www.fermacrisk.com

mariana.ibancovichi@fermacrisk.es

Inteligencia Artificial en CiberSeguridad

Material:

Presentaciones: PDF
Ejercicios: Python, Cython, R y Jupyterlab

Duration: 30 h

Price: 5.900 €

COURSE OBJECTIVE

Curso avanzado sobre el uso de la inteligencia artificial para fortalecer la ciberseguridad de los bancos. Se explica brevemente la metodología XOI para medir el ciberriesgo.

Se expone la visión global del CiberRiesgo, los ciberataques y pérdidas que han sufrido las entidades financieras, las metodologías y buenas practicas sobre ciberseguridad en los procesos de negocio y se explican algunos estándares técnicos para la gestión y control, tales como el NIST, Cobit 5 e ISO 27001.

Se exponen metodologías de Cyber Risk Appetite, Cyber Risk Limits y Cyber Risk Tolerance para la gobernanza y control del CiberRiesgo.

Se exponen metodologías tradicionales como la regresión logística y otras, innovadoras, de machine learning, tales como: árboles de decisión, naive bayes, KKN, Regresión logística LASSO, random forest, redes neuronales, redes bayesianas, Support Vector Machines, gradient boosting tree, etc

Se explica el uso de la inteligencia artificial y en particular del machine learning y deep learning para fortalecer la ciberseguridad, se muestran modelos avanzados para detectar anomalías, fraudes transaccionales, phishing, ataques cibernéticos, intrusiones y malware.

Hay cuatro módulos dedicados al deep learning avanzado, el de redes neuronales convolucionadas para el reconocimiento facial, el Generative Adversarial Network (GAN) para detectar ataques adversos de algoritmos de machine learning, las redes neuronales recurrentes para la clasificación de eventos del CiberRiesgo y la multicapa perceptron para la detección de intrusiones y anomalías.

Los ejercicios se han desarrollado en dos potentes lenguajes, Python y R, y se presentan en el entorno JupyterLab para fortalecer el aprendizaje.

¿QUIÉNES DEBEN ASISTIR?

Este programa esta dirigido a directores, gerentes, consultores, reguladores, auditores y analistas de riesgos, riesgos operacionales, ciberriesgos así como aquellos profesionales que se encuentren implantando medidas de

ciberseguridad. Profesionistas que trabajen en entidades bancarias, cajas de ahorro y todas aquellas empresas que se encuentren expuestas al ciberriesgos. Se requiere conocimientos estadísticos y matemáticos.

CiberSeguridad en Basilea III

Módulo 1: CiberResilencia

- CiberRiesgos en la banca
- CiberRiesgos en Latinoamérica y Europa.
- **Normas y directrices de ciberresiliencia**
- Caso Estudio 1: iniciativas regulatorias recientes: los requisitos mínimos de Australia, Alemania y EE. UU
- **Cibergobernanza**
    - Estrategia de ciberseguridad
    - Roles y responsabilidades de gestión
    - Reconocimiento de la importancia de la junta directiva y la alta gerencia
    - Variedad de enfoques de supervisión con respecto a la segunda y tercera líneas de defensa (3LD)
    - Caso de Estudio 2: Roles y responsabilidades de los directores de seguridad de la información (CISO) en la cibergobernanza
    - Cultura de sensibilización sobre el riesgo cibernético
    - Arquitectura y estándares
    - Fuerza laboral de ciberseguridad
    - Caso de Estudio 3: Marcos para la formación profesional en ciberseguridad y programas de certificación
- **Enfoques de gestión de riesgos, pruebas y respuesta y recuperación de incidentes**
    - Métodos para supervisar la ciberresiliencia
        - Los especialistas en riesgos evalúan la gestión y los controles de seguridad de la información
        - Las jurisdicciones se involucran cada vez más con la industria para abordar la ciberresiliencia
    - Pruebas de controles de seguridad de la información y garantía independiente
        - El mapeo y la clasificación de los servicios comerciales deben informar las pruebas y el aseguramiento
        - Prueba de Penetración
        - Taxonomía de controles de riesgo cibernético
    - Pruebas de respuesta y recuperación y ejercicio
        - Evaluación de continuidad del servicio, planes de respuesta y recuperación y aprendizaje continuo
        - Ejercicio conjunto público-privado
        - Caso de Estudio 4: “Exercise Resilient Shield”
    - Métricas de ciberseguridad y resiliencia
        - Las métricas de ciberseguridad y resiliencia
        - Indicadores emergentes emergentes de resiliencia
- **Comunicación e intercambio de información**
    - Descripción general de los marcos de intercambio de información entre jurisdicciones
    - Compartir entre bancos o peers información
    - Caso de Estudio 5: FS-ISAC: características y beneficios clave
    - Compartir de los bancos a los reguladores
    - Compartir entre los reguladores

- Caso de Estudio 6 - Intercambio bilateral de información sobre seguridad cibernética entre la Autoridad Monetaria de Hong Kong (HKMA) y la Autoridad Monetaria de Singapur (MAS)

Módulo 2: CiberRiesgos

- Visión Actual del Ciberriesgo
- identificación de los Ciberriesgos
    - Malware y otras amenazas
- Ciber-Seguridad en la práctica
    -
    - Gobierno de la Seguridad
    - Gestión del Riesgo
    - Políticas de Seguridad
    - Política de Salvaguardas
    - Planes de Contingencias
- Auditorías de Seguridad
- Algunos Ciberriesgos
    - Exploits Kits
    - Fuga de información
    - Pishing
    - Ataque DDoS
    - Internet de las cosas
    - Ataque a infraestructuras
    - Botnets
    - Troyanos
    - Malware Avanzado
    - Ransomware
    - APT´s
- Evitación, Aceptación, Mitigación o transferencias de los Ciber-Riesgos (Ciber-Seguros)
- Respuesta a Incidentes
- Aspectos Legales de la Respuesta a Incidentes
- Informática Forense
- Compliance Digital
- Inteligencia en Fuentes Abiertas
- Defensa de la Marca. Derechos de Propiedad Intelectual
- Reputación Digital. Comunicación de Crisis
- Fraude y Gestión de la Identidad Online
- Derecho Informático y de las TIC´s
- Derecho Procesal y Derechos Humanos en el Ciber-Espacio
- Responsabilidad Penal de las Personas Jurídicas
- Criptografía y Sistemas de Autenticación
- Ciber-Seguridad Industrial (IT/OT)
- Ciber-Seguridad Lógica
- Aseguramiento
- CiberRiesgos en la banca
- Robos financieros
- Ataques en las transacciones bancarias
- Robo de tarjetas de crédito
- Banca Mayorista
- Ciber ataque Lazarus en el sistema SWIFT
- Recursos de los bancos destinados en ciberseguridad
- Cloud service provider (CSP)
- Análisis de los principales proveedores CSP
- Análisis y duración de los apagones en el servicio Cloud

Módulo 3: Gestión del CiberRiesgo

- Enterprise Risk Management en el ciberriesgo
- Involucración de la alta dirección
- Ciberseguridad en los procesos de negocios
- Identificación de:
- Activos críticos del banco
- Funciones de negocio críticas
- Socios comerciales críticos: clientes, proveedores, outsourcing
- Data crítica, conexiones críticas
- Principales amenazas al banco
- Framework for Improving Critical Infrastructure Cybersecurity NIST
- Principales Estándares técnicos
    - NIST 800-53
    - Cobit 5
    - ISO 27001
- Politicas y control del ciberRiesgo
- Gobernanza del CiberRiesgo en la práctica
- Líneas de defensa
- Análisis del riesgo
- Mapas de probabilidad e impacto
- Estrategias de mitigación de CiberRiesgo
    - Identidad y gestión de los accesos
    - Protección de la data
    - Security analytics usando machine learning
    - NIST CSF pillars
    - Higiene de seguridad
    - Recovery time objective
    - Recovery point objective
    - SSDLC
    - Gestión del riesgo de la tecnología de terceros
- Arquitectura de seguridad
- Entorno Cloud y mobile security

Módulo 4: Medición de Ciberataques usando Enfoque XOI: Exposición, Ocurrencia e Impacto

- Definición de la exposición
- Selección de los KRIs
- Modelización y condicionamiento de la exposición
- Definición de hipótesis
- Modelización y condicionamiento de la ocurrencia
- Cuantificación de la ocurrencia
- Cuantificación del impacto
- Tipos de indicadores
- Predecibilidad de los indicadores
- Redes Bayesianas
- El modelo de escenario de la red bayesiana
- Interpretación gráfica
- Simulación usando redes bayesianas
- Modelización de XOI para Ciberriesgos en la banca
- Escenarios de CiberRiesgos
- Ciberataques en la banca
- **Ejercicio 1:** Modelización XOI en ciberataques usando redes bayesianas en Python y R

Módulo 5: Cyber Risk Appetite

- Principios de una metodología efectiva de Cyber Risk Appetite

- Definiciones y análisis:
    - Risk appetite framework
    - Risk Appetite Statement
    - Risk Tolerance
    - Risk Capacity
    - Risk Profile
- Establecimiento de Límites en el CiberRiesgo
- Principios de Efectividad del Cyber Risk Appetite Statement
- Establecimiento de Límites y Métricas en CiberRiesgos
- Establecimiento de límites de riesgo y tolerancia en CibeRiesgos
- Incorporación del Cyber Risk Appetite en la toma de decisión, nuevos productos, nuevas líneas de negocio, etc.
- Planes de mitigación

Machine Learning para la Ciberseguridad

Módulo 6: Machine Learning

- Inteligencia Artificial
- Definición del Machine Learning
- Metodología del Machine Learning
    - Almacenamiento de la Data
    - Abstracción
    - Generalización
    - Evaluación
- Aprendizaje Supervisado
- Aprendizaje No Supervisado
- Aprendizaje por Refuerzo
- Deep Learning
- Tipología de algoritmos de Machine Learning
- Pasos para implementar un algoritmo
    - Recogida de información
    - Análisis Exploratorio
    - Entrenamiento del modelo
    - Evaluación del Modelo
    - Mejoras al modelo
    - Machine Learning en riesgo crédito de consumo
- Machine Learning en modelos de credit scoring
- Análisis de principales herramientas: R, Python, Microsoft Azure, SAS Enterprise Miner, SAS Visual Analytics, Knime, IBM SPSS Modellller, Spark,,etc.

Módulo 7: Inteligencia artificial IA para la CiberSeguridad en Banca

- Inteligencia artificial IA para la ciberseguridad
- Detección de anomalías en la seguridad cibernética
    - Modelos avanzados de deep learning
- Uso del Aprendizaje Supervisado en la ciberseguridad
- Uso del Aprendizaje No Supervisado en la ciberseguridad
- Detección y mitigación del Phishing
    - SVM
    - Clustering
- Deep Learning para la detección de ataques y malware
    - Redes Neuronales recurrentes
- Detección de instrusiones
- Network Traffic Analysis
- Detección de botnets
- Machine learning para detectar ataques DDoS

- Detección de fraude en transacciones financieras
- Detección en sensores
- Analítica de fraudes en banca
- Técnicas avanzadas de machine learning para ciberseguridad
- Principales vendors de IA para ciberseguridad
- Herramientas de visualización

Aprendizaje No Supervisado para detección anomalias

Módulo 8: Modelos no supervisados

- Clusters Jerárquicos
- K-Means
- Algoritmo estándar
- Distancia Euclidiana
- Análisis de Componentes principales (PCA)
- Visualización avanzada de PCA
- Eigenvectores e Eigenvalores
- **Ejercicio 2:** Componentes principales en R y SAS
- **Ejercicio 3:** Detección de anomalías con K-Means R

Aprendizaje Supervisado para detectar Fraudes y anomalias

Módulo 9: Regresión Logística y Regresión LASSO

- Modelos de detección de fraude transaccional
- Modelos Econométricos
    - Regresión Logit
    - Regresión probit
    - Regresión Piecewise
    - Modelos de supervivencia
- Modelos de Machine Learning
    - Regresión Lasso
    - Regresión Ridge
- Riesgo de Modelo en la regresión logística
- **Ejercicio 4:** Fraud score Regresión Logística en SAS y R
- **Ejercicio 5:** Fraud score Regresión Logística Lasso en R

Módulo 10: Árboles, KNN y Naive Bayes

- Árboles de Decisión
    - Modelización
    - Ventajas e inconvenientes
    - Procesos de Recursión y Particionamiento
    - Recursive partitioning tree
    - Pruning Decision tree
    - Conditional inference tree
    - Visualización de árboles
    - Medición de la predicción de árboles de decisión
    - Modelo CHAID
    - Modelo C5.0
- K-Nearest Neighbors KNN
    - Modelización
    - Ventajas e inconvenientes

    - Distancia Euclidiana
    - Distancia Manhattan
    - Selección del valor K
- Modelo Probabilístico: Naive Bayes
    - Bayes Ingenuo
    - Teorema de Bayes
    - Estimador de Laplace
    - Clasificación con Naive Bayes
    - Ventajas e inconvenientes
- **Ejercicio 6:** Detección de anomalías con árbol de decisión R
- **Ejercicio 7:** Detección de anomalías KNN en R y SAS
- **Ejercicio 8:** Detección de anomalías Naive Bayes en R

Módulo 11: Support Vector Machine SVM

- SVM con variables dummy
- SVM
- Hiperplano óptimo
- Support Vectors
- Añadir costes
- Ventajas e Inconvenientes
- Visualiización del SVM
- Tuning SVM
- Truco de Kernel
- **Ejercicio 9:** Detección de anomalías Support Vector Machine en R
- **Ejercicio 10:** Fraud Score support Vector Machine en Python data 2

Módulo 12: Redes Neuronales (Neural Networks NN)

- Neurona artifical
- Entrenamiento de Perceptron
- Perceptrón
- Algoritmo de backpropagation
- Procedimientos de entrenamiento
- Tuning NN
- Visualización de NN
- Ventajas e inconvenientes
- **Ejercicio 11:** Fraud Score usando Redes Neuronales: perceptron multicapas en R data 1
- **Ejercicio 12:** Fraud Score Redes Neuronales en Python data 2

Módulo 14: Ensemble Learning para Phishing

- Modelos de conjuntos
- Bagging
- Bagging trees
- Random Forest
- Boosting
- Adaboost
- Gradient Boosting Trees
- Ventajas e inconvenientes
- **Ejercicio 14:** Detección de phishing Boosting en R
- **Ejercicio 15:** Detección de phishing en R
- **Ejercicio 16:** Detección de phishing Random Forest, R y Python
- **Ejercicio 17:** Detección de phishing Gradient Boosting Trees

Módulo 15: Validación de modelos de Machine Learning

- Validación Out of Sample y Out of time
- Verificación p-values en regresiones
- Validación de series temporales MSE, MAD
- Diagnóstico de los residuos
- Validación cruzada
- Bootstrapping del error
- Matriz de confusión caso binario
- Matriz de confusión caso multinomial
- Curva ROC
- Intervalos de confianza
- Jackknifing con test de poder discriminante
- Bootstrapping con test de poder discriminante
- Estadístico Kappa
- K-Fold Cross Validation
- Análisis Semafórico
- **Ejercicio 18:** K-Fold Cross Validation de modelos de machine learning y deep learning en Python y R
- **Ejercicio 19:** Estimación curva ROC en Python y R
- **Ejercicio 20:** Bootstrapping de ROC en R
- **Ejercicio 21:** Estimación Kappa y matriz de confusión multinomial y binaria en Python y R

Deep Learning: anomalías, intrusiones, Reconocimiento Facial y ataques adversos

Módulo 16: Deep Learning

- Definición y concepto del deep learning
- ¿Porque ahora el uso del deep learning?
- Arquitecturas de redes neuronales
- Función de activación
    - Sigmoidal
    - Rectified linear unit
    - Hipertangente
    - Softmax
- Función de costes
- Optimización con Gradiente descendiente
- Uso de Tensorflow
- Uso de Tensorboard
- R deep Learning
- Python deep Learning
- Uso del deep learning
    - ¿Cuantas capas ocultas?
    - ¿Cuantas neuronas, 100, 1000?
    - ¿Cuantas épocas y tamñao del batch size?
    - ¿Cual es la mejor función de activación?
- Software Deep Learning: Caffe, H20, Keras, Microsoft, Matlab, etc.
- Software de implementación: Nvidia y Cuda
- Harware, CPU, GPU y entornos cloud
- Tipología de Deep Learning
- **Feedforward neural network**
    - Perceptrón Multicapa
- **Redes neuronales convolucionales**
    - Uso del deep learning en la clasificación de imágenes
- **Redes neuronales recurrentes**
    - Series temporales

- Long Short Term Memory

Módulo 17: Deep Learning Redes Neuronales Feed Forward para anomalías, intrusiones y análisis de tráfico

- Ciberriesgos intrusiones
- Network traffic analysis
- Single Layer Perceptron
- Multiple Layer Perceptron
- Arquitecturas de redes neuronales
- Función de activación
  - Sigmoidal
  - Rectified linear unit (Relu)
  - Elu
  - Selu
  - Hipertangente hiperbólica
  - Softmax
  - Otras
- Back-propagation
  - Derivadas direccionales
  - Gradientes
  - Jacobianos
  - Regla de la cadena
  - Optimización y mínimos locales y globales
- **Ejercicio 22:** Detección de anomalías de series temporales usando LSTM
- **Ejercicio 23:** Detección de intrusiones usando redes neuronales convolucionadas
- **Ejercicio 24:** Network traffic análisis usando redes neuronales multicapa perceptron

Módulo 18: Deep Learning Redes Neuronales Convolucionales CNN para Reconocimiento facial

- Reconocimiento Facial para la ciberseguridad
- CNN para imagenes
- Diseño y arquitecturas
- Operación de convolución
- Gradiente Descendiente
- Filter
- Strider
- Padding
- Subsampling
- Pooling
- Fully connected
- Credit Scoring usando CNN
- Estudios recientes de CNN aplicados al riesgo crédito y scoring
- **Ejercicio 25:** Reconocimiento Facial usando Deep Learning CNN

Módulo 19: Deep Learning Redes Neuronales Recurrentes RNN

- Selección y clasificación de ciberriesgos
- Natural Language Processing
- Natural Language Processing (NLP) text classification
- Long Term Short Term Memory (LSTM)
- Hopfield
- Bidirectional associative memory
- Gradiente Descendiente
- Metodos de optimización globales
- RNN y LSTM en las finanzas
- Modelos unidireccionales y bidireccionales

- Deep Bidirectional Transformers for Language Understanding
    - BERT Google
- **Ejercicio 26:** Deep Learning CNN vs RNN para la clasificación de documentos
- **Ejercicio 27:** Credit Scoring usando Deep Learning LSTM

Módulo 20: Adversarial machine learning

- Ataques adversos para la ciberseguridad
- Tipología de ataques adversos
- Muestras adversarias
- Generative Adversarial Network (GAN)
- Fast Gradient Sign Method (FGSM)
- Creación de muestras de malware adversarial utilizando GAN
- **Ejercicio 28:** Ataque basado en gradiente en clasificación de imagen errónea