**Curso en línea**

**INGENIERÍA Y GESTIÓN DE LA CIBERSEGURIDAD**

**Del 27 setiembre al 17 octubre 2021**

## INFORMACIÓN GENERAL DEL CURSO

### DESCRIPCIÓN DEL CURSO

| | |
|---|---|
| **Título** | **INGENIERÍA Y GESTIÓN DE LA CIBERSEGURIDAD** |
| **Objetivo** | Obtener una visión general de la ciberseguridad desde el punto de vista técnico, operativo y de gestión, brindando conocimientos y competencias básicas para participar en actividades y grupos de trabajo relativos a la ciberseguridad. |
| **Duración** | 30 horas |
| **Costo de formación** | **0** |
| **Código del curso** | **21OI27699AMS-S** |

### DESCRIPCIÓN DEL CURSO

El avance tecnológico nos llevado a tecnificar nuestras vidas, la masificación del acceso a las telecomunicaciones y al Internet nos hace vivir conectados todo el tiempo, la competencia y la producción en serie hace posible acceder más fácilmente a variedad de equipos terminales para conectarnos a Internet, la moda tiende a la utilización de redes sociales y medios de comunicación electrónicos, compras en línea, acceso a contenidos por demanda, juegos en línea, etc. Podemos decir que vivimos, también, en un mundo virtual, un mundo paralelo constituido por todas conexiones, plataformas tecnológicas y toda la información que circulan o almacenan en ellas; y al igual que tomamos consideraciones de seguridad en el mundo físico, se debe proteger este mundo virtual y todos sus elementos. En este contexto, surge la necesidad de la ciberseguridad.

El curso cubre los aspectos fundamentales de ingeniería, gestión y regulación que se deben abordar para entender la importancia y necesidad de la ciberseguridad. Los temas a tratar tienen que ver con el tratamiento de riesgos, las amenazas, las vulnerabilidades, los tipos ataques, gestión de la ciberseguridad, entre otros.

### RESULTADOS DEL APRENDIZAJE

Al finalizar el curso, el participante habrá obtenido los conocimientos y competencias básicas de ciberseguridad y podrá ser capaz de entender, apoyar y participar en actividades y programas de ciberseguridad en una organización.

### A QUIÉN VA DIRIGIDO

- Directivos, funcionarios, especialistas, profesionales o técnicos de organizaciones de todo tamaño y cualquier rubro, sea público o privada, que tengan interés en entender la importancia y necesidad de la ciberseguridad.
- Auditores, consultores, funcionarios, investigadores que tengan interés en introducirse en la temática de la ciberseguridad.

## REQUISITOS DE ADMISIÓN

Se requiere poseer experiencia, formación o especialización 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<br>- ISO/IEC 27032 Senior Lead Cybersecurity Manager.<br>- ISO/IEC 27001 Lead Implementer - Information Security Management System<br>- ISO/IEC 27001 Lead Auditor - Information Security Management System<br>- ISO/IEC 20000 Lead Auditor - Service Management System<br>- Information Security Course certificado por el Ministery of Science, ICT and Future Planning, República de Corea del Sur.<br>- Diploma en IT Management certificado por el centre for development of advanced computing C-DAC, India<br>- Diplomado en auditoría y seguridad de tecnologías de la información, UNMSM, Perú. | |

## CONTENIDO DEL CURSO

**Semana I:**

**Módulo 1: Aspectos fundamentales de la ciberseguridad**

- … Subtema 1: Conceptos básicos de ciberseguridad
- … Subtema 2: Estándares de la Unión Internacional de Telecomunicaciones y la ISO/IEC
- … Subtema 3: Estado de la ciberseguridad global
- … Subtema 4: Tipos de atacantes y asuntos legales
- … Subtema 5: Organización y gobernanza de la ciberseguridad
- … Subtema 6: La ciberseguridad a nivel personal

**Semana II:**

**Módulo 2: Gestión técnica de la ciberseguridad**

- … Subtema 1: Gestión de Riesgos de ciberseguridad. Amenazas y Vulnerabilidades.
- … Subtema 2: Ingeniería Social
- … Subtema 3: Arquitectura de seguridad
- … Subtema 4: Seguridad de red y comunicaciones
- … Subtema 5: Identidad, acceso y criptografía
- … Subtema 6: Seguridad en el usuario final
- …

**Semana III:**

**Módulo 3: Asegurando la ciberseguridad**

- … Subtema 1: Operaciones de ciberseguridad
- … Subtema 2: Análisis y pruebas de penetración
- … Subtema 3: Prevención y respuesta a incidentes de ciberseguridad

… Subtema 4: Continuidad del negocio

… Subtema 5: Investigación forense en ciberseguridad

… Subtema 6: Concientización y capacitación en ciberseguridad

## CRONOGRAMA DEL CURSO

| Semana / Sesión | Tema | Ejercicios e interacciones |
|---|---|---|
| **Semana 1** | Módulo 1: Aspectos fundamentales de la ciberseguridad | Desarrollar Retos:<br>• Foro del módulo para aportes, preguntas y respuestas.<br>• Actividad/tarea del módulo: Aplicación de conceptos de ciberseguridad |
| **Semana 2** | Módulo 2: Gestión técnica de la ciberseguridad | Desarrollar Retos:<br>• Foro del módulo para aportes, preguntas y respuestas<br>• Actividad/tarea del módulo: Análisis de riesgos. Amenazas y vulnerabilidades<br>• Foro Debate: Infraestructuras críticas. amenazas y vulnerabilidades |
| **Semana 3** | Módulo 3: Asegurando la ciberseguridad | Desarrollar Retos:<br>• Foro del módulo para aportes, preguntas y respuestas<br>• Actividad/tarea del módulo: Pruebas y análisis de penetración. |

## 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 1u 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%.

## COORDINACION DEL CURSO

| Coordinación Académica | Coordinador UIT |
|---|---|
| Eduardo M. Rodriguez Ávila | Rodrigo Robles<br>Oficina Regional de la UIT para las Américas<br>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/ingenieria-y-gestion-de-la-ciberseguridad

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