

Especialización

# Gestión de Riesgos Ciberseguridad y Ethical Hacking

Risk Management, Cybersecurity, and Ethical Hacking Specialist  
Programa de Formación Internacional

# Programa de Formación Internacional

## **Gestión de Riesgos Ciberseguridad y Ethical Hacking**

Especialización Profesional de 240 horas en Gestión de Riesgos, Ciberseguridad y Ethical Hacking, orientada al desarrollo de competencias para identificar, analizar y tratar riesgos cibernéticos, reconocer amenazas y vulnerabilidades, fortalecer controles y aplicar técnicas de Ethical Hacking en entornos controlados y autorizados, con certificación y aval universitario en Estados Unidos.

Conviértete en experto en gestión de riesgos de ciberseguridad y Ethical Hacking, con competencias para evaluar vulnerabilidades, analizar vectores de ataque, realizar pruebas de penetración, implementar medidas de protección y fortalecer las capacidades de prevención, detección, respuesta y resiliencia cibernética de las organizaciones.

**240 Horas**



**5 Módulos**



**Certificación**



## **¿Quien es un Experto en Ciberseguridad y Hacking Ético?**

Es un profesional capacitado para identificar y gestionar riesgos cibernéticos, detectar amenazas y vulnerabilidades, evaluar sistemas, redes y aplicaciones, y aplicar técnicas de hacking ético y pruebas de penetración en entornos autorizados. Su labor contribuye a prevenir ataques, fortalecer controles, mitigar vulnerabilidades y mejorar la capacidad de detección, respuesta y resiliencia cibernética de las organizaciones.

# Objetivo general

Formar profesionales con competencias integrales para identificar, analizar, evaluar, tratar y monitorear riesgos asociados a la ciberseguridad, mediante la aplicación de metodologías de gestión del riesgo, marcos y buenas prácticas internacionales, desarrollando capacidades para identificar amenazas y vulnerabilidades, evaluar vectores de ataque, implementar controles y estrategias de respuesta, así como aplicar técnicas de Ethical Hacking y pruebas de penetración en entornos controlados y autorizados, con el propósito de fortalecer la prevención, protección, detección y respuesta frente a amenazas cibernéticas y contribuir a la resiliencia y continuidad de las organizaciones.

## Objetivos específicos

- Comprender los principios, conceptos y metodologías fundamentales de la gestión de riesgos aplicados al contexto de la ciberseguridad.
- Identificar amenazas, vulnerabilidades, activos críticos y escenarios de riesgo que puedan afectar la operación y continuidad de las organizaciones.
- Aplicar metodologías para el análisis, evaluación, tratamiento y monitoreo de riesgos, alineadas con buenas prácticas y estándares internacionales.
- Reconocer los principales vectores de ataque, técnicas, tácticas y procedimientos utilizados por actores maliciosos en entornos digitales.
- Desarrollar capacidades para identificar y evaluar vulnerabilidades presentes en sistemas, redes, aplicaciones e infraestructuras tecnológicas.
- Aplicar técnicas y metodologías de Ethical Hacking en entornos controlados y autorizados, con el propósito de evaluar la exposición de las organizaciones frente a posibles ciberataques.
- Comprender los fundamentos y etapas de las pruebas de penetración, desde la recopilación de información y análisis de vulnerabilidades hasta la explotación controlada y elaboración de reportes técnicos.
- Diseñar e implementar controles y estrategias orientadas a prevenir, detectar, responder y recuperarse frente a incidentes y amenazas de ciberseguridad.

- Fortalecer las capacidades para liderar, coordinar y apoyar programas de ciberseguridad basados en riesgos y orientados a los objetivos estratégicos de la organización.
- Analizar los resultados de evaluaciones técnicas y de riesgos para formular recomendaciones, planes de tratamiento y acciones de mejora.
- Integrar la gestión de riesgos, la ciberseguridad y el Ethical Hacking como herramientas complementarias para fortalecer la resiliencia cibernética de las organizaciones.
- Promover una cultura de prevención, gestión del riesgo y mejora continua frente a amenazas y desafíos asociados al entorno digital.

## Metodología

El programa se desarrolla en modalidad virtual mediante una plataforma e-learning SaaS que permite acceder a contenidos, actividades y evaluaciones desde internet, de forma flexible y sin necesidad de instalar software. La metodología combina aprendizaje autónomo, recursos multimedia, lecturas técnicas, ejercicios prácticos, casos empresariales y evaluaciones para fortalecer la gestión de riesgos en seguridad de la información.

A lo largo del proceso, los participantes aprenderán a identificar activos, amenazas y vulnerabilidades, evaluar riesgos, implementar controles, elaborar planes de tratamiento y apoyar la implementación y auditoría de Sistemas de Gestión de Seguridad de la Información (SGSI). Además, contarán con tutorías virtuales semanales y espacios de interacción académica que facilitan la resolución de dudas, el intercambio de experiencias y la aplicación práctica de los conocimientos en entornos organizacionales reales.

### Recursos necesarios



+



+



## Equipo Académico



### Juan Carlos Echeverri Garcés

Abogado en Colombia y licenciado en México, con más de 20 años de experiencia en derecho penal, criminalística y cumplimiento normativo. CEO de Risk Group International, donde ha liderado por más de 14 años estrategias de prevención de LA/FT/FPADM, corrupción y fraude. Ha sido Oficial de Cumplimiento en diversos sectores e implementador de SARLAFT, SAGRILAF y PTEE. Magíster en Criminalística, Criminología e Investigación Criminal y Magíster en Aseguramiento y Auditoría de la Información perito en poligrafía acreditado internacionalmente y consultor en riesgos, auditoría forense, ciberseguridad y gobierno corporativo.

### Docente

#### Andrea Giraldo Mejía

Abogada con MBA en Gestión de Riesgos y más de 10 años de experiencia en cumplimiento normativo, gobierno corporativo, protección de datos y programas SARLAFT/SAGRILAF en los sectores salud, financiero y asegurador. Ha liderado programas integrales de cumplimiento, ética y privacidad, fortaleciendo el control interno y la gestión auditoria de entes de control con resultados sobresalientes. Experta en debida diligencia, protección de datos y formación ética, con certificaciones en auditoría interna y cumplimiento.



### Docente

#### Nathaly Stephanie Perilla Ramos

Abogada de la Universidad Nacional, especialista en Derecho Privado Económico y Gerencia de Proyectos Informáticos, y magíster en Derecho Informático. Experta en compliance, protección de datos y prevención de riesgos LA/FT/FPADM, con más de cinco años de experiencia liderando SAGRILAF, ética empresarial y gobierno corporativo en diversos sectores. Ha desarrollado manuales SARLAFT, matrices de riesgo, capacitaciones y reportes a la UIAF.



# Plan de Estudios

## 1 Modulo

### Gestión de Riesgos ISO 31000

La ISO 31000 Risk Management Professional Certification I31000RM™ prepara a la persona candidata para comprender, aplicar y comunicar los fundamentos de la gestión del riesgo conforme a ISO 31000:2018, integrando sus principios, marco de referencia y proceso dentro de la toma de decisiones organizacionales.

### Concientización en Ciberseguridad

Fortalezca su defensa contra las amenazas digitales y dominar los aspectos esenciales de la seguridad en línea. Este programa gratuito incluye acceso a materiales de estudio oficiales y al examen de certificación oficial, con intentos ilimitados. Le ayudará a comprender los principios clave de seguridad, los vectores de ciberataque más comunes y las mejores prácticas para proteger los datos confidenciales.

## 2 Modulo

## 3 Modulo

### Fundamentos en Ciberseguridad

Entienda los fundamentos de las técnicas de protección de la información personal, incluyendo comunicaciones, aplicaciones, e inferencias de las bases de datos y procesamiento de datos. También conozca otros sistemas que soportan los derechos en línea que se refieren a censura y circunvención, secrecía, elecciones electrónicas, y privacidad en pagos y sistemas de identidad.

## Líder en Ciberseguridad

Proporciona conocimientos especializados en gobernanza de ciberseguridad, gestión de riesgos y estrategias de mitigación de amenazas. Los participantes aprenderán a evaluar riesgos, implementar marcos de seguridad y desarrollar planes de respuesta a incidentes. El programa abarca estándares del sector como ISO/IEC 27032 y el Marco de Ciberseguridad del NIST. Ideal para líderes de ciberseguridad, auditores y profesionales de TI, esta certificación dota a los participantes de las habilidades necesarias para diseñar y gestionar programas de seguridad sólidos.

## 4 Modulo

## 5 Modulo

### Hacking Ético

Con la certificación Ethical Hacking dominarás las técnicas, herramientas y metodologías más utilizadas para evaluar y fortalecer la ciberseguridad organizacional, defendiendo infraestructuras frente a ciberataques reales mediante un enfoque práctico. Aprenderás a detectar ataques de ingeniería social, realizar inteligencia en fuentes públicas (OSINT) y analizar redes para identificar activos, puertos y sistemas operativos. Además, evaluarás y explotarás vulnerabilidades comunes en ambientes controlados y redactarás informes técnicos y ejecutivos para la alta dirección, desarrollando competencias para anticiparte a las amenazas e implementar estrategias preventivas eficaces.

## Certificación y Aval Universitario Internacional

Certificado Por



Avalado Por



Dictado Por



La formación como Risk Management, Cybersecurity, and Ethical Hacking Specialist es impartida por Risk Group Institute en alianza con Certiprof entidades especializada con más de dos décadas de experiencia en capacitación avanzada en gestión del riesgo, protección de datos, ciberseguridad y seguridad de la información, cuenta con certificación y aval académico internacional otorgados por el Center of Education and Leadership (CEL), institución educativa con sede en Miami, Florida, en convenio académico con Florida Global University (FGU – USA).

Las certificaciones representan un proceso formal que valida las habilidades, conocimientos y competencias de los estudiantes en áreas específicas. Emitidas por el Centro de Educación y Liderazgo (CEL), estas certificaciones culminan con la entrega de un certificado que acredita el cumplimiento de los criterios y estándares establecidos por nuestro aliado académico, Florida Global University (FGU). El aval académico es un distintivo de calidad otorgado por FGU a programas de estudio, cursos, talleres y seminarios. Este reconocimiento certifica que la metodología y la evaluación del programa cumplen con los más altos estándares de calidad y relevancia académica. Las certificaciones con aval académico no solo validan competencias, sino que también garantizan que el programa de estudio cumple con exigentes estándares de calidad académica

## Authorized Training Partner



**Certiprof es un organismo internacional de certificación con presencia en más de 100 países**, comprometido con los más altos estándares internacionales en certificación profesional. Somos miembros de organizaciones como ANSI, el Institute for Credentialing Excellence (I.C.E.), el IT Certification Council (ITCC) y Agile Alliance. Además, nuestras credenciales digitales se emiten a través de BadgeClaimed y cumplen con el estándar Open Badges 3.0 de 1EdTech, garantizando credenciales seguras, verificables y con reconocimiento internacional.

# Recibe 5 Certificados por Niveles

