Seguridad en el Ciclo de Desarrollo de Software

Guía de asignatura

Última actualización: julio de 2020

1. Información general

Nombre de la asignatura	Seguridad en el Ciclo de Desarrollo de Software
Código	11310061
Tipo de asignatura	Electiva
Número de créditos	2
Tipo de crédito	1A+1B
Horas de trabajo semanal con acompañamiento directo del profesor	64
Horas semanales de trabajo independiente del estudiante	32
Prerrequisitos	Bases de datos
Correquisitos	Ninguno
Horario	Lunes y Miércoles 16:00 a 18:00
Líder de área	Daniel Díaz Correo: danielo.diaz@urosario.edu.co
Salón	Salón virtual. Link en e-aulas o aquí: https://urosario.zoom.us/j/2844285888

2. Información del profesor y monitor

Nombre del profesor	**Martín Bedoya**
Perfil profesional	Ingeniero de sistemas experto en seguridad ofensiva, pruebas de penetración, ingeniería social, Ethical Hacking, desarrollo de exploits y análisis de Malware. Desarrollador fullstack con conocimientos sólidos en el ciclo de vida seguro de desarrollo de software. Martín es líder del área de desarrollo seguro de la unidad de ciberseguridad en Colombia de la multinacional japonesa NTT DATA.
Correo electrónico institucional	martin.bedoya@urosario.edu.co
Lugar y horario de atención	Viernes de 16:00 a 18:00 (Atención Mixta)
Página web u otros medios (opcional)	

3. Resumen y propósitos del curso

En la actualidad se presenta un sin número de incidentes informáticos debidos en gran medida a software construido sin una perspectiva de seguridad. Estos incidentes genera impactos para las organizaciones y para los usuarios de las mismas que pueden llegar a ser determinantes para la continuidad de operación de una organización. Bien sea que una organización desarrolle software o lo adquiera es fundamental conocer la forma de tener software con una superficie de ataque lo más reducida posible que evite poner en riesgo el resto de activos de información de una organización.

El propósito de este curso es formar estudiantes con capacidades técnicas que les permitan apoyar labores propias de un ciclo de desarrollo del software seguro, las cuales incluyen al menos diseño, identificación de requerimientos, implementación, pruebas, puesta a producción, mantenimiento y disposición final.

El objetivo de este curso es dar a conocer buenas prácticas en los procesos de desarrollo o adquisición de software seguro con el fin de construir aplicativos que cumplen requerimientos de seguridad (disponibilidad, confidencialidad, integridad, registro, no repudio, gobierno, autenticidad y cumplimiento).

4. Conceptos fundamentales

1. Introducción al desarrollo de software
2. Estándares y guías de construcción de software seguro
3. Arquitectura de software seguro
4. Seguridad en el desarrollo de software
5. Seguridad en el diseño
6. Manejo de información sensible
7. Seguridad en la adquisición de software
8. Disposición final del software

5. Resultados de aprendizaje esperados (RAE)

1. Conocer las buenas prácticas de seguridad en los procesos de desarrollo o adquisición de software.
2. Entender las técnicas para la implementación de software de manera segura.
3. Identificar los requerimientos de seguridad (disponibilidad, confidencialidad, integridad, registro, no repudio, gobierno, autenticidad y cumplimiento) más importantes.
4. Adquirir habilidades para el aseguramiento del ciclo de desarrollo del software.

6. Modalidad del curso

Remota: Todos sus estudiantes estarán presencialmente en la Universidad.

7. Estrategias de aprendizaje

- Análisis de casos
- Desarrollo de un proyecto de curso
- Talleres o ejercicios
- Enfoque de Aprender a Aprender: Aprendizaje activo, autorregulado, colaborativo, significativo, reflexivo

8. Actividades de evaluación

Se evalúa a través de laboratorios los cuales representan el 80% de la nota del curso, es decir 4 cortes. Adicionalmente existe un proyecto final de curso que los estudiantes comienzan desde la semana 7 aproximadamente y terminan en la última semana de clase, el cual vale el 20% de la nota total del curso. Un laboratorio puede ser intercambiado por un test u otra actividad de evaluación en función de la temática y la necesidad. Una tabla que representa lo anterior se muestra a continuación:

Corte	Actividad de evaluación	Porcentaje
Corte 1 (10%)	Taller 1 Desarrollo de Software	10 %
Corte 2 (30%)	Taller 2 Modelado de amenazas	10 %
	Taller 3 Validación de entradas	10%
	Taller 4 Gestión de sesiones	10%
Corte 3 (20%)	Taller 5 Criptografía	10 %
	Taller 6 SAST & DAST	10 %
Corte 4 (20%)	Parcial Teórico - Práctico	20 %
Corte 5 (20%)	Proyecto	20 %

9. Programación de actividades

Fecha (Sesión)	Tema	Descripción de la actividad	Trabajo independiente del estudiante	Recursos que apoyan la actividad
Sesión 1-2 30 Ene 1 Feb	Introducción – Ingeniería de software	Clase magistral, discusión, ejercicios.	Selección de MS a desarrollar	[1]
Sesión 2-3 6 Feb 8 Feb	Agilidad en el SDLC – Gestión de Requerimientos	Clase magistral, discusión, ejercicios.	Lab o Taller	[1]
Sesión 3-4 13 Feb 15 Feb	SOA – DevSecOps	Clase magistral, discusión, ejercicios.	Lab o Taller	[2]
Sesión 5-6 20 Feb 22 Feb	Integración de microservicios	Clase magistral, discusión, ejercicios.	Lab o Taller	[3] Cap 2 [4] Cap 2
Sesión 7-8 27 Feb 1 Marzo	Module 02 Security Requirements Gathering	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 3 [2] Cap 3
Sesión 9-10 6 Marzo 8 Marzo	Module 03 Secure Application Design and Architecture	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 4 [2] Cap 4
Sesión 11-12 13 Marzo 15 Marzo	Module 04: Secure Coding Practices for Input Validation	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 5 [2] Cap 5
Sesión 13-14 20 Marzo 22 Marzo	Module 05: Secure Coding Practices for Authentication and Authorization	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 6 [2] Cap 6
Sesión 15-16 27 Marzo 29 Marzo	Module 06: Secure Coding Practices for Cryptography	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 7 [2] Cap 7
Sesión 17-18 10 Abril 12 Abril	Module 07 Secure Coding Practices for Session Management	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 8 [2] Cap 8

Sesión 19-20 17 Abril 19 Abril	Module 08 Secure Coding Practices for Error Handling and Logging	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 9 [2] Cap 9
Sesión 21-22-23 24 Abril 26 Abril 1 Mayo	Module 09 Static and Dynamic Application Security Testing (SAST & DAST)	Clase magistral, discusión, ejercicios.	Lab o Taller	[1] Cap 10 [2] Cap 10
Sesión 24-25 3 Mayo 8 Mayo	Module 10 Secure Deployment and Maintenance	Clase magistral, discusión, ejercicios.	Lab o Taller	[2] Cap [3] Cap 1
Sesión 26-27 10 Mayo 15 Mayo	Mobile Application Security	Clase magistral, discusión, ejercicios.	Lab o Taller	
Sesión 28-29-30 17 Mayo 22 Mayo 24 Mayo	Ethical Hacking Avanzado sobre aplicaciones web y móviles	Clase magistral, discusión, ejercicios.	Lab o Taller	
Sesión 31-32 29 May 31 May	**Examen Final** **Sustentación proyecto**			

10. Factores de éxito para este curso

A continuación se sugieren una serie de acciones que pueden contribuir, de manera significativa, con el logro de metas y consecuentemente propiciar una experiencia exitosa en este curso:

1. Planificar y organizar el tiempo de trabajo individual que le dedicará al curso

2. Organizar el sitio y los materiales de estudios

3. Tener un grupo de estudio, procurar el apoyo de compañeros

4. Cultivar la **disciplina y la constancia**, trabajar semanalmente, no permitir que se acumulen temas ni trabajos

5. Realizar constantemente una autoevaluación, determinar si las acciones realizadas son productivas o si por el contrario se debe cambiar de estrategias

6. Asistir a las horas de consulta del profesor, participar en clase, no quedarse nunca con la duda

7. Utilizar los espacios destinados para consultas y resolución de dudas, tales como **Sala Gauss y Sala Knuth**

8. Propiciar espacios para el descanso y la higiene mental, procurar tener buenos hábitos de

sueño

9. Tener presente en todo momento valores como la honestidad y la sinceridad, al final no se trata solo de aprobar un examen, se trata de **aprender y adquirir conocimientos**. El fraude es un autoengaño.

11. Bibliografía y recursos

1. CSSLP Certification All-in-One Exam Guide, Second Edition. Wm. Arthur Conklin, Daniel Paul Shoemaker, Second edition, McGraw Hill Professional, 2019, 1260441695, 9781260441697, 464 páginas.
2. Certified Application Security Engineer (CASE) JAVA Courseware. EC-Council.

12. Bibliografía y recursos complementarios

- The Open Web Application Security Project. OWASP Testing Guide V4. 2014.

13. Acuerdos para el desarrollo del curso

- Los laboratorios deben ser entregados a tiempo. Si los laboratorios son recibidos con un retraso de hasta 1 semana, estos serán calificados sobre 4.0. Entregas con retrasos superiores a 1 semana no serán consideradas como válidas.
- No se realizará aproximación de notas al final del semestre. Las notas solo serán cambiadas con base en reclamos OPORTUNOS dentro de los límites de tiempo determinados por el Reglamento Académico.
- Si por motivos de fuerza mayor el estudiante falta a algún parcial o quiz, deberá seguir el procedimiento regular determinado por el Reglamento Académico para presentar supletorios. No habrá acuerdos informales al respecto. No se eximirá a ningún estudiante de ningún examen.
- La asignatura no tiene ningún tipo de Bono. Los exámenes parciales se realizarán de forma sincrónica a través de la plataforma zoom, durante el examen el estudiante debe tener la cámara encendida.
- Los estudiantes se deben conectar a la sesión de Zoom en el horario establecido.
- Los estudiantes podrán hacer intervenciones a través del chat o levantando la mano por medio de la herramienta disponible en zoom.
- En el momento de la intervención y según la calidad de la conexión a internet, se solicita que el estudiante active su cámara.
- Mientras no esté haciendo una intervención se solicita al estudiante desactivar su micrófono.
- Todas las sesiones serán grabadas y quedarán disponibles en el aula virtual del curso y en el repositorio institucional. Este material es de consulta y repaso y no pretende reemplazar la participación de los estudiantes en las sesiones. Sin embargo, es de gran utilidad en los casos eventuales en los que alguno de los participantes presente fallas en la conexión.

- Con el propósito de afianzar el modelo pedagógico contemplado en el Proyecto Educativo Institucional y promover un rendimiento académico óptimo, es necesario asegurar un espacio de interacción entre estudiantes y profesores que facilite la reflexión y el debate académico en torno al conocimiento. En este sentido, se valora la participación en las actividades académicas y esta se considera como un deber y un derecho del estudiante. (Artículo 48 Reglamento Académico). De no asistir a más del 80% de las clases el 15% se pierde con 0.0.
- Si el estudiante se presenta 20 minutos luego de dar inicio a alguna evaluación parcial o final, no podrá presentarla y deberá solicitar supletorio siguiendo la reglamentación institucional.

14. Respeto y no discriminación

Si tiene alguna discapacidad, sea esta visible o no, y requiere algún tipo de apoyo para estar en igualdad de condiciones con los(as) demás estudiantes, por favor informar a su profesor(a) para que puedan realizarse ajustes razonables al curso a la mayor brevedad posible. De igual forma, si no cuenta con los recursos tecnológicos requeridos para el desarrollo del curso, por favor informe de manera oportuna a la Secretaría Académica de su programa o a la Dirección de Estudiantes, de manera que se pueda atender a tiempo su requerimiento.

Recuerde que es deber de todas las personas respetar los derechos de quienes hacen parte de la comunidad Rosarista. Cualquier situación de acoso, acoso sexual, discriminación o matoneo, sea presencial o virtual, es inaceptable. Quien se sienta en alguna de estas situaciones puede denunciar su ocurrencia contactando al equipo de la Coordinación de Psicología y Calidad de Vida de la Decanatura del Medio Universitario (Teléfono o WhatsApp 322 2485756).