



DIPLOMATURA EN

Compliance en Seguridad Informática

Transforma tu futuro con un enfoque teórico-práctico de seguridad informática basada en el cumplimiento de estándares internacionales



Duración:

120 hs. (72 hs. sincrónicas y 48 hs. asincrónicas).

Días y horarios:

Del 5 de mayo al 26 de noviembre. Lunes y miércoles de 18:00 a 21:00 hs.

Calendario de encuentros:

Mayo	5	7	12	14	19	21	26	28	
Junio	2	4	9	11	16	18	23	25	30
Julio	2	7	9	14	16	21	23	28	30
Agosto	4	6	11	13	18	20	25	27	
Septiembre	1	3	8	10	15	17	22	24	29
Octubre	1	6	8	13	15	20	22	27	29
Noviembre	3	5	10	12	17	19	24	26	

Modalidad:

Virtual.

Aranceles (*):

Matrícula: \$30000.

Externos: Contado \$624000 ó 6 cuotas de \$130000.

Colegio Ingenieros Especialistas de Santa Fe, Descuentos Corporativos y Empleados públicos:
Contado \$500000 ó 6 cuotas \$104000.

Comunidad UAI: Contado \$437000 ó 6 cuotas de \$91000.

Extranjeros no residentes en Argentina ():**

Matrícula: USD 20.

Aranceles: Contado USD 650 o 6 cuotas de USD 130

Universidad Abierta Interamericana

UAI

(*) En caso de elegir la opción de pago al contado, deberá avisarnos al momento de abonar la matrícula, o dentro del primer mes de cursado a uai.extensionrosario@uai.edu.ar ó al WhatsApp: +54 9 11 2182-3616. Transcurrido ese período la opción ya no será válida y deberá pagar obligatoriamente las cuotas mensuales según el valor establecido en cada capacitación.

(**) Los aranceles de esta actividad comprenden únicamente los conceptos de matrícula y cuota. Todo impuesto, tasa o contribución asociada a los pagos en dólares estadounidenses que pudiera ser aplicada por el país de origen, así como cualquier otra suma que se adicione en virtud de las tarifas vigentes en la entidad bancaria al momento de realizar la transacción, queda a exclusivo cargo del alumno.

Dirigido a:

Profesionales de TI y Ciberseguridad
Administradores de sistemas y redes
Consultores de seguridad informática
Especialistas en protección de datos
Ejecutivos y Directivos
Ejecutivos responsables de la gestión de riesgos en organizaciones
Profesionales del Derecho
Profesionales de Auditoría
Emprendedores y Empresarios
Estudiantes Universitarios Avanzados
Funcionarios Públicos y ONGs

Enfoque general:

La diplomatura proporciona una formación integral que no solo aborde los aspectos teóricos del compliance aplicado a la ciberseguridad, sino que también ofrezca herramientas prácticas para su implementación efectiva en las organizaciones.

Objetivos:

Objetivos Generales

1. Comprender el Marco Normativo
2. Desarrollar Habilidades Prácticas

Objetivos Específicos

1. Identificar Normativas Clave

2. Diseñar Programas de Compliance
3. Evaluar Riesgos Tecnológicos
4. Fomentar la Ética Organizacional
5. Realizar Auditorías Efectivas
6. Simular Respuestas a Incidentes

Beneficios:

Visión global e innovadora de la actividad profesional
Liderazgo potenciado mediante la implementación de normas internacionales
Gestión estratégica del Compliance
Adaptación a Nuevas Amenaza
Mejora de Competencias Técnicas
Desarrollo de Habilidades en Compliance
Perspectiva Integral
Enfoque Práctico
Networking Profesional
Certificados expedidos por la Universidad

Resultados de Aprendizaje:

- Comprender el marco normativo internacional y nacional en materia de compliance y seguridad informática, demostrando la capacidad para identificar normativas claves aplicables en el contexto corporativo.
- Desarrollar habilidades prácticas para diseñar e implementar programas de compliance efectivos, aplicando políticas y procedimientos que aseguren el cumplimiento normativo en las organizaciones.
- Evaluar riesgos tecnológicos mediante la identificación y análisis de amenazas, utilizando matrices de riesgo para proponer estrategias de mitigación adecuadas a cada situación.
- Fomentar la ética organizacional mediante la creación e implementación de un código de ética, promoviendo una cultura de cumplimiento y responsabilidad dentro de la empresa.
- Realizar auditorías efectivas en el ámbito de ciberseguridad, demostrando competencias en la evaluación y mejora continua de los programas de compliance establecidos.
- Simular respuestas a ciberincidentes a través de talleres prácticos, mostrando la habilidad para actuar ante situaciones críticas y gestionar crisis en el entorno digital.
- Analizar casos prácticos reales de ciberincidentes, integrando los conocimientos adquiridos para evaluar las lecciones aprendidas y mejorar las prácticas organizacionales.
- Explorar tendencias futuras en compliance y seguridad informática, identificando el impacto de nuevas tecnologías emergentes sobre las estrategias de cumplimiento y seguridad en las organizaciones.

Contenidos:

MÓDULO 1: INTRODUCCIÓN AL COMPLIANCE Y SEGURIDAD INFORMÁTICA

Conceptos Fundamentales. Definición de Compliance y su importancia en el entorno corporativo. Introducción a la ciberseguridad: amenazas y riesgos actuales. Marco Normativo Internacional Tratados y convenciones internacionales sobre Compliance. Normativas relevantes (ISO 37001, GDPR, etc.).

MÓDULO 2: MARCO NORMATIVO NACIONAL EN ARGENTINA

Legislación Argentina sobre Compliance Ley de Responsabilidad Penal de las Personas Jurídicas. Regulaciones específicas sobre protección de datos (Ley de Protección de Datos Personales). Seguridad Informática en el contexto argentino Análisis de la legislación argentina vinculada a Seguridad Informática. Políticas públicas y estrategias nacionales para la seguridad informática.

MÓDULO 3: IMPLEMENTACIÓN DE PROGRAMAS DE COMPLIANCE

Diseño y Desarrollo de un Programa de Compliance Componentes esenciales: políticas, procedimientos y controles internos. Rol del Compliance Officer en la implementación. Evaluación y Auditoría Métodos para evaluar la efectividad del programa. Auditorías internas y externas en el ámbito de ciberseguridad. Herramientas tecnológicas para la detección y prevención del lavado de dinero (KYC, monitoreo transaccional).

MÓDULO 4: GESTIÓN DE RIESGOS EN SEGURIDAD INFORMÁTICA

Identificación y Análisis de Riesgos Métodos para identificar riesgos tecnológicos. Matrices de riesgo y su aplicación en el contexto corporativo. Estrategias de Mitigación Desarrollo de políticas para la prevención y respuesta ante incidentes cibernéticos. Evidencia digital y normas vinculadas Continuidad del negocio y gestión de crisis.

MÓDULO 5: ÉTICA Y CULTURA ORGANIZACIONAL

Ética Empresarial en el Compliance Creación e implementación de un Código de Ética. La importancia de la cultura organizacional en el cumplimiento normativo. Formación y Sensibilización Programas de capacitación para empleados sobre ciberseguridad y compliance.

MÓDULO 6: CASOS PRÁCTICOS Y TALLERES ESTUDIO DE CASOS REALES

Análisis de incidentes cibernéticos en empresas argentinas. Talleres Prácticos Simulaciones sobre respuesta a incidentes cibernéticos. Ejercicios prácticos sobre auditoría y evaluación del cumplimiento.

MÓDULO 7: TENDENCIAS FUTURAS EN COMPLIANCE Y SEGURIDAD INFORMÁTICA

Nuevas Tecnologías y Desafíos Impacto de tecnologías emergentes (IA, blockchain) en el compliance. Perspectivas Globales Comparativa con otros países en materia de compliance y ciberseguridad

***Espacios dedicados a evaluaciones intermedias y un proyecto final que integra lo aprendido**

Dictantes:

MARÍA EUGENIA CASCO (Directora)

Magister en Tecnología Educativa, Ingeniera en Sistemas Informáticos

SILVIA V. PONCIO (Directora)

Magister en Emprendimiento e Innovación, y en Psicoinformática Educativa
Ingeniera en Sistemas Informáticos - Doctorando

SANTIAGO ROATTA

Magister en Arquitectura de Computadoras y Procesamiento Paralelo
Ingeniero electrónico.

SANTIAGO FRANCHI

Magister en Dirección de Tecnologías de la Información y en Ciberinteligencia
Licenciado en Administración

GILDA AGUSTINA AMSLER

Ingeniera en Sistemas Informáticos

Contacto:



uai.extensionrosario@uai.edu.ar



Envíanos un mensaje en WhatsApp: [+54 9 11 21823616](https://wa.me/5491121823616)

Universidad Abierta Interamericana

UAI