XXXVIII SIMPOSIO NACIONAL DE PROFESORES DE PRÁCTICA PROFESIONAL

XXXVIII SIMPOSIO NACIONAL DE PROFESORES DE PRÁCTICA PROFESIONAL

Universidad:
UNIVERSIDAD DE BUENOS AIRES

Título:
FORMACIÓN Y CAPACITACIÓN EN ESTÁNDARES DE CONTROL Y MEJORES PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN LOS REGISTROS CONTABLES. EL DESAFÍO TECNOLÓGICO DEL CONTADOR PÚBLICO EN EL SIGLO XXI.

Autor:
Esp. Diego Sebastián Escobar
(Ayudante de 1ra Regular – Facultad de Ciencias Económicas – Universidad de Buenos Aires y Profesor de Tecnología de la Información – Facultad de Ciencias Económicas y Empresariales – Universidad del Salvador)

UNSTA 50 Años 1965 -2015
Facultad de Economía y Administración

XXXVIII SIMPOSIO NACIONAL DE PROFESORES DE PRÁCTICA PROFESIONAL

Universidad:
UNIVERSIDAD DE BUENOS AIRES

Título:
FORMACIÓN Y CAPACITACIÓN EN ESTÁNDARES DE CONTROL Y MEJORES PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN LOS REGISTROS CONTABLES. EL DESAFÍO TECNOLÓGICO DEL CONTADOR PÚBLICO EN EL SIGLO XXI.

Autor:
Esp. Diego Sebastián Escobar
(Ayudante de 1ra Regular – Facultad de Ciencias Económicas – Universidad de Buenos Aires y Profesor de Tecnología de la Información – Facultad de Ciencias Económicas y Empresariales – Universidad del Salvador)

Resumen

Con el vertiginoso avance de las tecnologías de información y comunicación en las organizaciones resulta imposible ignorar los cambios en los procesos, procedimientos, documentación y soportes en los registros contables. Los archivos en papel que ayer se utilizaban, hoy se encuentran reemplazados por registros en soporte tecnológico que pueden ser: servidores físicos, servidores virtualizados o aplicaciones en la nube.

Asimismo, con las modificaciones surgidas en la unificación del Código Civil y Comercial, en donde se establece que se requiere de un "dictamen técnico de Contador Público" para el cambio de un sistema de registros convencional a uno informatizado, haciendo hincapié en "la inviolabilidad, verosimilitud y completitud del sistema"[1], plantea la necesidad de capacitar a los estudiantes paraidentificar aquellas herramientas, estándares y mejores prácticas para dar respuesta a las necesidades actuales de las organizaciones.

El objetivo del presente trabajo es analizar e identificar aquellos marcos de gestión y buenas prácticas en Tecnología y Seguridad de la información utilizadas para evaluar la inviolabilidad, verosimilitud y completitud de la información contenida en los sistemas de registros contables en un contexto tecnológico.

[1]Nota N° 1: Congreso de la Nación Argentina, 2014, Código Civil y Comercial, Artículo N° 329 - Actos sujetos a autorización.

ÍNDICE TEMÁTICO

FORMACIÓN Y CAPACITACIÓN EN ESTÁNDARES DE CONTROL Y MEJORES PRÁCTICAS DE SEGURIDAD INFORMÁTICA EN LOS REGISTROS CONTABLES. EL DESAFÍO TECNOLÓGICO DEL CONTADOR PÚBLICO EN EL SIGLO XXI

1. INTRODUCCIÓN

Con el vertiginoso avance de las tecnologías de información y comunicación en las organizaciones resulta imposible ignorar los cambios en los procesos, procedimientos, documentación y soportes en los registros contables. Los archivos en papel que ayer se utilizaban, hoy se encuentran reemplazados por registros en soporte tecnológico que pueden ser: servidores físicos, servidores virtualizados o aplicaciones en la nube.

Asimismo, con las modificaciones surgidas en la unificación del Código Civil y Comercial, en donde se establece que se requiere de un "dictamen técnico de Contador Público" para el cambio de un sistema de registros convencional a uno informatizado, haciendo hincapié en "la inviolabilidad, verosimilitud y completitud del sistema"[2], plantea la necesidad de capacitar a los estudiantes para identificar aquellas herramientas, estándares y mejores prácticas para dar respuesta a las necesidades actuales de las organizaciones.

El objetivo del presente trabajo es identificar aquellos marcos de gestión y buenas prácticas en Tecnología y Seguridad de la información utilizadas para evaluar la inviolabilidad, verosimilitud y completitud de la información contenida en los sistemas de registros contables. En la sección N° 1 se analizan los elementos básicos de un sistema contable y enla sección N° 2 se enumeran diferentes marcos de gestión y mejores prácticas para cada uno de los elementos señalados.

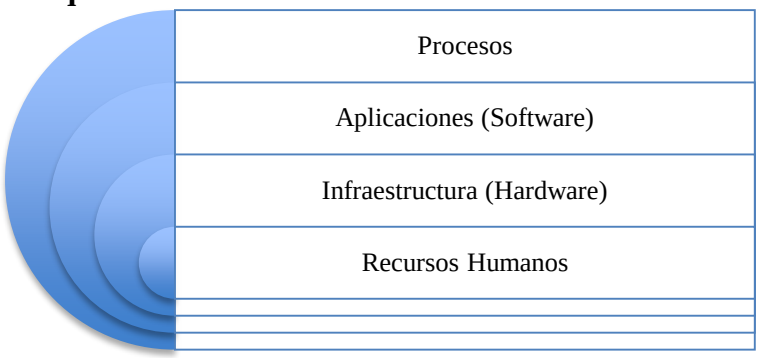
2. INTERRELACIÓN DE LOS ELEMENTOS DEL SISTEMA CONTABLE

Existen diferentes elementos que forman el sistema de información contable, entre los cuales se pueden destacar: 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. Pero resulta fundamental establecer la dependencia y relación entre ellos.

Una vez identificados los elementos, se deberían inventariar 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.

[2]Nota N° 2: Ídem nota N° 1.

Esquema N° 1: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:

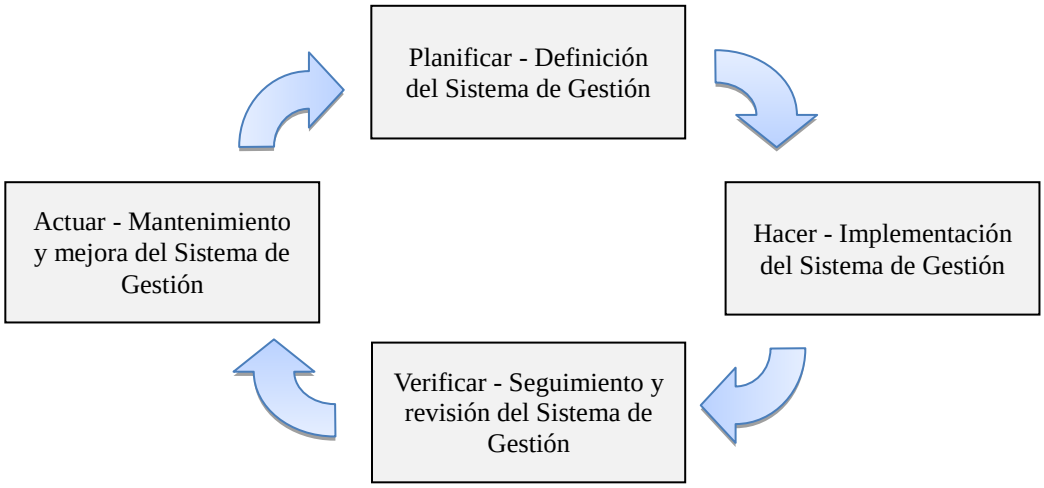
3. MEJORES PRÁCTICAS Y ESTÁNDARES

3.1. 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° 2: Principios básicos de un sistema de gestión (P-H-V-A)



Fuente: ISO 9.001[3]

Cada uno de los principios incluye las siguientes características:

Tabla N° 1: 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[4]

[3]Nota N° 3: International Organization for Standardization (2008), ISO 9001 Sets out the requirements of a quality management system. Edición Digital.

[4]Nota N° 4:International Organization for Standardization - International Electrotechnical Commission. (2013), ISO/IEC 27.001 Information technology - Security techniques - Information security management systems - Requirements. Edición Digital.

Estas normas, contribuyen a los Sistemas Contables ya que:

- 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 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.

3.2.Análisis de la estructura del control interno organizacional.

En el mercado existe el Informe COSO[5] 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"[6]

[5]Nota N° 5:Committee of SponsoringOrganizations of theTreadway Commission, COSO, (2013), Internal Control – Integraded Framework. Edición digital. Mayo de 2013.

[6]Nota N° 6: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

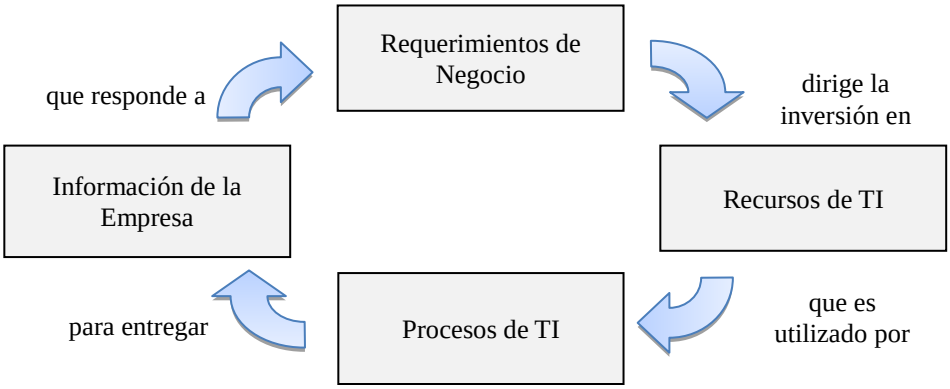
Esquema N° 3: Informe COSO 2.

Fuente: Informe COSO 2.[7]

3.3.Para gestionar los procesos de TI.

Objetivos de Control para Información y Tecnologías Relacionadas[8] (COBIT), es una 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° 4: Principio básico de COBIT



Fuente: IT GovernanceInstitute

[7]Nota N° 7:Ídem nota N° 5.

[8]Nota N° 8:IT GovernanceInstitute, (2013), Objetivos de Control para Información y Tecnologías Relacionadas (COBIT 5, Control Objectives for Information and relatedTechnology). ISACA (InformationSystemsAudit and Control Association). Accedido desde www.itgi.org

3.4.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.

3.5. 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."[9]

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 mínimos a tener en cuenta para implantar en la Gestión de la Seguridad:

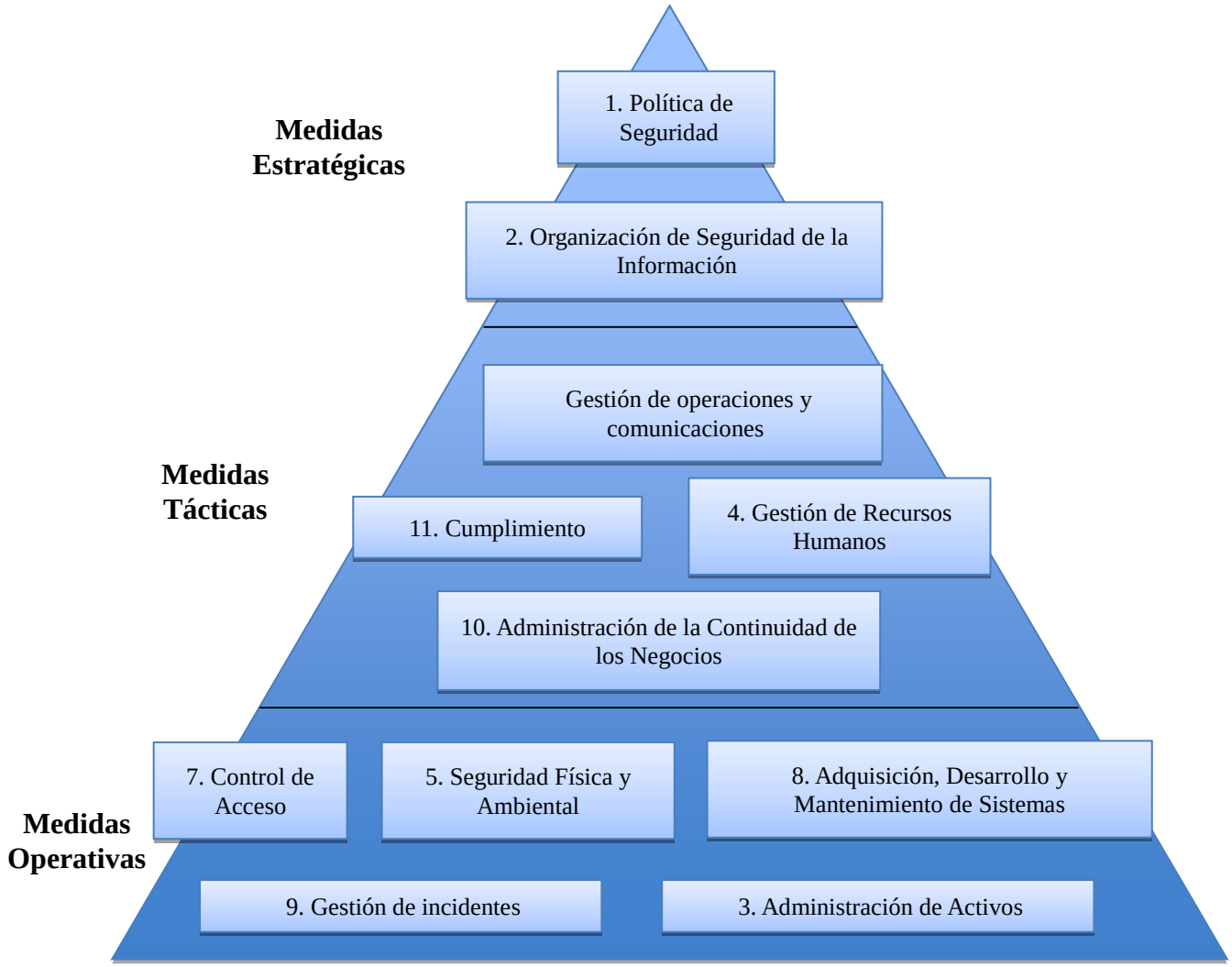
Cuadro N° 1: Dominios de la ISO/IEC 27.001	
Aspectos cubiertos por la norma ISO/IEC 27.001	1. Política de Seguridad.
	2. Organización de Seguridad de la Información.
	3. Administración de Activos.
	4. Gestión de Recursos Humanos.
	5. Seguridad Física y Ambiental.
	Gestión de operaciones y comunicaciones.
	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	

[9]Nota N° 9:International Organization for Standardization - International Electrotechnical Commission. (2013), ISO/IEC 27.001 Information technology - Security techniques - Information security management systems - Requirements. Edición Digital.

El autor destaca que cada uno de los aspectos cubiertos corresponde a características en los sistemas de gestión de la seguridad que no se 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° 5: Niveles organizacionales y los dominios establecidos por la ISO/IEC 27.001.



Fuente: ISO/IEC 27.001

[10]Nota N° 10:Ídem nota N° 9.

4. CONCLUSIONES

Como se indicó precedentemente, la legislación actual impacta en el funcionamiento del sistema de información contable. 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
- 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 el esquema Nº 6 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° 6: 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 contenidos programáticos.

5. BIBLIOGRAFÍAGENERAL

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.

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

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

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. (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 Argentina de Consejos Profesionales en Ciencias Económicas. (2011), Marco Conceptual - RT 1 República Argentina.

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"

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 GovernanceInstitute, (2013), “Objetivos de Control para Información y Tecnologías Relacionadas” (COBIT 5, Control Objectives for Information and relatedTechnology). ISACA (InformationSystemsAudit and Control Association). Accedido desde www.itgi.org

Laudon, K, y Laudon, J. (2012), "Sistemas de Información Gerencial", Editorial. Prentice Hall, Hispanoamericana, 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 A. R. (2001), Fraudes y Libros Contables, La Ley, 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

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. (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., 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.