## INVITACIÓN

Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad fue creado por la Federación Latinoamericana de Bancos - FELABAN y su Comité Latinoamericano de Seguridad Bancaria - CELAES. Este programa se impartirá en República Dominicana en alianza con la Pontificia Universidad Católica Madre y Maestra PUCMM.

## OBJETIVO

El principal objetivo de El Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad, está enfocado en ampliar y fortalecer los conocimientos de sus participantes en las distintas áreas de la prevención del fraude y riesgo tecnológico, brindando los conocimientos técnicos adecuados sobre la materia.

## ¿A QUIÉN ESTÁ DIRIGIDO ESTE PROGRAMA?

El público objetivo del Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad está enfocado en Directivos, Gerentes y Ejecutivos de entidades del sector financiero o personas que por su trabajo e intereses profesionales requieren ampliar sus conocimientos sobre prevención de fraude y riesgo tecnológico.

## PERFIL DEL EGRESADO

Este Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad 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 mitigar el fraude y riesgo tecnológico en sus instituciones.

## DURACIÓN

El Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad, fue estructurado para ser estudiado en seis (6) módulos cada uno, con una duración de dos (2) meses virtuales (7 semanas) más 20 horas de cátedra presencial.

**INVERSIÓN**
US$1,050 por módulo, por participante

**PARA INFORMACIÓN**
Alexandra Espinal
caespinal@aba.org.do

Indira Jiménez
ijimenez@aba.org.do

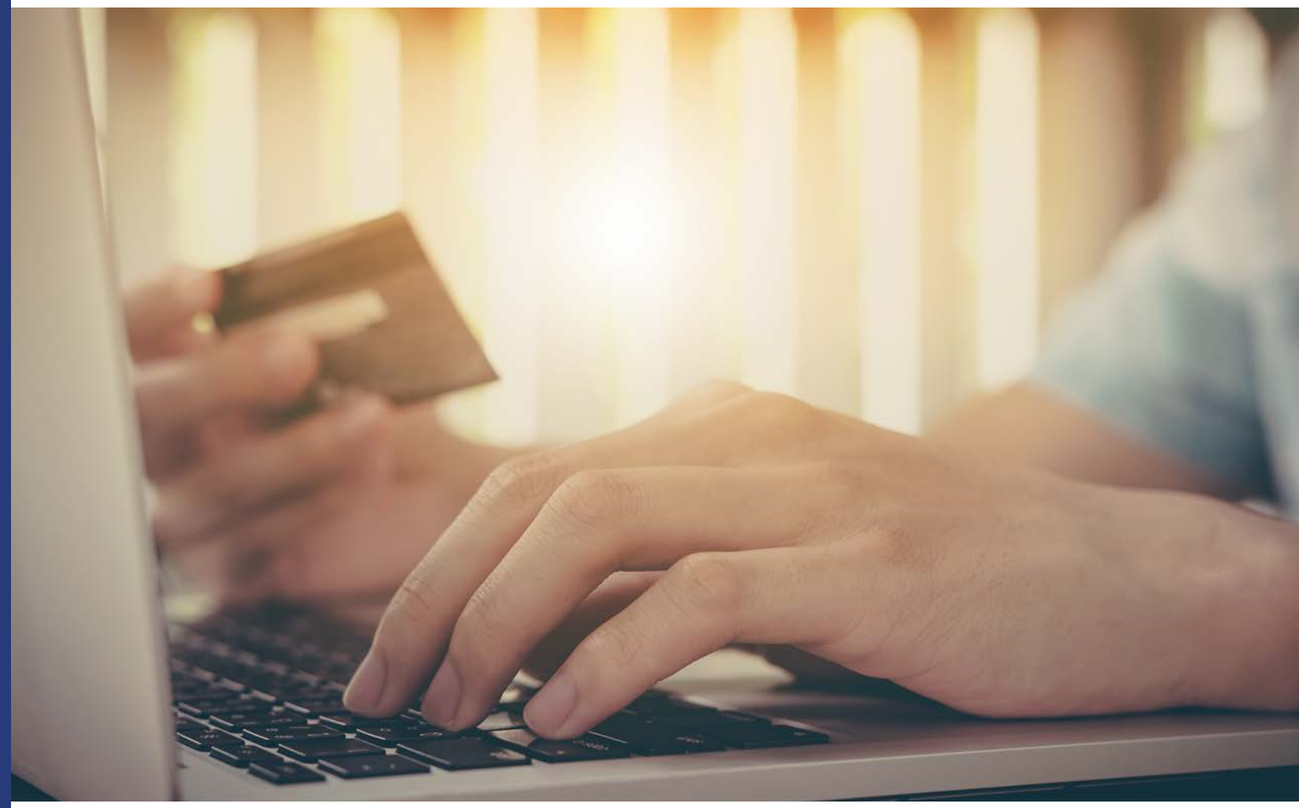
**Tel.** (809) 541-5211
**Fax** (809) 541-9171

## SÍGUENOS

Asociación de Bancos Comerciales de RD
@aba_rd
@bancosrd

**Asociación de Bancos Comerciales de la República Dominicana, Inc. (ABA)**
Av. Winston Churchill esq. Luis F. Thomen Torre BHD, Piso 6, Santo Domingo, R.D.

# Módulo IV. Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad



## Fecha de Inicio

## 25 Noviembre 2019

## ¿POR QUÉ ES IMPORTANTE ESTE PROGRAMA?

La creciente evolución del cibercrimen y lo rentable que llega a ser, ha impulsado una gran oleada de fraudes donde sus principales víctimas son los bancos y sus clientes.

Se calcula que el impacto económico de dicha actividad puede llegar a ser para el 2020 de unos USD$ 7 trillones a nivel mundial, es por esto que tenemos que estar preparados para afrontar esta situación lo que se ha convertido en una prioridad; ataques como CARBANAK donde robaron más de 1000 millones de dólares a entidades financieras en más de 30 países utilizando spear Phishing, y otros más recientes como los presentados a bancos en India, México, Rusia, Canadá, Chile y USA donde los ciberdelincuentes vulneraron la seguridad y materializaron fraudes por decenas de millones de dólares, varios grupos de Hacker como Lazarus Group, APT Group, que están generado miles de ataques diariamente a diferentes empresas con el fin de apoderar de la información y materializar fraudes, campas de malware como Emotet las cuales usan datos adjuntos maliciosos en Word y PDF para infectar y tomar posesión de las máquinas.

FELABAN lo invita a prepararse en el Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad, en el cual por medio de 6 módulos se aprenderá cómo opera el delincuente y cuáles son las principales modalidades de fraude, cómo deben las empresas administrar la ciberseguridad y los riesgos, identificar cómo, cuándo y desde dónde un atacante puede vulnerar la seguridad de su empresa. Es esta la mejor opción y oportunidad para educarse de la mano de expertos catedráticos de diferentes países.

## CONTENIDO

Los contenidos del Programa de Formación en Prevención de Riesgos Integrales de Ciberseguridad, han sido elaborados por un equipo multidisciplinario, conformado por expertos en la materia que se desarrolla. Los catedráticos son profesionales con amplia experiencia en la dirección, administración y manejo de la prevención y seguridad en el sector bancario.

El temario del Diplomado 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.

## METODOLOGÍA Y MATERIAL DIDÁCTICO

**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 maestros de cada uno de los módulos del Programa 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.

| MÓDULO | TEMA | CATEDRÁTICOS |
|---|---|---|
| MÓDULO I | **Introducción a los Delitos Informáticos que afectan al Sistema bancario** | **Santiago Rodríguez -** Ecuador |
| MÓDULO II | **Problemática Global del Cibercrimen.** | **Cnel. Fredy Bautista García -**Colombia |
| MÓDULO III | **Administración y Gestión de los Riesgos** | **Juan Martín García Parra** - Colombia |
| MÓDULO IV | **Informática Forense.** | **Ferney Taborda Araque -** Colombia |
| MÓDULO V | **Administración de la Seguridad I.T.** | **Jose Ariel Bejarano M. -** Colombia |
| MÓDULO VI | **Gestión del Riesgo de Fraude Interno y Externo** | **Carlos Ramirez Acosta**- México |

# PROGRAMA ACADÉMICO

**MÓDULO I. Introducción a los Delitos Informáticos. Glosario de términos**
**Catedrático:** Santiago Rodríguez - Ecuador
- Introducción.
- Conceptualización.
- Características del delito.
- Tipificación de los delitos.
- Impacto de los delitos informáticos.

**MÓDULO II. Problemática Global del Cibercrimen**
**Catedrático:** Cnel. 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.

**MÓDULO III. Administración y Gestión de los Riesgos**
**Catedrático:** Juan Martín García 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 T.I.

**MÓDULO IV. Informática Forense**
**Catedrático:** Ferney Taborda 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 TI**
**Catedrático:** Jose Ariel Bejarano M. - Colombia
1. Gobierno de TI Y Gobierno de seguridad.
- Estándares y mejore prácticas para el gobierno TI.
- Gobierno TI Y la gestión del riesgo.
- Gobierno de Ciberseguridad.

2. Gestión de Seguridad de la Información.
- Gobierno y roles en la gestión de seguridad.
- Marco general de la gestión de seguridad.
- Marco de referencia para un proceso de gestión de seguridad.

3. Gestión Seguridad TI.
- Arquitectura de Red.
- Protocolos y control de tráfico.
- Controles criptográficos.
- Control de Acceso Lógico y Físico.
- Seguridad en aplicaciones.
- Desarrollo seguro – Mejores prácticas.
- Seguridad en Bases de Datos.
- Gestión de vulnerabilidades.

4. Monitoreo Continuo de seguridad de la información y respuesta a incidentes.
- Marco de referencia de Ciberseguridad y monitoreo continuo.
- Marco de referencia para gestión de incidentes.

5. Gestión de la seguridad con terceros.
6. Seguridad en Nube.
7. Continuidad del negocio.

**MÓDULO VI. Gestión del Riesgo de Fraude Interno y Externo**
**Catedrático:** Carlos Ramirez Acosta- México
- Normas básicas de gestión del riesgo y de la prevención del Fraude.
- Metodologías de Evaluación de Riesgos con base en el Modelo ACFE-COSO.
- Análisis de Responsabilidades y Métodos para la Determinación de Responsables.
- Recursos para el establecimiento de Personal Confiable.
- Uso de Herramientas de Evaluación de Credibilidad y de Control de Confianza, para Orientar investigaciones.
- Polígrafo (“Detector de mentiras”).
- Metodología Ocular-Motora (detección del engaño a través de análisis ocular).
- Pruebas de Integridad y Honestidad (test computarizados).
- Análisis de Estrés de la Voz.
- Análisis de las Microexpresiones.
- Validez de las Pruebas Digitales en el Proceso Investigativo.
- Perfilamiento del Delincuente.
- Prevención y Tratamiento de Sabotaje y Espionaje Comercial.
- Entrevista e Interrogatorio en Entidades Financieras.
- Conveniencia del Emprendimiento de Procesos Judiciales.
- Análisis de la Corrupción y del Crimen Organizado Transnacional.