Smart Computing
Strategic Communication

SCC016 Seguridad Informática

Objetivo: Este curso tiene por objetivo analizar y entender los riesgos existentes ante hechos fortuitos y ataques, permitiendo detectar vulnerabilidades. Estudia los tipos y formas de daños o ataques que pueden producirse. Propone una metodología de planes de contingencia para prevenir, detectar y minimizar estos riesgos.

Dirigido a:

- Público en General
- Directores, Gerentes Generales y Propietarios
- Especialistas de Informática y Estudiantes de Informática
- Auditores, Encargados de Seguridad Informática
- Free Lancers

Alcances:

- Obtener los fundamentos básicos para manejar:
  - Asegurabilidad de los Datos
  - Asegurabilidad de Identidad

Contenido:

1. **Descripción general de las áreas en las que se enfoca la seguridad.** Describe las bases en las que se analiza y planifica el aseguramiento de la información.

2. **Capas y Niveles de Seguridad.** Definición de Seguridad informática y Seguridad de la información. Triángulo fundamental de la seguridad informática (CIA)

3. **Diagnóstico de Vulnerabilidades.** Conocido como Hacking Ético. En este curso el alumno aprenderá técnicas básicas para la realización de ataques en redes de datos, así como el proceso que siguen los profesionales de la seguridad al momento de identificar, enumerar y describir las vulnerabilidades que aparecen en un sistema informático.

4. **Planes de Contingencia.** Se presenta el Plan de contingencias como un instrumento de gestión para el buen gobierno de las Tecnologías de la Información y las Comunicaciones. Dicho plan contiene las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de una compañía. La aplicación del plan de contingencias como un caso particular del plan de continuidad del negocio aplicado al departamento de informática o tecnologías.

5. **Normativas Internas, Externas y Generales**. Describe las principales normativas de seguridad, cómo se diferencian y cómo seleccionar la más apropiada.

6. **Definición de la Visión Tecnológica**

7. **El papel del oficial de seguridad ISO (Internet Security Officer)**

8. **Metodologías, Fundamentos de la normativo ISO, Cobit e ITIL.**

9. **Trazabilidad.** Se presenta la importancia del manejo de la seguridad de la información basada en la tecnología y la necesidad de que puede ser confidencial; centralizada y tener un alto valor. Puede ser divulgada, mal utilizada, ser robada, borrada o saboteada. Cómo afecta su disponibilidad y la pone en riesgo. Se presenta cómo lograr un seguimiento seguro de la información.

10. **Planeación y Mediciones.** El propósito del plan de seguridad de sistemas informáticos es proporcionar una visión general de los requisitos de seguridad del sistema y se describen los controles para cumplir esos requisitos.

11. **Auditoría Informática forense, sus fundamentos, alcances y ejecución** auxiliados de herramientas tecnológicas.

12. **Continuidad**. El campo de la seguridad de la información ha crecido y evolucionado considerablemente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial. Este campo ofrece muchas áreas de especialización, incluidos la auditoría de sistemas de información, planificación de la continuidad del negocio, ciencia forense digital y administración de sistemas de gestión de seguridad, entre otros. En este curso se trata cómo garantizar la continuidad como medida a pesar de posibles violaciones a la seguridad.

Requerimientos técnicos: Se requiere que el estudiante tenga dominio de las condiciones básicas relacionadas con el manejo de herramientas informáticas y de comunicación.