

EC-COUNCIL · PROGRAMA EJECUTIVO

Certified Chief Information Security Officer (C|CISO) v4

El estándar de oro en liderazgo de ciberseguridad para la alta dirección, ahora potenciado con capacidades de IA

¿Por qué debería asistir?

El Certified Chief Information Security Officer (C|CISO) es un programa de nivel ejecutivo, diseñado para formar y certificar a los líderes responsables de desarrollar y dirigir la estrategia de ciberseguridad de una organización. Desarrollado por CISOs en ejercicio, combina una comprensión profunda de la ciberseguridad con las habilidades de liderazgo, finanzas y planificación estratégica necesarias para tener éxito en un rol ejecutivo.

La versión 4 prepara a los líderes para integrar la IA en la gestión de riesgos, el cumplimiento, los pronósticos y la gobernanza, con responsabilidad y transparencia. Obtener la credencial C|CISO demuestra que usted está preparado para alinear la seguridad con los objetivos del negocio, gestionar el riesgo empresarial y comunicarse con la junta directiva y la alta dirección.

5 días	5	8	War games	IA
DURACIÓN	DOMINIOS	ÁREAS DE HABILIDAD	EN CLASES EN VIVO	GOBERNANZA Y RIESGO

CISO — Chief Information Security Officer

¿Quién debería participar?

Aspirantes a CISO y líderes
Futuros CISOs y líderes de seguridad que se preparan para roles ejecutivos y de cara a la junta directiva.

Gerentes y arquitectos
Gerentes y arquitectos de seguridad que buscan pasar de gestionar herramientas a liderar la estrategia de seguridad.

GRC, riesgo y cumplimiento
Profesionales de gobierno, riesgo y cumplimiento que necesitan una visión ejecutiva del programa de seguridad.

CTOs y consultores
CTOs y líderes técnicos que pasan a roles ejecutivos, y consultores que se preparan para posiciones de junta o asesoría.

Objetivos de aprendizaje

- Alinear la ciberseguridad y la estrategia de seguridad de IA con los objetivos del negocio
- Liderar la gobernanza, el cumplimiento y la estrategia de riesgo de la IA, alineada con NIST AI RMF y la Ley de IA de la UE
- Comunicarse eficazmente con la junta directiva y la alta dirección, traduciendo el riesgo cibernético en impacto de negocio
- Gestionar programas y presupuestos de seguridad a nivel empresarial, con análisis de ROI, CAPEX y OPEX
- Diseñar e implementar programas estratégicos de seguridad con una estructura de gobierno clara
- Gestionar proveedores, contratos y riesgo de terceros con apoyo de herramientas de IA
- Dirigir las operaciones de seguridad, el SOC y la respuesta a incidentes
- Desarrollar talento, planes de sucesión y una cultura de seguridad, con liderazgo ético

Áreas de habilidad del programa

Gobierno y estrategia de seguridad | Riesgo, cumplimiento y GRC | IA, automatización y tecnologías emergentes | Liderazgo, ética y presencia ejecutiva | Gestión financiera y de proveedores | Operaciones de seguridad, SOC e incidentes | Fundamentos técnicos y de arquitectura | Privacidad, concienciación y cultura

Programa del curso

Duración: 5 días

Módulo	Contenido
Módulo 1 Día 1	01 **Gobierno, gestión de riesgos, seguridad, cumplimiento, privacidad y auditoría:** gobierno de la seguridad alineado con el negocio; análisis cuantitativo y cualitativo de riesgos (ISO 27005, NIST); regulaciones (GDPR, HIPAA, SOX, PCI DSS, DPDP Act, Ley de IA de la UE); marcos NIST CSF, ISO 27001, COBIT, MITRE ATT&CK y Zero Trust; programas de auditoría con herramientas GRC y auditoría con IA.
Módulo 2 Día 2	02 **Liderazgo ejecutivo organizacional:** presencia ejecutiva, comunicación con la junta y gestión de partes interesadas; inteligencia emocional, social y cultural; liderazgo de equipos inclusivos, multifuncionales y virtuales; sucesión, desarrollo de talento y mentoría; liderazgo ético y gobierno de la IA; resiliencia y adaptabilidad.
Módulo 3 Día 3	03 **Controles de seguridad de la información, gestión del programa y operaciones:** operación del programa de seguridad, marcos de monitoreo y medición del desempeño; arquitectura segura para pipelines de IA/ML, APIs y automatización del SOC; IA en SIEM/SOAR; respuesta a incidentes, forense digital e inteligencia de amenazas con IA.
Módulo 4 Día 4	04 **Competencias centrales de seguridad de la información:** seguridad de redes, endpoints, nube y aplicaciones; SDLC seguro, DevSecOps y pruebas SAST, DAST e IAST; marcos de arquitectura empresarial (TOGAF, Zachman, SABSA, FEAF); privacidad y evaluaciones de impacto; comunicación de crisis, concienciación y cultura de seguridad.
Módulo 5 Día 5	05 **Planificación estratégica, finanzas, adquisiciones y gestión de proveedores:** presupuesto, planificación financiera y ROI de las inversiones en seguridad; estrategias CAPEX y OPEX y análisis costo-beneficio; presupuestos y pronósticos con IA; adquisiciones y contratos (SLA, MSA, términos y condiciones); riesgo de terceros y análisis de contratos con IA y NLP.



Los juegos de guerra (war games) de C|CISO v4 son simulacros de una brecha de seguridad que se hacen en clase, guiados por el instructor. Los participantes tienen que tomar decisiones como lo haría un CISO mientras el incidente avanza.

Qué son: una técnica que viene del ámbito militar y que hoy usan muchas empresas para preparar respuestas. En el curso, los candidatos participan en ejercicios que imitan lo que ocurre durante una brecha real.

- Para qué sirven: mejoran la toma de decisiones y dan experiencia en el manejo de incidentes. El CISO tiene que adaptarse a cambios del negocio, regulaciones nuevas, amenazas emergentes y tecnologías que cambian rápido, y el simulacro entrena eso sin el costo de un incidente real.

- Qué integran: todo lo visto en el curso (gobierno, riesgo, liderazgo, controles, finanzas y proveedores) se aplica en el ejercicio, lo que refuerza los conocimientos.
  Cuándo se hacen: EC-Council incluye sesiones de war games en todas las clases en vivo de C|CISO.

Examen

Duración: 2.5 horas

Examen C|CISO

Título	EC-Council Certified Chief Information Security Officer (C|CISO) – Versión 4		
Código	712-50	**N.º de preguntas**	150
Formato	Opción múltiple basada en escenarios	**Duración**	2.5 horas
Aprobación	60 % – 85 %, según la forma del examen	**Plataforma**	EC-Council Exam Portal

Examen Associate C|CISO

Examen	EC-Council Associate C|CISO Certification		
N.º de preguntas	150 (opción múltiple)	**Duración**	2 horas
Aprobación	70 %		

Requisitos de elegibilidad

- **Experiencia requerida:** cinco años de experiencia en al menos tres de los cinco dominios C|CISO. Con cinco años en los cinco dominios puede presentar el examen sin capacitación; con cinco años en solo tres dominios, la capacitación es obligatoria.
- **Exenciones:** algunas certificaciones reconocidas y estudios superiores en seguridad de la información pueden sustituir hasta tres años de experiencia por dominio.

Associate C|CISO: para quienes aún no cumplen la experiencia

Si no tiene cinco años de experiencia en tres dominios, pero sí dos o más años en al menos uno (o posee CISSP, CISM o CISA), puede participar en el programa **Associate C|CISO**. Asiste a la misma capacitación que los candidatos C|CISO, que es obligatoria antes del examen Associate, y aprende los requisitos del rol ejecutivo para planificar su carrera hacia el liderazgo en seguridad.

Información general

- War games en todas las clases en vivo: simulaciones guiadas por el instructor de lo que ocurre durante una brecha de seguridad
- Acreditada por ANAB (ANSI), certificación base aprobada por el DoD 8570/8140, reconocida por las Fuerzas Armadas de EE. UU. y alineada con los estándares de GCHQ
- Mapeada al DoD Cyber Workforce Framework (DCWF) y al NICE Cybersecurity Workforce Framework