

Los DELITOS relacionados con EL USO DE INFORMACIÓN y herramientas de IT se incrementaron en el último año un 31% . Conozca las principales reglamentaciones y el alcance de su Responsabilidad como Directivo, así como las medidas recomendadas para reducir los riesgos a que se expone

A quién está dirigido?

- Directivos, Gerentes, Responsables y profesionales de TI de Seguridad de la Información y Auditoría.
- Empresarios, profesionales y comunidad en general con conocimientos básicos de sistemas que estén interesados en la materia.

Objetivos Académicos:

Que el asistente sea capaz de:

- Identificar Bienes Intangibles a proteger
- Cumplimentar Regulación Legal respectiva
- Actuar conforme el Alcance de su responsabilidad como directivo o empleado
- Aplicar las Herramientas disponibles desde aspectos funcionales y técnicos
- Promover la utilización de los instrumentos legales que orienten a una Política de Seguridad sólida en su organización.
- Poner en práctica medidas de implementación para cumplir con los aspectos legales vigentes.

Cuerpo Docente ISEC LEGAL

- Equipo multidisciplinario de Consultores Certificados en Tecnologías de la Información y Abogados Especializados en Delitos Informáticos, así como otros referentes especialistas invitados.

Material de estudio: Incluido en el dictado del curso.

Requisitos aprobación: 75 % asistencia, aprobación de examen final.

CRONOGRAMA:

Fecha de inicio: Agosto 2008

16 clases presenciales 18.30 hs a 21.30 hs.

Clases especiales y talleres prácticos de carácter opcional los días jueves 18.30 hs

Valor del programa de capacitación:

\$ 3500 más IVA.

Descuento par ex alumnos 10 %.

Sede: Information Security SA, Bartolomé Mitre 948

TEMARIO:

TRACK 1: INTRODUCCION GENERAL.

MODULO 1: INTRODUCCIÓN AL DERECHO INFORMÁTICO.

Tendencias Internacionales (USA, CCEE, Latam). Marco General: Situación Actual. Relación general entre Informática y Derecho. Supuestos de responsabilidad en el entorno digital.

MODULO 2: MARCO TEORICO - LEYES Y REGULACIONES RELACIONADAS

Leyes Locales : revisión de las principales regulaciones a nivel nacional. Leyes y Regulaciones Internacionales. Análisis de Casos y Jurisprudencia. Estado de la jurisprudencia nacional e internacional acerca de los tópicos del curso: "leading cases".

TRACK 2: IMPLEMENTACION PRÁCTICA POR PROCESOS:

En los siguientes Módulos se analiza cada problemática relacionada con las principales regulaciones relacionadas, así como los riesgos relativos para la Organización, Directivos, Usuarios, Responsables de TI, de Seguridad y Auditoría, y las Medidas Concretas de Implementación para reducir o acotar los riesgos y responsabilidades mencionados

MODULO 3: Confidencialidad de la información e intercambio con terceros

MODULO 4: Uso de Herramientas Informáticas en General

MODULO 5: Uso del Correo Electrónico y Mensajería Instantánea

MODULO 6: Regulación Legal de Internet

MODULO 7: Ilícitos Cometidos Usando las TIC's

MODULO 8: Régimen Legal de Protección de Datos Personales

MODULO 9: Régimen Legal de las Telecomunicaciones

MODULO 10: Régimen Jurídico de Protección de la Propiedad Intelectual

MODULO 11: El Comercio Electrónico y la Problemática de la Contratación On Line

MODULO 12: Contratos de Servicios y Productos Informáticos

MODULO 13: Privacidad e Intimidad de los Usuarios de TI

MODULO 14: Regulación de las Nuevas Tecnologías

MODULO 15: Conservación de Logs y Evidencias. Investigación y Análisis Forense

TRACK 3 : CONSOLIDACION

MODULO 16: Mantenimiento del Sistema de Protección en el Tiempo:

Revisión de las principales regulaciones aplicables y de los riesgos para la Organización, Directivos, Usuarios, Responsables de TI, de Seguridad de la Información y de Auditoría

Elaboración de un plan de mantenimiento que incluya las acciones a cumplimentar por los distintos departamentos de la Organización

CLASE ESPECIAL 1:

Análisis de un caso de robo de información por parte de un empleado luego contratado por la competencia

Elaboración de acuerdos de confidencialidad y no competencia

Diseño de una política de seguridad de la información de la empresa

CLASE ESPECIAL 2 :

Elaboración de un Plan de Concientización y su Implementación en la organización

Elaboración de un Manual de uso de herramientas informáticas. Convenios de Confidencialidad

CLASE ESPECIAL 3 :

Diseño del contenido de una política de uso sobre el correo corporativo y correo personal en la empresa. Accesos remotos y transferencia de archivos.

CLASE ESPECIAL 4:

Medidas de protección del Site Corporativo. Cómo prevenir un ataque DOS. Elaboración de Política de Términos y Condiciones del Site.

CLASE ESPECIAL 5:

Etapas en la investigación y detección de un ilícito informático.

CLASE ESPECIAL 6:

Jacobo Cohen Imach - Mercado Libre y su Política de Protección Intelectual de Terceros.

Software Legal: presentación institucional. Sus actividades y servicios en la actualidad.

Iron Mountain: El contrato de escrow de software

CLASE ESPECIAL 7:

Seguridad en operaciones de Home Banking. Derechos del consumidor e Internet.

CLASE ESPECIAL 8:

Medidas básicas para implementar medidas de auditoría en los sistemas de información de la empresa.

Clase Adicional: Evaluación Final

Cierre: entrega de Certificados.

Informes: Information Security SA

Bartolomé Mitre 948

education.center@isec-global.com