FORTALECIMIENTO DE COMPETENCIAS DOCENTES EN GESTIÓN DE RIESGOS DE TI, CIBERSEGURIDAD Y CONTINUIDAD DE NEGOCIOS: UNA EXPERIENCIA PRÁCTICA PARA LA ENSEÑANZA UNIVERSITARIA

Sandra M. Corrales[1], Marcelo A. García[2]

[1] Facultad de Ciencias Económicas, Sociales y Jurídicas, Universidad Nacional de Salta, Av. Bolivia 5150, CP 4400, Ciudad de Salta, Argentina
[2] Facultad de Ciencias Económicas, Universidad Nacional de Tucumán, Av. Independencia 1900, CP 4000, San Miguel de Tucumán, Argentina

[1]scorrales@eco.unsa.edu.ar, [2]mgarcia@face.unt.edu.ar

Resumen. El trabajo presenta una experiencia de formación docente en gestión de riesgos de TI, ciberseguridad y continuidad de negocios, desarrollada en el marco del Programa de Producción y Colaboración Académica – Colaboratorio DUTI. La propuesta consistió en un taller destinado a docentes universitarios de carreras de Ciencias Económicas, con el fin de fortalecer sus competencias en la identificación, evaluación y tratamiento de riesgos tecnológicos, así como en la planificación de la continuidad operativa ante incidentes de seguridad. La intervención se estructuró en dos encuentros teórico-prácticos. En el primero, los participantes trabajaron con estándares internacionales (ISO 31000 [1], ISO 27005 [2], National Institute of Standards and Technology - NIST, Instituto Nacional de Estándares y Tecnología - SP 800-30 [3]) y elaboraron una matriz de riesgos simplificada. En el segundo, diseñaron un plan de continuidad de negocios básico, aplicando los principios de la ciberresiliencia. Posteriormente, parte de este material se aplicó en la asignatura "Seguridad y Control en Sistemas Informáticos" de la Universidad Nacional de Tucumán, con resultados positivos en el aprendizaje estudiantil. Los autores destacan que los casos prácticos y la bibliografía propuesta constituyen recursos transferibles a distintas universidades, favoreciendo una enseñanza más contextualizada y orientada a la formación de profesionales preparados para enfrentar los desafíos de la seguridad digital.

Palabras clave: aplicación práctica, gestión de riesgos de TI, ciberseguridad, continuidad de negocios

1 INTRODUCCIÓN

En el marco del "Programa de Producción y Colaboración Académica - Colaboratorio DUTI", se llevó a cabo un taller dirigido a docentes universitarios en sistemas y

tecnologías de la información, con el objetivo de fortalecer sus competencias en Gestión de Riesgos de TI, Ciberseguridad y Continuidad de Negocios. Este taller tiene una relevancia significativa debido al creciente protagonismo que los riesgos tecnológicos y la seguridad de la información tienen en la gestión organizacional, especialmente en un contexto universitario. La propuesta didáctica desarrollada durante el taller busca formalizar una metodología de enseñanza práctica que pueda ser implementada en las facultades de Ciencias Económicas del país, específicamente en las carreras de Contador Público y Licenciatura en Administración.

2 PLANIFICACIÓN DE LA INTERVENCIÓN Y DE SU SEGUIMIENTO

2.1 Objetivo general

Presentar una propuesta didáctica basada en talleres de formación docente en gestión de riesgos de TI, ciberseguridad y continuidad de negocios, con el fin de evidenciar su impacto en el fortalecimiento de competencias docentes y en la generación de recursos prácticos transferibles a la enseñanza universitaria en ciencias económicas.

2.2 Objetivos específicos

- Fortalecer las competencias docentes en gestión de riesgos de TI, ciberseguridad y continuidad de negocios mediante actividades teórico-prácticas.
- Desarrollar y aplicar casos prácticos transferibles a la enseñanza universitaria en ciencias económicas.
- Propiciar la colaboración académica entre docentes de distintas universidades, favoreciendo la innovación pedagógica y el intercambio de buenas prácticas.

3 METODOLOGÍA

El trabajo se enmarca en una metodología de investigación–acción educativa, entendida como un proceso que combina la intervención práctica con la reflexión sistemática para generar conocimiento aplicable al ámbito docente. En este caso, la acción consistió en el diseño y desarrollo de talleres de formación en gestión de riesgos de TI, ciberseguridad y continuidad de negocios, dirigidos a docentes universitarios de carreras de Ciencias Económicas.

Los talleres se estructuraron en dos encuentros teórico–prácticos. En el primero, se abordaron conceptos y marcos normativos internacionales (ISO 31000, ISO 27005, NIST SP 800-30) y se aplicaron a través de una matriz simplificada de gestión de riesgos. En el segundo, se trabajó sobre la seguridad de la información y la continuidad de negocios, elaborando un plan básico orientado a la ciberresiliencia institucional.

La investigación–acción permitió que los participantes no fueran meros receptores de contenidos, sino protagonistas en la construcción de soluciones prácticas y transferibles al aula. La evaluación se realizó a partir de la participación activa de los docentes,

de la producción de casos prácticos y de la posterior aplicación de los materiales en la enseñanza universitaria, lo que aportó evidencias sobre el fortalecimiento de competencias y la colaboración académica entre instituciones.

4 RESULTADOS

4.1 Desarrollo del taller

La intervención se estructuró en dos encuentros teórico-prácticos, en los cuales se combinaron conceptos y ejercicios de aprendizaje.

El primer encuentro se centró en la introducción a la gestión de riesgos de TI, la identificación y valoración de riesgos, y su tratamiento. Se presentaron los principales estándares internacionales como ISO 31000 [1], ISO 27005 [2] y NIST SP 800-30 [3], así como metodologías para la identificación de amenazas y vulnerabilidades. Se discutieron estrategias de tratamiento de riesgos, junto con controles de seguridad organizacionales, físicos y tecnológicos.

El segundo encuentro abordó la gestión de la seguridad de la información, con un enfoque en la triada CID (Confidencialidad, Integridad, Disponibilidad) y la gestión de la continuidad del negocio. Se introdujo el Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001[4] y el Sistema de Gestión de Continuidad del Negocio (SGCN) conforme a ISO 22301 [5].

En ambos encuentros, se planteó un caso de aplicación práctica para afianzar los aspectos teóricos abordados.

Para el primer encuentro, la aplicación práctica consistió en identificar riesgos en un caso de estudio proporcionado, utilizando una matriz simplificada. Este ejercicio permitió a los participantes evaluar amenazas y vulnerabilidades, asignar probabilidades e impactos, y finalmente proponer estrategias para el tratamiento de los riesgos identificados. Los asistentes pudieron experimentar de primera mano el proceso de gestión de riesgos de TI, aplicando marcos de cumplimiento y metodologías discutidas durante el taller.

Este ejercicio fue sistematizado posteriormente en una Guía de Trabajo Práctico que puede ser utilizada por docentes de distintas facultades como ficha didáctica para orientar la resolución del caso.

En el segundo encuentro, la aplicación práctica consistió en la creación de un plan de continuidad de negocios simplificado para un departamento académico ficticio. Este ejercicio se enfocó en asegurar la continuidad de las clases y la protección de datos críticos en caso de un incidente de seguridad. Esta actividad permitió a los participantes comprender la importancia de la ciberresiliencia y la necesidad de estar preparados para mantener la operatividad organizacional ante posibles incidentes.

Al igual que en el primer encuentro, el material fue organizado en una Guía de Estrategias de Continuidad, que constituye un recurso pedagógico transferible y replicable en otras instituciones universitarias.

En consecuencia, se elaboraron dos insumos de apoyo: un listado de procesos críticos frecuentes en instituciones de educación superior y un repertorio de escenarios disruptivos posibles. Estos insumos, construidos a partir del relevamiento bibliográfico y la experiencia docente, se incorporaron como materiales de referencia para enriquecer la aplicación práctica

Los indicadores de evaluación definidos para observar el cambio en las competencias de los docentes mostraron resultados positivos. Ellos manifestaron una mayor habilidad para identificar y valorar riesgos de TI, diseñar estrategias de tratamiento de riesgos, y desarrollar planes de continuidad del negocio.

Los dos casos prácticos desarrollados podrán ser utilizados en las distintas unidades de estudio de universidades del país, específicamente en las carreras de Contador Público y Licenciatura en Administración. Los casos permitirán a los estudiantes aplicar los conceptos de gestión de riesgos de TI, ciberseguridad y continuidad de negocios en escenarios reales, reforzando así los contenidos teóricos abordados en las asignaturas.

Además de las aplicaciones prácticas, se presentará bibliografía de consulta sobre los temas abordados durante el taller.

Finalmente, se hace hincapié en que los resultados del taller no solo evidencian una mejora en las competencias de los docentes en gestión de riesgos de TI, ciberseguridad y continuidad de negocios, sino que también proporcionan herramientas prácticas que podrán ser utilizadas en el aula para enriquecer la formación de los estudiantes. Los casos prácticos y los apuntes desarrollados serán recursos valiosos para las instituciones universitarias del país, contribuyendo a la formación de profesionales capaces de enfrentar los desafíos de la ciberseguridad en un mundo cada vez más digitalizado.

4.2 Recursos didácticos producidos

Un aporte relevante del trabajo, además del desarrollo del taller y de su aplicación en el aula, es la elaboración de recursos didácticos diseñados por los autores para facilitar la enseñanza de la gestión de riesgos de TI y de la continuidad operativa. Estas fichas fueron construidas a partir de la sistematización bibliográfica y de la propia experiencia docente, y posteriormente enriquecidas durante el taller con los aportes y la práctica de los docentes participantes. Su inclusión como insumos pedagógicos constituye un resultado en sí mismo, dado que amplía el impacto de la propuesta al poner a disposición de otros docentes materiales listos para ser utilizados en la formación académica.

Objetivo: Identificar y evaluar los riesgos asociados con los activos críticos de una unidad académica universitaria	**Unidad Académica**: (*Dirección de Alumnos, Dirección de Títulos y otras*)
Identificación de Activos Críticos (AC): (reconozcan los principales activos críticos de la unidad seleccionada)	*Datos estudiantiles, sistemas de gestión académica, infraestructura de red*
Análisis de Amenazas y Vulnerabilidades: (efectúen un modelado de amenazas e identifiquen las vulnerabilidades sobre los AC)	*Ciberataques, fallas de seguridad física*
Evaluación de Riesgos: (evalúen los riesgos utilizando un método cualitativo o cuantitativo)	*Probabilidad y el impacto de cada riesgo identificado*
Tratamiento de Riesgos: (especifiquen el tipo de tratamiento para cada riesgo. Si se "mitiga", seleccione controles adecuados tomando como referencia el Anexo A de ISO 27001. Establezcan el riesgo residual para cada caso)	

Fig. 1. Ficha de trabajo práctico para la gestión de riesgos de TI en una unidad académica. Fuente: Elaboración propia de los autores, con adaptación del editor para su presentación en formato de ficha.

Objetivo: Identificar escenarios disruptivos y proponer estrategias de continuidad operativa para procesos críticos en una unidad académica universitaria.	**Unidad Académica**: (*Dirección de Alumnos, Dirección de Títulos y otras*)
Análisis de Impacto en el Negocio (BIA): (realicen un listado de los tres principales procesos críticos)	**Procesos Críticos** *(Complete junto a criticidad por juicio de expertos)*
Identificación de escenarios disruptivos: (identifiquen posibles escenarios disruptivos que podrían afectar la continuidad de las operaciones)	*(por ejemplo, ciberataques, fallas de infraestructura)*
	(Identifiquen el impacto o las consecuencias para la institución)

Fig. 2. Ficha de trabajo práctico para la elaboración de estrategias de continuidad operativa en una unidad académica. Fuente: Elaboración propia de los autores, con adaptación del editor para su presentación en formato de ficha.

Tabla 1. Procesos críticos frecuentes en instituciones de educación superior

Unidad Académica	Proceso Crítico
Asuntos Académicos	– Gestión de matrículas y reinscripciones de estudiantes – Registro y actualización de datos estudiantiles – Administración de planes de estudio y carga académica – Turnos regulares de exámenes
Gestión Administrativa	– Elaboración y ejecución del presupuesto anual – Control de ingresos y egresos – Gestión de pagos a proveedores y personal docente
Infraestructura Tecnológica y Redes	– Mantenimiento y actualización de la red informática – Gestión de servidores y bases de datos académicas – Soporte técnico y atención a incidentes de TI
Planificación y Desarrollo Curricular	– Diseño y revisión de planes de estudios – Coordinación de actividades académicas y eventos – Evaluación y mejora continua de programas académicos
Relaciones Institucionales y Comunicación	– Comunicación interna y externa – Relaciones con otros departamentos y universidades – Relaciones Internacionales e intercambio estudiantil – Gestión de eventos académicos y conferencias
Personal	– Contratación y gestión del personal académico y administrativo – Desarrollo profesional y capacitación continua – Administración de nóminas y beneficios laborales

Fuente: Elaboración propia de los autores, con adaptación del editor para su presentación en formato de ficha

Tabla 2. Escenarios disruptivos posibles en instituciones de educación superior

Tipo Escenario	Escenario Disruptivo
Ciberataque a la Infraestructura Tecnológica	– Interrupción de la red informática y sistemas académicos – Pérdida de datos estudiantiles y académicos – Bloqueo de acceso a sistemas clave para la gestión académica y administrativa
Falla del Sistema de Gestión Administrativa	– Error crítico en la ejecución del presupuesto anual – Pérdida o corrupción de datos financieros – Incapacidad para realizar pagos a proveedores o personal docente
Desastre Natural	– Inundación o incendio en instalaciones universitarias – Daño a equipos informáticos y documentación física – Interrupción de las actividades académicas y administrativas por tiempo indefinido
Pandemia o Crisis de Salud Pública	– Brotes de enfermedades contagiosas entre estudiantes y personal (COVID o Dengue) – Necesidad de implementar medidas de distanciamiento social – Impacto en la continuidad de las clases presenciales y administración académica
Problemas de Suministro Energético	– Apagones prolongados que afectan la disponibilidad de sistemas informáticos – Incapacidad para mantener operativos los equipos esenciales – Interrupción de actividades académicas y administrativas por falta de energía eléctrica
Ataques Físicos o Vandalismo	– Daños a la infraestructura física de la facultad – Robo o destrucción de equipos tecnológicos – Interrupción de las actividades diarias y posibles riesgos para la seguridad física de estudiantes y personal

Fuente: Elaboración propia de los autores, con adaptación del editor para su presentación en formato de ficha

4.3 Aplicación en el Aula

En el marco de la asignatura "Seguridad y Control en Sistemas Informáticos" de la Facultad de Ciencias Económicas de la Universidad Nacional de Tucumán, se desarrolló una actividad práctica destinada a fortalecer las competencias de los alumnos en la Gestión de Riesgos de TI. La actividad fue realizada el 03 de septiembre de 2024, cuando una docente de la Universidad Nacional de Salta dictó una clase presencial sobre esta temática. La clase utilizó como base el material desarrollado en el colaboratorio

DUTI, adaptándolo a la realidad académica y profesional de los estudiantes de la institución.

El enfoque pedagógico de la clase se centró en proporcionar a los alumnos herramientas y conocimientos prácticos aplicables a escenarios reales en la gestión de riesgos tecnológicos. Posteriormente, los estudiantes participaron en una actividad de aplicación práctica, donde, utilizando los conceptos abordados en la clase, debieron identificar y evaluar riesgos tecnológicos en la unidad académica. Como parte de las consignas, se aclaró que para la resolución de los ejercicios podían apoyarse en diferentes recursos: en el caso de la gestión de riesgos de TI, se permitía utilizar herramientas de inteligencia artificial o el modelo de referencia del Instituto Nacional de Ciberseguridad de España (INCIBE); en la elaboración de estrategias de continuidad, se sugería considerar tanto los procesos críticos previamente sistematizados como los escenarios disruptivos propuestos, además de apoyarse en IA, en documentos de INCIBE y en informes de la European Union Agency for Cybersecurity (ENISA, Agencia de Ciberseguridad de la Unión Europea). Estas aclaraciones reforzaron la dimensión práctica de la actividad, al ofrecer guías y fuentes diversas sin reemplazar el análisis crítico que debían realizar los estudiantes.

El temario detallado de esta actividad se adjunta en el anexo de este trabajo. Los resultados obtenidos fueron altamente positivos. Los estudiantes demostraron una mejora en su capacidad para identificar, analizar y tratar riesgos tecnológicos, lo que evidencia el impacto formativo del taller. Asimismo, la experiencia de colaboración entre docentes de distintas universidades fue enriquecedora, promoviendo un intercambio académico significativo que contribuyó al fortalecimiento de las competencias docentes y estudiantiles.

En resumen, la aplicación de esta metodología en el aula no solo facilitó la transferencia de conocimientos teóricos, sino que también consolidó el aprendizaje práctico de los alumnos, integrando de manera efectiva los contenidos en la formación profesional de futuros contadores públicos y licenciados en administración.

4.4 Material de Consulta

Entre los materiales disponibles para profundizar en la temática se destacan documentos elaborados por el INCIBE [6 – 8] y por la Information Systems Audit and Control Association (ISACA [9], Asociación de Auditoría y Control de Sistemas de Información), los cuales constituyen marcos de referencia relevantes para la gestión de riesgos de TI, la ciberseguridad y la continuidad de negocios:

- INCIBE (2017). Gestión de Riesgos: Una guía de aproximación para el empresario. España.
- INCIBE (s.f.). Plan de Contingencia y Continuidad de Negocio. España.
- INCIBE (2024). Continuidad de Negocio: Políticas de Seguridad para la Pyme. España.
- ISACA (2009). Marco de Riesgo de TI. EEUU.

5 CONCLUSIONES

El taller de Gestión de Riesgos de TI, Ciberseguridad y Continuidad de Negocios realizado en el marco del "Programa de Producción y Colaboración Académica - Colaboratorio DUTI" ha demostrado ser una herramienta eficaz para fortalecer las competencias de los docentes universitarios en estas áreas críticas. La metodología aplicada, que combinó teoría y práctica a través de ejercicios interactivos, facilitó la comprensión y aplicación de los conceptos, permitiendo a los docentes integrar estos conocimientos en sus programas de estudio.

El desarrollo de casos prácticos específicos para cada encuentro del taller resultó especialmente efectivo. En el primer encuentro, el ejercicio de identificación y tratamiento de riesgos mediante una matriz simplificada permitió a los docentes experimentar el proceso de gestión de riesgos de TI de manera tangible. En el segundo encuentro, la identificación de estrategias de continuidad ante escenarios disruptivos proporcionó una visión clara de la importancia de la ciber resiliencia y la preparación ante incidentes de seguridad.

Las limitaciones encontradas incluyen la diversidad en el nivel de conocimientos previos de los participantes, lo que requirió una adaptación del contenido y las actividades. Además, la duración del taller podría ser ampliada para abordar con mayor profundidad algunos temas específicos y permitir una práctica más exhaustiva de los casos.

Las recomendaciones para futuros trabajos incluyen la realización de talleres más extensivos, con módulos adicionales que aborden áreas complementarias. Asimismo, se sugiere la creación de una red de colaboración entre los docentes participantes, para fomentar el intercambio de buenas prácticas y la actualización continua en estos temas.

Los casos prácticos desarrollados, junto con la bibliografía recomendada, serán recursos valiosos para las instituciones universitarias del país. Estos materiales permitirán a los docentes enriquecer sus clases y proporcionar a los estudiantes una formación más práctica y aplicada en gestión de riesgos de TI, ciberseguridad y continuidad de negocios.

Se considera que la propuesta didáctica presentada en este trabajo no solo ha mejorado la formación de los docentes, sino que también ha sentado las bases para la implementación de una enseñanza más efectiva y contextualizada en las facultades de ciencias económicas del país. Esta iniciativa contribuirá significativamente a la formación de futuros profesionales capaces de enfrentar los desafíos de la ciberseguridad en un mundo cada vez más digitalizado.

Finalmente, se hace referencia a la experiencia llevada a cabo en el aula, bajo la modalidad presencial. La implementación de la metodología desarrollada en el taller del colaboratorio DUTI, aplicada en el marco de la asignatura "Seguridad y Control en Sistemas Informáticos", demostró ser una herramienta pedagógica efectiva para el fortalecimiento de competencias clave en gestión de riesgos de TI, ciberseguridad y continuidad de negocios. Los resultados positivos obtenidos, tanto en el desempeño de los alumnos como en la colaboración académica entre instituciones, resaltan la relevancia de integrar enfoques prácticos y colaborativos en la enseñanza universitaria. Esta experiencia ha permitido consolidar un modelo de enseñanza aplicable en las facultades de

Ciencias Económicas del país, contribuyendo a la formación de los futuros profesionales en ciencias económicas, en esta temática.

6 REFERENCIAS BIBLIOGRÁFICAS

1. IRAM, Instituto Argentino de Normalización y Certificación (2018). Norma ISO 31000. Gestión del riesgo. Principios y directrices. Buenos Aires, Argentina.
2. IRAM, Instituto Argentino de Normalización y Certificación (2021). Norma ISO 27002. Tecnología de la información. Técnicas de seguridad. Código de buenas prácticas para los controles de la seguridad de la información. Buenos Aires, Argentina.
3. ISO/IEC (2022). ISO/IEC 27001. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. Buenos Aires, Argentina: Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad (IRAM).
4. ISO/IEC (2019). ISO/IEC 22301. Seguridad y resiliencia. Sistemas de gestión de continuidad del negocio. Requisitos. Buenos Aires, Argentina: Subcomité de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad (IRAM).
5. National Institute of Standards and Technology (NIST) (2012). Guide for Conducting Risk Assessments (SP 800-30, Revision 1). Gaithersburg, MD: U.S. Department of Commerce.
6. INCIBE (Instituto Nacional de Ciberseguridad de España) (2017). Gestión de Riesgos: Una guía de aproximación para el empresario. León, España.
7. INCIBE (Instituto Nacional de Ciberseguridad de España) (s.f.). Plan de Contingencia y Continuidad de Negocio. León, España.
8. INCIBE (Instituto Nacional de Ciberseguridad de España) (2024). Continuidad de Negocio: Políticas de Seguridad para la Pyme. León, España.
9. ISACA (Information Systems Audit and Control Association) (2009). Marco de Riesgos de TI. Rolling Meadows, IL, USA.