Postgrado Internacional en Ciberseguridad para

Tecnologías Actuales y Emergentes

Incluye preparación para la certificación
“CC- Certified in Cybersecurity” de ISC2

Impartido por ISEADE El Salvador y la Universidad Sergio Arboleda de Colombia.

UNIVERSIDAD SERGIO ARBOLEDA

ISEADE BUSINESS SCHOOL FEPADE

Descripción General del Programa

El postgrado responde a los retos de un mundo hiperconectado, donde ciberamenazas como el ransomware y las filtraciones de datos afectan a organizaciones de cualquier tamaño.

El programa forma profesionales capaces de diseñar estrategias de ciberseguridad resilientes, integrando estándares globales como ISO 27001, NIST Cybersecurity Framework y MITRE ATT&CK.

Como valor diferencial, ofrece una preparación integral para la certificación ISC² Certified in Cybersecurity (CC), respaldada por ISC², entidad de referencia internacional en la materia. Esta certificación, disponible a través de la iniciativa One Million Certified in Cybersecurity, valida competencias en cinco dominios clave y fortalece la empleabilidad en roles estratégicos de ciberseguridad.

Dirigido a:

Gerentes informáticos, jefes de TI, coordinadores de seguridad digital o profesionales relacionados con las TIC y profesionales de otras áreas que cumplan con lo detallado en el apartado de requisitos de este brochure.

Objetivo General:

Formar profesionales capaces de liderar la ciberseguridad empresarial mediante competencias en gobernanza, gestión de riesgos, defensa y respuesta a incidentes, alineados con marcos internacionales (ISO 27001, NIST, MITRE ATT&CK) y con preparación integral para obtener la certificación internacional ISC² Certified in Cybersecurity (CC).

Metodología del programa

El programa sigue un enfoque andragógico y práctico, diseñado para profesionales adultos. Combina **clases online sincrónicas vía Zoom** con análisis de casos reales como el ataque a Colonial Pipeline o los recientes incidentes de **ransomware** en Latinoamérica, ejercicios aplicados (por ejemplo, **simulaciones de threat hunting**) y discusiones guiadas.

Se utilizan herramientas líderes como MITRE ATT&CK Navigator y marcos internacionales de referencia (ISO 27001/27005/31000, NIST CSF, CIS Controls v8).

La metodología busca integrar teoría y práctica mediante talleres, simulaciones, informes de riesgo y planes de respuesta a incidentes, ofreciendo al participante una experiencia formativa innovadora, directamente vinculada con los cinco dominios de la certificación ISC² Certified in Cybersecurity (CC).

Competencias

- Gestionar riesgos cibernéticos en entornos corporativos, IoT y cadenas de suministro aplicando estándares internacionales.
- Implementar gobernanza y cumplimiento en ciberseguridad, integrando regulaciones globales y riesgos post-cuánticos.
- Diseñar arquitecturas seguras con Zero Trust, control de accesos avanzados y defensas en entornos híbridos y multinube.
- Ejecutar respuestas efectivas a incidentes y planes de continuidad del negocio basados en estándares internacionales.
- Desarrollar ciberinteligencia y análisis avanzado de amenazas mediante OSINT, IA y técnicas de threat hunting.

Modalidad online sincrónico:

Clases sincrónicas en línea por ZOOM.

Requisito de asistencia a clases: 75% por módulo

Fecha de inicio

29 DE OCTUBRE DE 2025

Meses a ser impartido

OCTUBRE 2025 A JUNIO 2026

Duración 9 meses

90 HORAS

Graduación presencial y cóctel en julio de 2026

(Sujeto a cambios por motivos de fuerza mayor)

REQUISITOS DE INGRESO:

• Poseer título universitario de Ingeniería en Informática,
• Licenciado en Informática o carreras afines. (Profesional en otras áreas no afines de forma directa a las tecnologías de la información y las comunicaciones (TIC)

REQUISITOS DE INGRESO PARA PROFESIONALES DE OTRAS CARRERAS AFINES:

• **Opción 1:** Aprobar un examen de admisión
• **Opción 2:** Presentar constancia de la empresa en que trabaja indicando que se ha desempeñado en puestos de informática o directamente relacionados con esta área.

RECONOCIMIENTOS:

• Diploma físico de ISEADE-FEPADE.
• E-Diploma de ISEADE-FEPADE con Código Seguro de Verificación (CSV).
• Diploma digital emitido por la Universidad Sergio Arboleda, Colombia.

• Entrega de notas impresas el día de graduación.
• Entrega de notas digitales en caso la graduación sea online.

Certificación ISC² Certified in Cybersecurity (CC): Lo que debes saber

¿Qué es la certificación ISC²?

La certificación: **Certified in Cybersecurity (CC) de ISC²** es otorgada por la organización internacional líder en certificaciones de ciberseguridad, reconocida por sus rigurosos estándares técnicos, éticos y académicos. Con más de 265,000 profesionales certificados, ISC² cuenta con credenciales ampliamente avaladas por instituciones y organismos internacionales.

Dicha certificación es una credencial de nivel inicial, diseñada para quienes desean comenzar o transicionar su carrera hacia ciberseguridad.

No requiere experiencia laboral, solo aprobar un examen de 100 preguntas en 2 horas (puntuación mínima: 700/1000).

El examen CC evalúa conocimiento en cinco dominios fundamentales:

- Principios de Seguridad
- Conceptos de Continuidad del Negocio (BC)
- Recuperación ante Desastres (DR) y Respuesta a Incidentes
- Conceptos de Controles de Acceso
- Seguridad de Redes
- Operaciones de Seguridad

Nivel del postgrado.

El postgrado tiene como intención principal abordar las temáticas necesarias para profundizar en la disciplina de la ciberseguridad, enfatizando la proactividad en la protección de infraestructuras críticas, la gestión ética de datos y la alineación con regulaciones globales, y a la vez estructurando el currículo para el estudio paralelo y presentación exitosa del **examen ISC² Certified in Cybersecurity (CC)**.

***Esta certificación es renovable cada 3 años con 90 CPE, siendo un diferenciador en currículos para transiciones y ratificaciones laborales en ciberseguridad.**

Módulo 1: Gestión de Riesgos y Operaciones de Seguridad

Fechas de clases:
Octubre: 29,30
Noviembre: 4, 5, 6, 11, 12

Horario:
6:30 pm a 8:30 pm
(hora El Salvador).

Objetivo:

Desarrollar un marco integral de identificación y mitigación de riesgos en operaciones cibernéticas, incorporando IoT y cadenas de suministro, para una gestión dinámica que evolucione con las amenazas actuales.

Principales temas a abordar:

• Aplicación de ISO 31000 y 27005 combinada con MITRE ATT&CK para evaluaciones de riesgos cuantitativas.
• Análisis especializado de riesgos en entornos IoT, incluyendo exposición a dispositivos conectados.
• Estrategias de seguridad en cadenas de suministro para prevenir ataques de tercer nivel.
• Uso de herramientas de automatización (e.g., scripts de IA para priorización de riesgos) en operaciones diarias.
• Integración operativa alineada con el Dominio 5 de ISC² CC, con simulaciones de escenarios reales.

Dominios de la certificación CC relacionados:

Domain 5: Security Operations (gestión de riesgos operativos y mitigación continua).

Andrés Felipe Estupiñan / Colombia

Experto en ciberseguridad, con 12 años de experiencia en roles de seguridad de la información y ciberseguridad.

Ha participado como líder e ingeniero senior en múltiples proyectos de ciberseguridad en organizaciones públicas y privadas de Colombia y Ecuador, se ha desempeñado como catedrático de posgrado para varias universidades en Colombia. Cuenta con un Magister en seguridad de las tecnologías de la información y es Ingeniero en informática.

Módulo 2: Derecho de Ciberseguridad, Protección de Datos y Fomento de la IA

Fechas de clases:
Diciembre: 03, 05, 08, 10, 15, 16, 17

Horario:
6:30 pm a 8:30 pm
(hora El Salvador).

Objetivo:

Fortalecer las competencias legales y técnicas para aplicar las nuevas normativas salvadoreñas e internacionales en ciberseguridad, protección de datos y uso responsable de la inteligencia artificial.

Principales temas a abordar:

- Introducción y marco legal nacional reciente
- Derechos, bases legales y modelos internacionales
- Ciberseguridad: obligaciones, gestión de riesgos y marcos técnicos
- IA, protección de datos y riesgos algorítmicos
- Tratados, convenios y protocolos internacionales
- Modelos comparados y mejores prácticas regulatorias

Dominios de la certificación CC relacionados:

Domain 1: Security Principles (regulaciones, privacidad y ética legal).

Karla Alas / El Salvador

Socia de la firma Lexincorp – Central American Law Firm
Es catedrática de ISEADE-FEPADE en el Postgrado de Derecho y Nuevas Tecnologías y además forma parte de Legal Hackers, un movimiento global de abogados, políticos, diseñadores, tecnólogos y académicos que exploran y desarrollan soluciones creativas para algunos de los problemas más apremiantes en la intersección de la ley y la tecnología.

Es líder para el programa Womcy Geek de la Organización WOMCY (Women in Cibercrime) y pertenece al capítulo EL Salvador, de Internet Society. Becaria de la Escuela del Sur de Gobernabilidad en Internet. Licenciada en Ciencias Jurídicas de la Universidad José Matías Delgado.

Módulo 3: Gobernanza y Ciberseguridad: introduciendo la IA y post-cuántica

Fechas de clases:
Enero (2026): 6, 7, 8, 13, 14, 15, 20

Horario:
6:30 pm a 8:30 pm
(hora El Salvador).

Objetivo:

Fortalecer la gobernanza y el cumplimiento corporativo en ciberseguridad mediante la integración de marcos internacionales, el uso ético de la inteligencia artificial y la preparación frente a regulaciones y riesgos post-cuánticos.

Principales temas a abordar:

• Exploración del panorama de ciberseguridad local e internacional, incluyendo tendencias en adopción regulatoria y evolución del cibercrimen.
• Aplicación de marcos ISO 27000, NIST CSF y CIS Controls en la integración de la ciberseguridad con la gobernanza de TI.
• Incorporación de IA ética en procesos de gobernanza para optimizar decisiones basadas en datos.
• Análisis de regulaciones post-cuánticas y su impacto en la resiliencia organizacional.

Dominios de la certificación CC relacionados:

Domain 1: Security Principles (ética, regulaciones y marcos fundamentales).
Domain 5: Security Operations (gobernanza operativa y alineación estratégica).

Carlos Mauricio Blanco / Colombia

Actualmente es consultor independiente en Gobierno, Gestión, Riesgos, Seguridad y Auditoría de TI. Posee más de 20 años de experiencia en ciberseguridad, auditoría de sistemas y gestión de riesgos, con certificaciones internacionales como CISA, CISM, CRISC, CSX, ISO 27001 LA, ISO 31000 RM y COBIT 2019, además de haber trabajado en proyectos con el Banco Central y la Dirección de Impuestos Internos de República Dominicana
Ha sido profesor de tiempo completo en el programa de Ingeniería de Sistemas y Computación de la Universidad Católica de Colombia y catedrático en especializaciones de Auditoría y Seguridad de la Información.

Master en Gestión de Tecnologías de la Información y la Comunicación (Universidad Ramón Llull, España), y especializaciones en Auditoría de Sistemas de Información y Gerencia de Proyectos, además de Ingeniero de Sistemas.

Módulo 4: Estrategias de Defensa y Seguridad de Redes

Fechas de clases:
Febrero: 10, 11, 12, 17, 18, 19, 24

Horario:
6:30 pm a 8:30 pm
(hora El Salvador).

Objetivo:

Fortalecer las capacidades defensivas mediante arquitecturas modernas y adaptativas, enfocándose en entornos híbridos y amenazas impulsadas por IA, para una protección proactiva y que evolucione hacia modelos de seguridad predictiva.

Principales temas a abordar:

• Diseño de arquitecturas seguras con énfasis en control de accesos multifactor y segmentación dinámica
• Implementación de Zero Trust en entornos de nube (AWS/Azure) para mitigar brechas en infraestructuras distribuidas.
• Estrategias avanzadas contra ataques generados por IA, incluyendo detección de anomalías en tiempo real.
• Evaluación integrada de vulnerabilidades con herramientas de automatización y simulaciones de escenarios híbridos.

Dominios de la certificación CC relacionados:

Domain 3: Access Controls Concepts (gestión de identidades y accesos adaptativos).
Domain 4: Network Security (defensas en redes y nubes contra amenazas emergentes).

Diego Osorio Reina / Colombia

Experto en Ciberseguridad y socio fundador de la Compañía Colombiana en Ciberseguridad Locknet S.A. Cuenta con 22 años de experiencia como docente en pregrado y posgrado para varias universidades de Colombia, de igual forma es conferencista internacional en la materia y ha recibido varios premios por su labor como docente. Magister en seguridad de las tecnologías de la información y de las comunicaciones, CIO (Chief Information Officer).

Actualmente es consultor independiente en Gobierno, Gestión, Riesgos, Seguridad y Auditoría de TI. Posee más de 20 años de experiencia en ciberseguridad, auditoría de sistemas y gestión de riesgos, con certificaciones internacionales como CISA, CISM, CRISC, CSX, ISO 27001 LA, ISO 31000 RM y COBIT 2019, además de haber trabajado en proyectos con el Banco Central y la Dirección de Impuestos Internos de República Dominicana

Módulo 5: Respuesta a Incidentes y Continuidad del Negocio

Fechas de clases:
Marzo: 17, 18, 19, 23, 24, 25, 26

Horario:
6:30 pm a 8:30 pm
(hora El Salvador).

Objetivo:

Preparar para la gestión holística de incidentes y recuperación, integrando simulaciones avanzadas para una respuesta ágil que evolucione con amenazas híbridas.

Principales temas a abordar:

• Procesos estandarizados de respuesta a incidentes, desde detección hasta contención forense.
• Implementación de ISO 22301 para planes de continuidad del negocio en entornos post-incidente.
• Simulaciones prácticas con purple teaming para escenarios multi-vectoriales.
• Revisión intensiva de todos los dominios de ISC² CC, con enfoque en brechas y actualizaciones 2025.

Dominios de la certificación CC relacionados:

Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts (respuesta y recuperación integral).
Domain 5: Security Operations (simulaciones y preparación operativa).

Erica Milena Montoya / Colombia

Directora de Servicios de Seguridad de la Información en Smart Locknet desde mayo de 2023.

Previamente fue Consultora Senior en Opalus S.A.S. (2022-2023).

Tiene experiencia docente en seguridad de la información y ciberseguridad desde 2012. Es Máster en Gestión de Riesgos Digitales y Ciberseguridad por EALDE (2022) y Especialista en Seguridad de la Información por la Universidad Católica de Colombia (2020).

Módulo 6: Ciberinteligencia de Amenazas, Análisis Avanzado y preparación para la Certificación

Fechas de clases:
Abril: 21, 22, 23, 28, 29, 30
Mayo: 5, 6, 7, 12

Horario:
6:30 pm a 8:30 pm
(hora El Salvador).

Objetivo:

Capacitar en la generación y explotación de inteligencia de amenazas impulsada por IA, para una anticipación estratégica de ciberataques evolutivos, alineando con avances en análisis predictivo y una preparación culminante para la certificación ISC² CC.

Principales temas a abordar:

• Exploración en profundidad de MITRE ATT&CK para modelado de tácticas adversarias. Identificación y correlación de fuentes de inteligencia, desde OSINT hasta feeds automatizados.
• Desarrollo de ciberinteligencia mediante IA/ML para procesamiento de grandes volúmenes de datos.
• Análisis de amenazas emergentes como deepfakes y ransomware evolutivo, con casos de estudio 2025.
• Refuerzo del Dominio 5 de ISC² CC a través de laboratorios de threat hunting colaborativo, culminando en mock exams integrales.

Dominios de la certificación CC relacionados:

Domain 2: Business Continuity (BC), Disaster Recovery (DR) & Incident Response Concepts (respuesta y recuperación integral).
Domain 5: Security Operations (simulaciones y preparación operativa).

Diego Osorio Reina / Colombia

Experto en Ciberseguridad y socio fundador de la Compañía Colombiana en Ciberseguridad Locknet S.A. Cuenta con 22 años de experiencia como docente en pregrado y posgrado para varias universidades de Colombia, de igual forma es conferencista internacional en la materia y ha recibido varios premios por su labor como docente. Magister en seguridad de las tecnologías de la información y de las comunicaciones, CIO (Chief Information Officer).

Actualmente es consultor independiente en Gobierno, Gestión, Riesgos, Seguridad y Auditoría de TI. Posee más de 20 años de experiencia en ciberseguridad, auditoría de sistemas y gestión de riesgos, con certificaciones internacionales como CISA, CISM, CRISC, CSX, ISO 27001 LA, ISO 31000 RM y COBIT 2019, además de haber trabajado en proyectos con el Banco Central y la Dirección de Impuestos Internos de República Dominicana

Beneficios de descuento

Inversión:

9 cuotas mensuales de $138.00

Inversión total:

$1,242.00

Descuentos especiales:

- Descuento del 10% en todas las cuotas para graduados de Maestría o Postgrados de ISEADE Business School.
- Descuento del 10% al realizar pago de contado.

Descuentos empresariales:

- Descuento del 6% en todas las cuotas al inscribirse dos o cinco colaboradores de una misma empresa.
- Descuento del 10% en todas las cuotas al inscribirse seis a más colaboradores de una misma empresa.

Tasa 0%:

- Puede realizar el pago a tasa 0% interés
- 12 cuotas plazo con tarjeta de crédito emitida en El Salvador de BAC Credomatic, Cuscatlán, Davivienda Agrícola o Promerica.
- 24 cuotas plazo con tarjeta de crédito emitida en El Salvador Banco Promérica y Agrícola.

*IMPORTANTE:
Los descuentos son excluyentes entre sí y NO son combinables con tasa 0% interés.

Proceso de admisión

01

Iniciar su proceso de inscripción llenando el formulario de solicitud

HAZ CLICK:

¡Inscríbete aquí!

02

Enviar su documentación en formato digital:
- DUI (revés y derecho)
- Título Universitario
- NIT (únicamente para persona jurídica)
- Fotografía

03

Completar su usuario online y cancelar la primera cuota del programa

CONTÁCTANOS
E-mail: emercadeo@iseade.edu.sv
PBX: +(503) 2212-1700
Whatsapp: 7979-2843