CENTRO DE INNOVACIÓN EN INTELIGENCIA Y SEGURIDAD (CIIS)

UDLAP®
JENKINS GRADUATE SCHOOL

CURSO

CIBERSEGURIDAD: GESTIÓN Y RESPUESTA A INCIDENTES CIBERNÉTICOS

“GESTIONA LOS RIESGOS CON PRECISIÓN, EN EQUIPO Y ACTÚA RÁPIDO. PROTEGE LOS ACTIVOS CRÍTICOS DE INFORMACIÓN Y LA CONTINUIDAD DE TU ORGANIZACIÓN, FORTALECE SU RESILIENCIA”

DIRIGIDO A

Líderes del sector de Tecnologías de la Información y Ciberseguridad de organizaciones públicas o privadas de Latinoamérica.

Profesionales de la seguridad de la información y áreas de Tecnologías de la Información y Comunicaciones (TIC’s)

Responsables e integrantes de equipos de ciberseguridad.

Profesionales interesados en conocer los protocolos de atención y gestión de incidentes.

Abogadas y abogados del sector de tecnologías con conocimiento básico de TIC’s y seguridad de información.

BENEFICIOS

El participante desarrollará competencias para identificar y analizar estrategias, metodologías de aplicación y recursos para la seguridad de las operaciones relacionadas con las tecnologías de la información.

Los estudiantes aprenderán sobre la conformación de un centro de operaciones de seguridad, un equipo de respuesta a incidentes, así como los roles y responsabilidades, las herramientas de apoyo y los aspectos legales a considerar ante un incidente cibernético.

Se abordarán los marcos de referencia y estándares más utilizados a nivel global y ejercicios prácticos de aplicación.

BENEFICIOS

Contenido 50% teórico y 50% práctico.

Al finalizar el Curso, el estudiante será capaz de:

Explicar los componentes de las operaciones de seguridad.

Explicar los marcos de referencia y estándares aplicables a las operaciones de seguridad.

Aplicar los conocimientos para implementar un centro de operaciones de seguridad cibernética, establecer y mantener un equipo de respuesta a incidentes cibernéticos, así como las técnicas y herramientas de apoyo.

Evaluar el nivel de madurez de equipo de respuesta a incidentes cibernéticos.

Establecer y monitorear métricas apropiadas para un centro de operaciones de seguridad cibernética.

Explicar y aplicar la metodología forense y la cadena de custodia de evidencia digital.

INFORMACIÓN GENERAL

48 horas / 12 sesiones

Horarios:
Viernes de 18:00 a 21:00 h
Sábados de 9:00 a 14:00 h

Fechas:
Del viernes 07 mayo al 12 de junio 2021

Modalidad:
Online

Coordinador del programa de estudios:
Mtro. Ernesto Ibarra Sánchez

CONTENIDO

TEMA 1

Mtro. Radamés Hernández Alemán

INTRODUCCIÓN

1.1 Definiciones y conceptos
1.2 Ciberseguridad
1.3 Marcos de referencia y estándares
1.4 Marco de referencia NIST
1.5 Centro de Operaciones de Seguridad (SOC)
1.6 Gobierno de la seguridad corporativa
1.7 Roles y responsabilidades

TEMA 2

Mtro. Radamés Hernández Alemán

EQUIPOS DE RESPUESTA A INCIDENTES

2.1 Contexto general
2.2 Servicios de un CSIRT
2.3 Ámbitos de actuación de un CSIRT
2.4 Parámetros de diseño de un CSIRT
2.5 Tipos de estructura
2.6 Selección del Modelo de CSIRT
2.7 Roles y responsabilidades
2.8 Información de Seguridad y Gestión de Eventos (SIEM)

TEMA 3

Mtro. Radamés Hernández Alemán

EVALUACIÓN DE NIVEL DE MADUREZ CSIRT

3.1 SIM3: Modelo de Madurez para la Gestión de Incidentes de Seguridad
3.2 Estrategias para seguridad cibernética (Blue Team)
3.3 Gestión del ciclo de vida del CSIRT
3.4 Entidades de certificación
3.5 Protocolo de Semaforización (TLP)

TEMA 4

Mtro. Radamés Hernández Alemán

PROCEDIMIENTO DE MANEJO DE INCIDENTES CIBERNÉTICOS

4.1 Reporte de incidentes
4.2 Registro de incidentes
4.3 Clasificación de incidentes
4.4 Análisis de datos
4.5 Registros y pistas de auditoría
4.6 Investigación de soluciones
4.7 Propuestas de acciones
4.8 Erradicación y recuperación

TEMA 4.1

Mtro. Radamés Hernández Alemán

PROCEDIMIENTO DE MANEJO DE INCIDENTES CIBERNÉTICOS

4.9 Cierre de incidentes
4.10 Información y clasificación final
4.11 Archivo y análisis post incidente
4.12 SOC una visión integrada
4.13 Configuración de un SOC
4.14 Métricas para un SOC

TEMA 5

Mtro. Radamés Hernández Alemán

HERRAMIENTAS DE APOYO A LAS OPERACIONES DE SEGURIDAD

5.1 Herramientas de consulta de dominios
5.2 Herramientas de análisis de E-mail
5.3 Herramientas de monitoreo de red
5.4 Herramientas de auditoría
5.5 Herramientas de evaluación de vulnerabilidades
5.6 Herramientas de detección de intrusiones

TEMA 5.1

HERRAMIENTAS DE APOYO A LAS OPERACIONES DE SEGURIDAD 2

Mtro. Radamés Hernández Alemán

5.7 Herramientas de análisis de malware
5.8 Honeypots
5.9 Herramientas WiFi
5.10 SIEM (Open Source)
5.11 Herramientas de cifrado

TEMA 6

INFORMÁTICA FORENSE

Lic. Simón Mancilla Sánchez

6.1 Informática forense (generalidades)
6.2 Herramientas de forense digital
6.3 Identificación de indicios
6.4 Recolección de indicios
6.5 Embalaje de indicios
6.6 Etiquetado de indicios
6.7 Cadena de custodia
6.8 Localización, descubrimiento y aportación
6.9 Presentación de informes en procedimiento jurisdiccional

NOTA

Con invitados expertos internacionales y nacionales en la gestión de incidentes de sectores público, privado y académico (en sesiones sabatinas).

UDLAP®

JENKINS GRADUATE SCHOOL

/udlapjenkinsgs

/udlap-jenkins-graduate-s

55 7434 4824

informes@udlapjenkins.mx