Tercera Jornada Institucional de Investigación de la Universidad del Salvador. USAL, Buenos Aires, 2024.

Análisis de las variables de ciberseguridad en micro y pequeños estudios contables del AMBA.

Diego Sebastian Escobar y Alejandro Vera.

Cita:

Diego Sebastian Escobar y Alejandro Vera (2024). *Análisis de las variables de ciberseguridad en micro y pequeños estudios contables del AMBA. Tercera Jornada Institucional de Investigación de la Universidad del Salvador. USAL, Buenos Aires.*

Dirección estable: https://www.aacademica.org/escobards/78

ARK: https://n2t.net/ark:/13683/ptuD/t63

UNIVERSIDAD DEL SALVADOR

Eje 2: Desarrollo económico y generación de empleo de calidad

Título: "Análisis de las variables de ciberseguridad en micro y pequeños estudios contables del AMBA"

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

Proyecto: "Desarrollo de un modelo simplificado de capacitación y sensibilización en ciberseguridad para Contadores Públicos" (Código P20210100090US).

Autores:

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

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

Análisis de las variables de ciberseguridad en micro y pequeños estudios contables del AMBA

1. Introducción

En el contexto de la Tercera Jornada Institucional de Investigación de la Universidad del Salvador, se presenta el trabajo titulado "Análisis de las variables de ciberseguridad en micro y pequeños estudios contables del AMBA". Este estudio se enmarca en el proyecto "Desarrollo de un modelo simplificado de capacitación y sensibilización en ciberseguridad para Contadores Públicos" (Código P20210100090US).

El propósito central de este estudio es difundir un modelo simplificado de sistema de gestión de capacitación en ciberseguridad, específicamente diseñado para micro y pequeñas empresas que ofrecen servicios contables en el Área Metropolitana de Buenos Aires.

Este artículo se estructura en tres secciones. En la primera, se analiza el contexto actual de las micro y pequeñas empresas que brindan servicios contables en esta área geográfica. En la segunda, se identifican los estándares considerados para el desarrollo del modelo propuesto para estas entidades. Finalmente, en la tercera sección, se presenta una síntesis de la propuesta desarrollada, dirigida específicamente a las entidades objeto de estudio.

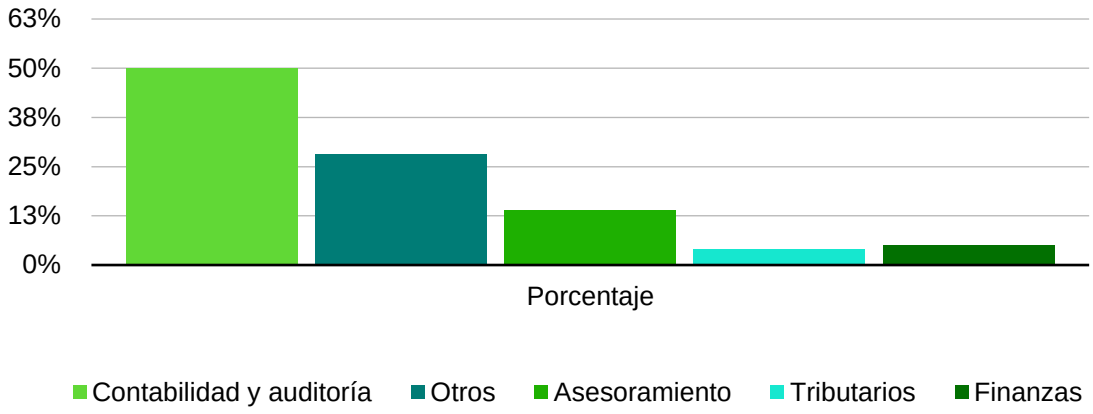
2. Desarrollo

2.1. 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 servicios ubicadas en el AMBA. Para ello, se realizó un relevamiento de 80 empresas, del cual se obtuvieron las siguientes conclusiones sobre su situación en la gestión de la seguridad de la información:

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

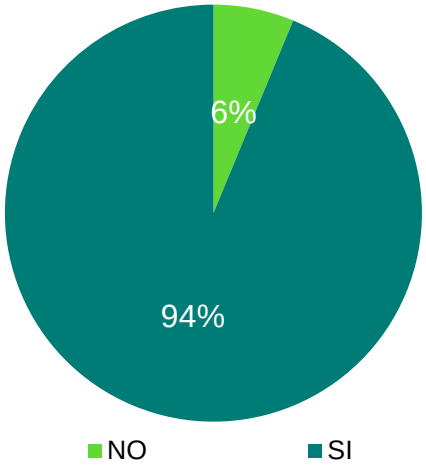
De las empresas relevadas, el 50% corresponden al rubro de contabilidad y auditoría, y el resto a otros tipos de servicios contables:



Fuente: Elaboración propia.

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

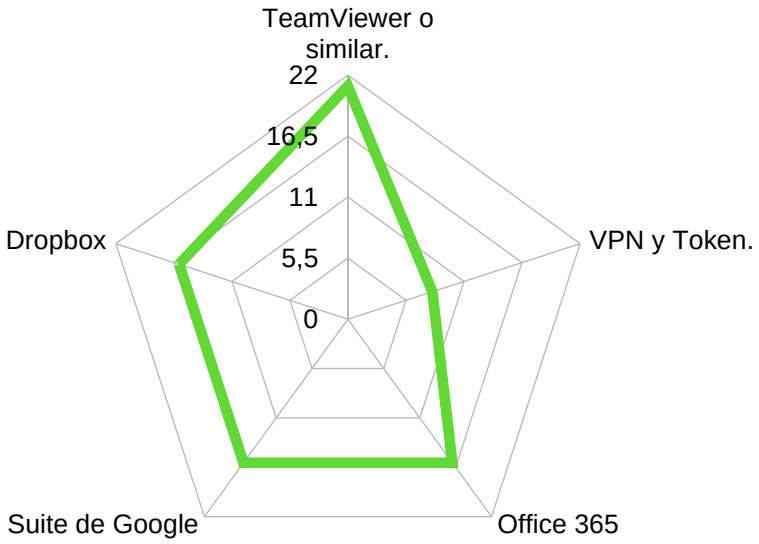
En relación con el contexto de pandemia y confinamiento el 94% de las empresas relevadas pudieron continuar con sus operaciones a distancia:



Fuente: Elaboración propia.

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

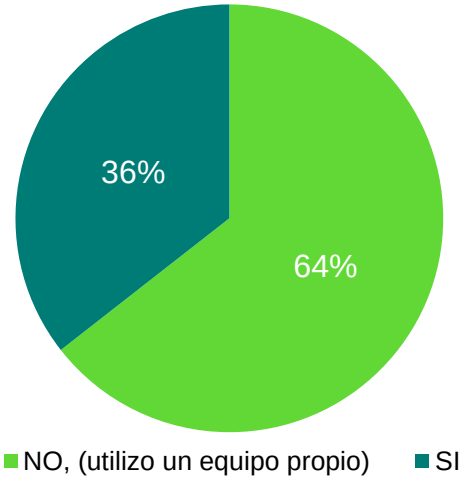
En relación con los tipos de tecnologías utilizados se pueden evidenciar el uso de servicios en la nube y aplicativos colaborativos:



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.

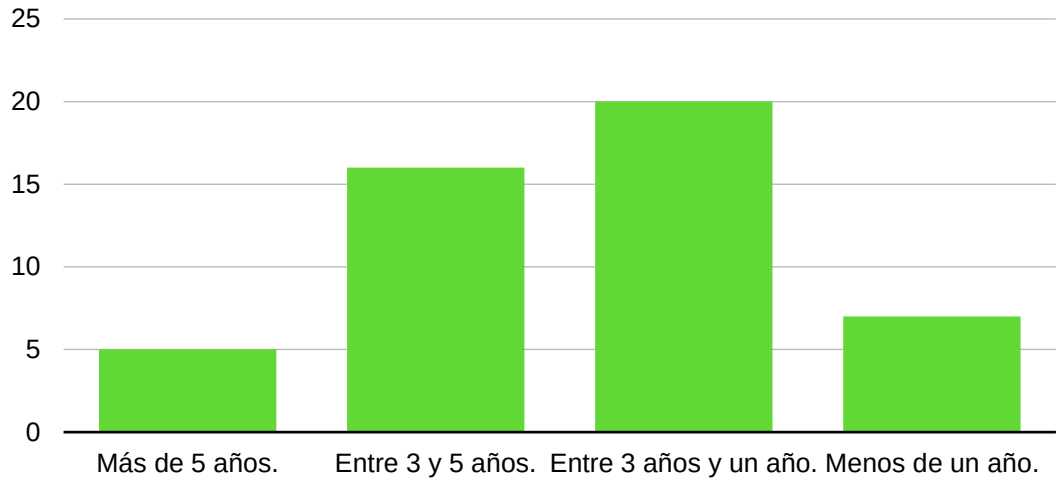
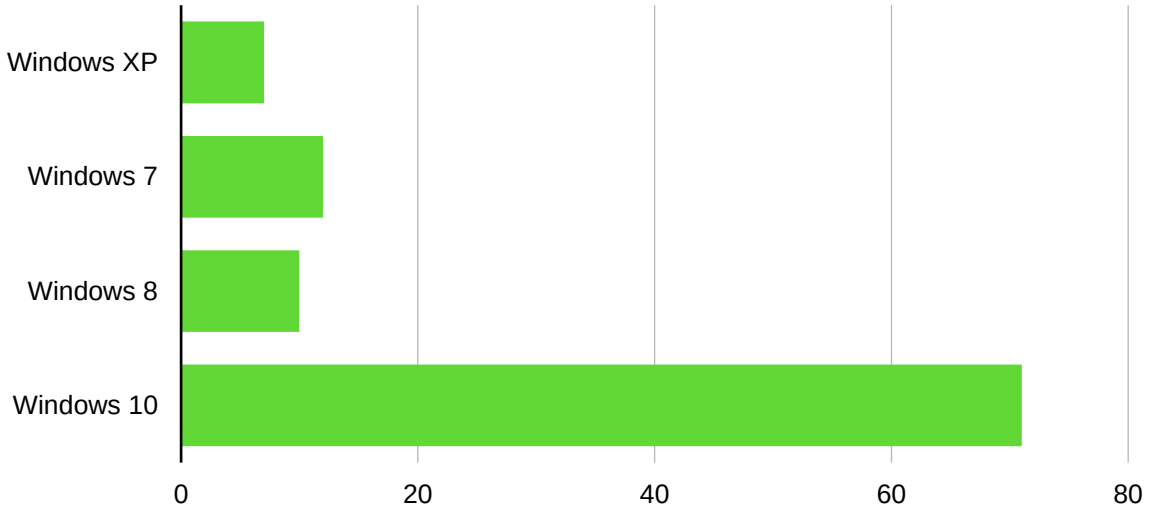


Gráfico N°6: Tipo de sistema operativo utilizado en su entorno de trabajo.

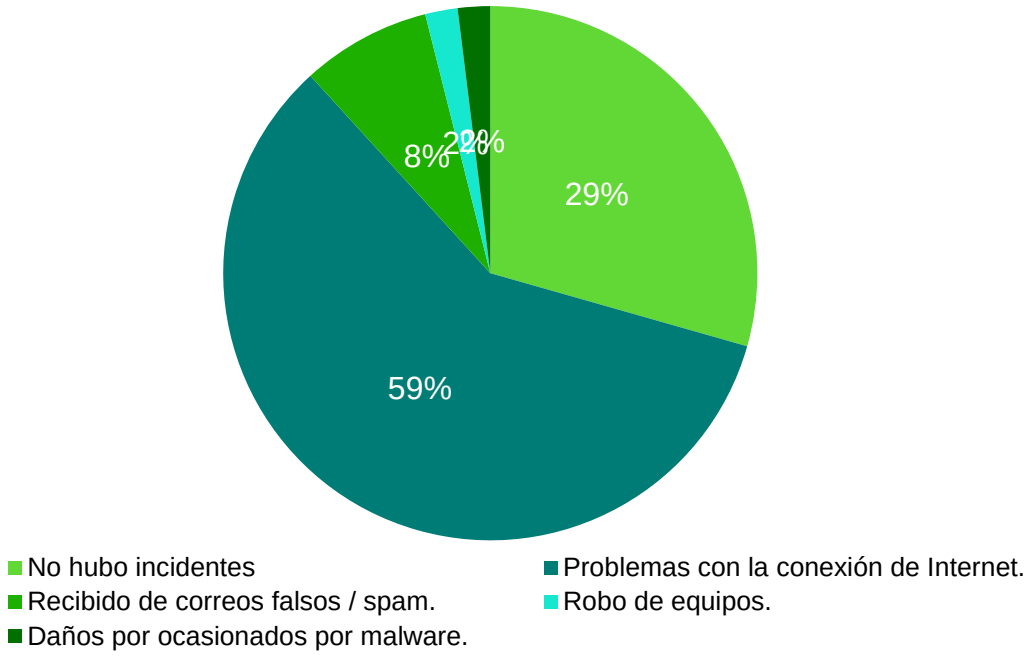
En relación con el sistema operativo utilizado, todos utilizan versiones de MS Windows, pero un 25% utilizan versiones que no tienen soporte por parte del proveedor:



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 contables. A continuación se analizará, el estándar internacional relacionado con el Sistema de Seguridad de la Información.

2.2. 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.

3. Reflexiones a modo de conclusiones.

Teniendo en cuenta estos dominios y el relevamiento de los entes en el AMBA, se pueden relacionar con las diferentes decisiones y funciones tomadas en los niveles de la organización, subdivididos 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

Las organizaciones deben establecer una política de seguridad de la información para todos los integrantes y definir los roles para la organización de la seguridad. No se necesitan estructuras burocráticas, pero sí roles y funciones claros.

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

Establecer procedimientos para la gestión de recursos humanos, cumplimiento de la ley de protección de datos personales y administración de la continuidad del negocio. Implementar una correcta gestión de las comunicaciones y operaciones en relación con las copias de respaldo.

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

Establecer medidas sobre el control de acceso lógico y físico, un plan operativo anual sobre la adquisición de tecnología, gestión de incidentes y gestión de los activos de información. Todos los accesos deben tener una política de contraseñas y configurar un segundo factor de autenticación. Establecer áreas físicamente seguras para el resguardo de equipos e información sensible. Implementar un plan anual para la inversión en equipos y herramientas de seguridad. Controlar y monitorear los incidentes que afecten la disponibilidad, confidencialidad e integridad de las operaciones. Tener un inventario de activos de información para identificar toda la información, establecer responsabilidades y lineamientos de clasificación.

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 contables deberían considerar la aplicación de las citadas medidas estratégicas, tácticas y operativas para administrar eficientemente la seguridad de la información y estar preparados para posibles incidentes que pueden afectar sus operaciones.

Es importante destacar que en la gestión de la ciberseguridad, solo un 20% corresponde a la implementación de herramientas o software específico, mientras que el 80% corresponde a tareas de gestión y control, requiriendo un abordaje interdisciplinario desde el análisis crítico de los riesgos 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/datos-personales.aspx

Diego Sebastian Escobar (2023). Asegurando la Resiliencia Empresarial: Conceptos fundamentales a considerar en la auditoría de la continuidad del negocio. XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE, Buenos Aires.

Diego Sebastián Escobar (2023). CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO. XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba, Córdoba.

Diego Sebastian Escobar (2023). Análisis de los cambios en los controles tecnológicos de la Comunicación A 7724 del BCRA en las entidades financieras. XXXV Jornadas Profesionales de Contabilidad, Auditoría y de Gestión y Costos. CGCE, Buenos Aires.

Diego Sebastian Escobar (2023). EL IMPACTO DE LAS NUEVAS TECNOLOGÍAS DE INFORMACIÓN EN LA FORMACIÓN PROFESIONAL DEL CONTADOR. XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba, Córdoba.

Diego Sebastian Escobar (2023). La profesión contable ante los desafíos de la inteligencia artificial Chat GPT. XXVI Congreso Nacional de Contabilidad. Colegio de Contadores del Paraguay, Asunción.

Diego Sebastián Escobar (2023). Características a considerar en la elaboración de planes de concientización en Ciberseguridad para Contadores Públicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (3-1), 1-7.

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.

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