



Universidad de la Sierra Sur

División de Estudios de Posgrado

Clave DGP: 200147

Maestría en Gobierno Electrónico

PROGRAMA DE ESTUDIO

NOMBRE DE LA ASIGNATURA

Seguridad en el Uso de TIC

CICLO	CLAVE DE LA ASIGNATURA	TOTAL DE HORAS
Cuarto semestre	1045	96

OBJETIVO(S) GENERAL(ES) DE LA ASIGNATURA

Identificar las diferentes amenazas y riesgos que enfrenta la administración pública y los ciudadanos al usar los medios electrónicos, para desarrollar estrategias de prevención en el manejo responsable de las TIC y realizar las diversas actividades y transacciones en los medios electrónicos de manera segura.

Conocer la legislación sobre el uso de las TIC y la protección de los derechos individuales para difundirlas y aplicarlas en el ámbito profesional, así como establecer el marco legal de los procesos de gobierno electrónico.

TEMAS Y SUBTEMAS

TEMA 1. Internet

- 1.1 Reseña Histórica
- 1.2 Definición y Características
- 1.3 Cómo conectarse a Internet
- 1.4 Implicaciones jurídicas del empleo de Internet

TEMA 2. Introducción a la seguridad de la información

- 2.1 Historia de la seguridad informática
- 2.2 Servicios de seguridad
- 2.3 Criptología, criptografía, criptoanálisis y esteganografía
- 2.4 Tipos de atacantes

TEMA 3. Anonimato y privacidad

- 3.1 Navegación anónima
- 3.2 Correo electrónico anónimo
- 3.3 La privacidad en las redes sociales
- 3.4 Protección frente al spyware y programas espía
- 3.5 Borrado de rastros en el computador
- 3.6 Leyes de protección de datos de carácter

TEMA 4. Autenticación y autorización

- 4.1 Tipos de autenticación
- 4.2 Métodos de autenticación
- 4.3 Autorización: permisos y control de acceso

TEMA 5. Seguridad en el gobierno electrónico

- 5.1. Elementos integrantes de las transacciones electrónicas en el gobierno electrónico
- 5.2. Fases de una transacción electrónica para gobierno electrónico
- 5.3. Dificultades de las transacciones electrónicas en el gobierno electrónico
- 5.4. Firma digital: definición, características, funcionamiento
- 5.5. Entidades de certificación y certificados digitales
- 5.6. El papel del Estado en la certificación y certificados digitales
- 5.7. Los medios de pago electrónicos
 - 5.7.1. Características de los medios de pago electrónico
 - 5.7.2. Clasificación de los medios de pago electrónicos
 - 5.7.3. Principales medios de pago electrónico en el mercado mundial
 - 5.7.4. Utilización de pagos electrónicos en el sector público

5.8 Los avances en México sobre la firma electrónica y los servicios electrónicos de pago de impuestos y servicios públicos

TEMA 6. Seguridad jurídica en el gobierno electrónico

- 6.1. Principios de seguridad jurídica en las transacciones electrónicas del gobierno electrónico
 - 6.1.1. Naturaleza jurídica de la firma digital
 - 6.1.2. Naturaleza jurídica de las entidades de certificación
 - 6.1.3. Aspectos jurídicos del pago
- 6.2. Funciones del sistema de seguridad jurídica en las transacciones electrónicas gubernamentales
- 6.3. Funcionamiento del sistema de seguridad jurídica en el gobierno electrónico
- 6.4. Principios que regulan el funcionamiento del sistema de seguridad jurídica en el gobierno electrónico
- 6.5. Leyes sobre gobierno electrónico en América Latina: gobierno-ciudadano, gobierno-empresa, gobierno-gobierno

ACTIVIDADES DE APRENDIZAJE:

Con docente:

- Análisis, síntesis y reflexiones de la literatura.
- Participaciones y discusiones abiertas y dirigidas de los alumnos sobre los temas.
- Revisión de estudios de casos, ejemplos y prácticas para vincular la teoría de la clase con la realidad.
- Asignación de diversas actividades a los alumnos que coadyuven a la reflexión y conocimiento en los alumnos de los temas de la asignatura.
- Las estrategias y material didáctico que considere el profesor para conducir el proceso de aprendizaje.

Independientes:

- Revisión de la literatura básica y complementaria de la asignatura.
- Análisis y síntesis de la literatura.
- Cualquier otra actividad que detone reflexiones e incremente sus conocimientos en el área.

CRITERIOS Y PROCEDIMIENTOS DE EVALUACIÓN Y ACREDITACIÓN

- La acreditación consistirá en tres evaluaciones parciales y una evaluación ordinaria.
- El promedio de las tres evaluaciones parciales corresponde al 50% de la calificación final, el restante 50% corresponde a la evaluación ordinaria.
- Los parámetros de las evaluaciones parciales serán a consideración del profesor en función del contenido y objetivo de esta asignatura, debiendo contar con evidencia escrita de las mismas.
- Para tener derecho a presentar las evaluaciones parciales y ordinaria, se deberán cubrir al menos el 85% de asistencias.
- Las evaluaciones parciales y ordinaria se efectuarán de acuerdo al calendario vigente de la Universidad.

BIBLIOGRAFÍA

Básica:

1. Gonzalo Álvarez Maraño y Pedro Pablo García (2004). Seguridad Informática para Empresas y Particulares. McGraw-Hill.
2. Mohammad S. Obaidat y Noureddine A. Boudriga (2007). Security of E-Systems and Computer Networks. Cambridge University Press.
3. Hernán Torres Álvarez (2005). El Sistema de Seguridad Jurídica en el Comercio Electrónico. Fondo Editorial de la Pontificia Universidad Católica del Perú.
4. Isidro Laso y Marta Iglesias (2002). Internet, Comercio Colaborativo y m-Comercio: Nuevos Modelos de Negocio. Ediciones Mundi-Prensa.

De consulta:

1. Gonzalo Asensio (2006). Seguridad en Internet Una Guía Práctica y Eficaz para Proteger su PC con Software Gratuito. Ediciones Nowtilus S.L.
2. Timothy Braithwaite (2002). Securing E-Business Systems. A Guide form Managers and Executives. John Wiley and Sons Inc.
3. Joao L. Monteiro, Paula M.C. Swatman y Luis Valadares Tavares (2003). Towards the Knowledge Society: E-Commerce, E-Business and E-Government. Kluwer Academic Publishers.

PERFIL PROFESIONAL DEL DOCENTE

- Maestría o Doctorado en áreas relacionadas con la seguridad de la información con formación en gobierno electrónico.
- Experiencia profesional y en investigación en el área.
- Experiencia docente mínimo a nivel licenciatura.