UNIVERSIDAD DE LA REPUBLICA

FACULTAD DE INGENIERIA

COMISIÓN ACADEMICA DE POSGRADO

DESCRIPCIÓN DEL PROGRAMA DE POSGRADO

Nombre del Programa: Especialización en seguridad informática

Montevideo – 2012

1. IDENTIFICACIÓN:

DE LA CARRERA
Nombre del Programa: Especialización en seguridad informática
Programa (especialización, maestría académica o profesional, o doctorado): Especialización

ÁREA ACADÉMICA
Área (Instituto/ Grupo/ Núcleo, etc.): Instituto de Computación
Institutos vinculados al Área: Instituto de Computación
Contacto institucional del Programa Nombre: Gustavo Betarte y Diego Vallespir Teléfono: 2711 42 44 E-mail: {gustun, dvallesp}@fing.edu.uy
Programa compartido con otra Institución: NO Nombre de la Institución: ---------- En caso afirmativo adjuntar copia del acuerdo establecido.

2. UBICACIÓN FÍSICA DEL PROGRAMA

Lugar y dirección completa de la sede del programa:

Instituto de Computación, Facultad de Ingeniería, Universidad de la República
Julio Herrera y Reissig 565

Nombre y teléfono de un contacto en la Institución Sede:

Nombre: Diego Vallespir

Teléfono: 2711 42 44 int. 128

Personal, instalaciones, y materiales disponibles para la realización del programa:

El Instituto de Computación cuenta con alrededor de 170 docentes, de los cuales alrededor de 30 poseen título de doctorado y alrededor de 35 poseen título de maestría (sin incluir los que cuentan con título de doctorado). Una cantidad importante de los mismos participa en el programa en forma estable u ocasionalmente a través de actividades puntuales.

Se cuenta con aulas y salas de computadoras de uso compartido de la Facultad de Ingeniería, así como de equipos especializados (hardware y software) disponible en los diversos grupos de investigación del InCo, que permiten dar los recursos necesarios para la realización de los trabajos de los estudiantes del programa. Asimismo, se cuenta con una sala de posgrados, equipada para 35 participantes, con proyector multimedia, PC, retroproyector y pantalla

También se cuenta con oficina para secretaría, con personal administrativo, con PC e impresora láser para edición del material de los cursos, se suministran carpetas y material impreso para cada curso.

3. OBJETIVOS DEL PROGRAMA

FINALIDAD:

El Diploma de Especialización en Seguridad Informática se dirige a profesionales en Informática, que deseen especializarse en el área de Seguridad Informática.

OBJETIVOS ESPECÍFICOS:

El objetivo de este plan de estudios es la formación de Especialistas en Seguridad Informática capacitándolos en las temáticas relacionadas en esta área. Este Diploma de Especialización se dirige a profesionales en informática, que deseen especializarse en el área Seguridad Informática y apunta a formar profesionales éticos capaces de implementar las mejores prácticas y tendencias, conocer y cumplir las normativas y regulaciones nacionales e internacionales, generar y transmitir conocimiento en el área de forma de alcanzar mayores y mejores niveles de seguridad de la información.

PERFIL DEL EGRESADO:

El egresado adquirirá la capacidad de aplicar con profundidad y solvencia en su actividad profesional los temas incluidos en el Diploma; asimismo, adquirirá los elementos metodológicos que junto con la capacidad de abordar bibliografía especializada le permitan comprender y emplear las nuevas tecnologías para la resolución de problemas relativos a la Seguridad Informática en su actividad profesional.
Se espera que el egresado de este diploma tenga la capacidad para:
- Dominar las áreas fundamentales de la Seguridad Informática
- Ser capaz de tomar decisiones éticas y practicar un comportamiento ético profesional
- Implementar un plan estratégico para gestionar la seguridad de la información en cualquier organización
- Gestionar los riesgos y el impacto que los mismos puedan tener en el negocio de la organización
- Conocer y aplicar las mejores prácticas, tendencias y herramientas para mitigar los riesgos asociados a las diferentes tecnologías de la información
- Implementar metodologías adecuadas para garantizar la continuidad del negocio de la organización
- Aprender nuevos modelos, técnicas y tecnologías cuando estas emergen, y apreciar la necesidad de ese desarrollo profesional continuo.
- Diagnosticar la situación de una organización y brindar asesoramiento en materia de seguridad informática
- Gestionar los incidentes de forma efectiva y profesional

4. ORGANIZACION Y NORMAS DE FUNCIONAMIENTO

Duración prevista del programa: La duración prevista para la realización de la Especialización en Seguridad Informática es de entre 12 a 18 meses, con una dedicación estimada de entre 15 y 20 horas semanales.

Número de plazas previstas (incluyendo becas si es aplicable): 35

Número mínimo de alumnos para realizar el programa: 5

Requisitos para obtener el título

Número de créditos mínimos de Actividad Programada: Mínimo de 70 créditos (el crédito es la unidad de medida de la carga de trabajo en los planes de estudio de la Facultad de Ingeniería, y equivale a quince horas de dedicación por parte del estudiante).

Horas presenciales mínimas de Actividad Programada: No corresponde

Estructura de la Actividad Programada (fundamentales y técnicas): cursos de entre 2 y 10 créditos cada uno.

Tesis: No corresponde

Otros:

Ingreso

Perfil de ingreso

Licenciado o Ingeniero en Computación de la Facultad de Ingeniería de la UDELAR, u otros estudios que garanticen el aprovechamiento de los estudios.

Requisitos de Ingreso

Podrán acceder al Diploma de Especialización en Seguridad Informática quienes posean título de grado, en informática, otorgado por la Universidad de la República cuya implementación conste de al menos 360 créditos, o quienes posean otros estudios que, a juicio de la SCAPA-Informática, acrediten una formación que permitan la realización y aprovechamiento del Diploma. La SCAPA-Informática podrá proponer la realización de cursos de nivelación en caso de ser necesario.

Criterios de selección de los candidatos

La admisión tendrá en cuenta los antecedentes del candidato, pudiéndose realizar una entrevista a los aspirantes para complementar la información presentada. La CAP resolverá la admisión de los candidatos en base a los antecedentes del candidato y al informe de la SCAPA-Informática.

5. CUERPO DOCENTE Y SUS ACTIVIDADES

Nombre/titulación/instituto	Horas aula anuales dedicadas al programa	Nº previsto de candidatos a orientar	Nº previsto de estudiantes a orientar en otros programas	Horas anuales de otras actividades vinculadas al programa
01. MSc. OMAR VIERA	40	N/A	--	0
02. MSc. MARIA URQUHART	40	N/A	--	0
03. Dra. DINA WONSEVER	40	N/A	--	20
04. Dra. SYLVIA DA ROSA	40	N/A	--	0
05. Dra. ADRIANA MAROTTA	40	N/A	--	20
06. Dr. RAUL RUGGIA	40	N/A	--	0
07. Dr. EDUARDO GRAMPIN	40	N/A	--	0
08. Dr. JAVIER BALIOSIAN	40	N/A	--	0
09. Dr. HECTOR CANCELA	40	N/A	--	0
10. Dr. ALEJANDRO GUTIERREZ	40	N/A	--	0
11. Dr. ALBERTO PARDO	40	N/A	--	0
12. Dr. GUSTAVO BETARTE	40	N/A	--	20
13. Dr. HERMANN STEFFEN	40	N/A	--	0
14. MSc. JUAN JOSE CABEZAS	40	N/A	--	0
15. Dra. CRISTINA CORNES	40	N/A	--	0
16. Dr. PABLO RODRIGUEZ BOCCA	40	N/A	--	0

17. Dr. ALVARO MARTIN	40	N/A	--	0
18. Dr. ANTONIO MAUTTONE	40	N/A	--	0
19. Dra. LIBERTAD TANSINI	40	N/A	--	0
20. Dr. PABLO EZZATTI	40	N/A	--	0
21. Dr. DIEGO VALLESPIR	40	N/A	--	100
22. Dr. FRANCO ROBLEDO	0	N/A	--	20
23. Dra. REGINA MOTZ	40	N/A	--	0
24. MSc. MARÍA EUGENIA CORTI	40	N/A	--	20
25. MSc. FELIPE ZIPITRÍA	40	N/A	--	0
26. Ing. ALEJANDRO BLANCO	40	N/A	--	0

6. CURRÍCULA

Asignatura nº 01: Fundamentos de Criptografía

Responsable de la asignatura (docente): Dr. Alfredo Viola
Instituto: Computación
Departamento: PROGRAMACIÓN — Arancel: $ 7.000
Nº de Créditos: 5 — Cupos:
Horas Presenciales: 30 hs.

Objetivos:

Presentar al estudiante los principios fundamentales de la criptografía, en donde se integren aspectos teóricos con laboratorios experimentales

Conocimientos previos exigidos:

Metodología de enseñanza:

20 hs. de clases teórico-prácticas.

10 hs. de laboratorio.

Forma de evaluación

Resolución de trabajos de laborario, y una entrega obligatoria con ejercicios resueltos.

Temario:

Algunos requerimientos de seguridad. Aproximación criptográfica en la propuesta de soluciones.

Criptografía de clave privada.

Criptografía de clave pública.

Promitivas criptográficas.

Infraestructura de Clave Pública (PKI).

Bibliografía:

Menezes, van Oorschot, Vanstone: Handbook of Cryptography http://www.cacr.math.uwaterloo.ca/hac/

6. CURRÍCULA

Asignatura nº 02: Gestión y Tecnologías de Procesos de Negocio

Responsable de la asignatura (docente): Ing. Andrea Delgado, MsC, Ing. Daniel Calegari,

Instituto: Computación
Departamento: Grupo COAL — Arancel: $ 17.000

Nº de Créditos: 10 Cupos:
Horas Presenciales: 48 hs

Objetivos:

Brindar una visión general de los temas asociados a la gestión y tecnologías de procesos de negocio, desde el punto de vista del desarrollo de software, presentando conceptos, técnicas, metodologías y herramientas asociadas. Presentar el ciclo de vida de los procesos de negocio, desde su modelado, implementación, ejecución y evaluación, incluyendo notaciones como BPMN, técnicas y herramientas para el modelado y especificación de procesos de negocio como los workflow patterns, así como lenguajes y herramientas para su ejecución (BPEL/XPDL). Brindar conceptos y enfoques para la mejora continua de procesos de negocio, incluyendo procesos, modelo de madurez BPMM, medidas de diseño y ejecución y técnicas como Process Mining para evaluación de la ejecución con herramientas como ProM. Presentar conceptos asociados para la implementación de procesos de negocio con orientación a Servicios (SOC), y su automatización con base en el Desarrollo Dirigido por Modelos (MDD).

Conocimientos previos exigidos:

Metodología de enseñanza:

Tres clases semanales teóricas, una clase semanal de laboratorio en máquina. Dos clases de presentaciones de trabajos finales por los estudiantes. En total son 60 horas de clases presenciales Se estima 1 hora adicional de estudio por cada hora de clase preencial, y 30 hs de estudio asistido, incluyendo comunicaciones personales o por via electrónica con el docente.

Forma de evaluación

Trabajo final en tema a definir con exposición al finalizar el dictado del mismo.

Temario:

1. Introducción a los Procesos de Negocio y tecnologías (3 hs)
   1.1. introducción, definiciones y conceptos (BP, BPMS, ciclo de vida, tipos de Procesos)
2. Patrones de procesos (Van der Aalst) (3 hs)
   2.1. Introducción, definiciones y conceptos
   2.2. Presentación y análisis de los patrones
3. Modelado de Procesos de Negocio (6 hs)
   3.1. introducción, lenguajes y notaciones
   3.2. Modelado con el estándar BPMN
   3.3. Herramientas de modelado con BPMN
   3.4. Caso práctico de estudio
4. Reglas de Negocio (3 hs)
   4.1. Introducción, definiciones y conceptos
   4.2. Modelado de procesos con reglas de negocio
5. Simulación de Procesos de Negocio (3 + 1,5 hs)
   5.1. Introducción, conceptos y definiciones
   5.2. Técnicas y plataformas de simulación de procesos de Negocio
   5.3. Caso práctico de estudio
6. Ejecución de Procesos de Negocio (3 + 1,5 hs)
   6.1. lenguajes de interpretación/ejecución (XPDL, BPEL), Workflows y Web Services (WS)
   6.2. plataformas de ejecución de procesos de Negocio (motores de procesos)
   6.3. Caso práctico de estudio
7. Procesos de Negocio y nuevos paradigmas de software (3 hs)
   7.1. Service Oriented Computing (SOC) (conceptos, servicios, estándares, SOA)
   7.2. Model Driven Development (MDD) (conceptos, metamodelos, estándares, MDA)
8. Enfoques de desarrollo con Procesos de Negocio (3 hs)
   8.1. Desarrollo con PN y Servicios y Dirigido por Modelos
   8.2. Estándar de modelado de servicios SoaML
   8.3. Herramientas de modelado con SoaML
   8.4. Caso práctico de estudio de los temas 7 y 8.
9. Madurez y medición de Procesos de Negocio (6 hs)
   9.1. Modelo de Madurez para Procesos de Negocio (Business Process Maturity Model, BPMM)
   9.2. Medición de Procesos de Negocio: medidas de diseño (modelos) y ejecución
   9.3. Caso práctico de estudio
10. Evaluación de ejecución de Procesos de Negocio (6 hs)
    10.1. Introducción, conceptos, técnicas de business intelligence (BI)
    10.2. Análisis de ejecución de procesos de negocio con Process Mining
    10.3. Herramienta ProM para Process Mining
    10.4 Caso práctico de estudio

Bibliografía:

-"Business Process Modeling Notation (BPMN)", Object Management Group (OMG), <http://www.omg.org/spec/BPMN/1.2/>, enero 2009

-"Business Process Maturity Model (BPMM)", Object Management Group (OMG), <http://www.omg.org/spec/BPMM/>, junio 2008

- "Service Oriented Architecture Modeling Language (SoaML)", Object Management Group (OMG), http://www.omg.org/spec/SoaML/, diciembre 2009

- Query/Views/Transformations (QVT), Object Management Group (OMG), http://www.omg.org/spec/QVT/1.0, (2008)

-"Workflow Patterns", van der Aalst, W.; ter Hofstede, A.; Kiepuszewski, B.; Barros, A., en Distributed and Parallel Databases, 14(3), pages 551, 2003.

- Business Process Management: A Survey, van der Aalst, W.M.P., ter Hofstede, A., Weske, M., In: International 3 Conference on Business Process Management, (2003)

-"Business Process Management, Concepts, Languages, Architectures", Weske, M., Springer-Verlag ISBN 978-3-540-73521-2, 2007.

-"Essential Business Process Modeling", Havey, M., O'Reilly, ISBN: 0-596-00843-0, 2005.

-"Metrics for Process Models: Empirical Foundations of Verification, Error Prediction and Guidelines for Correctness", Mendling J., Volume 6 of Lecture Notes in Business Information Processing (LNBIP). Springer-Verlag, 2008.

- Papers

Agrawal R.., Imielinsky, T., Swami, A. Mining Association Rules between Sets of Items in Large Databases, SIGMOD 1993, 207-216.

Agrawal R., Srikant, R. Fast Algorithms for Mining Association Rules in Large Databases. , VLDB 1994, pp. 485-499

Agrawal R., Srikant, R. . Mining Sequential Patterns, ICDE 1995, pp. 3-14.

Brin, S., Motwani , R., Silverstein, C. Beyond Market Baskets: Generalizing Association Rules to Correlations

Fawcett, T. ROC Graphs: Notes and Practical Considerations for Data Mining Researchers. Technical Report HPL-2003-4, HP Labs, 2003

Garofalakis, M, Rastogi, R., Shim, K. Mining Sequential Patterns with regular expressions constrains. IEEE/TDKE, Vol. 14 n. 3., pp. 530-552.

Flach, P. Putting Things in Order, On the fundamental role of ranking in classification and probability estimation. , 18th European Conference on Machine Learning, 2007.

Japkowicz, N. Learning from Imbalanced Data Sets: A Comparison of Various Strategies. AAAI Workshop, Technical Report WS-00-0

Oates, T. and Jensen, D. Large Datasets Lead to Overly Complex Models: an Explanation and a Solution. pp. 294. Proceedings of the Fourth International Conference on Knowledge Discovery and Data Mining, pp 294 - 298, 1998

Provost, F. Domingos, P. Tree Induction for Probability-based Ranking. Machine Learning, 52,3, September 2003, pp 199-215, 2003

Salzberg, S. On Comparing Classifiers: Pitfalls to Avoid and a Recommended Approach. Data Mining and Knowledge Discovery Journal, Kluwer Academic Publishers, 1, 317-327 (1997)

Srikant R, Agrawal, R. . Mining Generalized Association Rules. VLDB 1995, pp. 407-419

Srikant, R. Agrawal R. . Mining Sequential Patterns : generalization and performance improvements EDBT 1996, pp. 3-17

Libros

Tan Pang-Ning, Kumar Vipin , Steinbach Michael. Introduction to Data Mining. Addison-Wesley, ISBN 0321321367, Mayo 2005

Adamo, J.M. Data Mining for Association Rules and Sequential Patterns: Sequential and Parallel Algorithms. Springer, ISBN 0387950486, Dic 2000

Pyle, D. Data Preparation for Data Mining. Morgan Kaufmann Publishers, 1999

- A.,Business Process Mining: an Industrial Application, van der Aalst, W.M.P., Reijers, H. A., Medeiros, Information Systems Vol.32 Issue 5, 713-732, (2007)
-ProM, Process Mining Group, Eindhoven University of Technology, The Netherlands, http://prom.win.tue.nl/research/wiki

Asignatura nº 03: Inspección de Software: El proceso de Inspección

Responsable de la asignatura (docente): **:** M.Sc Diego Vallespir

Instituto: Computación
Departamento: Arancel: $8500
Nº de Créditos: 5 Cupos: **:**. Cupo máximo de 40 personas
Horas Presenciales: : 24 hs

Objetivos:
: La Inspección de software fue creada por Michael E. Fagan en el laboratorio de Kingston de IBM. La intención atrás de la Inspección es usar métodos estadísticos de gestión de la calidad y del proceso de software. Este método ha demostrado:

11. Ser uno de los métodos más efectivos en la remoción de defectos que se conoce actualmente
12. Tener una relación costo/beneficio mucho mejor que otros métodos de remoción de defectos
13. Permitir la gestión estadística de la calidad y del proceso de software

Este curso busca presentar al estudiante la Inspección de software y el proceso de Inspección de software.

Conocimientos previos exigidos:
Ninguno

Metodología de enseñanza:
El curso se dictará presencialmente en 24 horas de clases teórico/prácticas.
El estudiante deberá dedicar otras 24 horas de estudio individual, y 24 hs de Estudio asistido, que incluye preparación de trabajos, consulta con el docente por distintas vías, etc. Evaluación: 3hs.
Horas teórico-practicas: 48
Horas de Estudio Asistido: 24
Horas de evaluación: 3
Total horas: 75

Forma de evaluación

Participación en clase y examen al finalizar el curso

Temario:

Historia de la Inspección de software y comparación con otros métodos
Los beneficios y costos de la Inspección
Visión general de la Inspección
El proceso de Inspección: Inicio y documentación
El proceso de Inspección: Revisión
El proceso de Inspección: Conclusión
El proceso de Inspección: Mejora de procesos
El rol del líder de la Inspección

Bibliografía:

Software Inspection – Tom Gilb, Dorothy Graham– Addison-Wesley - 978-0201631814 – Enero 1994
Artículos actuales relacionados con cada ítem del temario

Asignatura nº 04: Liderando un equipo de desarrollo de software

Responsable de la asignatura (docente): Diego Vallespir

Instituto: omputación
Departamento:
Nº de Créditos: 5
Horas Presenciales: 24 hs

Arancel: $ 8.500
Cupos: máximo de 40 personas

Objetivos:
En la actualidad el software es desarrollado por equipos de personas. Los proyectos llevados adelante por estos equipos deben ser gestionados cuantitativamente para lograr cumplir con el cronograma, con los costos previstos y con los requerimientos acordados. Este curso tiene dos objetivos principales. Primero, presentar cuáles son los conocimientos y las habilidades necesarias para liderar efectivamente un equipo de desarrollo de software. Segundo, presentar cómo gestionar cuantitativamente proyectos de software usando medidas de calidad, costo y cronograma

Conocimientos previos exigidos: Ninguno

Metodología de enseñanza:
El curso se dictará presencialmente en 24 horas de clases teórico/prácticas.
El estudiante deberá dedicar otras 45 horas de estudio individual y asistido, consultas a docente, presenciales o por via electrónica, etc.).

Forma de evaluación

Participación en clase y examen al finalizar el curso. Hs Evaluación: 4

Temario:

1. El líder y el equipo
   - 1.1. Líder y liderazgo
   - 1.2. Equipos
   - 1.3. Motivación del equipo

2. Construcción de equipos
   - 2.1. Cómo se construyen los equipos
   - 2.2. El Team Software Process - Generalidades y despegue (Launch)

3. Trabajando en equipo
   - 3.1. Gestionando el plan
   - 3.2. Cómo y por qué mantener el foco en el producto
   - 3.3. La importancia de seguir el proceso
   - 3.4. Gestionando la calidad

4. Relacionamiento con la gerencia
   - 4.1. El soporte de la gerencia
   - 4.2. Reportando a la gerencia
   - 4.3. Protegiendo al equipo

5. Manteniendo y mejorando al equipo
   - 5.1. El desarrollo del equipo
   - 5.2. El desarrollo de los individuos
   - 5.3. La mejora de la productividad del equipo

Bibliografía:

TSP Leading a development team - Watts Humphrey – Addison-Wesley - 978-0321349620 – Setiembre 2005

Asignatura nº 05: Seguridad de Redes TCP/IP

Responsable de la asignatura (docente): Alejandro Blanco, Gustavo Betarte
Instituto: Computación
Departamento:
Nº de Créditos: 5
Horas Presenciales: 39
Arancel: $ 8.500
Cupos: Máximo 30 personas, mínimo 10

Objetivos:

El objetivo de este curso es introducir al estudiante en los conceptos básicos de la seguridad informática de redes de datos TCP/IP. El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas, con el objetivo de desarrollar, ampliar o mejorar las plataformas de comunicación de datos. Al finalizar el curso el alumno habrá adquirido los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir una red de datos TCP/IP y establecer los mecanismos de protección adecuados.

Conocimientos previos exigidos:

Profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad informática

Metodología de enseñanza:

El curso consiste de un 75% de exposiciones teóricas (30 hs) y el otro 25% (9 hs) de trabajos prácticos en grupos, que son realizados usando la infraestructura del LaSI (Laboratorio de Seguridad Informática).

El curso se dictará en 10 clases teóricas de 3 horas, 2 clases por semana, durante 5 semanas y 3 sesiones de laboratorio de 3 horas.

De esta forma, previendo una dedicación aproximada del estudiante de 0.5 horas de estudio por cada hora dictada (gran parte del trabajo se realiza en clase), los totales de horas se computan de la siguiente forma:

Horas teórico-practicas: 60

Horas de preparación del trabajo y estudio asitido: 10

Horas de evaluación: 5

Total horas: 75

Forma de evaluación

Se evaluarán los trabajos de laboratorio y un examen final. La realización de las prácticas de laboratorio es obligatoria.

Temario:

1. Repaso protocolo TCP/IP
    1. modelo de capas,
    2. interacción y servicios de capas del modelo,
    3. ARP/IP/TCP-UDP/aplicaciones

2. Problemas de Seguridad protocolo (redes) TCP/IP
    1. Autenticación del origen (IP spoofing)
    2. Interacción IP/MAC, ARP spoofing
    3. Ataques a protocolo de ruteo, ICMP.
    4. TCP session Hijacking, SYN Flooding
    5. Capa de Aplicación: Servicio DNS
    6. VLAN
3. Redes inalámbricas (WIFI).
    1. Requerimientos
    2. WEP, WPA, WPA2, EAP, 802.1X
    3. Integración con redes existentes
4. Seguridad IP (IPSec)
    1. Asociaciones de Seguridad (SA)
    2. Modos de funcionamiento (tunnel y transporte)
    3. Protocolo AH y ESP (encabezados y servicios que ofrecen)
    4. http://www.dafestino.com.uy/)
    5. IPsec y filtrado
5. VPN
    1. Que es una VPN? VPN sobre internet
    2. Implementación de VPN.
6. Firewalls
    1. Definición. Que puede hacer y que NO un Firewall.
    2. Filtrado de paquetes, con y sin estados. Generando reglas de filtrado.
    3. Logging
    4. Arquitecturas de Firewall.
    5. Tipos de Firewall.
    6. Servicios Proxy y NAT.

Bibliografía:

R. Anderson, Security Engineering – A Guide to Building Dependable Distributed Systems, Wiley, Third edition, 2008.

D. Gollmann, Computer Security, Wiley, 2006.

E. D. Zwicky, S. Cooper, & B. Chapman, Building Internet Firewalls, Ed. O'Reilly, 2nd Edition, 2000.

R. Ziegler, Ed. New Riders, Linux Firewalls 2nd Edition.

Charlie Kaufman, Radia Perlman & Mike Speciner, Network Security: Private Communication in a Public World (2nd Edition), Prentice Hall, 2002.

William Stallings, Network Security Essentials: Applications and Standards (4th Edition), Prentice Hall, 2010

J. Edney, W. A. Arbaugh, Real 802.11 Security: Wi-Fi Protected Access and 802.11i, Addison-Wesley Professional, 2003.

Asignatura nº 06: Seguridad de Sistemas Informáticos

Responsable de la asignatura (docente): Alejandro Blanco

Instituto: Computación

Departamento: Programación, Grupo de Seguridad Informática

Arancel: $ 8.500

Nº de Créditos: 5
Horas Presenciales: 36

Cupos: Máximo 30 personas, mínimo 10

Objetivos:

El objetivo de este curso es introducir al estudiante en los conceptos básicos de la seguridad informática. El curso está orientado a profesionales encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas, con el objetivo de desarrollar, ampliar o mejorar las plataformas de computación. Al finalizar el curso el alumno habrá adquirido los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir un sistema informático y establecer los mecanismos de protección adecuados que garanticen la seguridad del mismo.

Conocimientos previos exigidos:

Profesionales informáticos vinculados a la implantación o diseño de mecanismos de seguridad de la información

Metodología de enseñanza:

El curso consiste de un 75% de exposiciones teóricas (24hs) y el otro 25% (8hs) de trabajos prácticos en grupos, que son realizados usando la infraestructura del LaSI (Laboratorio de Seguridad Informática).

El cuso se dictará en 8 clases téoricas de 3 horas, 2 clase por semana, durante 4 semanas y 2 sesiones de laboratorio de 4 horas.

Forma de evaluación

Se evaluarán los trabajos de laboratorio y un examen final. La realización de las prácticas de laboratorio es obligatoria

Temario:

1. Bases y Motivación
    a. Introducción.
    b. Motivación, definiciones y objetivos de la seguridad informática.
    c. Principios de seguridad informática.
2. Seguridad de Sistemas
    a. Identificación, Autenticación
    b. Métodos de Autenticación
    c. Algoritmos y protocolos de autenticación.
3. Políticas de seguridad y mecanismos de control de acceso. Estructuras de control. Seguridad Multinivel.
4. Modelos de control de acceso
    a. Bell-La Padula,
    b. Chinese wall
    c. RBAC
5. Seguridad en Windows.
    a. Arquitectura Windows, Registry, Servicio de Directorio.
    b. Implementación de principals, sujetos y objetos en windows.
    c. Control de Acceso en Windows.
       Tokens, Access Control Lists, Autenticación, etc
    d. Gestión de la Seguridad
       Group Policies, Built-in Accounts, Auditoria, etc
6. Seguridad en Unix
    a. Principals y sujetos y objetos en Unix
    b. Principios generales de seguridad:
    c. programas suid, chroot
    d. variables de ambiente, search path
    e. inetd, wrappers
    f. Auditoria de Logs
    g. Como implementar Seguridad multinivel o RBAC en Unix.
       SELinux, sudo
    h. Hardening

Bibliografía:

R. Anderson, Security Engineering – A Guide to Building Dependable Distributed Systems, Wiley, Third edition, 2008.

D. Gollmann, Computer Security, Wiley, 2006.

R. Morris, K. Thompson, Password Security: A Case History, Comm. ACM, vol. 22, 1979.

D. Klein, "Foiling the Cracker": A Survey of, and Improvements to, Password Security, Proc. USENIX Security Workshop, 1990.

R.S. Sandhu, Lattice-Based Access Control Models, IEEE Computer, 1993.

D. Denning, A Lattice Model of Secure Information Flow, Comm. ACM, vol 19, 1976.

Michael M Swift et al, Improving the granularity of access control for Windows 2000, ACM Trans Inf Syst Secur, 2002

Microsoft, Microsoft Windows 2000 Security: Technical Reference, Microsoft Press, 2000

S. Garfinkel, G. Spafford & A. Schwartz, Practical Unix & Internet Security (3rd Edition), O'Reilly, 2003

Asignatura nº 07: Métodos Cuantitativos Gerenciales

Responsable de la asignatura (docente): Omar Viera
Instituto: Computación
Departamento:
Arancel: $ 15.500
Nº de Créditos: 10
Cupos: Máximo 35 personas
Horas Presenciales: 65

Objetivos:

- Manejar el empleo de modelos cuantitativos provenientes de la Investigación de Operaciones para apoyo a la toma de decisiones.
- Dar experiencia en la representación de problemas empleando modelos de optimización con restricciones.
- Presentar diversos modelos de uso corriente.

Conocimientos previos exigidos:

Metodología de enseñanza:
Clases teórico/prácticas de tres horas cuatro veces por semana

Forma de evaluación

Descripción de un problema real, su posterior modelación y la presentación y entrega de un informe.

Temario:

- Introducción a la modelación.
- Datos y modelos.
- Modelos de optimización con restricciones.
- Formulación de modelos de optimización con restricciones.
- Representación geométrica de modelos de optimización con restricciones.
- Teoría de decisión, árboles de decisión.
- Control de inventarios con demanda conocida.
- Control de inventarios con demanda aleatoria.
- Data Mining.

Bibliografía:

- Golden, Quantitative Concepts for Management. : Prentice Hall; 3rd edition (November 1988), ISBN: 0137466374
- Berry, Linoff: "Data Mining techniques for Martketing, Sales and Customer Support", Wyley & Sons, 1997.
- Apuntes de clase.

Asignatura nº 08: Métodos de Gestión de Proyectos

Responsable de la asignatura (docente): Ing. Daniel Meerhoff, Rudigger Von Sanden
Instituto: Computación
Departamento: Arancel: $ 15.500
Nº de Créditos: 10 Cupos: Máximo 35 personas
Horas Presenciales: 65

Objetivos:

Encuadrar la Gestión de Proyectos en la Teoría de Sistemas. Brindar a los participantes los conceptos fundamentales y metodológicos de las nuevas técnicas existentes para especificar, planificar, ejecutar y controlar proyectos, a fin de lograr proyectos "exitosos". Se abarcarán las técnicas tradicionales de gestión de proyectos, así como los principales conceptos de la metodología del PMI (Project Management Institute) y otros aportes recientes de la Teoría de las Restricciones (TOC) a la gestión de proyectos.

Conocimientos previos exigidos:

Metodología de enseñanza:
Las clases tendrán una duración de 3 horas, dos veces por semana durante 10 semanas, durante las cuales existirá una parte expositiva y otra de trabajo en grupos realizando el análisis de casos. Se plantearán algunos ejercicios para realizar fuera del horario de clase, algunos de los cuales serán obligatorios y servirán para la aprobación del curso.

Forma de evaluación

Mediante la evaluación de ejercicios y problemas obligatorios que serán planteados a lo largo del curso, así como el ejercicio final.

Temario:

1. Introducción. El enfoque de Sistemas y la Gestión de Proyectos.
2. Lista de control de diagnóstico y propuestasGestión del Alcance de un proyecto .
3. Planificación del alcance y evaluación de proyectos.
4. Definición del alcance – WBS.
5. Gestión del Tiempo.
6. Secuenciación de actividades, camino crítico, nivelación de recursos.
7. Software para gestión de proyectos.
8. Gestión de costos.
9. Planificación de costos.
10. Indicadores de Seguimiento, EVA.
11. Teoría de las restricciones aplicada a la gestión de proyectos.
12. Gestión de abastecimiento y contrataciones.
13. Gestión de Riesgo en proyectos.
14. Gestión de Calidad en proyectos.
15. Gestión de recursos humanos en proyectos.
16. Gestión de las comunicaciones

Bibliografía:

1.Project Management Institute. A guide to project management body of knowledge (PMBOK Guide) – 2000 Edition Project Management Institute, 2001, ISBN 1880410230

2.Jolyon Hallows. Information Systems project management: How to Deliver Function and Value in Information Technology Projects, AMACOM,1997, ISBN 0814403689 James P. Lewis. Project planning, scheduling and control, McGraw-Hill Trade, 2000, ISBN 0071360506

3.Robert Newbold. Project management in the fast lane: Applying the Theory of Constraints, Saint Lucie Press, 1998, ISBN 1574441957

4.Eliyahu M. Goldratt. Critical Chain, North River Press Publishing Corporation, 1997, ISBN 0884271536

Asignatura nº 09: Gestión de la Seguridad de la Información

Responsable de la asignatura (docente): Mag. Ing. María Eugenia Corti, Dr. Ing. Gustavo Betarte.
Instituto: Computación
Departamento: Arancel: $ 18.000
Nº de Créditos: 10 Cupos: Máximo 35 personas
Horas Presenciales: 77

Objetivos: El objetivo de este curso es introducir a los estudiantes en los principales conceptos y metodologías asociadas a la gestión de seguridad de la información, y en el marco normativo internacional y nacional existente. Llevar a la práctica una metodología de rápida aplicación para la implementación de un Sistema de Gestión de Seguridad de la Información. Presentar metodologías concretas para la gestión de riesgos y gestión de incidentes. Se abarcarán las principales conceptos entorno a la familia de normas ISO/IEC 27000.

Conocimientos previos exigidos: Ninguno

Metodología de enseñanza:
El cuso se dictará en clases de 3 horas, 3 veces por semana, durante 7 semanas. El curso estará dividido en un 50% de exposiciones teóricas y el otro 50% de trabajos prácticos, en grupos, en los que se aplicarán los conceptos teóricos introducidos. Cada trabajo práctico realizado en clase formará parte de un trabajo final que deberá ser entregado y presentado por el grupo al finalizar el curso.
(comprende una descripción de las horas de clase asignadas y su distribución en horas de práctico, horas de teórico, horas de laboratorio, etc. si corresponde)

Horas clase (teórico): 30
Horas clase (práctico): 24
Horas clase (laboratorio): 0
Horas consulta: 20
Horas evaluación: 3
Subtotal horas presenciales: 77
Horas estudio: 43
Horas resolución ejercicios/prácticos: 30
Horas proyecto final/monografía:0
Total de horas de dedicación del estudiante: 150

Forma de evaluación
El curso se evaluará a partir de:

- trabajos en clase
- un trabajo final y la presentación del mismo
- un examen final.

Temario:

1. Introducción.
    1. Definiciones y conceptos de gestión de seguridad de la información
    2. Confidencialidad, Integridad y Disponibilidad
    3. Marco normativo nacional e internacional
2. Sistema de Gestión de Seguridad de la Información
    2.1 Metodologías de implantación
    2.2 Principales desafíos a enfrentar
    2.3 Herramientas disponibles que faciliten la implantación
3. Gestión de Riesgos
    3.1 Introducción al proceso de gestión
    3.2 Metodologías de análisis de riesgo
    3.3 Tratamiento de riesgos
4. Gestión de incidentes
    4.1 Definición de incidentes
    4.2 Procesos de clasificación, análisis, tratamiento, resolución y cierre
    4.3 Control de flujos de información y procesos.
    4.4 Modelos organizacionales de Centros de Respuesta y su relación con el SGSI
5. Gestión de la continuidad del negocio
    5.1 Componentes del negocio
    5.2 Tipos de desastres que deben considerarse
    5.3 Análisis de Impacto del Negocio
    5.4 Desarrollo de estrategias de mitigación
    5.5 Plan de continuidad del negocio/ Plan de recuperación
    5.6 Entrenamiento, testeo y auditoría del Plan de Continuidad del Negocio.

Bibliografía:

Susan Snedaker, Business Continuity & Disaster Recovery for IT professionals**,** ISBN: 978-1-59749-172-3.

Gonzalo Alvarez Marañón y otro, Seguridad Informática para Empresas y Particulares, ISBN: 84-481-4008-7

C. Alberts y A. Dorofee, Managing Information Security Risks, ISBN: 0-321-11886-3

Asignatura nº 10: **Seguridad en Aplicaciones**

Responsable de la asignatura (docente): Dr. Ing. Gustavo Betarte
Instituto: Computación
Departamento: Arancel: $ 9.000
Nº de Créditos: 5 Cupos: Máximo 35 personas
Horas Presenciales: 39

Objetivos:
El objetivo de este curso es introducir a los estudiantes en los principales conceptos y metodologías asociadas a la seguridad en el desarrollo de aplicaciones. Conocer los pilares fundamentales del enfoque en seguridad a la hora de proyectos de desarrollo de aplicaciones. Comprender y aplicar la gestión del riesgo en los proyectos de desarrollo, enfocados en la seguridad del producto, y la consistencia del proceso.

Conocimientos previos exigidos: Ninguno

Metodología de enseñanza:

- Horas clase (teórico): 20
- Horas clase (práctico):
- Horas clase (laboratorio): 8
- Horas consulta: 8
- Horas evaluación: 3
    - Subtotal horas presenciales: 39
- Horas estudio: 36
- Horas resolución ejercicios/prácticos:
- Horas proyecto final/monografía:
    - Total de horas de dedicación del estudiante: 75

Forma de evaluación

El curso se evaluará a partir de:

- **los laboratorios**
- **un examen final de 2 hs.**

Temario:

1. Introducción.
   1.1 Presentación, revisión de conceptos.
   1.2 Un framework para la gestión de riesgos

2. Siete hitos para la seguridad en el software
   2.1 Code review
   2.2 Análisis de riesgos en la arquitectura
   2.3 Tests de penetración
   2.4 Test de seguridad basado en los riesgos
   2.5 Casos de abuso
   2.6 Requerimientos de seguridad
   2.7 Operaciones de seguridad
   2.8 Análisis externo

3. Taxonomía de errores de codificación
   3.1 Validación de la entrada y codificación
   3.2 Abusos de API
   3.3 Funcionalidad de seguridad
   3.4 Tiempo y estado
   3.5 Manejo de errores
   3.6 Calidad del código
   3.7 Encapsulación, Entorno

4. Aplicaciones Web
   4.1 Autenticación/autorización
   4.2 Manejo de sesiones
   4.3 OWASP Top Ten, mapeo en la taxonomía

Bibliografía:

Gary McGraw, Addison-Wesly Software Security Series, Software Security: Building Security In, ISBN: 0-321-35670-5.

Open Web Application Security Project, OWASP, http://www.owasp.org

7. INFORMACIONES COMPLEMENTARIAS

Antecedentes del Programa

Año de comienzo de actividades: Se prevé comenzar en 2012

No hay antecedentes directos respecto a este Diploma ya que es nuevo.
Sin embargo, varios de los cursos han sido dictados en el marco del Diploma de Especialización Estudios Avanzados en Computación.

Otras informaciones pertinentes:

La Sub Comisión Académica de Posgrado de Informática (SCAPA-Informática) supervisará las actividades ligadas al desarrollo del Diploma de Especialización en Seguridad Informática sin perjuicio de las competencias que correspondan a la Comisión Académica de Posgrado (CAP) y al Consejo de la Facultad de Ingeniería.
La SCAPA-Informática nombrará para cada estudiante un Director de Estudios, responsable de la organización de las actividades y de la orientación del mismo.

8. SUB-COMISIÓN ACADÉMICA DEL ÁREA

Integrantes:

Dra. Dina Wonsever

Dra Adriana Marotta

Dr. Alberto Pardo

MSc. Juan José Cabezas

Firmas:

Lugar y fecha:

9. APROBACIONES PARTICULARES

Fecha de aprobación Comisión/es Instituto/s del Área (o sector equivalente) : ***(Nº de expediente y anexar resolución)***
Fecha de aprobación Consejo de Facultad de Ingeniería ***(Nº de expediente y anexar resolución)***
Homologación Comisión Académica Posgrado UdelaR ***(Nº de expediente y anexar resolución)***
Aprobación por el Consejo Directivo Central ***(Nº de expediente y anexar resolución)***

10. ANEXOS

Se adjuntan el cv, en formato cvuy en su mayoría, de los docentes participantes del programa.