puede establecer su contribución al optimizar los requisitos de la información contable, convirtiéndose en el principal sostén del sistema contable en soporte tecnológico.

En el siguiente esquema se plantean los conceptos de la Seguridad de la Información que contribuyen al cumplimiento de los requisitos de la información contable.



El autor del presente trabajo destaca la definición de Teoría Contable publicada por la American Accounting Association en 1966, en donde se establece que “Nosotros definimos “teoría” como un conjunto consistente de principios hipotéticos, conceptuales y pragmáticos formando un marco de referencia general para un campo de estudio.

Extensión de la Teoría Contable:

Debido a los cambios en la tecnología y los avances en el

conocimiento de la conducta humana, el alcance y los métodos de la contabilidad están cambiando y se espera que continúen cambiando (...). Las principales áreas en las que están ocurriendo cambios, que pueden influir en la contabilidad del futuro, son percibidas como incluyendo:

- 1.2. Conocimiento de los procesos de decisión.
- 1.3. Conocimiento de las conductas humanas.
- 1.4. Tecnologías de la Computación y el diseño de sistemas.
- 1.5. Técnicas de medición y teoría de la información.”⁷

En el año 2013, cuarenta y siete años después, se han podido corroborar empíricamente los cambios sufridos en la disciplina contable por factores tecnológicos, normativos, legales, como también de índole social.

Al considerar que la Contabilidad toma conceptos de otras disciplinas, el autor del presente trabajo propone incluir a la Seguridad de la Información como una de las nuevas disciplinas influyentes en la contabilidad al considerar su innegable contribución al cumplimiento de los requisitos y el resguardo de la información contable.

⁷ American Accounting Association, 1966, “A Statement of Basic Accounting Theory”, AAA. Texto original: “We define “theory” as a cohesive set of hypothetical, conceptual and pragmatic principles forming a general frame of reference for a field of study.

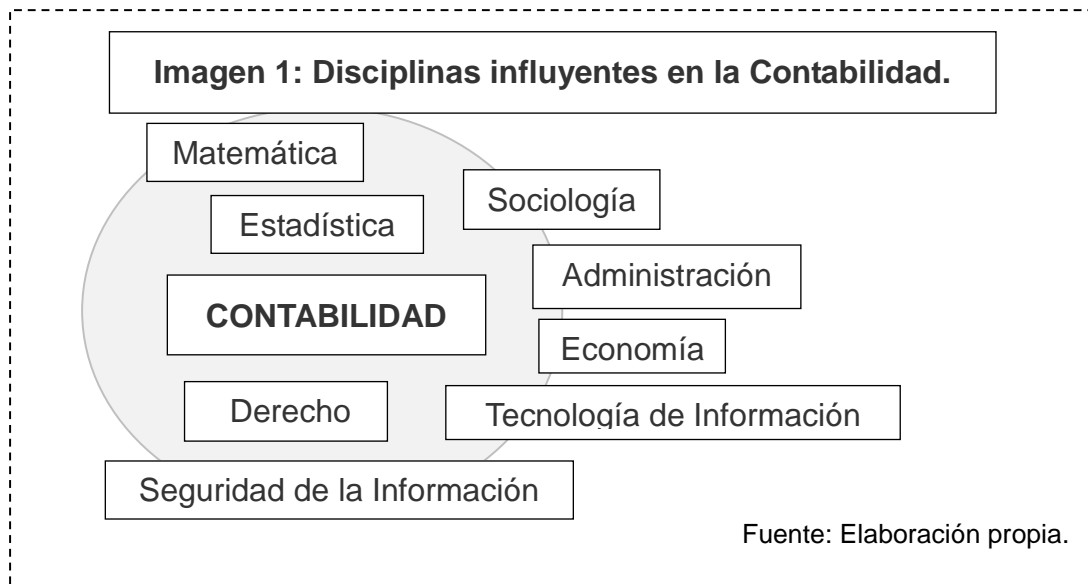
Extension of accounting Theory:

Because of technological changes and advances in knowledge of human behavior the scope and methods of accounting are changing and can be expected to continue to change. (...)

Major areas in which changes are occurring which will influence accounting in the future are perceived as including:

1. Knowledge of decision
2. Knowledge of human behavior.
3. Computer technology and system design.
4. Measurement techniques and information theory”.

Extraído de referencia bibliográfica N° [20].



Otro factor a destacar, es el planteo de la Seguridad de la Información como una disciplina separada de la Tecnología de la Información, ya que la misma incluye otros conceptos que no son específicamente tecnológicos como por ejemplo la Seguridad Física, que impacta en los activos de información de la organización.

Como se describió precedentemente, los elementos de los sistemas contables en un contexto tecnológico son los siguientes: Recursos Humanos, Medios de Registros, Cuentas a emplear, Aplicativos y Algoritmos para el registro de las operaciones, Modelos de informes a preparar, Sistemas operativos y Hardware, en donde la Seguridad de la información impacta en cada una de las partes como se puede observar en el siguiente cuadro:

Cuadro Nº 1: Elementos del Sistema contable y la Seguridad de la Información.		
Sistema de información contable en un contexto tecnológico	Elementos	Seguridad de la Información
	Recursos Humanos	Ética y compromiso con la organización
	Aplicaciones	Seguridad en los Aplicativos
	Sistemas Operativos	Seguridad en los Sistemas
	Hardware	Seguridad Física
Fuente: Elaboración Propia.		

Por todo lo expuesto, el objetivo de los siguientes capítulos consiste

en analizar la contribución de la Seguridad de la Información en los siguientes aspectos en los sistemas de registración contable:

- ✓ Legislación Nacional vigente.
- ✓ Doctrina del Derecho Contable.
- ✓ Disposiciones y resoluciones de los organismos de control.

1.4. Conclusiones particulares del Capítulo I.

La Contabilidad analizada como disciplina tiene influencia de numerosas ciencias básicas y aplicadas, que le aportan nuevas herramientas y características a cumplir para garantizar los requerimientos de la información de los diferentes grupos de interés.

El autor considera que la Seguridad de la Información debe contemplarse como una disciplina influyente sobre la contabilidad al contribuir con el cumplimiento de los requisitos de la información contable establecidos en el Marco Conceptual de la Información Contable e impactando en cada uno de los elementos que componen el sistema contable en una organización, como por ejemplo:

- Recursos Humanos,
- Medios de Registros,
- Cuentas a emplear,
- Aplicativos y Algoritmos para el registro de las operaciones,
- Modelos de informes a preparar,
- Sistemas operativos y Hardware.

Asimismo, la gestión de la Seguridad tiene efectos en cada uno de ellos, como en la administración la seguridad de los aplicativos y sistemas operativos, la seguridad física y la concientización del personal, entre otros. (Véase Cuadro N°1).

De esta manera, la Seguridad de la Información se convierte en el principal sostén de los requisitos a satisfacer por los Sistemas de Información Contable y no puede concebirse en el Siglo XXI una organización que prescindiera de las bondades que esta brinda.

- Capítulo II

2. MARCO LEGAL DE LOS REGISTROS CONTABLES.

2.1. Introducción.

En el presente capítulo se analiza el marco legal de los registros contables en contextos tecnológicos en la Ciudad Autónoma de Buenos Aires. En el mismo se describen los artículos relevantes del Código de Comercio, la Ley de Sociedades Comerciales y las opiniones más relevantes de la doctrina del derecho contable destacando la importancia de Seguridad de la Información en la legalidad de un sistema contable.

2.2. Obligación de llevar Registros Contables.

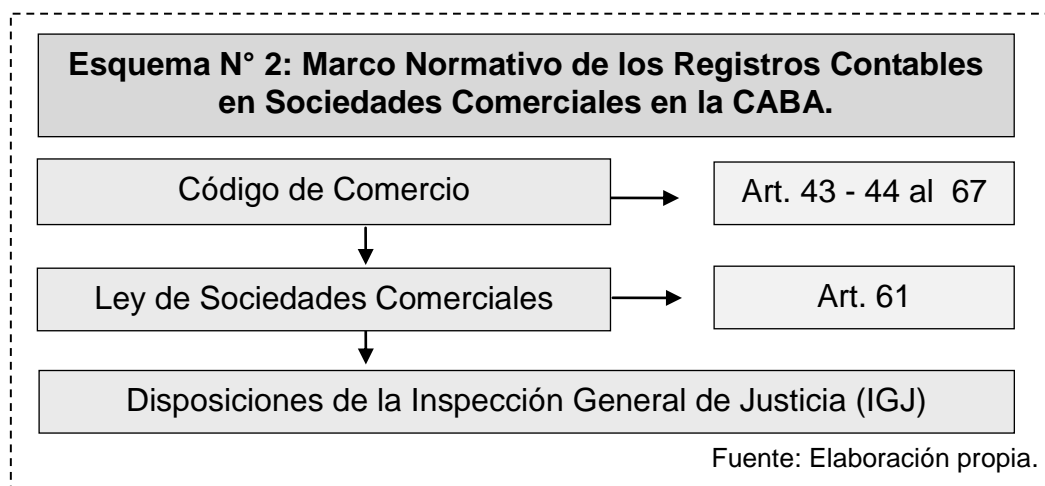
El Código de Comercio de la República Argentina, en el artículo 43 se establece que “todo comerciante está obligado a llevar cuenta y razón de sus operaciones y a tener una contabilidad mercantil organizada sobre una base contable uniforme y de la que resulte un cuadro verídico de sus negocios y una justificación clara de todos y cada uno de los actos susceptibles de registración contable. Las constancias contables deben complementarse con la documentación respectiva.”⁸ Por lo cual todo comerciante debe establecer, dependiendo de su envergadura, un sistema contable organizado en donde pueda registrar ordenadamente todas las transacciones consecuencia del desarrollo de sus actividades comerciales.

En el citado código se establece que los comerciantes deben indispensablemente llevar los libros “Diarios” e “Inventarios y Balances”; además los mismos deberán estar registrados, con la documentación

⁸ Véase referencia bibliográfica N° [35]

contable correspondiente, con una adecuada integración de un sistema de contabilidad y que le exijan “la importancia y la naturaleza de sus actividades de modo que de la contabilidad y documentación resulten con claridad los actos de su gestión y su situación patrimonial.”⁹

En el siguiente esquema se presenta el marco legal de las registraciones contables en la Ciudad Autónoma de Buenos Aires.



2.3. Los registros contables en formatos tecnológicos: Las características de la Ley de Sociedades Comerciales.

En el artículo 61 de la Ley de Sociedades Comerciales se establece que se podrán llevar libros de comercio en medios mecánicos, magnéticos o por ordenadores en la medida “que la autoridad de control o el Registro Público de Comercio autoricen la sustitución de los mismos (...), salvo el de Inventarios y Balances.”¹⁰

Para hacerse efectiva la autorización, se deberá realizar una petición que incluya una “adecuada descripción del sistema con un dictamen técnico o antecedentes de su utilización, lo que, una vez autorizada, deberá transcribirse en el libro de Inventarios y Balances.”¹¹

⁹ Véase referencia bibliográfica N° [34]

¹⁰ Véase referencia bibliográfica N° [35]

¹¹ Véase referencia bibliográfica N° [35]

La ley dispone también que el sistema de contabilización deba permitir “la individualización de las operaciones, las correspondientes cuentas deudoras y acreedoras y su posterior verificación, con arreglo al artículo 43 del Código de Comercio.”¹²

De esta manera, se autoriza la posibilidad de llevar el sistema contable en soportes tecnológicos, pero resulta muy importante cumplir con todos los requisitos expuestos, sino el ente es considerado que no mantiene los registros contables de legal forma conforme al plexo normativo vigente.

2.4. Requisitos exigidos en los Sistemas de Registración Contable.

Un sistema contable legalmente constituido para tutelar a los terceros en los conflictos individuales y universales, debe satisfacer fundamentalmente dos garantías:¹³

- Asegurar que los registros sean inalterables; ello implica las siguientes condiciones:
 - ✓ Que registraciones deben corresponder con el acontecimiento de los hechos y actos económicos;
 - ✓ Que una vez hecha las mismas, no puedan ser modificadas ni desaparezcan por “perención¹⁶ del soporte”¹⁴.
- Asegurar que las registraciones sean verificables:
 - ✓ Implica que deben estar expuestas, o volcarse, a un elemento que permita su fácil lectura y disponibilidad, para cuando un organismo de control, o el ámbito judicial lo solicite pertinente.

La doctrina no cuestiona los aspectos internos de su procesamiento, sino que pone énfasis en “cómo se registra en su faz de almacenamiento y conservación de los datos¹⁶ de modo de permitir la “inalterabilidad y verificabilidad”.¹⁵

Para cumplir con las dos garantías se plantea la necesidad de

¹² Véase referencia bibliográfica N° [35]

¹³ En los fundamentos en la exposición de Motivos de la L. 19550, Sec. IX, N 2, “in fine”, los miembros de la comisión Reformatoria dicen: la exigencia de la autorización previa, para el empleo de medios mecánicos u otros, se explican en función de que los métodos, en todo caso, deben asegurar la posibilidad de verificación y la imposibilidad de cambio, adulteración o sustitución de las registraciones.

¹⁴ Véase referencia bibliográfica N° [14]

¹⁵ Véase referencia bibliográfica N° [14]

incorporar conceptos y herramientas de la Seguridad de la Información para garantizar integridad, disponibilidad y confidencialidad del sistema de información contable.

2.5. Los Riesgos identificados por la Doctrina y el Derecho Contable de llevar una Contabilidad Informática.

Gran parte de la doctrina contable ha compartido en las últimas décadas preocupaciones referidas a los riesgos de que la contabilidad en contextos tecnológicos podría plantear en cuanto a la alteración y no verificabilidad de las registraciones.

En la siguiente tabla se enumeran los riesgos identificados derivados de la utilización de medios informáticos.

Tabla N° 2: Riesgos identificados por la Doctrina del Derecho Contable (Eduardo M. Favier Dubois).
1. Fraude por alteración del registro: “La alteración puede derivar, en primer lugar, de la conducta fraudulenta del usuario que altere cualquiera de las etapas del proceso: la entrada (información falsa), el procesamiento (programa fraudulento), el archivo, la conservación, la salida y la impresión de la información.”
2. Fraude por sustitución del soporte: “El usuario puede llevar un doble registro y exhibir el que más le conviene, o hacer una copia modificada para exhibir.”
3. Virus informático.
4. Perención del soporte ¹⁶ : “Dado que se trata de material tecnológico recientemente introducido a la industria de la informática, se carece de datos ciertos sobre la duración de los diversos soportes (magnéticos, ópticos, etc.), existiendo autorizadas opiniones que les asignan un lapso de perención entre cinco y diez años, según el uso, lo que impediría su consulta después de ese lapso.”
Véase referencia bibliográfica N° [14]

¹⁶ El autor Eduardo M. Dubois, utiliza el término, Perención del Soporte refiriéndose a la “durabilidad del soporte”; técnicamente está vinculada con la frecuencia de uso y las condiciones de ambientales de su resguardo.

2.6. La legalidad de un sistema de registros contables en contextos informáticos.

En jornadas profesionales derecho contable¹⁷ se ha concluido numerosas veces que la circunstancia de que se haya autorizado la utilización de libros contables por medios informáticos de registro¹⁸ no resulta suficiente para “considerar que su contabilidad está llevada de legal forma”.¹⁹ A tal efecto deberían verificarse en cada caso:

- “La transcripción del sistema en el libro de Inventarios y Balances llevado en legal forma.
- El efectivo cumplimiento del sistema oportunamente autorizado.
- Que dicho cumplimiento mantenga al presente la inalterabilidad y verificabilidad de las registraciones.”²⁰

Entender que basta con que los datos correspondientes estén “en el sistema contable – es decir, almacenados de la computadora –” a manera de simple complemento y no especificadas en el registro (impreso o no, pero sí imprimible de ser necesario), que observe adecuadamente todos esos requisitos intrínsecos, es incumplir con lo establecido en el artículo 61 de la Ley 19.550.

Por ello, cuando una entidad se defiende en cuanto al cumplimiento de la obligación de llevar los registros rubricados que incluyan las transacciones con detalle, justificando únicamente “que están en el sistema, está infringiendo dicha obligación”.²¹

2.7. Conclusiones particulares del Capítulo II.

En esta sección se analiza desde una perspectiva del derecho

¹⁷ Jornada sobre Derecho y Contabilidad Informática.

¹⁸ Establecido en el artículo N° 61 de la Ley de Sociedades Comerciales, N° 19550)

¹⁹ Véase referencia bibliográfica N° [38]

²⁰ Véase referencia bibliográfica N° [44]

²¹ Véase referencia bibliográfica N° [36]

contable las formalidades que deben cumplirse en una “contabilidad informatizada”. La Ley 19.550 de Sociedades Comerciales autoriza en el artículo 61 a llevar el sistema contabilidad en soportes tecnológicos, pero ello no es suficiente para que sea considerada en legal forma. Para eso deben observarse mínimamente los siguientes requisitos:

a. Pedir autorización y cumplir con las disposiciones de la autoridad de Control, que en la Ciudad Autónoma de Buenos Aires corresponde a la Inspección General de Justicia,

b. Puesta en funcionamiento y utilización del sistema oportunamente solicitado,

c. Transcripción del “sistema utilizado en el libro de inventarios y balances”²²,

d. Tomar las medidas necesarias para garantizar la inalterabilidad y verificabilidad de las registraciones contables.

La doctrina del derecho contable plantea la necesidad de que los sistemas de información contables deben garantizar la inalterabilidad y verificabilidad de sus registros como ya se ha expuesto. Para el cumplimiento de ambos principios se hace indispensable implementar normas o pautas de gestión y el uso de herramientas de Seguridad de la Información.

Estos requisitos no son tenidos en cuenta debidamente por gran cantidad de empresas en la República Argentina, razón por la cual en el caso de inspecciones o conflictos judiciales sufren las consecuencias derivadas de no contar con sistema de información contable legalmente constituido.

²² El libro inventario y balances es uno de los libros exigidos en el Código de Comercio.

- Capítulo III

3. REQUERIMIENTOS DE LA INSPECCIÓN GENERAL DE JUSTICIA EN EL ÁMBITO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES.

3.1. Introducción.

Si las sociedades comerciales implementan sistemas de registros en medios tecnológicos deben cumplir con los requisitos exigidos por los organismos de contralor. En el ámbito de la Ciudad Autónoma de Buenos Aires está presente la Inspección General de Justicia (IGJ) que tiene competencia de fiscalización de las Sociedades Comerciales, entre otras funciones.

La IGJ establece que los sistemas de registros contables deben cumplir con los requisitos enunciados a continuación:

Tabla N° 3: Requisitos de los Sistemas Contables (IGJ).
1. "Se lleven mediante los registros contables necesarios para disponer de un sistema de contabilidad orgánico, adecuado a la importancia y naturaleza de las actividades del ente."
2. "Los registros contables tengan una denominación inequívoca y concordante con la función que cumplan y se evite la superposición de registros que contengan información similar y puedan inducir a confusión."
3. "Ofrezcan elevado grado de inalterabilidad de las registraciones volcadas, el que estará sustentado en controles internos de tipo administrativo contable y otros de tipos operativos o programados, aplicables sobre la información de entrada, su procesamiento e información de salida. Dicha inalterabilidad buscará impedir que se genere más de un proceso de registración por cada hecho económico y que asimismo, toda anulación de cualquier proceso, se logre a través de un asiento de ajuste."
4. "Permitan determinar la evolución y situación del patrimonio, incluyendo los resultados obtenidos, individualizar los registros y datos de análisis en que se basan los informes contables y su correlación con los documentos o comprobantes respaldatorios y localizar

éstos a partir de los registros contables y viceversa, para lo cual los primeros deberán ser archivados en forma metódica que facilite la interrelación.”

Fuente: IGJ. Véase referencia bibliográfica N° [25].

Teniendo en cuenta estas características principales se analizarán las diferentes cuestiones que deben cumplirse para llevar a cabo la implantación de un sistema de información contable en un contexto tecnológico.

3.2. Condiciones de los sistemas de registración contable resguardados en medios tecnológicos.

La utilización de los sistemas de registros contables en medios de almacenamiento electrónicos como: compact disc, discos ópticos y microfilmes, ya sean microfichas o rollos²³, etc., debe ajustarse a los siguientes requerimientos:

- ✓ **Existencia de un sistema de numeración de los medios de almacenamiento.**

Los elementos utilizados como soporte de almacenamiento deberán ser numerados correlativamente desde el número uno (1) en adelante²⁴, para cada registro y por cada ejercicio económico, sin perjuicio del número de identificación de origen que les corresponda.

- ✓ **Cumplimiento de las características del soporte de almacenamiento de los registros contables.**

La información almacenada en el medio de soporte, no podrá ser eliminada ni reescrita, debiendo poder ser leída la cantidad de veces que fuere necesario, sin deteriorarse.²⁵ En el caso de la utilización de CDs y DVDs como medio de almacenamiento, no se deberían utilizar los

²³ El plexo normativo de la IGJ se especifican los siguientes medios de almacenamientos: compact disc, otros discos ópticos y microfilmes, o similares.

²⁴ Véase referencia bibliográfica N° [25].

²⁵ Véase referencia bibliográfica N° [26].

regrabables.

✓ **Calidad del soporte de almacenamiento de los registros contables.**

Los medios de registro deberán cumplir con patrones de calidad e inalterabilidad que “impidan cualquier alteración a la información guardada y permitan su conservación”²⁶ por el período de exigencia legal.

✓ **Establecimiento de controles internos a implementar en la operatoria de almacenamiento.**

La emisión de los soportes señalados deberá ser factible de obtenerse como parte de la operatoria habitual, debiendo los mismos estar “respaldados por normas escritas aprobadas por el órgano de administración de la sociedad y copiadas en el libro de Inventarios y Balances, o en un libro especial que cumpla con los requisitos formales del Código de Comercio.”²⁷

✓ **Demostración técnica del grado de inalterabilidad.**

En la normativa se establece que se debe demostrar “el grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto”²⁸, con lo cual se debería realizar una auditoría de la Seguridad de la Información del sistema contable para corroborar como mínimo las cuestiones enunciadas en el siguiente cuadro:

²⁶ Véase referencia bibliográfica N° [27].

²⁷ Véase referencia bibliográfica N° [28].

²⁸ Véase referencia bibliográfica N° [29].

Cuadro N° 2: Puntos de Auditoría de la Seguridad de la Información.		
Número	Descripción	Aclaraciones mínimas
1	Plataforma de Hardware utilizada.	Si el Hardware utilizado se corresponde con el nivel de transacciones de la operatoria de la empresa. Si se cambiaran los soportes, se debería poder consultar los registros anteriores en cualquier momento si así fuera requerido.
2	Plataforma de Software de Base y Aplicaciones utilizadas.	La correcta instalación y actualización del Software utilizado, con herramientas debidamente instaladas.
3	Políticas de Gestión de Seguridad informática	Las políticas de seguridad implementadas.
4	Control de Accesos Lógicos y Físicos	Análisis de los Controles de Accesos Lógicos y Físicos implementados.
5	Back-up / Archivo de la documentación respaldatoria / Plan de contingencia	La política de copias de respaldo y su correcta comprobación.
6	Pautas de Confiabilidad.	Análisis de las pautas de confidencialidad con los empleados Implementadas.
7	Integridad de los Registros Contables	Comprobación de la utilización de Funciones de Hash para garantizar la inalterabilidad de los registros en los diferentes soportes.
Fuente: Elaboración Propia.		

También se establecen las particularidades que deben contener las actas de registración de los registros contables en formato tecnológico. La información contable a incluir deberá contener:

- ✓ Número de acta inicial y final.
- ✓ Número de identificación del soporte.
- ✓ Cantidad de registros en él contenida.
- ✓ Período que corresponde.

Además, se debe cumplir con los siguientes requisitos:

- ✓ “Deben ser firmadas por el representante legal de la sociedad”, y
- ✓ “Trimestralmente, el órgano de fiscalización, verificará el cumplimiento

de las condiciones señaladas en los incisos que anteceden, emitiendo al respecto un informe especial que se registrará con su firma en el libro de Inventarios y Balances.”²⁹

3.3. Trámites y requisitos solicitados por la IGJ.

Para iniciar el trámite de autorización para el empleo de ordenadores se deben cumplir con los siguientes elementos:

Cuadro N° 3: Autorización para empleo de ordenadores (IGJ).		
Elementos	Características	Notas
1. Primer testimonio de escritura pública o instrumento privado original con los recaudos del artículo 36, incisos 1 y 2.	<p>Si se solicita la autorización de sistema en medios ópticos:</p> <ul style="list-style-type: none"> - La resolución social debe contener expresamente el compromiso de preservar la posibilidad de lectura de los medios de registración durante el período en que la ley determina obligatoria su exigibilidad. - Extender en listados de papel los registros que solicite cualquier organismo de contralor, tribunal de justicia u otra autoridad competente con atribuciones al efecto. <p>Para el caso de progresos tecnológicos:</p> <ul style="list-style-type: none"> - Mantener la vigencia de las máquinas lectoras durante el período que la ley determina como exigibles a los registros contables, o bien el compromiso de volcar la información necesaria en los nuevos medios de registración que incorpore la tecnología. 	Para el desarrollo de esta actividad requiere los conocimientos de un Contador Público.
2. Las siguientes piezas firmadas por el representante legal o apoderado con facultades suficientes y por contador público independiente.	<ul style="list-style-type: none"> a) La exposición amplia y precisa del sistema de registración contable a utilizar. Debe incluirse la denominación exacta de los registros que se llevarán mediante el sistema y la de los libros que se reemplazan. b) Flujograma exponiendo el circuito administrativo–contable de los registros a autorizar; c) Demostración técnica del grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto; 	Para el desarrollo de esta actividad la norma requiere los conocimientos de un Contador Público matriculado, pero sería adecuado un experto en tecnología de la Información y

²⁹ Véase referencia bibliográfica N° [30].

	<p>d) El sistema y periodicidad en la numeración de los registros;</p> <p>e) La nómina de los libros y registros contables autorizados a la fecha de la presentación, indicando sus datos y fecha de rúbrica o autorización y la fecha y folio de la última registración practicada;</p> <p>f) Modelos en blanco por duplicado y uno ejemplificativo;</p> <p>g) Plan de cuentas.</p>	Seguridad de la información.
3. Dictamen de precalificación de un contador público.		Se requiere el título de Contador Público.
Fuente: IGJ – Véase referencia bibliográfica N° [29].		

Una vez aprobado el trámite de autorización hay que cumplir con los siguientes informes dispuestos por la IGJ:

- Informe Anual.
- Informa de actualización técnica.
- Otros que requiera la IGJ.

En el siguiente cuadro se especifican las características más relevantes:

Cuadro N° 4: Informes periódicos medios magnéticos u otros. (IGJ)		
Informes	Características	Profesionales
I- Información anual; certificación.	<p>Las sociedades que obtengan la autorización requerida por el artículo 61 de la Ley N° 19.550, deberán, a partir del ejercicio económico de cierre inmediato siguiente a ella, dentro de los ciento veinte (120) días de cada cierre, presentar a la Inspección General de Justicia un informe especial suscripto por contador público independiente, conteniendo:</p> <ol style="list-style-type: none"> 1. La descripción exacta del sistema utilizado durante el ejercicio económico. 2. Opinión fundada sobre la concordancia existente entre el sistema de registración contable utilizado durante dicho ejercicio y el oportunamente 	Se requiere el título de Contador Público.

	<p>autorizado.</p> <p>De no existir observaciones, se emitirá a la sociedad una certificación que así lo indicará, la cual deberá ser agregada al libro de Inventarios y Balances y será condición necesaria para que se considere a la contabilidad regularmente llevada.</p>	
II- Informe de actualización técnica.	* Este informe se desarrolla a continuación.	Se requiere de un profesional en Tecnología y/o Contador Público.
III – Otros que requiera la IGJ.	Podrá reglamentar el cumplimiento de recaudos adicionales, incluida la exigencia de que, si su volumen lo justificare, el movimiento contable de la sociedad sea volcado a soporte papel.	Se requiere el título de Contador Público.
Fuente: IGJ - Véase referencia bibliográfica N° [25].		

- Informe bianual de actualización técnica.

Este informe debe ser presentado cada dos años, acompañado del formulario correspondiente y copia de la autorización emitida y un informe de un Técnico Informático y/o Contador Público Nacional con la firma legalizada por la superintendencia de la matrícula respectiva. “En caso de informarse la obsolescencia del sistema utilizado, debe incluirse un proyecto de actualización técnica del mismo y de las medidas y reemplazos necesarios para lo que se deberá pedir una nueva autorización. La documentación debe contener también la firma del representante legal de la sociedad o ser ratificada mediante escrito suscripto por el mismo con firma y cargo certificados notarialmente.”³⁰

3.4. Conclusiones Particulares del Capítulo III.

La Inspección General de Justicia describe rigurosas características a cumplir en el caso que una Sociedad Comercial solicite llevar los registros y libros contables en soportes tecnológicos.

En la Resolución General 7 del año 2005 se enuncian los diferentes

³⁰ Véase referencia bibliográfica N° [24].

trámites a efectuar para autorizar y mantener los sistemas contables. Para obtener la autorización hay que cumplir con los siguientes requisitos relacionados con la seguridad de la información:

- La exposición amplia y precisa del sistema de registración contable a utilizar. Debe incluirse la denominación exacta de los registros que se llevarán mediante el sistema y la de los libros que se reemplazan; y
- Demostración técnica del grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto;

En donde resulta necesario el auxilio de un especialista para el análisis de los siguientes puntos de control sugeridos en el capítulo:

- Plataforma de Hardware utilizada.
- Plataforma de Software de Base y Aplicaciones utilizadas.
- Políticas de Gestión de Seguridad de la Información.
- Control de Accesos Lógicos y Físicos.
- Back-up / Archivo de la documentación respaldatoria.
- Plan de contingencia.
- Pautas de Confiabilidad.
- Integridad de los Registros Contables.

La misma opinión surge para el caso del Información bianual de actualización técnica en donde resulta ineludible la actuación profesional de un especialista en tecnología y seguridad con un Contador Público matriculado.

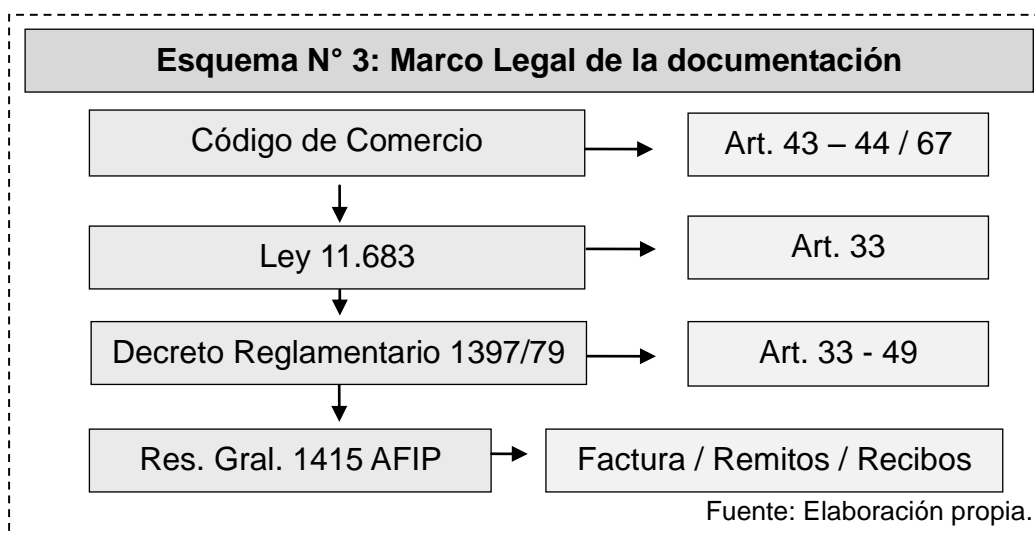
- Capítulo IV

4. PROCEDIMIENTO GENERAL DE EMISIÓN, CONVERSIÓN Y CONSERVACIÓN DE LA DOCUMENTACIÓN RESPALDATORIA DE LOS REGISTROS CONTABLES.

4.1. Introducción.

Además de las disposiciones establecidas por la Inspección General de Justicia, la Administración Federal de Ingresos Públicos (AFIP) establece normas a implementar en los sistemas de información contable para la emisión, conversión y conservación de la documentación respaldatoria.

En el siguiente esquema se especifican las normas relacionadas con la documentación respaldatoria vigente:



En este capítulo se analizarán las Resoluciones Generales (RG) que establecen normas y procedimientos en el tratamiento de la documentación respaldatoria de los registros contables.

4.2. Régimen de emisión de comprobantes y registración de Operaciones.

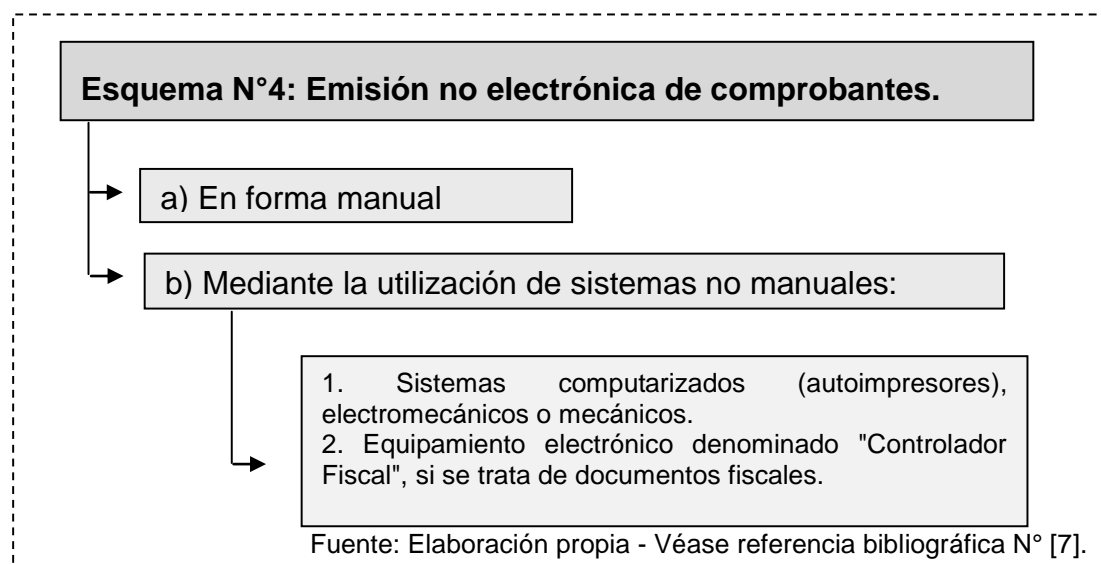
La AFIP establece que la emisión de los comprobantes se efectuará en forma manual, mediante sistemas no manuales, o la emisión electrónica. A continuación se desarrollan las partes pertinentes de cada una.

4.2.1. Sistemas de emisión manual y mediante sistemas no manuales.

La emisión manual de comprobantes será en forma manuscrita, utilizando un talonario de facturas o documentos equivalentes, mediante la utilización de computadoras (únicamente si se las utiliza como procesador de texto), o del equipamiento electrónico denominado "Controlador Fiscal", si se trata de documentos no fiscales homologados o documentos no fiscales.

La emisión de documentación mediante la utilización de sistemas no manuales se basa en sistemas computarizados (autoimpresores), electromecánicos o mecánicos; y en los citados equipos denominados "Controladores Fiscales", si se trata de documentos fiscales.

Para la emisión de comprobantes podrán utilizarse, en forma complementaria o alternativa: sistemas manuales y computarizados. Asimismo, se deberá disponer de comprobantes impresos por imprenta para su utilización cuando se encuentre inoperable el sistema no manual de emisión.



✓ REQUISITOS TÉCNICOS DE SISTEMAS NO MANUALES:

Los sujetos exentos frente al impuesto al valor agregado cuando cumplan con determinadas características³¹, podrán imprimir sus comprobantes sin intervención de una imprenta o empresa gráfica, siempre que utilicen un sistema de impresión con tecnología láser o electrónica por deposición de iones, que cumpla mínimamente con los siguientes requisitos técnicos:

a) Impresora:

1. *Velocidad de impresión no menor a CINCUENTA (50) páginas por minuto;*
2. *Impresión de fondo de seguridad.*

b) Computadora;

1. *Memoria RAM no menor a OCHO (8) megabytes.*
2. *Disco rígido o capacidad de almacenamiento en disco rígido superior a SESENTA (60) megabytes.*³²

Pero no se establecen requisitos relacionados con la seguridad de la información.

4.2.2. Régimen especial de emisión y almacenamiento de duplicados electrónicos.

De conformidad con lo establecido por la Resolución General N° 1361, *“los sujetos que revistan el carácter de responsables inscritos o exentos frente al impuesto al valor agregado, podrán optar por el régimen especial de emisión y almacenamiento de duplicados de comprobantes electrónicos.”*³³

El régimen especial de emisión y almacenamiento electrónico comprende³⁴ DOS (2) sistemas de emisión de comprobantes electrónicos:

- a) "Régimen de Emisión de Comprobantes Electrónicos", que en adelante se denominará "R.E.C.E.".

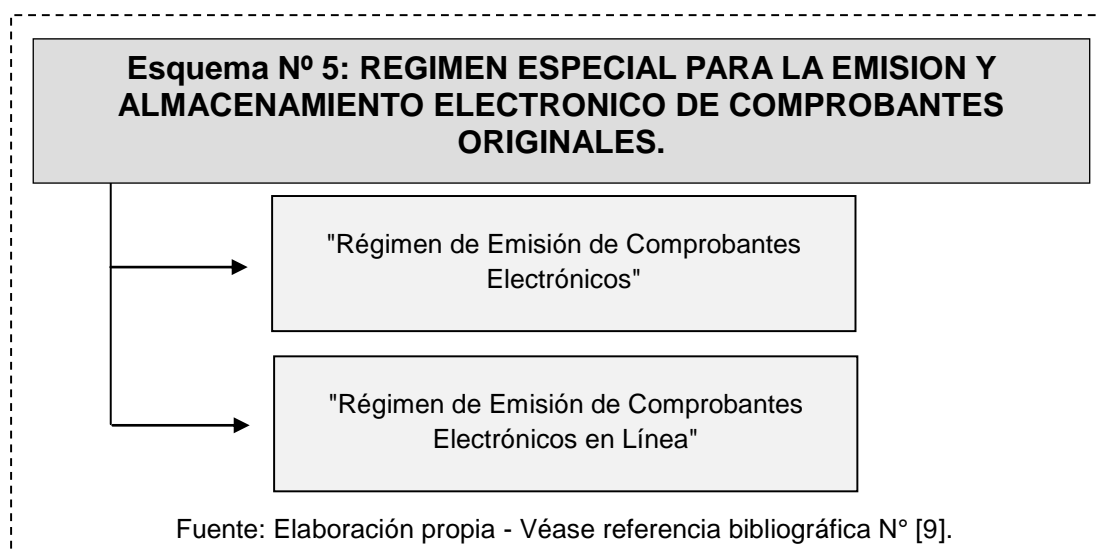
³¹ Cuando se encuentren dentro de la jurisdicción de la Dirección de Operaciones Grandes Contribuyentes Nacionales o comprendidos en el Sistema Integrado de Control Especial.

³² Véase referencia bibliográfica N° [7].

³³ Véase referencia bibliográfica N° [2].

³⁴ Véase referencia bibliográfica N° [9].

b) "Régimen de Emisión de Comprobantes Electrónicos en Línea", que en adelante se denominará "R.C.E.L."



En este régimen se encuentran comprendidos los contribuyentes y/o responsables que revistan con el carácter de inscriptos en el impuesto al valor agregado y los que se encuentren adheridos al Régimen Simplificado para Pequeños Contribuyentes (RS) – (Monotributo). Los sujetos obligados por las disposiciones legales sólo podrán utilizar el R.E.C.E. mientras que los optativos podrán utilizar cualquiera de los dos.

- SOLICITUD DE AUTORIZACION DE EMISION DEL COMPROBANTE ELECTRONICO:

A los efectos de confeccionar los comprobantes electrónicos originales³⁵, deberán "solicitar por Internet a esta Administración Federal la autorización de emisión pertinente."³⁶

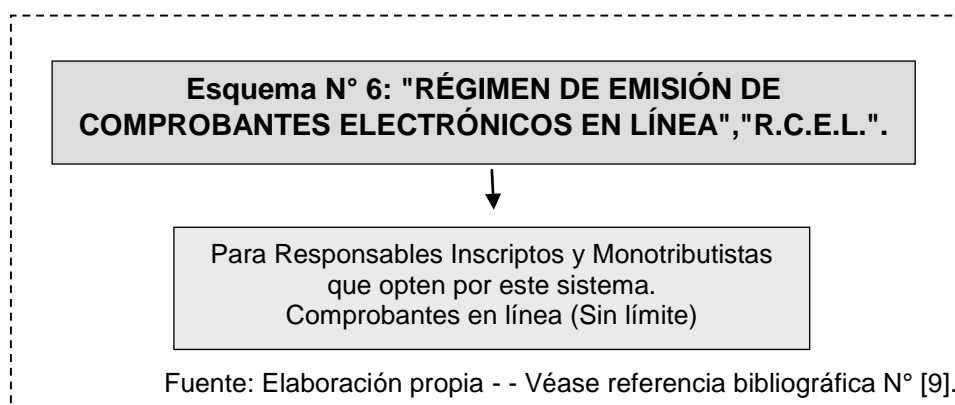
De tratarse de los contribuyentes que utilicen el sistema "R.E.C.E.", la solicitud se realizará mediante alguna o algunas de las siguientes opciones:

³⁵ Establecido por la AFIP como "clases "A", "A" con leyenda "PAGO EN C.B.U. INFORMADA", "M", "B" y/o "C" según corresponda".

³⁶ Véase referencia bibliográfica N° [10].

- Procedimiento Mediante Aplicativos
- Procedimiento Mediante Web Services
- Procedimiento Mediante Factura en Línea

De tratarse de los sujetos que opten por el sistema "R.C.E.L.", y en tanto no se encuentren obligados, deberán solicitar a la Administración Federal la autorización de emisión pertinente.



Dicha solicitud se realizará utilizando el servicio "Comprobantes en línea" para lo cual deberá contar con "Clave Fiscal" habilitada con Nivel de Seguridad 2.³⁷ En este caso no habrá límite de comprobantes, pero el sistema de facturación es equivalente al anterior.

4.3. Registración de la documentación respaldatoria.

Los comprobantes que se emitan o se reciban como respaldo documental de las operaciones realizadas serán registrados en libros o registros correspondientes. Dicha registración se efectuará en forma manual o mediante la utilización de sistemas computarizados utilizados.

Los libros o registros se deben encontrar en el domicilio fiscal del contribuyente y/o responsable a disposición del personal fiscalizador de la Administración Federal.

En el siguiente cuadro se especifican las características a cumplir:

³⁷ La AFIP establece 4 niveles de seguridad para obtener la clave fiscal, con características específicas para personas físicas, jurídicas y sucesiones indivisas. En cada uno de los niveles se establecen requisitos específicos para su obtención y particularidades en relación a los posibles trámites a realizar a través de internet.

Cuadro N° 5: Clasificación de las formas de Registración.	
Registración en forma manual	Cuando las registraciones se efectúen mediante métodos manuales, los libros o registros deberán estar encuadernados y foliados. Se considera, también, como método manual, la modalidad de transcribir a libros copiadores la registración previamente efectuada en hojas móviles copiativas.
Registración mediante la utilización de sistemas computarizados	En el caso de utilizarse sistemas computarizados para efectuar la registración, las hojas contendrán DOS (2) numeraciones: “a) Una preimpresión al momento de su adquisición, que debe ser progresiva —no necesariamente consecutiva—, y b) otra asignada por el sistema utilizado, que debe ser consecutiva y progresiva.” ³⁸
Fuente: Elaboración propia - Véase referencia bibliográfica N° [10].	

4.3.1. Régimen de Almacenamiento Electrónico de Comprobantes

De acuerdo con lo dispuesto por la Resolución General N° 1361, los “contribuyentes y responsables que se encuentran obligados a utilizar sistemas computarizados para efectuar las registraciones de los comprobantes emitidos y recibidos y almacenar electrónicamente dichas registraciones”³⁹, así como los que optaron por él, deberán efectuar:

a) La registración de los comprobantes emitidos y recibidos, de acuerdo con los diseños de registro especificados en la Resolución General N° 1361.

b) El almacenamiento y el resguardo de las registraciones de los comprobantes emitidos y recibidos, en la forma, plazo y características que se establecen a continuación:

A. Soportes para el almacenamiento.

Los archivos de los duplicados electrónicos de comprobantes deberán almacenarse por mes calendario en alguno de los soportes detallados en el

³⁸ Véase referencia bibliográfica N° [8].

³⁹ Véase referencia bibliográfica N° [6].

Cuadro N° 2, no pudiendo contener estos últimos datos referidos a distintos períodos.

Cuadro N° 6: ESPECIFICACIONES SOBRE LOS SOPORTES DE UNICA GRABACION Y MULTIPLES LECTURAS (WORM).			
Tipo de Soporte	Descripción	Capacidad de almacenamiento	Vida útil requerida
CD-ROM	Discos compactos	650 Megabytes	Mayor a 10 años
DVD-ROM	Discos Versátiles Digitales	3.95 Gigabytes	Mayor a 10 años
OPTICAL DISK	Discos ópticos	Desde 1 Gigabyte en adelante	Mayor a 10 años
Fuente: Resolución General - Véase referencia bibliográfica N° [2].			

El contribuyente podrá cambiar el tipo de soporte a utilizar siempre que se trate de cualquiera de los detallados.

B. Backup y lugar de resguardo.

El sujeto adherido al régimen deberá resguardar dos (2) copias de los archivos en soportes independientes y en lugares que aseguren su integridad y protección física. Las copias deberán encontrarse a disposición del personal fiscalizador de esta Administración Federal y conservarse según el siguiente detalle:

“a) Una de ellas en el domicilio fiscal del responsable, o en el determinado conforme las previsiones de la Resolución General N° 418.

b) La restante en una edificación que diste a más de DOSCIENTOS (200) metros del lugar donde se almacena la copia indicada en el inciso precedente.”⁴⁰

⁴⁰ Véase referencia bibliográfica N° [4].

C. Plazo para el resguardo de las copias.

El resguardo de las copias mencionadas en el artículo precedente “deberá efectuarse dentro de los primeros QUINCE (15) días del mes inmediato siguiente a aquél en el cual se haya producido la emisión del comprobante.”⁴¹

D. Código de Seguridad.

Sobre los archivos de los duplicados electrónicos se ejecutará un algoritmo de seguridad, cuyo proceso resultará una secuencia de caracteres representativa de su contenido denominada "Código de Seguridad —CS—"⁴², el cual deberá resguardarse en el mismo soporte. A tal fin, se utilizará el programa aplicativo que aprobará la Administración Federal.

E. Modificación de la Información Almacenada.

Cuando se produzca una modificación de la información almacenada de en los soportes mencionados se deberá confeccionar un nuevo soporte que contenga la información y "*Código de Seguridad —CS—*" rectificativos.

4.3.2. Conservación de comprobantes comerciales.

Un punto relevante en relación con los registros y documentación respaldatoria, es la obligación de un ente de resguardar los comprobantes citados consecuencia del desarrollo de una actividad.

A continuación se analizarán las partes pertinentes más importantes de la Resolución General N° 1361 en relación con la Conservación de registros y documentación respaldatoria.

⁴¹ Véase referencia bibliográfica N° [5].

⁴² Véase referencia bibliográfica N° [6].

✓ **Conservación de comprobantes y registros.**

La documentación respaldatoria y los libros o registros, deberán permanecer a disposición de esta Administración Federal en el domicilio fiscal del contribuyente y/o responsable. Las copias y los originales de los comprobantes emitidos o recibidos, respectivamente, y los libros o registros utilizados, serán conservados en archivo, de acuerdo con lo establecido por el artículo 48 de la Reglamentación de la Ley N° 11.683.

El remito, la guía o documento equivalente, las notas de pedido, órdenes de trabajo, presupuestos y/o documentos de análogas características serán conservados durante un período no inferior a los DOS (2) años contados a partir de la fecha de su emisión inclusive.

4.3.3. Cuestiones específicas de la emisión de comprobantes electrónicos.

En la transferencia de las facturas por el sistema de web service se utiliza tecnología PKI, “pero los certificados no validan a una persona sino a una computadora que interactúa con los servidores de AFIP. No se utiliza firma digital.”⁴³

“Las facturas electrónicas con la sola implementación de las especificaciones de AFIP, son un documento tributario que no tiene asegurada su integridad, en especial en lo referido al detalle de lo facturado.” Para lograrlo es necesario calcular su hash o mejor aun, firmarlo electrónicamente o digitalmente cuando sea posible.

“Si bien las críticas expuestas en forma tacita o explicita pueden resultar muy duras, las mismas surgen a la luz como consecuencia de los avances tecnológicos y de la necesidad de actualización permanente a la que estamos obligados.”⁴⁴

En relación con la emisión de la factura digital, la AFIP autorizará o rechazará la solicitud de emisión de comprobantes electrónicos. Los mismos no tendrán efectos fiscales frente a terceros hasta que este Organismo

⁴³ Véase referencia bibliográfica N° [37].

⁴⁴ Véase referencia bibliográfica N° [31].

otorgue el Código de Autorización Electrónico "C.A.E.". ⁴⁵

En todos los casos, cuando se detecten inconsistencias en los datos vinculados al emisor, la AFIP puede rechazar la solicitud pudiendo éste emitir un comprobante a través de otros medios si correspondiere; o solicitar nuevamente la autorización de emisión electrónica, una vez subsanado el inconveniente. El responsable deberá “conservar por el término de DOS (2) años la constancia de recibo de la solicitud que emite el sistema como prueba de su recepción por parte de este organismo.”⁴⁶

4.4. Conclusiones particulares del Capítulo IV.

El avance de la tecnología⁴⁷ es incesante y la legislación debería acompañar los nuevos medios de registración y procesamiento de información.

“En el campo impositivo se estableció para los contribuyentes la posibilidad de almacenar el duplicado de facturas, notas de débito y crédito, mediante el cual se puede guardar la información en medios electrónicos”⁴⁸ bajo ciertos requisitos explícitos.

En los sistemas previstos por la AFIP para la emisión de comprobantes, manuales, no manuales y electrónicos, deben cumplir con las siguientes condiciones con el resguardo de la información:

- Soportes para el almacenamiento: Se deben utilizar soportes de única grabación y múltiples lecturas como CD-ROM, DVD-ROM y OPTICAL DISK.
- Políticas de Backup: El sujeto adherido al régimen deberá resguardar dos (2) copias de los archivos en soportes independientes y en lugares que aseguren su integridad y protección física.
- Plazo para el resguardo de las copias: El resguardo de las copias deberá efectuarse dentro de los primeros QUINCE (15) días del mes.
- La utilización de un Código de Seguridad sobre los duplicados electrónicos.
- Procedimientos en la modificación de la Información Almacenada.

Según el académico Alfredo R. Popritkin, “le otorga valor probatorio la

⁴⁵ Véase referencia bibliográfica N° [11].

⁴⁶ Véase referencia bibliográfica N° [11].

⁴⁷ Véase referencia bibliográfica N° [42].

⁴⁸ Véase referencia bibliográfica N° [39].

imposibilidad de modificar su contenido a través del uso de soportes de única grabación y múltiples lecturas (no regrabables) y el control fehaciente de la fecha de generación. Disminuye su valor probatorio la facilidad de modificación de su contenido o generación de copias adulteradas sin posibilidad de control fehaciente de la fecha de grabación.⁴⁹ Para poder contrarrestar esta posibilidad de fraude y cambio de los archivos utilizados, se deberían emplear algún algoritmo confiable de hash para asegurar la integridad de la información.

⁴⁹ Véase referencia bibliográfica N° [40].

- Capítulo V

5. IMPLICANCIAS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA DE INFORMACIÓN CONTABLE.

5.1. Introducción.

En el año 2000, en la República Argentina se promulgó la ley 25.326 de Protección de Datos Personales, en donde se estableció, entre otras obligaciones, que las bases de datos o archivos públicos y privados, destinados a proporcionar informes, deben estar inscriptos en un registro especial.

En el sistema de registros contables de las organizaciones existen numerosas bases de datos que contienen y analizan información personal, emitiendo diferentes tipos de informes cuyos archivos deberían estar registrados para cumplir con el marco legal vigente.⁵⁰

En este capítulo, se analiza la ley de la Protección da Datos personales y su vinculación con la información contenida en los Sistemas de información Contable informatizados.

5.2. Reconocimiento de las Bases de Datos presentes en las Organizaciones. Conceptos y objetivos de la Ley 25.326.

El principal objetivo de la 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

⁵⁰ Véase referencia bibliográfica N° [16].

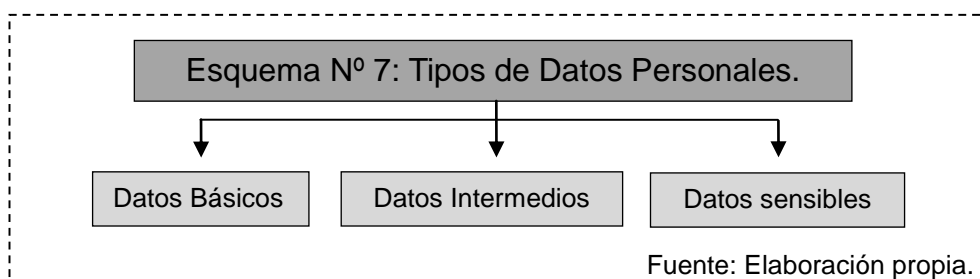
intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.”¹⁶ La ley toma en cuenta tanto los datos de las personas de físicas como los de las de existencia ideal.

A continuación se analizan las secciones más relevantes de la ley, prestando mayor interés a la emisión y conservación de comprobantes comerciales.

5.3. 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”⁵¹.

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.



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.

⁵¹ Véase referencia bibliográfica N° [43].

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.”⁵²

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

Cuadro N° 7: Comprobantes y documentación de Comercio.		
Tipo de Comprobante	Características	Tipo de Dato
Facturas	Si determina el cliente	Datos Intermedios
Notas de Débito	Si determina el cliente	Datos Intermedios
Notas de Crédito	Si determina el cliente	Datos Intermedios
Remitos	Si determina el cliente	Datos Intermedios
Cupones de Tarjeta de Crédito / Débito.	Si determina el cliente	Datos Intermedios
Fuente: Elaboración propia.		

Cuadro N° 8: Comprobantes Internos.		
Tipo de Comprobante	Características	Tipo de Dato
Órdenes de Pago	Si determina el Cliente	Datos Intermedios
Órdenes de Fabricación	Si determina el Cliente	Datos Intermedios
Legajos de Clientes	Siempre	Datos Intermedios
Asientos Diarios	-	Datos Intermedios
Papeles de Trabajo que	-	Datos Intermedios

⁵² Véase referencia bibliográfica N° [33].

determinan Clientes.		
Fuente: Elaboración propia.		

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 los mismos, sus gustos y preferencias por productos o marcas, entre otras cosas.

Con respecto a las Bases de Datos existentes en una empresa, se encontraron las siguientes:

Cuadro Nº 9: 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.	

Cuadro Nº 10: Relacionados con otras personas físicas y jurídicas.		
Tipo de Comprobante	Características	Tipo de Dato
Sistemas de órdenes de compra y órdenes de pago.	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 conformados por datos intermedios y sensibles, que son utilizados para confeccionar declaraciones juradas, aportes y contribuciones, asignaciones familiares, entre otros.

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 DNPDP. No se

debería considerar únicamente como una obligación, sino también como una ventaja competitiva en el manejo de la información.

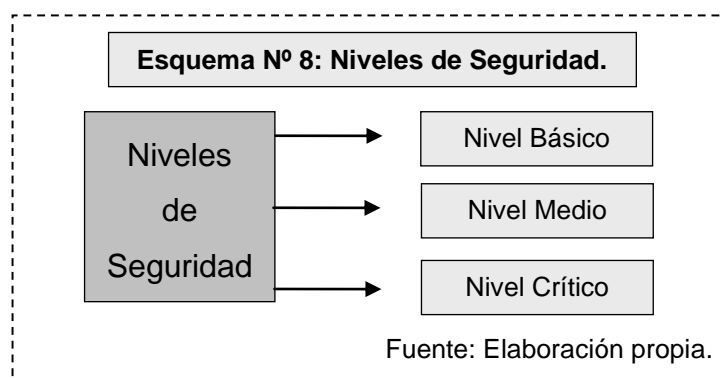
5.4. Seguridad de los Datos

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 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 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.⁵³



⁵³ A los interesados en ampliar la información sobre el tema, podrán consultar en página web indicada en la bibliografía del presente trabajo la resolución completa N° 11/2006 de la DNPDP. Véase referencia bibliográfica N° [13].

• **MEDIDAS DE SEGURIDAD DEL NIVEL BASICO:**⁵⁴

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"

⁵⁴ Véase referencia bibliográfica N° [13].

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 - Véase referencia bibliográfica N° [13].

• MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:⁵⁵

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 N° 25.326, deban guardar secreto de la información personal por expresa disposición legal (como el secreto bancario):

Tabla N° 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”.

⁵⁵ Véase referencia bibliográfica N° [13].

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 - Véase referencia bibliográfica N° [13].

• MEDIDAS DE SEGURIDAD DEL NIVEL CRÍTICO:⁵⁶

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 N° 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

⁵⁶ Véase referencia bibliográfica N° [27].

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 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 - Véase referencia bibliográfica N° [13].

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.

5.5. Conclusiones particulares del Capítulo V.

En los sistemas de registros contables existen numerosas bases de datos en donde se almacenan documentos comerciales, de uso interno, legajos, entre otros; la ley 25.326 establece que las destinadas a proporcionar informes deben inscribirse en el Registro que al efecto habilite el organismo de control. La información contenida en los sistemas contables no es exclusivamente para uso interno, ya que las empresas utilizan estos datos para realizar diversos reportes como: Estados Contables, informes de Responsabilidad Social Empresaria, de marketing, etc., que son distribuidas a usuarios, sucursales o al holding al cual pertenecen y a organismos

externos a las mismas.

La ley plantea que todas las bases de datos están sujetas al reglamento de esta ley, pero la DNPDP aconseja registrar las bases de datos que tengan un impacto significativo en la sociedad.

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

- Capítulo VI

6. PAUTAS MÍNIMAS DE AUDITORÍA INTERNA DE SEGURIDAD DE LA INFORMACIÓN EN SISTEMAS CONTABLES.

6.1. Introducción.

Desarrollados todos los puntos propuestos en el plan de trabajo, en el presente capítulo se propone un esbozo de pautas mínimas de auditoría interna para el cumplimiento de las normas vigentes en la Ciudad Autónoma de Buenos Aires relacionada con la Seguridad de la Información.

El objetivo del mismo no es abarcar un análisis exhaustivo, sino contemplar las cuestiones más relevantes y pasibles de sanciones a los entes relacionados con el sistema contable y enunciar aquellas normas de adhesión voluntaria que contribuyen al cumplimiento de las mismas.

6.2. Pautas mínimas de auditoría interna para el cumplimiento de las normativas vigentes para entes organizados como Sociedades Comerciales en la Ciudad Autónoma de Buenos Aires.

En el siguiente cuadro se especifican las pautas mínimas de control para ser consideradas en el sistema contable:

Cuadro N° 11: Pautas mínimas de auditoría interna de la Seguridad de la Información de un Sistema Contable en soporte tecnológico.

Numeración	Descripción	Observaciones
A.	<i>Código Comercial</i>	
A.1.	Existe autorización de Inspección General de Justicia (IGJ).	
A.2.	Se encuentra en funcionamiento el sistema solicitado.	
A.3.	Se encuentra transcripto el sistema en funcionamiento en el libro correspondiente.	
B.	<i>Informes y exigencias de la Inspección General de Justicia</i>	
B.1.	Trámite de Autorización completo en la Inspección General de Justicia.	
B.1.1.	Se encuentra el primer testimonio de escritura pública o instrumento privado original con la intención y los motivos para llevar el Sistema de Registros Contables medios digitales.	
B.1.2.	Se encuentra documentado las características del sistema empleado (Incluyendo las particulares del proceso y de la Seguridad de los mismos.)	
B.1.3.	Se encuentra el dictamen de precalificación de un Contador Público.	
B.2.	Presentación de los Informes Periódicos ante la IGJ.	
B.2.1.	Existe informe anual / certificación, con la descripción exacta del sistema utilizado durante el ejercicio económico.	
B.2.2.	Existe el informe de actualización técnica.	
B.3.	Condiciones para garantizar en los Sistemas de registración contable para ser considerados en legal forma.	
B.3.1.	Sistema de Numeración de los Medios de Almacenamiento.	
B.3.2.	Características del soporte de almacenamiento los registros contables.	
B.3.3.	Calidad del soporte de almacenamiento los registros contables.	
B.3.4.	Controles internos a implementar en la operatoria de almacenamiento.	
B.3.5.	Demostración técnica del grado de inalterabilidad.	
B.3.6.	Existencia de Actas de Registración.	

C.	Disposiciones de a la AFIP en el Resguardo la emisión y resguardo en soporte tecnológicos de comprobantes, manuales, no manuales y electrónicos.	
C.1.	Utilización de soportes para el almacenamiento de única grabación y múltiples lecturas.	
C.2.	Implementación de Políticas de Backup. (El sujeto adherido al régimen deberá resguardar dos (2) copias de los archivos en soportes independientes y en lugares que aseguren su integridad y protección física.)	
C.3.	Se cumple con el plazo de 15 días para el resguardo de las copias.	
C.4.	La utilización de un Código de Seguridad sobre los duplicados electrónicos	
C.5.	Procedimientos en la modificación de la Información Almacenada.	
D.	Disposiciones de la Dirección Nacional de Protección de Datos Personales, dependiendo de la envergadura de la organización los sistemas de registros contables deberían cumplir con el siguiente:	
D.1.	Se encuentran registradas las Bases de las Bases de Datos en el registro de la Dirección Nacional de Protección de Datos Personales.	
D.2.	Medidas de Seguridad de Nivel Básico	
D.2.1.	Se encuentran documentadas las funciones y obligaciones del personal.	
D.2.2.	Se encuentra documentada la descripción de los archivos con datos de carácter personal y los sistemas de información que los tratan.	
D.2.3.	Se encuentran documentadas 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.	
D.2.4.	Se encuentra establecido un Registro de incidentes de seguridad. (Notificación, gestión y respuesta ante los incidentes de seguridad.)	
D.2.5.	Se establecieron los procedimientos para efectuar las copias de respaldo y de recuperación de datos.	
D.2.6.	Se encuentran los procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información.	
D.2.7.	Existe un procedimiento para el control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados	
D.2.8.	Se encuentran establecidas las medidas de prevención a efectos de impedir amenazas de software malicioso.	

D.2.9.	Se encuentran establecidos los procedimientos para garantizar una adecuada Gestión de los Soportes tecnológicos.	
D.3.	MEDIDAS DE SEGURIDAD DE NIVEL MEDIO.	
D.3.1.	Se encuentra identificado al responsable (u órgano específico) de Seguridad.	
D. 3.2.	Se realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales.	
D.3.3.	Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.	
D.3.4.	Existe un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal.	
D.3.5.	Existe un sistema de gestión del soporte e información contenida en ellos.	
D.4.	MEDIDAS DE SEGURIDAD DE NIVEL CRÍTICO	
D.4.1.	Si se distribuyen soportes que contengan archivos con datos de carácter personal; Se implementan medidas para cifrar los datos durante su transporte.	
D.4.2.	Existe un registro de accesos a las bases de datos con información crítica.	
D.4.3.	Se dispone de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo los equipos de procesamiento habituales.	
D.4.4.	Si los datos de carácter personal que se transmiten a través de redes de comunicación, se deberán establecer mecanismos de cifrado o cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas.	
D.5.	Medidas de Seguridad en el Tratamiento y conservación de los datos personales contenidos en los Archivos y registros contables, (Disposición 9 DNPDP de 2008).	

D.5.1	<p>El documento de Seguridad de Datos Personales debe incluir:</p> <ul style="list-style-type: none"> - Funciones y obligaciones del personal o contratados. - Descripción de los archivos con datos personales y los sistemas que los tratan. - Descripción de las rutinas de control de datos y acciones a seguir ante errores. - Registros de incidentes de seguridad. - Procedimiento para efectuar las copias de respaldo y recuperación de datos. - Procedimientos de identificación y autenticación de los Usuarios de datos. - Control de acceso de Usuarios de datos. - Medidas de prevención frente a amenazas de software malicioso. - Procedimiento que garantice la adecuada Gestión de los Soportes de datos. 	
-------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

6.3. Normativas de cumplimiento optativo que contribuyen al cumplimiento de normas legales vigentes.

Para el cumplimiento de todas las normas analizadas se establece la necesidad de adoptar procedimientos para la administrar eficientemente la Seguridad de la Información en las organizaciones.

En la práctica profesional existen numerosas normativas, guías de buenas prácticas y estándares a seguir relacionadas con la seguridad y el control interno. Entre las más difundidas se destacan: El Informe COSO, el Marco Normativo de la serie ISO/IEC 27000, los requerimientos dispuestos en la ley estadounidense Sarbanes Oxley y el Marco COBIT.

Como se analizó en los capítulos anteriores, las normas establecidas por la IGJ, la AFIP, la DNPDP, entre otras, impactan en el funcionamiento del sistema de información contable y en el cumplimiento de la legislación vigente. Para ello es recomendable la implementación de Sistemas de Gestión de Seguridad de la Información para contribuir a una eficiente administración de seguridad en las organizaciones.

Imagen N° 3: El sistema de Información Contable y las Normas de Seguridad de la Información.



Fuente: Elaboración propia.

En la imagen N°3 se puede observar el conjunto de normas relacionadas con la seguridad de la información que impactan en el funcionamiento del sistema de información contable, requiriendo un abordaje interdisciplinario de la seguridad desde un análisis crítico de las herramientas de seguridad implementadas hasta una revisión de las necesidades del negocio en cada organización.

- Capítulo VII

7. CONCLUSIONES FINALES DEL TRABAJO

Como se indicó en la introducción, en el desarrollo del presente trabajo final de especialización el autor ha intentado establecer todos los aspectos en donde la Seguridad de la Información impacta e influye en los sistemas de registros contables.

A continuación se plasman las reflexiones más relevantes analizadas desde la perspectiva de contabilidad, desde su definición de disciplina hasta la teneduría de libros, teniendo presente los diversos plexos normativos vigentes en el ámbito de la Ciudad Autónoma de Buenos Aires.

✓ La Seguridad de la Información y la Teoría General Contable.

La Contabilidad como disciplina recibe influencias de numerosas ciencias y técnicas que le aportan diversas cuestiones para cumplir con sus fines específicos. Teniendo en cuenta los requisitos básicos de la seguridad de la información: integridad, confidencialidad y disponibilidad, se puede trazar una estrecha vinculación con lo establecido en el Marco Conceptual de Información Contable de la RT N°16 del CPCECABA⁵⁷, ya que aporta considerablemente una mejora en los atributos de la información destinada a los usuarios de los Estados Contables.

Bajo el reconocimiento de este contexto el autor considera que la Seguridad de la Información debe contemplarse como una de las disciplinas influyente en la Teoría General de la Contabilidad, al contribuir con el

⁵⁷ CPCECABA: Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.

cumplimiento de los requisitos planteados para la información contable.

✓ **Garantías planteadas a nivel doctrinario para los Sistemas de Información Contable en soporte tecnológico.**

La ley de Sociedades Comerciales en el artículo 61 establece la autorización a las empresas a llevar el Sistema de Registros Contables en medios tecnológicos. Pero para ello se debe cumplir mínimamente con los siguientes requisitos:

- a. Obtener la aprobación de la Autoridad de Control.⁵⁸
- b. Puesta en funcionamiento y utilización efectiva del sistema oportunamente solicitado.
- c. Trascrición del sistema en el libro de inventarios y balances.
- d. Implementar las medidas necesarias para garantizar la inalterabilidad y verificabilidad de las registraciones contables.

La Doctrina del Derecho Contable plantea que además de cumplir con estos requisitos en los sistemas contables se deben garantizar la inalterabilidad y verificabilidad de sus registros para que sean considerados legítimos.

Para cumplir con estas garantías se vuelve indispensable la utilización de herramientas y la gestión de la Seguridad de la Información en las organizaciones.

El presente tema no es tenido en cuenta por gran cantidad de empresas en la Republica Argentina que luego en diferentes inspecciones o en conflictos judiciales sufren las consecuencias de no contar con sistema de información contable legalmente constituido.

⁵⁸ En la Ciudad Autónoma de Buenos Aires corresponde a la Inspección General de Justicia.

✓ **Normas de las Seguridad de la Información contempladas en diferentes organismos de contralor en la Ciudad Autónoma de Buenos Aires.**

La Inspección General de Justicia mediante la Resolución General 7 de 2005 dispone los trámites necesarios para autorizar e implementar sistemas contables en soporte magnético. Para obtener la citada autorización resulta necesario el cumplimiento de numerosas medidas relacionadas con la seguridad de la información.

La IGJ requiere además de una exposición amplia y precisa del sistema de registración a utilizar, una “demostración técnica del grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto”, en donde resulta necesaria la intervención de un especialista en seguridad para expedirse sobre los siguientes puntos de control dispuestos en la norma: Plataforma de hardware y software utilizadas, las políticas de gestión de Seguridad de la Información, control de accesos y backup de documentación respaldatoria, plan de contingencia y pautas de confiabilidad e integridad de los registros contables.

Por otra parte la Administración Federal de Ingresos Públicos establece un procedimiento general de emisión, conversión y conservación de la documentación respaldatoria en formato electrónico o resguardo de la copia del formato físico de los Registros Contables.

Analizadas las resoluciones, se puede establecer que la AFIP exige que la documentación respaldatoria sea resguardada en soportes de única grabación y múltiples lecturas, establecer una política de Backup asegurando su integridad y protección física, utilizar un Código de Seguridad sobre los duplicados electrónicos y características en el caso que se modificara Información almacenada.

A partir de la vigencia de la Ley de Protección de datos personales, las entidades que posean bases de datos utilizadas para generar informes deben registrar dichas bases y cumplir con las disposiciones emitidas por el organismo de control.

En los sistemas de registros contables existen numerosas bases de datos en donde se almacenan documentos comerciales, documentos

internos y legajos, entre otros, que deben ser registrados ya que las empresas utilizan estos datos para realizar diversos informes como los Estados Contables y las Declaraciones Juradas.

En las disposiciones de la Dirección Nacional de Protección de Datos Personales se establece que las empresas deben adoptar las medidas técnicas y organizativas que resulten necesarias para garantizar la seguridad de la información tratada.

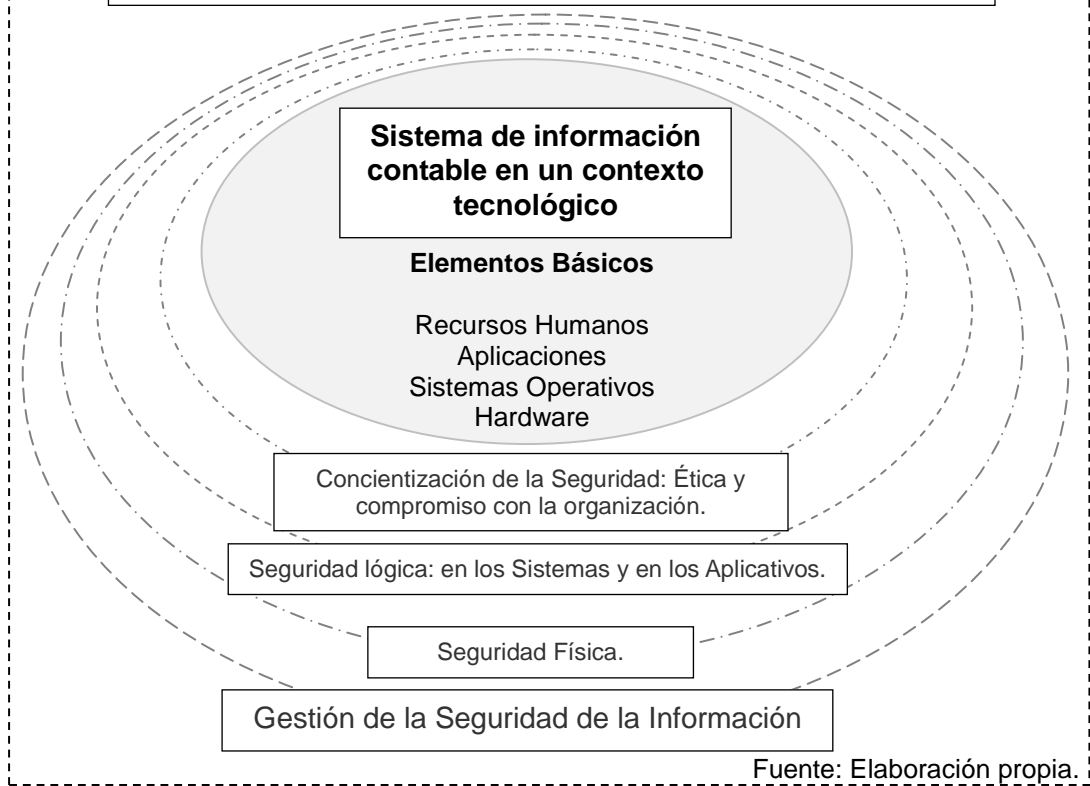
Las disposiciones mas relevantes a considerar en la administración de la seguridad en los sistemas contables son la N° 11 de 2006, en donde se establecen medidas de seguridad de nivel básico, medio y crítico, y la disposición N° 9 de 2008 en donde se establecen las medidas de seguridad en el tratamiento y conservación de los datos personales contenidos en las bases de datos.

✓ **Conclusiones Finales**

Al identificar los elementos básicos que componen un sistema contable se destacan: los Recursos Humanos, Medios de Registración, Cuentas a emplear, Aplicativos y Algoritmos para el registro de las operaciones, Modelos de Informes a preparar, Sistemas Aplicativos (Software de Base y Aplicativos) y Hardware. En este punto la gestión de la seguridad influye en cada uno de los elementos identificados, desde la seguridad lógica de los aplicativos y sistemas operativos, la seguridad física y hasta en la concientización del personal.

En la siguiente imagen se puede apreciar diferentes dominios de la Seguridad de la Información y el sistema de información contable.

Imagen N°2: Elementos de sistema de Información Contable y la Seguridad de la Información.



De esta manera, la Seguridad de la Información se convierte en el principal sostén de los requisitos a satisfacer por los Sistemas de Información Contable y no puede concebirse en el Siglo XXI que una organización prescindiera de los beneficios que esta brinda.

- Anexo A: Características de los Sistemas de Registros Contables.

A. SISTEMAS DE REGISTRACIÓN CONTABLE.

A.1. La contabilidad como un sistema.

La contabilidad en una organización es considerada un sistema de información; por lo tanto está constituida por un conjunto de elementos interrelacionados. Russell Ackoff define a un sistema como "un conjunto de elementos interrelacionados, de cualquier clase; por ejemplo, conceptos, objetos, o personas." El conjunto de elementos tiene las tres propiedades siguientes:

1. Las propiedades o comportamiento de cada parte del conjunto tienen un efecto sobre las propiedades o el comportamiento del conjunto como un todo.
2. Las propiedades y comportamiento de cada parte y el modo en que afectan el todo dependen de aquellos correspondientes, al menos, a alguna parte del conjunto. Por lo tanto, ninguna parte tiene un efecto independiente sobre el otro.
3. Todo posible subgrupo de elementos del conjunto tiene las dos primeras propiedades. Cada uno tiene un efecto y ninguno puede tener un efecto independiente sobre el todo. Por lo tanto los elementos no pueden ser organizados en subgrupos independientes."⁵⁹

Al definir a la contabilidad como un sistema, se pueden identificar todos los elementos operativos existentes en ella, ya que para cumplir con

⁵⁹ Véase referencia bibliográfica N° [1].

los requisitos de la Información Contable⁶⁰ es necesaria su adecuada clasificación y organización.

La principal función del Sistema de Información Contable es tomar primordialmente información de una empresa referidos a los elementos identificados como parte de ese Sistema Contable, analizarla, procesarla y resumirla de tal forma que cumpla con los criterios básicos establecidos por el ente emisor o por otros organismos que ejercen control, para presentar diferentes tipos de Informes a usuarios dependiendo del ente.

A.2. Elementos del sistema contable.

A continuación se enumeran los elementos principales que forman partes de un sistema contable y la composición de los mismos varía en relación con la envergadura del ente.

Tabla N° 7: Elementos del Sistema Contable.
- Recursos Humanos
- Medios de Registros
- Cuentas a emplear
- Comprobantes
- Algoritmos para el registro de las operaciones
- Mecanismos de Control
- Modelos de informes a preparar.
Fuente: Elaboración propia.

- Tipos de comprobantes

Existen numerosos documentos utilizados en el Sistema de Información Contable; los mismos pueden ser clasificados genéricamente como de uso interno o de uso externo.

En los de uso interno se incluyen a todos aquellos necesarios para la organización de la actividad que realice el ente y a los papeles de trabajo contables; y los de uso externo tienen vinculación con el entorno de la

⁶⁰ En el punto, 1.3.1. se enuncian los requisitos de la información contable, emitidos por la RT 16 de la FACPCE.

organización, al cual están destinadas, que pueden o no tener un una regulación fiscal o especial. En el siguiente cuadro se expone la clasificación de comprobantes.

Cuadro N° 12: Comprobantes internos y externos.		
Comprobantes de Circulación Externa	Con regulación fiscal o especial	Facturas
		Tiques
		Remitos
		Notas de Débito
		Notas de Crédito
		Recibos
		Formularios de impuestos, tasas y contribuciones.
		Declaraciones Juradas
		Formularios de Pago de Contribuciones Sociales (Aportes y retenciones)
		Recibos de Sueldos y Jornales
	Otros	Pagarés
		Cheques
		Letras de Cambio
		Certificados de depósitos
		Prendas
		Hipotecas
		Órdenes de Compra
Notas de pedido o venta		
Comprobantes de Circulación Interna	Organización de la actividad	Órdenes de Pago
		Órdenes de fabricación
		Requisiciones de almacenes y depósitos
		Vales de Tesorería
		Vales de Materiales
		Parte de Stock
		Movimiento de Caja
		Rendición de fondo fijo
		Solicitud y legajos de créditos
		Asientos diarios
	Otros	Papeles vinculados a registros Contables
		Legajos del personal
Fuente: Elaboración Propia.		

La identificación de los diferentes comprobantes utilizados en los sistemas contables resulta relevante en la organización del sistema contable, ya que los mismos contienen información sensible personal y los clientes de la empresa. Esto resulta fuertemente vinculado con la descripción de las bases de datos contempladas en la Ley de Protección de Datos Personales analizada en el capítulo 5 del presente trabajo.

A.3. Teneduría de libros y utilización de software.

La “teneduría de libros”⁶¹ puede ser realizada mediante registros manuales o utilizarse programas específicos. En los entes en donde se desarrolla un sistema de registros manuales, una vez definidos los hechos y transacciones a ser registrados contablemente y las cuentas a utilizar, corresponde su transcripción en “los registros contables cronológicos (diarios) y temáticos (mayores).”⁶²

Cuando no se utiliza un “Programa de Teneduría de Libros la obtención y procesamiento de la información es trabajosa”⁶³. La utilización de este tipo de software, permite que cada uno de los importes cargados en cada asiento se asigne, tanto a una cuenta, como a uno o más atributos, permitiendo la preparación de informes contables por atributos, basándose en los importes asignados y en las cuentas imputadas.

La mayoría de los negocios que recurren a la utilización de los designados genéricamente como “programas de teneduría de libros” pueden optar por sistemas aplicativos estándar, o desarrollados exclusivamente para las necesidades de la entidad. Cuando los entes utilizan mecanismos manuales para contabilizar sus operaciones, incrementan considerablemente los riesgos de cometer errores en la registración de transacciones, disminuyendo significativamente la calidad de la información.

⁶¹ La Teneduría de Libros, en este sentido se refiere a la “llevar lo libros contables”.

⁶² Véase referencia bibliográfica N° [19].

⁶³ Denominación propuesta por Enrique Fowler Newton, “Planes de Cuentas y Manuales de Procedimientos Contables” Capítulo 1, Véase referencia bibliográfica N° [18].

- Bibliografía específica.

[1] ACKOFF RUSSELL L., La ciencia de la edad en los Sistemas: Mas allá de la ingeniería industrial, la investigación operativa y la ciencia de la administración, Operations Research, Mayo-junio de 1973, Citado por: LOPEZ SANTISO, Horacio, Un nuevo enfoque sobre la auditoría y sus normas, Federación Argentina de Consejos Profesionales en Ciencias Económicas, La Plata, 1976, 8 p.

[2] AFIP (Argentina). Resolución General 1361 (AFIP), Facturación y Registración – Procedimiento y emisión de comprobantes, Artículo 62. Accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[3] AFIP (Argentina). Resolución General 1361 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información, Artículo 42. Infoleg accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[4] AFIP (Argentina). Resolución General 1361 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información, Artículo 18. Infoleg accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[5] AFIP (Argentina). Resolución General 1361 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información, Artículo 19. Infoleg accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[6] AFIP (Argentina). Resolución General 1361 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información, Artículo 42. Infoleg accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[7] AFIP (Argentina). Resolución General 1415 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información, Artículo 22. Accedido desde www.infoleg.gov.ar el 28 de Marzo de 2011.

[8] AFIP (Argentina). Resolución General 1415 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información, Artículo 40. Infoleg accedido desde www.infoleg.gov.ar el 28 de Marzo de 2011.

[9] AFIP (Argentina). Resolución General 2485 (AFIP). Accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[10] AFIP (Argentina). Resolución General 2485, Emisión y almacenamiento electrónico de comprobantes originales, Artículo 23. Accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[11] AFIP (Argentina). Resolución General 2485, Emisión y almacenamiento electrónico de comprobantes originales, Artículo 27 y 28. Accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

[12] American Accounting Association, "A Statement of Basic Accounting Theory", AAA. 1966.

[13] Dirección Nacional de Protección de Datos Personales. Disposición 11/2006, Medidas de Seguridad. Buenos Aires, Argentina. 2003, accedido desde <http://www.jus.gov.ar/datos-personales.aspx>

[14] Dubois E. M. F., La Contabilidad Informática ¿Brinda Seguridad Jurídica en su actual implementación?, Revista Errepar [en línea]. Julio de 2001. [consultada el 20 de Agosto de 2011]. Disponible en: http://www.legalmania.com.ar/derecho/contabilidad_informatica.htm

[15] Enrique Fowler Newton, "Planes de Cuentas y Manuales de Procedimientos Contables, Capítulo 1, Editorial La Ley, 2009, Buenos Aires, p 9.

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

[17] Federación Argentina de Consejos Profesionales en Ciencias Económicas, Marco Conceptual - RT 16. República Argentina, 2011.

[18] Fowler Newton E., Planes de Cuentas y Manuales de Procedimientos Contables, Capítulo 1, Editorial La Ley, 2009, Buenos Aires, p 5.

[19] Fowler Newton, Enrique, "Organización de Sistemas Contables", Capítulo 2 Los sistemas contables, Ediciones Contabilidad Moderna SAIC Buenos Aires 1982, 10 p.

[20] García Casella C. L. y Rodríguez de Ramírez M. C., "Elementos para una Teoría General de la Contabilidad", Capítulo 1, Buenos Aires, 2001, p.107-109.

[21] García Casella, C. L., "Método Científico para las Investigaciones en General", Informe presentado en el I Encuentro Universitario de Investigaciones del Área Contable, 1995.

[22] Gómez López J., Guía de campo de hackers, Capítulo I., Alfaomega Grupo Editor, México, 2010, 17 p.

[23] Gustavo A., Exposición en la Asignatura: Gestión Estratégica de la Seguridad Informática II. Maestría en Seguridad Informática. Junio 2011.

[24] Inspección General de Justicia. Ministerio de Justicia y Derechos Humanos. 09 de Octubre de 2011. Disponible en <http://www.jus.gov.ar/IGJ/guia.php>

[25] Inspección General de Justicia. Resolución General 7 de 2005. Artículo 286 - Inciso 1. Boletín Oficial de la República Argentina, 23 de Agosto de 2005.

[26] Inspección General de Justicia. Resolución General 7 de 2005. Artículo 286 - Inciso 2. Boletín Oficial de la República Argentina, 23 de Agosto de 2005.

[27] Inspección General de Justicia. Resolución General 7 de 2005. Artículo 286 - Inciso 3. Boletín Oficial de la República Argentina, 23 de Agosto de 2005.

[28] Inspección General de Justicia. Resolución General 7 de 2005. Artículo 286 - Inciso 5. Boletín Oficial de la República Argentina, 23 de Agosto de 2005.

[29] Inspección General de Justicia. Resolución General 7 de 2005. Artículo 282. Boletín Oficial de la República Argentina, 23 de Agosto de 2005.

[30] Inspección General de Justicia. Resolución General 7 de 2005. Artículo 286 - Inciso 6 y 7. Boletín Oficial de la República Argentina, 23 de Agosto de 2005.

[31] Instituto Argentino de Derecho Contable (IADECO), Derecho Contable [en línea]. Diciembre de 2011. [consultada el 01 de Julio de 2012]. Disponible en: "<http://www.iadeco.org/dercont.htm>"

[32] Ley 19950, Ley de Sociedades Comerciales, Artículo 61, Boletín Oficial de la República Argentina, 30 de Marzo de 1984, Buenos Aires.

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

[34] Ley 2637, Código de Comercio de la República Argentina, Artículo 44, Boletín Oficial de la República Argentina, Buenos Aires. Publicado en R.N. Tomo II, 05 de Octubre de 1889.

[35] Ley 2637, Código de Comercio de la República Argentina, Boletín Oficial de la República Argentina, Buenos Aires, Publicado en R.N. Tomo II, 05 de Octubre de 1889.

[36] Molina, J. C., Los subdiarios y la obligatoriedad de su rubricación, Impuestos, LVII-1999-A, Ed. La Ley, p. 1550.

[37] Pastor J. S., Bessana G. A. e Iglesias S. G., Procedimiento General para la Emisión, Conversión y Conservación de la documentación respaldatoria en los sistemas de registros contables. Aspectos legales y técnicos. En: 18° Congreso Nacional de Profesionales en Ciencias Económicas: (18, 2010, CABA), Área V. Administración y Sistemas. Buenos Aires, Argentina. Junio de 2010. 281 p.

[38] Popritkin A. R., Fraudes y Libros Contables, La Ley, Buenos Aires, 2001

p 274.

[39] Popritkin A. R., Fraudes y Libros Contables, La Ley, Buenos Aires, 2001 p 35.

[40] Popritkin A. R., Fraudes y Libros Contables, La Ley, Buenos Aires, 2001 p 36.

[41] Real Academia Española, Seguro/ra [en línea]. Diciembre de 2011. [consultada el 01 de Julio de 2012]. Disponible en: <http://lema.rae.es/drae/?val=Seguro>

[42] Sosa, T. E., Medios informáticos y el proceso que viene. Validez probatoria y eficiencia procesal. La Ley, Buenos Aires. 9/7/99, P. 649

[43] 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.

[44] Universidad Notarial Argentina, Instituto de Derecho Comercial, Condiciones de la legalidad de la contabilidad informática, Conclusiones, 8/6/2000.

- Bibliografía General.

ACKOFF RUSSELL L., La ciencia de la edad en los Sistemas: Mas allá de la ingeniería industrial, la investigación operativa y la ciencia de la administración, Operations Research, Mayo-junio de 1973, Citado por: LOPEZ SANTISO, Horacio, Un nuevo enfoque sobre la auditoría y sus normas, Federación Argentina de Consejos Profesionales en Ciencias Económicas, La Plata, 1976.

AFIP (Argentina). Resolución General 1361 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información. Infoleg accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

AFIP (Argentina). Resolución General 1415 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información. Accedido desde www.infoleg.gov.ar el 28 de Marzo de 2011.

AFIP (Argentina). Resolución General 2485 (AFIP). Accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

AFIP (Argentina). Resolución General 2485, Emisión y almacenamiento electrónico de comprobantes originales. Accedido desde www.infoleg.gov.ar el 24 de Marzo de 2011.

American Accounting Association, "A Statement of Basic Accounting Theory", AAA. 1966.

Dirección Nacional de Protección de Datos Personales. Disposición 11/2006, Medidas de Seguridad de Nivel Básico. Buenos Aires, Argentina. 2003, accedido desde <http://www.jus.gob.ar/datos-personales.aspx>

Dubois E. M. F., La Contabilidad Informática ¿Brinda Seguridad Jurídica en su actual implementación?, Revista Errepar [en línea]. Julio de 2001. [consultada el 20 de Agosto de 2011]. Disponible en: http://www.legalmania.com.ar/derecho/contabilidad_informatica.htm

Enrique Fowler Newton, "Planes de Cuentas y Manuales de Procedimientos Contables, Capítulo 1, Editorial La Ley, Buenos Aires, 2009.

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

Federación Argentina de Consejos Profesionales en Ciencias Económicas, Marco Conceptual - RT 16. República Argentina, 2011.

Fowler Newton E., Planes de Cuentas y Manuales de Procedimientos Contables, Capítulo 1, Editorial La Ley, 2009, Buenos Aires.

Fowler Newton, Enrique, "Organización de Sistemas Contables", Capítulo 2 Los sistemas contables, Ediciones Contabilidad Moderna SAIC Buenos Aires 1982.

García Casella C. L. y Rodríguez de Ramírez M. C., "Elementos para una Teoría General de la Contabilidad", Capítulo 1, Buenos Aires, 2001.

García Casella, C. L., "Método Científico para las Investigaciones en General", Informe presentado en el I Encuentro Universitario de Investigaciones del Área Contable, 1995.

Gómez López J., Guía de campo de hackers, Capítulo I., Alfaomega Grupo Editor, México, 2010.

Gustavo A., Exposición en la Asignatura: Gestión Estratégica de la Seguridad Informática II. Maestría en Seguridad Informática. Junio 2011.

Inspección General de Justicia. Ministerio de Justicia y Derechos Humanos. 09 de Octubre de 2011. Disponible en <http://www.jus.gov.ar/IGJ/guia.php>

Inspección General de Justicia. Resolución General 7 de 2005. Boletín Oficial de la República Argentina, 23 de Agosto de 2005.

Ley 19950, Ley de Sociedades Comerciales, Boletín Oficial de la República Argentina Buenos Aires, 30 de Marzo de 1984.

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

Ley 2637, Código de Comercio de la República Argentina, Boletín Oficial de la República Argentina, Buenos Aires. Publicado en R.N. Tomo II, 05 de Octubre de 1889.

Molina, J. C., Los subdiarios y la obligatoriedad de su rubricación, Impuestos, LVII-1999-A, Ed. La Ley, p. 1550.

Pastor J. S., Bessana G. A. e Iglesias S. G., Procedimiento General para la Emisión, Conversión y Conservación de la documentación respaldatoria en los sistemas de registros contables. Aspectos legales y técnicos. En: 18° Congreso Nacional de Profesionales en Ciencias Económicas: (18, 2010, CABA), Área V. Administración y Sistemas. Buenos Aires, Argentina. Junio de 2010.

Popritkin A. R., Fraudes y Libros Contables, La Ley, Buenos Aires, 2001.

Sosa, T. E., Medios informáticos y el proceso que viene. Validez probatoria y

eficiencia procesal. La Ley, Buenos Aires. 1999.

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.

Universidad Notarial Argentina, Instituto de Derecho Comercial, Condiciones de la legalidad de la contabilidad informática, Conclusiones, 2000.

- Índices específicos

Índice de Tablas

Tablas	Páginas
TABLA N° 1: REQUISITOS DE LA INFORMACIÓN CONTENIDA EN LOS ESTADOS CONTABLES.	5
TABLA N° 2: RIESGOS IDENTIFICADOS POR LA DOCTRINA DEL DERECHO CONTABLE (EDUARDO M. FAVIER DUBOIS).	13
TABLA N° 3: REQUISITOS DE LOS SISTEMAS CONTABLES (IGJ).	16
TABLA N° 4: MEDIDAS DE SEGURIDAD DEL NIVEL BÁSICO.	40
TABLA N° 5: MEDIDAS DE SEGURIDAD DEL NIVEL MEDIO.	41
TABLA N° 6: MEDIDAS DE SEGURIDAD DE NIVEL CRÍTICO.	42
TABLA N° 7: ELEMENTOS DEL SISTEMA CONTABLE.	57

Índice de Esquemas

Esquemas	Páginas
ESQUEMA N° 1: APORTES DE LA SEGURIDAD DE LA INFORMACIÓN A LA CONTABILIDAD.	6
ESQUEMA N° 2: MARCO NORMATIVO DE LOS REGISTROS CONTABLES EN SOCIEDADES COMERCIALES EN LA CABA.	11
ESQUEMA N° 3: MARCO LEGAL DE LA DOMUMENTACIÓN.	24
ESQUEMA N° 4: EMISIÓN NO ELECTRÓNICA DE COMPROBANTES.	25

ESQUEMA N° 5: REGIMEN ESPECIAL PARA LA EMISION Y ALMACENAMIENTO ELECTRONICO DE COMPROBANTES ORIGINALES.	27
ESQUEMA N° 6: "RÉGIMEN DE EMISIÓN DE COMPROBANTES ELECTRÓNICOS EN LÍNEA", "R.C.E.L.".	28
ESQUEMA N° 7: TIPOS DE DATOS PERSONALES.	36
ESQUEMA N° 8: NIVELES DE SEGURIDAD.	39

Índice de Imágenes

Imágenes	Páginas
IMAGEN N° 1: DISCIPLINAS INFLUYENTES EN LA CONTABILIDAD.	8
IMAGEN N° 2: EL SISTEMA DE INFORMACIÓN CONTABLE Y LAS NORMAS DE SEGURIDAD DE LA INFORMACIÓN.	50
IMAGEN N° 3: ELEMENTOS DE SISTEMA DE INFORMACIÓN CONTABLE Y LA SEGURIDAD DE LA INFORMACIÓN.	55

Índice de Cuadros

Cuadros	Páginas
CUADRO N° 1: ELEMENTOS DEL SISTEMA CONTABLE Y LA SEGURIDAD DE LA INFORMACIÓN.	8
CUADRO N° 2: PUNTOS DE AUDITORÍA DE LA SEGURIDAD DE LA INFORMACIÓN.	19
CUADRO N° 3: AUTORIZACIÓN PARA EMPLEO DE ORDENADORES (IGJ).	20
CUADRO N° 4: INFORMES PERIÓDICOS MEDIOS MAGNÉTICOS U OTROS. (IGJ)	21
CUADRO N° 5: CLASIFICACIÓN DE LAS FORMAS DE REGISTRACIÓN	29
CUADRO N° 6: ESPECIFICACIONES SOBRE LOS SOPORTES DE UNICA GRABACION Y MULTIPLES LECTURAS (WORM).	30

CUADRO N° 7: COMPROBANTES Y DOCUMENTACIÓN DE COMERCIO.	37
CUADRO N° 8: COMPROBANTES INTERNOS.	37
CUADRO N° 9: RELACIONADOS CON LOS EMPLEADOS.	38
CUADRO N° 10: RELACIONADOS CON OTRAS PERSONAS FÍSICAS Y JURÍDICAS.	38
CUADRO N° 11: PAUTAS MÍNIMAS DE AUDITORÍA INTERNA DE LA SEGURIDAD DE LA INFORMACIÓN DE UN SISTEMA CONTABLE EN SOPORTE TECNOLÓGICO.	46
CUADRO N° 12: COMPROBANTES INTERNOS Y EXTERNOS.	58