

# COMPLIANCE ENFOCADO A LA CIBERSEGURIDAD

ENFOQUE INTERNACIONAL Y PRÁCTICO



Modalidad:  
**100% ONLINE**



Inicio: **3 de septiembre**  
Finaliza: **10 de octubre**

**CURSADA:** MARTES Y JUEVES DE 19 A 21 H (ARG).  
12 CLASES.



## CERTIFICACIÓN UNIVERSITARIA

En el marco de los programas de estudio de  
**Compliance Integral®.**

INFORMES POR EMAIL:  
**INSCRIPCIONES@UMSA.EDU.AR**

VISITÁ NUESTRA WEB

[WWW.UMSA.EDU.AR](http://WWW.UMSA.EDU.AR)

CERTIFICACIÓN OFICIAL DE UMSA JUNTO A:



**Dirigido a:**



Dirigido a profesionales y ejecutivos de empresas, organizaciones, ONGs, y entes públicos y privados. Y en general, a los particulares interesados en adquirir las herramientas y los conocimientos para gestionar o supervisar los riesgos de ciberseguridad asociados al uso de la tecnología.



## Cronograma

**Inicio:** 3 de septiembre de 2024

**Finalización:** 10 de octubre de 2024

**Días y horarios de cursada:** martes y jueves de 19 a 21 h (Arg).

**Modalidad:** 100% online a través del campus virtual de UMSA.

12 clases de 2 horas semanales sumando un total de 24 h.



## Cuerpo Docente y Expertos Invitados

### Grin, Esteban

Director del área de Auditoría en Riesgos de IT y Protección de datos, Grupo Techint. Más de 25 años en auditoría, seguridad e implementación de sistemas de información. Miembro de la división de Auditoría Interna de IDEA y del club de CISOs de Argentina. Expositor en diferentes eventos relacionados con seguridad de la información, auditoría de sistemas, riesgos y control. CISA| MBA (IAE) | Diseñador Industrial (UBA).

### Paradela, Juan Manuel

CISO, Allianz Argentina. Más de veinte años de experiencia en seguridad de la información, gestión de riesgos, compliance, data privacy, third party risk assurance y auditorías TI. Experiencia en roles de liderazgo en ciberseguridad en diversas industrias: eléctricas, telcos, agro, entretenimiento, electrónica, retail y seguros. Formación en Ingeniería en Sistemas, MBA en Dirección de Sistemas, Posgrado en Economía y especializaciones en seguridad y protección de datos.

### Pierri, Federico

Director Nacional de CiberSeguridad, Secretaría de Innovación, Ciencia y Tecnología, Jefatura de Gabinete de Ministros, Presidencia de la Nación.

### Segura, Pablo

Data Privacy Director, Mercado Libre.

### López Galanes, Santiago

CISO, Tecpetrol.

### Zurdo, Gabriel

BTR Consulting, especialista internacional en ciberseguridad.

### Nigohosian, Gustavo

Director de los Programas de Governance y del Programa Ejecutivo en Compliance Integral®.



## Objetivos del Programa

- Comprender el impacto del uso de la tecnología en las organizaciones, sus principales riesgos y amenazas desde el punto de vista de la ciberseguridad.
- Obtener, junto a profesionales con amplia trayectoria, una visión moderna y práctica de los principales aspectos a considerar al momento de evaluar el cumplimiento de un programa de ciberseguridad.
- Entender cómo la implementación de un adecuado esquema de gobierno, políticas, procedimientos, metodologías de control y el uso de la tecnología nos permitirá mitigar los riesgos de ciberseguridad.

### Metodología innovadora de enseñanza:

Las clases son dictadas con foco en la participación activa, lo que garantiza que al final del entrenamiento los asistentes internalicen los objetivos del programa:

Clases dictadas por directores y gerentes que lideran o lideraron áreas de seguridad informática, auditoría de sistemas y control en empresas de relevancia.

Abordaje y discusión de situaciones reales, mediante un enfoque práctico de la problemática y los riesgos asociados.

Consolidación de conocimientos con trabajos prácticos integradores. No multiple choice.





### MÓDULO 1: EL RIESGO DE CIBERSEGURIDAD HOY (2 H)

- Conceptos generales de ciberseguridad
- Tendencias en cibercrimen
- Principales vectores de ataque
- El impacto en las organizaciones
- Ciberseguridad personal

### MÓDULO 2: EL GOBIERNO DE CIBERSEGURIDAD (2 H)

- Marco normativo de ciberseguridad
- Estructura del área de seguridad
- Gestión estratégica y mapa de riesgos de ciberseguridad
- Aspectos claves para el tratamiento en el directorio

### MÓDULO 3: LAS FUNCIONES DE CIBERSEGURIDAD (4 H)

- Identificar
- Detectar
- Proteger
- Responder
- Recuperar

### MÓDULO 4: CONCIENTIZACIÓN (2 H)

- El usuario – el eslabón más débil
- Vectores de ataque al usuario
- Campañas de concientización
- Ataques éticos

### MÓDULO 5: GESTIÓN DE ACCESOS (2 H)

- Esquema de mínimos accesos
- Gestión de accesos basado en roles
- Segregación de funciones
- Controles para la gestión de accesos



### **MÓDULO 6: CLASIFICACIÓN Y PROTECCIÓN DE LA INFORMACIÓN (2 H)**

- La información como activo crítico
- Materialidad y niveles de clasificación
- Roles y responsabilidades
- Tecnología para la clasificación y protección de la información

### **MÓDULO 7: GESTIÓN DE INCIDENTES (2 H)**

- Procedimientos para la gestión de incidentes
- Comités de crisis
- Estrategias de recupero
- Estrategia de comunicación

### **MÓDULO 8: MÓDULO 8 – ANÁLISIS FORENSES (2 H)**

- La informática forense
- Etapas de una investigación
- Herramientas
- Presentación de los resultados

**Integración (6 h).**





**UMSA**  
UNIVERSIDAD  
DEL MUSEO SOCIAL ARGENTINO

**N**  
ESCUELA DE  
**NEGOCIOS**