XLIV Simposio Nacional de Profesores de Práctica Profesional. Universidad Nacional de Córdoba, Cordoba, 2023.

CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO.

Diego Sebastián Escobar.

Cita:

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.*

Dirección estable: https://www.aacademica.org/escobards/73

ARK: https://n2t.net/ark:/13683/ptuD/3hu

XLIV SIMPOSIO NACIONAL DE PROFESORES DE PRÁCTICA PROFESIONAL

FACULTAD DE CIENCIAS ECONÓMICAS

UNC Universidad Nacional de Córdoba

Título del trabajo:

CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO

Autor:

Diego Sebastián Escobar

Universidad de Buenos Aires – Facultad de Ciencias Económicas

Área: Actualización de contenidos programáticos

CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO

Resumen

En un entorno empresarial cada vez más digitalizado y vulnerable a amenazas cibernéticas, la ciberresiliencia ha emergido como un componente crítico para la supervivencia y el éxito de las organizaciones a nivel internacional. En el marco del XLIV Simposio Nacional de Profesores de Práctica Profesional someto al análisis de los asistentes la presente ponencia con el objetivo de analizar el concepto de ciberresiliencia y la importancia de incorporarlo en la formación actual del Contador Público.

La ciberresiliencia es definida como “la capacidad de una organización para resistir, adaptarse y recuperarse de los ciberataques” (OBS Business School, 2023), es esencial en un mundo donde las amenazas cibernéticas son una realidad constante. Los Contadores Públicos, tradicionalmente asociados con la contabilidad, tributación y la auditoría financiera, ahora desempeñan un papel fundamental en la gestión de riesgos cibernéticos y la seguridad financiera.

En este contexto, los Contadores Públicos enfrentan desafíos significativos en la formación profesional. La falta de conciencia y la necesidad de capacitación en ciberseguridad son obstáculos importantes que deben superarse.

La seguridad cibernética y la gestión de riesgos cibernéticos ya no son responsabilidades exclusivas de las áreas de tecnología de la información, sino que debe ser gestionada interdisciplinariamente para cumplir con un abordaje integral. Los profesionales en Ciencias Económicas, deben tener un papel proactivo en la defensa contra las amenazas cibernéticas, contribuyendo a la seguridad financiera y a la continuidad de las operaciones en un mundo digital en constante evolución. La ciberresiliencia no solo protegen infraestructuras tecnológicas, sino que también fortalece la confianza del público en las organizaciones.

CIBERRESILIENCIA: UN NUEVO DESAFÍO EN LA FORMACIÓN DEL CONTADOR PÚBLICO

ÍNDICE TEMÁTICO

1. INTRODUCCIÓN

En un mundo cada vez más interconectado y digitalizado, la ciberseguridad se ha convertido en una prioridad crítica para las organizaciones en Argentina y en todo el mundo. La creciente sofisticación de las ciber amenazas ha llevado a una reevaluación profunda de cómo las empresas y las instituciones se preparan para enfrentar estos desafíos. En este contexto, el rol del Contador Público ha experimentado una transformación significativa, ya que se encuentra involucrado en la promoción de la ciberresiliencia en las organizaciones.

En la era digital actual, donde la tecnología de la información impacta en los procesos de los negocios, la ciberseguridad se ha convertido en una preocupación constante. Los ciberataques, que van desde intrusiones en la red hasta el robo de datos confidenciales, han demostrado ser un desafío constante y de rápida evolución para la integridad de la información y la continuidad de las operaciones empresariales.

En este contexto, la ciberresiliencia se presenta como un principio fundamental para garantizar la supervivencia y la prosperidad de las organizaciones en el mundo digital. La ciberresiliencia se refiere a la “capacidad de una organización para resistir, adaptarse y recuperarse de los impactos de los ciberataques de manera efectiva y eficiente” (OBS Business School, 2023). Si bien esta capacidad es crucial para todas las entidades, en esta ponencia enfocamos nuestra atención en el desempeño de los Contadores Públicos en la promoción y el fortalecimiento de la ciberresiliencia en el ámbito empresarial.

Los Contadores Públicos, tradicionalmente conocidos por su función en la contabilidad y la auditoría financiera, se han convertido en actores fundamentales en la gestión de riesgos de ciberseguridad. Su comprensión profunda de los procesos financieros y su capacidad para evaluar riesgos y salvaguardar la integridad de los datos financieros los coloca en una posición estratégica para abordar los desafíos que plantea el ciberespacio.

En la presente investigación, analizamos la relación entre la ciberresiliencia y el rol del Contador Público, destacando cómo su conocimiento y habilidades pueden contribuir a proteger los activos críticos de una organización y garantizar la continuidad de sus operaciones en un mundo cada vez más amenazado por ciberataques. Además, analizamos los desafíos que enfrentan los Contadores Públicos en este contexto y ofrecemos recomendaciones para promover la ciberresiliencia en el ámbito corporativo.

2. OBJETIVO DE LA INVESTIGACIÓN

El objetivo de esta investigación es analizar y comprender cómo la ciberresiliencia se ha convertido en un nuevo desafío en la formación del Contador Público en la actualidad. A través de la recopilación de opiniones expertas en ciberseguridad, se busca:

- Identificar las transformaciones y evolución de la ciberseguridad en el contexto empresarial y su impacto en la profesión contable.

- Explorar el papel que el Contador Público desempeña en la promoción de la ciberresiliencia en las organizaciones y cómo esta función ha evolucionado en respuesta a las amenazas cibernéticas.

- Analizar las habilidades y conocimientos adicionales requeridos por los Contadores Públicos para abordar eficazmente la ciberresiliencia en su práctica profesional.

- Proponer recomendaciones para adaptar la formación de Contadores Públicos y su práctica profesional, de modo que se integren aspectos clave de la ciberresiliencia y se preparen para enfrentar los desafíos cibernéticos en el entorno empresarial actual.

Mediante esta investigación, se pretende contribuir al entendimiento de cómo la ciberresiliencia debería ser tenida en cuenta en la formación y práctica del Contador Público, y considerarse en el desarrollo de programas educativos y la adaptación de la profesión a las demandas de ciberseguridad en constante cambio.

3. IDENTIFICACIÓN DEL PROBLEMA: LA IMPORTANCIA DE LA CIBERRESILIENCIA Y SU IMPACTO EN LA FORMACIÓN PROFESIONAL

La ciberresiliencia es la “capacidad de una organización para impedir, resistir y recuperarse de los incidentes de ciberseguridad que puedan afectar a sus operaciones, datos, reputación y confianza” (IBM, 2023). La ciberresiliencia se relaciona con la capacidad de una organización para resistir y recuperarse de ataques cibernéticos de la siguiente manera:

- La capacidad de resistir implica tener medidas de prevención y detección que reduzcan la probabilidad y el impacto de los ataques cibernéticos, así como una respuesta rápida y eficaz que contenga y mitigue los daños causados por los ataques.

- La capacidad de recuperarse implica tener planes de continuidad y recuperación que permitan restaurar las funciones críticas y los servicios afectados por los ataques, así como una mejora continua que aprenda de las lecciones y refuerce las capacidades.

La ciberresiliencia es importante porque las amenazas cibernéticas son cada vez más frecuentes, sofisticadas y dañinas, y pueden causar pérdidas económicas, incumplimientos legales, daños a la imagen y pérdida de clientes. Para ser ciberresilientes, las organizaciones deben adoptar una estrategia holística que incluya medidas de prevención, detección, respuesta y recuperación, así como una cultura de seguridad y una mejora continua.

En un mundo cada vez más digitalizado y conectado, las organizaciones se enfrentan a una amenaza constante: los ciberataques. Estos ataques cibernéticos representan una seria preocupación para empresas, instituciones gubernamentales y organizaciones sin fines de lucro. La vulnerabilidad de los sistemas de información y la integridad de los datos se encuentran en el punto de mira de una serie de actores maliciosos que buscan aprovecharse de las debilidades de la ciberseguridad.

La ciberresiliencia, entendida como la capacidad de una organización para resistir, adaptarse y recuperarse de los ciberataques, se ha convertido en una temática crucial para la supervivencia y la continuidad de las operaciones de las organizaciones. Los ciberataques pueden resultar en la pérdida de datos confidenciales, la interrupción de servicios críticos, la degradación de la confianza del cliente y pérdidas financieras significativas.

En este contexto, las organizaciones confían en la profesión contable para garantizar la integridad y la precisión de sus registros financieros y cumplir con las regulaciones y normativas vigentes. Sin embargo, la seguridad de estos registros se encuentra en riesgo debido a la creciente sofisticación de los ciberataques.

4. EL IMPACTO DE LOS CIBERATAQUES

El impacto de los ciberataques afecta de diversas maneras en las organizaciones:

- Integridad de los datos financieros: Los ciberataques pueden resultar en la manipulación o la destrucción de datos financieros, lo que afecta directamente a la precisión de los estados contables y a la toma de decisiones informadas.

- Gestión de riesgos: La gestión de riesgos cibernéticos impacta en la contabilidad pública. La falta de ciberresiliencia puede exponer a las organizaciones a riesgos financieros significativos y a sanciones regulatorias.

- Confianza: La confianza del público en la integridad de los informes financieros es fundamental. Los ciberataques exitosos pueden erosionar esta confianza y dañar la relación entre las organizaciones y sus stakeholders.

Por lo tanto, es necesario comprender el impacto de la falta de ciberresiliencia en las organizaciones y cómo los contadores públicos pueden desempeñar un papel esencial en la prevención y mitigación de los riesgos cibernéticos.

5. EL ROL DEL CONTADOR PÚBLICO EN LA CIBERRESILIENCIA Y LA PREPARACIÓN PARA EL FUTURO

El Contador Público, tradicionalmente conocido por su función en la contabilidad, tributación y auditoría financiera, necesita actualizarse para abordar los nuevos desafíos en la ciberseguridad y la gestión de riesgos cibernéticos.

En un mundo donde las amenazas cibernéticas son inevitables, es esencial que los profesionales estén preparados para enfrentar este nuevo desafío. Esto incluye la adquisición de habilidades y conocimientos adicionales en ciberseguridad, la comprensión de las mejores prácticas en gestión de riesgos cibernéticos y la capacidad de evaluar la resiliencia de una organización ante las amenazas cibernéticas.

6. CONCLUSIONES

En un entorno empresarial y tecnológico en constante evolución, la ciberresiliencia se ha convertido en un pilar fundamental para la supervivencia y el éxito de las organizaciones en todo el mundo. En la presente ponencia, se ha abordado la relación entre la ciberresiliencia y el rol del Contador Público en la actualidad, a continuación se plantean los siguientes ejes de debate para ser analizados:

Importancia de la Ciberresiliencia: Se plantea la creciente importancia de la ciberresiliencia en el contexto empresarial actual. Las amenazas cibernéticas son una realidad constante y, en muchos casos, inevitables; en este entorno, la ciberresiliencia no solo implica la prevención de ataques, sino también la capacidad de adaptarse y recuperarse rápidamente cuando se producen incidentes.

El Rol Evolutivo de la profesión: Tradicionalmente centrados en la contabilidad, tribulación y la auditoría financiera, en la actualidad los Contadores Públicos deberían capacitarse en la gestión de riesgos cibernéticos, la ciberseguridad y la ciberresiliencia organizacional.

La protección de los activos de información: Se destaca la importancia crítica de los activos financieros y la información contable en las organizaciones.

La conciencia y la formación son claves: Los desafíos que enfrentan los Contadores en el ámbito de la ciberresiliencia son notables. La necesidad de una sensibilización y capacitación adecuada en ciberseguridad son obstáculos que deben abordarse. Los profesionales contables deben mantenerse al día con las últimas amenazas y mejores prácticas para ser efectivos en su función de protección de activos.

En resumen, se destaca la necesidad del Contador Público en la promoción y el fortalecimiento de la ciberresiliencia en las organizaciones argentinas. La ciberseguridad

y la gestión de riesgos cibernéticos ya no son responsabilidades exclusivas de los departamentos de tecnología de la información, sino que se han convertido en una necesidad para la profesión contable. Los Contadores Públicos, al asumir este papel proactivo en la defensa contra las amenazas cibernéticas, pueden contribuir de manera significativa a la seguridad financiera y a la continuidad de las operaciones en un mundo digital en constante cambio. La ciberresiliencia se convierte así en un factor diferenciador que no solo protege los activos financieros, sino que también fortalece la confianza del público y en las organizaciones.

7. BIBLIOGRAFÍA

ciberseguridad.com. (17 de septiembre de 2023). DE LA CIBERSEGURIDAD A LA CIBERRESILIENCIA. Obtenido de CIBERSEGURIDAD: https://ciberseguridad.com/guias/ciberresiliencia/

IBM. (20 de Agosto de 2023). ¿Qué es la ciberresiliencia? Obtenido de Definición de ciberresiliencia: https://www.ibm.com/es-es/topics/cyber-resilience

OBS Business School. (2023). Ciberresiliencia: Todo lo que necesitas saber. Madrid: https://www.obsbusiness.school/blog/ciberresiliencia-todo-lo-que-necesitas-saber.

Suarez Kimura, E. B., Escobar, D. S., & De Franceschi, R. L. (2014). El rol del profesional en Ciencias Económicas en la planificación estratégica de las tecnologías de información. In *XXXVI Simposio Nacional de Profesores de Práctica Profesional. FACULTAD DE CIENCIAS ECONÓMICAS UNIVERSIDAD ARGENTINA DE LA EMPRESA (UADE). PINAMAR, BUENOS AIRES* (Vol. 18, p. 19).

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. (2011). INCLUSIÓN DE CONCEPTOS BÁSICOS DE SEGURIDAD DE LA INFORMACIÓN EN LA FORMACIÓN DEL CONTADOR PÚBLICO. XXXIII Simposio Nacional de Profesores de Práctica Profesional. Universidad de La Plata, La Plata.

Escobar, D. S. (2011). La seguridad de la información y su contribución a la contabilidad. Mesa de Ciencias de la Secretaría de Investigación y Doctorado, Rumbo al Centenario 1913-2013. Secretaría de Investigación y Doctorado, FCE, UBA, Ciudad Autónoma de 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. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0817_EscobarDS.pdf

Escobar, D. S. (2017). Ciberseguridad documental de los sistemas contables legales. XI Congreso Internacional de Economía y Gestión. UBA, CABA.

Escobar, D. S. (2017). Concientización y capacitación del educando en la criticidad de la información contable en el ámbito de la práctica profesional. XXXIX SIMPOSIO DE PROFESORES DE PRÁCTICA PROFESIONAL. UNIVERSIDAD NACIONAL DE CATAMARCA, San Fernando del Valle de Catamarca.

Escobar, D. S. (2017). Formación del contador público en tecnología y seguridad de la información: Propuesta de reforma curricular. (Trabajo Final de Posgrado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tpos/1502-1116_EscobarDS.pdf

Escobar, D. S. (2018). Replanteo en el análisis de las contingencias, oportunidades y amenazas de los desvíos en los Estados Financieros Prospectivos. Gestión Joven, (18), 11.

Escobar, D. S. (2019). Repensando la seguridad de los registros contables. I jornada de Ciberseguridad del Consejo Profesional en Ciencias Económicas. Consejo Profesional en Ciencias Económicas, CABA.

Escobar, D. S. (2022). Análisis de los modelos de gestión de Ciberseguridad en la elaboración de planes de concientización y capacitación para Contadores Públicos. Publicaciones de la Comisión de Estudios sobre Sistemas de Registro, (2-5), 1-7.

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

Escobar, D. S. (2022). Identificación de los elementos para la descripción de un Modelo contable alternativo para el tratamiento de los activos de información. Sexta Jornada de Investigación Contable, Ética e Innovación: La Obra de Carlos Luis García Casella. Universidad de Buenos Aires - Facultad de Ciencias Económicas, Buenos Aires.

Escobar, D. S. (2022). Identificación de los elementos para la descripción de un Modelo contable alternativo para el tratamiento de los activos de información. Sexta Jornada de Investigación Contable, Ética e Innovación: La Obra de Carlos Luis García Casella. Universidad de Buenos Aires - Facultad de Ciencias Económicas, Buenos Aires.

Escobar, D. S. (2022). Identificación de los riesgos de los registros contables alojados en servicios de computación en la nube. XLIII Simposio Nacional de Profesores de Práctica Profesional. UNCUYO, Mendoza.

Escobar, D. S. (2022). Propuesta de un modelo contable que refleje el carácter de activo que la información corporativa representa para una entidad bancaria. (Tesis de Doctorado. Universidad de Buenos Aires.) Recuperado de http://bibliotecadigital.econ.uba.ar/download/tesis/1501-1323_EscobarDS.pdf

Escobar, D. S. (2022). Universo o dominio del discurso contable de los activos de información. ECON 2022. UBA, 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.