

# UNIVERSIDAD DE BUENOS AIRES

## Facultad de Ciencias Económicas

### Departamento de Sistemas

Asignatura: **SEGURIDAD INFORMÁTICA Y PRINCIPIOS DE AUDITORIA**

Código: **662**

### *Plan Vigente (\*)*

Cátedra: **Director Carrera Licenciatura en Sistemas de Información de las Organizaciones**

Carrera: (\*) Lic. en Sistemas de Información de las Organizaciones (RCS N.º 1825/24)

**Aprobado por Res. Consejo Directivo (FCE)**

**Nro.: 3492/25**

## **AUDITORIA Y SEGURIDAD DE LOS SISTEMAS DE INFORMACION**

### **A. ENCUADRE GENERAL.**

#### **A.1. CONTENIDOS MÍNIMOS.**

Gestión y técnicas de la seguridad informática. Estándares, marcos de trabajo y regulaciones. Gestión de riesgos. Amenazas, vulnerabilidades y consecuencias. Procedimientos y controles. Planes de seguridad y contingencia. Organización del área de seguridad. Criptografía. Organización del área de seguridad. Principios, objetivos y técnicas de auditoría informática. Software de seguridad y auditoría. Ciberseguridad

#### **A.2. RAZONES QUE JUSTIFICAN LA INCLUSIÓN DE LA ASIGNATURA DENTRO DEL PLAN DE ESTUDIOS. SU IMPORTANCIA EN LA FORMACIÓN PROFESIONAL.**

Por lo explicado anteriormente, seguridad se vuelven centrales en la formación de un profesional de informática. Conocer los diferentes tipos de ataques, amenazas y vulnerabilidades a los que pueden estar expuestos los sistemas informáticos, implementar medidas de seguridad para reducir los riesgos en las organizaciones, aprender las buenas prácticas de seguridad según estándares, reportar los resultados de las evaluaciones de seguridad a las partes interesadas clave, realizar seguimiento y hacer asesorar en a las organizaciones en estos temas, se vuelven conocimientos muy demandados a los profesionales. Es por esta razón que se han incorporado estos conocimientos dentro de una materia específica dedicada al tema, dentro del ciclo profesional de la Carrera.

#### **A.3. UBICACIÓN DE LA ASIGNATURA EN EL CURRÍCULUM Y REQUISITOS PARA SU ESTUDIO.**

La asignatura se encuentra ubicada en el tramo final del ciclo profesional.

Requisitos: Sistemas de Datos (Cod. 663)

#### **A.4 OBJETIVOS DE APRENDIZAJE.**

- Conocer los diferentes tipos de ataques, amenazas y vulnerabilidades a los que pueden estar expuestos los sistemas informáticos.
- Poder implementar medidas de seguridad para reducir los riesgos en las organizaciones.
- Aprender las buenas prácticas de seguridad según estándares.
- Conocer herramientas de software y aplicaciones para evaluar la seguridad.
- Conocer los procesos de gestión necesarios para desarrollar un plan de seguridad.

- Desarrollar e implementar un enfoque basado en el riesgo que cumpla con los estándares de auditoría de TI.
- Diseñar auditorías de TI específicas para verificar si los sistemas de información están protegidos, controlados y proporcionan valor a la organización.

## **B. PROGRAMA ANALÍTICO.**

### **UNIDAD TEMÁTICA I: INTRODUCCIÓN A LA SEGURIDAD DE LA INFORMACIÓN**

**Objetivos del aprendizaje:** Introducir al alumno en los conocimientos básicos de seguridad de la información.

**Contenido:**

- Integridad, confiabilidad y disponibilidad de la información. Privacidad.
- Amenazas,
- Vulnerabilidades
- Impacto. Consecuencias.
- Ciberseguridad, ciberdefensa.

### **UNIDAD TEMÁTICA II: NORMAS, ESTÁNDARES Y LEGISLACIÓN SOBRE AUDITORIA DE SISTEMAS Y SEGURIDAD DE LA INFORMACIÓN**

**Objetivos del aprendizaje:** Analizar el marco normativo y los estándares aplicables a la gestión de la seguridad y la auditoría de sistemas.

**Contenido:**

- Principales marcos de referencia, normativas y estándares de seguridad, nacionales e internacionales.
- Obligatoriedad de la aplicación de las normas según la Entidad Emisora
- Legislación nacional aplicable en seguridad de la información y protección de datos personales.
- Relación con las Normas Técnicas Profesionales

### **UNIDAD TEMÁTICA III: GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**

**Objetivos del aprendizaje:** Analizar cómo debe ser el gobierno y la gestión de la seguridad de la información.

**Contenido:**

- Gobierno de la seguridad de la información.
- Organización y estructuras del área de seguridad.
- Estrategia y políticas de seguridad de la información.
- Planes de seguridad y contingencia
- Concientización y cultura en seguridad de la información
- Sistema de Gestión de la Seguridad de la Información (SGSI).
- Justificación económica de las inversiones en seguridad.

### **UNIDAD TEMÁTICA IV: ANÁLISIS Y GESTION DEL RIESGO**

**Objetivos del aprendizaje:** Comprender la importancia de gestionar eficazmente los riesgos vinculado con el uso de tecnologías de la información.

**Contenido:**

- Conceptos generales
- Proceso de gestión de riesgos
- Desarrollo del estándar ISO/IEC 27005
- Métodos utilizados en el análisis de riesgo. Matriz de Riesgo.
- Gestión de activos de información

### **UNIDAD TEMÁTICA V: PROCEDIMIENTOS Y CONTROLES**

**Objetivos del aprendizaje:** Estudiar los diferentes procedimientos y controles que pueden aplicarse a los distintos componentes de un sistema informático.

**Contenido:**

- Clasificación de los controles. Controles generales y controles de aplicación. Importancia del Control Interno.
- Seguridad en el área de sistemas.
- Seguridad física
- Seguridad en el acceso a los sistemas
- Seguridad en el ingreso y almacenamiento de datos
- Seguridad de redes y telecomunicaciones
- Seguridad en el desarrollo de sistemas y en aplicaciones preplaneadas.
- Seguridad en el software de base
- Seguridad en las operaciones
- Seguridad en servicios tercerizados

- Criptografía
- Software de seguridad de la información

## **UNIDAD TEMÁTICA VI: AUDITORIA DE SISTEMAS**

**Objetivos del aprendizaje:** Analizar las diferentes metodologías y normas aplicables para realizar auditorías informáticas.

### **Contenido:**

- Metodologías y técnicas de auditoría.
- Auditoría de sistemas basada en riesgos.
- Normas profesionales y guías de auditoría.
- Perfil del auditor de sistemas
- El informe del auditor. Los papeles de trabajo.
- Delitos informáticos

## **C. BIBLIOGRAFÍA.**

### **C.1. BIBLIOGRAFÍA OBLIGATORIA.**

- Programa INTERREG (España – Portugal). “Manual de seguridad informática en la empresa”. 2018.
- ISO/IEC 27001:2022: La versión más reciente de la norma internacional para sistemas de gestión de seguridad de la información, publicada en octubre de 2022.
- ISO/IEC 27002:2022: Actualización de la guía de buenas prácticas para controles de seguridad de la información, también publicada en 2022.
- ISO/IEC 27007:2020: Guía para la auditoría de sistemas de gestión de seguridad de la información, revisada en 2020.
- Objetivos de Control. Directrices Generales. Modelo de Madurez. Seguridad de la Información. Versión 5.0. COBIT (Control Objectives for Information and Related Technology). IT Governance Institute. ISACA. 2019. EE UU. Castellano.
- Normas NIST SP 800-53 Rev. 5: Controles de seguridad y privacidad para sistemas de información federales en Estados Unidos, ampliamente utilizado como referencia internacional - 2020
- Raúl Saroka et. Al. Gestión de la Seguridad y Privacidad de la Información. 2015. Colegio de las Américas (Colam). Colombia.
- Fundación Telefónica, Ciberseguridad, la protección de la información en un mundo digital. 2016. Madrid (España).
- Mintic. Colombia. G.ES.05 Diseño e implementación de una estrategia de seguridad de la información. Guía Técnica, versión 1.0. 29 de abril de 2015.
- Tupia Consultores y Auditores – Administración de la Seguridad de la Información. 2010. Lima. Perú.

- COSO (Committee of Sponsoring Organizations of the Treadway Commission). Gestión del Riesgo Empresarial Integrando Estrategia y Desempeño. Resumen Ejecutivo. 2017.
- Dejan Kosutic. Ciberseguridad en 9 pasos. El manual sobre seguridad de la información para el gerente. 2012.
- Gobierno Corporativo, riesgo y cumplimiento. 12 principios de Seguridad de la información, Londres, diciembre de 2010.  
[https://www.isc2.org/uploadedfiles/press\\_releases/isfsecurityprinciples\\_final\\_121510](https://www.isc2.org/uploadedfiles/press_releases/isfsecurityprinciples_final_121510).
- Gobierno de la Ciudad Autónoma de Buenos Aires. Marco Normativo de IT.
- Implantación de un SGSI en la empresa  
[https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia\\_apoyo\\_SGSI.pdf](https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf)
- Isabel Casares San José et.al. Introducción a la Gestión Integral de Riesgos Empresariales Enfoque: ISO 31000. 2016 - Lima, Perú. PLATINUM EDITORIAL S.A.C.
- Ian Cooke. Fundamentos de la auditoría de SI: Innovación en el proceso de auditoría de TI. ISACA Journal Volume 2, 2018
- Jennifer Bayuk, El papel de la tecnología en la gestión del riesgo empresarial. ISACA Journal Volume 2, 2018
- MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. 2012.
- MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro III - Guía de Técnicas. 2012.
- PUIG FAURA, Sonia: LA PRUEBA ELECTRÓNICA: SUS IMPLICACIONES EN LA SEGURIDAD DE LA EMPRESA. Tesis Doctoral. Universitat Ramon Llull.  
<https://www.tdx.cat/bitstream/handle/10803/285237/TESI%20DOCTORAL%20S%C3%92NIA%20PUIG%20FAURA.pdf?sequence=1>. 2015.
- ARENS, Alvin A - ELDER, Randal J. – BEASLEY, Mark S.: AUDITORIA, UN ENFOQUE INTEGRAL. 11ª. Edición. Pearson Education. Mexico 2007.
- Federación Argentina de Consejos Profesionales de Ciencias Económicas. Resolución Técnica 37. Normas de Auditoría, revisión, otros encargos de aseguramiento, certificación y otros servicios relacionados.

## C.2. BIBLIOGRAFÍA AMPLIATORIA.

- Jeimy Cano. “Gobierno y Gestión de la Seguridad de la Información. Dos conceptos complementarios para comprender la inevitabilidad de la falla” – Blog de Jeimy Cano – 2015 – Disponible en: [insecurityit.blogspot.com.ar/2015/04/gestion-y-gobierno-de-la-seguridad-de.html](http://insecurityit.blogspot.com.ar/2015/04/gestion-y-gobierno-de-la-seguridad-de.html)
- Jeimy Cano. “La estrategia en seguridad de la información. Descubriendo permanentemente la inseguridad de la información”. Blog de Jeimy Cano – 2013. Disponible en: <http://insecurityit.blogspot.com.ar/2013/04/la-estrategia-en-seguridad-de-la.html>

- Jeimy Cano. “La Gerencia de la Seguridad de la Información: Evolución y Retos Emergentes” – 2011 - Disponible en: <http://www.isaca.org/Journal/archives/2011/Volume-5/Documents/jolv5-11-LaGerencia.pdf>
- Jeimy Cano, - La Inseguridad de la Información: Motivador de la Práctica de Cumplimiento Corporativo, ISACA Journal - Vol. 3, 2013. Disponible en <http://www.isaca.org/Journal/archives/2013/Volume-6/Pages/Information-Insecurity-Motivator-of-Corporate-Compliance-Practice-Spanish.aspx>
- Jeimy Cano. – Computación Forense - Descubriendo rastros informáticos. 2da. Edición, Editorial Alfaomega, 2015
- Jeimy Cano. Ciberriesgo. Aprendizaje de un riesgo sistémico, emergente y disruptivo. Junio 2019
- Prandini, P. y Pallero, M. “Vulnerabilidades, amenazas y riesgo en ‘texto claro’” – Magazcitur Año 4, Número 2 – 2013 – Disponible en: <http://www.magazcitur.com.mx/?p=2193#.Vgb7dpfnPCs>
- Bursztein, Sara. “Factor humano: el talón de Aquiles de la seguridad I – La percepción del valor de la información”. Revista Magazcitur, Octubre 2014, disponible en <http://www.magazcitur.com.mx/?p=2735#.ViKTFcVnPCs>
- COBIT 5 for information security, presentación en castellano por Patricia Prandini y Rodolfo Szuster, <http://www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx>
- Comunicación BCRA 5374 de Requisitos Mínimos de gestión, implementación y Control de los Riesgos Relacionados con Tecnología Informática, Sistemas de Información y Recursos Asociados para Entidades Financieras. Año 2012.
- Information Technology Auditing (Inglés) 4th Edición. South-Western College Pub; 2015.
- ISACA: Certified Information Systems Auditor, CISA Review Manual 2016/2017, ISBN: 978-160420-200-7.
- Global Technology Audit Guide (GTAG) 3 – Continuous Auditing
- Global Technology Audit Guide (GTAG) 4 – Management of IT Auditing.
- Global Technology Audit Guide (GTAG) 5 – Managing and Auditing Privacy Risks
- Global Technology Audit Guide (GTAG) 6 – Managing and Auditing IT Vulnerabilities
- Global Technology Audit Guide (GTAG) 8 – Auditing Application Controls
- Global Technology Audit Guide (GTAG) 11 – Developing the IT Audit Plan
- Global Technology Audit Guide (GTAG) 12 – Auditing IT Projects
- Global Technology Audit Guide (GTAG) 13 – Fraud Prevention and Detection in an Automated World
- Global Technology Audit Guide (GTAG) 14 – Auditing User-Developed Applications
- Sandra Senft et. Al, Information Technology Control and Audit, Fourth Edition, , Frederick Gallegos, and Aleksandra Davis, 2013, by Taylor & Francis Group, LLC

- IT Standards, Guidelines, and Tools and Techniques for Audit and Assurance and Control Professionals, 2010 ISACA
- Federación Argentina de Consejos Profesionales de Ciencias Económicas. Informe 15 del CECYT. Auditoría en Ambientes Computarizados.
- Banco Central de la República Argentina. Comunicación "A" 4609.
- MAGGIORE, Marcia L., PRANDINI, María Patricia: Nomas Internacionales y Nacionales vinculadas a la Seguridad de la Información. Editorial Buyatti. Marzo de 2010.

#### **D. METODOLOGÍA DE LA CONDUCCIÓN DEL PROCESO DE ENSEÑANZA Y APRENDIZAJE.**

Al comienzo del cuatrimestre se entrega el cronograma de clases junto con la bibliografía asociada a cada punto. Ello permite que el alumno pueda estudiar previamente los temas que se desarrollarán en clase, buscando de este modo una participación activa frente a los temas dados, posibilitando además resolver las dudas que pudieron haber surgido con la lectura del material.

Las clases tienen un doble propósito. Por un lado, se abordan aquellos puntos de la bibliografía que resulten más importantes o que presenten mayor problemática. Se utilizan ejemplos y casos reales para permitir que los alumnos comprendan mejor el tema. Por otro lado, se presentan situaciones problemáticas a fin de que los alumnos puedan resolverlas, en base a lo que estudiaron, o a su propia experiencia laboral. Se busca siempre vincular y validar los temas tratados con experiencias reales aportadas por el docente o por los propios alumnos.

Se utiliza la plataforma virtual de la Facultad para difundir material de estudio y links de interés; también se aprovecha el foro virtual para responder dudas y plantear eventualmente discusiones de interés general.

Se fomenta en todo momento la participación en clase de los alumnos, teniendo libertad para expresar sus propias opiniones y puntos de vista. Los alumnos pueden interrumpir a los docentes para recabar aclaraciones cuando las explicaciones no sean lo suficientemente claras.

#### **E. METODOLOGÍA DE EVALUACIÓN**

##### **a) Cursos presenciales y semipresenciales**

Los alumnos serán evaluados, como mínimo, con dos exámenes escritos –en días y horarios de clase- (Resolución CD 386/2006) que contemplarán aspectos teóricos - prácticos de la asignatura. Se destaca que solos serán examinados los alumnos regulares e inscriptos en cada curso.

De acuerdo con la normativa vigente, el alumno podrá recuperar un parcial cuya nota haya sido inferior a 4 (cuatro) puntos o en caso de ausencia. La instancia de recuperatorio también podrá ser utilizada para aquellos casos que tengan calificaciones iguales o superiores a 4 (cuatro) y menores a 7 (siete) y deseen elevar la nota para alcanzar la promoción.

La calificación obtenida en el examen recuperatorio reemplazará a la nota del parcial que se recupera.

Los alumnos que de acuerdo con la Resolución CD 455/2006:

1. hubieran aprobado todas las instancias de evaluación (nota parcial 4 o más puntos) y la nota final fuere siete (7) puntos o más de promedio, serán promovidos automáticamente y su calificación será el promedio resultante de ellas. Cabe agregar que debe entenderse que las evaluaciones individuales serán aquellas que respondan a los exámenes parciales en forma directa o luego de haber aprobado la única prueba recuperatoria a que tienen derecho.
2. hubieran aprobado todas las instancias de evaluación (nota parcial 4 o más puntos) y la nota final fuere cuatro (4) puntos o más puntos de promedio, pero inferiores a siete (7) serán considerados "regulares" a los fines de rendir un examen final de la asignatura, cabe destacar al igual que en el punto anterior sean ellas obtenidas en forma directa o luego de haber aprobado la única prueba recuperatoria a que tienen derecho,
3. que hubieran obtenido, luego de todas las instancias de evaluación, notas finales inferiores a cuatro (4) puntos de promedio se les asignará la nota "insuficiente".

Dado que solamente serán calificados los alumnos inscriptos en la lista del curso respectivo, que brinda la Facultad, aquellos alumnos que hayan asistido a las clases en carácter de oyentes o voluntarios no podrán presentarse a rendir los exámenes parciales respectivos, por cuanto la Facultad no labrará acta alguna en tales condiciones ni se admitirán cambios de curso o la rendición de exámenes parciales en otros cursos.

#### **b) Régimen de exámenes finales, intensivos, magistrales y libres**

El examen final integrador comprenderá temas teóricos prácticos de la asignatura, debiendo el alumno aprobar con un puntaje que alcance por lo menos un 60% de los contenidos.

Por consiguiente, los alumnos que obtengan una calificación inferior a 4 (cuatro) puntos serán considerados insuficientes y aquellos con una calificación igual o superior a 4 (cuatro) aprobarán la asignatura con dicha nota (Resolución CD 406/2006).

En el caso de cursos intensivos la evaluación se realizará con una nota final para cada alumno inscripto, que surgirá de un único examen final, el promedio de dos exámenes, la combinación de seguimiento de lectura y trabajos prácticos con exámenes parciales

Las calificaciones deberán ser informadas a los alumnos dentro de los 15 días corridos siguientes a la fecha del examen final. En caso de no existir aula disponible, el acto de lectura y entrega de notas se realizará en Sala de Profesores (Resolución CD 374/2006)

**c) Criterio de confección del promedio de notas finales**

En los casos en que fuere necesario expresar en número entero el promedio de notas parciales o de estas y el examen parcial, se aplicará el número entero superior si la fracción fuere de 0.50 puntos o más y el número entero inferior si fuere de 0.49 o menos. Cuando la nota fuese de 3.01 a 3.99 se calificará con 3 (tres) puntos. (Resolución CS 4994/93).