UPSKILLING & RESKILLING EN EL SECTOR FINANCIERO

RIESGO TECNOLÓGICO Y OPERACIONAL

CIBERAMENAZAS I ELEMENTOS DE LA TECNOLOGÍA DE SEGURIDAD I FORMAS DE GESTIONAR EL RIESGO OPERACIONAL Y REPUTACIONAL

PROGRAMA EXECUTIVE

nemesis
UNA COMPAÑÍA BESPOKE

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

CGRE
Club de Gestión de Riesgos de España

ASBA
ASOCIACIÓN DE SUPERVISORES BANCARIOS DE LAS AMÉRICAS

Nuestra Misión

Contribuyendo al fortalecimiento de los conocimientos en el ámbito financiero y bancario

Némesis es una **empresa líder** dedicada a la formación de profesionales en gestión de riesgos. Nos enorgullece ofrecer un entorno educativo dinámico y centrado en el estudiante, **donde la teoría se encuentra con la práctica** y la innovación impulsa el aprendizaje.

Como parte integral de nuestra visión global, hemos establecido colaboraciones estratégicas con instituciones y organizaciones internacionales líderes en la gestión de riesgos. Estos convenios no solo enriquecen su experiencia educativa sino que también les brindan la oportunidad de conectarse con perspectivas globales y prácticas innovadoras en el campo.

Introducción

RIESGO TECNOLÓGICO Y OPERACIONAL

En un mundo cada vez más digitalizado, la tecnología juega un papel crucial en el funcionamiento de las organizaciones. Sin embargo, **junto con los avances tecnológicos vienen una serie de desafíos y riesgos,** especialmente en lo que respecta al ámbito de la tecnología y la seguridad de la información. Eventos recientes, como el ataque a **SolarWinds** en 2020 o el ransomware **WannaCry** en 2017, han demostrado el impacto significativo que pueden tener en diversas organizaciones.

La adopción de tecnologías disruptivas, como la **inteligencia artificial (IA)**, presenta una serie de riesgos y desafíos únicos.
Uno de estos desafíos es la **privacidad y seguridad de los datos**:

- El uso de IA implica el procesamiento de grandes cantidades de datos, lo que puede aumentar el riesgo de brechas de seguridad y violaciones de privacidad si estos datos no se manejan adecuadamente.
- La protección de la información sensible se vuelve fundamental en un entorno digital en constante evolución.

En este programa, exploraremos en detalle los conceptos clave relacionados con el riesgo tecnológico y operativo, así como las mejores prácticas para mitigar y gestionar estas amenazas.

Programa

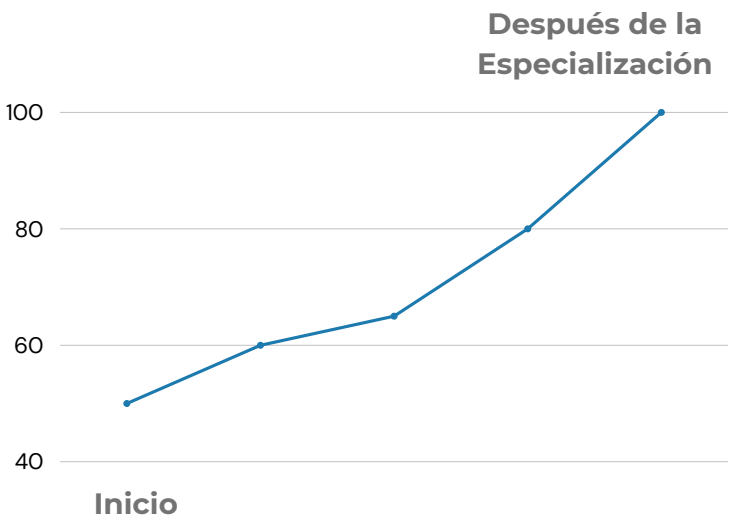
8
Semanas de especialización online

40
Horas de formación

98%
Nuestros estudiantes trabajan a tiempo completo, combinando sus estudios con sus responsabilidades profesionales.

100%
Accede a la experiencia de instructores líderes en la industria que guiarán tu camino hacia la excelencia en gestión de riesgos.

Objetivos



Con este programa transformas tu carrera:

Al finalizar el programa tendrás:

- Un conocimiento profundo de los principios de gestión de riesgos
- Amplia Red de Contactos Profesionales
- Reconocimiento Profesional

Amplitud y Especialización

Capacitar a los participantes en el uso de herramientas avanzadas de análisis de riesgos cibernéticos para identificar y mitigar vulnerabilidades en la infraestructura de TI de la organización

Cumplimiento Normativo y Basilea

Proporcionar orientación sobre cómo implementar medidas de seguridad de datos de acuerdo con regulaciones como el Reglamento General de Protección de Datos (GDPR) para garantizar el cumplimiento normativo en la gestión de riesgos tecnológicos

Gestión Proactiva y Estratégica

Desarrollar un plan estratégico de continuidad del negocio que incluya protocolos de respuesta ante desastres específicos para eventos como ciberataques masivos o interrupciones graves en la infraestructura tecnológica.

Adaptación a Escenarios Complejos

Gestionar escenarios de ataque cibernético sofisticados para que los participantes identifiquen la respuesta y mitigación de amenazas emergentes, como ataques de ransomware dirigidos o brechas de seguridad en la nube.

Beneficios

A través del análisis especializado de riesgos tecnológicos y operacionales, los participantes adquieren conocimientos y destrezas para identificar vulnerabilidades en la infraestructura de TI, así como para implementar medidas de seguridad de datos en cumplimiento con regulaciones como el GDPR.

Además, están preparados para desarrollar planes estratégicos de continuidad del negocio que les permitan responder proactivamente a eventos críticos, como ataques de ransomware y brechas de seguridad en la nube.

Expertos a tu alcance

Nuestros profesores son expertos en sus campos y son seleccionados cuidadosamente para garantizar una enseñanza de alta calidad.

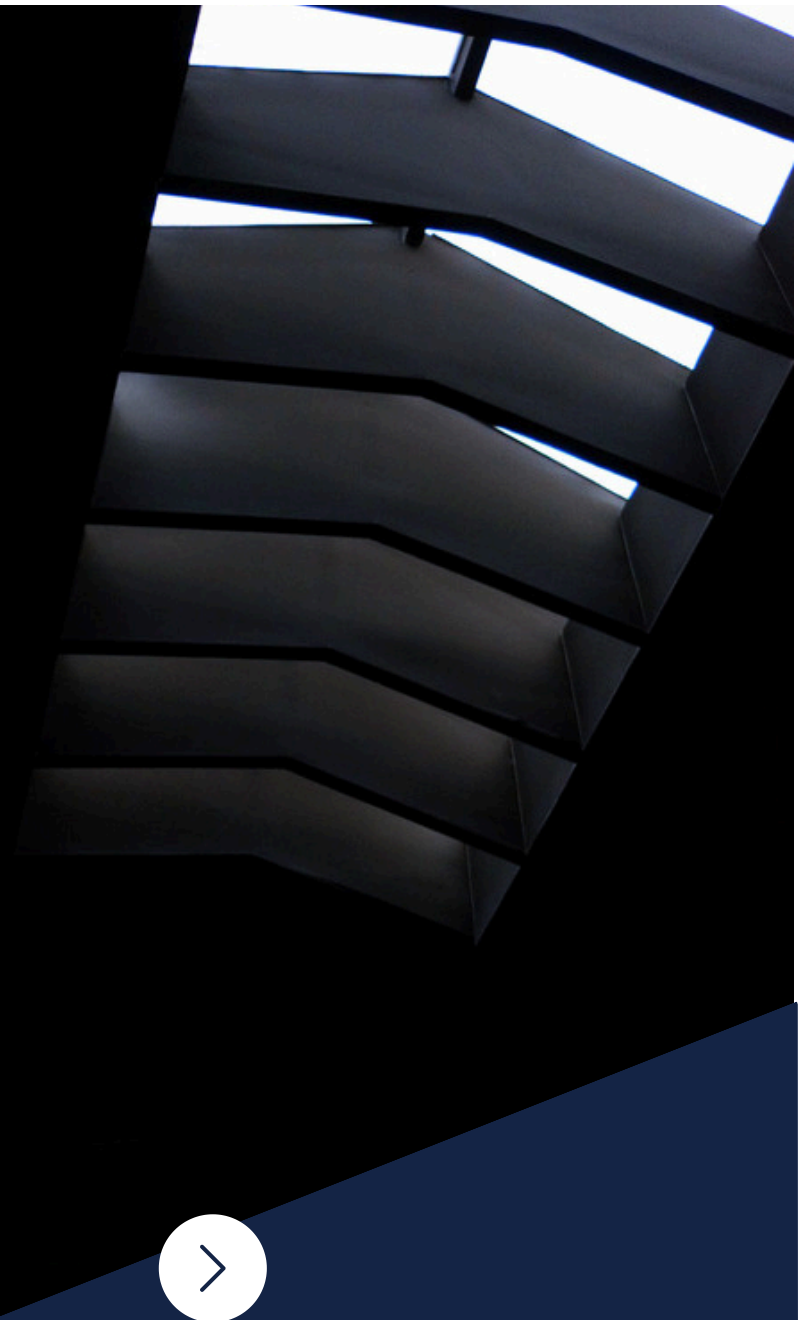
Red global

Únete a una comunidad de profesionales comprometidos que comparten conocimientos, experiencias y mejores prácticas

Actualización continua

Estamos dedicados a mantenernos al día con las últimas tendencias y regulaciones, garantizando que nuestros programas estén siempre actualizados.

Metodología FlexLearn



Campus virtual

Los participantes estudian de forma individual y a su propio ritmo las lecciones magistrales impartidas por los profesores.

Streaming

Sesiones live que incluyen casos de estudio relevantes y fomentan la participación activa de los asistentes.

Evaluación

Podrás realizar un seguimiento de su progreso, alcance sus objetivos con la ayuda de nuestros asesores y tutores.

Acreditación

Acreditación europea del **Club de Gestión de Riesgos de España**, la **Asociación de Supervisores Bancarios de las Américas**, con el aval de la **Federación Latinoamericana de Bancos**.

www.nemesisrisk.com

Temario

01
MÓDULO

Riesgo Tecnológico y Ciberseguridad

1. Riesgo Tecnológico
2. Tipos de Riesgo Tecnológico
3. Ciberamenazas. Análisis del estado actual del cibercrimen
4. Elementos de la tecnología de Seguridad
5. Gestión del riesgo en las organizaciones
6. Evaluación de Riesgos de IT
7. Mitigación y respuesta al riesgo IT
8. Gobierno de la Seguridad IT.

02
MÓDULO

Riesgos No Financieros:

Operacional, Reputacional, Estratégico y de Negocio

1. Entendiendo el riesgo operacional
2. Formas de gestionar el riesgo operacional
3. Mitigación de riesgos
4. Capital regulatorio
5. Factores de riesgo operacional
6. Riesgo Estratégico y de Negocio
7. Riesgo Reputacional

Programa

Ruta de aprendizaje por Módulo:

1 semana: Acceso a Campus virtual

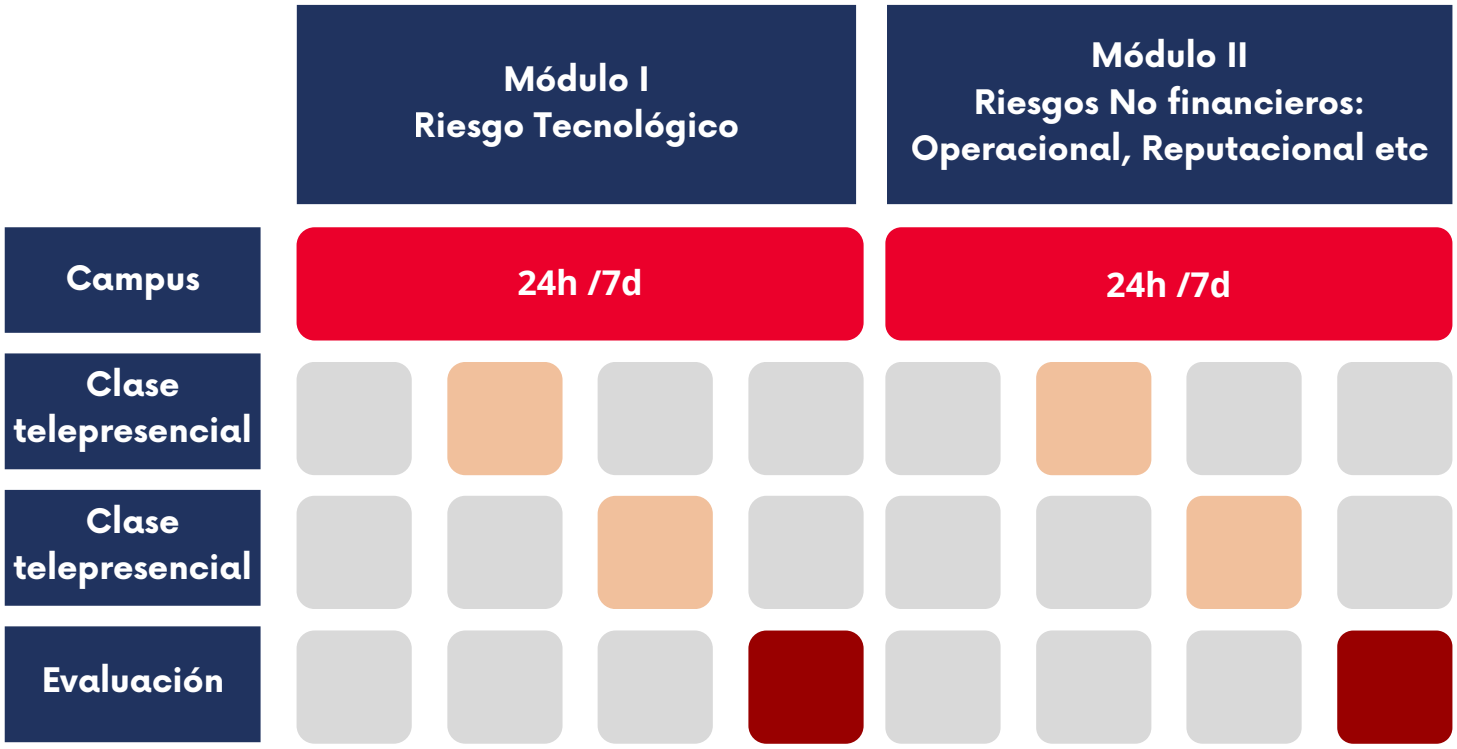
- Contenido teórico: recursos, vídeos, lecturas recomendadas...
- Disponibilidad 24/7 desde el inicio hasta la finalización del programa

2 y 3 semana: Clase con el profesor

- Clase en tiempo real con el profesor
- Oportunidad para preguntas, casos prácticos y debates en vivo
- Material didáctico disponible para la revisión del participante

4 semana: Evaluación de la materia

RIESGO TECNOLÓGICO Y OPERACIONAL



Docentes

Julio López Moreno

Chief Information Security Officer (CISO)

Chief Information Security Officer (CISO) de la Banca Corporativa y de Inversión del Grupo BBVA.Es miembro profesional de la asociación ISACA, poseyendo la certificación CRISC.

Jordi García Ribas

Ex Director De BBVA España En Riesgo Operacional

Miembro del CGRE, Socio de Quantitative Risk Research y Vicepresidente de Operational Risk Exchange. Director de Business Management en Santander, Ex director de BBVA España en riesgo operacional

Contacta con nosotros

Nemesis Formación

www.nemesisrisk.com

info@nemesisrisk.com

+34 91 859 90 10

Estaremos encantados de ayudarte para cualquier duda o consulta.