Seminario I. Ciberseguridad

Programa

El estudiante propondrá acciones de ciberseguridad dentro de las estrategias de seguridad ciudadana, para prevenir o disuadir el delito o como medida de detección e identificación del infractor.

Unidad 1

Seguridad en el mundo virtual

Se le llama Ciberseguridad a la parte de la seguridad que se ocupa de los delitos cometidos en el ciberespacio y la prevención de los mismos.

La ciberseguridad es el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno. Los activos de la organización y los usuarios son los dispositivos informáticos conectados, los usuarios, los servicios/aplicaciones, los sistemas de comunicaciones, las comunicaciones multimedios, y la totalidad de la información transmitida y/o almacenada en el ciberentorno. La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad, integridad, que puede incluir la autenticidad y el no repudio; así como la confidencialidad.

En esta unidad analizaremos diferentes definiciones de Ciberseguridad, así como los conceptos de cibercrimen y cuáles son las amenazas que se pueden encontrar.

Investigarás y analizarás la importancia de las leyes que rigen, usos y funcionamientos tanto nivel nacional como local, también analizarás la implementación de estrategias de ciberseguridad donde relaciones la seguridad ciudadana con la ciberseguridad.

Objetivos de Aprendizaje

El estudiante identificará el concepto de Ciberseguridad y su relación con la seguridad ciudadana.

Contenido

Elementos de la Ciberseguridad.
Seguridad ciudadana y Ciberseguridad.
Derechos fundamentales en el ciberespacio.
Principios y elementos de la Ciberseguridad.

Unidad 2

Elementos y principios de las políticas de Ciberseguridad

En la presente unidad analizarás la importancia de la seguridad informática y la necesidad de una protección de los sistemas y redes, ya que es un tanto crítica, pues la explotación de las vulnerabilidades es tan efectiva que pueden desmantelar por completo todas las infraestructuras, ocasionando así desastres asociados a fallos informáticos.

La estrategia actual es adoptar medidas preventivas para adelantarse al atacante.

Conocerás estrategias y políticas que aseguren que el modo de operación de un sistema sea seguro; estas estrategias deberán garantizar que el acceso a la información sea autorizado y no haya sido modificada, que los sistemas y los datos estén disponibles para los usuarios. Para esto, existen diferentes mecanismos que permiten lograrlo, los cuales también explorarás.

Conocer algunos casos específicos de implementación de políticas de ciberseguridad te permitirá acercarte a la realidad y ver con mayor claridad las situaciones de riesgo que ya se han presentado y diferentes formas de abordarlas.

Objetivos de Aprendizaje

El estudiante diseñará una propuesta de seguridad cibernética a partir de la identificación de los elementos de una política de ciberseguridad.

Contenido

Elementos normativos, principios normativos y política pública o social.
Implementación de políticas de ciberseguridad y ataques en el ciberespacio
Estrategias normativas nacionales, locales y empresariales.

Unidad 3

Evaluación de políticas de ciberseguridad

El ciberespacio es un medio con gran potencial, pues la era de la computación electrónica de una manera u otra ha llegado. La inercia de las fuerzas de la historia, o de las fuerzas del mercado, irremediablemente la hubieran traído.

La variedad de sus aplicaciones iniciales detonó una avalancha de cambios en nuestro entorno, los cuales se comentarán en tres ejes: dentro del sector empresarial, en el sector público y en la vida cotidiana de la sociedad.

Los sistemas de control informático, como las redes sociales, tienen la finalidad de comunicar a personas de todo el mundo, enviando información de un usuario a otro a través de datos de texto, números, en tiempo real o aun cuando un usuario no esté en línea. Estos sistemas facilitan

la administración de las distintas versiones de cada producto, así como las posibles especializaciones realizadas.

Se dice que las nuevas tecnologías de la información son un arma de doble filo, ya que aumentan nuestras capacidades y nuestro poder, pero a su vez hacen a sus usuarios más vulnerables a la vigilancia y a la manipulación.

En esta unidad revisarás diferentes estrategias cibernéticas, las normas de control que se van planteando en el establecimiento de limitaciones a la concepción, así como herramientas metodológicas.

Objetivos de Aprendizaje
El estudiante analizará los modelos y sistemas de control y seguridad para contrarrestar las amenazas en el ciberespacio a nivel local y empresarial.

Contenido
Modelos de sistema de control a nivel local y empresarial.
Amenazas en el ciberespacio a nivel local y empresarial.
Acciones de medida de seguridad en el ciberespacio a nivel local y empresarial.