UNIVERSIDAD DE Belgrano
BUENOS AIRES - ARGENTINA

Educación Continua 2013

Curso
GESTIÓN TACTICA DE LA SEGURIDAD DE LA INFORMACIÓN

Breve introducción

Hoy en día las organizaciones están tomando mayor conciencia sobre la importancia de gestionar la seguridad de la información, siendo éste su principal activo, y un medio necesario para garantizar la continuidad de sus servicios en particular, y del negocio en general.

La Universidad de Belgrano entiende que en un proyecto de implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) participan empleados de todos los niveles jerárquicos, con diferentes competencias. Por esta razón ha planificado la enseñanza del tema en 3 cursos independientes, y a la vez complementarios, dirigidos al nivel estratégico, táctico y operativo.

Este curso de Gestión Táctica de la Seguridad de la Información está dirigido al nivel gerencial o de mandos altos y medios. También puede ser tomado por personas que no tengan este nivel pero que aspiren a tenerlo.

Es un curso que, pese a su corta duración, enseñará con un buen nivel de profundidad los requisitos y las buenas prácticas necesarias para Diseñar; Implementar, Operar Monitorear, Mantener, Mejorar y Auditar un SGSI. Del mismo modo aportará metodologías para desarrollar un Sistema de Gestión de Riesgos, un proceso de Continuidad de negocio y un proceso de Auditoría Interna de la Gestión de la Seguridad de la información.

Características del Curso

Este curso se caracteriza por abordar, en la menor carga horaria necesaria, las principales problemáticas de los Gestión Táctica de la Seguridad de la Información incluyendo la administración de los activos sensibles de la información. Además, a través de un enfoque táctico operativo, integra la gestión de los riesgos de seguridad con la planificación de la Gestión de la continuidad del negocio (BCM), elaborando planes de continuidad de negocio (BCP), planes de contingencia y planes de Recuperación ante Desastres (DRP).
Los conceptos de la Gestión Táctica de la Seguridad de la Información se complementan con la visión Sistémica de Gestión de Riesgos (SGR) apoyándose en las mejores normas y prácticas internacionales, principalmente las normas ISO/IEC. Por último, capacita al alumno en Auditorías Internas de un Sistema de Gestión de Seguridad de la Información, conforme al cumplimiento de normas, marcos, leyes y regulaciones referidas a la seguridad de la información.

El valor del curso se resume en las siguientes fortalezas:

1. El curso explica a nivel Táctico los conceptos necesarios para una buena administración de la seguridad de la información dentro de toda la organización, así como también indica los requisitos para desarrollar un Sistema documentado que permita una futura certificación ISO/IEC 27001.

2. Tiene un abordaje interesante en lo que respecta a la gestión y tratamiento de riesgos, integrada como un sistema de gestión en sí mismo.

3. El cuerpo académico tiene una excelente trayectoria en temas de seguridad de la información y gestión de riesgos, habiendo participado tanto en proyectos de implementación comoen auditorías de certificación de Sistemas de Gestión de la Seguridad de la Información (IRAM-ISO/IEC 270001) y Sistemas de Gestión de Servicios de Tecnologías de la Información (IRAM-ISO/IEC 20000-1), en Argentina, Chile y Bolivia.

4. El curso tiene un enfoque práctico para fijar conocimientos y facilitar su implementación en organizaciones.

5. La modalidad de clases está pensada para personas que tienen mucha carga de trabajo, o que viven en el interior o países limítrofes

6. El curso pude articularse con el curso de Gestión Tecnológica de la Seguridad de la Información (nivel Operativo), y próximamente con el curso de IT Governance (nivel Estratégico)

Destinatarios

Gerentes de empresas y de oficinas públicas que requieran implementar los procesos de Gestión de la Seguridad de la Información, Gerentes de Sistemas, oficiales de seguridad, analistas de seguridad, líderes de proyecto, analistas de sistemas, consultores, auditores y profesores universitarios.

Objetivos

Brindar una sólida formación a través del desarrollo de conceptosy metodologías para el diseño eficaz de un Sistema de Gestión de Seguridad de la Información,tanto en los aspectos tácticos operativos como organizacionales.

Desarrollar estrategiaspara la implementación de los procesos delSistema de Gestión de Seguridad de la Informaciónen diversas áreas o tipos de organizaciones, considerando el cumplimiento de las distintas normativas de referencia.

Brindar al participante tácticas para una operación ágil del Sistema de Gestión de Seguridad de la Información, así como la definición de las métricas para el monitoreo de las características de seguridad

Dar criterios para la implementación de una correcta gestión de riesgos, alineado con cada uno de los objetivos de control y en pos de garantizar la continuidad del negocio.

Duración del curso

El curso completo tiene una duración de63horas reloj, desarrolladas de acuerdo a la siguiente modalidad:

3 módulos (a realizarse en encuentros semanales de 9hs cada uno)

Contenidos

El programa completo está compuesto por 3 módulos:

Módulo 1: Gestión de la Seguridad de la información

Módulo 2: Sistema de Gestión de riesgos y Continuidad del negocio

Módulo 3: Auditoría y Compliance de Sistemas de Gestión de la Seguridad de la Información

Gestión de la Seguridad de la información

Objetivos:

Enseñar al alumno el concepto de Sistemas de Gestión y el enfoque en el proceso de negocio. Sensibilizar sobre los problemas de seguridad de la información que amenazan a las organizaciones. Explicar los requisitos de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en la norma IRAM-ISO/IEC 27001 para elaborar un diseño adecuado a cada organización. Explicar cómo debe planificarse la implementación de un SGSI, considerando las buenas prácticas que proporcional la guía IRAM-ISO/IEC 27002.

Contenidos:

Introducción a la Seguridad de la información
A. Antecedentes de la seguridad de la información - Nivelación de conceptos; Definiciones. - Aplicación del concepto GRC (Gobierno-Riesgo-Cumplimiento).
B. Enfoque PDCA para Sistemas de gestión de seguridad de la información - Elementos de un sistema de Gestión - Visión de los procesos.
C. Esquema del Sistemas de gestión de seguridad de la información - Elementos de los esquemas de seguridad y control - Concepto de Controles y Objetivos de control

Requisitos del Sistema de Gestión de Seguridad de la Información(SGSI) conforme a la norma ISO/IEC 27001
D. Serie de normasISO/IEC 27000 - Marco de gestión de la seguridad de la información planteado por la familia ISO/IEC 27000.
E. Requisitos de la Norma ISO/IEC 27001 - Requisitos de la documentación del SGSI - Capítulos de la norma ISO/IEC 27001: Responsabilidad de la Dirección; Auditoría Interna del SGSI; Revisión del SGSI, El rol de la Dirección; Mejora del SGSI
F. Control de Objetivos y Controles - Requisitos del Anexo A de la norma ISO/IEC 27001
Planificación de la implementación de un SGSI
G. Buenas prácticas de la Norma ISO/IEC 27002 - Antecedentes de la norma ISO/IEC 27002 - Recomendaciones para su utilización
H. Modelos de Planificación: - Requisitos para la planificación. Visión del contexto - Planificación del SGSI, Diseño e implementación del SGSI.. - Despliegue de estrategias para la implementación de Controles de seguridad de la información - Modelos: PMI; ISO/IEC 27003
I. Preparación de la organización - Personas. Tecnología, procedimientos - Métricas de desempeño de los procesos del SGSI

Sistema de Gestión de riesgos y Continuidad del negocio

Objetivos:

Enseñar normas y marcos metodológicos para abordar la Gestión de los riesgos en una organización. Sensibilizar sobre la problemática que enfrentan las organizaciones respecto de la administración de sus riesgos, y el rol de un Sistema de Gestión de Riesgos (SGR) como apoyo imprescindible a la gestión de la seguridad de la información y de la gestión de la continuidad del negocio.

Contenidos:

Gestión de Riesgos
A. Gestión de riesgos - Marcos de referencia. - Identificación, análisis, evaluación, tratamiento, monitoreo y revisión. - Metodologías para el análisis y Evaluación de los riesgos de SI en el marco de un SGSI
B. Implementación de un Sistema de Gestión de Riesgos -Principales problemas que tienen las organizaciones en materia de gestión de riesgos

-Sistemas de gestión de riesgos (SGR)
C. Elaboración del SGR - Herramientas de soporte al SGR y a la metodología de evaluación. - Herramientas de Auto evaluación de los riesgo
Continuidad del Negocio
C. Análisis de impacto - BIA (Business Impact Analysis) - Marcos de referencia y metodología
D. Elaboración de Planes - Plan de continuidad del negocio.
- Plan de contingencia. - Plan de recuperación de desastres.

Auditoría y Compliance de Sistemas de Gestión de la Seguridad de la Información

Objetivos:

Enseñar conceptos y procesos de Auditoría Interna de Sistemas de Gestión de la Seguridad de la Información, dar recomendaciones para abordar el tema, y explicar cuáles son las principales normas, reglamentaciones y leyes aplicables al tema de seguridad de la Información, indicando en qué casos aplica cada una de ellas.

Contenidos:

Auditoría de SGSI y cumplimiento con marcos legales, regulatorios y normas internacionales, o internas de la organización
A. Conceptos de Auditoría - Enfoques. - Auditorías Internas, su planificación y ejecución - Preparación documental de las auditorías
B.1 Proceso de Auditorías de Sistema de Gestión ISO/IEC 27007 - Administración del programa y Planes de auditorías. - Ejecución de la auditoría - Devolución de hallazgos - Rol del auditor y del auditor líder
C. Criterios para auditar el Anexo A de la ISO /IEC 27001 - Objetivos de control y controles a auditar - Recomendaciones basadas en ISO/IEC 27002
Compliance
D. Referencia al cumplimientos con otras Normas y frameworks - Normas ISO; Cobit; SOX; COSO;Basilea II; PCI DSS
E. Cumplimiento de Leyes a través de su reglamentación - Análisis de Ley 25.326 de Protección de Datos Personales, Ley 26.388 de Delito Informático y Ley 25.506 de Firma Digital.

- Circulares del BCRA (Banco Central de la República Argentina): A-4609 y A-4793
- Modelo de ONTI (Oficina Nacional de Tecnologías de Información) de políticas de S.I.

Coordinación Académica

CEBALLOS, Jorge Luis

Ing. Especialista en Sistemas de Información
Profesor de nivel grado y posgrado en temas de Calidad y Seguridad de la Información en UB, UTN, UBA. UnLaM. Disertante en varios congresos y seminarios de calidad de software del país y de Latinoamérica.

Ingeniero Mecánico con post-grados en Calidad dictados por la UTN, ITBA,
Becas entre las que se destacan:
"Total Quality Management" en JAPON (Mayo-Junio 1993);
"Information Security Expert" – DGQ (Deutsche Gesellshaft für Qualität) ISO 27001" (2007)

Profesor de Ingeniería de Software IV: Testing y Calidad de la Licenciatura en Sistemas de Información y de la Ingeniería en Informática de la Universidad de Belgrano (UB),
Profesor de Gestión Estratégica de la Seguridad de la Información II en la Universidad de Buenos Aires (UBA),
Profesor de Inspección y Ensayos en la Maestría en Ingeniería en Calidad (UTN).
Profesor en Tópicos avanzados de Diseño de Softwarede la Maestría en Informática (UnLaM)

Disertante en varios congresos y seminarios de calidad de software y seguridad de la información en el país y Latinoamérica.
Ha dictado diferentes cursos de formación y prácticas referidas a Seguridad de la Información, Gestión de Riesgos, Gestión de Calidad, Certificación de productos software, Productividad y Lean Manufacturing.

Desempeñó funciones en la actividad privada y en la función pública en tareas de Diseño y desarrollo del sistema de gestión de calidad y de Seguridad de la Información; Criterios de evaluación de proyectos y Metodologías de productividad y mejora continua.
Fue gerente de calidad en diversas empresas autopartistas.

Actualmente se desempeña como coordinador de laboratorios de Tecnología de la Información, en el Instituto Nacional de Normalización y Certificación (IRAM). Además es auditor IRAM de las normas ISO/IEC 27001 e ISO/IEC 20000-1. También como capacitador dicta cursos en temas de Calidad de software, Gestión de Riesgos, Gestión de Servicios de Tecnología de la Información y en Seguridad de la Información.
En el Ministerio de Desarrollo Económico del GCBA asiste al área de Organización y Métodos en la mejora de la calidad y seguridad de los procesos administrativos de gobierno

Cuerpo Académico

- **ALDEGANI, Gustavo**

  Consultor Independiente en Seguridad Informática con 29 años de experiencia en Implementación de Sistemas Seguros en empresas, organizaciones militares y de gobierno de Argentina, América Latina y Estados Unidos.

  Profesor de la Facultad de Ingeniería y Tecnología Informática de la Universidad de Belgrano.
  Director de la Carrera de Especialista en Seguridad Informática del CCAT (Centro de Capacitación de Alta Tecnología).
  Redactor de la Comunidad de Seguridad Informática de ITSitio.com.
  Consultor contratado por la ONTI (Oficina Nacional de Tecnologías de la Información de la Argentina) entre 2004 y 2007 para el Proyecto de Infraestructura Nacional de Firma Digital.

  Cuenta con 11 libros publicados sobre Seguridad Informática, algunos de los cuales fueron utilizados como libros de texto de la materia en Universidades Nacionales y Privadas de Argentina.

- **ANGELERI, Paula María**

Lic. en Sistemas de Información de la Universidad de Belgrano (UB) y
Master of Information Systems (CGU, USA). Becada por Asociación Fulbright, UB, CGU.

Trayectoria docente a nivel grado y posgrado en materias de Ingeniería de Software, Base de Datos, Seguridad de la Información (UB, UTN), Ingeniería de Requerimientos(CAECE), y Seguridad de la Información (UBA). A cargo de la cátedra de Gestión de la Seguridad de la Información II de MSI de UBA (desde 2011).
Directora de tesis y trabajos finales de posgrado y de grado en UTN, UNNE, UB, UBA.
Coordinadora del Área de Ingeniería de Software y Base de datos en UB.
Directora de carreras de informática de la Facultad de Ingeniería y Tecnología Informática de la Universidad de Belgrano (UB).

Representa a la Argentina en los comités técnicos de ISO (International Standardization Organizartion) e IEC (International Electrotechnical Commission) JTC1-SC7 Software and systems engineering, e ISO/TMB/RM Technical Management Board/ Risk Management. Fue Coordinadora del Subcomité de Calidad en Tecnología de la Información, Coordinadora del Subcomité de Gestión de Riesgos de IRAM, Coordinadora del Subcomité de Seguridad de la Información de IRAM, Consultora del BID (Banco Interamericano de Desarrollo) y Responsable técnica del programa Calidad de software en un proyecto multilateral entre Argentina, Uruguay, Brasil, y Chile.

Se especializa en temas de projectmanagement, sistemas de gestión de la calidad, sistemas de gestión de servicios de TI, sistemas de gestión de seguridad de la información, de gestión de riesgos, y mejora de procesos, dando conferencias a nivel nacional e internacional (México, Colombia y Perú).
Auditora Líder de IRAM em certificaciones IRAM-ISO 9001, IRAM-ISO/IEC 20000-1 e IRAM-ISO/IEC 27001.
Ha publicado y dado ponencias en Congresos Nacionales e Internacionales (USA, Perú), en temas de Calidad de produtos software, Sistemas de Gestión de Servicios para la Continuidad del negocio, Sistemas de Gestión integrados de Calidad, Servicios de Tecnología de la Información y Seguridad de la Información.

Es directora de un proyecto de investigación en UB sobre Evaluación de productos de software (desde 2010), ha participado del proyecto Iberoamericano de investigación COMPETISOFT, del cual surgió el modelo COMPETISOFT de calidad de procesos de software, para PYMES (2006-2009), y ha participado en investigaciones sobre integración entre CRM y Dataware housing (DW), y entre DW y Knowledge Management en USA (1998-1999).

- **FOJO, Diego Hernán**

  Licenciado en Sistemas de Seguridad en Telecomunicaciones - IUPFA

  Auditor Líder /Lead Auditor - SGSI ISO 27001:2005 (A17447) - IRCA
  Information Security Expert – DGQ (Asociación Alemana para la Calidad)

  Consultor especializado en Seguridad de la Información. Durante más de12 años ha realizado numerosos trabajos de implementación de Sistemas de Gestión de Seguridad de la Información, basados en ISO/IEC 27001, tanto en empresas públicas como privadas.

  Es Auditor de certificación para IRAM Argentina en la norma IRAM/ISO/IEC 27001, con experiencia en auditorías en empresas de gran envergadura y en organismos públicos de Argentina, Chile y Bolivia.

  Posee una amplia experiencia en gestión de riesgos de TI y planes de continuidad de negocio.
  Ha capacitado a empresas de Argentina y Chile sobre Sistemas de Gestión de Seguridad de la información, Gestión de Servicios, Gestión de Riesgos y Compliance.
  Cuenta con experiencia en Gestión de Riesgos de TI y cumplimiento normativo (BCRA "A" 4609 / 5374) en entidades financieras.
  Ha participado y liderado proyectos de diseño seguro de redes de telecomunicaciones e implementación de sistemas de seguridad informática (Firewalls, IDS/IPS, Autenticación, Correlación de eventos, Antispam, Antivirus, etc.)

- **VICTTORIOSO, Sebastián**

  Licenciado en Sistemas de Seguridad en Telecomunicaciones - IUPFA

  Information Security Expert – DGQ (Asociación Alemana para la Calidad)
  Auditor Líder /Lead Auditor - SGSI ISO 27001:2005 - IRCA

  En la actualidad se desempeña como Gerente de Servicios Profesionales de ISETEC S.A., liderando proyectos de implementación de sistemas de gestión de seguridad de la información y gestión de riesgos de TI.
  Ha sido Ingeniero de redes en BANELCO, Gerente de Tecnología en NETVERK S.A., Oficial de Seguridad en Etek-Reycom y Consultor en Seguridad de la Información.
  Para el IRAM realiza auditorías de diagnóstico y de certificación en Argentina y países limítrofes bajo los requisitos de la Norma ISO/IEC 27001.

  Posee más de 12 años de experiencia en Seguridad de la Información, realizando sus actividades basadas en buenas prácticas y estándares o guías internacionales ISO/IEC 27001, ISO/IEC 27002, ITIL, Cobit, ISO19011, Octave, Magerit, CommonCriteria sobre: Controles Generales, Planes de Continuidad, Equipos de Respuesta a Incidentes, Arquitectura Segura de Redes de Comunicaciones, infraestructuras de tecnología complejas (Centros de Cómputos).
  Posee gran dominio de los criterios para la implementación de infraestructuras de TI, incluyendo plataformas Windows, Linux, Virtualización de Servidores, Equipos de seguridad (Firewall, IPS, Proxy, AntiSpam, VPN,etc.), Gestión de redes (SNMP, Syslog, monitoreo, etc.).

  Ha capacitado a varias empresas Argentinas sobre Sistemas de Gestión de Seguridad de la información, Gestión de Servicios, Gestión de Riesgos, Compliance y TI.

Consideraciones Generales

- Modalidad

Viernes de 17:00 hs a 21:30 hs. y Sábados de 9:00 hs a 13:30 hs. (cada tres semanas)

- Inicio

13 de Septiembre de 2013

- Cronograma de clases

Cursadas Módulo 1: 13 y 14 de septiembre; 4, 5, 25 y 26 de Octubre 2013

Cursadas Módulo 2: 15 y 16 de noviembre; 6 y 7 de Diciembre 2013

Cursadas Módulo 3: 28 y 29 de Marzo 2014; 18 y 19 de Abril 2014

Duración

63 Hs.

- Asistencia Mínima

75% de las clases

- Sede de Dictado

Dpto. de Estudios de Posgrado y Ed. Continua, Lavalle 485 (Microcentro)

- Metodología

- Se realizan desarrollos conceptuales teóricos sobre cada tema y presentación de casos de aplicación.
- Los alumnos organizados en grupos de 3 a 4 personas elaboran, con asistencia docente, trabajos prácticos de seguimiento de cada tema, incluido un entregable de un proyecto de planificación del SGSI, en base a lo visto en clase o sobre Análisis de casos.
- Los proyectos más destacados serán presentados a sus compañeros, analizados, y debatidos.

- Admisión

- Profesionales de nivel universitario de carreras de Licenciatura en Sistemas, Ingeniería en Informática o carreras afines, o en su defecto, personal que demuestre 2 (dos) años de experiencia comprobada en actividades relacionadas con tecnología de la información.

- Se requiere el envío de un CV actualizado, de la extensión que se prefiera, y fotocopia de título universitario, doble faz, si lo tuviera. En caso de solicitar el certificado de curso de posgrado se requiere presentar en Admisiones el original, lo que será asentado en la fotocopia por la persona que lo viera.

- En caso de no contar con título de grado, solicitar entrevista de admisión para diagnosticar nivel de conocimientos y perfil del alumno a seguridad.TI@ub.edu.ar con copia a educación.continua@ub.edu.ar

- Aprobación

- Nota de Examen, o Trabajo práctico de cada módulo igual o superior a 5 (cinco).
- Presentismo: 75%, asistiendo mínimo a 9 clases de 12.

- Material Didáctico

Especificaciones del material a entregar. Impreso, digital, etc.

- Certificación

La Universidad de Belgrano extenderá el respectivo certificado a quienes tengan la asistencia mínima exigida.