

PROGRAMA

Prevención del Fraude en el ámbito de **la Ciberseguridad y Machine Learning**



DETALLES DEL PROGRAMA

-  **Costo total:** 25 horas de soporte por persona
-  **Duración:** 120 horas (4 horas semanales)
-  **Modalidad:** Remoto en vivo (Horario de España)



Diploma acreditado por la
Universidad Rey Juan Carlos de España



Universidad
Rey Juan Carlos

Plus Ti

PRE-INSCRIPCIÓN



Información del curso

Se trata de un convenio de colaboración para la creación de un espacio de formación específico en materia de fraude y ciberseguridad en medios de pago para el sector financiero, que busca proporcionar una visión global del ecosistema, que les permita reconocer los principales actores en el crimen financiero, que desarrollen capacidades para liderar y planear una estrategia de corto, mediano y largo plazo y un esquema interdisciplinario de protección y de prevención de fraude.

Es un espacio de formación superior con un diploma acreditado por la Universidad Rey Juan Carlos de España, que les permitirá a los participantes poder utilizar distintos elementos para mejorar su capacitación y conocer ¿cuáles son los problemas en materia de fraude y ciberseguridad?, además de ¿cómo se pueden proteger?, ¿cuáles son las mejores estrategias de defensa?, cómo los están atacando? y muy importante, ¿cómo utilizar todas estas nuevas tecnologías y el conocimiento matemático para poder contener todo este tipo de daño que se está causando a nuestra sociedad. La Universidad Rey Juan Carlos cuenta con personal con muchos años de experiencia, apasionados de la problemática del fraude, de la ciberseguridad, de la capacidad de protección, que les transferimos a nuestros alumnos para proteger las actividad en nuestra entidades. La Universidad Rey Juan Carlos, preparó en coordinación con Plus Technologies que cuenta con una amplia trayectoria en temas de combatir el crimen financiero, un programa que creemos se ajusta a las necesidades para fortalecer la formación de los profesionales de fraude



MÓDULO I

36 horas

Marco Conceptual

■ Principios de Ciberseguridad

Inteligencia de Amenazas.
Gestión de la Ciberseguridad.

■ Principios de Ciberseguridad

Conceptualización del riesgo.
Marco general de tipologías de riesgos.
Gestión del riesgo.
Tipologías de riesgos de fraude.
Auditoría interna.
Líneas de defensa.

■ Principios de Ciberseguridad

■ Efectos de la gestión del fraude derivados de la ausencia de:

Confidencialidad.
Integridad.
Disponibilidad.
Autenticidad.
Trazabilidad.

■ Ciberseguridad y Cibercrimen.

Taxonomía de terminología de ciberseguridad.
El rol de la ciberseguridad contra el Cibercrimen.
Perfilamiento de criminales (motivaciones).
Como opera una red cibercriminal.
Controles y defensas para anticiparnos a fraudes.
Sinergias, cohesión entre Ciber, Fraude y Blanqueo.

MÓDULO II

36 horas

Normativa

■ Políticas de seguridad

Seguridad ascendente vs descendente.
Políticas de información de la seguridad -detalle.
Gestión de riesgos y auditoría interna.

■ Introducción a la seguridad de la información

ISO 27001.

PCI DSS.
Estándar PSD2.
Know Your Customer (KYC)

■ Introducción al marco de la ciberseguridad NIST

Introducción.
Identificar.
Proteger.
Detección.
Respuesta y recuperación.

■ Normativa banca abierta

MÓDULO III

36 horas

Ciberseguridad y Machine Learning

■ Operaciones de ciberseguridad y fraude

Introducción a las arquitecturas de seguridad.
Monitorización de la seguridad.
Monitorización de fraude.
Monitorización conjunta: Fusion Centers

■ SOC/CERT Gestión de incidentes

Equipo de respuesta de prevención de fraudes en SOC/CERT.

Cómo manejar de forma correcta la gestión de incidentes en la prevención de fraude.

Cómo manejar insiders dentro de la organización (Introducción)

■ Criptografía

Principios básicos de criptografía.

Aplicaciones de la criptografía.

■ Principios del Machine Learning

Ciencia de datos.

Principios básicos de inteligencia artificial y Machine Learning.

Machine Learning: primeros pasos.

Casos de uso y aplicación práctica.

■ Ciberseguridad y Cibercrimen.

Modelos de Machine Learning predictivos aplicados a Fraude.

Limpieza y preprocesado de datos 8.

Medidas de calidad de la información y el proceso.

Función de coste.

Modelos supervisados.

Modelos no supervisados.

Detección de anomalías.

Modelos abiertos de intercambio de

Machine Learning ONNX.

MÓDULO IV

10 horas

Fraude en Medios de Pagos

■ Medios de pago y sus amenazas

Ecosistema de medios de pagos y sus amenazas.

Cibercrimen Financiero y perfil del defraudador.

■ Investigación y gestión de casos

Ecosistema de medios de pagos y sus amenazas.

Cibercrimen Financiero y perfil del defraudador.

■ Evolución

Nuevos actores en el ecosistema financiero y sus amenaza.

MÓDULO IV

10 horas

Gestión de Fraude

■ Ingeniería de seguridad en prevención de fraude.

Técnicas de ataque / APT.

Estrategias de prevención y contención.

Detección de Procesos basados en logs.

■ Estudios de caso

■ Mitre y prevención de fraude.

Métricas y medidas de fraude y ciberseguridad basadas en Mitre vectores de ataque y Defensas (Realms).

■ Prevención de fraude, técnicas y falsos positivos.

Análisis de casos de fraude de los últimos años

Técnicas de Investigación

Mejores prácticas en la prevención de fraude y seguridad

Caso Práctico DFS

■ Fundamentos del Darkweb

MÓDULO V

10 horas

Desarrollo de habilidades blandas

■ Gestión de equipos y toma de decisiones

Liderazgo

Toma de decisiones.

■ Gestión del fraude y el entorno de negocio.

Cómo hacer y presentar un business case.

Negociación 3D (arriba, igual, abajo)

Gestión, Estrategia y Organización