MANEJO Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD

Del 25 de octubre al 14 de noviembre de 2021

INFORMACIÓN GENERAL DEL CURSO

DESCRIPCIÓN DEL CURSO

Título	**MANEJO Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD**
Objetivo	Conocer y familiarizarse con los elementos involucrados en el Manejo y respuesta a incidentes de ciberseguridad
Fechas	25 de octubre al 14 de noviembre de 2021
Duración	30 de horas
Fecha límite de registro	22 October 2021
Costo de formación	Sin costo
Código del curso	21OI27700AMS-S

DESCRIPCIÓN DEL CURSO

En este curso se desarrollará el proceso de manejo y respuesta a incidentes de ciberseguridad, siguiendo los estándares y las mejores prácticas internacionales. Además, se proporcionarán los fundamentos teóricos para incrementar el grado de entendimiento, comprensión y las capacidades en ciberseguridad.

RESULTADOS DEL APRENDIZAJE

Al finalizar el curso el estudiante comprenderá los roles y responsabilidades en el manejo y respuesta a incidentes de ciberseguridad, desarrollando capacidades y habilidades para el manejo y respuesta a incidentes de ciberseguridad en diferentes escenarios y situaciones, de acuerdo a los estándares y buenas prácticas internacionales.

A QUIÉN VA DIRIGIDO

- Profesionales en tecnologías de la información, ciberseguridad y seguridad de la información
- Miembros de un CSIRT y profesionales interesados en formar parte de un CSIRT.
- Personas desempeñando cualquier función en ciberseguridad en una organización.
- Miembros de la Alta Dirección, Auditoría o contraloría, Recursos Humanos, Relaciones Públicas, y Asuntos Legales, cuyas funciones involucren el entendimiento de la gestión y respuesta a los incidentes de ciberseguridad.
- Directivos, funcionarios, especialistas, profesionales o técnicos de organizaciones de todo tamaño y cualquier rubro, sea público o privada, que tengan interés o requieren conocer los procesos de manejo y respuesta a incidentes.
- Auditores, consultores, funcionarios, investigadores que tengan interés en introducirse en la temática de la ciberseguridad.

REQUISITOS DE ADMISIÓN

Se recomienda poseer experiencia, formación o especialización a nivel profesional o técnico en alguna rama de las tecnologías de la información y comunicación.

TUTORES / INSTRUCTORES

Nombre del Tutor / Instructor	Información de Contacto
Eduardo M. Rodriguez Ávila	**eduardo.rodriguez@ieee.org**
Especialista en telecomunicaciones y tecnologías de la información - ISO/IEC 27032 Senior Lead Cybersecurity Manager. - ISO/IEC 27001 Lead Implementer - Information Security Management System - ISO/IEC 27001 Lead Auditor - Information Security Management System - ISO/IEC 20000 Lead Auditor - Service Management System - Information Security Course certificado por el Ministery of Science, ICT and Future Planning, República de Corea del Sur. - Diploma en IT Management certificado por el centre for development of advanced computing C-DAC, India - Diplomado en auditoría y seguridad de tecnologías de la información, UNMSM, Perú.	

CONTENIDO DEL CURSO

MODULO 1: INTRODUCCIÓN A LA GESTIÓN DE INCIDENTES DE CIBERSEGURIDAD
Tema 1. Introducción a los incidentes en ciberseguridad
1.1. Definición de incidentes de ciberseguridad
1.2. Características de un incidente
1.3. Conceptos esenciales para la atención de incidentes
1.4. Los roles de usuarios en la gestión de incidentes

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

MODULO 2: MANEJO Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD
Tema 3. Manejo de incidentes
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. Definición de bloques de acción

MODULO 3: RECURSOS PARA EL MANEJO Y RESPUESTA A INCIDENTES DE CIBERSEGURIDAD
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. Establecimiento de equipos de respuesta a incidentes
6.1. Diseño de un CSIRT
6.2 Operación de un CSIRT

CRONOGRAMA DEL CURSO

Semana / Sesión	Tema	Ejercicios e interacciones
Semana 1	Módulo 1: Introducción a la gestión de incidentes de ciberseguridad	Desarrollar Retos: • Foro del módulo para aportes, preguntas y respuestas. Actividad/tarea del módulo: Aplicación de conceptos de gestión de incidentes de ciberseguridad
Semana 2	Módulo 2: Manejo y respuesta a incidentes de ciberseguridad	Desarrollar Retos: • Foro del módulo para aportes, preguntas y respuestas • Actividad/tarea del módulo: Manejo y respuesta a incidentes en escenarios específicos. Foro Debate: Actualidad, manejo y respuesta a incidentes de ciberseguridad
Semana 3	Módulo 3: Recursos para el manejo y respuesta a incidentes de ciberseguridad	Desarrollar Retos: • Foro del módulo para aportes, preguntas y respuestas Actividad/tarea del módulo: CSIRT, servicios y aplicaciones.

METODOLOGIA

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

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 un foro 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%.

COORDINACION DEL CURSO

Coordinación Académica	Coordinador UIT
Eduardo M. Rodriguez Ávila	Rodrigo Robles Oficina Regional de la UIT para las Américas rodrigo.robles@itu.int

REGISTRO

Creación de la cuenta en ITU Academy

El proceso de inscripción y el pago deben ser realizados en línea a través del Portal ITU Academy. Para registrarse en el curso es **NECESARIO**, primero, crear una cuenta en la plataforma en el siguiente enlace.

Inscripción en el curso

Una vez creada la cuenta nueva, ya se puede realizar la inscripción para el curso en línea en el siguiente enlace https://academy.itu.int/training-courses/full-catalogue/manejo-y-respuesta-incidentes-de-ciberseguridad

También es posible registrarse en el curso deseado por medio de nuestro catálogo de cursos.