Agosto 2025

Universidad de Puerto Rico
Recinto de Río Piedras
Facultad de Administración de Empresas
Instituto de Estadística y Sistemas Computadorizados de Información

SICI 4275

PRONTUARIO

I. Título:
Controles y Seguridad en los Sistemas Computadorizados de Información

II. Codificación del curso:
SICI 4275

III. Cantidad de horas/crédito:
Tres créditos, tres horas semanales de reunión, un semestre

IV. Pre-requisito:
SICI 4015, SICI 4266 ó SICI 4405; SICI 4278

V. Co-requisito:
ADMI 4417

VI. Descripción del curso:

Estudio de las medidas de control y seguridad que deben existir en las operaciones de sistemas de una organización, y de las medidas para recuperarse en caso de ocurrir incidentes que provoquen pérdidas en los datos y en los recursos de informática.

Orientación hacia la preparación de un plan de recuperación en caso de desastres.

VII. Objetivos de aprendizaje:

Objetivos Generales:

1. Valorará la protección de los recursos de sistemas en una organización e identificará maneras en que esta protección puede lograrse.
2. Identificará factores de riesgo en los sistemas de información y evaluará las implicaciones de dichos factores.

3. Preparará un plan de recuperación en casos de desastres para las operaciones de sistemas de información de una organización.
4. Identificará y evaluará aspectos éticos, de relaciones interpersonales, de comunicación efectiva y de trabajo en equipo relacionados con labores típicas de un profesional de sistemas, como la adquisición de recursos de informática y la estimación del tiempo que toma llevar a cabo tareas que le han sido asignadas.

Objetivos Específicos:

En este curso, el estudiante:

1. Aprenderá a diseñar una estructura de controles para Sistemas de Información.
2. Se familiarizará con las herramientas disponibles en el mercado para llevar a cabo pruebas como parte de las auditorias de Sistemas de Información.
3. Conocerá los estándares y pronunciamientos relevantes a los controles, la seguridad y la ética en los Sistemas de Información.
4. Se familiarizará con las organizaciones que emiten pronunciamientos y estándares relevantes al área de Sistemas de Información.
5. Conocerá las herramientas utilizadas para recopilar datos sobre los controles y la seguridad en los Sistemas de Información.
6. Aprenderá los conceptos, relevantes al curso, que se cubren en el examen para la Certificación como Auditor de Sistemas de Información.
7. Aprenderá a preparar planes para la recuperación de las funciones de informática en caso de un desastre.
8. Comprenderá la importancia de la ética en su desempeño profesional e identificará áreas de su profesión en las que los aspectos éticos requieren atención especial.

VIII. Texto:

Otero, A. (2019) *Information Technology Control and Audit*, Fifth Edition, CRC Press. (ISBN-10: 1498752284) (ISBN-13: 978-1-4987-5228-2)

IX. Bosquejo de contenido y distribución de tiempo:

TEMA	HORAS
1. Aspectos Introductorios a) La Necesidad de Controles Internos Especializados para Sistemas de Información b) La Necesidad de Llevar a Cabo Análisis sobre los Controles en los Sistemas de Información c) La Importancia de la Ética en los Sistemas de Información d) Discusión de Otros Conceptos Básicos	3
2. Controles Internos Especializados para el Área de Sistemas de Información a) Controles Administrativos, Gerenciales y Operacionales b) Controles Ambientales y Físicos c) Controles para el área de Desarrollo de Sistemas d) Controles para el Área de Manejo de Datos e) Controles de Aplicación f) Controles para Nuevas Tecnologías g) Otros Controles	15
3. El Análisis de los Controles en los Sistemas de Información a) Pasos a Seguir b) Análisis de Riesgo c) Estándares y Pronunciamientos Relevantes d) Programas, Herramientas y Técnicas	4.5
4. Herramientas para las Pruebas a ser Llevadas a cabo Durante los Análisis de los Controles en los Sistemas de Información	3
5. La Profesión de Auditor de Sistemas de Información a) Organizaciones Profesionales b) Estándares y Pronunciamientos c) Certificaciones Profesionales d) Oportunidades de Desarrollo Profesional y de Empleo	3
6. Organización y Administración de la Función de Auditoría de Sistemas de Información	3
7. Planificación para Casos de Desastre	6
8. Proyecto sobre la planificación para casos de desastres	3
Tres Exámenes	4.5
TOTAL DE HORAS	**45**

X. Estrategias instruccionales:

A. Lista mínima de estrategias instruccionales

1. Estrategia instruccional principal:

a. El curso enfatizará el enfoque de “Project Based Learning”. Los estudiantes practicarán los conceptos y las técnicas mayormente mediante ejercicios y proyectos, como una manera de profundizar en el aprendizaje y de apoyar el desarrollo de un nivel adecuado de destreza. Muchas de las actividades de práctica se llevarán a cabo en el salón de clases. Otras se llevarán a cabo en sesiones fuera del salón de clases supervisadas por el profesor.

2. Otras estrategias instruccionales:

a. Conferencias por el profesor.

b. Lecturas asignadas.

c. La participación activa de los estudiantes es muy importante para lograr los objetivos del curso. El profesor deberá promover dicha participación.

d. Las estrategias instruccionales incluirán el uso de la tecnología para apoyar y hacer más efectivo y eficiente el proceso de enseñanza y aprendizaje. Por ejemplo, se utilizarán proyectores digitales para presentar el material a ser discutido. Además, se utilizará el acceso a Internet para presentar material que ilustre los temas discutidos.

e. El profesor enfatizará los aspectos funcionales de los conceptos y de las técnicas estudiadas, pero sin descuidar los aspectos teóricos.

f. La preparación de asignaciones individuales y grupales fuera del salón de clase será una parte importante de las estrategias instruccionales de este curso.

g. Presentaciones orales

El curso podrá tener hasta un máximo de 11.25 horas en modalidad alterna.

XI. Recursos de aprendizaje o instalaciones mínimas disponibles o requeridos:

A. El estudiante debe tener acceso a una computadora personal durante el tiempo de reunión del curso y fuera de este horario, sea en un laboratorio de computadoras o en su casa.

B. La computadora personal debe tener micrófono, bocinas y cámara de video y los siguientes programas de computadora: procesador de palabras, hoja de cálculo, editor de presentaciones y sistema para la administración de bases de datos.

C. Acceso de alta velocidad a la Internet, especialmente durante el tiempo de reunión del curso.

D. Acceso a su cuenta de correo electrónico institucional.

E. Acceso a la plataforma de educación a distancia requerida (e.g. Moodle).

F. Acceso a la plataforma de reuniones virtuales requerida (e.g. Zoom).

XII. Estrategias de evaluación:

Exámenes y Pruebas Corta	70%
Asignaciones y Casos	10%
Proyecto Final y Presentación	20%
Total	100%

XIII. Estrategias de Avalúo

Se utilizará la estrategia de avalúo orientada a la creación de un proyecto final.

XIV. Sistema de Calificación:

Se utilizará la curva estándar.

100% - 90%	A
89% - 80%	B
79% - 70%	C
69% - 60%	D
59% - 0%	F

NO HAY CURVA

XV. Acomodo Razonable:

"La Universidad de Puerto Rico (UPR) reconoce el derecho que tienen los estudiantes con impedimentos a una educación post secundaria inclusiva, equitativa y comparable. Conforme a su política hacia los estudiantes con impedimentos, fundamentada en la legislación federal y estatal, todo estudiante cualificado con impedimentos tiene derecho a la igual participación de aquellos servicios, programas y actividades que están disponibles de naturaleza física, mental o sensorial y que por ello se ha afectado, sustancialmente, una o más actividades principales de la vida como lo es su área de estudios post secundarios, tiene derecho a recibir acomodos o modificaciones razonables. De usted requerir acomodo o modificación razonable en este curso, debe notificarlo al profesor sobre el mismo, sin necesidad de divulgar su condición o diagnóstico. De manera simultánea, debe solicitar a la Oficina de Servicios a Estudiantes con Impedimentos (OSEI) de la unidad o Recinto, en forma expedita, su necesidad de modificación o acomodo razonable."

XVI. Integridad Académica:

«La Universidad de Puerto Rico promueve los más altos estándares de integridad académica y científica. El Artículo 6.2 del Reglamento General de Estudiantes de la UPR (Certificación 13, 2009-2010, de la Junta de Síndicos) establece que "la deshonestidad académica incluye, pero no se limita a: acciones fraudulentas, la obtención de notas o grados académicos valiéndose de falsas o fraudulentas simulaciones, copiar total o parcialmente la labor académica de otra persona, plagiar total o parcialmente el trabajo de otra persona, copiar total o parcialmente las respuestas de otra persona a las preguntas de un examen, haciendo o consiguiendo que otro tome en su nombre cualquier prueba o examen oral o escrito, así como la ayuda o facilitación para que otra persona incurra en la referida conducta". Cualquiera de estas acciones estará sujeta a sanciones disciplinarias en conformidad con el procedimiento disciplinario establecido en el Reglamento General de Estudiantes de la UPR vigente. Para velar por la integridad y seguridad de los datos de los usuarios, todo curso híbrido, a distancia y en línea deberá ofrecerse mediante la plataforma institucional de gestión de aprendizaje o por herramientas requeridas por el curso, la cual utiliza protocolos seguros de conexión y autenticación. El sistema autentica la identidad del usuario utilizando el nombre de usuario y contraseña asignados en su cuenta institucional. El usuario es responsable de mantener segura, proteger, y no compartir su contraseña con otras personas».

Política de Integridad Académica de la Universidad de Puerto Rico, Recinto de Río Piedras: Certificación Núm. 64 Año Académico 2022-2023 del Senado Académico: La Universidad de Puerto Rico promueve los más altos estándares de integridad académica y científica. El Recinto de Río Piedras de la Universidad de Puerto Rico (UPRRP) está comprometido con mantener y promover un ambiente intelectual y ético basado en los principios de integridad y rigor académico, confianza, respeto mutuo y diálogo sereno entre las personas de la comunidad universitaria esenciales para el logro de su misión. La integridad implica la firme adherencia a un conjunto de valores éticos fundamentales, tales

como la honestidad, el respeto y la responsabilidad. La integridad académica es parte, no solo de la enseñanza y el aprendizaje, sino de las relaciones e interacciones consustanciales al proceso educativo, investigativo y administrativo. Debe permear todos los ámbitos de la vida y la comunidad universitaria. Esta Política de Integridad Académica (de ahora en adelante Política) se sostiene en el quehacer académico compartido entre los integrantes de la comunidad universitaria al promulgar y afianzar estos valores mediante la educación, el diálogo y la prevención. Se enfoca, principalmente, en el ámbito estudiantil en el proceso de enseñanza y aprendizaje y la investigación. Sin embargo, la integridad académica atañe a todos los integrantes de la comunidad universitaria: estudiantes, personal docente y no docente. https://senado.uprrp.edu/wp-content/uploads/2023/01/CSA-64-2022-2023.pdf

XVII. Política y Procedimiento Para El Manejo De Situaciones De Discrimen Por Sexo o Género En La Universidad De Puerto Rico:

La Política y procedimientos para el manejo de situaciones de discrimen por sexo o género en la Universidad de Puerto Rico, Certificación 107 (2021-2022) de la Junta de Gobierno, asegura que la Universidad de Puerto Rico, como institución de educación superior y centro laboral, protege los derechos y ofrece un ambiente seguro a todas las personas que interactúan en ella, ya sea a estudiantes, empleados, contratistas o visitantes. La misma tiene como fin promover un ambiente de respeto a la diversidad y los derechos de los integrantes de la comunidad universitaria y establece un protocolo para el manejo de situaciones relacionadas con las siguientes conductas prohibidas: discrimen por razón de sexo, género, embarazo, hostigamiento sexual, violencia sexual, violencia doméstica, violencia en cita y acecho, en el ambiente de trabajo y estudio.

XVIII. Diversidad, Equidad e Inclusión

La Universidad de Puerto Rico asume el compromiso de establecer un entorno que valore la diversidad, promueva la equidad y aspire a la inclusión plena de toda su comunidad universitaria. Los cursos se ofrecerán promoviendo un ambiente inclusivo y equitativo, garantizando la participación de estudiantes con diversas trayectorias, experiencias y habilidades. Así, la Universidad de Puerto Rico reitera su dedicación al cumplimiento de los principios de diversidad, equidad e inclusión en sus programas académicos.

XIX. Plan De Contingencia En Caso De Surgir Una Emergencia o Interrupción De Clases:

En caso de surgir una emergencia o interrupción de clases, el profesor se comunicará con los estudiantes vía correo electrónico institucional u otros medios disponibles para coordinar la continuidad del ofrecimiento.

El plan de contingencia debe preservar la modalidad en la que el curso fue creado y programado en la oferta académica.

XX. Bibliografía:

(2006). *FIPS 200 – Minimum Security Requirements for Federal Information and Federal Information Systems*, Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. (*https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf*)

(2012). *NIST Special Publication 800-30 Rev. 1 – Guide for Conducting Risk Assessments*, Joint Task Force Transformation Initiative, National Institute of Standards and Technology. *(https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf)*

(2015). *CISA Review Manual*, 26th Edition. , Information Systems Audit and Control Association.

(2018). *Framework for improving Critical Infrastructure Cybersecurity V1.1*, National Institute of Standards and Technology. *(https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf)*

(2019). *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*, Information Systems Audit and Control Association.

(2019). *COBIT 2019 Framework: Governance & Management Solutions*, Information Systems Audit and Control Association.

(2019). *COBIT 2019 Implementation Guide*, Information Systems Audit and Control Association.

(2019). *COBIT 2019 Framework: Introduction & Methodology*, Information Systems Audit and Control Association.

(2020). *NIST Special Publication 800-53 Rev. 5 – Security and Privacy Controls for Information Systems and Organizations*, Joint Task Force, National Institute of Standards and Technology. *(https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final)*

(2021). *Internet Crime Report 2020*. Internet Crime Complaint Center at the Federal Bureau of Investigation.

(2021). *Internet Elder Fraud Report 2020*. Internet Crime Complaint Center at the Federal Bureau of Investigation.

Baxter, C. (2021). *IT Audit in Practice: Survival When You are Small - Business Continuity and Resilience*, ISACA Journal, Vol.3, pp. 3-11. Information Systems Audit and Control Association.

Bonin, B. (2020). *Pandemic-Driven Remote Working and Risk Management Strategies*, ISACA Journal, Vol.5, pp. 25-29. Information Systems Audit and Control Association.

Curtis, B. (2020). *Are Organizations Actually Performing Risk-Based Audits?*, ISACA Journal, Vol.4, pp. 1-5. Information Systems Audit and Control Association.

Harisaiprasad, K. (2020). *Addressing Risk Using the New Enterprise Security Risk Management Cycle*, ISACA Journal, Vol.5, pp. 1-5. Information Systems Audit and Control Association.

Lacey, D. (2013). *Advanced Persistent Threats: How to Manage Risk to Your Business*, Information Systems Audit and Control Association.

Marron, J., Gopstein, A. and Bogle, D. (2021). Benefits of an Updated Mapping between the NIST Cybersecurity Framework and the NERC Critical Infrastructure Protection Standards, NIST Cybersecurity White Paper. National Institute of Standards and Technology. (*https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.09292021.pdf*)

Nieles, M., Dempsey, K. & Pillitteri, V. (2017). *NIST Special Publication 800-12 Rev. 1 – An Introduction to Information Security*, National Institute of Standards and Technology. National Institute of Standards and Technology. (*https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf*)

Raval, V. & Sharma, R. (2020). *The Human Elements of Risk*, ISACA Journal, Vol.3, pp. 15-19. Information Systems Audit and Control Association.

Ross, R., Pillitteri, V., Graubart. R., Bodeau, D. & McQuaid, R. (2019). *NIST Special Publication 800-160 Vol. 2 - Developing Cyber Resilient Systems: A Systems Security Engineering Approach.* National Institute of Standards and Technology. (*https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf*)

Swanson, M., Hash, J. & Bowen, P. (2006). *NIST Special Publication 800-18 Rev. 1 – Guide for Developing Security Plans for Federal Information Systems*, National Institute of Standards and Technology. (*https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf*)

Swanson, M., Bowen, P., Wohl Phillips, A., Gallup, A. and Lynes, D. (2010). *NIST Special Publication 800-34 Rev. 1 – Contingency Planning Guide for Federal Information Systems*, National Institute of Standards and Technology. (*https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf*)