JORNADA DE INVESTIGACIÓN. UNIVERSIDAD DEL SALVADOR FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES - USAL, Buenos Aires, 2024.

Evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA.

Diego Sebastián Escobar.

Cita:

Diego Sebastián Escobar (2024). *Evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA. JORNADA DE INVESTIGACIÓN. UNIVERSIDAD DEL SALVADOR FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES - USAL, Buenos Aires.*

Dirección estable: https://www.aacademica.org/escobards/76

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

UNIVERSIDAD DEL SALVADOR
FACULTAD CIENCIAS ECONÓMICAS Y EMPRESARIALES

JORNADA DE INVESTIGACIÓN

Martes 17 de septiembre de 2024

Título: "Evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA"

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

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

Índice temático

1. Introducción

En el contexto de la Jornada de Investigación de la Facultad de Ciencias Económicas y Empresariales de la Universidad del Salvador, presentamos a consideración de todos los asistentes el presente trabajo denominado "Evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA".

Este trabajo se encuentra encuadrado 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 el diagnóstico de las prácticas de ciberseguridad en micro y pequeños estudios contables en el Área Metropolitana de Buenos Aires.

2. Conceptos preliminanares

El Sistema de Gestión de Seguridad de la Información (SGSI) es definido como un “Proceso sistemático, documentado y conocido por toda la organización. 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 norma 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	

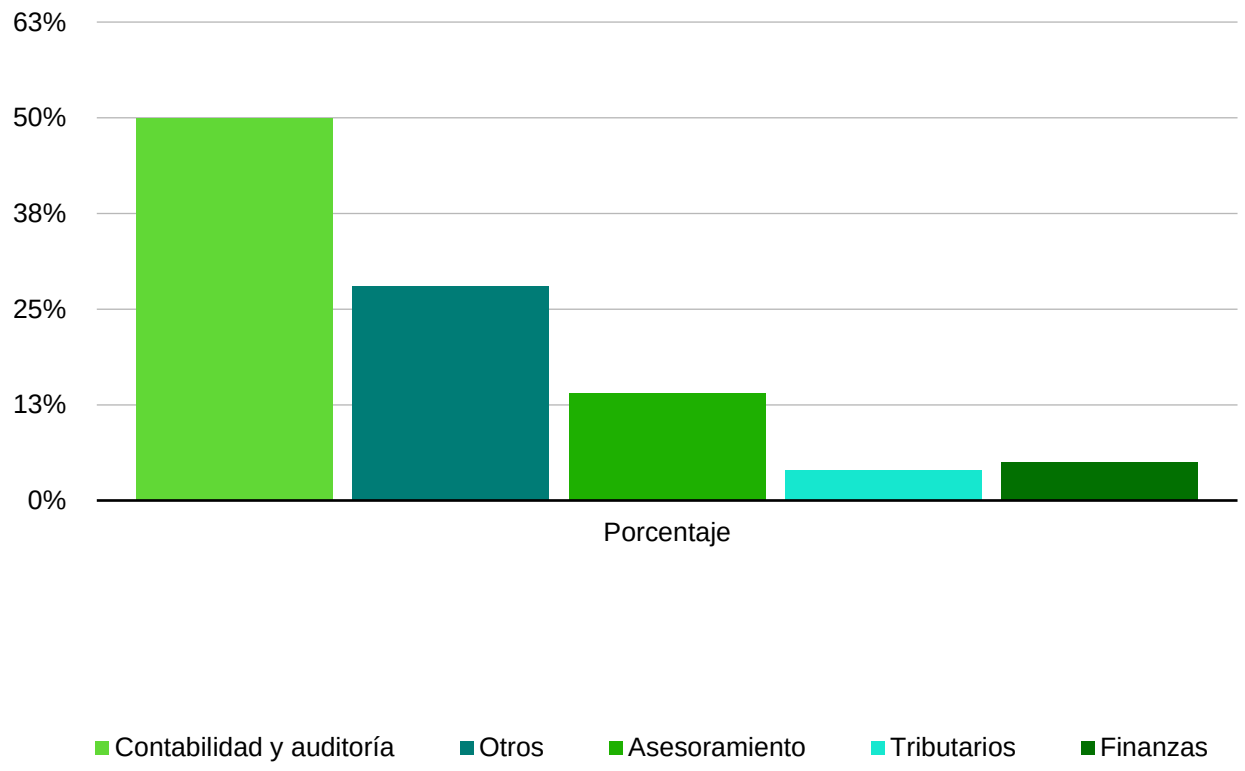
Cada uno de estos dominios debe estar presente en el modelo de gestión para micro y pequeños entes. El autor destaca que cada uno de los aspectos cubiertos corresponde a características en los sistemas de gestión de la seguridad que no se encuentran exclusivamente relacionados con términos tecnológicos, ya que en la administración de la seguridad se necesita redactar políticas estratégicas, normas, procedimientos, inventarios de activos de información y establecer controles a los procesos en los entes.

3. 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:

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

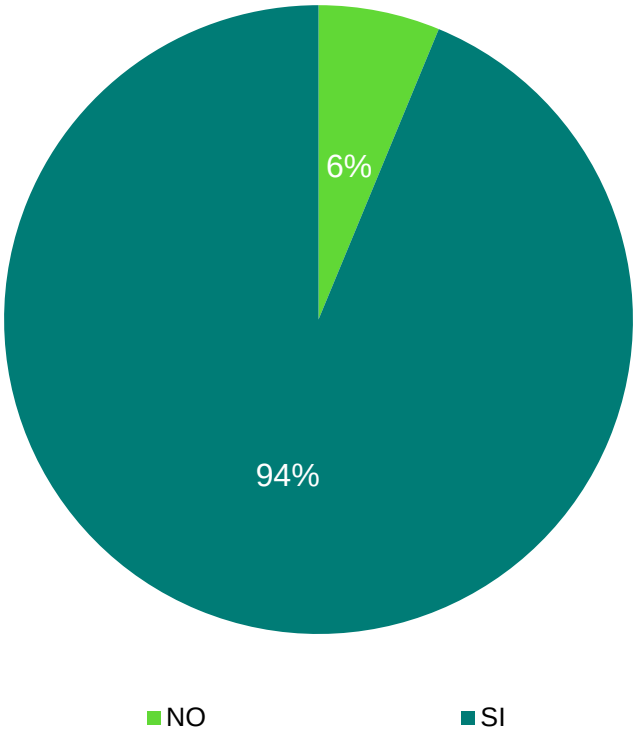
De las empresas relevadas, el 50% corresponden al rubro de contabilidad y auditoría, y el resto a otros tipos de servicios contables:



Fuente: Elaboración propia.

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

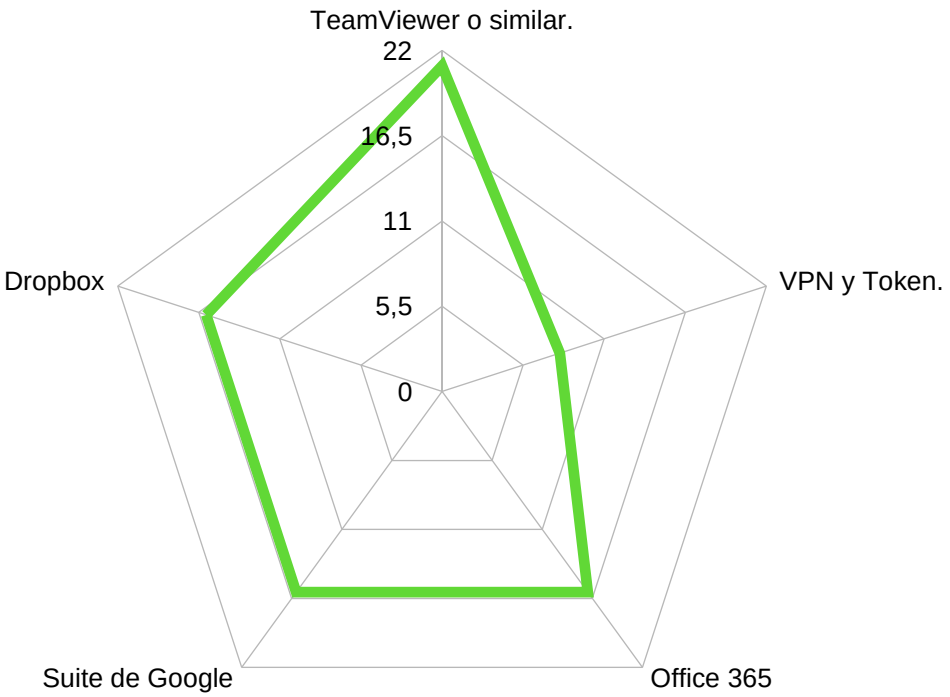
En relación con el contexto de pandemia y confinamiento el 94% de las empresas relevadas pudieron continuar con sus operaciones a distancia:



Fuente: Elaboración propia.

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

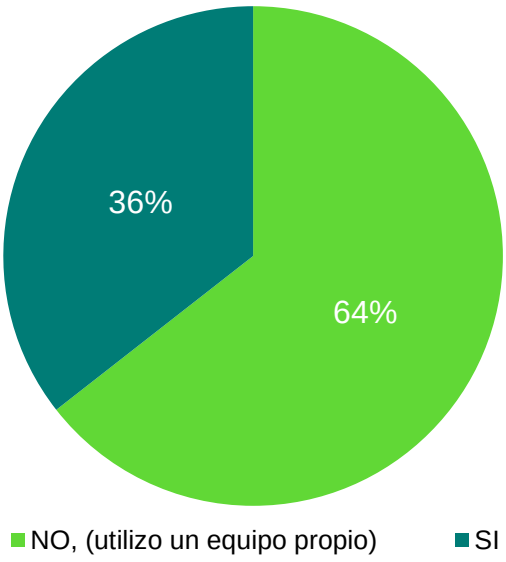
En relación con los tipos de tecnologías utilizados se pueden evidenciar el uso de servicios en la nube y aplicativos colaborativos:



Fuente: Elaboración propia.

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

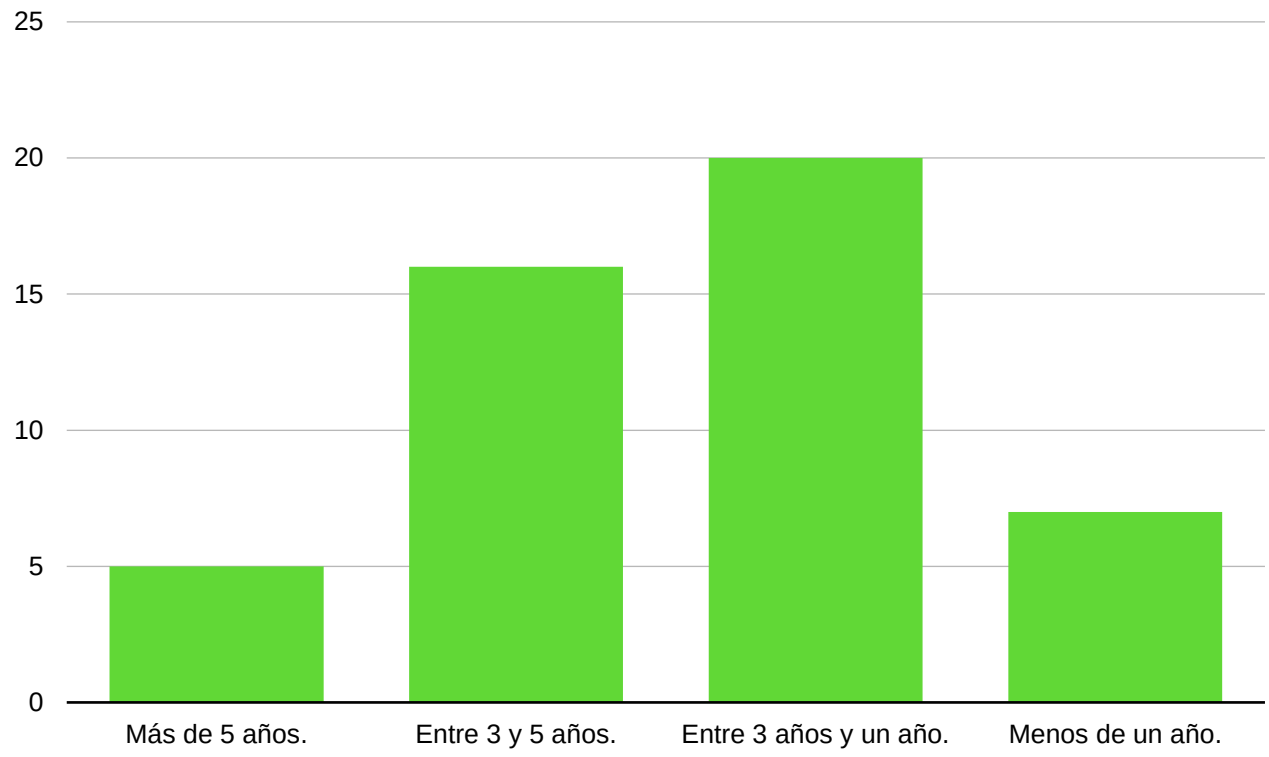
En relación con el desarrollo de las tareas, el 64% los analistas utilizaron equipos propios para desarrollar las tareas:



Fuente: Elaboración propia.

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

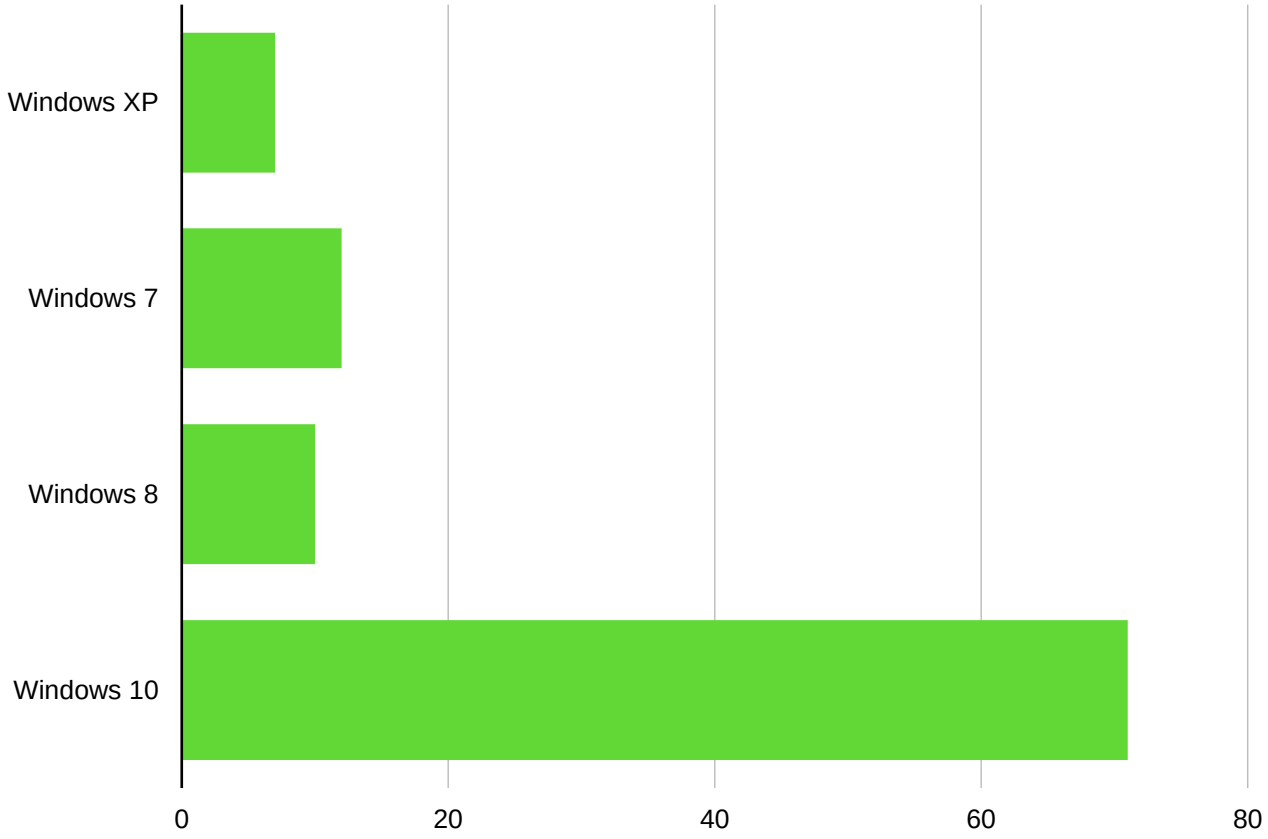
En relación con el desarrollo de las tareas, el 40% de los equipos utilizados tiene una antigüedad superior a los 3 años:



Fuente: Elaboración propia.

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

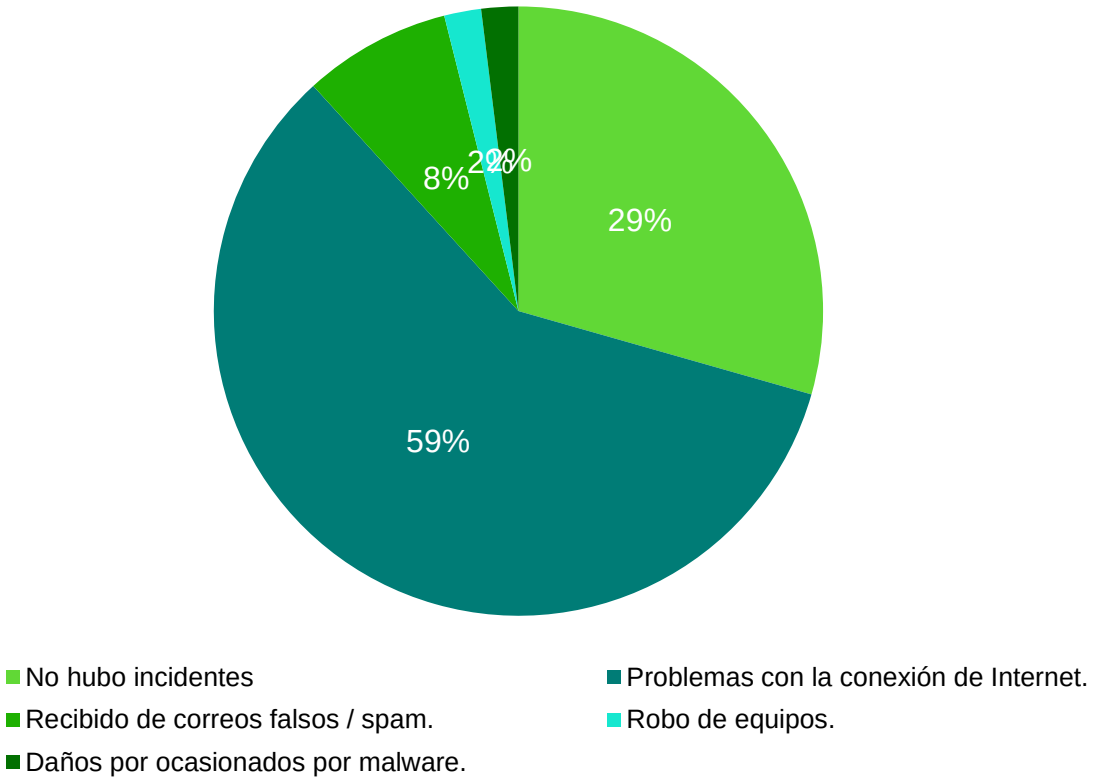
En relación con el sistema operativo utilizado, todos utilizan versiones de MS Windows, pero un 25% utilizan versiones que no tienen soporte por parte del proveedor:



Fuente: Elaboración propia.

3.7. 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.

4. Reflexiones a modo de conclusiones

La evaluación de las prácticas de ciberseguridad en micro y pequeños estudios contables del AMBA revela una serie de desafíos significativos que enfrentan estas organizaciones en cuanto a la protección de la información. Entre los principales hallazgos, se observa que una porción considerable de los estudios contables aún no cuenta con políticas formales de ciberseguridad, lo que expone sus operaciones a

riesgos considerables, como brechas de seguridad, vulnerabilidad ante ataques cibernéticos y pérdidas de datos críticos.

Del relevamiento de 80 empresas, se llegaron a las siguientes conclusiones sobre su situación actual en la gestión de la seguridad de la información:

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

- En el contexto de pandemia y confinamiento, el 94% de las empresas relevadas pudieron continuar con sus operaciones a distancia.

- En relación con los tipos de tecnologías utilizados, se evidenció el uso de servicios en la nube y aplicativos colaborativos.

- El 64% de los analistas utilizaron equipos propios para desarrollar las tareas.

- El 40% de los equipos utilizados tiene una antigüedad superior a los 3 años.

- Todos utilizan versiones de MS Windows, pero un 25% utilizan versiones que no tienen soporte por parte del proveedor.

- El 71% de los relevados fueron afectados por algún tipo de evento de seguridad.

Durante la pandemia de COVID-19, muchas de estas empresas debieron adaptarse rápidamente a entornos de trabajo remoto. Si bien la mayoría logró mantener la continuidad operativa, el uso de equipos no gestionados y sistemas operativos desactualizados incrementó las vulnerabilidades, lo que llevó a un aumento en la incidencia de eventos de seguridad. El 71% de las empresas reportó algún tipo de incidente que afectó la disponibilidad, confidencialidad o integridad de la información,

lo que pone de manifiesto la necesidad urgente de mejorar sus sistemas de seguridad.

A partir de este diagnóstico, resulta claro que es fundamental avanzar en la capacitación y sensibilización en ciberseguridad para estos estudios, especialmente en lo que respecta a la implementación de controles básicos de seguridad, la actualización de tecnologías y la adopción de políticas de gestión de riesgos. El desarrollo de un Sistema de Gestión de Seguridad de la Información (SGSI), basado en la norma ISO/IEC/IRAM 27.001, se presenta como una solución viable y necesaria para garantizar un nivel adecuado de seguridad de la información.

En conclusión, las micro y pequeñas empresas del sector contable del AMBA deben priorizar la adopción de medidas concretas de ciberseguridad para salvaguardar su información, optimizar sus recursos tecnológicos y mitigar los riesgos asociados a un entorno digital cada vez más complejo y desafiante. Solo a través de una gestión adecuada de la seguridad de la información podrán asegurar la sostenibilidad y competitividad de sus operaciones en el mediano y largo plazo.

5. Bibliografía

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. (2022). Capacitación y concientización en seguridad de la información. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-2), 1-6.

Escobar, D. S. (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.

Escobar, D. S. (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.

Escobar, D. S. (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.

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, Cordoba.

Escobar, D. S. (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, Cordoba.

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. (2022). El rol del Contador en la era digital. In VI Jornadas de Orientación Vocacional. UBA.

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

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.

Escobar, Diego Sebastián. (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. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0817_EscobarDS.pdf

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