**Red de Centros de Excelencia de la UIT para la Región de las Américas**

**INSTITUTO NACIONAL DE INVESTIGACIÓN Y CAPACITACIÓN DE TELECOMUNICACIONES**

**Curso en línea**

**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**

# INFORMACIÓN GENERAL DEL CURSO

## DESCRIPCIÓN DEL CURSO

| | |
|---|---|
| **Título** | **SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN** |
| **Objetivo** | El objetivo del curso es adquirir los conocimientos necesarios para entender el funcionamiento de un Sistema de Gestión de Seguridad de la Información (SGSI) y proponer un diseño de un proyecto de implementación. |
| **Duración** | 40 horas |
| **Precio** | 300 USD |
| **Código del curso** | **21OI26457AMS-S** |

## DESCRIPCIÓN DEL CURSO

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma. el público en general debe tener el know-how del mismo a fin de tener la cultura de la prevención en cuanto a su información que dispone.

- Adquirir conocimientos conceptos básicos de Gestión de la Seguridad de la Información y las normas internacionales relacionadas.
- Conocer experiencias para que el alumno tenga referencias de como diseñar una estructura de Gobierno de Seguridad de la Información en su organización.
- Adquirir conocimientos necesarios para diseñar un plan de implementación de un SGSI.
- Entender la importancia del monitoreo de un SGSI.
- Entender la necesidad de la revisión del SGSI y adquirir conocimientos básicos para planificar.

## RESULTADOS DEL APRENDIZAJE

Concebir, diseñar, implantar y realizar un seguimiento de políticas de seguridad y planes directores dentro del marco de una empresa o una organización que posibilite el establecimiento de un marco apropiado de seguridad previamente establecido.

Capacidad para realizar una evaluación de los riesgos de seguridad inherentes en una organización a partir de los procesos establecidos en la misma y realizar un análisis y gestión de los riesgos que puedan existir.

Capacidad para realizar una identificación de las amenazas que puedan afectar a la seguridad de una organización y establecer los mecanismos de respuesta apropiados a cada una de ellas.

Conocer y gestionar los procesos de evaluación, certificación y acreditación de la seguridad de los sistemas de información teniendo en cuenta las entidades involucradas, así como las responsabilidades y funciones de cada una de ellas.

## A QUIÉN VA DIRIGIDO

Gerentes, jefes, Oficiales de Seguridad, Jefes de proyectos, Administradores, Abogados, Profesionales y técnicos en TI, Profesionales de S.I

## REQUISITOS DE ADMISIÓN

Ninguna.

## TUTORES / INSTRUCTORES

| Nombre del Tutor / Instructor | Información de Contacto |
|---|---|
| **Evelyn Grace Gonzáles Zúñiga** | **evelyngonzaleszuniga@gmail.com** |
| Magister en Dirección Estratégica de TI con mención en Telecomunicaciones.<br>Ingeniera de Sistemas de la Universidad Católica de Santa MaríaExperiencia de 12 años en la Gestión del área de TI, Seguridad de la Información<br>conforme a ISO 27001, Implementación de controles de seguridad bajo COBIT y la<br>ISO 27002, Gestión de Riesgos conforme a ISO 31000.<br>Miembro del Comité Técnico de Normalización de Codificación e Intercambio<br>Electrónico de Datos - INDECOPI.<br>Amplio conocimiento en la Ley de Protección de datos personales | |

## CONTENIDO DEL CURSO

### Semana 1 – Introducción

- Introducción a la Seguridad de la Información.
- Familia ISO 27000 (Normas de Seguridad de la Información).

### Semana 2 – Gobierno

- Conformación del Comité de Seguridad de la Información.
- Elaboración de una Política de Seguridad de la Información.
- ¿Cómo coordinar con el Comité de Seguridad de la Información?
- Definición de alcance del SGSI (Selección de Procesos).

### Semana 3 – Planificación

- Gestión de Activos.

- Gestión de Riesgos.
- Plan de Trabajo de Implementación.
- Plan de Concientización y Capacitación.
- Resumen - Caso Práctico.

**Semana 4 – Monitoreo**

- Gestión de Incidentes.
- Gestión de Indicadores.
- Seguimiento de la Gestión de Seguridad de la Información.

**Semana 5 – Revisión**

- Gestión de Auditorías Internas.
- Gestión de Auditorías Externas.

## CRONOGRAMA DEL CURSO

| Semana / Sesión | Tema | Ejercicios e interacciones |
|---|---|---|
| **Semana 1** | Introducción:<br>• Introducción a la Seguridad de la Información.<br>• Familia ISO 27000 (Normas de Seguridad de la Información). | Actividad 1:<br>1. Investigue acerca de la Organización Internacional de Estandarización - ISO:<br>• ¿Cómo se desarrolla una norma ISO?<br>• ¿Qué institución tiene el rol de adoptar/adaptar la norma ISO en su país?<br>• Describa 03 normas ISOs relacionados a sistemas de gestión diferentes a la ISO 27001.<br>2. Investigue normativas internacionales relativas a seguridad de la información (no considerar las normas ISO).<br>• ¿Qué normativas relacionadas a Seguridad de la Información existen en su país? Describa la relación con Seguridad de mínimo 03 normas<br>• Describir cinco razones para que una Entidad decida implementar un Sistema de Gestión de Seguridad de la Información.<br>3. Investigue acerca de la Unión Internacional de Telecomunicaciones.<br>• Qué es la Unión Internacional de Telecomunicaciones.<br>• De acuerdo con la Recomendación UIT-T X.1205.<br>• ¿Qué es la “ciberseguridad”?<br>4. Investigue conceptos.<br>• Describir diferencias y similitudes entre "seguridad de la información", "seguridad informática", "ciberseguridad". |
| **Semana 2** | Gobierno:<br>• Conformación del Comité de Seguridad de la Información. | 1. Describa las diferencias y similitudes entre “Gobierno de Seguridad de la Información” y “Gobierno de las Tecnologías de la Información”.<br>2. Describa los principales actores o interesados en la seguridad de la información en su Organización. En cada caso describa cuáles son sus intereses y/o funciones para la seguridad de la información. |

| | | |
|---|---|---|
| | • Elaboración de una Política de Seguridad de la Información.<br>• ¿Cómo coordinar con el Comité de Seguridad de la Información?<br>• Definición de alcance del SGSI (Selección de Procesos). | 3. Describa está conformado el Comité de Gestión de la Seguridad de la Información en su organización y especifique las funciones que realizan. Si no hubiere este Comité en su Organización, describa su propuesta de conformación y funciones.<br>4. Elaborar el documento de aplicabilidad considerando las secciones desde A.5.1 hasta A.6.1 (considerar información de referencia de la empresa/institución donde labora).<br>5. Elaborar una política general y una política específica.<br><br>Participación en el foro de debate<br>Evaluación parcial. |
| **Semana 3** | Planificación:<br>• Gestión de Activos.<br>• Gestión de Riesgos.<br>• Plan de Trabajo de Implementación.<br>• Plan de Concientización y Capacitación.<br>• Resumen - Caso Práctico. | Tomando como referencia a su Organización desarrolle lo siguiente:<br><br>1. Definir alcance:<br>• Describir la misión, visión y objetivos de su empresa.<br>• Incluir el organigrama e Indicar el número de trabajadores.<br>• Describa como resumen los productos y/o servicios que brinda su organización<br><br>2. Evaluación del riesgo y plan de tratamiento.<br>• Identifique y describa 03 activos de información.<br>• Identifique y describa 03 riesgo asociados a los activos de información.<br>• Identifique y describa 03 amenazas y 03.<br>• vulnerabilidades por cada riesgo identificado.<br>• Valore la probabilidad e impacto de cada riesgo identificado.<br>• Describa el plan de tratamiento por cada riesgo<br><br>3. Indicadores<br>• Identifique y describa 03 indicadores de seguridad de la información asociados a los riesgos identificados |
| **Semana 4** | Monitoreo:<br>• Gestión de Incidentes.<br>• Gestión de Indicadores.<br>• Seguimiento de la Gestión de Seguridad de la Información. | Tomando como referencia a su Organización registre un incidente y desarrolle lo siguiente:<br><br>1. Describa un incidente de seguridad de la información que genere daño grave a su organización.<br>• ¿qué características de la seguridad de la información ha afectado (confidencialidad, integridad, disponibilidad)?<br>• ¿cómo gestionaría el incidente para minimizar su impacto y dar continuidad al negocio de su organización?<br>2. Describa o diagrame la interacción del equipo de respuesta a incidentes con el comité de crisis y planes de continuidad/DRP en relación con el incidente de seguridad. |

| | | |
|---|---|---|
| | | 3. Describa una lista de proyectos de seguridad, pero incrementar la madurez de seguridad de la información en su organización |
| **Semana 5** | Revisión<br>• Gestión de Auditorías Internas.<br>• Gestión de Auditorías Externas | Tomando como referencia a su Organización desarrolle lo siguiente:<br>1. Preparación.<br>• Describa el alcance de auditoría interna (indicar que procesos auditará).<br>• Elabore un plan de auditoría interna para un año.<br>• Elabore una lista de preguntas para realizar la auditoría interna.<br>2. Ejecución<br>• Responder las preguntas de auditoría interna.<br>4. Resultados<br>• Elabore el informe de auditoría interna.<br>Participación el foro de debate<br>Evaluación de conocimiento. |

## 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 |
|---|---|
| Iris Pretel Trejo<br>INICTEL-UNI<br>ipretel@inictel-uni.edu.pe | Rodrigo Robles<br>Oficina Regional de la UIT para las Américas<br>rodrigo.robles@itu.int |

## REGISTRO Y PAGO

### 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.

### 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/sistema-de-gestion-de-seguridad-de-la-informacion

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

### Inscripción en el curso

1. **Pago en línea**
   Se aplica una tarifa de formación de **USD 300** por participante para este curso. El pago debe ser realizado a través del sistema en línea utilizando el enlace mencionado anteriormente para la inscripción en: https://academy.itu.int/training-courses/full-catalogue/sistema-de-gestion-de-seguridad-de-la-informacion

2. **Transferencia bancaria internacional**
   Cuando no sea posible realizar el pago a través del sistema en línea, es posible seleccionar la opción de *offline payment* para generar una factura a través del miso enlace del curso. Descargue la factura para realizar una transferencia bancaria a la cuenta de la UIT que se indica a continuación, y remita el comprobante de la transferencia y la copia de la factura a hcbmail@itu.int, con copia para el Coordinador de Curso en UIT. **Todas las tarifas sobre transacciones bancarias deben ser sufragadas por el participante.**

   **En el caso de que los documentos referentes al pago no sean enviados, la inscripción en el curso no será confirmada.**

3. **Pago en grupo**
   Si desea pagar por más de un participante mediante transferencia bancaria y necesita una factura para todos ellos, cree una cuenta como **Contacto institucional**. Los contactos institucionales son usuarios que representan una organización. Cualquier estudiante puede solicitar ser un contacto institucional o pertenecer a cualquier organización existente.

   Para hacer esto, diríjase a su página de perfil haciendo clic en el botón **"Mi cuenta"** en el menú del usuario. Al final de esta página debería ver dos botones:

a. Si desea **convertirse en un contacto institucional**, haga clic en el **botón "Solicitar ser un contacto institucional"**. Esto lo redirigirá a un pequeño formulario que le pedirá el nombre de la organización. Después de completar el nombre de la organización que desea representar, haga clic en **"continuar"** y se creará una solicitud. Un administrador de la Academia de la UIT revisará manualmente esta solicitud y la aceptará o denegará en consecuencia.

| **ITU BANK ACCOUNT DETAILS:** | |
|---|---|
| Name and Address of Bank: | UBS Switzerland AG<br>Case postale 2600<br>CH 1211 Geneva 2<br>Switzerland |
| Beneficiary: | Union Internationale des Télécommunications |
| Account number: | 240-C8108252.2 (USD) |
| Swift: | UBSWCHZH80A |
| IBAN | CH54 0024 0240 C810 8252 2 |
| Amount: | USD 300 |
| Payment Reference: | CoE-AMS 26457- P.40591.1.02 |

## 4. Otros métodos de pago

En caso de que las regulaciones nacionales restrinjan la posibilidad de completar el pago mediante las opciones informadas, le solicitamos contactar al Coordinador de la UIT para mayor asistencia.