Información General del Curso

UIT y INSTITUTO NACIONAL DE INVESTIGACIÓN Y CAPACITACIÓN DE TELECOMUNICACIONES

Título	GESTIÓN DE INCIDENCIAS EN CIBERSEGURIDAD
Modalidad	Virtual
Fechas	1 -30 Junio 2022
Duración	30 horas
Último día para registro	30 de Mayo de 2022
Costo	Costo USD 120.00
Descripción	En este curso se desarrollará el proceso de automatización de acciones en casos de incidencias en la ciberseguridad de un entorno digital, siguiendo los estándares para las mejores prácticas en el sector. Además, se proporcionarán los fundamentos teóricos para incrementar el grado de entendimiento, comprensión y capacidades en ciberseguridad. El curso provee las capacidades para poder gestionar incidencias en ciberseguridad y atender cada escenario con una solución personalizada.
Código del curso	22OI27843AMS-S

1.OBJETIVOS DEL CURSO

Analizar el proceso de gestión de incidencias en escenarios de fallas de seguridad y profundizar en el proceso de automatización para determinar las acciones de cada caso.

2. RESULTADOS DEL APRENDIZAJE

Al finalizar el curso, el estudiante va a tener la capacidad de profundizar en el proceso de gestión de incidencias en ciberseguridad, además será capaz de profundizar en un software especializado de gestión de incidencias de ciberseguridad a través de los laboratorios que se realizarán en el curso.

3. A QUIÉN VA DIRIGIDO

Profesionales en tecnologías de la información, personal a cargo de respuesta a incidencias, ingenieros de sistemas y ciberseguridad, y cualquier interesado en averiguaciones de incidencias en ciberseguridad o control de la ciberseguridad.

4.REQUISITOS DE ADMISIÓN

Se recomienda poseer formación o experiencia en alguna rama de la informática a nivel técnico o a nivel de gestión. Además, se recomienda tener conocimientos de programación básicos en lenguaje javascript.

5.TUTORES/INSTRUCTORES

Nombre del(os) Tutor(es)/Instructor(es)	Información de Contacto
Ayner Antonio Pérez Tito	aynerantonio@gmail.com
Ingeniero de Telecomunicaciones de la Pontificia Universidad Católica del Perú con una maestría en Ingeniería de Ciberseguridad en la Universidad de Warwick en Reino Unido. Con experiencia previa en arquitectura de redes, seguridad perimetral y de terminales de usuario. Actualmente se desempeña como Ingeniero de Seguridad en Londres desarrollando soluciones prácticas para distintos entornos en una de las más grandes compañías, dedicadas de forma independiente, a brindar servicios de seguridad digital.	

6.CONTENIDO DEL CURSO

Tema 1. Introducción a las incidencias en ciberseguridad
1.1. Definición de incidencias de ciberseguridad
1.2. Cuáles son las características de una incidencia
1.3. Conceptos esenciales para la atención de incidencias
1.4. Los roles de usuarios en la gestión de incidencias
1.5. Acciones y herramientas de orquestación de soluciones

Tema 2. El gestor de incidencias
2.1. El ciclo de vida de una incidencia
2.2. El entorno del gestor de incidencias
2.3. Gestión de aplicaciones (orquestación)
2.4. Casos de estudio

Tema 3. Automatización del manejo de incidencias
3.1. Manejo de tiempos de resolución
3.2. Priorización de eventos
3.3. Definición de procesos de resolución de incidencias
3.4. Acciones post resolución de eventos

Tema 4. Desarrollo de un proceso de resolución
4.1. Integración de soluciones al gestor de incidencias
4.2. Introducción a playbooks
4.3. Automatización de acciones en playbooks
4.4. Ejecución de playbooks sobre incidentes

Tema 5. Recursos e información para el manejo de incidencias
5.1. Fuentes de inteligencia de eventos de ciberseguridad
5.2. Manejo de lecciones aprendidas (Base de conocimiento interno)
5.3. Guías para el manejo de casos (Workbooks)
5.4. Escalamiento ante incidencias críticas

Tema 6. Ejercicio práctico
6.1. Desarrollo de un caso de uso en el gestor de incidencias

7.CRONOGRAMA DEL CURSO

Semana / Sesión	Tema	Ejercicios e interacciones
Semana 1	Introducción a las incidencias en ciberseguridad El gestor de incidencias	Practica de análisis de incidencias en un gestor
Semana 2	Automatización del manejo de incidencias Desarrollo de un proceso de resolución	Recursos e información para el manejo de incidencias Ejercicio práctico
Semana 3	Recursos e información para el manejo de incidencias Ejercicio práctico	Desarrollo de un playbook para un incidente Evaluación final

8.METODOLOGÍA

El presente curso es en línea/asincrónico. La metodología que orienta este curso será eminentemente participativa. La estrategia metodológica utilizada para el desarrollo de curso propone al participante una diversidad de actividades.

Se espera que cada estudiante participe mediante la lectura del material que estará disponible desde el inicio del curso, aportes escritos a los debates, foros, actividades, ejercicios de refuerzo y exámenes que serán definidos y los cuales serán realizadas en forma asincrónica. Esta técnica asegurará la flexibilidad de tiempo necesaria para que cada participante pueda organizarse de la manera que mejor le convenga.

Los participantes aprobados en el curso según los criterios de evaluación que sean indicados por los tutores y todos aquellos que sean aprobados recibirán un Certificado que será emitido por vía electrónica

9.EVALUACIÓN Y CALIFICACIÓN

El curso propone un sistema de evaluación combinado el cual se compone de: foros de debate, actividades y evaluaciones. Las fechas de cada uno de estos ítems están definidas en el cronograma. El sistema de calificación de este curso se explica a continuación junto con los porcentajes de peso de cada una de las actividades a evaluar.

Pesos de evaluación

- Foro de debate (20%): Tendrán un peso del 20% sobre la calificación final. Se realizará 1 u 2 foros de debate en el curso. Cada estudiante deberá participar un mínimo de dos veces en el foro con aportes de valor para obtener el 100% del porcentaje semanalmente. En caso de participar una vez obtendrá en 50% y en caso de no participar será un 0%.
- Actividades (60%): también denominados retos, actividades, laboratorios u trabajos individuales tendrán un peso total del 60% y estarán compuestas de algunas de estas opciones: desarrollo de trabajos individuales, retos trabajos grupales, actividades con entrega en la plataforma.
- Evaluaciones (20%): Las evaluaciones del presente curso tendrán un peso total del 20% y podrán efectuarse mediante dos exámenes en línea, El esquema para este curso está indicado en el cronograma de actividades.
- Aprobación: Para aprobar este curso se debe completar un acumulado de mínimo 60%.

10.COORDINACIÓN DEL CURSO

Coordinación Académica: Nombre: Iris Pretel Trejo Email: ipretel@inictel-uni.edu.pe	Coordinador UIT: Nombre: Rodrigo Robles Email: Rodrigo.robles@itu.int