Cronograma: Cyber Security Pack

Día de la lección	Temas a impartir	Recursos a utilizar	Actividades a realizar	Objetivo de la lección

Clase 1.
 	
-Normal Edition Lunes 5pm-9pm
 	
-Girl Power Edition Martes 5pm-9pm
	▪ Introducción a los conceptos de Ciberseguridad.
	▪ Manejo seguro de la Seguridad de la Información.
	  o Confidencialidad
	  o Integridad
	  o Disponibilidad
	▪ Como gestionar un sistema de información seguro.
	▪ Temas legales, éticos y cumplimiento.
	▪ Terminología y marco de Seguridad de la información (NIST – NISE).
	▪ Control de accesos, autenticación, controles de autorización de acceso a la información.
	▪ Ingeniería social.
	▪ Practicas comunes de Ciber crimen.
		▪ Casos de usos para que los alumnos comprendan la diferencia entre Confidencialidad, Integridad y Disponibilidad de la información.
		▪ Bibliografía generada por iQ4.
		▪ Bibliografía adicional de CSX Cybersecurity Fundamentals Study Guide, 2nd Ed eBook
			▪ 4 horas de clase.
			▪ Con un descanso de 15 minutos.
			▪ Tomar asistencia.
			▪ Introducción y presentación del programa a todos los alumnos, junto con la metodología de Examen.
			▪ Presentación de la plataforma de iQ4 y revisión de los reglamentos de conducta (Asistencia, participación en clase, Quiz y exámenes).
			▪ Resumen de los temas que se darán en clase.
			▪ Introducción a clase 1.
				▪ Comprender los conceptos de Ciberseguridad.
				▪ Diferenciar los conceptos básicos de confidencialidad, integridad y disponibilidad.
				▪ Saber gestionar los controles de acceso a la información.
				▪ Identificar la importancia y los impactos del cumplimiento de las normativas legales y éticas.
				▪ Entender las prácticas de ciber crimen.

			▪ Casos de uso para afianzar los conocimientos teóricos previamente impartidos. ▪ Preguntas/dudas de lo visto en clase. ▪ Tomar asistencia. ▪ Quiz para fijar los contenidos adquiridos y validar comprensión de los temas explicados. ▪ Finalización de la clase.	
Clase 2. -Normal Edition Jueves 5pm-9pm **-Girl Power Edition Viernes 5pm-9pm**	▪ Introducción a DRP (Recuperación de Desastres) o Planes y procesos o Política de respaldos o Recuperación de información de manera segura. o HA. Alta Disponibilidad de recurso y tolerancia a Fallos. ▪ Introducción a la gestión de riesgos (orientado a Tecnología de la información). o Vista general al proceso de gestión de riesgos. o Distintos tipos de procesos para mitigar el riesgo. o Procesos Cuantitativo y procesos cualitativo. ▪ Cálculo matemático / estadístico de dichos procesos. Manejo y Gestión segura de Cambios.	▪ Caso de uso para que los alumnos definan un plan eficiente para recuperación ante un incidente de Seguridad. (esta actividad será realizada en grupos). ▪ Caso de uso para que los alumnos calculen el Riesgo cuantitativo y puedan comprender el modelo matemático. ▪ Bibliografía generada por iQ4. ▪ Bibliografía adicional de CSX Cybersecurity Fundamentals Study Guide, 2nd Ed eBook	▪ 4 horas de clase. ▪ Con un descanso de 15 minutos. ▪ Tomar asistencia. ▪ Preguntas y sesión de repaso de clase anterior. ▪ Resumen de los temas que se darán en la clase 2. ▪ Introducción a la clase 2. ▪ Laboratorio práctico y/o casos de uso para afianzar los conocimientos teóricos previamente impartidos. ▪ Validación y preguntas de lo visto en clase. ▪ Tomar asistencia. ▪ Finalización de la clase.	▪ Entender los conceptos y procesos de DRP. ▪ Comprender cómo funciona el proceso de gestión de riesgos y conocer sus formar de aplicación. ▪ Identificar las políticas eficientes de manejo de riesgo y recuperación ante incidentes de seguridad.

	○ Segregación de responsabilidades (SOD). ○ Elementos de proceso de cambios exitoso. ○ Modelo de madurez CMM.			
Clase 3 -Normal Edition Lunes 5pm-9pm **-Girl Power Edition Martes 5pm-9pm** **Clase 4 -Normal Edition Jueves 5pm-9pm** **-Girl Power Edition Viernes 5pm-9pm**	▪ Tecnologías de conexión: Movil y protocolos wi fi, SATCOM, bluetooth, NFC, ANT, Infrarrojo, USB, Remote wipe, Geolocalización vs Geofencing, contraseñas, Pins, Push notifications, conteiners. ▪ Tipos de ataques (con afectación directa a Redes): Introducción a distintos tipos de ataques relacionados con los protocolos previamente estudiados. ▪ Protocolos y procesos de autenticación: Comprender el funcionamiento de los procesos críticos de autentificación de usuarios en distintas tecnologías, manteniendo la confidencialidad, integridad y disponibilidad de la información: Firma digital, DNSSEC, SSH secure shell, S/MIME, SRTP, LDAP, FTP, SFTP, SNMP v3, SSL / TLS, HTTP, Sec POP, IMAP. ▪ Infraestructura en Redes: Entender los principios de arquitectura en redes seguras. Default gateway, Tolerancia a fallas, HSRP. ▪ Protocolos de encriptación: Comprender los conceptos de los protocolos criptográficos que generan capas de encriptación para asegurar la confidencialidad de la	▪ Captura de paquetes de comunicaciones de red en distintos protocolos, disección y análisis de esta información para comprender el funcionamiento de los distintos protocolos. ▪ Utilización de herramientas de uso libre como Wireshark. ▪ Armado de infraestructura de Redes utilizando virtualización. Luego se enviará tráfico real para identificar fallas en la construcción de dicha infraestructura. ▪ Bibliografía generada por iQ4. ▪ Bibliografía de CSX Cybersecurity Fundamentals Study Guide, 2nd Ed eBook	▪ 4 horas cada clase ▪ Con un descanso de 20 minutos. ▪ Tomas asistencia. ▪ Preguntas y sesión de repaso de clase anterior. ▪ Resumen de los temas que se darán en las clases 3 y 4. ▪ Introducción a las clases 3 y 4. ▪ Laboratorio práctico y/o casos de uso para afianzar los conocimientos teóricos previamente impartidos. ▪ Validación y preguntas de lo visto en clase. ▪ Tomar asistencia. ▪ Finalización de la clase.	▪ Comprender y adquirir los conceptos fundamentales de Redes informáticas sobre los cuales se basan muchas de las prácticas de Ciber Seguridad. ▪ Saber diagramar una arquitectura de red correcta, donde se deberían ubicar los diferentes componentes de una red segura (Firewall, IPS, IDS, Web Servers, Honeypots, etc). ▪ Identificar los distintos tipos de ataques. ▪ Comprender los protocolos y procesos de autenticación.

	información. WEP, 802.11, WPA, TKIP, WPA2, CCMP.			
Clase 5 -Normal Edition Lunes 5pm-9pm **-Girl Power Edition Martes 5pm-9pm** **Clase 6 -Normal Edition Jueves 5pm-9pm** **-Girl Power Edition Viernes 5pm-9pm**	▪ Identificación y autenticación de usuarios, accesos de servicios como SSL, LDAP, Kerberos, TACACS y CHAP. ▪ RADIUS, Autenticación, Autorización y control de conexiones. ▪ Proceso de SSO o Single sign on. ▪ Comandos básicos de Linux. o Logging in and logout. o Interfaz gráfica e interfaz de línea de comando. o Software libre y abierto. o Projecto GNU. o FHS o Jerarquía standard de filesystems. ▪ Manejo de archivos en Linux, diferencia con otros Sistemas Operativos. ▪ Sistemas embebidos. Principios básicos de Android e iOS. ▪ Introducción a Linux Shell, aprender a trabajar con variables, llamar a variables y ver los valores asociados a ellas, exportar y dar de baja comandos. ▪ Shell globing. (Librería para comprender como manejar los parámetros especiales de Linux) ▪ Manejo de directorios jerárquicos y archivos en Linux. o Archivos y path names. o Ver contenido de los directorios. o Crear nuevos directorios. o Crear nuevos archivos.	▪ Laboratorio 1. cómo instalar y configurar Linux en una PC. Utilización de VM para abrir distintas distribuciones de Linux. ▪ Instalación y configuración de interfaz gráfica en Linux. ▪ Laboratorio 2. Ejercicios para comprender como ejecutar los comandos aprendidos en clases. Por ejemplo, generar un comando para indicar el día, mes y año actual, luego guardar esa información en una variable para utilizarla en un script de Linux. ▪ Laboratorio 3. Generar en el laboratorio virtual un directorio complejo con sub-directorios, files, y ejecutables, poder navegar y comprender un directorio jerárquico. ▪ Laboratorio 4. Generar una VM agregar, discos duros formatear discos usando ext4, Cree una entrada en el archivo fstab que apunte al directorio / Respaldo como punto de montaje para montarlo permanentemente después de cualquier reinicio o apagado. ▪ Bibliografía generada por iQ4.	▪ 4 horas cada clase. ▪ Con un descanso de 20 minutos. ▪ Tomar asistencia. ▪ Preguntas y sesión de repaso de clase anterior. ▪ Resumen de los temas que se darán en las clases 5 y 6. ▪ Introducción a las clases 5 y 6. ▪ Laboratorio práctico y/o casos de uso para afianzar los conocimientos teóricos previamente impartidos. ▪ Validación y preguntas de lo visto en clase. ▪ Tomar asistencia. ▪ Finalización de la clase.	▪ Conocer Sistemas Operativos como Kali / Devian ▪ Entender los comandos críticos y la arquitectura / file system de UNIX. ▪ Saber cómo manejar variables en Linux Shell. ▪ Entender cómo gestionar y extraer datos de Linux.

	○ Copiar archivos y directorios. ○ Mover, borrar, encontrar archivos y directorios. ○ Comprimir archivos. ○ I/O redireccionamiento. ○ Standard Input/Output/Error. ○ Redireccionar StrOut., strin, strerr. ○ Extraer datos de archivos. ▪ Comprender el procesamiento de textos en Linux. vi editor			
Clase 7 -Normal Edition Lunes 5pm-9pm **-Girl Power Edition Martes 5pm-9pm** **Clase 8 -Normal Edition Jueves 5pm-9pm** **-Girl Power Edition Viernes**	▪ Conceptos básicos e introductorios de Criptografía. Historia, Conceptos Básicos, principios de esteganografía. ▪ Criptogramas por permutación. ▪ Cifrado por sustitución. Monoalfabeto, polialfabetos y máquinas de encriptación (Enigma). ▪ Criptoanálisis. ○ Criptoanálisis por fuerza bruta. ○ Análisis de frecuencias. ○ Métodos de Kasisnksy y Babbage. ▪ Criptosistemas modernos. ○ Aritmética modular. ○ Cifrado de flujo, adición, conversión de bases, OTP, Trivium. ○ Cifrado por números aleatorios. ▪ Criptosistemas simétricos modernos, métodos de encadenamiento de bloques. (Blockchain). ▪ Protocolos de encriptación: DES, AES, 3DES, Skipjacki, IDEA. ▪ Funciones Hash.	▪ Laboratorio 1. Encriptación por transposición, los alumnos deberán descifrar un texto encriptado mediante la transposición de sus caracteres. ▪ Laboratorio 2. Técnicas de Criptoanálisis, utilización de herramientas y procedimientos matemáticos / aritméticos. ▪ Laboratorio 3. Laboratorio de encriptamiento de flujo. ▪ Bibliografía generada por iQ4.	▪ 4 horas cada clase. ▪ Con un descanso de 15 minutos. ▪ Tomar asistencia. ▪ Preguntas y sesión de repaso de clase anterior. ▪ Resumen de los temas que se darán en las clases 7 y 8. ▪ Introducción a las clases 7 y 8. ▪ Laboratorio práctico y/o casos de uso para afianzar los conocimientos teóricos previamente impartidos. ▪ Validación y preguntas de lo visto en clase. ▪ Tomar asistencia. ▪ Finalización de la clase.	▪ Comprender los conceptos fundamentales de Criptografía. ▪ Entender los principios de esteganofrafía. ▪ Identificar los protocolos de encriptación. ▪ Identificar los métodos de Blockchain. ▪ Conocer los diferentes entes certificadores.

5pm-9pm	▪ Criptosistemas asimétricos. Manejo de llaves, teoría de números y funciones. ▪ RSA, curva elíptica. ▪ Llaves públicas y privadas, arquitectura y funcionamiento de estos modelos de encriptación. ▪ Certificados Digitales y entes certificadores (sitios seguros). ▪ Sistema Nacional Costarricense de Certificación Digital.			
Clase 9 -Normal Edition Lunes 5pm-9pm **-Girl Power Edition Martes 5pm-9pm** **Clase 10 -Normal Edition Jueves 5pm-9pm** **-Girl Power Edition Viernes 5pm-9pm**	▪ Conceptos introductorios de Seguridad en el desarrollo de aplicaciones. ▪ Introducción a SDL, metodologías Cascada y Agile, SCRUM y Extreme programming. ▪ introducción a DevOps, porque es tan importante? Automatización de procesos y baselining. ▪ Evaluación de vulnerabilidades durante el desarrollo de software. o Provisionamiento y deprovisionamiento. o Controles de versiones y proceso de manejo de cambios. o Validación y manejo de errores del sistema. o Normalización de datos. o SQL Injection y stored procedures. o Manejo de memorias para evitar stack overflow y buffer overflow. (Spectre – Meltdown). o Exposición inapropiada de datos. o VMS. ▪ Teoría y Laboratorio guiado	▪ Laboratorio 1. Los alumnos deberán revisar un pseudo – código generado en Python para comprender como se convierten las cuentas bancarias locales en cuentas internacionales (IBAM). Comprender el algoritmo es el objetivo principal de la capacitación. Los alumnos no deberán desarrollar código, sino comprender como leer una pseudo rutina a nivel alto. ▪ Laboratorio 2. Utilización de dia-installer para la generación de arquitectura de software, el objetivo es que los alumnos puedan conceptualizar un diseño de software en base a un requerimiento de un cliente. ▪ Laboratorio 3.Retos. Los alumnos deberán poder realizar compras ficticias en un servidor de compras online, pero deberán encontrar las vulnerabilidades en el sistema para poder realizar compras sin pagar dinero virtual. El objetivo de este laboratorio es que los alumnos comprendan la	▪ 4 horas cada clase. ▪ Con un descanso de 15 minutos. ▪ Tomar asistencia. ▪ Preguntas y sesión de repaso de clase anterior. ▪ Resumen de los temas que se darán en las clases 9 y 10. ▪ Introducción a las clases 9 y 10. ▪ Laboratorio práctico y/o casos de uso para afianzar los conocimientos teóricos previamente impartidos. ▪ Validación y preguntas de lo visto en clase. ▪ Tomar asistencia. ▪ Finalización de la clase.	▪ Comprender los conceptos de seguridad en el desarrollo de aplicaciones. ▪ Saber cómo aplicar las prácticas de programación segura. ▪ Comprender los métodos Waterfall vs Agile, Scrum y extreme programming. ▪ Entender la gestión de vulnerabilidades en el desarrollo de software. ▪ Conocer el proceso de testeo durante el desarrollo de aplicaciones.

	○ Configuraciones seguras ○ Cómo vulnerar un proceso de autentificación mal desarrollado. ○ Cómo vulnerar un proceso de validación mal codificado. ○ Llamada inseguras de datos. ▪ Calidad y testeo en el desarrollo de aplicaciones.	importancia de la validación de datos. ▪ Laboratorio 4. Rediseñar una arquitectura de software que posee fallas de seguridad (utilizando la aplicación DIA), la nueva arquitectura de SW debe ser escalable, tolerable a fallas y debe poder realizar procesos de automatización. ▪ Bibliografía generada por iQ4.		
Clase 11 -Normal Edition Lunes 5pm-9pm **-Girl Power Edition Martes 5pm-9pm**	▪ Etapas de un proceso de Pentest y herramientas comúnmente usadas para realizar este tipo de procedimientos. Pentest y Vscanning. ○ Alcance – Pre- ○ Reconocimiento. ○ Descubrimiento y evaluación de vulnerabilidades. ○ Beneficio ○ Análisis y reporte. ▪ Análisis y laboratorio de tipos de ataques. ○ Brute Force Attacks. ○ SQL Injection. ○ Ataque de XSS ○ Ataque de CSFR ○ Ataques de command injection ▪ Tipos de ataques dependiendo de estrategia de IoC ○ <u>Service Side:</u> Evasión de web firewall, ejecución remota de comandos, inclusión remota de archivos, ataques en la capa de sesión. ○ <u>Lado del cliente:</u> Ataques a nivel de navegador, ataques	▪ Laboratorio 1. Utilización de herramientas para realizar un pentest, APT List. ○ ZenMap ○ Kali, OpenVas ○ DWA / Metasploit ▪ Laboratorio 2. Utilización de herramientas para realizar una simulación de ataques. ○ DWA / Metasploit ○ BURP ○ BURP / PRO ○ ZAP ▪ Laboratorio 3. Comprender y diseñar estrategias de detección y de protección. ○ WAF. ○ MOD_Seguridad ○ Sec Dev ▪ Laboratorio 4. Comprender los distintos tipos de ataques y su ejecución en VMs y los distintos tipos estrategia de defensa. ▪ Bibliografía generada por iQ4. ▪ CSX Cybersecurity Fundamentals Study Guide, 2nd Ed eBook.	▪ 4 horas de clase. ▪ Con un descanso de 15 minutos. ▪ Tomar asistencia. ▪ Preguntas y sesión de repaso de clase anterior. ▪ Resumen de los temas que se dará en la clase 11. ▪ Introducción a la clase 11. ▪ Laboratorio práctico y/o casos de uso para afianzar los conocimientos teóricos previamente impartidos. ▪ Validación y preguntas de lo visto en clase. ▪ Tomar asistencia. ▪ Finalización de la clase.	▪ Entender cómo es el proceso de Pentest e identificar las herramientas que se utilizan. ▪ Identificar los tipos de ataques y cómo mitigarlos. ▪ Comprender cómo se pueden realizar campañas de afectación de servicios utilizando las herramientas y procesos previamente aprendidos en clase; y cómo prevenirlas.

	a nivel de DNS, Cross Site Scripting.			
Clase 12 -Normal Edition Jueves 5pm-9pm **-Girl Power Edition Viernes 5pm-9pm** **Clase 13 -Normal Edition Lunes 5pm-9pm** **-Girl Power Edition Martes 5pm-9pm**	▪ Intrducción a la Ciber seguridad o Objetivos. o Gobernanza. o Importancia de los dominios de Cyber Seguridad. ▪ Revisión de los conceptos iniciales. o Proceso de Gestión de Riesgos. o Ataques comunes y vectores de ataques. o Políticas de Ciber Seguridad. o Controles de Seguridad ▪ Principios de Arquitectura de Seguridad. o Modelo OSI. o Estrategia de defensa y de ataque. o Aislamiento y segmentación durante incidentes de Seguridad. o Logging, monitoreo y detección de eventos de seguridad. o Técnica y aplicaciones de encriptamiento. ▪ Principios de Seguridad en Redes, Sistemas, Aplicaciones y datos. o Estrategia de Gestión de la vulnerabilidad o Estrategia para pruebas de penetración. o Conceptos fundamentales de Seguridad en Redes. o Conceptos fundamentales de Seguridad en	▪ Mock Exam 1. ▪ Mock Exam 2. ▪ Mock Exam 3. ▪ Mock Exam 4. ▪ Bibliografia generada por iQ4. ▪ CSX Cybersecurity Fundamentals Study Guide, 2nd Ed eBook	▪ 4 horas cada clase. ▪ Con un descanso de 15 minutos. ▪ Tomar asistencia. ▪ Preguntas y sesión de repaso de clase anterior. ▪ Resumen de los temas que se darán en las clases 12 y 13. ▪ Introducción a las clases 12 y 13. ▪ Validación y preguntas de lo visto en clase. ▪ Repaso general. ▪ Tomar asistencia. ▪ Finalización de la clase.	▪ Comprender los conceptos básicos de Ciber Seguridad ▪ Identificar los principios de arquitectura de Seguridad en Redes, Sistemas, Aplicaciones y datos. ▪ Definir estrategias de seguridad.

	Aplicaciones y Sistemas Operativos. ▪ Incorporación de tecnologías disruptivas y estrategias de seguridad para adoptarlas. o Threat landscape actual. o APT. Amenazas persistentes avanzadas. o Seguridad en tecnología móvil. ▪ Seguridad en la nube y herramientas de colaboración.			
▪ Clase 14, Normal Edition: Lunes 5pm-9pm y Girl Power Edition: Martes 5pm-9pm, los alumnos se preparan y se unificaran los contenidos, rendirá el Examen Final del curso (con una duración máxima de 4 horas también). ▪ Los alumnos tendrán la posibilidad de rendir un examen de reposición en caso de no aprobar el Examen Final del curso, en un plazo no mayor a 5 días hábiles luego de la aplicación del Examen Final.				