Universidad de Buenos Aires

Facultad de Ciencias Económicas,
Ciencias Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis de Maestría

Formación del Contador Público en Tecnología y Seguridad de la Información. Propuesta de reforma curricular.

Autor: Diego Sebastián Escobar

Directora: Elsa Beatriz Suarez Kimura

Co-directora: Romina de Franceschi

Febrero de 2017

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.

"FIRMADO"
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 se ha incrementado vertiginosamente en los últimos años, convirtiéndose en un elemento indispensable en gran parte de las organizaciones para el desarrollo de sus actividades.

Lo que correspondía hace varios años a procesos y procedimientos en formato manual, pasaron a medios digitales, dependiendo progresivamente de la tecnología. En este contexto, y como una cuestión ineludible por obligaciones legales, está presente el sistema de información contable, en donde los organismos de control establecieron los requisitos en tecnología y seguridad de la información que deberían cumplirse para que sean considerados legalmente constituidos.

Con este entorno, pocos o escasos programas de estudios en Ciencias Económicas se actualizan con la celeridad en que ocurren los acontecimientos en el ámbito profesional, generando una brecha de nuevos contenidos que deben ser incorporados a los que el Contador Público egresado adquirió para satisfacer las necesidades profesionales.

La presente Tesis de Maestría tiene el objetivo de analizar los aspectos legales, normativos y tecnológicos de la Seguridad Informática en el almacenamiento, procesamiento, control y resguardo de los Registros Contables; plantear un diagnóstico y desarrollar una propuesta de reforma curricular del Contador con la inclusión de estos temas para una formación académica y profesional adecuada a los requerimientos actuales y a los desafíos futuros.

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

- Índice de Contenidos

- Declaración Jurada de Contenidos i

- Resumen ii

- Índice de Contenidos iii

- Prólogo viii

- Nómina de abreviaturas ix

Cuerpo Introductorio 1

- INTRODUCCIÓN 2
A - Presentación del problema 4
A.1. Antecedentes del tema 5
A.1.1. Antecedentes en el ámbito internacional 5
A.1.2. Antecedentes en el ámbito nacional 6
A.2. Planteo del problema 7
A.3. Objetivos 7
A.4. Alcance 8
A.5. Hipótesis 9
A.6. Estructura 9

Cuerpo Principal 11

- CAPÍTULO I - LAS INCUMBENCIAS PROFESIONALES DEL CONTADOR PÚBLICO EN LA REPÚBLICA ARGENTINA Y LA GESTIÓN DE LOS SISTEMAS DE INFORMACIÓN 12
1. 1. Introducción 12
1.2. La Ley número 20.488 de incumbencias profesionales y la administración de la Tecnología y Seguridad de la Información. 13
1.3. Conceptos impartidos en la asignatura “Tecnología de la Información” 15
1.4. Síntesis del capítulo I 16

CAPÍTULO II - MARCO LEGAL DE LOS REGISTROS CONTABLES EN LA REPÚBLICA ARGENTINA 17
2.1. Introducción 17
2.2. Obligación de llevar Registros Contables 17
2.3. Los registros contables en formatos tecnológicos: Las características de la Ley General de Sociedades 19
2.4. Requisitos exigidos en los Sistemas de Registración Contable 20
2.5. Los riesgos identificados por el Derecho para llevar una contabilidad informatizada 21
2.6. La legalidad de un sistema de registros contables en contextos informáticos 22
2.7. Síntesis del capítulo II 23

CAPÍTULO III - NORMAS DEL ORGANISMO REGULADOR EN EL ÁMBITO DE LA CIUDAD AUTÓNOMA DE BUENOS AIRES 24
3.1. Introducción 24
3.2. Condiciones de los Sistemas de registración contable resguardados en compact disc, otros discos ópticos y microfilmes 25
3.3. Trámites y requisitos solicitados por la Inspección General de Justicia (Resolución General número 7 de 2015). 28
3.4. Síntesis del capítulo III 35

CAPÍTULO IV - IMPLICANCIAS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA DE INFORMACIÓN CONTABLE..... 37
4.1. Introducción 37
4.2. Reconocimiento de las Bases de Datos utilizadas y almacenadas en las Organizaciones. Conceptos y objetivos de la Ley número 25.326 37
4.3. Clasificación de Datos Personales..... 38
4.4. Seguridad de los Datos..... 41
4.5. Síntesis del capítulo IV 46

CAPÍTULO V - LA CONTABILIDAD Y SU VINCULACIÓN CON LA TECNOLOGÍA Y SEGURIDAD DE LA INFORMÁTICA 47
5.1. Introducción 47
5.2. Concepto de Seguridad de la Información. 47
5.3. Concepto de Contabilidad..... 48
5.4. Requisitos de la Información contenida en los Estados Contables..... 49
5.5. Seguridad de la Información y su aporte a la Contabilidad 50
5.6. Síntesis del capítulo V 53

CAPÍTULO VI - GESTIÓN DE MEJORES PRÁCTICAS Y ESTÁNDARES DE CONTROL Y SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES. 54
6.1. Introducción 54
6.2. Interrelación de los elementos del sistema contable..... 54
6.3. Análisis de la calidad de los procesos administrativos 55
6.4. Análisis de la estructura del control interno organizacional..... 57
6.5. Para gestionar los procesos de TI 58
6.6. Para el análisis de las transacciones de la tarjeta de pago..... 58
6.7. Para gestionar la Seguridad de la Información de Sistemas Contables..... 59
6.8. Síntesis del capítulo VI 61

CAPÍTULO VII - IDENTIFICACIÓN DE LOS REQUERIMIENTOS ACTUALES DEL CONTADOR PÚBLICO..... 63

7.1. Introducción 63
7.2. Recomendaciones de instituciones mundiales 63
7.3. Recomendaciones en el ámbito profesional y académico profesional 64
7.4. Abordaje de contenidos 65
7.5. Propuestas a considerar discutidas en el ámbito universitario argentino 66

CAPÍTULO VIII - FORMACIÓN DEL CONTADOR PÚBLICO EN LA GESTIÓN Y CONTROL DE LOS SISTEMAS DE INFORMACIÓN. ESBOZO DE UNA PROPUESTA CURRICULAR SUPERADORA 67
8.1. Introducción 67
8.2. Fundamentación del cambio curricular 67
8.3. Objetivos de la reforma 68
8.4. Ejes principales de la propuesta. 69
8.5. Programa y competencias a adquirir por los educandos 72

Conclusiones Finales 73

CONCLUSIONES FINALES DEL TRABAJO 74

Anexos 83

- Anexo A: Características de la propuesta de programa 84
- Anexo B: Contenidos programáticos completos de la propuesta. 92
- Anexo C: Modelos de Gestión de la Seguridad de la Información y la Capacitación 103

Bibliografía 108

- Bibliografía específica 109
- Bibliografía general 113
- Índices específicos 117
Índice de Esquemas 117

Índice de Tablas 118
Índice de Gráficos 118
Índice de Cuadros 119

- Prólogo

La presente tesis de Maestría en Seguridad Informática es el resultado de numerosas horas de investigación, intentando reflejar en el mismo un pequeño aporte acotado para una reforma curricular de la carrera de grado de Contador en la República Argentina.

En primer lugar, el autor desea dedicar este logro a Elsa Beatriz Suarez Kimura por contagiar todo el entusiasmo ya que sin su ayuda esta obra no hubiera sido posible.

En segundo a su familia, Claudia Teresa Pszytula, Julieta Carolina Escobar, Jorge Horacio Escobar, Beatriz del Valle Salvador, Alérico Tomás Escobar, Alejandra Bak y Francisco Pszytula.

A quienes le han abierto puertas dando oportunidades en diferentes ámbitos: Luisa Fronti de García, Carlos Luis García Casella, Elizabeth Ierino, Silvia Iglesias, Graciela Braga y Ángel Romano Pozzi.

Y por último a esas personas que han tenido paciencia a lo largo de este tiempo: Ariel Cister, Laura Acevedo, Magalí Mendez, Ortiz Edgar Alejandro, Telma Roncagliolo, Mariana Mereles, Rodrigo Ezequiel Montero, Verónica Gabriela Cacciabue, Karina Zugaro, Valentín Alippi, Aldana Julieta Mucchielli y Marisa Andrea Valcárcel.

Diego Sebastián Escobar

- Nómina de abreviaturas

AIC: Asociación Interamericana de Contabilidad.

AFIP: Administración Federal de Ingresos Públicos.

ANPCyT: Agencia Nacional de Promoción Científica y Tecnológica.

CABA: Ciudad Autónoma de Buenos Aires.

COBIT: Objetivos de Control para Información y Tecnologías Relacionadas.

COSO: The Committee of Sponsoring Organizations of the Treadway Commission.

CODECE: Consejo de Decanos de Ciencias Económicas.

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

DNPDP: Dirección Nacional de Protección de Datos Personales.

FACPCE: Federación Argentina de Consejos Profesionales en Ciencias Económicas.

FONCyT: Fondo para la Investigación Científica y Tecnológica

IEC: International Electrotechnical Commission.

IFAC: International Federation of Accountants.

IGJ: Inspección General de Justicia.

IRAM: Instituto Argentino de Normalización y Certificación.

ISO: International Organization for Standardization.

PCI-DSS: Payment Card Industry Data Security Standard.

RT: Resolución Técnica aprobada por la FACPCE.

SGSI: Sistema de Gestión de Seguridad de la Información.

Cuerpo Introductorio

- Introducción

En las organizaciones existen múltiples sistemas de información cuya interrelación conforma información útil para la toma de decisiones en los diferentes niveles jerárquicos. 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 en todo tipo de entes.

La presente Tesis de Maestría tiene el objetivo de plantear un diagnóstico y desarrollar una propuesta de reforma curricular de la carrera del Contador Público con la inclusión de estos temas para una formación académica y profesional adecuada a los requerimientos actuales y a los desafíos futuros. 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 como jurisdicción la Ciudad Autónoma de Buenos Aires.

Actualmente en los planes de estudio, existe la asignatura denominada “Tecnología de la Información”, cuyo eje central radica en el conocimiento de los diferentes sistemas existentes, modelado de datos, características de hardware y ejemplos de software de gestión, basados en los escasos conocimientos que se impartían en la educación media en la década de los 90 (que en ese tiempo resultaba muy importante debido al desconocimiento de los conceptos básicos).

En la actualidad resulta necesario replantear qué conceptos deben ser impartidos en este espacio, considerando las características que el mercado presenta a la labor del contador, ya sea, como analista de gestión, en posiciones de administración, contabilización de impuestos, auditor, analista de procesos, o auxiliar en la justicia, entre otros, en donde está presente en

todos sus tipos la información y todo lo que ello conlleva.

El presente análisis pretende indicar aquellos temas relacionados con la seguridad que deben ser incorporados en la asignatura Tecnología de la Información (y eventualmente en la asignatura Auditoría) y que sea de utilidad para la profesión contable, independientemente al puesto que el profesional deba cubrir.

En el primer capítulo, se analizan las incumbencias profesionales del Contador Público y la gestión de los sistemas de información en la República Argentina.

Del capítulo 2 al 4, se plantea identificar aquellas normas legales, reglamentarias y de los organismos de control relacionadas con la seguridad de la información de cumplimiento obligatorio en los sistemas contables.

En el capítulo 5, en base a los anteriores, se analiza la vinculación de la Contabilidad y la Seguridad de la Información, desde la perspectiva del Derecho[1] y diferentes fuentes normativas aplicables.

En el capítulo 6, se plantean estándares, mejores prácticas, marcos teóricos y conceptuales que contribuyen a la gestión de la Tecnología y Seguridad de la información.

Por último, en los capítulos 7 y 8 se identificarán los requerimientos actuales del Contador Público y los conceptos de Seguridad de la Información que deberían incorporarse en la carrera de Contador en la asignatura Tecnología de la Información, presentando un esbozo de una propuesta curricular superadora.

[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° [01].

A - Presentación del problema.

Para que un sistema de información contable en un soporte tecnológico sea considerado de legal forma, debe cumplir con numerosos requisitos teóricos y tecnológicos de Seguridad de la Información establecidos en leyes, decretos, resoluciones y disposiciones de los organismos de control.

En este contexto, resulta necesario definir cuáles de estos conceptos específicos deben ser incluidos en la formación académica para que el Contador Público egresado pueda cumplir con los mismos.

En el año 2012, el Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales (CODECE) en su documento base para la acreditación de la carrera de Contador Público ha definido que “el objeto de su profesión es la "información" en todas sus formas, sea la misma generada dentro de las organizaciones, interactuando éstas entre sí o en su vinculación con el contexto”. Y considerando que en las organizaciones la información es uno de los activos intangibles de mayor valor en su patrimonio, deberían impartirse los conceptos claves para que los educandos universitarios aprehendan los conocimientos y prácticas que le permitan protegerla.

En esta línea de investigación, la presente Tesis de Maestría tiene el objetivo de analizar los aspectos legales, normativos y tecnológicos de la seguridad de la información en el almacenamiento, procesamiento, control y resguardo de los Registros Contables en sociedades comerciales; y desarrollar una propuesta de reforma curricular con la inclusión de aquellos temas ineludibles en la formación académica y profesional de acuerdo a los desafíos actuales y futuros.

A.1. Antecedentes del tema

En los últimos años, investigaciones en la disciplina Contable reconocen el cambio paulatino que ha tenido la profesión frente al avance de las nuevas tecnologías y comunicación en las organizaciones. A continuación, se describen los hitos más relevantes:

A.1.1. Antecedentes en el ámbito internacional

Una de las primeras publicaciones a nivel internacional data del año 1966 y corresponde a la *American Accounting Asociation* en donde se establece que "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:

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." [2]

Esto marcó un indicio de la vinculación de las tecnologías de información y comunicación con los sistemas contables y el desafío en la formación de los profesionales ante este avance, planteando un nuevo paradigma en la formación de los contadores.

---

[2] American Accounting Association, 1966, "A Statement of Basic Accounting Theory".
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. (…)
Mayor areas in which changes are occurring which well 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".
Véase referencia bibliográfica N° [02].

Cinco décadas posteriores, la Federación Internacional de Contadores (IFAC), organismo que nuclea a profesionales a nivel mundial, planteó en un documento que "el conocimiento principal en los programas profesionales de formación en contaduría puede dividirse en tres aspectos importantes:

a) contaduría, finanzas y conocimientos relacionados;

b) conocimiento organizacional y de negocios; y

c) conocimiento de tecnología de la información y competencias."[3]

Impulsando la incorporación de la tecnología como uno de los ejes principales en la formación actual del contador.

De la misma manera, la Comisión de Sistemas y Tecnologías de Información de la Asociación Interamericana de Contabilidad (AIC) viene difundiendo numerosos trabajos sobre el avance de los sistemas y la seguridad de la información en la profesión contable.

A.1.2. Antecedentes en el ámbito nacional

Una de las primeras investigaciones destacables en el ámbito nacional corresponde a la profesora emérita Luisa Fronti de García,[4] que, en su Tesis Doctoral en Ciencias Económicas en 1968, “La Formación del Contador Público en la UBA”, planteó la necesidad que el Contador en el futuro debería incorporar conocimientos en tecnología de la información para desarrollar sus actividades profesionales.

Otro importante aporte del año 2008 es la tesis de Doctorado en Contabilidad de Elsa Beatriz Suarez Kimura en donde se demuestran los aportes concretos de la Contabilidad a los Sistemas de Información y el rol del contador frente a los futuros cambios en la doctrina y la profesión.

Asimismo, cabe mencionar el pronunciamiento del Consejo de Decanos de Universidades Nacionales de Argentina (CODECE) que se ha citado precedentemente.

También en el ámbito nacional se destacan encuentros de profesionales y académicos en la materia, como Jornadas, Foros de discusión profesional, Congresos Nacionales y Simposios de Profesores de

[3] Véase referencia bibliográfica N° [03].
[4] Véase referencia bibliográfica N° [04].

Práctica Profesional, en donde año tras año se plantea la necesidad de actualizar los contenidos programáticos actuales.

A.2. Planteo del problema

El desconocimiento por parte del Contador Público de conceptos de Tecnología y Seguridad de la información, dificulta el adecuado cumplimiento de las exigencias normativas en los sistemas contables en un contexto tecnológico. Y por su vinculación profesional en la administración, auditoría o como perito auxiliar en el ámbito judicial, resulta necesario su conocimiento para un correcto cumplimiento normativo.

A.3. Objetivos

Se plantea el siguiente objetivo general:

Diagnosticar y proponer los alcances de una reforma curricular que satisfaga los conocimientos necesarios para dar cumplimiento a las exigencias normativas en el sistema de información contable.

Objetivos particulares.

Se definieron los siguientes objetivos particulares:

- Analizar el marco legal relacionado con el procedimiento general de emisión, conversión y conservación de la documentación respaldatoria en los Sistemas Contables.
- Determinar la normativa relevante del Código Civil y Comercial, la Ley General de Sociedades y la Inspección General de Justicia vigente desde agosto de 2015.
- Vincular los conceptos de la Ley número 25.326 de Protección de datos personales y disposiciones de la Dirección Nacional de

Protección de Datos Personales con el Sistema Contable.

- Analizar la Ley número 20.488 de Normas referentes al ejercicio de las profesiones relacionadas a las Ciencias Económicas y su vinculación con conceptos pertinentes en la investigación.
- Identificar y analizar la Seguridad de la Información como una de las disciplinas influyentes en la Contabilidad.
- Identificar normas y mejores prácticas que se vinculan con el sistema contable, como las Normas ISO relacionadas con la gestión de procesos, calidad, seguridad y tecnologías (27.001, 20.001, 22.301) y los entornos de control dispuestos por el Informe COSO y COBIT.
- Analizar estándares y buenas prácticas en la Gestión de: Proyectos, Riesgos de TI, Seguridad de la Información y Continuidad del Negocio.
- Identificar el rol del Contador en la elaboración de planes, políticas y procedimientos en la gestión de las Tecnologías y la Seguridad de Información.
- Analizar cómo debería ser la formación del Contador interpretando las normas del CODECE.[5]
- Identificar los contenidos en Tecnología y Seguridad de la Información que los Contadores Públicos deberían aprender y comprender para el cumplimiento de la legal forma de los Registros Contables.
- Proponer los contenidos curriculares que deberían incorporarse en la Carrera del Contador Público.

A.4. Alcance

La presente investigación cuenta con tres ejes principales. En una primera parte se analizará el marco normativo, prestando especial interés a los requisitos en Tecnología y Seguridad de la información para sociedades

[5] Definido en el artículo número 1 del estatuto: “El Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales, cuya sigla será CO.DE.C.E., es un organismo que tiene como objetivo general colaborar en las áreas de docencia, investigación y extensión propias de las Universidades conforme a sus respectivos estatutos. Su constitución se efectivizará a partir de la aprobación del presente estatuto, el que regirá su funcionamiento.” Véase referencia bibliográfica N° [38].

comerciales dispuestas en el ámbito de la Ciudad Autónoma de Buenos Aires.

En una segunda parte se identificarán los estándares y mejores prácticas que deben ser utilizados para dar cumplimiento a los requisitos identificados y como impactan en el ente.

Y en la última sección, se desarrollará una nómina de contenidos que contemplen todos los conceptos primordiales para satisfacer las necesidades de la profesión contable, sin ponderar la división por asignatura, que se debería debatir en el contexto de un proyecto de Plan de estudios.

A.5. Hipótesis

Para el desarrollo de la investigación de la presente tesis se plantea la siguiente hipótesis: “Para dar cumplimiento a las exigencias normativas en los Sistemas Contables en soporte tecnológico, se necesitan ampliar los contenidos de Tecnología de la Información y en particular los referidos a Seguridad en la carrera del Contador Público”.

A.6. Estructura

En la presente investigación se realiza un análisis documental basándose en el reconocimiento y articulación de los conceptos y variables suministradas por el contexto normativo y los requerimientos demandados a los Contadores Públicos.

Se llevan a cabo relevamientos bibliográficos que permiten actualizar los antecedentes correspondientes a las versiones finales propuestas de currículo de formación de los Contadores emitidas por IFAC, AIC, CODECE, entre otros de los temas propuestos y se efectúa un análisis conceptual de las teorías que subyacen, así como las posibilidades de integración de las mismas. El monitoreo de nuevos pronunciamientos es una constante que posibilita asegurar la validez de las conclusiones parciales y finales.

A partir de la identificación de las variables de formación tecnológica y

ética, se pretende arribar a un diagnóstico de la situación actual y de los cambios necesarios que debieran incluirse en futuros planes de estudios con la mira puesta en el perfil del Contador consensuado internacionalmente.

Cuerpo Principal

- Capítulo I

1. Las Incumbencias profesionales del Contador Público en la República Argentina y la Gestión de los Sistemas de Información.

1. 1. Introducción

Actualmente, las instituciones universitarias dedicadas a la formación de Contadores Públicos se centran en los aspectos técnicos y legales que deben satisfacer el sistema de registros contables en organizaciones con procesos contables manuales, estáticos y con una visión ajena y desvinculada de los sistemas y la tecnología de la información.

Pero es indudable el impacto que ha tenido las tecnologías de información y comunicación en los procesos administrativos, la documentación respaldatoria y en infinidad de elementos en una organización, las que terminan repercutiendo en aspectos formales, normativos y legales en el sistema de información contable. Un ejemplo insoslayable es concluyente al identificar que la mayoría de las sociedades comerciales inscriptas en la Inspección General de Justicia cuentan con sistemas contables en soporte tecnológico y dichos organismos reglamentaron requisitos a cumplir, o cuando una empresa consulta en un estudio las posibilidades de contratar un software en la nube para que la empresa vuelque su información transaccional.

Como se puede observar existen muchas variables a identificar en las cuales la Tecnología y la Seguridad de la Información deben ser impartidas desde la universidad para una formación orientada a las necesidades que requieren actualmente las organizaciones. En opinión del autor, los diversos

temas en la carrera debieran ser abordados de forma conjunta con las buenas prácticas actuales en Tecnología y Seguridad de la información.

El presente capítulo se dedicará a la identificación de los aspectos normativos de la Ley de incumbencias profesionales en Ciencias Económicas para el Contador Público y la gestión de los sistemas de información.

1.2. La Ley número 20.488 de incumbencias profesionales y la administración de la Tecnología y Seguridad de la Información.

En esta sección se analizarán los principales apartados existentes en la Ley de incumbencias de los profesionales en Ciencias Económicas, relacionadas a la profesión del Contador.

En el artículo número 13, la Ley número 20.488 establece que se requerirá el título de Contador Público o equivalente "en materia económica y contable cuando los dictámenes sirvan a fines judiciales, administrativos o estén destinados a hacer fe pública en relación con las siguientes cuestiones: "Elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo–contable" y la "aplicación e implantación de sistemas de procesamiento de datos y otros métodos en los aspectos contables y financieros del proceso de información gerencial."[6]

---

[6] Se requerirá título de Contador Público o equivalente:

a) En materia económica y contable cuando los dictámenes sirvan a fines judiciales, administrativos o estén destinados a hacer fe pública en relación con las cuestiones siguientes:
1. Preparación, análisis y proyección de estados contables, presupuestarios, de costos y de impuestos en empresas y otros entes.
2. Revisión de contabilidades y su documentación.
3. Disposiciones del Capítulo III, Título II, Libro I del Código de Comercio.
4. Organización contable de todo tipo de entes.
5. Elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo–contable.
6. Aplicación e implantación de sistemas de procesamiento de datos y otros métodos en los aspectos contables y financieros del proceso de información gerencial.
7. Liquidación de averías.
8. Dirección del relevamiento de inventarios que sirvan de base para la transferencia de negocios, para la constitución, fusión, escisión, disolución y liquidación de cualquier clase de entes y cesiones de cuotas sociales.
9. Intervención en las operaciones de transferencia de fondos de comercio, de acuerdo con las disposiciones de la Ley N° 11.867, a cuyo fin deberán realizar todas las gestiones que fueren menester para su objeto, inclusive hacer publicar los

Del citado artículo, se puede destacar la vinculación con la "implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo – contable". Partiendo de la base que en la actualidad se han desarrollado mejores prácticas y modelos de gestión que abarcan desde las normas ISO, Sistema de Gestión de la Calidad, Ambiental, Seguridad de la información y hasta la tecnología como un servicio, seguido de otras normas relacionadas como el control, Informe COSO, COBIT de ISACA, terminan impactando en los Sistemas de Información Contables y el donde el contador puede contribuir en la planificación, gestión y control de diferentes sistemas administrativos.

En esta línea, algunas de las comisiones del Consejo Profesional en Ciencias Económicas de la Ciudad Autónoma de Buenos Aires, como la de Sistemas de Registros[7], plantean la necesidad que los profesionales

---

edictos pertinentes en el Boletín Oficial, sin perjuicio de las funciones y facultades reservadas a otros profesionales en la mencionada norma legal.
10. Intervención juntamente con letrados en los contratos y estatutos de toda clase de sociedades civiles y comerciales cuando se planteen cuestiones de carácter financiero, económico, impositivo y contable.
11. Presentación con su firma de estados contables de bancos nacionales, provinciales, municipales, mixtos y particulares, de toda empresa, sociedad o institución pública, mixta o privada y de todo tipo de ente con patrimonio diferenciado.
En especial para las entidades financieras comprendidas en la Ley N° 18.061, cada Contador Público no podrá suscribir el balance de más de una entidad cumplimentándose asimismo el requisito expresado en el Art. N° 17 de esta Ley.
12. Toda otra cuestión en materia económica, financiera y contable con referencia a las funciones que le son propias de acuerdo con el presente artículo.

b) En materia judicial para la producción y firma de dictámenes relacionados con las siguientes cuestiones:
1. En los concursos de la Ley N° 19.551 para las funciones de síndico.
2. En las liquidaciones de averías y siniestros y en las cuestiones relacionadas con los transportes en general para realizar los cálculos y distribución correspondientes.
3. Para los estados de cuenta en las disoluciones, liquidaciones y todas las cuestiones patrimoniales de sociedades civiles y comerciales y las rendiciones de cuenta de administración de bienes.
4. En las compulsas o peritajes sobre libros, documentos y demás elementos concurrentes a la dilucidación de cuestiones de contabilidad y relacionadas con el comercio en general, sus prácticas, usos y costumbres.
5. Para dictámenes e informes contables en las administraciones e intervenciones judiciales.
6. En los juicios sucesorios para realizar y suscribir las cuentas particionarias juntamente con el letrado que intervenga.
7. Como perito en su materia en todos los fueros.

En la emisión de dictámenes, se deberán aplicar las normas de auditoría aprobadas por los organismos profesionales cuando ello sea pertinente.
Véase referencia bibliográfica N° [05]

[7] Comisión de Sistemas de Registros, Integridad y Autenticidad documental. Consejo

podrían, (realizando las especializaciones correspondientes), implantar estándares de sistemas de gestión y liderar a las auditorías sobre las normas ISO, independientemente de la legal forma.

Para lo cual se necesitaría un profesional con una visión integral sobre estos temas, para encarar las diferentes cuestiones especificadas en las incumbencias profesionales del Contador Público.

1.3. Conceptos impartidos en la asignatura "Tecnología de la Información".

En los actuales planes de estudio para Contadores Públicos, se imparten principalmente los siguientes conceptos:

Esquema N° 1: Conceptos impartidos actualmente.	Historia de la Computación
	Hardware
	Redes
	Bases de Datos
	Modelado de Datos y Lenguaje SQL
	Metodología y desarrollo de software

Fuente: Elaboración Propia.

Que si bien fueron incorporados en momentos en donde los educandos no recibían contenidos en la Educación Media.

Estos conceptos no representan la totalidad de los conocimientos que el Contador Público debiera adquirir para dar cumplimiento a las exigencias de un sistema contable en un contexto tecnológico.

1.4. Síntesis del capítulo I.

En la Ley número 20.488 se establecen como incumbencias del Contador Público: la elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo – contable, como también la aplicación e implantación de sistemas de procesamiento de datos en los aspectos contables y financieros del proceso de información gerencial; relacionando a la profesión en los métodos de procesamientos y soportes que son el contexto de la información contable.

Sin embargo, en los actuales planes de estudio para Contadores Públicos, se imparten principalmente conceptos relacionados con historia de la computación y fundamentos de hardware y software, centralizándose en la formación de un profesional ajeno a la Tecnología y Seguridad de la Información, omitiendo conceptos que debiera conocer para dar cumplimiento a la legal forma de un sistema contable en un contexto tecnológico.

- Capítulo II

2. MARCO LEGAL DE LOS REGISTROS CONTABLES EN LA REPÚBLICA ARGENTINA.

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 Civil y Comercial puesto en vigencia a partir del primero de agosto de 2015 y las opiniones más relevantes de la doctrina del derecho contable destacando la importancia de la Seguridad de la Información en la legalidad de un sistema contable.

2.2. Obligación de llevar Registros Contables.

El Código Civil y Comercial de la República Argentina en el artículo número 320 establece que "están obligadas a llevar contabilidad todas las personas jurídicas privadas y quienes realizan una actividad económica organizada o son titulares de una empresa o establecimiento comercial, industrial, agropecuario o de servicios. (…) Cualquier otra persona puede llevar contabilidad si solicita su inscripción y la habilitación de sus registros o la rubricación de los libros[8]...".[9] Por lo cual, todo comerciante debe

[8] Sin perjuicio de lo establecido en leyes especiales, quedan excluidas de las obligaciones previstas en esta Sección las personas humanas que desarrollan profesiones liberales o actividades agropecuarias y conexas no ejecutadas u organizadas en forma de empresa. Se consideran conexas las actividades dirigidas a la transformación o a la enajenación de

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 todas “las personas jurídicas privadas y quienes realizan una actividad económica organizada o son titulares de una empresa o establecimiento comercial, industrial, agropecuario o de servicios” deben indispensablemente llevar los libros “diario; inventario y balances; aquellos que corresponden a una adecuada integración de un sistema de contabilidad y que exige la importancia y la naturaleza de las actividades a desarrollar; y los que en forma especial impone este Código u otras leyes”[10]; además los mismos deberán estar:

- Inscriptos en el registro,
- Con la documentación contable correspondiente,
- Con una adecuada integración de un sistema de contabilidad; y
- “El interesado debe llevar su contabilidad mediante la utilización de libros y debe presentarlos, debidamente encuadernados, para su individualización en el Registro Público correspondiente.”[11]

El Código establece que “El titular puede, previa autorización del Registro Público de su domicilio:

a) sustituir uno o más libros, excepto el de Inventarios y Balances, o alguna de sus formalidades, por la utilización de ordenadores u otros medios mecánicos, magnéticos o electrónicos que permitan la individualización de las operaciones y de las correspondientes cuentas deudoras y acreedoras y su posterior verificación;

b) conservar la documentación en microfilm, discos ópticos u otros medios aptos para ese fin.” [12]

---

productos agropecuarios cuando están comprendidas en el ejercicio normal de tales actividades. También pueden ser eximidas de llevar contabilidad las actividades que, por el volumen de su giro, resulta inconveniente sujetar a tales deberes según determine cada jurisdicción local.

[9] Véase referencia bibliográfica N° [06].

[10] Véase referencia bibliográfica N° [07].

[11] Véase referencia bibliográfica N° [08].

[12] Véase referencia bibliográfica N° [09].

Dicha petición debe contener una adecuada descripción del sistema, con dictamen técnico de Contador Público e indicación de los antecedentes de su utilización. “Una vez aprobado, el pedido de autorización y la respectiva resolución del organismo de contralor, deben transcribirse en el libro de Inventarios y Balances.

La autorización sólo se debe otorgar si los medios alternativos son equivalentes, en cuanto a inviolabilidad, verosimilitud y completitud, a los sistemas cuyo reemplazo se solicita.”[13]

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

Esquema N° 2:
Marco Normativo de los Registros Contables en Sociedades Comerciales en la CABA.

- Código Civil y Comercial (2015)
- Ley General de Sociedades (2015)
- Disposiciones de la Inspección General de Justicia (IGJ) (07/2015)

Fuente: Elaboración propia.

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

En el artículo número 61 de la Ley General de Sociedades 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 autorice la sustitución de los mismos (…), salvo el de Inventarios y Balances.”[14]

Para hacerse efectiva la autorización, se deberá realizar una petición que incluya una “adecuada descripción del sistema con un dictamen técnico

[13] Véase referencia bibliográfica N° [09].
[14] Véase referencia bibliográfica N° [10].

o antecedentes de su utilización, lo que, una vez autorizada, deberá transcribirse en el libro de Inventarios y Balances."[15]

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."[16]

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:[17]

- Asegurar que los registros sean inalterables; ello implica las siguientes condiciones:
  - ✓ Que las registraciones deben coincidir con el acontecimiento de los hechos y actos económicos;
  - ✓ Que una vez hecha las mismas, no puedan ser modificadas ni puedan desaparecer por "perención[16] del soporte"[18].
- 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 considere 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

[15] Véase referencia bibliográfica N° [10].
[16] Véase referencia bibliográfica N° [10]
[17] En los fundamentos en la exposición de Motivos de la Ley número 19550, Sec. IX, N 2, "in fine", los miembros de la comisión expresan: 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.
[18] Véase referencia bibliográfica N° [11]

conservación de los datos[16] de modo de permitir la "inalterabilidad y verificabilidad".[19]

Para cumplir con estos dos requisitos se plantea la necesidad de 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 el Derecho para llevar una contabilidad informatizada.

Gran parte de la doctrina contable ha compartido en las últimas décadas preocupaciones referidas a los riesgos 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 por Eduardo M. Favier Dubois[19]:

Tabla N° 1: Riesgos identificados por el Derecho para llevar una contabilidad informatizada.
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[20]: “Dado que se trata de material tecnológico recientemente introducido a la industria de la informática, se carece de

[19] Véase referencia bibliográfica N° [11]

[20] 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.

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]

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

En jornadas profesionales de derecho contable[21] se ha concluido numerosas veces que la circunstancia de que haya autorizado la utilización de libros contables por medios informáticos de registro[22] no resulta suficiente para “considerar que su contabilidad está llevada de legal forma”.[23] 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.”[24]

Entender que basta con que los datos correspondientes estén “en el sistema contable – es decir, almacenados en 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 número 61 de la Ley General de Sociedades.

Por ello, cuando una entidad bancaria se defiende en cuanto al cumplimiento de la obligación de llevar los registros rubricados que incluyan las transacciones con detalle, “alegando que están en el sistema, está

[21] Jornada sobre Derecho y Contabilidad Informática.
[22] Véase referencia bibliográfica N° [10].
[23] Véase referencia bibliográfica N° [12].
[24] Véase referencia bibliográfica N° [13].

infringiendo dicha obligación”.[25]

2.7. Síntesis del capítulo II.

En esta sección se analiza desde una perspectiva del derecho contable las formalidades que deben cumplirse en una “contabilidad informatizada”. La Ley General de Sociedades autoriza en el artículo número 61 a llevar el sistema de 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”[26],

d. Tomar las medidas necesarias para garantizar la inviolabilidad, verosimilitud y completitud 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 cumplimento 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 un sistema de información contable legalmente constituido.

[25] Véase referencia bibliográfica N° [34].
[26] El libro inventario y balances es uno de los libros exigidos en el Código Civil y Comercial.

- Capítulo III

3. Normas del Organismo Regulador 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 control en cada jurisdicción. 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 en la Resolución General número 7 de 2015, establece que los sistemas de registros contables deben cumplir con los requisitos enunciados a continuación:

Tabla N° 2: 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.”
5. “Permitan obtener acceso como parte de la operatoria habitual, debiendo estar respaldado 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 impuestos por el Código Civil y Comercial de la Nación, leyes complementarias y especiales, así como lo requerido por estas Normas.”
Fuente: IGJ. [27]

Teniendo en cuenta estas características principales se analizan 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 rollos”[28], 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 adelante[29],

[27] Véase referencia bibliográfica N° [18].
[28] Véase referencia bibliográfica N° [14].
El plexo normativo de la IGJ se especifican los siguientes medios de almacenamientos: compact disc, otros discos ópticos y microfilmes, o similares.
[29] Véase referencia bibliográfica N° [14].

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.[30] En el caso de la utilización de CDs y DVDs como medio de almacenamiento, no se deberían utilizar los 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"[31] 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."[32]

---

[30] Véase referencia bibliográfica N° [14].
[31] Véase referencia bibliográfica N° [14].
[32] Véase referencia bibliográfica N° [14].

✓ **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"[33], 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:

Cuadro N° 1: Requisitos de la Seguridad de la Información en el Sistema Contable.		
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.[34]
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.[35]		

[33] Véase referencia bibliográfica N° [14].
[34] Por lo tanto, hay que considerar la generación que permite leerlos.
[35] Véase referencia bibliográfica N° [14].

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. [36]

Además, se debe cumplir con los siguientes requisitos con las actas señaladas:

- ✓ "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 que anteceden, emitiendo al respecto un informe especial que se registrará con su firma en el libro de Inventarios y Balances o en el libro de medios ópticos si los hubiere. 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."[37]

3.3. Trámites y requisitos solicitados por la Inspección General de Justicia (Resolución General número 7 de 2015).

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

- Primer testimonio de escritura pública o instrumento privado

[36] Véase referencia bibliográfica N° [14].
[37] Sistemas de registración contable en compact disc, otros discos ópticos y microfilmes. Véase referencia bibliográfica N° [14].

original con los recaudos del artículo número 37, incisos número 1 y 2.

- Informe de las características del sistema.
- Dictamen de precalificación de Contador Público

En el siguiente cuadro se especifican cada uno de ellos:

Cuadro N° 2: Autorización para empleo de ordenadores (IGJ).		
Elementos	**Características**	**Notas**
Primer testimonio de escritura pública o instrumento privado original con los recaudos del artículo número 37, incisos número 1 y 2, conteniendo la transcripción de la resolución del órgano de administración de la sociedad, de solicitar la autorización reglamentada en este artículo. La resolución del órgano de administración deberá contener:	"a. En el caso de sustitución de libros rubricados, la denominación exacta de los libros rubricados que se reemplazan y registros que se solicitan; b. En el caso de sustitución de autorizaciones previamente emitidas por este Organismo de acuerdo a las disposiciones del artículo número 61 de la Ley número 19.550: número de autorización que se reemplaza y registros por los que se efectúa la presentación. En caso de tratarse de una sustitución parcial, se indicarán los registros que continúan manteniéndose mediante la autorización ya emitida; c. El sistema de archivo a utilizar (medios ópticos, mecánicos u otros); d. La declaración expresa si el sistema y registros por los que se solicita autorización, han sido utilizados previo a la intervención del Organismo, indicando en su caso fecha de comienzo de utilización; e. Si se solicita la autorización de sistema en compact disc, otros discos ópticos y microfilmes, ya sean microfichas o rollos, deberá contener expresamente el compromiso de	Para el desarrollo de esta actividad se requieren los conocimientos de un Contador Público.

	preservar la posibilidad de lectura de los medios de registración y/o extender en listados de papel los registros, durante el período en que la ley determina obligatoria su exigibilidad; f. En caso de tercerización de archivo de documentación física y/o informática, deberá contener la denominación del tercero proveedor del servicio, radicación de los archivos y/o medio de procesamiento, vigencia del contrato y las políticas de seguridad en la información implementadas. g. Si el sistema de registración contable solicitado fuera de propio desarrollo, deberá surgir claramente la descripción del sistema, sus funciones, interfaces con las que opera y diagrama de módulos de conformidad con los requisitos dispuestos en el artículo número 326 de esta Norma, de modo tal que permitan la verificación prevista por el artículo número 335.”	
2. Las siguientes piezas firmadas por el representante legal o apoderado con facultades suficientes y por contador público independiente con su firma legalizada por la entidad que detenta la superintendencia de su matrícula, conteniendo:	“a. La exposición amplia y precisa del sistema de registración contable a utilizar, indicando los propósitos de la modificación propuesta; si se trata de la modificación o sustitución de un sistema anterior, deberán explicarse los motivos y las diferencias con el mismo. 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 completo. Deben surgir claramente los datos que ingresan a partir de la documentación contable (facturas de compras, ventas, ingresos, egresos, etc.), su procesamiento y la salida que genera, la cual será coincidente con todos los registros contables de la sociedad. De existir interfaces, conexiones remotas	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 Seguridad de la información.

	u otras similares deberá exponerse en el diagrama. c. Demostración técnica del grado de inalterabilidad de las registraciones a efectuar mediante el sistema propuesto; indicando software y hardware a utilizar, política de contraseñas, conexiones remotas, interfaces, etc. d. Metodología de generación de CD o DVD y metodología de archivo de documentación respaldatoria y de los soportes. En el caso de microfilms, CD o DVD se requiere archivo ignífugo. e. El sistema y periodicidad en la numeración de los registros. f. Estado de actualización de todos los registros, contables y legales 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. Dicho estado de actualización se presentará con un atraso que no supere los treinta (30) días; g. Modelos en blanco por duplicado y uno ejemplificativo conteniendo: denominación social y domicilio legal inscripto, denominación del registro o listado, ambos configurados con fecha y número de página sin determinar. h. Plan de cuentas incluyendo denominación y domicilio social inscripto.”	
3. Dictamen de precalificación de contador público, en el cual se verificará: a. la situación de la sociedad en relación a todos los supuestos de los art. 94 y 299 de la Ley número 19.550, así como el cumplimiento detallado de los artículos 326, 333, 334 y 335 (según corresponda), quórum y mayorías de la reunión del órgano de		Se requiere el título de Contador Público.

administración. **b. En el caso de sustitución de libros llevados bajo la modalidad de rúbrica y considerando las disposiciones del artículo número 342, informará si se ha previsto la solicitud de los libros necesarios para efectuar la discontinuación inmediata una vez emitida la autorización por parte de este Organismo, manteniendo la contabilidad actualizada a esa fecha.** **c. Radicación del archivo de la documentación respaldatoria y de los soportes.**	
Elaboración propia del cuadro. Fuente: IGJ.[38]	

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

- Informe Anual.
- Informe de actualización técnica.
- Otros que requiera el organismo.

En el siguiente cuadro se especifican las características más relevantes de los mismos:

Cuadro N° 3: Informes periódicos medios magnéticos u otros. (IGJ)[39]		
Informes	**Características**	**Profesionales**
- 1 - Información anual; certificación.	Las sociedades que obtengan la autorización requerida por el artículo número 61 de la Ley número 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: **1.** Informe especial suscripto por contador público independiente, conteniendo: a. La descripción exacta del sistema utilizado durante el ejercicio económico. Se informará si se han implementado	Se requiere el título de Contador Público.

[38] Véase referencia bibliográfica N° [35].
[39] Véase referencia bibliográfica N° [14].

	actualizaciones al sistema oportunamente aprobado, con indicación de versión original y versión actual, así como fecha de efecto. b. Opinión fundada sobre la concordancia existente entre el sistema de registración contable y diseño de registros utilizado durante dicho ejercicio y el oportunamente autorizado. c. Informará datos del libro Inventario y Balances en el que se ha transcripto las autorizaciones y/o bajas emitidas por el Organismo, la descripción de los sistemas aprobados, los diseños de registros y el plan de cuentas. d. En caso de detectarse discordancias entre el o los sistemas y diseños aprobados por el Organismo y los utilizados durante el ejercicio que se informa, el profesional interviniente acompañará detalle de las mismas, indicando fecha de efecto de cada una. e. Informará opinión sobre cumplimiento de todos los apartados del artículo número 326, 333 y/o 334, según corresponda. f. Junto con su informe, acompañará datos de la totalidad de los listados o registros utilizados durante el período que se informa, indicando: denominación, período, número inicial y final de cada soporte, libro o ficha y metodología de archivo de los mismos. En caso de medios ópticos indicará cumplimiento del artículo número 334, incisos número 5 y 6. g. Informará vigencia del contrato de tercerización de archivo de documentación física y/o informática, en caso de corresponder. **2.** Escrito debidamente suscripto por representante legal de la misma, con firma y cargo certificados notarialmente, invocando carácter de la presentación efectuada y ratificando la documentación acompañada por el profesional interviniente. **3**. Copia/s de la autorización/es vigente/s	

	para el ejercicio económico respectivo y copia de las actas labradas en cumplimiento de los incisos número 5 y 6 del artículo número 334 de estas Normas. De no existir observaciones se emitirá a la sociedad una certificación que lo indicará, la cual deberá ser agregada al libro de Inventarios y Balances. En el supuesto que en oportunidad del presente se verifique algún incumplimiento a las normas contenidas en el presente Título, la sociedad deberá regularizar su situación dentro de los noventa (90) días a contar desde la emisión de la constancia extendida por el Organismo.	
- II - Informe de actualización técnica. Sin perjuicio de la información a presentar conforme al apartado anterior, cada dos (2) años las sociedades deberán presentar:	**1.** Informe técnico emitido por contador público independiente sobre la situación de obsolescencia del sistema utilizado y, en su caso, un proyecto de actualización técnica del mismo y de las medidas y reemplazos necesarios, requiriendo nueva autorización conforme a lo dispuesto en el artículo número 328 anterior. Asimismo, dicho informe contendrá: a. Opinión fundada sobre la situación de obsolescencia del sistema oportunamente aprobado y estado de actualización técnica del mismo. b. Período bienal por el que se emite dicho informe. El mismo abarcará dos (2) ejercicios económicos y deberán ser coincidentes, cronológicamente, con los presentados en cumplimiento de la información anual requerida por el apartado I de este artículo. c. Datos del libro Inventario y Balances en el que se han transcripto las autorizaciones y/o bajas emitidas por el Organismo, la descripción del/ los sistemas aprobados, los diseños de registros y planes de cuentas. **2.** Escrito debidamente suscripto por representante legal de la misma, con firma y cargo certificados notarialmente, invocando carácter de la presentación efectuada y ratificando la documentación acompañada por el profesional	Se requiere el título de Contador Público.

	interviniente. **3.** Copia/s de la autorización/es vigente/s y/o bajas para el período bienal respectivo.	
- III - **Otros Informes**	La Inspección General de Justicia 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. La infracción a lo dispuesto en el presente artículo hará pasible a la sociedad, sus directores y síndico de hasta el máximo de la multa prevista en las leyes 19.550 y 22.315.	Se requiere el título de Contador Público.
Fuente: IGJ.[40]		

- **Profesionales comprometidos en los informes:**

Con la nueva Resolución General número 7/15 de la IGJ se especifica que el Informe Anual, el Informe de actualización técnica y los otros que requiera el organismo; deben estar acompañado del formulario correspondiente y un informe de un Contador Público con la firma legalizada por el organismo con poder de policía de la profesión. Bajo esta situación, surge la necesidad de contar con profesionales capacitados para comprender la problemática y trabajar interdisciplinariamente con especialistas en tecnología y seguridad y responder a estas demandas.

3.4. Síntesis 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 número 7 del año 2015 se enuncian los diferentes trámites a efectuar para autorizar y mantener los sistemas

[40] Véase referencia bibliográfica N° [14].

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;

Resulta necesaria la capacitación del contador y trabajar interdisciplinariamente con especialistas 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 Informe 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. IMPLICANCIAS DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN EL SISTEMA DE INFORMACIÓN CONTABLE.

4.1. Introducción.

En el año 2000, en la República Argentina se promulgó la Ley número 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.[41]

En este capítulo, se analiza la Ley de Protección de Datos personales y su vinculación con la información contenida en los sistemas contables informatizados.

4.2. Reconocimiento de las Bases de Datos presentes en las Organizaciones. Conceptos y objetivos de la Ley número 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

[41] Véase referencia bibliográfica N° [15].

destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre."[42] La ley toma en cuenta tanto los datos de las personas físicas como los de las personas jurídicas.

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

4.3. Clasificación de Datos Personales.

La ley número 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"[43].

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.

Esquema Nº 3: Clasificación de Datos Personales.

Fuente: Elaboración propia.

[42] Véase referencia bibliográfica N° [15].
[43] Véase referencia bibliográfica N° [16].

Con respecto a la categoría de datos, el artículo número 7 de la Ley establece que:

"1. Ninguna persona puede ser obligada a proporcionar datos sensibles.
2. Los datos sensibles sólo pueden ser recolectados y objeto de tratamiento cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas cuando no puedan ser identificados sus titulares.
3. Queda prohibida la formación de archivos, bancos o registros que almacenen información que directa o indirectamente revele datos sensibles. Sin perjuicio de ello, la Iglesia Católica, las asociaciones religiosas y las organizaciones políticas y sindicales podrán llevar un registro de sus miembros.
4. Los datos relativos a antecedentes penales o contravencionales sólo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas."[44]

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

Cuadro Nº 4: 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 / Debito.	Si determina el cliente	Datos Intermedios

Fuente: Elaboración propia.

[44] Véase referencia bibliográfica N° [17].

Cuadro Nº 5: 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 determinan Clientes.	-	Datos Intermedios
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 6: 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 7: 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.

4.4. 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.

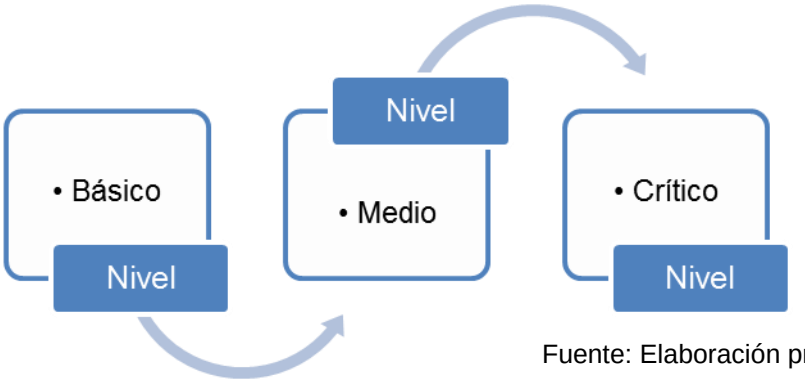
Queda prohibido registrar datos personales en archivos, registros o bancos que no reúnan condiciones técnicas de integridad, seguridad, como también los que no garanticen el cumplimiento de los términos de la presente ley.

En la disposición número 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.[45]

[45] A los interesados en ampliar la información el sobre el tema, podrán consultar en página web indicada en la bibliografía del presente trabajo la resolución completa Nº 11/2006 de la DNPDP. Véase referencia bibliográfica N° [18].

Esquema Nº 4: Niveles de Seguridad.



Fuente: Elaboración propia.

• MEDIDAS DE SEGURIDAD DEL NIVEL BASICO:[46]

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 número 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 3: 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

[46] Véase referencia bibliográfica N° [18].

efectos de su corrección. Todos los programas de ingreso de datos, cualquiera sea su modo de procesamiento (batch, interactivo, etc.), deben incluir en su diseño, rutinas de control, que minimicen la posibilidad de incorporar al sistema de información, datos ilógicos, incorrectos o faltantes”.
4. “Registros de incidentes de seguridad”.
5. “Procedimientos para efectuar las copias de respaldo y de recuperación de datos”.
6. “Relación actualizada entre Sistemas de Información y usuarios de datos con autorización para su uso”.
7. “Procedimientos de identificación y autenticación de los usuarios de datos autorizados para utilizar determinados sistemas de información”.
8. “Control de acceso de usuarios a datos y recursos necesarios para la realización de sus tareas para lo cual deben estar autorizados”.
9. “Medidas de prevención a efectos de impedir amenazas de software malicioso (virus, troyanos, etc.) que puedan afectar archivos con datos de carácter personal”.
Fuente: Disposición número 11/2006 – DNPDP.[47]

• MEDIDAS DE SEGURIDAD DE NIVEL MEDIO:[48]

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 número 10 de la Ley número 25.326, deban guardar secreto de la información personal por expresa disposición legal (como el secreto bancario):

[47] Véase referencia bibliográfica N° [18].
[48] Véase referencia bibliográfica N° [19].

Tabla Nº 4: Medidas de Seguridad del Nivel Medio.
1. “El Instructivo de seguridad deberá identificar al Responsable (u órgano específico) de Seguridad”.
2. “Realización de auditorías (internas o externas) que verifiquen el cumplimiento de los procedimientos e instrucciones vigentes en materia de seguridad para datos personales”.
3. “Limitar la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información”.
4. “Establecer un control de acceso físico a los locales donde se encuentren situados los sistemas de información con datos de carácter personal”.
5. “Gestión de Soportes e información contenida en ellos”.
6. “Los registros de incidentes de seguridad, en el caso de tener que recuperar datos, deberán identificar la persona que recuperó y/o modificó dichos datos. Será necesaria la autorización en forma fehaciente del responsable del archivo informatizado”.
7. “Las pruebas de funcionamiento de los sistemas de información, realizadas con anterioridad a su puesta operativa, no se realizarán con datos/archivos reales, a menos que se aseguren los niveles de seguridad correspondientes al tipo de datos informatizados tratados”.
Fuente: Disposición número 11/2006 – DNPDP.[49]

• MEDIDAS DE SEGURIDAD DEL NIVEL CRÍTICO:[50]

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:

[49] Véase referencia bibliográfica N° [18].
[50] Véase referencia bibliográfica N° [19].

Tabla Nº 5: Medidas de Seguridad de Nivel Crítico.
1. "**Distribución de soportes**: cuando se distribuyan soportes que contengan archivos con datos de carácter personal —incluidas las copias de respaldo—, se deberán cifrar dichos datos (o utilizar cualquier otro mecanismo) a fin de garantizar que no puedan ser leídos o manipulados durante su transporte."
2. "**Registro de accesos**: se deberá disponer de un registro de accesos con información que identifique al usuario que accedió, cuando lo hizo (fecha y hora), tipo de acceso y si ha sido autorizado o denegado. En el caso que el acceso haya sido autorizado se deberá identificar el dato accedido y el tratamiento que se le dio al mismo (baja, rectificación, etc.). Este registro de accesos deberá ser analizado periódicamente por el responsable de seguridad y deberá ser conservado como minino por el término de un TRES (3) años."
3. "**Copias de respaldo**: además de las que se mantengan en la localización donde residan los datos deberán implementarse copias de resguardo externas, situadas fuera de la localización, en caja ignífuga y a prueba de gases o bien en una caja de seguridad bancaria, cualquiera de ellas situadas a prudencial distancia de la aludida localización. Deberá disponerse de un procedimiento de recuperación de esa información y de tratamiento de la misma en caso de contingencias que pongan no operativo el/los equipos de procesamiento habituales."
4. "**Transmisión de datos**: los datos de carácter personal que se transmitan a través de redes de comunicación, deberán serlo cifrados o utilizando cualquier otro mecanismo que impida su lectura y/o tratamiento por parte de personas no autorizadas."
Fuente: Disposición número 11/2006 – DNPDP.[51]

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

[51] Véase referencia bibliográfica N° [18].

incumplimiento de estos requisitos dará lugar a las sanciones administrativas previstas en la ley.

4.5. Síntesis del capítulo IV.

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 número 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 V

5. LA CONTABILIDAD Y SU VINCULACIÓN CON LA TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN.

5.1. Introducción.

El presente capítulo persigue el objetivo de desarrollar brevemente cuestiones básicas de la Tecnología y la Seguridad de la Información y su aporte a la Teoría General Contable.

El autor considera necesario el citado análisis ya que plantea las bases teóricas de las disciplinas que se analizan en la presente tesis.

5.2. 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"[52]. 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."[53]

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

[52] Definición extraída de la Real Academia Española; Véase referencia bibliográfica N° [24].
[53] Véase referencia bibliográfica N° [20].

- 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."[54]

5.3. Concepto de Contabilidad.

La contabilidad como disciplina, fue conceptualizada por el Profesor Emérito Dr. Carlos Luís García Casella, quien expresa 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 cumplimento de sus metas a través de un método basado en un conjunto de supuestos básicos [...]"[55].

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

---

[54] Véase referencia bibliográfica N° [21].
[55] Informe presentado en el 1er Encuentro Universitario de Investigaciones del Área Contable. Véase referencia bibliográfica N° [22].

- 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.

5.4. Requisitos de la Información contenida en los Estados Contables.

En la Resolución Técnica número 16[56], 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° 6: 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	
Elaboración propia. Fuente: FACPCE.[57]	

[56] Extraído de la FACPCE. Véase referencia bibliográfica N° [23].
[57] Véase referencia bibliográfica N° [23].

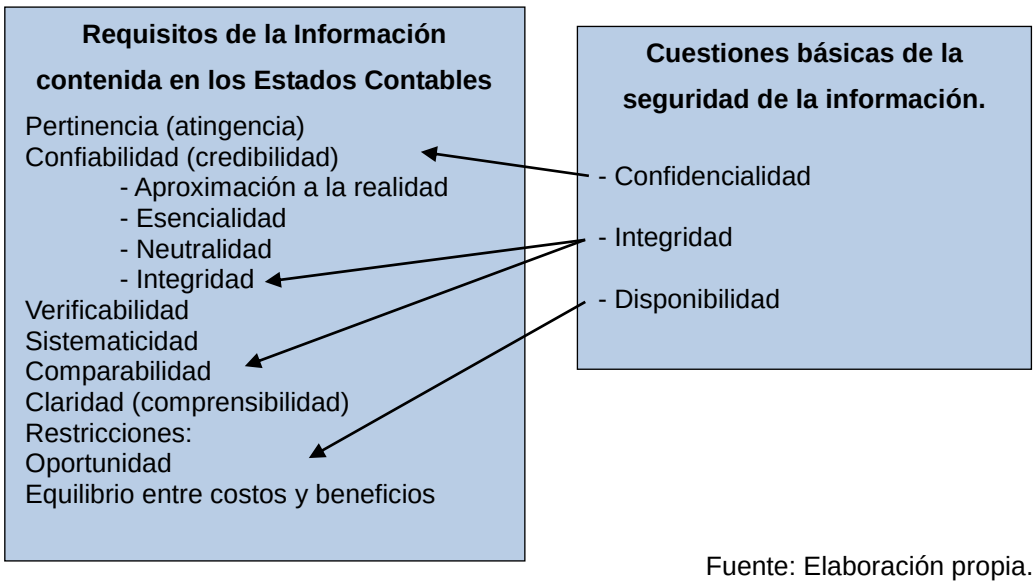
5.5. Seguridad de la Información y su aporte a la Contabilidad.

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 “Tecnología y Seguridad de la 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.

Esquema Nº 5: Aportes de la Seguridad de la Información a la Contabilidad.



Fuente: Elaboración propia.

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:

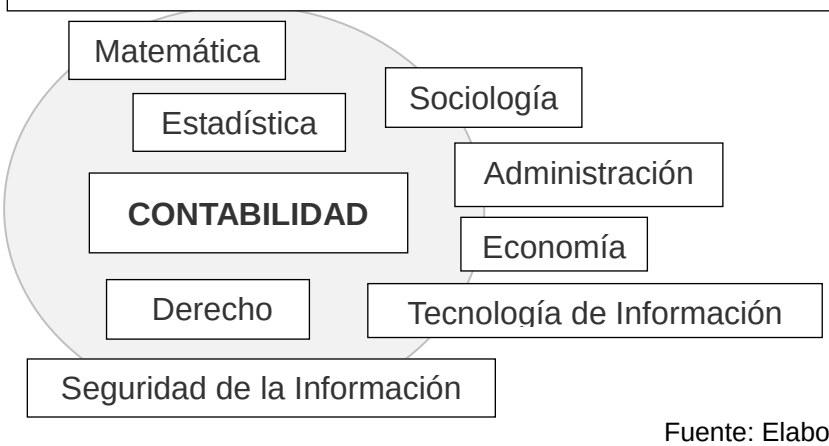
- Conocimiento de los procesos de decisión.
- Conocimiento de las conductas humanas.
- Tecnologías de la computación y el diseño de sistemas.
- Técnicas de medición y teoría de la información.”[58]

En el año 2015, cuarenta y nueve 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 cumplimento de los requisitos y el resguardo de la información contable.

[58] Extraído de la referencia bibliográfica N° [02].

Esquema N° 6: Disciplinas influyentes en la Contabilidad.



Fuente: Elaboración propia.

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 8: Elementos del Sistema contable y la Seguridad de la Información.

	Elementos	Seguridad de la Información
Sistema de información contable en un contexto tecnológico	Recursos Humanos	Ética y compromiso con la organización
	Aplicaciones	Seguridad en los Aplicativos
	Sistemas Operativos	Seguridad en los Sistemas Operativos o Software de base
	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.
- ✓ Disposiciones y resoluciones de los organizamos de control.

5.6. Síntesis del capítulo V.

La Contabilidad analizada como disciplina es influida por 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 "Tecnología y 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°8).

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 prescinda de las bondades que ella brinda.

- Capítulo VI

6. GESTIÓN DE MEJORES PRÁCTICAS Y ESTÁNDARES DE CONTROL Y SEGURIDAD DE LA INFORMACIÓN EN LAS ORGANIZACIONES.

6.1. Introducción.

El objetivo del presente capítulo es analizar e identificar aquellos marcos de gestión y buenas prácticas de Tecnología y Seguridad de la información existentes y aplicables al sistema contable.

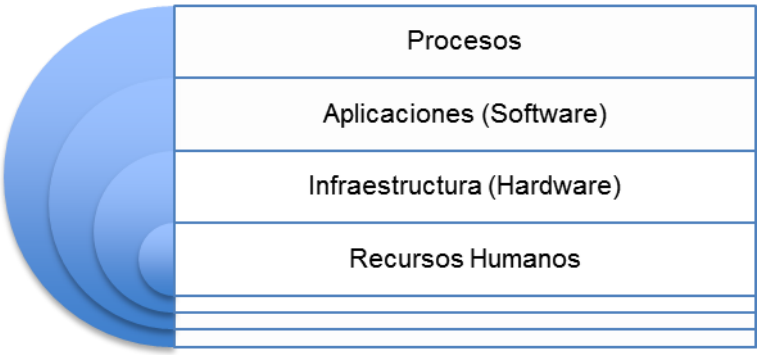
En el mismo se analizarán los más relevantes a la currícula del Contador y a los interesados en profundizar en los mismos invitamos consultar el Anexo C de la presente tesis.

6.2. Interrelación de los elementos del sistema contable.

Como se identificó en el capítulo precedente, existen diferentes elementos que forman el sistema de información contable, pero resulta fundamental establecer la dependencia y relación entre ellos.

Primero, resulta primordial reconocer los procesos y procedimientos que lo componen. En una segunda etapa, vincular las aplicaciones, módulos y herramientas informáticas utilizadas para cada uno de los procesos y la infraestructura tecnológica; y por último los recursos humanos relacionados.

Esquema N° 7: Elementos de los sistemas contables.



Fuente: Elaboración propia.

Considerando esta dependencia, se puede identificar cómo repercuten con las Tecnologías de Información a los procesos del Sistema Contable, contribuyendo en:

- Establecer Controles y Procesos.
- Mejorar la Calidad de la Auditoría Financiera.
- Incrementar la eficacia y eficiencia de las operaciones.
- Mejorar la administración de TI.

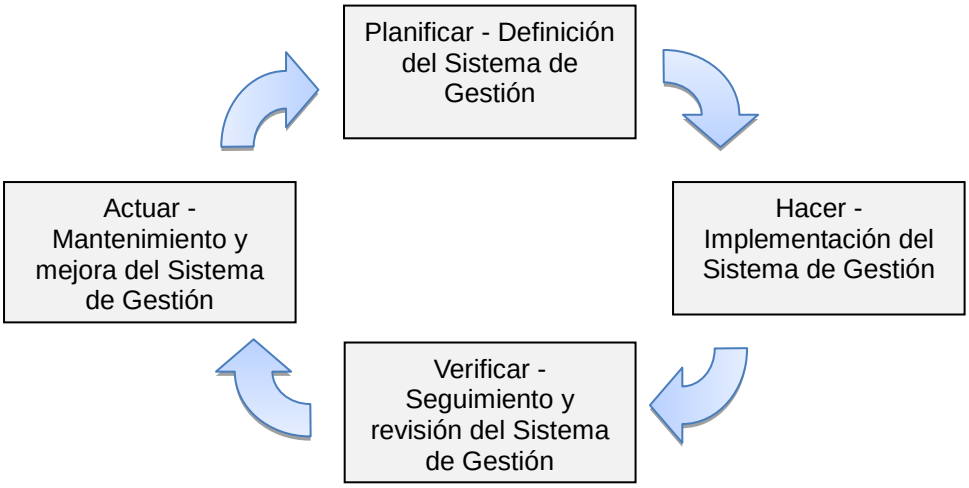
A continuación, se establecen las normas básicas a considerar para los diferentes elementos de los sistemas contables:

6.3. Análisis de la calidad de los procesos administrativos.

La ISO/IRAM 9001 plantea los requisitos para implantar un Sistema de Gestión de la Calidad, que puede utilizarse para su aplicación interna por las organizaciones. Brindando la posibilidad de certificar la calidad de los procesos.

Todo sistema de gestión debe tener como base el modelo que es denominado “P-H-V-A” que involucra a los siguientes principios básicos: Planificar, Hacer, Verificar y Actuar. Los mismos deben ser considerados para contribuir con la mejora continua en todo proceso. En la siguiente imagen se identifican los mismos:

Esquema N° 8: Principios básicos de un sistema de gestión (P-H-V-A)



Fuente: ISO 9.001[59]

Cada uno de los principios incluye las siguientes características:

Tabla N° 7: Detalle de los principios básicos.
Planificar: se relaciona con el establecimiento de políticas, objetivos, procesos y procedimientos con el fin de entregar resultados acordes con las políticas y objetivos globales de una organización.
Hacer: se relaciona con la implementación y gestión de la política, los controles, procesos y procedimientos del sistema.
Verificar: significa medir el desempeño del proceso contra la política y los objetivos planteados y reportar los resultados a la dirección, para su revisión.
Actuar: implica emprender acciones preventivas o correctivas teniendo en cuenta los resultados de la auditoría, sistema de gestión, la revisión por la dirección, u otra información relevante, para lograr la mejora continua.
Fuente: ISO/IEC 27.001[60]

Estas normas, contribuyen a ***los Sistemas Contables:***

- Contiene los requisitos generales y los requisitos para gestionar la documentación empresaria.
- Establecen requisitos que debe cumplir la dirección de la organización, tales como definir la política, asegurar que las

[59] Véase referencia bibliográfica N° [25].
[60] Véase referencia bibliográfica N° [26].

responsabilidades y autoridades estén definidas, aprobar objetivos etc.

- Análisis y mejora continua de los procesos y procedimientos.
- Permiten la implantación de otras normas ISO.

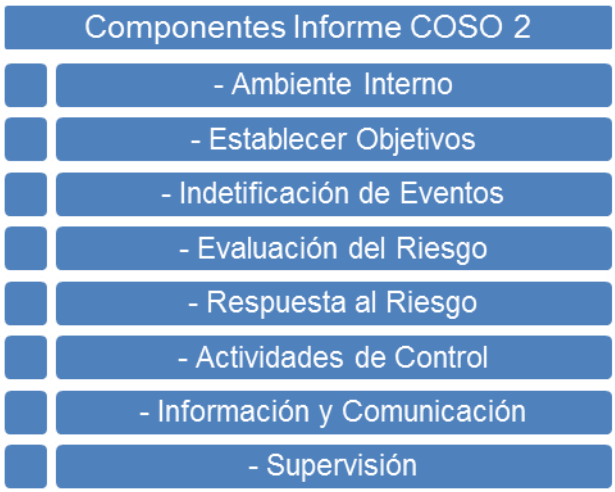
En la presente sección se analizan las cuestiones fundamentales a tener en cuenta al establecer un sistema de gestión según las buenas prácticas generalmente aceptadas y su vinculación con los niveles de decisión en las organizaciones.

6.4. Análisis de la estructura del control interno organizacional.

En el campo del ejercicio profesional existe un marco de referencia denominado "Informe COSO"[61], en el cual se define al control interno, "como un proceso efectuado por la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de los objetivos dentro de las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y normas"[62]

Esquema N° 9: Informe COSO 2.



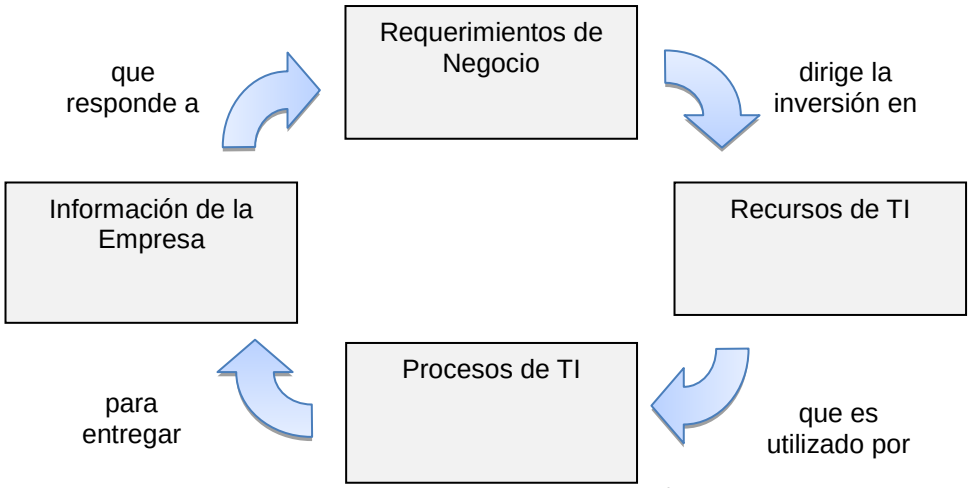
Fuente: Informe COSO 2.[63]

[61] Véase referencia bibliográfica N° [27]
[62] Véase referencia bibliográfica N° [28]
[63] Véase referencia bibliográfica N° [27]

6.5. Para gestionar los procesos de TI.

Objetivos de Control para Información y Tecnologías Relacionadas[64] (COBIT), es un marco de trabajo y un conjunto de herramientas de Gobierno de Tecnología de Información (TI) que permite a la gerencia cerrar la brecha entre los requerimientos de control, aspectos técnicos y riesgos de negocios. COBIT habilita el desarrollo de políticas claras y buenas prácticas para el control de TI en todas las áreas de la organización.

Esquema N° 10: Principio básico de COBIT



Fuente: IT Governance Institute[65]

6.6. Para el análisis de las transacciones de la tarjeta de pago:

Las Normas de Seguridad de Datos (DSS) de la Industria de Tarjetas de Pago (PCI) se desarrollaron para fomentar y mejorar la seguridad de los datos del titular de la tarjeta y para facilitar la adopción de medidas de seguridad consistentes a nivel mundial.

Las PCI DSS constituyen un conjunto mínimo de requisitos para proteger datos de titulares de tarjetas y se pueden mejorar con el uso de controles y prácticas adicionales para mitigar otros riesgos.

[64] Véase referencia bibliográfica N° [29].
[65] Véase referencia bibliográfica N° [29].

6.7. Para gestionar la Seguridad de la Información de Sistemas Contables.

El Sistema de Gestión de Seguridad de la Información es definido como un "Proceso sistemático, documentado y conocido por toda la organización. Y basado en un enfoque por riesgo de negocio, el SGSI es un modelo para el establecimiento, implementación, operación, control, revisión, mantenimiento y mejora de la seguridad de la información."[66]

Enfocado en este concepto, la norma ISO/IEC 27.001 brinda un modelo para el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de un SGSI. La misma establece los siguientes 11 dominios a tener en cuenta para implantar en la Gestión de la Seguridad:

Cuadro N° 9: Dominios de la ISO/IEC 27.001	
Aspectos cubiertos por la norma ISO/IEC 27.001	1. Política de Seguridad.
	2. Organización de Seguridad de la Información.
	3. Administración de Activos.
	4. Gestión de Recursos Humanos.
	5. Seguridad Física y Ambiental.
	6. Gestión de operaciones y comunicaciones.
	7. Control de Acceso.
	8. Adquisición, Desarrollo y Mantenimiento de sistemas.
	9. Gestión de incidentes.
	10. Administración de la Continuidad de los Negocios.
	11. Cumplimiento de la normativa Legal Vigente.
Fuente: ISO/IEC 27.001	

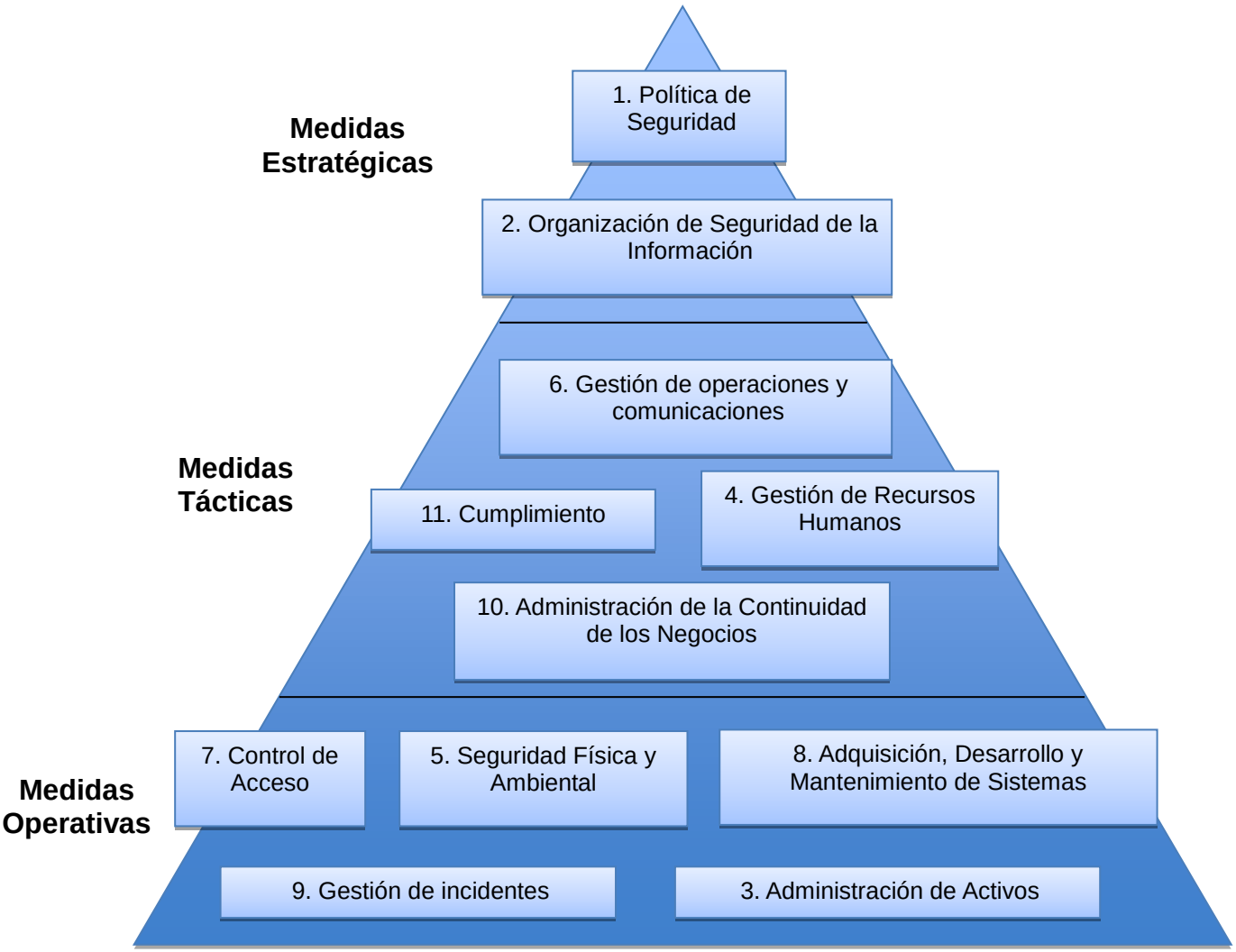
El autor destaca que cada uno de los aspectos cubiertos corresponde a características en los sistemas de gestión de la seguridad que no se

[66] Véase referencia bibliográfica N° [26].

encuentran exclusivamente relacionados con términos tecnológicos, ya que en la administración de la seguridad se necesita redactar políticas estratégicas, normas, procedimientos, inventarios de activos de información y hasta establecer controles a los procesos en los entes.

Teniendo en cuenta estos principios, se los pueden relacionar con las diferentes decisiones y funciones tomadas en los niveles de la organización, en los cuales se pueden subdividir en decisiones estratégicas, tácticas y operativas.

Esquema N° 11: Niveles organizacionales y los dominios establecidos por la ISO/IEC 27.001.



Fuente: ISO/IEC/IRAM 27.001[67]

[67] Véase referencia bibliográfica N° [26].

6.8. Síntesis del capítulo VI.

Como se analizó en los capítulos anteriores, las normas establecidas por la IGJ, 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 buenas prácticas y estándares para contribuir a una eficiente administración de los sistemas en las organizaciones; entre los que destacan:

- COBIT 5
- PCI-DSS
- ISO 9001
- Informe COSO
- ISO/IEC/IRAM 27001

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

En la imagen Nº3 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.

Esquema N° 12: El sistema de Información Contable y las Normas de Seguridad de la Información.

Fuente: Elaboración propia.

De las mencionadas, la ISO/IEC/IRAM 27.001 establece un Marco Normativo con los requisitos fundamentales para implementar un sistema de Gestión de Seguridad de la Información, definiendo el objetivo del SGSI como el de “establecer, implementar, operar, supervisar, revisar, mantener y mejorar” un sistema de seguridad de la información.

Para la implementación del mismo resulta necesaria la gestión, implantación de los procesos, procedimientos, documentación, conocimiento de los objetivos y requisitos para el procesamiento de la información que una organización ha desarrollado para el apoyo a sus operaciones y actividades económicas.

Para la formación del Contador Público, resulta necesario considerar estos marcos normativos para ser incorporados en los conocimientos del contador.

- Capítulo VII

7. IDENTIFICACIÓN DE LOS REQUERIMIENTOS ACTUALES DE FORMACIÓN DEL CONTADOR PÚBLICO.

7.1. Introducción.

En el presente capítulo se analizan los contenidos mínimos de Tecnología y Seguridad de la Información que los contadores deberían ser capacitados para cumplir con los requerimientos actuales del sistema de información contable.

7.2. Recomendaciones de instituciones mundiales.

En octubre de 2013, La Asociación Interamericana de Contabilidad (AIC) emitió una recomendación para "crear conciencia en la profesión contable de participar activamente en la definición de políticas relativas con la seguridad de la información"[68] en donde se destaca con carácter de urgente para la profesión contable "la identificación de los activos de información considerando los posibles riesgos asociados como parte de una adecuada administración de los mismos."[69]

En el ámbito nacional, el Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales (CODECE), emitió un documento base para la acreditación de la carrera de Contador Público[70], en donde se incluyeron dentro de las áreas temáticas y contenidos curriculares mínimos los siguientes temas para ser considerado por las universidades,

[68] Véase referencia bibliográfica N° [30].
[69] Véase referencia bibliográfica N° [30].
[70] Véase referencia bibliográfica N° [31].

incluyendo a la Seguridad de los sistemas:

- Sistemas Administrativos.
- Conceptualización y clasificación de modelos.
- Caracterización y elementos constitutivos.
- Teoría General de los Sistemas.
- Metodología para los estudios administrativos.
- Desarrollo de las etapas para el estudio de sistemas e implementación.
- Aspectos tecnológicos de los medios de procesamiento y comunicaciones.
- Software de base y utilitarios.
- Redes.
- Evaluación de sistemas aplicativos.
- Seguridad en los sistemas de información.

7.3. Recomendaciones en el ámbito profesional y académico profesional.

En el ámbito de la Facultad de Ciencias Económicas, en el Centro de Modelos Contables, se vienen desarrollando diferentes proyectos financiados UBACyT[71] y FONCyT[72], en donde se analizan y se plantean las incumbencias del profesional en Ciencias Económicas ante las Nuevas Tecnologías de Información y Comunicación.

Asimismo, en el ámbito del Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires, se publican informes de la Comisión de Estudios sobre Sistemas de Registros, su integridad y

[71] "Los UBACyT son proyectos de investigación acreditados y financiados por la UBA que tienen como fin realizar una contribución real al conocimiento del tema investigado y contribuir a la formación de investigadores." Definición publicada en la página institucional de la UBA. Véase referencia bibliográfica N° [36].

[72] "La Agencia Nacional de Promoción Científica y Tecnológica (ANPCyT) apoya, a través del Fondo para la Investigación Científica y Tecnológica (FonCyT), proyectos de investigación cuya finalidad sea la generación de nuevos conocimientos científicos y tecnológicos." Véase referencia bibliográfica N° [37].

autenticidad documental, en los cuales se plantea la problemática actual de los sistemas de registros informatizados.

7.4. Abordaje de contenidos.

Considerando los contenidos programáticos de Tecnología y Seguridad de la información para cumplir con la legal forma de los sistemas contables, se encuentra lo dispuesto en:

- El Código Civil y Comercial de la Nación,
- La Ley General de Sociedades,
- Las Resoluciones de la Inspección General de Justicia,
- La Ley de Habeas Data, y
- Las Disposiciones de la Dirección de Protección de Datos Personales.

Como también, estándares y marcos de gestión enfocados en:

- Gestión de los Procesos y Tecnología de la Información,
- Administración de Proyectos de Tecnología de la Información,
- Gestión de Riesgos,
- Gestión de la Seguridad de la Información y
- Gestión de la Continuidad del Negocio.
- Control Interno.

Para cada uno de los temas, existen marcos de gestión en los cuales se pueden impartir los conocimientos elementales analizados en el capítulo anterior: ISO 9001, COBIT, PCI-DSS, Informe COSO, ISO/IEC 27001 y PMBOK. El autor considera que por la diversidad de temas no deben impartirse con profundidad, sino que debe darse a conocer la herramienta, para qué resultaría útil su aplicación y por qué debería ser considerada para el Contador Público.

7.5. Propuestas a considerar discutidas en el ámbito universitario argentino.

En diferentes foros y jornadas se manifestaron diferentes ideas acerca de la forma de encarar la asignatura Tecnología de la Información. Existe una corriente extremista que propone eliminar la asignatura de los programas y que las demás asignaturas absorban los contenidos correspondientes en relación con la Tecnología de Información. Otra corriente indica que los contenidos conceptuales de la asignatura estén orientados en conocimientos de técnicos de hardware e incluyan prácticas de software de gestión como SAP u Oracle, pero estos conceptos no son los apropiados para llegar a entender los requerimientos de los diferentes sistemas contables en relación a la normativa vigente.

En este plano, la primera corriente considera que los temas relacionados de la asignatura deben impartirse en el resto de las asignaturas, dado que la tecnología es transversal a la currícula del contador.

La otra corriente considera que la asignatura debe enfocarse en las competencias de los alumnos con software del mercado, pero ambas propuestas no resultan integrales según los requerimientos que la sociedad requiere. Dado que en todas las asignaturas no se pueden impartir los contenidos dictados en la misma, ya que requeriría la formación y capacitación de los docentes para presentar a los alumnos los conceptos teórico-técnicos de los conceptos tecnológicos asociados a los contenidos, ni tampoco dictar clases de un software de gestión vigente.

En el próximo capítulo, se plantearán las características y contenidos que deberían contener la asignatura analizada.

- Capítulo VIII

8. FORMACIÓN DEL CONTADOR PÚBLICO EN LA GESTIÓN Y CONTROL DE LOS SISTEMAS DE INFORMACIÓN. ESBOZO DE UNA PROPUESTA CURRICULAR SUPERADORA.

8.1. Introducción.

En el presente capítulo se planteará en base a los programas de tecnología de la información de la Universidad de Buenos Aires y la Universidad del Salvador, los contenidos que deberían agregarse para cubrir las necesidades mínimas que requerirían los contadores públicos en materia de Seguridad de la información.

8.2. Fundamentación del cambio curricular.

La información en todas sus formas se ha convertido en unos de los intangibles más importantes en las organizaciones. Junto con los sistemas, esta información impacta transversalmente en los procesos administrativos y por ende en toda la organización.

El avance de estas tecnologías, comprenden un campo de conocimiento que no es ajeno a la formación de los contadores, y resulta fundamental para una adecuada gestión, control y análisis de operaciones y procesos administrativos – contable de una organización. En este contexto, los procesos generan una dependencia hacia la tecnología al ser soporte de los mismos y requiere ser interpretada en su conjunto por los profesionales en Ciencias Económicas, y en especial el Contador Público ya que por sus incumbencias está involucrado entre otras cuestiones, “hacer fe pública en

relación” a:

- Elaboración e implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo–contable.
- Revisión de contabilidades y su documentación.
- Organización contable de todo tipo de entes.
- Aplicación e implantación de sistemas de procesamiento de datos y otros métodos en los aspectos contables y financieros del proceso de información gerencial.

Los contenidos indicados en su conjunto, plantean brindarle al alumno una visión actual y futura de la tecnología y seguridad de información en los procesos de negocio y en el sistema de información contable, para las responsabilidades actuales y desafíos futuros del egresado.

8.3. Objetivos de la reforma curricular.

El objetivo principal de la asignatura es brindar al alumno una visión del impacto de la tecnología en las organizaciones, identificando su implicancia del sistema contable y las incumbencias profesionales del Contador.

Se desprenden los siguientes objetivos particulares:

- Identificar el rol de Contador Público en la administración de la Tecnología de la Información en los entes.
- Reconocer los aspectos fundamentales de infraestructura de hardware, fundamentos de software y bases de datos.
- Determinar y reconocer el impacto de los diferentes sistemas de información que apoyan la toma de decisiones en las organizaciones.
- Obtener, adquirir e identificar las mejores prácticas en la planificación y gestión de los recursos informáticos.
- Adquirir la visión estratégica en la vinculación de la tecnología de la

información y los procesos de negocio.

- Adquirir los conceptos básicos para la administración de proyectos de tecnología de la información.

- Identificar la repercusión de las redes sociales, el comercio electrónico y el pago electrónico en los procesos administrativo-contables.

- Comprender los principales aspectos de la planificación, desarrollo y evaluación de los sistemas de información.

- Identificar la problemática del cumplimento legal, ético y de responsabilidad social en el empleo de las tecnologías de información.

- Entender la problemática del resguardo la información personal, laboral y empresarial en la era de la información.

- Identificar y adquirir las herramientas necesarias para analizar los requisitos de la legalidad del sistema de registros contables en contexto tecnológico.

- Definir e identificar las herramientas necesarias en la Gestión de Riesgos, Seguridad de la Información, Continuidad del Negocio, Control y Auditoría de los procesos críticos de la información contable.

8.4. Ejes principales de la reforma.

Para el desarrollo de los todos los conceptos integrados, el autor propone agrupar los contenidos en los siguientes ejes principales:

Módulo I: Cuestiones Fundamentales de la Tecnología de Información.
Módulo II: Administración de los Recursos Informáticos.
Módulo III: Ética, seguridad y control de la Información.

Para abarcar los contenidos mínimos de “Tecnología y Seguridad de la Información” para Contadores Públicos y cumplir con los requerimientos del mercado, resulta necesario impartir los siguientes conceptos:

El sistema de Información Contable en Contexto Tecnológico

- Sistema de Registros contables: Conceptualización. Características. Legal

Forma. Su vinculación con otros sistemas organizacionales.

- Digitalización del Libro Diario e Inventario y Balances. Implicancias legales. Código Civil y Comercial de la Nación.
- Sistemas de Información Contables en soportes tecnológicos. Principios del derecho contable. Características. Riesgos planteados por el derecho contable a los Sistemas de Registros.
- Normativa aplicable: Disposiciones de la Inspección General de Justicia de la Ciudad Autónoma de Buenos Aires. Requisitos, inscripción e informes a presentar por el Contador Público. Mejores prácticas a implementar para garantizar su cumplimiento. Resguardo de Documentación Respaldatoria.

Gestión de los Sistemas de Información y Gobierno de TI

- Gobierno de Tecnología de la Información. Sistemas de Gestión de Servicios de Tecnología de la Información. La Tecnología de información como un servicio.
- Recomendaciones de la Federación Internacional de Contadores (IFAC).
- Marcos Normativos y Mejores prácticas aplicables. Marcos de Control COSO y Objetivos de Control para Información y Tecnologías Relacionadas (COBIT).
- El fenómeno de la desconexión. Miopía Tecnológica. Responsabilidades de la dirección, los usuarios y del área de IT.

Gestión de Proyectos

- Concepto. Caracterización de la Administración de Proyectos Informáticos. Roles involucrados.
- Etapas del ciclo de vida de la administración de un proyecto. Factores críticos para el éxito. Administración de Riesgos en los Proyectos.
- Soluciones tecnológicas aplicadas a la administración de los Proyectos Informáticos.

Comercio Electrónico y Redes Sociales

- Canales Electrónicos de Pago. Nuevas herramientas y consideraciones. Fraudes en Canales Electrónicos. Normas PCI-DSS: Tarjetas de pago.

- Redes Sociales. Tipos. Fundamentos. Categorías.
- Gestión estratégica de las Redes Sociales. El rol del Administrador de contenidos e imágenes digitales corporativas.

Aspectos Legales y Normativos de la Tecnología

- Delitos y Abusos Informáticos. Características en la República Argentina. El Rol del Contador Público en Pericias en soportes tecnológicos.
- Responsabilidad de las organizaciones para con sus colaboradores. Efectos en la salud por la utilización de tecnologías informáticas. Enfermedades asociadas con la actividad.
- Convenios de confidencialidad. Gestión del departamento de Recursos Humanos.

Ley de Protección de Datos Personales

- Ley de Habeas Data en la Argentina. Repercusiones en el Sistema de Información Contable. Disposiciones Generales de la Dirección Nacional de Protección de Datos Personales. Niveles de Seguridad.

Impactos de la Contabilidad en Computación en la Nube y XBRL

- Implicancias del Sistema Contable en la Nube. Administración de los sistemas de Información en la Nube. Repercusiones Legales en la Argentina.
- XBRL Lenguaje extensible de informes de negocios (eXtensible Business Reporting Language). Conceptos fundamentales. Utilización en el mundo y en la República Argentina.

Fundamentos Criptográficos

- Historia de la Criptografía. Clasificación. Criptografía simétrica vs asimétrica. Criptografía Simétrica. Características. Diferencias entre DES, 3DES y AES.
- Firma Electrónica y Digital. Fundamentos legales y tecnológicos. Ley de Firma Digital en la República Argentina.
- Función de Hash. Características en la gestión de documentos.

Gestión de los Riesgos y Continuidad del Negocio

- Conceptualización de Riesgo. Análisis de probabilidad e impacto. Riesgo residual y salvaguardas.
- Implementación de un Sistema de Gestión de Riesgos. Normas ISO e IRAM aplicables.
- Análisis del Impacto en el Negocio (BIA). Planes de contingencia y continuidad de las operaciones del negocio. Planes de Recuperación ante desastres.
- Implementación de un Sistema de Gestión de Continuidad de Negocio. Normas ISO e IRAM relacionadas.

Gestión de la Seguridad de la Información

- Principios de la Seguridad de la Información. Su relación con otras disciplinas. Seguridad de la Información Vs Seguridad Informática.
- Implementación de un Sistema de Gestión de Seguridad de la Información. Elementos y dominios. Normas ISO e IRAM aplicables.
- Implementación de buenas prácticas en las empresas. Su relación con la Gestión de Riesgos de Tecnología de la Información e impacto en el Sistema de Registros Contables.
- Concepto de Código Malicioso. Tipos de virus informáticos. Cuidados en Internet. Herramientas a implementar.

8.5. Programa y competencias a adquirir por los educandos.

Con el objetivo de una administración adecuada y progresiva de los ejes centrales, en el anexo A de la presente tesis se plantea la distribución de las diferentes actividades y las competencias a adquirir por los educandos.

Conclusiones Finales

- Conclusiones Finales del Trabajo.

Para el desarrollo de la investigación de la presente tesis se planteó la siguiente hipótesis: “Para dar cumplimiento a las exigencias normativas en los Sistemas Contables en soporte tecnológico, se necesitan incorporar contenidos de Tecnología y Seguridad de la Información en la carrera del Contador Público”.

Sobre esta base y para encarar el objeto de análisis acorde al alcance propuesto en la misma, se desarrollaron los siguientes ejes:

- El análisis de la Ley de Incumbencias Profesionales en Ciencias Económicas, el Marco Legal y Normativo de los Organismos de Control del sistema contable en un Contexto Tecnológico.
- La vinculación de la Contabilidad con la Tecnología y Seguridad de la Información, como base teórica para la identificación de las mejores prácticas y estándares en los sistemas contables en las organizaciones.
- El planteo de los requerimientos actuales del Contador Público y una propuesta curricular superadora para la asignatura Tecnología de la Información.

A continuación, se plasman las reflexiones más relevantes analizadas desde la perspectiva de la contabilidad, teniendo presente los diversos cuerpos normativos vigentes en el ámbito de la Ciudad Autónoma de Buenos Aires.

LA INFORMACIÓN Y LA FORMACIÓN DEL CONTADOR PÚBLICO

Para que un sistema de información contable en un soporte tecnológico sea considerado de legal forma, debe cumplir con numerosos requisitos teóricos y tecnológicos de Seguridad de la Información establecidos en leyes, decretos, resoluciones y disposiciones de los organismos de control.

En este contexto, resulta necesario definir cuáles de estos conceptos específicos deben ser incluidos en la formación académica para que el Contador Público egresado pueda cumplir con los mismos.

Como se indicó en el cuerpo introductorio, el CODECE en su documento base para la acreditación de la carrera de Contador Público ha definido que “el objeto de su profesión es la "información" en todas sus formas, sea la misma generada dentro de las organizaciones, interactuando éstas entre sí o en su vinculación con el contexto”. Y si las organizaciones consideran que la información es uno de los activos intangibles de mayor valor en su patrimonio, deberían impartirse los conceptos claves para que los educandos universitarios aprehendan los conocimientos y prácticas que le permitan protegerla.

ANÁLISIS DEL MARCO NORMATIVO

- ✓ **Ley de Incumbencias Profesionales en Ciencias Económicas.**

En el artículo número 13, la Ley número 20.488 establece que se requerirá el título de Contador Público o equivalente “en materia económica y contable cuando los dictámenes sirvan a fines judiciales, administrativos o estén destinados a hacer fe pública en relación con las siguientes cuestiones: (…) “implantación de políticas, sistemas, métodos y procedimientos de trabajo administrativo – contable (…)”[73]. Partiendo de la base que en la actualidad se han desarrollado mejores prácticas y modelos

[73] Véase referencia bibliográfica N° [5].

de gestión que abarcan por ejemplo, las normas ISO, terminan impactando en los Sistemas de Información Contables y en dónde el contador puede contribuir en la planificación, gestión y control de diferentes sistemas administrativos.

En esta línea, algunas comisiones de Consejo Profesional en Ciencias Económicas de la Ciudad de Buenos Aires, como la de Sistemas de Registros[74], plantean la necesidad que los profesionales podrían, (haciendo las especializaciones correspondientes) implantar estándares de sistemas de gestión y liderar a las auditorías sobre las normas ISO, independientemente de la legal forma.

Para lo cual se necesitaría un profesional con una visión integral de estos temas, además de lo expuesto, para cumplir con el alcance de las incumbencias profesionales del Contador Público.

- ✓ **Marco legal y garantías planteadas a nivel doctrinario para los sistemas contables en soporte tecnológico.**

La ley General de Sociedades en el artículo número 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.[75]

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

c. Trascripción del sistema en el libro de inventarios y balances.

d. Tomar las medidas necesarias para garantizar la inviolabilidad, verosimilitud y completitud 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

[74] Sistemas de Registros, Integridad y Autenticidad documental. CPCECABA.
[75] En la Ciudad Autónoma de Buenos Aires corresponde a la Inspección General de Justicia.

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.

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

Como ya se ha mencionado en el capítulo número 3, la Inspección General de Justicia mediante la Resolución General número 7 de 2015 dispone los trámites necesarios para autorizar e implementar sistemas contables en soporte magnético.

Este organismo 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 Ley de Protección de datos personales plantea que 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 más relevantes a considerar en la administración de la seguridad en los sistemas contables son la Nº 11 de 2006, en donde se establecen medidas de seguridad de nivel básico, medio y crítico, y la disposición número 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.

LA CONTABILIDAD, MEJORES PRÁCTICAS Y ESTÁNDARES DE CONTROL DE SEGURIDAD DE SISTEMAS DE INFORMACIÓN DE LA ORGANIZACIÓN

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 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 la concientización del personal.

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

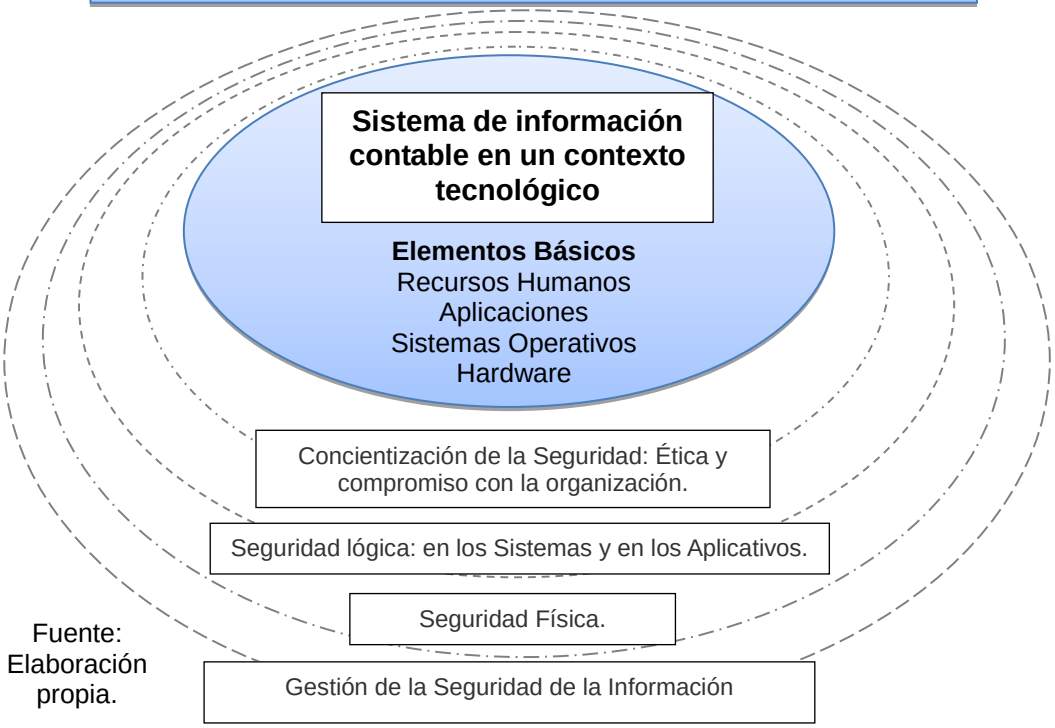
La Contabilidad como disciplina recibe influencias de numerosas ciencias y técnicas que le aportan diversas cuestiones para cumplir con sus fines específicos. Teniendo en cuenta los requisitos básicos de la seguridad de la información: integridad, confidencialidad y disponibilidad, se puede trazar una estrecha vinculación con lo establecido en el Marco Conceptual de Información Contable de la RT N°16 del CPCECABA[76], ya que aporta considerablemente una mejora en los atributos de la información destinada a los usuarios de los Estados Contables.

[76] CPCECABA: Consejo Profesional de Ciencias Económicas de la Ciudad Autónoma de Buenos Aires.

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 cumplimiento de los requisitos planteados para la información contable.

El siguiente esquema se plantean los elementos y los contenidos relacionados con la seguridad de la información.

Esquema N° 13: Elementos del sistema de Información Contable y la Seguridad de la Información.



Fuente: Elaboración propia.

- ✓ **Mejores prácticas y estándares.**

Considerando cómo las normas establecidas por la IGJ y la DNPDP impactan en el funcionamiento del sistema de información contable y en el cumplimiento de la legislación vigente, es recomendable la implementación de buenas prácticas y estándares para contribuir a una eficiente administración de los sistemas en las organizaciones. Los más relevantes y aplicables al sistema contable son:

- ISO 9001 e ISO/IEC/IRAM 27001

- COBIT 5
- PCI-DSS
- Informe COSO

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 prescinda de los beneficios que esta brinda. Nos hemos referido a cada uno de ellos en los capítulos precedentes.

REQUERIMIENTOS ACTUALES DEL CONTADOR PÚBLICO Y CONTENIDOS A INCORPORAR.

Considerando los contenidos programáticos de Tecnología y Seguridad de la información para cumplir con la legal forma de los sistemas contables, se encuentra lo dispuesto en:

- El Código Civil y Comercial de la Nación,
- La Ley General de Sociedades,
- Las Resoluciones de la Inspección General de Justicia,
- La Ley de Habeas Data, y
- Las Disposiciones de la Dirección de Protección de Datos Personales.

Se identifican los siguientes, estándares y marcos de gestión enfocados en los requerimientos conceptuales que debe impartirse en la formación del contador:

- Gestión de los Procesos y Tecnología de la Información,
- Administración de Proyectos de Tecnología de la Información,
- Gestión de Riesgos,
- Gestión de la Seguridad de la Información,

- Gestión de la Continuidad del Negocio, y
- Control Interno.

Para abarcar los contenidos mínimos de Tecnología y Seguridad de la Información para Contadores Públicos, resulta necesario la incorporación de los siguientes conceptos:

- **El sistema de Información Contable en Contexto Tecnológico**
- **Gestión de los Sistemas de Información y Gobierno de TI**
- **Gestión de Proyectos de Tecnología de la Información**
- **Comercio Electrónico y Redes Sociales**
- **Aspectos Legales y Normativos de la Tecnología**
- **Ley de Protección de Datos Personales**
- **Impactos de la Contabilidad en Computación en la Nube y XBRL**
- **Fundamentos Criptográficos**
- **Gestión de los Riesgos y Continuidad del Negocio**
- **Gestión de la Seguridad de la Información**

Sobre esta base, se plantea:

- La necesidad de reconsiderar el plan de carrera del Contador Público actual y los contenidos impartidos sobre “Tecnología de la Información”.
- Articular los conocimientos y contenidos relevantes a los que el Contador Público necesitará conocer en el ejercicio de la profesión.
- Incorporar a la currícula, los contenidos en Tecnología y Seguridad de la Información sobre la necesidad de la legal forma y el cumplimiento normativo emitido por los organismos de control.

Por todo lo expuesto se acepta la hipótesis planteada en la presente tesis. Los contenidos curriculares necesarios recomendados para actualizar y completar la formación del Profesional en Ciencias Económicas en materia de Tecnología y Seguridad de la Información se exponen, en sus ejes fundamentales en estas conclusiones y se completan luego con un desarrollo detallado en el Anexo B que figura a continuación.

El autor se ha concentrado en poner énfasis, y fundamentar los contenidos necesarios para cubrir los requerimientos de conocimientos específicos. Deja a consideración de la Comisión Curricular que debe actuar a los efectos de la reforma del Plan de Estudios, la evaluación de alternativas y la determinación de su distribución entre las asignaturas.

La variedad y extensión de los contenidos propuestos como necesarios no podrían desarrollarse, con los alcances recomendados, en una única asignatura de régimen cuatrimestral.

Por razones metodológicas y de alcance, la presente investigación se desarrolló, como ya ha sido indicado en la introducción, dentro del ámbito de la Ciudad Autónoma de Buenos Aires. Sin embargo la validez de la propuesta es extensible a todos los planes de estudio de profesionales en Ciencias Económicas de las distintas Facultades del país.

Por la razón indicada, los profesores examinadores de la misma recomiendan que, no solamente se ponga en conocimiento de las autoridades académicas de la Facultad de Ciencias Económicas de la Universidad de Buenos Aires, sino se arbitren los medios como para divulgarla entre las distintas universidades nacionales del país.

Consideramos, salvo mejor opinión, que sería una contribución adicional importante como aporte para acelerar el proceso de adecuación de la formación curricular de los futuros profesionales en Ciencias Económicas en los conocimientos sobre Tecnología y Seguridad de la Información que se han definido y fundamentado en la presente tesis.

Anexos

- Anexo A: Características de la propuesta de programa.

PROGRAMA

Contenidos:	Tecnología y Seguridad de la Información.

1. CICLO:

Básico		**Superior/Profesional**	**X**

2. COMPETENCIAS A ADQUIRIR EN TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN:

- ***ESPECÍFICAS***

CE01 - Identificar la contribución de los profesionales en Ciencias Económicas y en especial la del Contador Público en los sistemas de información.
CE02 - Entender la organización bajo el criterio de la Teoría General de los Sistemas.
CE03 - Plantear ejemplos de los componentes de los sistemas de información del mundo real, demostrando fácilmente los distintos elementos de un sistema de información y su relación con los procesos de negocio.
CE04 - Identificar los principales tipos y usos de sistemas de microcomputadoras, computadoras de rango medio, las grandes computadoras centrales y computación en la nube en las organizaciones.
CE05 - Resumir e identificar las principales tecnologías y los usos de los periféricos de cómputo para entrada, salida y almacenamiento.
CE06 - Determinar los sistemas informáticos y los periféricos que en una primera instancia recomendaría para un negocio, y explicar las razones de la elección.
CE07 - Reconocer los diferentes desarrollos y tendencias más importantes en la industria, tecnologías y las aplicaciones de negocio de las telecomunicaciones y de las tecnologías de Internet.
CE08 - Proporcionar ejemplos del valor de negocio de las aplicaciones de Internet, intranet y extranet.
CE09 - Explicar las funciones de los principales tipos de hardware, software,

medios y servicios de redes de telecomunicaciones y su relación con un sistema de información contable en un contexto tecnológico.
CE10 - Reconocer y plantear ejemplos de los principales tipos de software de aplicaciones y de sistemas.
CE11 - Identificar el propósito de algunos paquetes populares de software para la productividad y la computación colaborativa de los usuarios finales.
CE12 - Destacar las funciones del sistema operativo y su impacto en las actividades.
CE13 - Describir los principales usos del software, de las herramientas y de los lenguajes de programación informáticos.
CE14 - Explicar el valor de negocio de implementar procesos y tecnologías de administración de recursos de datos en una organización.
CE15 - Ejemplificar cada uno de los siguientes conceptos existentes en un sistema de registros contables: a) Tipos principales de bases de datos. b) Almacenes de datos y minería de datos. c) Elementos lógicos de datos. d) Estructuras fundamentales de base de datos. e) Desarrollo de bases de datos.
CE16 - Identificar la estructura de computación en la nube y ejemplificar como impacta en los procesos de negocio.
CE17 - Explicar el concepto de sistema de apoyo a la toma de decisiones y cómo difiere de los sistemas tradicionales de información administrativa.
CE18 - Destacar cómo los siguientes sistemas de información apoyan las necesidades de información de ejecutivos, administradores y profesionales de negocios: a) Sistemas ejecutivos de información b) Portales de información empresarial c) Sistemas de administración del conocimiento.
CE19 - Plantear ejemplos de las diversas formas en que los sistemas expertos se utilizan en situaciones de toma de decisiones empresariales. Y ejemplificar la manera en que la reingeniería de los procesos de negocio con frecuencia implica el uso estratégico de las tecnologías de Internet.
CE20 - Identificar el valor de negocio de utilizar las tecnologías de Internet para convertirse en un competidor ágil o para formar una empresa virtual.
CE21 - Explicar cómo los sistemas de administración del conocimiento pueden ayudar a un negocio a obtener ventajas estratégicas.
CE22 - Analizar la función de la planeación en el uso empresarial de la tecnología de información, utilizando como ejemplos el enfoque de escenarios y la planeación para lograr una ventaja competitiva.
CE23 - Analizar la función de la planeación y de los modelos de negocio en el desarrollo de estrategias, arquitecturas y aplicaciones de negocio/TI.
CE24 - Identificar varias soluciones de administración del cambio para la resistencia del usuario final a la implantación de nuevas estrategias y aplicaciones de negocio basadas en TI.
CE25 - Identificar cada uno de los componentes de la administración de la tecnología de información y utilizar ejemplos para mostrar cómo podrían implementarse en una empresa.
CE26 - Explicar cómo se pueden reducir las fallas en la administración de la TI mediante la participación de administradores de negocios en la planeación y administración de la TI.
CE27 - Identificar varias consideraciones que afectan la selección de aplicaciones de TI, plataformas de TI, políticas de acceso a datos y métodos de desarrollo de sistemas de una empresa global de negocios.

CE28 - Interpretar los marcos de gestión COBIT e Informe COSO en las organizaciones y su impacto en el sistema de información contable.
CE29 - Identificar la metodología de administración de proyectos y utilizar software a nivel de operador para gestionar proyectos.
CE30 - Identificar las principales categorías y tendencias de las aplicaciones del comercio electrónico.
CE31 - Identificar y dar ejemplos de varios factores clave y requisitos de tienda en la red necesarios para tener éxito en el comercio electrónico.
CE32 - Concientizar sobre las medidas básicas de seguridad a operar en canales electrónicos con el objetivo de minimizar los riesgos asociados al uso.
CE33 - Identificar riesgos y la salvaguardas a implementar en la utilización de los canales electrónicos en base a las normas PCI-DSS Tarjetas de Pago y su cumplimiento en el sistema de registros contables.
CE34 - Describir y dar ejemplos para mostrar cómo podría utilizar cada uno de los pasos del ciclo de desarrollo de sistemas de información e implementar un sistema de información empresarial.
CE35 - Identificar las actividades que participan en la implantación de nuevos sistemas de información.
CE36 - Describir diversos factores de evaluación que deben considerarse al evaluar la adquisición del hardware, software y servicios de sistemas de información.
CE37 - Identificar varias soluciones de administración del cambio para vencer la resistencia del usuario final a la implantación de nuevos sistemas de información.
CE40 - Identificar varios tipos de estrategias y defensas de administración de la seguridad y explicar cómo se pueden utilizar para garantizar la seguridad de las aplicaciones empresariales de la tecnología de información.
CE41 - Identificar el impacto de la Ley de datos personales en el Sistema de Información Contable.
CE42 - Reconocer e identificar los pasos para registrar las Bases de Datos existentes en el sistema de información contable en la Dirección Nacional de Protección de Datos personales.
CE43 - Identificar los diferentes métodos de resguardo de la información sensible del ente.
CE44 - Aplicar el uso de la Firma Digital y Firma Electrónica en las organizaciones.
CE45 - Interpretar un balance emitido en formato Lenguaje eXtensible de Informes de Negocios (eXtensible Business Reporting Language).
CE46 - Identificar y definir los principales riesgos de los procesos y tecnologías en las organizaciones.
CE47 - Reconocer la importancia de implementar un Sistema de Gestión de Riesgos y Continuidad operativa del Negocio.
CE48 - Definir y diferenciar la Seguridad de la Información y la Seguridad Informática e identificar las principales amenazas y vulnerabilidades del código malicioso.
CE49 - Implementar los pasos de un sistema de Gestión de Seguridad de Seguridad de la Información.
CE50 - Identificar los principales pasos en la auditoría de Sistemas y su vinculación en la emisión de los estados contables.

- ***TRANSVERSALES***

CT01 - Explicar con ejemplos concretos cómo las aplicaciones de negocio de los sistemas de información pueden apoyar los procesos de negocio de una empresa, la toma ejecutiva de decisiones y las estrategias para lograr una ventaja competitiva.
CT02 - Identificar los principales desafíos a los que un gerente se puede enfrentar a la hora de administrar el uso de la tecnología de información de manera exitosa y ética en su empresa.
CT03 - Identificar y dar ejemplos para mostrar los siguientes aspectos de los sistemas de administración de las relaciones con los clientes, de administración de recursos empresariales y de administración de la cadena de suministro. a) Procesos de negocio que soportan b) Valor proporcionado al cliente y al negocio c) Retos y tendencias potenciales
CT04 - Identificar los cambios que ocurren en la forma y el uso del apoyo a la toma de decisiones en los negocios.
CT06 - Identificar la función y las alternativas de generación de reportes de los sistemas de información administrativa.
CT07 - Identificar varios retos culturales, políticos y geoeconómicos que enfrentan los administradores en la administración de las tecnologías de información globales.
CT08 - Explicar el efecto de la tendencia hacia una estrategia de negocios transnacional en la estrategia global de negocio/TI de organizaciones de negocios internacionales.
CT09 - Identificar algunas estrategias competitivas básicas, y explicar cómo pueden utilizar las tecnologías de información para confrontar las fuerzas competitivas a las que se enfrenta un negocio.
CT10 - Identificar algunos usos estratégicos de las tecnologías de Internet y dar ejemplos de cómo proporcionan ventajas competitivas a un negocio.
CT11 - Evaluar financieramente proyectos de TI en base la metodología "Costo total de propietario".
CT12 - Identificar los procesos esenciales de un sistema de comercio electrónico y dar ejemplos de cómo se implementan en las aplicaciones del comercio electrónico.
CT13 - Identificar varios aspectos éticos sobre cómo el uso de tecnologías de información en los negocios afecta el empleo, la individualidad, las condiciones laborales, la confidencialidad, el crimen, la salud y las soluciones a problemas sociales.
CT14 - Identificar la normativa legal vigente para considerar de legal forma el sistema de información contable en contexto tecnológico.
CT15 - Identificar y explicar el valor de negocio de diversos tipos de mercados de comercio electrónico.
CT14 - Identificar mejores prácticas de las Normas ISO e IRAM en la gestión de procesos y tecnologías de la información.
CT16 - Proponer varias formas en que los administradores y profesionales de negocios pueden ayudar a reducir los efectos perjudiciales y aumentar los efectos benéficos del uso de tecnología de información.
CT17 - Implementar las medidas necesarias para que un sistema de

información contable informatizado sea considerado de legal forma en la República Argentina.
CT18 - Identificar las implicancias para el Contador Público en la República Argentina de la ley estadounidense Sarbanes Oxley.

3. BIBLIOGRAFÍA

AFIP (Argentina). (2011), Resolución General N° 1361 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información. Infoleg accedido desde www.infoleg.gov.ar el 24 de marzo de 2016.

AFIP (Argentina). (2011), Resolución General N° 1415 (AFIP), Régimen de Emisión de Comprobantes, Registración de Operaciones e Información. Accedido desde www.infoleg.gov.ar el 28 de marzo de 2016.

AFIP (Argentina). (2011), Resolución General N° 2484. Accedido desde www.infoleg.gov.ar el 24 de marzo de 2016.

AFIP (Argentina). (2011), Resolución General N° 2485, Emisión y almacenamiento electrónico de comprobantes originales. Accedido desde www.infoleg.gov.ar el 24 de marzo de 2016.

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

Asociación Interamericana de Contabilidad. (2013), XXX Conferencia Interamericana de Contabilidad, Uruguay 2013. "Conclusión y recomendaciones", Área 9 – Sistemas y Tecnología de la Información. Accedido de http://www.contadores-aic.org/

Brihuega Arboledas, D. (2014), "BackTrack 5, Hacking de Redes inalámbricas." Aflaomega Ra-Ma, México.

Burgos, A. (2009), "Seguridad, Proteja sus datos y privacidad", Editorial Users, Buenos Aires.

Cano Martinez, J. (2009), "Computación Forense, descubriendo los rastros informáticos"; Aflaomeda Ra-Ma, México.

Chalupowicz, D. G. (2006), "Responsabilidad Corporativa, informe COSO: la ley Sarbanes Oxley". Auditoría Interna y externa. 2ra. Edición. Buenos Aires.

Committee of Sponsoring Organizations of the Treadway Commission – COSO. (2013), Internal Control – Integraded Framework. Edición digital - mayo 2013.

Congreso de la Nación. (2015), Código Civil y Comercial de la República Argentina, Boletín Oficial de la República Argentina, Buenos Aires.

Congreso de la Nación. (2015), Ley N° 19950, Ley General de Sociedades, Boletín Oficial de la República Argentina Buenos Aires.

Congreso de la Nación. (2000), Ley N° 25326, Ley de Habeas Data, Boletín oficial de la República Argentina, Buenos Aires.

CPCECABA, Congreso Metropolitano 60° Aniversario del C.P. C.E.C.A.B.A. Material de Expositores, accesible desde www.consejo.arg.ar

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

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

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

Escobar, D. S. (2014), “Gestión de mejoras prácticas y estándares de control y tecnologías en los sistemas contables”, ASOCIACIÓN INTERAMERICANA DE CONTABILIDAD”, Comisión Técnica de Sistemas y Tecnologías de Información, Charla Cibernética. Octubre 2014.

Escobar, D. S. (2010), “Aportes de la Ley de Protección de datos personales en el Sistema de Información Contable. Nuevos conocimientos del Contador Público en la era de la información.” 18º Congreso Nacional de Profesionales en Ciencias Económicas”, Ciudad Autónoma de Buenos Aires.

Escobar, D. S. (2014), “El Sistema de Gestión de Seguridad de la Información y las incumbencias profesionales del Contador Público.” Área: Actualización de contenidos programáticos. XXXV Simposio Nacional de Profesores de Práctica Profesional.

Escobar, D. S. (2014), “Implicancias legales de la Firma Digital y Electrónica en el resguardo de documentación respaldatoria y registros contables.” Presentado en la VII Jornada Nacional de Derecho Contable, Junio de 2014, Consejo Profesional de Ciencias Económicas de Santa Fe, Ciudad de Rosario.

Federación Argentina de Consejos Profesionales en Ciencias Económicas. (2011), Marco Conceptual - RT 16. Buenos Aires.

Fowler Newton E. (2009), “Planes de Cuentas y Manuales de Procedimientos Contables”, Editorial La Ley, Buenos Aires.

Fowler Newton, E. (1982), “Organización de Sistemas Contables, Ediciones Contabilidad Moderna SAIC Buenos Aires.

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

Fronti de García, L. (1968), “La Formación del Contador Público en la UBA”, Tesis Doctoral. Facultad de Ciencias Económicas, Universidad de Buenos Aires. Accedida desde www.economicas.uba.ar.

García Casella C. L. y Rodríguez de Ramírez M. C. (2001), “Elementos para una Teoría General de la Contabilidad”, Buenos Aires.

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

Gómez López, J. y otros. (2010), “Administración Avanzada de los sistemas informáticos”; Aflaomeda Ra-Ma, México.

Gómez Vieites, A., Suarez Rey, C. (2007). “Sistemas de Información. Herramientas prácticas para la gestión empresarial”. 2da Edición. Editorial Alfaomega.

Gómez Vieites, A. (2011), “Enciclopedia de la Seguridad Informática”, 2da edición. Alfaomega Ra-Ma, México.

Inspección General de Justicia. (2014), Resoluciones Generales. Accedidas desde www.Infoleg.com.ar 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. (2015), Resolución General N° 7 de 2015. Boletín Oficial de la República Argentina.

Instituto Autónomo de Derecho Contable, IADECO (2011) “Nuevos Aportes al Derecho Contable”, Libro de Ponencias, Editorial Errepar, Buenos Aires.

International Auditing Practices Committee (of the International Federation of Accountants). (2001), “Electronic Commerce Using the Internet or Other Public Networks – Effect on the Audit of Financial Statements”. Exposure Draft. New.

International Organization for Standardization - International Electrotechnical Commission. (2013), ISO/IEC 27.001 Information technology - Security techniques - Information security management systems – Requirements. Edición Digital.

International Organization for Standardization - International Electrotechnical Commission. (2005), ISO/IEC 20.001 Gestión de servicios de TI (Tecnologías de la Información).

International Organization for Standardization (2008), ISO 9001 Sets out the requirements of a quality management system. Edición Digital.

Katz, M. (2013), “Redes y Seguridad”, Aflaomega, México.

LAUDON, K, y LAUDON, J. (2012) "Sistemas de Información Gerencial", Editorial. Prentice Hall, Hispanoamericana, México.

Marshall B. Romney, P. Steinbart J. (2012); “Accounting Information Systems”, 12th Edition, New Jersey.

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

Oz Effy. (2008). “Administración de los Sistemas de Información”. 5ta Edición. Editorial Thomson Learning. México.

Pastor J. S., Bessana G. A. e Iglesias S. G. (2010), “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.

Popritkin Alfredo R., (2001), “Fraudes y Libros Contables”, Editorial La Ley, Buenos Aires.

Portantier Fabián, (2012), “Seguridad Informática”, RedUsers. Buenos Aires.

Sallis E., Caracciolo C., y Rodríguez M. (2010), “Ethical Hacking, Un enfoque metodológico para profesionales”, Editorial Alfaomega. Buenos Aires.

Saroka, R. (2002), “Sistemas de Información en la era de digital”, Fundación Osde. Buenos Aires.

Scolnik, H. (2014), “¿Qué es la seguridad informática?”, Editorial PAIDOS, Buenos Aires.

Security Standards Council LLC, (2013), (PCI-DSS) “Normas de seguridad de datos, Requisitos y procedimientos de evaluación de seguridad”, Industria de Tarjetas de Pago (PCI), Versión 3, accedido desde www.pcisecuritystandards.org

Silberschatz Abraham, Korth Henry F., Sudarshan S. Fundamentos de Bases de Datos. 5ta. Edición. Editorial Mc Graw-Hill. Año 2006.

Spina, C E.; (2008), “Factura Electrónica”, 2 edición, Osmar D. Buyatti Librería Editorial, Buenos Aires.

Stallings, W. (2004), “Comunicaciones y Redes de Computadores”. 7ma Edición. Editorial Pearson Prentice Hall.

Stallings, W. (2006), “Organización y arquitectura de computadores”. 7ma Edición. Editorial Pearson Prentice Hall.

Stallings, W. (2005), “Sistemas Operativos”, 5ta Edición. Editorial Pearson Prentice Hall.

Stallings, W. (2010), “Cryptography and Security Network, Principles and Practices”, Pearson Education.

Suarez Kimura E. y Escobar, D. S. (2010). “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.

Suarez Kimura, E. B., Escobar, D. S. y De Franceschi, R. L. (2014), “El rol del profesional en Ciencias Económicas en la planificación estratégica de las tecnologías de información”. XXXVI Simposio Nacional de Profesores de Práctica Profesional. Facultad de Ciencias Económicas. Universidad Argentina de la Empresa. Pinamar.

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

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

Tricoci Guillermo A. (2005). La Sociedad del Conocimiento. Amenazas y Oportunidades. Congreso Metropolitano de Ciencias Económicas. Buenos Aires.

Tricoci Guillermo A. y Benvenuto O. (2008). “El impacto de las Industrias Tics y la Sociedad del Conocimiento en la Argentina”. Ediciones Cooperativas. Buenos Aires.

Universidad Notarial Argentina (2000). Instituto de Derecho Comercial, “Condiciones de la legalidad de la contabilidad informática”, Conclusiones generales. Buenos Aires.

- Anexo B: Contenidos programáticos completos de la propuesta.

UNIDADES TEMÁTICAS Y CONTENIDOS

MÓDULO I: CUESTIONES FUNDAMENTALES DE LA TECNOLOGÍA DE INFORMACIÓN

UNIDAD 1: LA TECNOLOGÍA DE LA INFORMACIÓN Y LA INCUMBENCIA PROFESIONAL DEL CONTADOR PÚBLICO

1.1. LA ERA DIGITAL Y LA SOCIEDAD DEL CONOCIMIENTO.
1.1.1 La era digital. Implicancias en otras disciplinas. Concepto de Sistemas de Información. Diferencia entre dato e información.
1.1.2. Teoría general de los sistemas.
1.1.3. Evolución de los sistemas de información en las organizaciones.

1.2. ROL DEL CONTADOR PÚBLICO Y LAS TECNOLOGÍAS DE INFORMACIÓN.
1.2.1. La ley en el ejercicio de la profesión en Ciencias Económicas y sus incumbencias en la gestión de la tecnología.
1.2.1. El rol del Contador Público en: Proyectos de Sistemas de Información, Implementación de Políticas de Sistemas, y como Auditor Interno, Externo o Forense en las organizaciones.

UNIDAD 2: INFRAESTRUCTURA DE LA TECNOLOGÍA DE LA INFORMACION

2.1. TECNOLOGÍA DE LOS COMPUTADORES.

2.1.1. Computadoras: concepto y estructura. Diferencias entre Hardware y Software.

2.1.2. Generaciones de computadoras. Evolución. Su vinculación con la contabilidad.

2.1.3. Clasificación de Computadoras: Sistemas de microcomputadoras, sistemas de rango medio. Sistemas de computadoras centrales (Mainframe).

2.2. ARQUITECTURA DE HARDWARE.

2.1.2. Unidad Central de Procesamiento: componentes, características y funciones.

2.1.3. Memoria principal: características, tipos y funciones. Representación interna de datos.

2.1.4. Dispositivos y medios para la entrada de datos. Dispositivos y medios para almacenamiento externo de datos.

2.3. INFRAESTRUCTURA DE COMUNICACIONES.

2.3.1. Sistemas de Comunicaciones. Concepto, topologías y clasificación.

2.3.2. Redes de comunicaciones. Tipos. Componentes. Medios de transmisión. Procesadores de Comunicaciones.

2.3.3. Conectividad: dispositivos y estándares. IP pública y privada. Protocolo TCP/IP de Internet.

2.3.4. Internet, Intranet y extranet. El uso de Internet en los negocios.

UNIDAD 3: SOFTWARE Y ADMINISTRACIÓN DE DATOS.

3.1. SOFTWARE.

3.1.1. Concepto de Software. La interrelación entre el software y el hardware. Tipos de Software: Firmware, de base y de Aplicación

3.1.2. Esquemas de licenciamiento de software. Software propietario, de Código abierto y gratis.

3.1.3. Sistemas Operativos: concepto, tipos y funciones. Criterios de selección de un sistema operativo. Linux y Sistemas Propietarios.
3.1.4. Lenguajes de programación: concepto, evolución y tipos de lenguajes. Criterios de selección de un lenguaje. Compiladores, intérpretes y entornos.

3.2. RECURSOS DE DATOS.
3.2.1. Bases de Datos: concepto y características. Tipos de archivos tradicionales. Modelado de datos. Tipos y Herramientas de modelado de datos.
3.2.3. Tipos de archivos tradicionales. Métodos de organización y acceso. Archivos tradicionales vs. Bases de datos.
3.2.4. Bases de Datos: concepto y características. Sistema de Administración de Bases de Datos (SABD): concepto y componentes. Tipos de SABD: características, ventajas y desventajas. Lenguajes de definición y consulta.

3.3. COMPUTACIÓN EN LA NUBE
3.3.1 Computación en la nube. Concepto y características. Tipos de infraestructura.
3.3.2. Ventajas y desventajas de su utilización.

MÓDULO II: ADMINISTRACIÓN DE LOS RECURSOS INFORMATICOS

UNIDAD 4: SISTEMAS QUE APOYAN LA TOMA DE DECISIONES DE INFORMACIÓN EN LAS ORGANIZACIONES

4.1. DISTINTOS TIPOS DE SISTEMAS DE INFORMACION.
4.1.1. Sistemas según niveles de la organización: Sistemas de procesamiento de transacciones, Sistemas para la administración táctica o nivel gerencial y Sistemas para la administración estratégica.
4.1.2. Sistemas para distintas funciones organizativas. Sistemas de manufactura y producción. Sistemas de contabilidad y finanzas. Sistemas de Recursos Humanos.

4.1.3. Los sistemas según su aporte a las metas organizacionales. Sistemas de información estratégicos y sistemas para la administración del cambio organizativo.

4.2. DISTINTAS APLICACIONES INFORMATICAS EN LAS ORGANIZACIONES.

4.2.1. La integración de los sistemas de información. Sistemas altamente integrados funcionalmente: planificación de recursos empresariales (ERP), administración de relaciones con clientes (CRM), sistemas de cadena de abastecimiento.

4.2.2. Sistemas para el análisis de información en la toma de decisiones. Sistemas de inteligencia de negocios. Tableros de comando. Minería de datos. Inteligencia de Negocios. Almacenes de Datos.

4.2.3. La integración de recursos humanos y del conocimiento en las organizaciones mediante sistemas de información: sistemas de colaboración empresarial y sistemas de administración del conocimiento.

4.3. GESTIÓN DEL SISTEMA DE INFORMACIÓN CONTABLE.

4.3.1. Sistema de Registros contables: Conceptualización. Características. Su vinculación con otros sistemas organizacionales.

4.3.2. Digitalización del Libro Diario e Inventario y Balances. Implicancias legales. Código Civil y Comercial.

UNIDAD 5: PLANIFICACIÓN Y GESTIÓN DE LOS RECURSOS INFORMÁTICOS

5.1. LOS PROCESOS DE NEGOCIO Y LAS TECNOLOGÍAS DE INFORMACIÓN.

5.1.1. Identificación de los procesos del negocio. Clasificación. Cadena de valor. Impacto de las tecnologías en los procesos.

5.1.2. Relación entre los Procesos de Negocios y los Sistemas de Información. Documentación de los procesos. Cursograma y flujograma de procesos. Normas ISO e IRAM de Calidad aplicables.

5.1.3. Administración de Recursos Informáticos. La Cultura de la Organización y su relación con el uso de las tecnologías de información.

5.2. PLANEAMIENTO ESTRATEGICO DE SISTEMAS DE INFORMACION.

5.2.1. El Rol administrador del Contador Público en los Sistemas de Información y Tecnología de la Información desde una perspectiva estratégica.

5.2.2. La estrategia de negocios y su relación con la estrategia de los Sistemas de Información y de las Tecnologías de la Información.

5.2.3. Métodos y técnicas para el diseño y la puesta en práctica de un plan estratégico de Sistemas de Información. Su relación con los Proyectos de Sistemas. Análisis de Factibilidad. Justificación estratégica, operativa, técnica y económica.

5.3. SISTEMAS DE GESTIÓN Y GOBIERNO DE IT.

5.3.1. Gobierno de Tecnología de la Información. Sistemas de Gestión de Servicios de Tecnología de la Información. La Tecnología de información como un servicio.

5.3.2. Marcos Normativos y Mejores prácticas aplicables. Marcos de Control COSO y Objetivos de Control para Información y Tecnologías Relacionadas (COBIT). La Biblioteca de Infraestructura de Tecnologías de Información, (ITIL).

5.3.3. El fenómeno de la desconexión. Miopía Tecnológica. Responsabilidades de la dirección, los usuarios y del área de IT.

UNIDAD 6: ADMINISTRACION DE PROYECTOS

6.1. GESTIÓN DE PROYECTOS.

6.1.1. Concepto. Caracterización de la Administración de Proyectos Informáticos. Roles involucrados.

6.1.2. Etapas del ciclo de vida de la administración de un proyecto. Factores críticos para el éxito. Administración de Riesgos en los Proyectos.

6.1.3. Soluciones tecnológicas aplicadas a la administración de los Proyectos Informáticos.

6.2. EVALUACION ECONOMICA DE PROYECTOS.

6.2.1. Evaluación económica de proyectos. Evaluación costo - beneficio. Métodos financieros. Otros métodos de evaluación y selección de inversiones.

6.2.2. Componentes de costos. Costo total de propiedad (TCO). Determinación de Beneficios. Beneficios cuantificables y no cuantificables. Beneficios directos e indirectos.
6.2.3. Seguimiento de costos y de obtención de beneficios durante la ejecución. Fijación de metas e indicadores.

UNIDAD 7: REDES SOCIALES, COMERCIO ELECTRÓNICO Y PAGO ELECTRÓNICO

7.1. COMERCIO ELECTRONICO.
7.1.1. Concepto. Fundamentos. Categorías.
7.1.2. Impactos del comercio electrónico. Impactos en el perfil de gestión empresarial. Cambios en los modelos de negocio. Preponderancia del Servicio. Comunidad on-line. Nuevos roles y demandas. Oportunidades profesionales.
7.1.3. Canales Electrónicos de Pago. Nuevas herramientas y consideraciones. Fraudes en Canales Electrónicos. Normas PCI-DSS: Tarjetas de pago.

7.2. REDES SOCIALES.
7.2.1. Concepto de Redes Sociales. Tipos de redes. Fundamentos. Categorías.
7.3.1. Gestión estratégica de las Redes Sociales. El rol del Administrador de contenidos e imágenes digitales corporativas.

UNIDAD 8: PLANIFICIÓN, DESARROLLO Y EVALUACIÓN DE SISTEMAS DE INFORMACIÓN

8.1. EL CICLO DE VIDA DE LOS SISTEMAS DE INFORMACION.
8.1.1. El concepto de Ciclo de Vida de un Sistema de Información. El enfoque de sistemas.
8.1.2. Los requerimientos. Su análisis y definición. Participación de los diferentes sectores de la organización.
8.1.3. Adquisición o Desarrollo. Diferentes alternativas. Ventajas y desventajas en distintos contextos organizacionales.

8.1.4. Implementación. Administración del cambio. Rol del usuario y cultura de la organización. Estrategias y tácticas.

8.2. DESARROLLO.

8.2.1. Etapas genéricas del proceso de desarrollo. Concepto de cada fase, los productos a obtener y el rol de los usuarios.

8.2.2. Modelos de Desarrollo de Sistemas. Características. Ventajas y Desventajas.

8.2.3. Métodos Estructurados de Análisis y Diseño. Métodos Orientados a Objetos. Conceptualización. Objetivos y características de los principales artefactos utilizados.

8.2.4. Calidad del software. El valor de la calidad. Estándares en la gestión existentes.

8.3. ADQUISICION.

8.3.1. Adquisición y selección de software. Alternativas. Evaluación del Producto y del Proveedor.

8.3.2. Adquisición y selección de hardware, redes e infraestructura. Controles a realizar. Productos a obtener.

MÓDULO III: ÉTICA, SEGURIDAD Y CONTROL DE LA INFORMACIÓN.

UNIDAD 9: ASPECTOS ÉTICOS Y LEGALES DE LOS SISTEMAS DE INFORMACION

9.1. ETICA Y RESPONSABILIDAD SOCIAL EN EL EMPLEO DE TECNOLOGIAS DE LA INFORMACION.

9.1.1. Aspectos éticos en el manejo de la información y la tecnología.

9.1.2. Responsabilidad de las organizaciones para con sus colaboradores. Efectos en la salud por la utilización de tecnologías informáticas. Enfermedades.

9.1.3. Convenios de confidencialidad. Gestión del departamento de Recursos Humanos.

9.2. ASPECTOS LEGALES Y NORMATIVOS.

9.2.1. Propiedad intelectual. Derecho de Autor y Derechos conexos. Patentes. Marcas.

9.2.2. Cuestiones jurídicas e impositivas vinculadas al comercio electrónico e Internet en general.

9.2.3. Dominio y privacidad. Identidad. Reglas de registro. Derecho de Privacidad. Derecho al olvido en Internet.

9.2.4. Delitos y Abusos Informáticos. Características en la República Argentina. El Rol del Contador Público en Pericias en soportes y tecnológicos.

9.3. HABEAS DATA Y EL SISTEMA CONTABLE.

9.3.1. Ley de Habeas Data en la Argentina. Repercusiones en el Sistema de Información Contable.

9.3.2. La Dirección Nacional de Protección de Datos Personales. Disposiciones Generales. Niveles de Seguridad.

UNIDAD 10: CONTABILIDAD INFORMATIZADA

10.1. SISTEMAS DE INFORMACIÓN CONTABLES.

10.1.1. Sistemas de Información Contables en soportes tecnológicos. Principios del derecho contable. Características.

10.1.2. Riesgos planteados por el derecho de los Sistemas de Registros.

10.2. NORMATIVA APLICABLE.

10.2.1. Disposiciones de la Inspección General de Justicia de la Ciudad Autónoma de Buenos Aires. Requisitos, inscripción e informes a presentar por el Contador Público.

10.2.2. Mejores prácticas a implementar para garantizar su cumplimiento. Resguardo de Documentación Respaldatoria. Administración Federal de Ingresos Públicos.

10.3. IMPACTOS ACTUALES Y FUTUROS DE LA CONTABILIDAD Y LA TECNOLOGÍA.

10.3.1. Implicancias de la Contabilidad en la Nube. Administración de los sistemas de Información en la NUBE. Repercusiones Legales en la Argentina.
10.3.2. XBRL - Lenguaje eXtensible de Informes de Negocios (eXtensible Business Reporting Language). Conceptos fundamentales. Utilización en el mundo y en la República Argentina.

UNIDAD 11: CRIPTOGRAFÍA, GESTIÓN DE LOS RIESGOS Y LA SEGURIDAD DE LA INFORMACIÓN.

11.1 FUNDAMENTOS CRIPTOGRÁFICOS
11.1.1. Historia de la Criptografía. Clasificación. Criptografía simétrica vs asimétrica.
11.1.2. Criptografía Simétrica. Características. Diferencias entre DES, 3DES y AES.
11.1.3. Función de Hash. Características en la gestión de documentos.

11.2. FIRMA ELECTRÓNICA Y DIGITAL
11.2.1. Criptografía asimétrica. Características.
11.2.1. Firma Electrónica y Digital. Fundamentos legales y tecnológicos. Ley de Firma Digital en la República Argentina.
11.2.2. Gestión de documentos electrónicos. Componentes del Documento Digital. Uso de Herramientas Criptográficas en Información Respaldatoria Contable.

11.3. GESTIÓN DE RIESGOS.
11.3.1. Conceptualización de Riesgo. Análisis de probabilidad e impacto. Riesgo residual y salvaguardas.
11.3.2. Implementación de un Sistema de Gestión de Riesgos. Normas ISO e IRAM aplicables.

11.4. GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
11.4.1. Características principales y su relación con el negocio.
11.4.3. Análisis del Impacto en el Negocio (BIA). Planes de contingencia y continuidad de las operaciones del negocio. Planes de Recuperación ante desastres.

11.4.3. Implementación de un Sistema de Gestión de Continuidad de Negocio. Normas ISO e IRAM relacionadas.

11.5. GESTION DE LA SEGURIDAD DE LA INFORMACIÓN

11.5.1 Seguridad de la Información Vs Seguridad Informática.

11.5.2. Principios de la Seguridad de la Información. Su relación con otras disciplinas.

11.6. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

11.6.1. Implementación de un Sistema de Gestión de Seguridad de la Información. Elementos y dominios. Normas ISO e IRAM aplicables.

11.6.2. Implementación de buenas prácticas en las empresas. Su relación con la Gestión de Riesgos de Tecnología de la Información e impacto en el Sistema de Registros Contables.

11.7. CÓDIGO MALICIOSO.

11.7.1. Concepto de Código Malicioso. Tipos de virus informáticos.

11.7.2. Cuidados en Internet. Herramientas a implementar.

11.7.3. Resguardo de la Información.

UNIDAD 12: CONTROL Y AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

12.1. ENTORNO DE CONTROL

12.1.1. Creación de un entorno de control. Su justificación económica. Controles generales. Aseguramiento de la calidad. Normas de Control.

12.1.2. Informe COSO. Aplicabilidad. Diferencias entre Informe COSO II.

12.1.1. Controles generales. Herramientas y técnicas para lograr seguridad. Seguridad Física y Lógica.

12.1.2. Controles de las aplicaciones. Controles de entradas, de proceso y de salidas. Impacto de los controles en los procesos de negocio.

12.1.3. Vulnerabilidades y amenazas. Razones de la Vulnerabilidad de un sistema. Impacto de la conectividad. Amenazas. Físicas y Lógicas.

12.2. AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN.

12.2.1. Tipos de auditoría.

12.2.2. Vinculación de la Auditoría de Sistemas y la de Estados Contables.

12.2.3. Ley estadounidense Sarbanes Oxley y su impacto en el Rol del Contador Público.

12.2.4. Nociones de la informática forense. Su vinculación con las actividades del Contador con Perito en la Justicia.

- Anexo C: Modelos de Gestión de la Seguridad de la Información y la Capacitación.

En la actualidad existen varios marcos normativos, estándares, buenas prácticas y bibliografía que contextualiza la capacitación y concientización de la seguridad de la información en la organización. A continuación, se describen los modelos más destacables en relación al tema de investigación.

- **Modelo de Gestión de la Seguridad Informática**

El Modelo de Negocio de Seguridad Informática o "The Business Model for Information Security" (BMIS) fue desarrollado y difundido por la asociación ISACA. La principal característica de este modelo radica en el establecimiento como ejes fundamentales en la gestión de la seguridad a las personas, procesos, tecnologías y organización del ente:

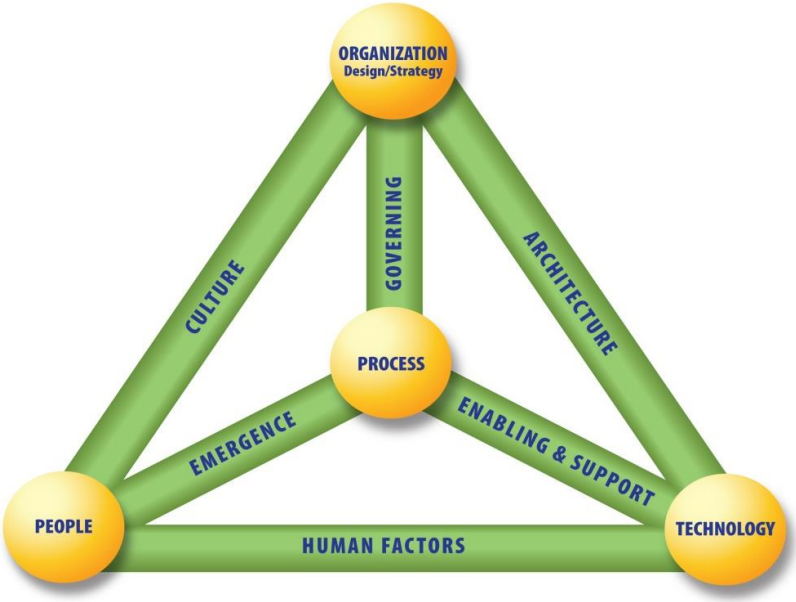


Gráfico Nº1: "The Business Model for Information Security" (BMIS).[77]

[77] Véase referencia bibliográfica N° [32]

Al analizar el mismo se puede destacar el rol que se le da a la Cultura, ya que se establece como una de las aristas del modelo en tanto define la relación entre la organización de la entidad y a las personas, pero este marco solo tiene en cuenta a las personas involucradas internamente en la organización, y no contempla a las externas.

- **Modelo ISO/IEC 27.001**

Por otro lado, la ISO/IEC 27.001 establece los lineamientos para implementar un Sistema de Gestión de la Seguridad de la Información. En el siguiente gráfico se pueden identificar los dominios de la misma y su rol en la organización.

En relación con la concientización y capacitación, desarrolla un punto denominado “Capacitación, conocimiento y capacidad”, en donde se toman en cuenta a todos los usuarios del ente, además de exigir una “Política de Seguridad”, la cual se centra en los principios y el apoyo de la dirección; la “Organización de Seguridad de la Información” que requiere la normalización de los procesos; la capacitación y la “Gestión de operaciones y comunicaciones” que incluye la interna y como también a la externa.

- **COBIT**

COBIT (Objetivos de control para información y tecnologías relacionadas) es una guía de mejores prácticas presentado como Marco normativo, dirigida a la gestión de tecnología de la información (TI). En la misma se establecen principios, dominios, procesos y actividades para el gobierno de TI. En el siguiente gráfico, se puede analizar el “cubo de Cobit” con todos sus elementos:

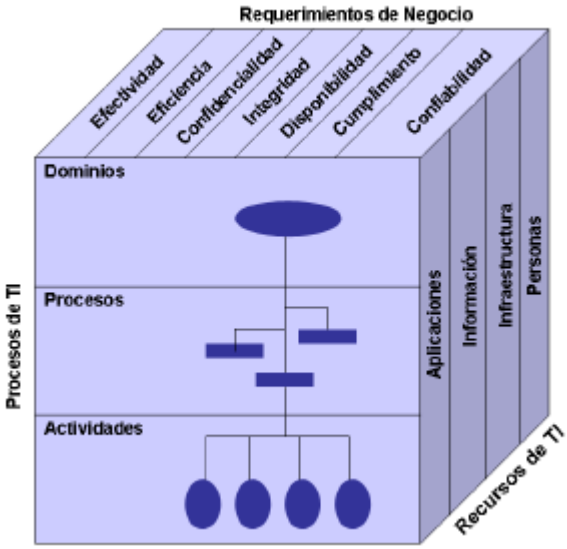


Gráfico Nº2: El Cubo de Cobit.[78]

En relación con la capacitación, el modelo de COBIT 5 establece como pilar fundamental el reforzamiento de la cultura organizacional a la "Culture, Ethics and Behaviour", pero este marco no se orienta exclusivamente a la gestión de la seguridad, sino a la administración de la tecnología en general.

- **Information Security Management Maturity Model (ISM3)**

El modelo de ISM3 (Information Security Management Maturity Model), ofrece un nuevo enfoque de los sistemas de gestión de seguridad de la información orientado exclusivamente a los sistemas de gestión de calidad, ISO 9.001 en las organizaciones.

Si bien es un modelo novedoso, no se orienta exclusivamente a la capacitación, pero, como establece Vicente A. (2010), el modelo "ISM3 proporciona un marco para ISM que puede utilizarse tanto por pequeñas organizaciones que realizan sus primeros esfuerzos, como a un nivel alto de sofisticación por grandes organizaciones como parte de sus procesos de seguridad de la información."

[78] Véase referencia bibliográfica N° [33].

- **Information Security Forum's Standard of Good Practice (SOGP).**

El modelo SOGP "Information Security Forum's Standard of Good Practice" es un marco con buenas prácticas basado en las experiencias del ISF (El Foro de Seguridad de la Información). Este estándar es una guía para la seguridad de la información enfocada exclusivamente en el negocio, la cual se organiza en cuatro categorías principales:

- Gobierno de la seguridad
- Requisitos de seguridad
- Marco de control
- Seguimiento y mejora de la seguridad

En el Foro de Seguridad de la Información (2010), se describe que este “estándar cubre temas como la estrategia de seguridad, la gestión de incidentes, la continuidad del negocio, la capacidad de recuperación y la gestión de crisis”, pero se basa en consejos prácticos para mejorar la capacidad de resistencia de la organización frente a una amplia gama de amenazas y eventos que pueden amenazar el éxito e incluso la supervivencia de la organización.

- **Otras normas.**

Existen otros modelos que analizan indirectamente cuestiones de seguridad. Uno de ellos es el caso de ITIL que tiene muchos puntos de contacto respecto a cuestiones de seguridad. Otra es la norma Prince2, que se orienta en la seguridad relacionada con la gestión de proyectos; también se puede destacar el modelo TLLJO, que se enfoca en la implementación de un SGSI, permitiendo un mayor control sobre el sistema a un precio moderadamente reducido.

Y, por último, el autor de la presente tesina destaca la norma SP800-53 del NIST, que fue tomada como base para la confección de la citada Comunicación A 5374 de BCRA, que establece los lineamientos específicos a cumplir en canales electrónicos en todo tipo de entes.

Bibliografía

- Bibliografía específica.

[01] Instituto Argentino de Derecho Contable (IADECO), “Derecho Contable” [en línea]. Diciembre de 2015. [consultada el 10 de diciembre de 2015]. Disponible en: "http://www.iadeco.org/dercont.htm"

[02] García Casella C. L. y Rodríguez de Ramírez M. C., “Elementos para una Teoría General de la Contabilidad”. [Traducción de: American Accounting Association, 1966, “A Statement of Basic Accounting Theory”.]

[03] Federación Internacional de Contadores (IFAC), “Formas Internacionales de Formación”; 2008, [consultada el 10 de noviembre de 2015]. Disponible en: “http://www.ifac.org/sites/default/files/downloads/ Spanish_Translation_Normas_Internacionales_de_ Formacion_2008.pdf”

[04] Luisa Fronti de García, “La Formación del Contador Público en la UBA”, Tesis Doctoral. 1968. Facultad de Ciencias Económicas, Universidad de Buenos Aires.

[05] Congreso de la Nación Argentina. “Ley N° 20.488. Ley de Incumbencias Profesionales en Ciencias Económicas.” Artículo N° 13 completo: Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

[06] Congreso de la Nación Argentina, “Código Civil y Comercial”, Sección 7ª, Contabilidad y estados contables, Artículo N° 320. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

[07] Congreso de la Nación Argentina, “Código Civil y Comercial”, Sección 7ª, Contabilidad y estados contables, Artículo N° 322. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

[08] Congreso de la Nación Argentina, “Código Civil y Comercial”, Sección 7ª, Contabilidad y estados contables, Artículo N° 323. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

[09] Congreso de la Nación Argentina, “Código Civil y Comercial”, Sección 7ª, Contabilidad y estados contables, Artículo N° 329. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

[10] Congreso de la Nación Argentina, “Ley N° 19950, Ley General de Sociedades”, Artículo N° 61, Boletín Oficial de la República Argentina, agosto de 2015, Buenos Aires.

[11] 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 2015]. Disponible en: http://www.legalmania.com.ar/derecho/contabilidad_informatica.htm

[12] Popritkin A. R., “Fraudes y Libros Contables”, La Ley, Buenos Aires, 2001 p 274.

[13] Universidad Notarial Argentina, Instituto de Derecho Comercial, “Condiciones de la legalidad de la contabilidad informática”, Conclusiones Generales, 8 de junio de 2000.

[14] Inspección General de Justicia. Resolución General N° 7 de 2015. Artículo N° 334. Boletín Oficial de la República Argentina. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

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

[16] Suarez Kimura E. B. 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. Septiembre, 2010. Facultad de Humanidades, Ciencias Sociales y de la Salud, Universidad Nacional de Santiago del Estero.

[17] Ley N° 25326, Ley de Habeas Data, Artículo N° 7, Boletín oficial de la República Argentina, Buenos Aires. 30 de octubre de 2000.

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

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

[20] Gómez López J., Guía de campo de Seguridad Informática, Capítulo I., Alfaomega Grupo Editor, México, 2010, 17 p.

[21] Aldegani G. (2011), “Compliance”. Exposición en la materia: “Gestión Estratégica de la Seguridad Informática II”. 18 de July de 2011. Maestría en Seguridad Informática. Buenos Aires.

[22] García Casella, C. L., “Método Científico para las Investigaciones en General”, Informe presentado en el 1er Encuentro Universitario de Investigaciones del Área Contable, 1995.

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

[24] 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

[25] International Organization for Standardization (2008), ISO 9001 Sets out the requirements of a quality management system. Edición Digital.

[26] International Organization for Standardization - International Electrotechnical Commission. (2013), ISO/IEC 27.001 Information technology - Security techniques - Information security management systems - Requirements. Edición Digital.

[27] Committee of Sponsoring Organizations of the Treadway Commission, COSO, (2013), Internal Control – Integraded Framework. Edición digital. Mayo de 2013.

[28] Instituto de Auditores Internos de Argentina. “Boletín de la Comisión de Normas y Asuntos Profesionales” Nº 9 - septiembre de 2003. Accedido desde https://www.iaia.org.ar/revistas/normaria/Normaria09.pdf

[29] IT Governance Institute, (2013), Objetivos de Control para Información y Tecnologías Relacionadas (COBIT 5, Control Objectives for Information and related Technology). ISACA (Information Systems Audit and Control Association). Accedido desde www.itgi.org

[30] XXX Conferencia Interamericana de Contabilidad, Uruguay 2013. “Conclusión y recomendaciones”, Área 9 – Sistemas y Tecnología de la Información. Accedido de http://www.contadores-aic.org/

[31] Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales (CODECE) (2012), Documento base para la acreditación de la carrera de carrera de Contador Público septiembre 2013.

[32] IT Governance Institute, (2013), Modelo de Gestión de la Seguridad Informática. ISACA (Information Systems Audit and Control Association). Accedido desde www.itgi.org

[33] IT Governance Institute, (2013), Objetivos de Control para Información y Tecnologías Relacionadas (COBIT 5, Control Objectives for Information and related Technology). ISACA (Information Systems Audit and Control Association). Accedido desde www.itgi.org

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

[35] Inspección General de Justicia. Resolución General N° 7 de 2015. Artículo N° 328. Boletín Oficial de la República Argentina. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

[36] Universidad de Buenos Aires. “Programación Científica UBACYT 2014/2017” diciembre de 2015. Accedido desde http://secinves.com.ar/guias/ubacyt

[37] Agencia Nacional de Promoción Científica y Tecnológica. “Fondo para la Investigación Científica y Tecnológica” diciembre de 2015. Accedido desde http://www.agencia.mincyt.gob.ar/frontend/agencia/fondo/foncyt

[38] Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales. “Estatuto” diciembre de 2015. Accedido desde http://www.codece.com.ar/docs/Estatuto01072011.pdf

- Bibliografía general.

Agencia Nacional de Promoción Científica y Tecnológica. “Fondo para la Investigación Científica y Tecnológica” diciembre de 2015. Accedido desde http://www.agencia.mincyt.gob.ar/frontend/agencia/fondo/foncyt

Aldegani G. (2011), “Compliance”. Exposición en la materia: “Gestión Estratégica de la Seguridad Informática II”. 18 de July de 2011. Maestría en Seguridad Informática. Buenos Aires.

American Accounting Association. (1966), “A Statement of Basic Accounting Theory”, AAA.

Asociación Interamericana de Contabilidad. (2013), XXX Conferencia Interamericana de Contabilidad, Uruguay 2013. “Conclusión y recomendaciones”, Área 9 – Sistemas y Tecnología de la Información. Accedido de http://www.contadores-aic.org/

Brihuega Arboledas, D. (2014), “BackTrack 5, Hacking de Redes inalámbricas.” Alfaomega Ra-Ma, México.

Burgos, A. (2009), “Seguridad, Proteja sus datos y privacidad”, Editorial Users, Buenos Aires.

Cano Martinez, J. (2009), “Computación Forense, descubriendo los rastros informáticos”; Alfaomega Ra-Ma, México.

Chalupowicz, D. G. (2006), “Responsabilidad Corporativa, informe COSO: la ley Sarbanes Oxley. Auditoría Interna y externa.” 2da. Edición. Buenos Aires.

Committee of Sponsoring Organizations of the Treadway Commission – COSO. (2013), “Internal Control – Integraded Framework”. Edición digital - Mayo 2013.

Congreso de la Nación Argentina. “Ley N° 20.488. Ley de Incumbencias Profesionales en Ciencias Económicas.” Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

Congreso de la Nación Argentina, “Código Civil y Comercial”, Sección 7ª, Contabilidad y estados contables. Accedido desde www.infoleg.gov.ar el 10 de diciembre de 2015.

Congreso de la Nación Argentina, “Ley N° 19950, Ley General de Sociedades”, Artículo N° 61, Boletín Oficial de la República Argentina, agosto de 2015, Buenos Aires.

Consejo de Decanos de Facultades de Ciencias Económicas de Universidades Nacionales. “Estatuto” diciembre de 2015. Accedido desde http://www.codece.com.ar/docs/Estatuto01072011.pdf

Dirección Nacional de Protección de Datos Personales. (2006), “Disposición N° 11/2006, Medidas de Seguridad”. Buenos Aires, Argentina., 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

Escobar, D. S. (2010), “Aportes de la Ley de Protección de datos personales en el Sistema de Información Contable. Nuevos conocimientos del Contador Público en la era de la información.” 18º Congreso Nacional de Profesionales en Ciencias Económicas”, Ciudad Autónoma de Buenos Aires.

Escobar, D. S. (2010), “Ley de Protección de Datos Personales, Revista Imagen Profesional”, de La Federación Argentina de Consejos Profesionales en Ciencias Económicas. Buenos Aires.

Escobar, D. S. (2013) 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. Facultad de Ciencias Económicas. Universidad de Buenos Aires.

Escobar, D. S. (2014), “El Sistema de Gestión de Seguridad de la Información y las incumbencias profesionales del Contador Público.” Área: Actualización de contenidos programáticos. XXXV Simposio Nacional de Profesores de Práctica Profesional. Concordia.

Escobar, D. S. (2014), “Gestión de mejoras prácticas y estándares de control y tecnologías en los sistemas contables”, Asociación Interamericana de Contabilidad”, octubre 2014.Comisión Técnica de Sistemas y Tecnologías de Información, Charla Cibernética.

Escobar, D. S. (2014), “Implicancias legales de la Firma Digital y Electrónica en el resguardo de documentación respaldatoria y registros contables.” Presentado en la VII JORNADA NACIONAL DE DERECHO CONTABLE, junio de 2014, Consejo Profesional de Ciencias Económicas de Santa Fe, Ciudad de Rosario.

Escobar, D. S. y otros. “Aspectos legales y formales del sistema de registro “Legal Forma”, Comisión de Estudios sobre Sistemas de Registros, su integridad y autenticidad documental, Informe 1, EDICION, Buenos Aires.

Federación Internacional de Contadores (IFAC), “Formas Internacionales de Formación”; 2008, [consultada el 10 de noviembre de 2015]. Disponible en: “http://www.ifac.org/sites/default/files/downloads/Spanish_Translation _Normas _Internacionales_de_ Formacion_2008.pdf”

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

Fowler Newton, E. (1982), “Organización de Sistemas Contables”. Ediciones Contabilidad Moderna. Buenos Aires.

Fowler Newton, E. (2009), “Planes de Cuentas y Manuales de Procedimientos Contables”. Editorial La Ley, Buenos Aires.

Fronti de García, L. (1968), “La Formación del Contador Público en la UBA”, Tesis Doctoral. Facultad de Ciencias Económicas, Universidad de Buenos Aires.

García Casella C. L. y Rodríguez de Ramírez M. C. (2001), “Elementos para una Teoría General de la Contabilidad”, Buenos Aires.

García Casella, C. L. (1995), “Método Científico para las Investigaciones en General”, Informe presentado en el 1er Encuentro Universitario de Investigaciones del Área Contable, Buenos Aires.

Gómez López J. (2010), “Guía de campo de hackers”, Alfaomega Grupo Editor, México.

Gómez López, J. y otros. (2010), “Administración Avanzada de los sistemas informáticos”; Alfaomega Ra-Ma, México.

Gómez Vieites, Á. (2011), “Enciclopedia de la Seguridad Informática”, 2da edición. Alfaomega Ra-Ma, México.

Inspección General de Justicia. (2015), “Resolución General N° 7 de 2015”. Boletín Oficial de la República Argentina, 23 de agosto de 2015.

Instituto Autónomo de Derecho Contable, IADECO. (2011), “Nuevos Aportes al Derecho Contable”, Libro de Ponencias, Editorial Errepar, Buenos Aires.

International Auditing Practices Committee (of the International Federation of Accountants). (2001), “Electronic Commerce Using the Internet or Other Public Networks – Effect on the Audit of Financial Statements”. Exposure Draft. New.

International Organization for Standardization - International Electrotechnical Commission. (2013), “ISO/IEC 27.001 Information technology - Security techniques - Information security management systems – Requirements”. Edición Digital.

International Organization for Standardization - International Electrotechnical Commission. (2005), “ISO/IEC 20.001 Gestión de servicios de TI” (Tecnologías de la Información). Edición Digital.

International Organization for Standardization (2008), “ISO 9001 Sets out the requirements of a quality management system”. Edición Digital.

IT Governance Institute, (2013), “Objetivos de Control para Información y Tecnologías Relacionadas” (COBIT 5, Control Objectives for Information and related Technology). ISACA (Information Systems Audit and Control Association). Accedido desde www.itgi.org

Katz, Matías; (2013), “Redes y Seguridad”, Aflaomega, México.

Laudon, K, y Laudon, J. (2012), "Sistemas de Información Gerencial", Editorial. Prentice Hall, Hispanoamericana, México.

Ley N° 19950, Ley General de Sociedades, Boletín Oficial de la República Argentina Buenos Aires, 2015.

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

Marshall B., Romney, y P, Steinbart J. (2012), “Accounting Information Systems”, 12th Edition, New Jersey.

Molina, J. C., (1999), “Los subdiarios y la obligatoriedad de su rubricación, Impuestos”, LVII-1999-A, Ed. La Ley, p. 1550. Buenos Aires.

Pastor J. S., Bessana G. A. e Iglesias S. G. (2010), “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.

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

Portantier, F. (2012), “Seguridad Informática”, RedUsers. Buenos Aires.

Sallis E., Caracciolo C., y Rodríguez M. (2010), “Ethical Hacking, Un enfoque metodológico para profesionales”, Editorial Alfaomega. Buenos Aires.

Saroka R. (2002), “Sistemas de Información en la era de digital”, Fundación Osde. Buenos Aires.

Scolnik, H. (2014), “¿Qué es la seguridad informática?”, Editorial PAIDOS, Buenos Aires.

Security Standards Council LLC. (2013), (PCI-DSS) “Normas de seguridad de datos, Requisitos y procedimientos de evaluación de seguridad”, Industria de Tarjetas de Pago (PCI), Versión 3, accedido desde www.pcisecuritystandards.org

Sosa, T. E., (1999), “Medios informáticos y el proceso que viene. Validez probatoria y eficiencia procesal”. La Ley, Buenos Aires.

Spina, C. E. (2008), “Factura Electrónica”, 2 edición, Osmar D. Buyatti Librería Editorial, Buenos Aires.

Stallings, W. (2010), “Cryptography and Security Network, Principles and Practices”, Pearson Education.

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

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

Suarez Kimura E. B. y Escobar, D. S. (2010), “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.

Suarez Kimura, E. B., Escobar, D. S. y De Franceschi, R. L. (2014), “El rol del profesional en Ciencias Económicas en la planificación estratégica de las tecnologías de información.”. XXXVI Simposio Nacional de Profesores de Práctica Profesional. Faculta de Ciencias Económicas, UADE. Pinamar.

Universidad de Buenos Aires. “Programación Científica UBACYT 2014/2017” diciembre de 2015. Accedido desde http://secinves.com.ar/guias/ubacyt

Universidad Notarial Argentina, Instituto de Derecho Comercial, (2000), “Condiciones de la legalidad de la contabilidad informática”, Conclusiones generales. Buenos Aires.

- **Documentos Consultados:**

Plan de estudio de la Maestría en Seguridad Informática. Universidad de Buenos Aires.

Plan de estudio de la Carrera de Contador Público. Universidad de Buenos Aires.

Plan de estudio de la Carrera de Contador Público. Universidad del Salvador.

Programa de la asignatura “Tecnología de la Información” de la Facultad de Ciencias Económicas, de la Universidad de Buenos Aires.

Programa de la asignatura “Tecnología de la Información” de la Facultad de Ciencias Económicas, de la Universidad del Salvador.

- Índices específicos

- **Índice de Esquemas**

Esquemas	Páginas
Esquema N° 1: Conceptos impartidos actualmente.	14
Esquema N° 2: Marco Normativo de los Registros Contables en Sociedades Comerciales en la CABA.	18
Esquema Nº 3: Clasificación de Datos Personales.	37
Esquema Nº 4: Niveles de Seguridad.	41
Esquema Nº 5: Aportes de la Seguridad de la Información a la Contabilidad.	49
Esquema N° 6: Disciplinas influyentes en la Contabilidad.	51
Esquema N° 7: Elementos de los sistemas contables.	54
Esquema N°8: Principios básicos de un sistema de gestión (P-H-V-A).	55
Esquema N° 9: Informe COSO 2.	56
Esquema N° 10: Principio básico de COBIT	57
Esquema N° 11: Niveles organizacionales y los dominios establecidos por la ISO/IEC 27.001.	59

Esquema N° 12: El sistema de Información Contable y las Normas de Seguridad de la Información.	61
Esquema N° 13: Elementos del sistema de Información Contable y la Seguridad de la Información.	78

- **Índice de Tablas**

Tablas	Páginas
Tabla N° 1: Riesgos identificados por el Derecho para llevar una contabilidad informatizada.	20
Tabla N° 2: Requisitos de los Sistemas Contables (IGJ).	23
Tabla Nº 3: Medidas de Seguridad del Nivel Básico.	41
Tabla Nº 4: Medidas de Seguridad del Nivel Medio.	43
Tabla Nº 5: Medidas de Seguridad de Nivel Crítico.	44
Tabla N° 6: Requisitos de la Información contenida en los Estados Contables.	48
Tabla N° 7: Detalle de los principios básicos.	55

- **Índice de Gráficos**

Cuadros	Páginas
Gráfico Nº1: “The Business Model for Information Security” (BMIS).	103

Gráfico Nº2: El Cubo de Cobit.	105

- **Índice de Cuadros**

Cuadros	Páginas
Cuadro N° 1: Requisitos de la Seguridad de la Información en el Sistema Contable.	26
Cuadro N° 2: Autorización para empleo de ordenadores (IGJ).	28
Cuadro N° 3: Informes periódicos medios magnéticos u otros. (IGJ).	31
Cuadro Nº 4: Comprobantes y documentación de Comercio.	38
Cuadro Nº 5: Comprobantes Internos.	39
Cuadro Nº 6: Relacionados con los empleados.	39
Cuadro Nº 7: Relacionados con otras personas físicas y jurídicas.	39
Cuadro Nº 8: Elementos del Sistema contable y la Seguridad de la Información.	51
Cuadro N° 9: Dominios de la ISO/IEC 27.001.	58

Universidad de Buenos Aires
Facultad de Ciencias Económicas, Ciencias Exactas y Naturales e Ingeniería
Maestría en Seguridad Informática

Tesis de Maestría

Formación del Contador Público en Tecnología y Seguridad de la Información.
Propuesta de reforma curricular.

Autor: Diego Sebastián Escobar
Director: Elsa Beatriz Suarez Kimura
Co-directora: Romina de Franceschi

Febrero de 2017
Cohorte 2010