CURSO

ANALISTA EN CIBERSEGURIDAD Y ANÁLISIS DE INFORMACIÓN CON BIG DATA

SELECT BUSINESS SCHOOL

EMV118

- CON CERTIFICACIÓN UNIVERSITARIA INTERNACIONAL + RECONOCIMIENTO DE 60 ECTS -

DESTINATARIOS

El Programa está especialmente diseñado para aquellas personas que estén interesadas en adquirir conocimientos sobre **Analista en Ciberseguridad y Análisis de Información con Big Data** y que quieran asegurarse un recorrido ascendente en esta área, con una especial elevación y consolidación de competencias.

Permite conocer la informática y la electrónica, la informática, conectividad e internet, los fundamentos de la información y electrónica forense, la ciberseguridad, la cibercriminalidad, el hacking ético, el análisis forense, el soporte de datos, el marco normativo, los dispositivos de telefonía móvil y big data business intelligence. Además, al final de cada unidad didáctica el alumno/a encontrará ejercicios de autoevaluación que le permitirán hacer un seguimiento autónomo sobre los conocimientos adquiridos hasta el momento y la necesidad o no de reforzarlos.

El alumno recibirá acceso a un curso inicial donde encontrará información sobre la metodología de aprendizaje, la titulación que recibirá, el funcionamiento del Campus Virtual, qué hacer una vez el alumno haya finalizado e información sobre Grupo Esneca Formación. Además, el alumno dispondrá de un servicio de **clases en directo**.

FICHA TÉCNICA

CARGA HORARIA
1500H

MODALIDAD
ONLINE
*La modalidad incluye módulos con clases en directo

CURSO INICIAL
ONLINE

TUTORIAS
PERSONALIZADAS

IDIOMA
CASTELLANO

DURACIÓN
HASTA UN AÑO
*Prorrogable

IMPORTE

VALOR ORIGINAL: ~~3880€~~
VALOR ACTUAL: 1940€

CERTIFICACIÓN OBTENIDA

Una vez finalizados los estudios y superadas las pruebas de evaluación, el alumno recibirá un diploma que certifica el "**ANALISTA EN CIBERSEGURIDAD Y ANÁLISIS DE INFORMACIÓN CON BIG DATA**", de SELECT BUSINESS SCHOOL, avalada por nuestra condición de socios de la CECAP y AEEN, máximas instituciones españolas en formación y de calidad.

Los diplomas llevan el sello de Notario Europeo, que da fe de la validez, contenidos y autenticidad del título a nivel nacional e internacional.

Además, el alumno recibirá una Certificación Universitaria Internacional de la Universidad Católica de Cuyo – DQ y Universidad de CLEA con un reconocimiento de **60 ECTS**.

REDES SOCIALES

www.facebook.com/SelectBusinessSchool

www.linkedin.com/school/select-business-school/

@select_business_school

www.escuelaselect.com

@escuela_select

www.escuelaselect.com/blog

CONTENIDO FORMATIVO

MÓDULO 1. INFORMÁTICA Y ELECTRÓNICA

UNIDAD DIDÁCTICA 1. INFORMÁTICA, CONECTIVIDAD E INTERNET

1. La informática
    - Conceptos básicos
2. Componentes de un sistema informático
3. Estructura básica de un sistema informático
4. Unidad central de proceso en un sistema informático
    - Estructura
5. Periféricos más usuales: conexión
6. Sistema operativo
7. Internet
8. Conectividad a Internet
    - Tipos de redes
    - Red inalámbrica

UNIDAD DIDÁCTICA 2. FUNDAMENTOS DE LA INFORMÁTICA Y ELECTRÓNICA FORENSE

1. Concepto de informática forense
2. Objetivos de la informática forense
3. Usos de la informática forense
4. El papel del perito informático
5. El laboratorio informático forense
6. Evidencia digital
    - Evidencias volátiles y no volátiles
    - Etiquetado de evidencias
7. Cadena de custodia

UNIDAD DIDÁCTICA 3. CIBERSEGURIDAD

1. El ciberespacio y su seguridad
2. Riesgos y amenazas de la ciberseguridad
    - Amenazas internas y externas
    - Principales riesgos y amenazas
3. Objetivos de la ciberseguridad
4. Líneas de acción de la ciberseguridad nacional
5. Instituto Nacional de Ciberseguridad

UNIDAD DIDÁCTICA 4. CIBERCRIMINALIDAD

1. Delito informático
    - Principales características del delito informático
2. Tipos de delito informático
3. Cibercriminalidad
    - Evolución de la sociedad española en el empleo de las nuevas tecnologías. Los delitos cibernéticos

UNIDAD DIDÁCTICA 5. HACKING ÉTICO

1. ¿Qué es el hacking ético?
    - Ética hacker
    - Valores de la ética hacker
    - Fases del Hacking Ético
    - Tipo de Hacking Ético
2. Aspectos legales del hacking ético
3. Perfiles del hacker
    - Hacker de sombrero negro
    - Hacker de sombrero blanco
    - Hacker de sombrero gris
    - Otros perfiles
4. Hacktivismo

UNIDAD DIDÁCTICA 6. ANÁLISIS FORENSE

1. El análisis forense
2. Etapas de un análisis forense
    - Estudio preliminar
    - Adquisición de datos
    - Análisis e investigación
    - Presentación y realización del informe pericial
3. Tipos de análisis forense
4. Requisitos para el análisis forense
5. Principales problemas

UNIDAD DIDÁCTICA 7. SOPORTE DE DATOS

1. Adquisición de datos: importancia en el análisis forense digital
2. Modelo de capas
3. Recuperación de archivos borrados
    - Dinámica del borrado de archivos
    - Características exigibles para recuperación de archivos y datos borrados
    - Principales herramientas para recuperación de datos
    - La acción de recuperación
4. Análisis de archivos
    - Firmas características
    - Documentos
    - Archivos gráficos y multimedia
    - Archivos ejecutables

UNIDAD DIDÁCTICA 8. SISTEMA DE GESTIÓN DE SEGURIDAD EN LA INFORMACIÓN SGSI

1. La sociedad de la información
2. ¿Qué es la seguridad de la información?
3. Importancia de la seguridad de la información
4. Principios básicos de seguridad de la información: confidencialidad, integridad y disponibilidad
    - Principio Básico de Confidencialidad
    - Principio Básico de Integridad
    - Disponibilidad
5. Descripción de los riesgos de la seguridad
6. Selección de controles

7. Factores de éxito en la seguridad de la información
8. Introducción a los sistemas de gestión de seguridad de la información
9. Beneficios aportados por un sistema de seguridad de la información

UNIDAD DIDÁCTICA 9. MARCO NORMATIVO

1. Marco normativo
2. Normativa sobre seguridad de la información
    - Planes de acción para la utilización más segura de Internet
    - Estrategias para una sociedad de la información más segura
    - Ataques contra los sistemas de información
    - La lucha contra los delitos informáticos
    - La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
3. Normativa relacionada con la ciberseguridad
4. Legislación sobre delitos informáticos

MÓDULO 2. DISPOSITIVOS DE TELEFONÍA MÓVIL

UNIDAD DIDÁCTICA 1. REDES DE TELEFONÍA MÓVIL

1. Telefonía móvil
    - El espectro radioeléctrico
    - La telefonía vía radio
    - Los sistemas celulares
    - Telefonía móvil automática
    - Terminales
    - Tipología y características
2. Sistemas de comunicación en las redes de telefonía móvil
    - CDMA
    - GSM
    - iDEN

UNIDAD DIDÁCTICA 2. DISPOSITIVOS MÓVILES

1. Teléfonos móviles inteligentes: Smartphone
    - Definición
    - Historia
2. Symbian
3. Windows Phone
    - Características Comunes de Windows Mobile
4. iPhone OS
    - iPhone SDK
5. Android
    - Características
    - Arquitectura de Android

UNIDAD DIDÁCTICA 3. LAS REDES SOCIALES EN LOS DISPOSITIVOS MÓVILES

1. Redes Sociales en dispositivos móviles
2. Tipos de redes
3. Riesgos de las redes
    - Contraseñas y certificados digitales
    - Pautas de seguridad y privacidad en las redes sociales
    - Actualización y protección de dispositivos móviles

- Envío de información sensible por WhatsApp o a partir de WiFi pública
- Geolocalización: Foursquare

UNIDAD DIDÁCTICA 4. SEGURIDAD EN TELEFONÍA MÓVILES

1. Importancia de la seguridad y protección de datos de telefonía móvil
    - Conceptos básicos de seguridad
    - Capas de los dispositivos móviles
2. Ciberseguridad
3. Delitos en telefonía móvil
    - Cibercriminalidad
    - Amenazas en los dispositivos móviles

UNIDAD DIDÁCTICA 5. INFORMÁTICA FORENSE

1. Concepto de informática forense
2. Objetivos de la informática forense
    - La evidencia digital
    - La cadena de custodia
3. Usos de la informática forense
4. El papel del perito informático

UNIDAD DIDÁCTICA 6. PERITAJE EN TELEFONÍA MÓVIL

1. Análisis forense
    - Requisitos para el análisis forense
    - Principales problemas
2. Metodología para el análisis forense
    - Asegurar la escena
    - Identificar la evidencia
    - Adquisición de evidencias
    - Análisis e investigación de la evidencia
    - Informe pericial

UNIDAD DIDÁCTICA 7. SOPORTE DE DATOS

1. Adquisición de datos: importancia en el análisis forense digital
2. Modelo de capas
3. Recuperación de archivos borrados
    - Dinámica del borrado de archivos
    - Características exigibles para recuperación de archivos y datos borrados
    - Principales herramientas para recuperación de datos
    - La acción de recuperación
4. Análisis de archivos
    - Firmas características
    - Documentos
    - Archivos gráficos y multimedia
    - Archivos ejecutables

UNIDAD DIDÁCTICA 8. EQUIPOS ESPECÍFICOS PARA EL ANÁLISIS FORENSE DE DATOS DE TELEFONÍA MÓVIL

1. Equipos de análisis forense para teléfonos móviles
    - MSAB Office
    - MSAB Kiosk
    - MSAB Tablet

- MSAB Field
- Cellebrite UFED Touch Ultimate
- Cellebrite UFED 4PC
- Cellebrite UFED Touch Chinex

2. Herramientas forenses para Whatssap

UNIDAD DIDÁCTICA 9. MARCO NORMATIVO

1. Marco normativo
2. Normativa sobre seguridad de la información
    - Planes de acción para la utilización más segura de Internet
    - Estrategias para una sociedad de la información más segura
    - Ataques contra los sistemas de información
    - La lucha contra los delitos informáticos
    - La Agencia Europea de Seguridad de las Redes y de la información (ENISA)
3. Normativa relacionada con la ciberseguridad
4. Legislación sobre delitos informáticos

MÓDULO 3. BIG DATA Y BUSINESS INTELLIGENCE

UNIDAD DIDÁCTICA 1. ARQUITECTURA BI.

UNIDAD DIDÁCTICA 2. DATA SCIENCE.

UNIDAD DIDÁCTICA 3. BIG DATA Y BASES DE DATOS NOSQL.

UNIDAD DIDÁCTICA 4. ANÁLISIS DE DATOS CON PHYTON.

UNIDAD DIDÁCTICA 5. HERRAMIENTA PLATEAU.

UNIDAD DIDÁCTICA 6. HERRAMIENTA POWERBI.

UNIDAD DIDÁCTICA 7. PROGRAMACIÓN R.

UNIDAD DIDÁCTICA 8. REGULACIÓN Y ESCENARIOS PARA EL USO DEL DATO.

UNIDAD DIDÁCTICA 9. NUEVA REGULACIÓN MARCO EUROPEO PRIVACIDAD Y SEGURIDAD.