Temática: Contabilidad y Ciberseguridad

Modelo de Sistema de Gestión de Seguridad de la Información Contable para micro y pequeños entes prestadores de servicios

Palabras clave: Seguridad, Información, Micro ente, Ciberseguridad, SGSE

Diego Sebastián Escobar

Profesor Adjunto interino de Teoría Contable. Facultad de Ciencias Económicas. UBA

Profesor Adjunto de Tecnología de la información. Facultad de Ciencias Económicas y Empresariales. USAL.

1. Introducción

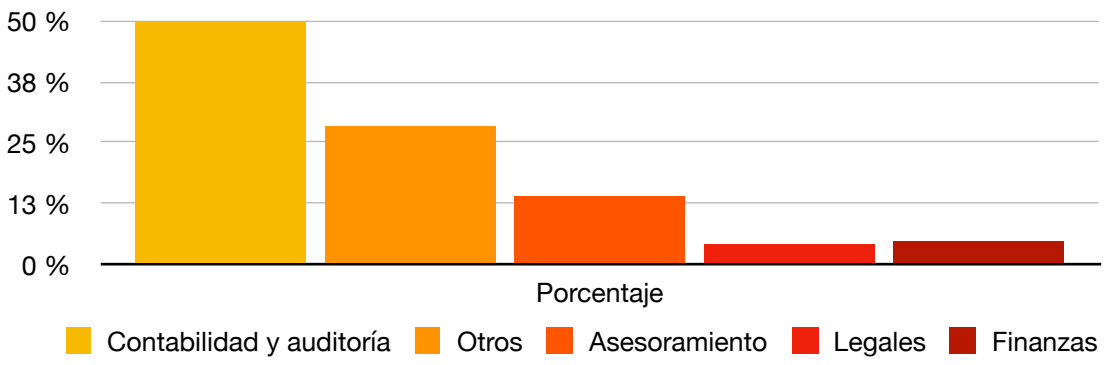
El presente trabajo tiene el objetivo de difundir un modelo de sistema de gestión de seguridad de la información simplificado para micro y pequeños entes prestadores de servicios en el ámbito del Área Metropolitana del Buenos Aires.
En el presente artículo se establecen 3 secciones; en la primera parte se analiza el contexto actual de las micro y pequeñas empresas existentes en el área identificado.
En la segunda sección se identifican los estándares considerados para el desarrollo del modelo propuesto para este tipo de entidades. Y por último, se presenta una síntesis de la propuesta desarrollada para el tipo de entidad objeto de estudio.

2. Síntesis de la situación en la gestión de la seguridad de información en pequeñas empresas de servicios

En esta primera sección se identifica el contexto actual de las micro y pequeñas empresas prestadoras de servicio ubicadas en el AMBA; para ello se realizó un relevamiento de 80 empresas de las cuales se llegaron a las siguientes conclusiones sobre su situación actual en la gestión de la seguridad de la información:

Gráfico N°1: Análisis del rubro económico que desarrollan sus actividades.

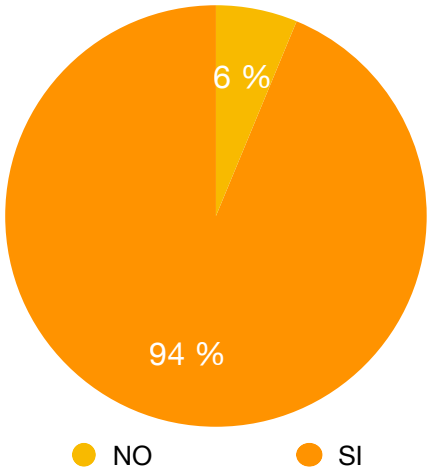
De las empresas relevadas, el 50% corresponden al rubro de contabilidad y auditoría, y el resto a otros tipos de servicio:



Fuente: Elaboración propia.

Gráfico N°2: Sí en el contexto de confinamiento por la pandemia de COVID-19 pudieron desarrollar sus actividades a distancia.

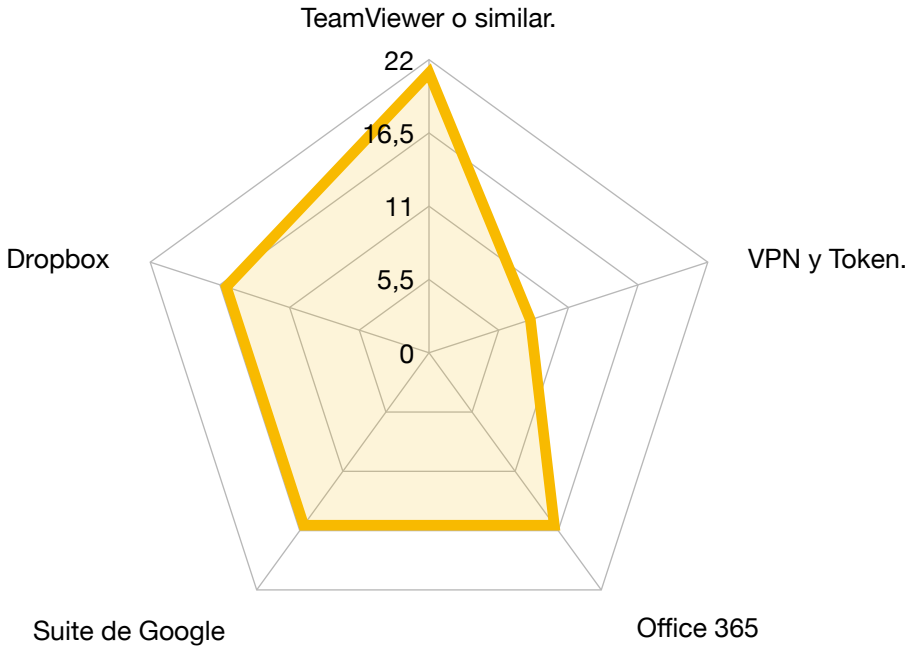
En relación con el contexto de pandemia y confinamiento el 94% de las empresas relevadas pudieron continuar con sus operaciones a distancia:



Fuente: Elaboración propia.

Gráfico N°3: Tipo de tecnologías utilizadas para desarrollar las tareas a distancia.

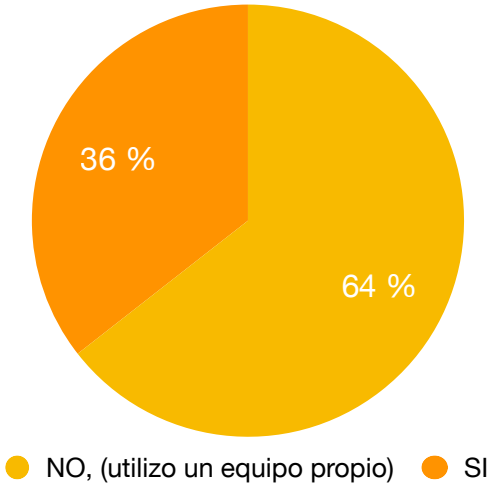
En relación con los tipos de tecnologías utilizados se pueden evidenciar el uso de servicios en la nube y aplicativos colaborativos:



Fuente: Elaboración propia.

Gráfico N°4: Equipos utilizados para el desarrollo de actividades a distancia.

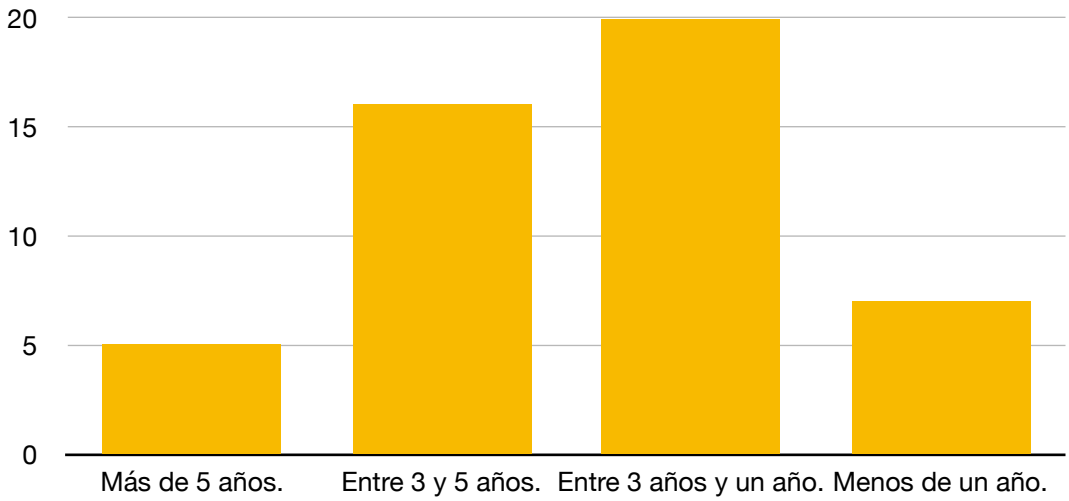
En relación con el desarrollo de las tareas, el 64% los analistas utilizaron equipos propios para desarrollar las tareas:



Fuente: Elaboración propia.

Gráfico N°5: Antigüedad que tienen los equipos informáticos utilizados para las tareas en el confinamiento.

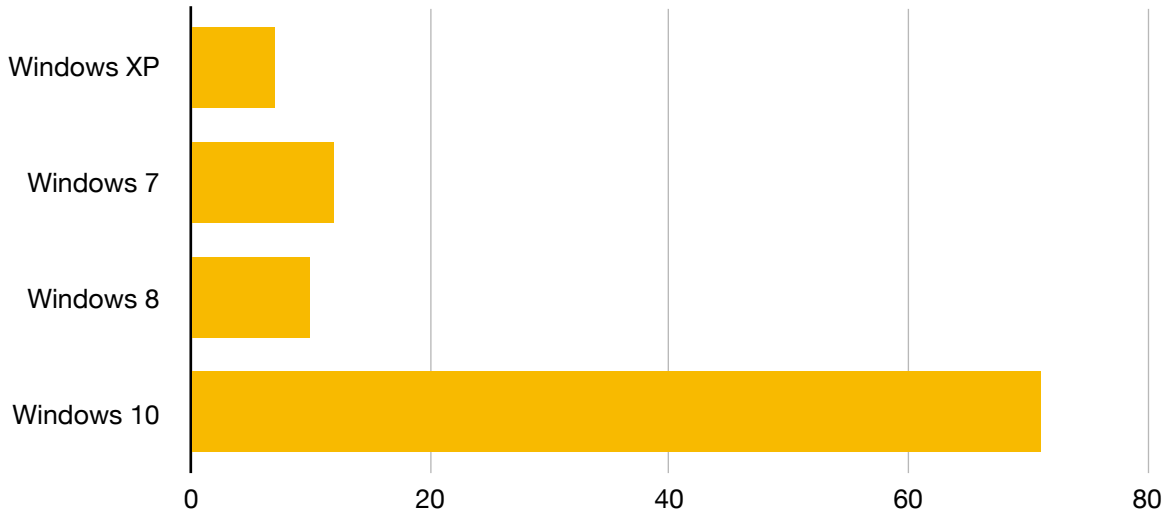
En relación con el desarrollo de las tareas, el 40% de los equipos utilizados tiene una antigüedad superior a los 3 años:



Fuente: Elaboración propia.

Gráfico N°6: Tipo de sistema operativo utilizado en su entorno de trabajo.

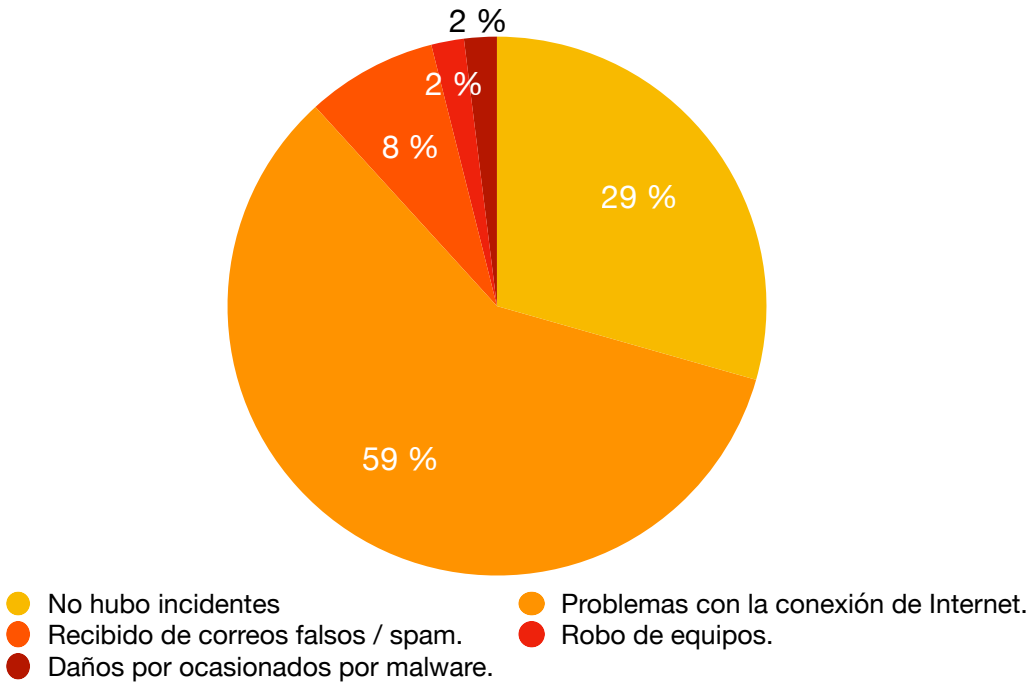
En relación con el sistema operativo utilizado, todos utilizan versiones de MS Windows, pero un 25% utilizan versiones que no tienen soporte por parte del proveedor:



Fuente: Elaboración propia.

Gráfico N°7: Tipos de incidentes que hayan afectado la disponibilidad, confidencialidad o integridad de la información:

En relación con los incidentes, el 71% de los relevados fueron afectados por algún tipo de evento de seguridad:



Fuente: Elaboración propia.

A partir de los riesgos identificados precedentemente, se tomarán como base para el desarrollo del modelo adaptado a micro y pequeños entes. A continuación se analizará, el estándar internacional relacionado con el Sistema de Seguridad de la Información.

3. Estándares y buenas prácticas analizadas 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." (ISO/IEC/IRAM 27.001).
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/IRAM 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

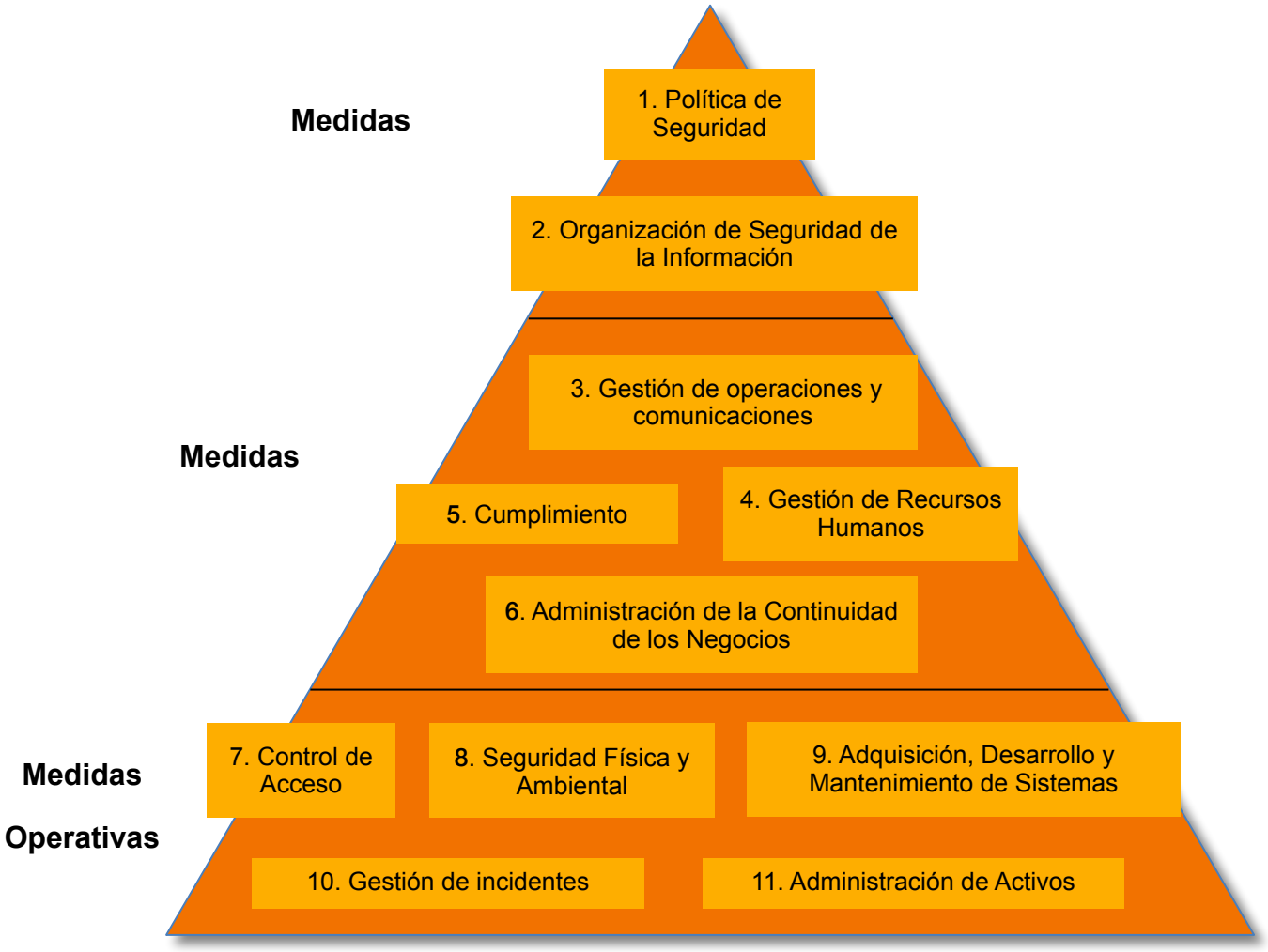
Cada uno de estos dominios tienen que estar presentes en el modelo de gestión para micro y pequeños entes. El autor destaca que cada uno de los aspectos cubiertos corresponde a características en los sistemas de gestión de la seguridad que no se encuentran exclusivamente relacionados con términos tecnológicos, 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.

En la siguiente sección y a modo de conclusión se detallarán las características del modelo propuesto orientado para micro y pequeños entes dedicados a servicios.

4. Modelo de SGSI propuesto para micro y pequeñas empresas prestadoras de servicios en el AMBA.

Teniendo en cuenta estos dominios indicados y en base al relevamiento de los entes en el AMBA, 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.

Cuadro N° 2: Niveles organizacionales y los dominios establecidos por la ISO/IEC/IRAM 27.001.



Fuente: Análisis propio a partir de la ISO/IEC/IRAM 27.001

Medidas estratégicas

Dentro de las medidas estratégicas, las organizaciones tienen que establecer una política de seguridad de la información para todos los integrantes y establecer los roles para la organización de la seguridad; dadas las características de los micro y pequeños entes no se necesitan estructuras burocráticas, pero si establecer roles y funciones internos.

1 . Política de Seguridad
Las organizaciones tienen que establecer un documento de alto nivel en donde se defina la política de seguridad de la información y una revisión anual de la misma.

2. Organización de la seguridad de la información
En lo que respecta a la organización interna, se tiene que enfatizar en el compromiso de los máximos responsables en los entes sobre la seguridad de la información y se deberían asignar los responsabilidades en roles y funciones en la misma.

Medidas tácticas

En relación con las medidas tácticas a implementar, se deben establecer procedimientos para la gestión de recursos humanos, cumplimiento de la ley de protección de datos personales y administración de la continuidad del negocio.

3 . Gestión de las comunicaciones y operaciones
Los entes debe implementar una correcta gestión de las comunicaciones y operaciones en relación a la las copias de respaldo o Backup.

4. Gestión de recursos humanos
Establecer las medidas necesarias antes del empleo, incluyendo capacitación y concientización sobre medidas sobre ciberseguridad, firmar los convenios de confidencialidad necesarios y una vez terminada la relación contractual que se devuelva la información contenida en equipos y en formato de papel.

5. Cumplimiento legal
Los entes deben cumplir con lo dispuesto en la Ley de proyección de datos personales y las disposiciones de la Agencia de Accesos a la Información Pública en el ámbito de la República Argentina.

6. Administración de la continuidad del negocio
Las organizaciones deben gestionar los riesgos y la continuidad del negocio, como también administrar el mantenimiento y evaluación de los planes de continuidad del negocio en caso de diferentes escenarios en donde peligre la continuidad operativa.

Medidas operativas

En relación con las medidas operativas, las micro y pymes de servicios, deben establecer medidas sobre el control de acceso lógico y físico, poseer un plan operativo anual sobre la adquisición de tecnología, gestión de incidentes y gestión de los activos de información.

7. Control del acceso
Los entes tienen que establecer los requerimientos de los controles lógicos a los sistemas operativos, aplicativos y servicios por internet. Todos los accesos deben tener una política de contraseñas y configurar segundo factor de autenticación.

8. Seguridad física y ambiental
Los entes tienen que establecer áreas físicamente seguras, para el resguardo de equipos e información sensible.

9. Adquisición, desarrollo y mantenimiento de los sistemas de información
Los entes deben establecer un plan anual para la inversión en equipos y herramientas de seguridad.

10. Gestión de un incidente en la seguridad de la información
Los deben establecer un control y monitoreo de los incidentes que afecten la disponibilidad, confidencialidad e integridad de las operaciones.

11. Administración de activos
Los entes necesitan tener un inventario de activos de información para identificar toda la información que tienen, establecer las responsabilidades, lineamientos de clasificación, etiquetado y manejo de la información corporativa.

Por todo lo expuesto, las micro y pequeños entes prestadores de servicios deberían considerar la aplicación de las citadas medidas estratégicas, tácticas y operativas para poder administrar eficientemente la Seguridad de la Información y estar preparados para los posibles incidentes que pueden afectar sus operaciones.

Asimismo se destaca que en la gestión de la ciberseguridad, solo un 20% corresponde a la implementación de herramientas o software específico, el 80% corresponde a tareas de gestión y control, requiriendo un abordaje interdisciplinario de la seguridad desde el análisis crítico de los riesgos existente hasta una revisión de las necesidades del negocio en cada ente.

5. Bibliografía

Agencia de Acceso a la Información Pública (AAIP). (2006), “Disposición N° 11/2006, Medidas de Seguridad”. Buenos Aires, Argentina., accedido desde http://www.jus.gob.ar/

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

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 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”

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

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 (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

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.