ASBA
ASOCIACIÓN DE SUPERVISORES BANCARIOS DE LAS AMÉRICAS

CGRE
Club de Gestión de Riesgos de España

FELABAN
FEDERACIÓN LATINOAMERICANA DE BANCOS

CIBERSEGURIDAD Y RIESGO OPERACIONAL

CERTIFICACIÓN ESPECIALIZADA

NEMESIS CERTIFICACIÓN NCRTC

nemesis

Para más información: +34 91 859 90 10 info@nemesisrisk.com WWW.NEMESISRISK.COM

Únete a nuestra familia de profesionales en riesgos y síguenos

PROGRAMA

NCRTC está diseñado para sacar máximo rendimiento de su aprendizaje mientras que compaginas tu vida laboral con la privada

8 SEMANAS
ESPECIALIZACIÓN ONLINE
30 HORAS DE FORMACIÓN
A TRAVÉS DE UN CAMPUS VIRTUAL

PRÓXIMA EDICIÓN
MATRÍCULA ABIERTA

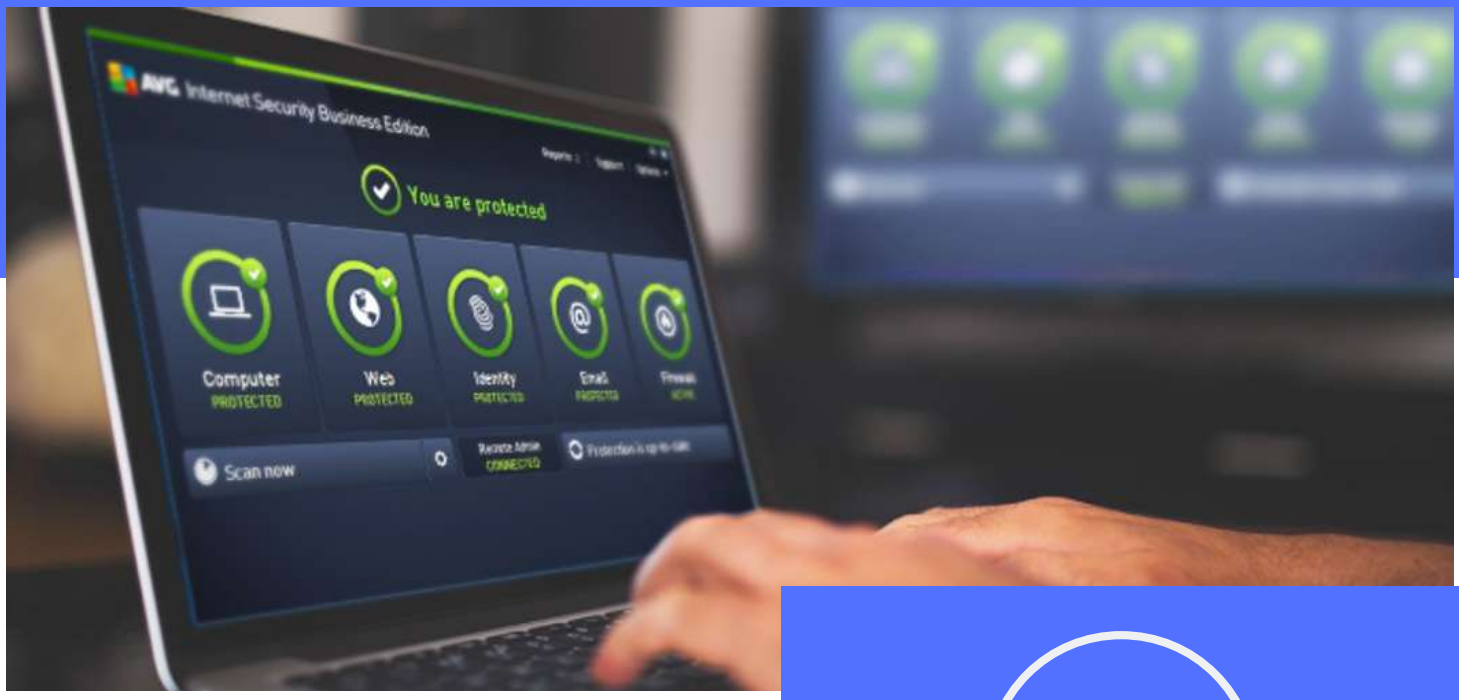
INNOVACIÓN Y DEDICACIÓN

- Las Certificaciones especializadas Nemesis aprovechan la experiencia de más de 15 años en el campo de formación dedicada a profesionales en riesgos, la investigación y la gestión para darle una ventaja en cualquier mercado, en cualquier economía. Con este programa, usted aumentará sus capacidades con las herramientas basadas en la gestión del riesgo
- Aumentará su impacto en la organización con un buen entendimiento de los riesgos tecnológicos. Y todo esto se logra en un ambiente de colaboración entre compañeros de clase con diferentes nacionalidades.

DESAFÍO Y CONFIANZA

- El programa **NCRTC** está diseñado para ejecutivos que buscan desafiarse a sí mismos, replantear lo convencional y destacar en su institución
- Con el aprendizaje online, y la colaboración con profesores y compañeros de renombre, usted ampliará su perspectiva. Empoderado con herramientas y métodos de vanguardia, usted resolverá retos complejos y aprovechará oportunidades estratégicas

OBJETIVOS ACADÉMICOS



JUSTIFICACIÓN DEL PROGRAMA

- Está diseñado para difundir la cultura del riesgo dentro de la organización.
- 2018 - El año en el que la Ciberseguridad ha entrado en las estrategias de las empresas, independientemente de su t amaño o sector.
- Conocer el riesgo desde la perspectiva financiera, aprender a valorarlo y a controlarlo.
- Contemplar el riesgo como una posible oportunidad de negocio.

DIRIGIDO A

- Ejecutivos de cuenta, directores de sucursales, etc
- Profesionales de entidades reguladoras: Bancos centrales y supervisores
- Profesionales en riesgos que desean mejorar sus conocimientos en riesgos tecnológicos
- Agencias de bolsa
- Consultores, auditores
- Directivos de empresa , de Banca de Inversiones
- Instituciones públicas: Seguridad Social, Fuerzas Armadas, Policía

TITULACIÓN

Una vez finalizado satisfactoriamente el programa, el participante recibirá el título internacional con la doble acreditación del Club de Gestión de Riesgos de España (CGRE), la Asociación de Supervisores Bancarios de las Americas (ASBA) y avalado por la Federación Latinoamericana de Bancos (FELABAN).

ASBA Asociación de Supervisores Bancarios de las Américas
CGRE Club de Gestión de Riesgos de España
FELABAN

¿POR QUÉ SEGUIR ÉSTE PROGRAMA?

INNOVADOR Y ACTUALIZADO

Brinda al alumno un enfoque integral sobre la Gestión de Riesgo
Tecnológico y Ciberseguridad, Riesgo Operacional y Reputacional
Cuenta con un contenido innovador y actualizado según las ultimas normativas

LOS MEJORES PROFESIONALES

Es un programa desarrollado por ejecutivos altamente especializados, con amplia experiencia teórica, práctica y académica

DIRIGIDO A

Administración y gerencia de riesgos, tanto en el sector privado como en supervisoras

DOBLE ACREDITACIÓN

Finalizando el programa y una vez superadas todas las pruebas obtendrás un certificado con acreditación europea (CGRE) y el aval latinomamericano (ASBA y FELABAN)

NEMESIS CREE QUE

"LA INNOVACIÓN DISTINGUE A LOS LÍDERES DE LOS SEGUIDORES"

Steve Jobs

100% ONLINE

¿POR QUÉ ESTUDIAR CIBERSEGURIDAD?

- En una época en la cual la tecnología digital esta presente a diario en nuestras vidas y en todas las carreras, cualquier persona debería concienciar la importancia de saber como mantener la seguridad a la par.En el trabajo, esto ayudará a las empresas a mantener protocolos robustos. En casa, le ayudará a proteger su propia información.
- Aparte de simplemente no hacer clic en archivos adjuntos de correo electrónico sospechosos, hay cosas que casi todos los empleados pueden hacer para mejorar la seguridad de la empresa y hacerse trabajadores más valiosos.
- **Nuestra Certificación te ayudará a encontrar la solución que más se adapte a tus necesidades...**

ÉSTE PROGRAMA TE AYUDARÁ INDEPENDIENTEMENTE DE TU CARRERA ...

Corporación

En las comunicaciones corporativas, usted debe considerar su impacto reputacional en el negocio y en la confianza de la marca

Área legal

El equipo jurídico debe velar que las cláusulas de garantía se incorporen en los contratos de proveedores y clientes

Informática

Los profesionales de la seguridad deben realizar exámenes y pruebas de control de calidad para la verificación funcional y de seguridad

Administración

La administración de la empresa debe velar por que exista un buen plan de respuesta ante incidentes de seguridad para hacer frente a cualquier vulnerabilidad

Gestoria

Los gestores de productos deben asesorar sobre las características que debe contemplar la seguridad

RRHH

Los recursos humanos y /o el departamento de IT, identifiquen competencias que deben formar parte de los perfiles profesionales en materia de seguridad

¿CÓMO SE ESTUDIA?

- **EL PROGRAMA CONSTA DE 2 MÓDULOS ***

- **AL FINALIZAR CADA UNO DE LOS MÓDULOS ENCONTRARÁ UNA AUTOEVALUACIÓN**
- **ESTA PERMITIRÁ CONOCER EN CADA MOMENTO EL GRADO DE CONSECUCIÓN DE LOS OBJETIVOS**

- **CURSAR Y APROBAR TODOS LOS MÓDULOS**
- **OBTENER UNA CALIFICACIÓN IGUAL O SUPERIOR A 5/10 EN CADA UNO DE LOS MÓDULOS, PARA SUPERAR LA CERTIFICACIÓN.**

ACTUALIZACIÓN CERTIFICACIÓN VALIDEZ

Cada 2 años los participantes podrán validar su Certificación a través de un programa de renovación que consiste en la realización de un módulo de actualización de las normas y superar un test de autoevaluación.

(Programa sujeto a un mínimo de participantes)

CLAUSTRO

JULIO LOPEZ

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.
Tiene también el título de Director de Seguridad Privada emitido por el Ministerio del Interior y cursó el Programa Avanzado en Tesorería y Derivados en el IEB.

JUAN ANTONIO DE JUAN

Director de metodologías, en el área de Riesgos del Grupo BBVA hasta 2015.
En la actualidad trabaja como consultor en el sector financiero y en formación cuantitativa en master especializados.
Doctor por la Universidad de Salamanca, donde se licencio en Administración y Dirección de Empresas y en ciencias Matemáticas, y es profesor de Algebra.
Cuenta con la Certificación Financial Risk Manager (FRM) concedida por el GARP.

JORDI GARCÍA RIBAS

Miembro del CGRE, CEO de Nodos Risk Consulting
Socio de Quantitative Risk Research
Vicepresidente de Operational Risk Exchange
Trabajo en España en BBVA, como Director de Riesgo Operacional del Grupo y miembro del Comité de Riesgos, en Banco Santander
Es profesor y conferencista de Riesgo Operacional, Reputacional, Gestión Integral de Riesgos, Gestión Estratégica del Riesgo y Control Interno. Licenciado en Ciencias Físicas por la Universidad de Barcelona.

EUGENIO ROGERO GONZÁLEZ

Profesional en riesgos y finanzas
Consejero de BBVA Colombia
Ha sido Chief Risk Officer en BBVA Puerto Rico y Argentina, Director de Riesgos Mayoristas México y América del Sur.Licenciado en Ciencias Empresariales

ALEJANDRO FRANCO HIDALGO

BBVA Ingeniería España. Estrategia y Desarrollo de Riesgos, Finanzas, Contabilidad y Recursos Humanos.
Licenciado en ADE por la UAM con máster en Gestión de Riesgos (BME), Gestión de Carteras (IEB) y Bolsas y Mercados Financieros (UAM)

CONTENIDO

Módulo I

RIESGO TECNOLÓGICO YCIBERSEGURIDAD

1. Introducción
2. Ciberamenazas. Análisis del estado actual del cibercrimen: Convergencia entre cibercrimen y terrorismo y El negocio del cibercrimen en cifras
3. Métodos y herramientas de ataque: Tipos de virus informáticos, Métodos de ataque, Ataques de Ingeniería Social, Técnicas de Ingeniería Social, Ingeniería Social: enfoque basado en la Tecnología, CEO Scam, Ciberextorsión o Ramsomware, Ataques de denegación de servicio (DoS/DDoS), Ataques de tipo "Man in the Middle", Comunidades criminales y "Crime as a Service", La "dark web" y la "deep web"
4. Principales eventos recientes de ciberseguridad: Wannacry, Carbanak, Ataque a la red SWIFT, RSA SecurID Breach, Hacking de la cuenta de Twitter de la Associated Press americana
5. Elementos de la tecnología de seguridad: El modelo TCP/IP, Controles, Control de Acceso, Single Sign-On, Métodos de Control de Acceso, One-Time Passwords,
6. Gestión del riesgo en las organizaciones
Riesgo de negocio versus riesgo de TI
Identificación del riesgo y métodos de análisis
Estrategia de tecnologías de información del negocio
7. Evaluación de riesgos TI: Estructura y cultura de la organización, Políticas, Estándares y procedimientos, Tecnología, Arquitectura, Controles, Metodologías de análisis de riesgos, Evaluación de riesgo cuantitativa y cualitativa
8. Mitigación y respuesta al riesgo tecnológico: Opciones de respuesta al riesgo, Técnicas de análisis, Análisis de coste-beneficio, Retorno sobre la inversión, Características del riesgo inherente y el riesgo residual, Business Continuity Planning y Disaster Recovery Planning, Sitios de contingencia
9. Monitorización y reporte de riesgos: Indicadores clave de riesgo y clave de desempeño
10. Gobierno de seguridad de tecnología de la información: Metas y objetivos del negocio, Definiciones de roles y responsabilidades,
El rol del CISO en una compañía

Módulo II

RIESGO OPERACIONAL Y REPUTACIONAL

I.La gestión del riesgo operacional y reputacional

1. Generalidades
2. Gestión cualitativa del riesgo operacional
3. Gestión por procesos e indicadores
4. Gestión cuantitativa del riesgo operacional
5. Capital por riesgo operacional
6. Modelo de gestión del riesgo operacional
7. Riesgo reputacional
Modelización del riesgo operacional
8. Marco regulatorio. Segmentación. Identificación de drivers
Método del Indicador Básico y Estándar

II.Método de los Modelos Avanzados (Advanced Measurement Approach- AMA)

9.Características del riesgo operacional y pasos a seguir en la modelización
10.Identificación de fuentes de información
Bases de datos interna y externas Escenarios
Factores de entorno de negocio y control de riesgos (Business Environment and internal control factors – BEICFs)
Segmentación
11.Identificación de drivers del riesgo operacional susceptibles de ser modelizados
12. Modelización de drivers. Distribución de pérdidas. Mitigación del riesgo

¿CÓMO MATRICULARSE?

El perfil de un alumno Nemesis:

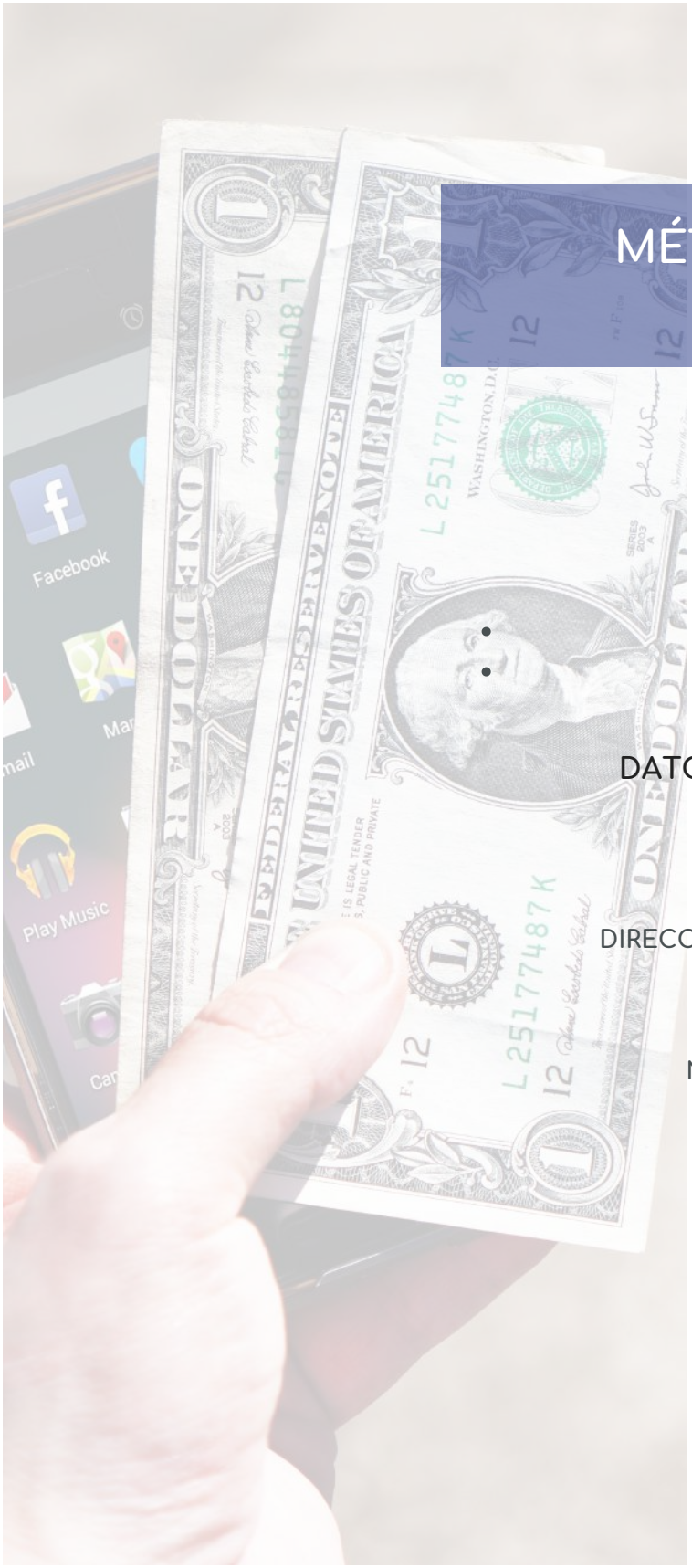
PROFESIONAL EN RIESGOS CON AÑOS DE EXPERIENCIA LABORAL

MOTIVADO PARA MARCAR LA DIFERENCIA EN SU EMPRESA, INDUSTRIA Y COMUNIDAD

APTITUD PARA EL ÉXITO EN UN PROGRAMA RIGUROSO PERO FLEXIBLE

Pasos a seguir para matricularse

- Realiza la inscripción en www.nemesisrisk.com o a traves de info@nemesisrisk.com
- Es necesario que registres tus datos en nuestro formulario de inscripción
- Si dispones de un código cliente debes indicarlo en el formulario para beneficiarte de nuestros descuentos
- Formas de pago: Único pago mediante transferencia bancaria. Una vez comprobada la transferencia, Nemesis proporcionará las claves de acceso
- Habla con tu departamento de capacitación si la certificación es viable para entrar en vuestro plan de formación y presupuesto anual
- Consulta con nosotros el programa de becas para participantes que se autofinancian la certificación (plazas limitadas y no acumulable con otras promociones)



MÉTODOS DE PAGO

- Tarjeta de crédito
- Transferencia bancaria

DATOS PARA TRANSFERENCIA BANCARIA

NEMESIS FORMACIÓN, S.L
CIF:B-86937976
DIRECCIÓN: CALLE JAZMINES, 4, TORRELODONES
28250 MADRID - ESPAÑA

NOMBRE DE LA ENTIDAD BANCARIA: BANKIA
IBAN: ES4820382447646000611284
CODIGO SWIFT: CAHMESMMXXX
SUCURSAL: 2447

ASBA
ASOCIACIÓN DE SUPERVISORES BANCARIOS DE LAS AMÉRICAS

CGRE
Club de Gestión de Riesgos de España

FELABAN
FEDERACIÓN LATINOAMERICANA DE BANCOS

MATRÍCULA E INSCRIPCIÓN
www.nemesisrisk.com

nemesis