MÓDULO DE GESTIÓN, NORMAS Y MODELOS DE LA CIBERSEGURIDAD

SÍLABO (20 hr)

El desarrollo de esta materia presenta los fundamentos de Ciberseguridad, el marco de referencia, modelos, metodología de la gestión de TI; el marco para la mejora de la seguridad cibernética en infraestructuras críticas.

El módulo es teórico, con una duración total de 20 horas. Se dictará en español.

PROGRAMACIÓN DE CONTENIDOS

Clase (4hr)	Contenido
1	Fundamentos de Ciberseguridad, Gobierno TI, Riesgo, cumplimiento.
2	Modelos, arquitectura, metodología y buenas prácticas de la gestión TI: COBIT, TOGAF, ITIL, CISSP.
3	Sistemas de Gestión de la Seguridad de la Información, familia ISO27K; Industria de tarjetas de pago (PCI) Norma de seguridad de datos.
4	Cybersecurity Framework CSF de NIST, núcleo de estructura, capas de implementación (identificar, proteger).
5	Cybersecurity Framework CSF de NIST, capas de implementación (detectar, responder, recuperar), perfil de estructura.

MÓDULO DE ANALISIS OPERATIVOS DE CIBERSEGURIDAD (22 hr)

Esta materia presenta los diferentes equipos de respuesta a incidentes; las fases de un ethical hacking, el uso de múltiples estrategias de ataque que identifican las debilidades y vulnerabilidades de diferentes entornos permitiendo reforzar los controles de los sistemas de seguridad para lograr minimizar el riesgo de incidentes; técnicas de penetración para evaluar de manera controlada las brechas de seguridad; el tratamiento de colectar huellas y evidencias para el análisis forense digital; recuperación de servicios y continuidad del negocio.

El módulo es teórico, con una duración total de 22 horas. El 50% será dictado en español y el otro 50% en inglés.

PROGRAMACIÓN DE CONTENIDOS

Clase (4hr)	Contenido
1	Equipos de Ciberseguridad – Fundamentos de ethical hacking
2	Técnicas de ethical hacking
3	Fundamentos de penetration testing
4	Técnicas de penetration testing, análisis de vulnerabilidades
5	Fundamentos, procesos y técnicas del análisis forense digital
6 (2hr)	Normas y modelos de respuesta para la continuidad de negocio, plan de recuperación ante desastres en Tecnología de la Información.

MÓDULO DE HERRAMIENTAS DE ANÁLISIS EN CIBERSEGURIDAD

(22 horas)

Esta materia presenta las diferentes herramientas computacionales utilizadas en los diferentes estados del análisis de la ciberseguridad, Ethical Hacking, análisis de penetración, diagnóstico forense; Python aplicado al análisis de la ciberseguridad.

Incluye una parte teórica y una parte práctica, haciendo un total de 22 horas. El 50% será dictado en español y el otro 50% en inglés.

PROGRAMACIÓN DE CONTENIDOS

Clase (4hr)	Contenido
1	Herramientas de ethical hacking (1)
2	Herramientas de ethical hacking (2)
3	Herramientas de penetration testing (1)
4	Herramientas de penetration testing (2)
5	Herramientas de análisis forense digital
6 (2hr)	Python aplicado a la Ciberseguridad

MÓDULO DE ENTRENAMIENTO PLATAFORMA DE SEGURIDAD (22 horas)

Esta materia presenta la capacidad para configurar, instalar y administrar el día a día de una plataforma de seguridad; su operación, monitoreo y mantenimiento en redes corporativas.

El módulo es práctico, con una duración total de 22 horas. Se dictará en inglés.

PROGRAMACIÓN DE CONTENIDOS

Clase (4hr)	Contenido
1	Introduction and Initial Configuration, Security Fabric, Firewall Policies
2	Network Address Translation (NAT), Firewall Authentication, Logging and Monitoring
3	Certificate Operations, Web Filtering, Application Control, Antivirus
4	Intrusion Prevention and Denial of Service, SSL VPN, Routing, SD-WAN Local Breakout
5	Virtual Firewalls, Layer 2 Switching, IPsec VPN, Single Sign-On (SSO)
6 (2hr)	High Availability (HA), Diagnostics

MÓDULO DE TÓPICOS DE SEGURIDAD EN TECNOLOGIAS EMERGENTES (20 horas)

Esta materia presenta algunas de las diversas tecnologías emergentes que se están desarrollando e implantando a nivel global y su impacto en la seguridad computacional.

Incluye una parte teórica y una parte práctica haciendo un total de 20 horas. Se dictará en inglés.

PROGRAMACIÓN DE CONTENIDOS

Clase (4hr)	Contenido
1	Microservicios, Container, Serverless, Edge Computing
2	Computación Cuántica
3	Blockchain
4	Software-Defined Networking (SDN)
5	Industrial IOT Security (IIOT)
6	Robotic Process Automation (RPA)
7	Artificial Intelligence (AI)

VII. Distribución de Asignaturas por Áreas del Perfil Académico

El currículo consta de 5 Módulos que se desarrollan de manera intensiva en cuatro meses, en el horario de Sábado y Domingo de 8 :00 am a 11: 20 am
Las horas académicas son de 50 minutos

El Plan de Estudios es el siguiente:

N°	MÓDULOS	HORAS TEORÍA	HORAS PRÁCTICA	TOTAL HORAS
1	Gestión, Normas y Modelos de la Ciberseguridad	20		20
2	Análisis Operativos de Ciberseguridad	22		22
3	Herramientas de Análisis en Ciberseguridad		22	22
4	Entrenamiento Plataforma de Seguridad		22	22
5	Tópicos d Seguridad en Tecnologías Emergentes	20		20
	TOTAL	62	44	106