GUIA DOCENTE DE LA ESPECIALIDAD CIBERSEGURIDAD

AREA: TECNOLOGÍA CÓDIGO: GDE-653
AUTOR: SPAIN BUSINESS SCHOOL

IDENTIFICACIÓN DE LA ESPECIALIDAD

- Tipo: Especialidad
- Periodo de impartición: Tercer Cuatrimestre
- Nº de créditos (horas): 15 ECTS (375 horas)
- Idioma en que se imparte: Español
- Metodología: Blended

LOS PROFESORES

- Gustavo Vallejo
  Soy un profesional con 20 años de experiencia, 12 de los cuales en Seguridad de la Información. Realicé responsabilidades de consultor senior, especialista técnico, arquitecto de soluciones, líder del equipo y director del proyecto.

  Gerente de servicios de seguridad en Open-Sec. Anteriormente responsable de seguridad en Telefónica ingeniería de Seguridad en Perú.

- Francisco Sanz Moya
  Ingeniero informático por la universidad Autónoma de Madrid. Licenciado en marketing y gestión comercial por ESIC. Varias certificaciones CISCO

  Fundador, Co-CEO, CTO de TSS Ciberseguridad

- Christian Gutiérrez González
  Técnico de sistemas y redes informáticas. Máster en Ciberseguridad. Experto en ciberseguridad ofensiva.

  Fundador, Co-CEO de TSS Ciberseguridad

PRESENTACIÓN Y OBJETIVOS

La ciberseguridad es la práctica de proteger equipos, redes, aplicaciones de software, sistemas críticos y datos de posibles amenazas digitales. Las organizaciones tienen la responsabilidad de proteger los datos para mantener la confianza del cliente y cumplir la normativa. Utilizan medidas y herramientas de ciberseguridad para proteger los datos confidenciales del acceso no autorizado, así como para evitar interrupciones en las operaciones empresariales debido a una actividad de red no deseada. Las organizaciones implementan la ciberseguridad al optimizar la defensa digital entre las personas, los procesos y las tecnologías.

En los negocios de varios sectores, como la energía, el transporte, el comercio al detalle y la fabricación, use sistemas digitales y conectividad de alta velocidad para proporcionar un servicio eficiente al cliente y ejecutar operaciones empresariales rentables. Igual que protegen los recursos físicos, deben proteger también los recursos digitales y los sistemas frente al acceso no intencionado. El evento no intencionado de incumplimiento y acceso no autorizado a un sistema informático, una red o recursos conectados se denomina ciberataque. El éxito de un ciberataque produce la exposición, sustracción, eliminación o alteración de datos confidenciales. Las medidas de ciberseguridad defienden frente a ciberataques y proporcionan los siguientes beneficios.

Es por lo tanto que el curso intenta cumplir los objetivos:

- Prevención o reducción del costo de las brechas
  Las organizaciones que implementan estrategias de ciberseguridad minimizan las consecuencias no deseadas de ciberataques que pueden afectar a la reputación empresarial, las capacidades financieras, las operaciones empresariales y la confianza del cliente. Por ejemplo, las compañías activan planes de recuperación de desastres para contener las posibles intrusiones y minimizar las interrupciones en las operaciones empresariales.

- Mantenimiento de la conformidad normativa
  Las empresas de sectores y regiones específicos deben cumplir con los requisitos normativos para proteger los datos confidenciales frente a posibles riesgos cibernéticos. Por ejemplo, las empresas que operan en Europa deben cumplir el Reglamento General de Protección de Datos (GDPR), que espera que las organizaciones adopten las medidas de ciberseguridad adecuadas para garantizar la privacidad de los datos.

- Mitigación de las ciberamenazas en desarrollo
  Los ciberataques evolucionan a la par que las tecnologías cambiantes. Los delincuentes utilizan nuevas herramientas y elaboran nuevas estrategias para el acceso no autorizado al sistema. Las organizaciones emplean y actualizan las medidas de ciberseguridad para mantenerse al día de estas tecnologías y herramientas de ataque digital nuevas y en desarrollo.

COMPETENCIAS

- Adquirir las capacidades necesarias para obtener, mantener y procesar evidencias digitales utilizando procedimientos y herramientas específicas.

- Desarrollar técnicas y utilizar herramientas que exploten al máximo tus habilidades y conocimientos para la realización de pruebas de intrusión a sistemas y redes.
- Obtener una visión general e introductoria al mundo de la ciberseguridad, explicando los ataques más relevantes y cómo mitigarlos.
- Conocer el mundo de la ingeniería inversa y el análisis de código malicioso, asumiendo los procesos para entender el funcionamiento de los ficheros que trabajan a bajo nivel en sistemas y redes.
- Asimilar los conocimientos suficientes para gestionar y establecer unas políticas claras de seguridad para el componente móvil de un sistema de información.
- Conocer los fundamentos de la monitorización y correlación de eventos de seguridad, mediante el estudio, la elaboración e interpretación de informes reales.
- Realizar desarrollos en programación segura y mejorar tus habilidades en auditoría de seguridad en el análisis y evaluación del código fuente de las aplicaciones.

PROGRAMA

MODULO 1: CIBERSEGURIDAD Y HACKING ÉTICO

1. Introducción a la ciberseguridad
    - Introducción
        - Certificado (Validez, ventajas)
        - Objetivo
        - Metodología
        - Materiales didácticos
        - Oportunidades laborales
        - Definición de hacker
        - Hackers conocidos
        - Hacking ético, profesión
        - Perfil del Hacker ético
        - Tipos de auditorías
    - Arquitectura de redes
        - Introducción
        - Modelo OSI
        - NAT vs Bridge
    - Kali Linux
        - Introducción a Linux.
        - Uso de comandos
        - Creación del laboratorio del curso
        - Instalación de las máquinas virtuales
        - Kali Linux y Parrot.

2. Recolección y escaneo de datos
    - Recolección de Información y Anonimato
        - Introducción
        - Uso de herramientas de red (Whois, Traceroute, ping…)
        - Google dorks
        - Owasp-Mantra (http-headers, Passive-recon…)
        - Extracción de metadatos (FOCA)
        - Plugins de Firefox útiles
        - Técnicas OSINT

    - Ingeniería social
    - Uso de herramientas de Kali
    - Recolección de información de una red lan
    - Anonimato (Tor, uso de vpn)
- Escaneo
    - Análisis de servicios y puertos
        - Nmap (uso de la herramienta en sus distintos tipos de escaneo)
        - Evasión de firewalls
    - Análisis de vulnerabilidades
        - Clasificación de las mismas
        - Acunetix
        - Nessus
        - Cmsmap
        - Wpscan
        - Joomscan
        - Zap

3-4. Análisis y explotación

- Análisis de situación
- Búsqueda de exploits
- Ataque manual y automatizado
- Metasploit
- Ataque directo e inverso
- Pivoting
- Post-explotación
- Escala de privilegios
- Backdoors
- Extracción de información sensible y útil

5. Lenguajes de hacking

- Python
    - Introducción Python-hacking
    - Introducción a la programación Python
    - Uso de librerías específicas
- Ruby
    - Introducción Ruby-hacking
    - Introducción a la programación Ruby
    - Implementación a metasploit

6. Auditorías web

- Auditorías Web
- Taxonomía de un ataque
- Ejemplos de vulnerabilidades y ataques:
    - Inyección Sql
    - Xss
    - LFI
    - Inyección de código
    - RFI
    - Phising

7. Infraestructuras de hacking

- Hacking Infraestructuras
- Redes
    - Linux
    - Windows
    - OS
- Escalada de privilegios de cero a 100
    - Shell scripting
    - Linux

- Windows

8. Auditoria de password y wifi
   - Password Cracking
     - Diferencias entre tipos de ataque
     - Ataques on line y off line
     - Hashcat
     - Hydra
     - Ophcrack
     - Metasploit (auxiliares)
     - John
     - Cracking on line
   - Auditoras WIFI
     - Uso de Airgeddon

9. Malware
   - Malware
   - Configuración de un troyano
   - Uso de crypter
   - Crypters on line
   - Modding desde cero
   - Evaluación del malware
   - Métodos de infección

10. Informática forense
    - Forense
    - Introducción a la informática forense
    - Evidencia digital
    - Análisis de datos
    - Mail
    - Forense en redes y geo.
    - Forense móviles
    - Elaboración de informe

11. Realización informe pentest

MODULO 2: DIRECCIÓN DE LA CIBERSEGURIDAD

1. Gobierno del dato e información
   a. Tipo de datos e identidad de la información
   b. Ciclo de vida de la información
   c. Seguridad de la información

   ¿Qué aprenderemos?
   - Conocer los distintos tipos de datos digitales que existen y sus distintos tránsitos en medios digitales. Incluye la descripción de la identidad de la información digital.
   - Describir cada una de las fases del ciclo de vida de la información en medios digitales.
   - Conocer los requisitos del estándar ISO/IEC 27001:2013 - Sistema de Gestión de Seguridad de la Información como medio para realizar la protección de la información.
   - Elaboración de un plan de gestión de datos e información.

2. Gestión del riesgo operacional

a. Gestión de procesos y activos
b. Gestión de vulnerabilidades
c. Gestión del riesgo

¿Qué aprenderemos?

- Entender la estructura y organización de los procesos que soportan al negocio y la relación de los activos (recursos) que se necesitan proteger.
- Conocer las fuentes de declaración, scoring de vulnerabilidades, incluyendo los procesos y tecnologías necesarias para identificarlos dentro de los activos.
- Conocer los procesos de gestión de riesgos basado en el estándar ISO 31000:2018 - Gestión del Riesgo.
- Elaboración de un plan de gestión de riesgo operacional.

3. Leyes y regulaciones en el entorno de los datos
    a. Protección de datos personales
    b. Delitos informáticos y convenios internacionales
    c. Protección de evidencias informáticas

¿Qué aprenderemos?

- Identificar las leyes entorno a la protección de datos personales y su relación con la seguridad de la información.
- Identificar las leyes entorno a delitos informáticos y convenios internacionales en materia de delitos informáticos.
- Conocer las técnicas, procedimientos y regulaciones entorno a las evidencias informáticas que serán utilizadas para análisis forense.
- Elaboración un procedimiento de evidencias informáticas.

4. Ofrecimiento de servicios en la nube
    a. Tipos y características de servicios en nube
    b. Marco normativo de servicio en nube
    c. Servicios de seguridad en la nube

¿Qué aprenderemos?

- Entender los tipos y características de los servicios en nube que soportan la arquitectura empresarial.
- Identificar los estándares y buenas prácticas entorno a la seguridad de la información en servicios en nube.
- Conocer la descripción de los servicios de seguridad que ofrecen los servicios en la nube.
- Elaboración de modelo de autenticación a servicios en nube.

5. Gestión de defensa y respuesta a incidentes
    a. Amenazas avanzadas
    b. Detección de eventos
    c. Respuesta de incidentes

¿Qué aprenderemos?

- Identificar las prácticas entorno a la identificación de amenazas avanzadas, usando técnicas de ciber-inteligencia.
- Conocer los procesos y tecnologías que permiten automatizar la detección de eventos de seguridad.
- Conocer los procesos y tecnologías que permiten automatizar la respuesta ante incidentes de seguridad.
- Elaboración de plan de respuesta ante incidentes.

6. Arquitectura de seguridad
    a. Arquitectura empresarial
    b. Marco de ciberseguridad

c. Modelos de arquitectura de seguridad

¿Qué aprenderemos?

- Conocer el modelo de organización de servicios digitales dentro de la tecnología de la información basada en el modelo de TOGAF.
- Entender de las funciones del marco de ciberseguridad basada en NIST CyberSeguridad y su alineación a estándares y buenas prácticas en seguridad.
- Identificar los modelos de arquitectura de seguridad que existen para brindar seguridad a la arquitectura empresarial.
- Elaboración de diseño de arquitectura de seguridad.

7. MLSec. Machine Learning para la Cibersegruidad
   a. Machine Learning & NLP
   b. Deep Learning, Reinforcement Learning y GANs
   c. ML para la Ciberseguridad (MLSec)

¿Qué aprenderemos?

- Entender el Machine Learning a través de una exploración de los algoritmos más importantes supervisados y no supervisados. Incluye exploración de técnicas para manejo de lenguaje (NLP).
- Entender el Deep Learning y sus variantes más importantes como CNN o RNN. Adicionalmente entender el aprendizaje reforzado (reinforcement learning) y GANs (redes generativas antagónicas).
- Presentación de diversos casos de uso de ML aplicado a la Ciberseguridad (MLSec) tomando en cuenta tanto un enfoque defensivo como ofensivo.
- 2 laboratorios en donde se implementan aplicaciones de MLSec usando técnicas de ML y Deep Learning respectivamente. Uso de Python y Open Source.

8. Seguridad en las operaciones
   a. Gestión de servicio TI
   b. Seguridad en desarrollo de software
   c. Seguridad física

¿Qué aprenderemos?

- Identificar los servicios TI que soportan la arquitectura empresarial y que deben ser protegidos por la arquitectura de seguridad.
- Identificar los componentes de desarrollo de software que necesitan de seguridad para entregar aplicaciones seguras.
- Reconocer los ambientes físicos en donde se realizan procesamiento o tránsito de la información para brindarles seguridad.
- Elaboración de plan de protección de servicio de TI y desarrollo.

9. Evaluación de postura de seguridad
   a. Ejercicio de ataque y respuesta
   b. Monitoreo y evaluación de controles
   c. Auditoría interna

¿Qué aprenderemos?

- Identificar los modelos para realizar ejercicios de ataque y respuesta a la arquitectura de seguridad.
- Definir los modelos de monitoreo y evaluación de los controles implementados dentro de la arquitectura de seguridad.
- Realizar la auditoría interna bajo el estándar ISO 19011 para revisar el correcto funcionamiento de los controles implementados.
- Elaboración de plan de verificación de postura de seguridad

METODOLOGÍA Y PLAN DE TRABAJO

En cada sesión el profesor expondrá los principales aspectos del correspondiente tema, ilustrándolos con ejemplos y datos. Se espera que el alumno, previo estudio del material asignado a cada sesión (notas técnicas y otros documentos disponibles en el Campus online), exponga sus puntos de vista respecto a los temas tratados.

La metodología para el aprendizaje y evaluación de sus contenidos, se encuentra adaptada al modelo de formación continua y a distancia de SBS. Los conocimientos de la asignatura se adquieren a través del estudio razonado de las unidades didácticas del temario consignado, así como del material didáctico complementario que se ponga a disposición. Además, es preciso que las y los estudiantes realicen las actividades de evaluación continua y aprendizaje planificadas y que oportunamente se informarán.
Las dudas conceptuales que surjan tras el estudio razonado de las unidades y del material complementario deben plantearse en el foro de tutorías y/o vía mail.

MÉTODOS DE EVALUACIÓN

Para la evaluación final del curso se tendrán en cuenta los siguientes criterios:

- 50% Módulo de Ciberseguridad y Hacking ético.
  - En este módulo será necesaria la entrega de un proyecto
- 50% Módulo de Dirección de la Ciberseguridad
  - Este módulo se evaluará a través de un examen tipo test

BIBLIOGRAFÍAS

- Notas Técnicas propias.
- Otra documentación en el campus