SAGRADO
Universidad del Sagrado Corazón

PRONTUARIO

TÍTULO: Seguridad y rendimiento de sistemas

CODIFICACIÓN: CCO 341

PRERREQUISITO: Sistemas operativos (CCO 340)

CRÉDITOS: 3 créditos | 24 horas de reunión presencial | 21 horas en línea | 1 semestre

DESCRIPCIÓN

Discusión de diversos aspectos de la implantación de sistemas operativos enfatizando protección de recursos, seguridad y rendimiento. Se enfatizan ejemplos escogidos entre sistemas implantados en máquinas disponibles comercialmente. Se requiere un proyecto de programación y un proyecto de investigación. Este curso es una electiva para estudiantes del Programa de Ciencias de Cómputos. Curso dictado parcialmente en línea.

JUSTIFICACIÓN

En el área de las computadoras la tendencia actual es a distribuir el trabajo y/o datos entre varias computadoras que se conectan e intercomunican. El profesional en el área de ciencias de cómputos debe conocer las características y los objetivos de los diferentes sistemas operativos, así como los mecanismos de seguridad y evaluación asociados a éstos. Es importante también el que conozcan varias familias de sistemas operativos disponibles para hacer uso de las técnicas asociadas con su implantación en el desempeño de sus labores.

COMPETENCIAS

El curso desarrolla en el o la estudiante las siguientes competencias:

- Cuestionamiento crítico
- Emprendimiento e innovación
- Investigación y exploración
- Comunicación
- Sentido ético y justicia social

OBJETIVOS

1. Al finalizar el curso el o la estudiante será capaz de:

2. Explicar los mecanismos de seguridad de un sistema.
3. Explicar los mecanismos de medición de rendimiento de un sistema.
4. Analizar comparativamente diferentes sistemas operativos.

5. Analizar críticamente los puntos vulnerables de un sistema y hacer recomendaciones para hacerlo más seguro.

6. Desarrollar destrezas de trabajo en equipo.

7. Manejar de forma adecuada y responsable la tecnología, demostrando sentido de ética en su desempeño profesional y personal.

8. Desarrollar destrezas de autoaprendizaje.

9. Expresar sus ideas de forma clara y coherente en forma oral y escrita, especialmente en la producción de documentación de sistemas.

10. Utilizar múltiples fuentes de información integradamente en el desarrollo de una investigación sobre aspectos de seguridad de un sistema operativo disponible comercialmente.

11. Integrar la teoría y la práctica a través de proyectos de investigación y de programación.

CONTENIDO

I. Seguridad
   A. Requisitos de seguridad
   B. Mecanismos / Modos de seguridad
      1. "Password"
      2. Auditoría
      3. Seguridad externa
      4. Criptografía
      5. Ataques a sistemas
      6. Aspectos éticos
      7. Otros

II. Medidas de rendimiento, monitoreo y evaluación de sistemas operativos

   A. Medidas de rendimiento
   B. Técnicas para la evaluación de rendimiento
   C. Necesidad de monitoreo y evaluación
   D. Saturación

III. Estudio y comparación de sistemas operativos

   A. UNIX y LINUX
   B. Macintosh
   C. Windows y Windows NT
   D. Otros

METODOLOGÍA

Se recomiendan las siguientes estrategias de la metodología de aprendizaje activo:

Conferencias
Análisis crítico y discusión de lecturas del libro de texto y de otras fuentes
Proyectos de programación
Proyecto de investigación
Presentación oral y con recursos multimedios (presentación electrónica)
Uso de sistema de educación a distancia para acceder al componente en línea del curso
Uso de recursos disponibles en la Internet

RECURSOS:

Acceso a la Internet y al World Wide Web.

EVALUACIÓN

Exámenes parciales	40%
Programas.	30%
Proyecto final	30%
Total	100%

AVALÚO DEL APRENDIZAJE

Se aplica la rúbrica de avalúo institucional a la actividad central del curso.

BIBLIOGRAFÍA

TEXTO

Deitel, Harvey M., Deitel, Paul J. and Choffnes, David R. Operating Systems 3era edición. Upper Saddle River: Prentice Hall, 2004.

REFERENCIAS:

Bace, Rebecca Gurley. Intrusion Detection. Indianapolis: Macmillan, 2000.

Cohen, Frederick B. A Short Course on Computer Viruses. John Wiley and Sons, 1994.

Feiler, Jesse. Macintosh OS X The Complete Reference. Berkeley: Osborne/McGraw-Hill, 2001.

Deitel, Harvey and Deitel, Paul. C How to Program 5ta edición.Upper Saddle River: Prentice Hall, 2006.

Ivens, Kathy and Gardinier, Kenton. Windows 2000 The Complete Reference. Berkeley: Osborne/McGraw-Hill, 2000.

McInerney, Michael. Windows NT Security. Upper Saddle River: Prentice-Hall, 2000.

Miller, David Donald. Open VMS Operating Systems Concepts. Digital Press, 1997.

Moritsogu, Steve. Practical UNIX. Indianapolis: Que, 2000.

Musa, John D. et al. Software Reliability Measurement, Prediction, Application 2da edición. Boston: MacGraw-Hill, 2004.

Nebett, Gary. Windows NT/2000 Native API Reference. Indianapolis: New Riders Publishing, 2000.

Reinstein, Robert, et al. Windows NT Troubleshooting and Configuration. Indianapolis: Sams Publishing, 1997.

Russell, Deborah and Gangemi, G.T. Computer Security Basics. Sebastopol: O'Reilly, 1991.

Rutstein, Charles B. Windows NT Security. Boston: MacGraw-Hill, 1997.

Sethi, Joginder. Open VMS Performance Management. Digital Press, 2000.

Schetina, Erik, Green, Ken and Carlson, Jacob. Internet Site Security. Boston: Addison Wesley, 2002.

Silberschatz, Avi, et al. Operating Systems Concepts 7ma edición. Hoboken: Wiley, 2004.

Singhal, Mukesh and Shivaratri, Niranjan G. Advanced Concepts in Operating Systems. Boston: MacGraw-Hill, 1994.

Stallings, William. Operating Systems. 5ta edición. Upper Saddle River: Prentice-Hall, 2004.

Xie, Min, Poh, Kim-Leng and Dai, Yuan Shun. Computing Systems Reliability: Models and Analisys. Springer, 2004.

DIRECCIONES ELECTRÓNICAS

http://williamstallings.com
http://www.sigops.org/
http://www.microsoft.com
http://www.sun.com
http://webster.cs.ucr.edu/
http://www.ant.org.ar/cursos/curso_intro/sistop.html
http://www.computerhope.com/os.htm#01
http://www.personal.kent.edu/~rmuhamma/OpSystems/os.html
http://www.linux.org/
http://www.nondot.org/sabre/os/articles
http://www.reliasoft.com/
http://www.weibull.com/systemrelwebcontents.htm
http://src.alionscience.com/
http://reliability.sandia.gov/
http://www.cert.org/homeusers/HomeComputerSecurity/
http://www.jmu.edu/computing/security/
http://csrc.nist.gov/

Puede encontrar más recursos de información relacionados a los temas del curso en la página de la biblioteca http://biblioteca.sagrado.edu/

Las bases de datos electrónicas a las cuales la Biblioteca Madre María Teresa Guevara está suscrita directamente y a través del Consorcio COBIMET, incluyen libros, documentos, artículos de revistas y periódicos y otros recursos de información relacionados con los temas del curso. Al utilizarlas siga los siguientes pasos:

Para **acceder desde cualquier lugar en la Universidad**

- escriba la dirección **http://biblioteca.sagrado.edu/,**
- seleccione **Biblioteca Virtual** y aparecerá la página en donde podrá acceder a las bases de datos, por disciplina o en orden alfabético.

Para **acceder fuera de la Universidad**

- escriba la dirección **http://biblioteca.sagrado.edu/,**
- seleccione **Biblioteca Virtual** y aparecerá la página en donde podrá acceder a las bases de datos, por disciplina o en orden alfabético.
- escriba el nombre del usuario y la contraseña

El nombre de usuario y la contraseña, los solicita personalmente en la Biblioteca.

ACOMODO RAZONABLE

Para obtener información detallada del proceso y la documentación requerida, debe visitar la oficina correspondiente. Para garantizar igualdad de condiciones, en cumplimiento de la Ley ADA (1990) y el Acta de Rehabilitación (1973), según enmendada, todo estudiante que necesite servicios de acomodo razonable o asistencia especial deberá completar el proceso establecido por la Vicepresidencia de Asuntos Académicos.

INTEGRIDAD ACADÉMICA

Esta política aplica a todo estudiante matriculado en la Universidad del Sagrado Corazón para tomar cursos con o sin crédito académico. Una falta de integridad académica es todo acto u omisión que no demuestre la honestidad, transparencia y responsabilidad que debe caracterizar toda actividad académica. Todo estudiante que falte a la política de honradez, fraude y plagio se expone a las siguientes sanciones: recibirá nota de cero en la evaluación y/o repetición del trabajo en el seminario, nota de F(*) en el seminario: suspensión o expulsión según se establece en el documento de Política de Integridad Académica con fecha de efectividad de noviembre 2022.

CURSOS DE INVESTIGACIÓN

“Este curso puede requerir que los estudiantes practiquen tareas relacionadas al proceso de investigación, tales como: toma de consentimiento o asentimiento informado, administración de instrumentos, realización de entrevistas, observaciones o grupos focales, entre otros. Estas tareas son parte de un ejercicio académico y no se utilizará la información recopilada para compartirla con terceros o divulgar en otros escenarios que no sean el salón de clases junto al profesor que enseña el curso. Todo estudiante que vaya a interactuar con sujetos humanos como parte de su práctica en investigación tiene que estar certificado en ética con sujetos humanos en la investigación por el *Collaborative Institutional Training Iniciative* (*CITI Program*), al igual que su profesor”