



IBI UNIVERSIDAD BANCARIA

DECRETO EJECUTIVO N° 952 de 11 de Noviembre de 2016

Asociación Bancaria de Panamá

LA FEDERACIÓN LATINOAMERICANA DE BANCOS - FELABAN Y EL COMITÉ LATINOAMERICANO DE SEGURIDAD BANCARIA - CELAES

LE OFRECEN EL

“DIPLOMADO EN PREVENCIÓN DE RIESGOS INTEGRALES EN LA SEGURIDAD BANCARIA”

FECHA DE INICIO: 23 de enero de 2017

COSTO: USD\$ 660.00 por módulo

INFORMACIÓN GENERAL:

El Diplomado en Prevención de Riesgos Integrales en la Seguridad Bancaria se crea bajo la responsabilidad de la Federación Latinoamericana de Bancos - FELABAN y su Comité Técnico en Expertos de Seguridad Bancaria – CELAES, adscrito a FELABAN.

Este diplomado se impartirá en los países latinoamericanos, con el apoyo de las asociaciones de Bancos miembros de FELABAN, y en alianza con una Universidad de reconocido prestigio en cada país.

DIRIGIDO A: Personal ejecutivo de mandos medios y altos de entidades del sector financiero.

OBJETIVO: Está enfocado en ampliar y fortalecer los conocimientos de sus participantes en las distintas áreas de la prevención del fraude y riesgo tecnológico en los países miembros de FELABAN, brindando los conocimientos técnicos adecuados sobre la materia.

PERFIL DEL EGRESADO: El Diplomado en Prevención de Riesgos Integrales en la Seguridad Bancaria permitirá al profesional tener capacidad para formarse como líder en esta materia y capacitarse en la toma de decisiones; así como entrenarse para la implementación de estrategias que conduzcan a detectar, gestionar y mitigar el Fraude y Riesgo Tecnológico en sus sistemas e instituciones.

DURACIÓN: El Diplomado en Prevención de Riesgos Integrales en la Seguridad Bancaria fue estructurado para ser estudiado en seis módulos cada uno, con una duración de dos meses virtuales (7 semanas), para un total de 20 horas de cátedra presencial.

FACILITADORES: Los catedráticos son profesionales con amplia experiencia en la dirección, administración y manejo de la prevención y seguridad en el sector bancario.

PARA MAYOR INFORMACIÓN:

Central Telefónica (507) 263-2031, fax (507) 263-3250, correo electrónico: informacion@ubancaria.ac.pa

Para inscripciones ver la página web: www.ubancaria.ac.pa

METODOLOGÍA Y MATERIAL DIDÁCTICO:

- El Diplomado en Prevención de Riesgos Integrales en la Seguridad Bancaria tiene un componente virtual y un componente presencial:
- Cátedra virtual: nuestros cursos cuentan con múltiples herramientas en el educador virtual “Virtual Applications”, donde el alumno encontrará lo necesario para realizar su estudio, conocer los trabajos que va desarrollando y los que le queden por concluir. Cada semana, el alumno deberá estudiar los contenidos preestablecidos por su tutor, al igual que deberá realizar las correspondientes evaluaciones y ejercicios que le permitan ejercitarse, poniendo en práctica los conocimientos teóricos adquiridos
- Cátedra presencial: Los **facilitadores** de cada uno de los módulos del Diplomado se trasladarán a cada uno de los países donde se desarrolle el mismo, e impartirán veinte (20) horas de cátedra a los estudiantes en la universidad designada para tal fin.

Contenido: Los contenidos del Diplomado en Prevención de Riesgos Integrales en la Seguridad Bancaria han sido elaborados por un equipo multidisciplinario, conformado por expertos en la materia que se desarrolla. El temario del curso tiene un formato dinámico e interactivo, de manera que se podrá participar activamente en el proceso de aprendizaje → En la construcción del mismo se han utilizado una serie de iconos y links, que requieren su participación en el descubrimiento de los contenidos → De esta manera, el seguimiento del curso se convierte en una experiencia dinámica que requiere de una participación activa del alumno, lo que facilita la rapidez en la comprensión y uso de la información.

▪ **Evaluación:** Las calificaciones de cada módulo estarán conformadas por las evaluaciones de la parte virtual del programa, la calificación del trabajo de investigación y la del examen final. El módulo deberá ser aprobado con un puntaje de 81/100

▪ **Metodología a Aplicar:** Durante el período de enseñanza virtual, el facilitador transmitirá a los participantes, material de lectura relacionado con cada uno de los temas que conforman el módulo, independientemente del material que haya elaborado el propio instructor a fin de complementarlo. Las lecturas complementarias del material guía, serán remitidas oportunamente y se harán preguntas que serán transmitidas vía internet para que sean respondidas por cada participante. Este diplomado tiene en todos sus módulos enseñanza práctica a través de casos de estudio.

▪ **Forma de pago:** Anticipado antes del inicio de cada módulo, en el IBI.

▪ **Inscripciones:** Instituto Bancario Internacional

▪ **Lugar de clases:** Instituto Bancario Internacional, Ciudad de Panamá

▪ Estos pagos comprenden las clases virtuales, las clases presenciales, material de estudio, un coffee break por la mañana, almuerzo los días jueves y viernes y certificados de aprobación emitidos por IBI y FELABAN.

▪ Para tener derecho al certificado de aprobación del Diplomado se tiene que haber aprobado y pagado todos los módulos, según las condiciones de este Programa.

▪ **Horario de clases presenciales en Panamá:** la última semana de estudio de cada módulo al terminarlo así:

▪ Jueves, de 08:00 a.m. A 05:00 p.m. (8 horas)

▪ Viernes, de 08:00 a.m. A 05:00 p.m. (8 horas)

▪ Sábado, de 08:00 a.m. A 12:00 m.d. (4 horas)

▪ Fecha de inicio de cada módulo en Panamá:

▪ Módulo I: Glosario de términos relacionados con los delitos informáticos - Cátedra virtual: 23 enero de 2017 - Cátedra presencial : 16 de marzo de 2017

▪ Módulo II: Problemática global del cibercrimen.- Cátedra virtual 20 de marzo de 2017– Cátedra presencial: 11 de mayo de 2017

▪ Módulo III: Administración y gestión de los riesgos . - Cátedra virtual: 15 de mayo de 2017– Cátedra presencial: 6 de julio de 2017

▪ Módulo IV: Informática Forense - Cátedra virtual: 10 de julio de 2017 – Cátedra presencial: 31 agosto de 2017

▪ Módulo V: Administración de la Seguridad T.I. - Cátedra virtual:4 de septiembre de 2017 – Cátedra presencial: 26 de octubre 2017

▪ Módulo VI: Gestión del Riesgo de Fraude Interno y Externo - Cátedra virtual: 30 de octubre de 2017– Cátedra presencial: 18 de enero de 2018

MÓDULO I: GLOSARIO DE TÉRMINOS RELACIONADOS CON LOS DELITOS INFORMÁTICOS**Profesor: Santiago Rodriguez (Ecuador)**

- Botnets
- Carding
- Hacker
- Cracker
- Hoax
- Keylogger
- Malware
- Pharming
- Phishing
- Pruebas de concepto
- Re-mailer
- Scam o Phishing laboral
- SMiShing
- Spam o Correo basura
- Spammer
- Spammer lists
- Spear phishing
- Spoofing
- IP Spoofing
- ARP Spoofing
- Web Spoofing
- Tramas de “pump and dump”
- Vishing
- Web bug
- Glosario términos de ataque red y ejemplos de ataques
- Ataques Web ejemplo ataque
- Malware - ejemplos
- Glosario Cybersecurity y Cybercrimen

MÓDULO II: PROBLEMÁTICA GLOBAL DEL CIBERCRIMEN.**Profesor: Coronel Fredy Bautista García (Colombia)**

- Conceptos
- Tipos de amenazas
- Ciberdelincuencia.
- Modalidades de Fraude.
- Cloud, Big Data.
- El crimen organizado
- Correlación y minería de datos
- Rol de la Banca para prevenir amenazas
- Migración de ataques físicos a lógicos
- Fuga de información
- Legislación en Latinoamérica.
- Armonización del cibercrimen en el ámbito internacional. -conductas afines en varios países.
- Modelos y mecanismos de cooperación internacional para enfrentar la amenaza.
- Tendencias globales y propuestas de modelos de investigación conjunta (ámbito judicial y sector financiero)
- Análisis de casuística sobre incidentes relevantes de Ciberdelincuencia y Ciberataques.
- Riesgo Reputacional.
- Seguridad Perimetral. Análisis de casos de Vulnerabilidad.
- Relación del desarrollo militar/científico con los riesgos de ciberseguridad.

MÓDULO III: ADMINISTRACIÓN Y GESTIÓN DE LOS RIESGOS.

Profesor: Juan Martin Garcia Parra (Colombia)

- Establecer Riesgos
- Establecer Criterios o Principios de Gestión del Riesgo
- Valoración del Riesgo
- Metodología Para el Análisis de Riesgos
- Procesos para Evaluación de Riesgos
- Plan de Tratamientos de Riesgos
- Comunicación y Monitoreo de Riesgos
- Responsabilidades del riesgo
- Amenazas y Vulnerabilidades de TI

MÓDULO IV: INFORMÁTICA FORENSE

Profesor: Ferney de Jesus Tabora Araque (Colombia)

- Introducción a la Informática forense, herramientas y procedimientos.
- Recopilación y preservación de evidencias digital.
- Análisis de datos y reconstrucción de evidencias
- Retos y dificultades en un análisis forense
- Análisis forense en sistemas operativos
- Análisis forense en red y dispositivos móviles
- Creación y presentación de Informes técnicos.

MÓDULO V: ADMINISTRACIÓN DE LA SEGURIDAD T.I.

Profesor: José Ariel Bejarano (Colombia)

Gobierno de TI y /Ciberseguridad .

- Estándares y mejores prácticas

Gestión de la Seguridad de la información

- Clasificación y gestión de activos de información

Gestión del control de Acceso

- Gestión de usuarios
- Control acceso Físico
- Autenticación Robusta
- Perfilamiento, segregación roles y permisos.

Seguridad de la Red

- Arquitectura y segmentación de la red
- Protocolos de seguridad

Seguridad de las aplicaciones

- Ciclo de desarrollo
- Hardening y actualizaciones de Seguridad
- Gestión de vulnerabilidades

Identificación de vulnerabilidades y planes de remediación.

Gestión de terceros**Continuidad del negocio**

- BIA
- DRP

Conceptos sobre Seguridad en la Nube

MÓDULO VI: GESTIÓN DEL RIESGO DE FRAUDE INTERNO Y EXTERNO

Profesor: Carlos Ramirez Acosta (México)

- Normas básicas de gestión del riesgo
- Metodologías de Evaluación de Riesgos
- Métodos Para la Determinación de Responsables
- Recursos Para el Establecimiento de Personal Confiable
- Uso del Polígrafo para Orientar Investigaciones
- Validez de las pruebas Digitales en el Proceso Investigativo
- Perfilamiento del Delincuente
- Prevención de Sabotaje y Espionaje Industrial
- Entrevista e Interrogatorio
- Conveniencia del Emprendimiento de Procesos Judiciales
- Corrupción