Aspectos Legales de las Tecnologías de la Información en el marco de la Seguridad de la información

El delito informático implica actividades criminales que los países han tratado de encuadrar en figuras típicas de carácter tradicional. Sin embargo, debe destacarse que el desarrollo de las técnicas informáticas ha generado nuevas posibilidades de uso indebido de los sistemas, impulsando lo que se conoce como cibercrimen y creando la necesidad de regulación y análisis de los riesgos técnicos.

Objetivos generales

Este curso está orientado a las nociones legales básicas que deben considerarse en el ámbito de la informática, repasando los tópicos centrales del derecho informático y de seguridad de la información de una organización.

Requisitos previos

Conocimiento básico sobre tecnología y delitos informáticos.

Público Objetivo

El curso está orientado a administradores de IT, responsables de seguridad, área de legales y cualquier persona comprometida con el análisis interno o externo de seguridad en una organización y a personas interesadas en la investigación del cibercrimen.

Finalizado el curso, el asistente será capaz de:

- Entender los aspectos legales de distintas acciones informáticas realizadas a diario.
- Entender los riesgos legales que implican no considerar las adecuaciones a la normativa vigente.
- Diseñar y desarrollar sistemas de información respetando la normativa vigente.
- Mejorar sus aptitudes para el diseño y desarrollo de políticas de seguridad de la información.

Este curso complementa el otro curso **"Delitos informáticos y prevención del cibercrimen"** dictado por **Segu-Info.**

Material a entregar

Presentaciones utilizadas durante el curso y certificado de asistencia y aprobación, ambos en formato digital.

Duración y Modalidad

Este curso teórico/práctico tiene una duración de **24 horas** y la modalidad de cursada es presencial. También puede ser desarrollado ***in-company***.

Instructores

Marcelo Temperini es Abogado (UNL), especializado en Derecho Informático. Director de El Derecho Informático y Socio Fundador de AsegurarTe, empresa dedicada a la Seguridad de la Información.
Es Técnico Analista de Seguridad y Vulnerabilidad de Redes de Información de CISCO.
Actualmente es Doctorando (CONICET) dedicado a la investigación de Delitos Informáticos y Cibercrimen en el Centro de Investigación de la Facultad de Ciencias Jurídicas y Sociales de la Universidad Nacional del Litoral.

Cristian Borghello es Licenciado en Sistemas (UTN), desarrollador, Certified Information Systems Security Professional (CISSP), Certificate of Cloud Security Knowledge (CCSK), Microsoft MVP (Most Valuable Professional) Security.
Actualmente es Director de **Segu-Info** y **Segu-Kids** y se desempeña como consultor independiente en Seguridad de la Información.
Ha brindado cursos y dictado congresos y seminarios nacionales e internacionales sobre Seguridad de la Información.

Temario

Protección de Datos Personales

- Conceptos. Principios Generales de los Datos Personales
- Seguridad en los Datos Personales. Relación con la norma ISO/IEC 27001
- Clasificación de las DB según su contenido. Obligatoriedad de Registro de las DB
- Calidad de los Datos. Consentimiento. Información
- Finalidad. Seguridad. Confidencialidad
- Derechos de los titulares de los datos.
- Control. Medidas de Seguridad
- Responsabilidad en la empresa. Riesgos
- Contratos y su regulación
- Los datos personales en los Términos y Condiciones
- Aspectos legales a tener en cuenta en los desarrollos de sistemas con datos personales
- Leyendas en los emails

Políticas de Seguridad y Control Laboral en la empresa

- Privacidad. Concepto. Importancia
- Control en la Empresa u Organización
- Políticas de Uso Aceptable. Necesidad
- Características: Proporcionalidad. Políticas. Redacción. Información. Capacitación. Consentimiento
- Niveles de Control. Clases. Monitoreo y Acceso
- Sistemas de Monitoreo. Riesgos Corporativos
- Seguridad de la Información, Productividad, Inseguridad Jurídica
- Responsabilidad Civil y Penal. Privacidad Interna

- Email corporativo y email privado
- Situaciones especiales. Dominios
- El riesgo de los Delitos Informáticos
- Casos prácticos y Modelos de Políticas de Control
- Acuerdos de confidencialidad con personal interno y con terceros

Propiedad Intelectual y Licencias

- Propiedad Intelectual. Conceptos
- Protección de creaciones intelectuales
- Free Software Foundation y el Software Libre
- Software de Dominio Público
- Regulación por Licencias
- Copyright y Copyleft. GPL
- Software no libre. Semilibre y Software Privativo
- Software Privativo. Software Comercial

Aspectos Legales en los Contratos de Desarrollo de Software

- Desarrollo de Software. Aspectos a tener en cuenta en la regulación
- Cesión de código fuente
- Plazos. Etapas del desarrollo
- Formas de Entrega. Exclusividad. Intransmisibilidad
- Condiciones de ejecución. Ámbito de aplicación
- Provisión del Hardware. Mantenimiento
- Seguridad de la Información
- Deber de confidencialidad
- Manuales de Uso
- Tipo de Licencia. Duración
- Deber de colaboración
- Capacitación al personal
- Responsabilidad y Garantías

Aspectos Legales del Cloud Computing

- Contratos. Clasificación y Libertad contractual
- Términos y Condiciones de Servicios (TOS). Evolución. La ingeniería jurídica en los servicios en internet
- Datos Personales en Cloud Computing
- Propiedad Intelectual en Cloud Computingt
- Confidencialidad. Contratos
- Régimen de Responsabilidad. Contenidos. Servicios
- Contratos. Garantías. Pre contractuales. Contractuales. Post contractuales. Sistemas de Seguros
- Service Level Agreement (SLA). Privacy Level Agreement (PLA)
- Continuidad del Servicio. Posibilidad de Auditorías
- Pruebas y evidencia digital. Gestión de la Seguridad. Servicio Técnico

- Cláusulas contractuales comunes a tener en cuenta
- Casos Prácticos. Google. Contratos. CUG. Microsoft. Facebook

Delitos Informáticos

- Derecho y Seguridad de la Información
- Derecho Penal. Concepto de Delitos Informáticos
- La protección del bien jurídico. Clasificación
- El problema de la Pornografía Infantil
- Acceso indebido a las comunicaciones. Hacking
- La punición del hacking y sus diferentes posturas en el mundo
- Difusión de comunicaciones electrónicas
- Acceso indebido a bases de Datos Personales
- Fraudes Electrónicos. Phishing. El problema de su tipificación
- La captura ilegítima de datos confidenciales
- Cracking. Malware
- Anonymous y el hacktivismo
- La revelación de secretos. Delito
- El problema de los delitos informáticos. CaaS (Crime as a Service)
- Investigación. Recolección de evidencias
- El convenio de Cibercriminalidad de Budapest