

---

**Formulario de aprobación de curso de posgrado/educación permanente**

**Asignatura: Gobernanza y Gestión Estratégica de la Seguridad de la Información**

(Si el nombre contiene siglas deberán ser aclaradas)

**Modalidad:**

(posgrado, educación permanente o ambas)

**Posgrado**

**Educación permanente**

---

**Profesor de la asignatura** <sup>1</sup>: Dr. Raúl Saroka y Mg. Patricia Prandini, Universidad de Buenos Aires, Argentina.

(título, nombre, grado o cargo, instituto o institución)

**Profesor Responsable Local** <sup>1</sup>: Dr. Ing. Gustavo Betarte, Profesor Titular, Instituto de Computación.

(título, nombre, grado, instituto)

**Otros docentes de la Facultad:**

(título, nombre, grado, instituto)

**Docentes fuera de Facultad:**

(título, nombre, cargo, institución, país)

<sup>1</sup> Agregar CV si el curso se dicta por primera vez.

(Si el profesor de la asignatura no es docente de la Facultad se deberá designar un responsable local)

[Si es curso de posgrado]

**Programa(s) de posgrado:** Especialización de Seguridad Informática y Maestría en Seguridad Informática

**Instituto o unidad:** Computación

**Departamento o área:** Programación, Grupo de Seguridad Informática

---

**Horas Presenciales:** 30

(se deberán discriminar las horas en el ítem Metodología de enseñanza)

**Nº de Créditos:** 5

[Exclusivamente para curso de posgrado]

(de acuerdo a la definición de la UdelaR, un crédito equivale a 15 horas de dedicación del estudiante según se detalla en el ítem Metodología de enseñanza)

**Público objetivo:**

Profesionales y estudiantes interesados en los aspectos organizacionales de la seguridad de la información, y en particular, profesionales informáticos que consideren la posibilidad de convertirse en CISO o bien, de interactuar con ese rol.

**Cupos:** Máximo 30 personas

(si corresponde, se indicará el número de plazas, mínimo y máximo y los criterios de selección. Asimismo, se adjuntará en nota aparte los fundamentos de los cupos propuestos. Si no existe indicación particular para el cupo máximo, el criterio general será el orden de inscripción, hasta completar el cupo asignado)

**Objetivos:**

El objetivo de este curso es que los estudiantes comprendan los aspectos fundamentales de la gobernanza y la gestión estratégica de la seguridad de la información en la organización y puedan desempeñarse como gerentes o CISO en la actualidad o en el futuro o bien, interactuar con ese rol.

---

**Conocimientos previos exigidos:**

Profesionales informáticos que se desempeñen en áreas de Seguridad informática/de la información o en áreas de TI y que deseen adquirir o mejorar sus habilidades en la gestión estratégica de la seguridad de la información en la organización.

**Conocimientos previos recomendados:**

Se considera conveniente haber cursado la materia Gestión de la Seguridad de la Información o tener conocimientos de la materia.

---

**Metodología de enseñanza:**

Las clases consisten en un 70% de exposiciones de los docentes y un 30% de resolución de casos y debate.

El curso se dictará en 9 clases virtuales sincrónicas más una de evaluación presencial, de 3 horas cada una, durante 5 semanas.

(comprende una descripción de la metodología de enseñanza y de las horas dedicadas por el estudiante a la asignatura, distribuidas en horas presenciales -de clase práctica, teórico, laboratorio, consulta, etc.- y no presenciales de trabajo personal del estudiante)

Descripción de la metodología:  
[Obligatorio]

Detalle de horas:

- Horas de clase (teórico): 27
- Horas de clase (práctico):
- Horas de clase (laboratorio):
- Horas de consulta:
- Horas de evaluación: 3
  - Subtotal de horas presenciales: 30
- Horas de estudio: 20
- Horas de resolución de ejercicios/prácticos: 10
- Horas proyecto final/monografía: 15
  - Total de horas de dedicación del estudiante: 75

**Forma de evaluación:**

[Indique la forma de evaluación para estudiantes de posgrado, si corresponde]

[Indique la forma de evaluación para estudiantes de educación permanente, si corresponde]

Se evaluarán los trabajos prácticos grupales, un proyecto final grupal y un examen final individual presencial.

---

### Temario:

1. La seguridad de la información en el contexto organizacional
  - a. Estrategia de seguridad de la información.
  - b. Plan estratégico de la seguridad de la información
  - c. Alineamiento con la Estrategia del negocio
  - d. Vinculación con la estrategia de la tecnología informática
  - e. Política y normativa interna de la seguridad de la información
  - f. Aspectos económicos y financieros de las inversiones en seguridad de la información
  - g. Tercerización (outsourcing) desde el punto de vista de la seguridad de la información
2. Gobernanza de la seguridad de la información.
  - a. Definición
  - b. Relevancia del tema
  - c. Diferencias con la gestión de la seguridad de la información
  - d. COBIT 2019 como marco para el gobierno y la gestión de la Información y la Tecnología
  - e. Otros marcos regulatorios (NIST, ENISA, etc.)
3. Gestión y evaluación de la Seguridad de la información
  - a. Clasificación de información
  - b. Modelos de madurez
4. El recurso humano y la seguridad de la información
  - a. Roles en el área de Seguridad de la información
  - b. La función del CISO
    - i. Funciones y perfil
    - ii. Los primeros 100 días del CISO
5. Cultura de la Ciberseguridad
  - a. Relevancia e implicancias
  - b. Programas de Concientización
6. Cumplimiento
  - a. Definición
  - b. Normativa interna y externa
  - c. Relevancia

---

### Bibliografía:

(título del libro-nombre del autor-editorial-ISBN-fecha de edición)

#### **BIBLIOGRAFÍA GENERAL OBLIGATORIA**

- Además de las presentaciones, se entregará material sobre los temas tratados en cada clase.
- ISACA (2019) Marco COBIT 2019: Objetivos de Gobierno y Gestión. Disponible en <https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9DEAS> - Recuperado febrero 2024
- McGraw, G. Miguez, S and Chess, B. (2017) - CISO Report: Four CISO tribes and where to find them" - Disponible en: <https://www.garymcgraw.com/wp-content/uploads/2018/01/CISO-2017.pdf> - Recuperado febrero 2024

#### **BIBLIOGRAFÍA GENERAL COMPLEMENTARIA**

- Cano, Jeimy (2016) - Manual de un CISO - Ediciones de la U - ISBN 9789587625837
- INCIBE - Kit de concientización - Disponible en: <https://www.incibe.es/empresas/formacion/kit-concienciacion>

- ISO/IEC (2022) 27001:2022 - Disponible en: <https://www.iso.org/standard/27001>. Recuperado febrero 2024 (en inglés)
  - ISO/IEC (2022) 27002:2022 - - Disponible en: <https://www.iso.org/standard/75652.html>. Recuperado febrero 2024 (en inglés)
  - Oberlaender, Michael S. (2013) - C(I)SO - And Now What? How to Successfully Build Security by Design - CreateSpace Independent Publishing Platform -ISBN 1480237418
  - OEA-AWS (2019). Clasificación de datos - Disponible en: <https://www.oas.org/es/sms/cicte/docs/ESP-Clasificacion-de-Datos.pdf> - Recuperado febrero 2024.
-

**Datos del curso**

---

**Fecha de inicio y finalización:** 22 de julio al 22 de agosto (lunes y jueves).

**Horario y Salón:** Dictado híbrido (9 clases virtuales sincrónicas y 1 evaluación final presencial)

**Arancel:** \$ 24.000 pesos uruguayos

[Si la modalidad no corresponde indique "no corresponde". Si el curso contempla otorgar becas, indíquelo]

**Arancel para estudiantes inscriptos en la modalidad posgrado:** \$ 24.000 pesos uruguayos

**Arancel para estudiantes inscriptos en la modalidad educación permanente:** \$ 24.000 pesos uruguayos

---