FCEFyN
FACULTAD DE CIENCIAS EXACTAS, FÍSICAS y NATURALES

UNC Universidad Nacional de Córdoba

Asignatura: **Seguridad Informática**

Código:10-09813	RTF	8
Semestre: Octavo	Carga Horaria	80
Bloque: Tecnologías Aplicadas (TA)	Horas de Práctica	40

Departamento: Computación

Correlativas:

- Redes de Computadoras
- Calidad de Software y Hardware-Software

Contenido Sintético:

- Historia y descripción general.
- Herramientas relevantes, estándares y / o restricciones de ingeniería.
- Seguridad e integridad de los datos.
- Vulnerabilidades: factores técnicos y humanos.
- Modelos de protección de recursos.
- Criptografía de clave pública y secreta.
- Códigos de autenticación de mensajes.
- Seguridad de red y web.
- Autenticación.
- Informática de confianza.
- Ataques de canal lateral.
- Desarrollo de software seguro.

Competencias Genéricas: (Contribuciones: A = Alto; M = Medio; B = Bajo)

- CG2: Concebir, diseñar y desarrollar proyectos de ingeniería (sistemas, componentes, productos o procesos).(B)
- CG4: Utilizar de manera efectiva las técnicas y herramientas de aplicación en ingeniería. (A)
- CG6: Desempeñarse de manera efectiva en equipos de trabajo. (M)
- CG7: Comunicarse con efectividad. (A)
- CG8: Actuar con ética, responsabilidad profesional y compromiso social, considerando el impacto económico, social y ambiental de su actividad en el contexto local y global. (A)

Aprobado por HCD: 1042-HCD-2023 RES: Fecha: 27/11/2023

Competencias Específicas: (Contribuciones: A = Alto; M = Medio; B = Bajo)

- CE10 Proyecto, Dirección y Aseguramiento de la calidad en lo referido a Seguridad Informática. (A)
- CE10.3 Asegurar la seguridad informática de los sistemas proyectados y desarrollados. (A)

Presentación

La humanidad depende cada vez más de la infraestructura informática para desarrollar prácticamente todas las facetas de la vida moderna: transporte, comunicaciones, atención médica, educación, generación y distribución de energía, solo por nombrar algunas. También se ha puesto en evidencia, con ataques desenfrenados y violaciones de esta infraestructura, que los graduados en ingeniería en computación tienen un papel cada vez más importante en el diseño e implementación de sistemas que sean seguros y puedan mantener la información privada.

La seguridad informática representa un tema transversal omnipresente en todas las demás áreas de la currícula de ingeniería en computación, incluidos los fundamentos del desarrollo de software, la gestión de datos, los sistemas operativos, las redes y las comunicaciones, la informática paralela y distribuida, los fundamentos de los sistemas y la inteligencia artificial. Como consecuencia, la seguridad informática debe incorporarse a la mentalidad filosófica de los graduados en ingeniería en computación para que todo trabajo que se espera de un graduado sea inherentemente seguro.

El área de conocimiento de la seguridad o “Security Knowledge Area” (SKA) es un nombre actualizado en el año 2013 para el área de conocimiento anteriormente conocida como “Information Assurance and Security” (IAS). Ahora bien, desde el año 2017 el SKA pasó a denominarse Ciberseguridad y se constituyó en una disciplina informática con sus propias directrices[1][2]. Los seis temas transversales de la ciberseguridad, relevantes para los graduados en ingeniería en computación son: confidencialidad, integridad, disponibilidad, riesgo, pensamiento sistémico y pensamiento del adversario. De estos temas transversales, la mentalidad o pensamiento del adversario no suele estar cubierto en las otras áreas de conocimiento y debe incluirse en esta unidad referida a seguridad informática o de ahora en más, ciberseguridad.

Los estudiantes también deben aprender conceptos de seguridad informática como autenticación, autorización y no repudio. Necesitan aprender sobre vulnerabilidades y riesgos del sistema y comprender las amenazas contra los sistemas de información. Como tal, es necesario cubrir los principios para proteger los sistemas y complementar los principios de diseño de sistemas de computación cubiertos en las asignaturas correlativas, incluidos principios como seguridad por diseño, privacidad por diseño o defensa en profundidad. Otro concepto importante es la noción de aseguramiento en términos de garantizar una certificación y de que los mecanismos implementados están a la altura de las políticas de seguridad establecidas para datos, procesos y sistemas.

[1] https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf

[2] https://www.cybok.org/

Contenidos

Unidad 1. Peligros y combatientes en la guerra contra la ciberdelincuencia
Historias de guerra. Actores maliciosos. Impacto de las amenazas. El centro de operaciones de seguridad moderno. Trayectos de formación como defensor.

Unidad 2. Criptografía
Criptografía histórica. Criptografía simétrica. Criptografía de bloque moderna. Criptografía de clave pública. Funciones de hash. Infraestructuras de clave pública.

Unidad 3. Principios de la seguridad de red
ICMP. Utilidades Ping y Traceroute. Verificación de conectividad. MAC e IP. ARP. Problemas de seguridad de ARP. Capa de transporte. Confiabilidad de la capa de transporte. Dispositivos de seguridad de red. Firewall. IDS. IPS. WAF. IPsec. Concentradores VPN.

Unidad 4. Amenazas y ataques comunes
Malware: virus, troyanos, gusanos, ransomware. Ataques comunes: reconocimiento, acceso e ingeniería social. Denegación de servicio, desbordamientos del búfer y evasión.

Unidad 5. Ataques a la red y a sus servicios
Detalles del PDU de IP. Vulnerabilidad de IP. Vulnerabilidades de TCP y UDP. Servicios IP. Vulnerabilidad de las aplicaciones de red. Tipos de datos de seguridad. Registros de terminales. Registros de red.

Unidad 6. Defensa
Estrategias de defensa de una red. Defensa en profundidad. Conceptos del control de acceso. Uso y funcionamiento de autenticación, autorización y registro. Políticas, regulaciones y estándares de seguridad.

Unidad 7. Observación de la operación de red
Monitoreo de red. Herramientas de monitoreo. Inteligencia de amenazas. Fuentes de información. Servicios de inteligencia de amenazas. Protocolos de monitoreo. Tecnologías de seguridad.

Unidad 8. Evaluación de vulnerabilidades
Vulnerabilidad, amenaza y riesgo. Perfiles de redes y servidores. Sistema de puntuación de vulnerabilidades comunes. CVSS. Registros de vulnerabilidades, debilidades y patrones de ataque. Administrador de dispositivos de seguridad.

Unidad 9. Alertas y respuesta a incidentes de seguridad
Fuentes de alertas. Evaluación de alertas. Investigación de datos de red. Manejo de evidencia y atribución de ataques. Cyber Kill Chain. Mitre Att@ck. Respuesta ante incidentes.

Unidad 10. Construcción de software seguro
Seguridad en el ciclo de desarrollo de software. Seguridad como requerimiento funcional. Casos de mal uso. Estándares de codificación segura. Análisis estático de código. Análisis de vulnerabilidades.

Metodología de enseñanza

El desarrollo general de la materia se sustenta en clases teórico-prácticas. Por ello las estrategias de enseñanza seleccionadas para llevar adelante esta propuesta son la exposición dialogada, el estudio de casos y la resolución de problemas. Cada unidad se desarrollará a partir de material bibliográfico propuesto por el equipo de cátedra más los que aporte el estudiante al buscar contenidos en internet a partir de las referencias. Se ofrecerán trabajos prácticos que orientarán el proceso de lectura y análisis del contenido como forma de evaluación y acreditación de cada unidad. Los trabajos prácticos estarán guiados por los casos de estudio presentados en cada unidad y se orientan a resolver problemas concretos aportando los contenidos teóricos necesarios para su resolución.

En ambientes de laboratorio el estudiante podrá representar casos de estudio, verificar su implementación a partir de consignas y aproximarse a la realidad de los problemas planteados.

Evaluación

En el marco de la propuesta, el equipo de cátedra ha decidido realizar el seguimiento de los alumnos con una propuesta mixta que incluye: toma de un mínimo de cuatro exámenes parciales con un recuperatorio y evaluación formativa. Los parciales buscan evidenciar los conocimientos y competencias adquiridas a través de presentación de casos prácticos (análisis, resolución de problemas, etc.) y/o respuestas a preguntas conceptuales. Constituyen en sí mismos una instancia de evaluación formativa ya que luego los estudiantes reciben realimentación de los errores cometidos.

Cada Actividad Práctica o de Laboratorio grupal propuesta (ver debajo) demanda la presentación de implementaciones funcionales e informes, donde los estudiantes explican individualmente las diferentes partes de la solución propuesta y particularmente sus detalles constructivos. Es el momento donde el estudiante pone en juego su participación en el equipo, el rol y peso de sus decisiones, su capacidad de comunicar detalles de diseño, y su correcto manejo y comprensión de las decisiones tecnológicas presentes en la solución. Para la entrega que demande cada prototipo el equipo de cátedra genera un repositorio virtual con control de versiones y los criterios de evaluación sobre esta producción del estudiante son los siguientes:

- Puntualidad en la entrega de las producciones.
- Uso de la escritura académica.
- Integración y pertinencia de conceptos.
- Claridad en la formulación de las producciones.
- Vinculación teoría práctica.

La evaluación de las competencias se realizará mediante una rúbrica construida en base a los resultados de aprendizaje propuestos.

Condiciones de aprobación

Condiciones de regularización

- Asistir al 80% de las clases.
- Aprobar todas las actividades prácticas de laboratorio con al menos el 60% o más de los criterios de evaluación expresados en la sección anterior.
- Alcanzar el criterio de aceptación mínimo para los resultados de aprendizaje propuestos.
- Aprobar al menos tres parciales, Incluidos los recuperatorios que correspondan según el régimen de estudiantes, con el 60% o más de los contenidos evaluados.

Condiciones de aprobación por promoción (no requiere examen final)

- Cumplir con todas las condiciones de regularización.
- Aprobar cada uno de los cuatro parciales propuestos, Incluidos los recuperatorios que correspondan según el régimen de estudiantes, con el 60% o más de los contenidos evaluados.

Condiciones de aprobación por examen final

- Todas las condiciones de regularización expuestas anteriormente.
- Aprobación de un examen final con el 60% o más de los contenidos evaluados.

Para la nota final se promedian las notas obtenidas en cada una de las actividades prácticas y de laboratorio, y el resultado se promedia con las notas de los parciales.

Actividades prácticas y de laboratorio

Se propone la realización de 6 (seis) actividades donde se pongan en práctica los conocimientos adquiridos en la asignatura y se desarrollen las competencias esperadas. Estos trabajos se realizan en grupos lo que permitirá que desarrollen competencias de trabajo en equipo y coordinación de tareas.

APL1 – Malware STUXNET: En esta propuesta los estudiantes profundizan sobre el contexto geopolítico que motivó la construcción del malware STUXNET, los detalles de su diseño, el objetivo perseguido y las consecuencias posteriores al ataque.

APL2 – Encriptar y desencriptar: En este trabajo los estudiantes utilizan diferentes aplicaciones para encriptar, desencriptar, producir y verificar hashes, utilizando criptografía simétrica y asimétrica. Se enfrentan con el problema de la generación de claves robustas y descubren herramientas para administrar múltiples claves robustas de forma segura y aplicable al trabajo profesional cotidiano.

APL3 – Ataque a una base de datos SQL: En esta propuesta los estudiantes analizan casos de ataques de inyección de código SQL, que permite escribir sentencias SQL en un sitio web y recibir una respuesta de la base de datos. El objetivo es visualizar los riesgos de manipulación de una base de datos. El equipo de cátedra entrega un escenario virtual para llevar adelante el ataque, concretarlo, capturar el tráfico en un archivo PCAP y luego analizar con Wireshark los detalles del ataque y elaborar conclusiones.

APL4 – Investigación de tráfico de red: En este caso los estudiantes deben investigar un malware exploit, interpretar datos HTTP y DNS para aislar al actor de amenazas y aislar terminales afectadas en un escenario virtual entregado por el equipo de cátedra.

APL5 – Monitoreo de red: En este trabajo deben preparar un ambiente virtual para monitoreo de alertas con un sistema SIEM (Security Information and Event Management). Se entregarán diferentes escenarios recogidos en máquinas virtuales para que respondan preguntas a fin de tratar alertas de seguridad.

APL6 – Construcción de software seguro: En este laboratorio la propuesta es indagar sobre las consecuencias del tratamiento de los requerimientos de seguridad de una aplicación en términos de requerimientos funcionales. Descubrir alternativas open source para la generación de código seguro y utilizar herramientas para escaneo de vulnerabilidades de una aplicación conteniendo código seguro.

Desagregado de competencias y resultados de aprendizaje

Los resultados de aprendizaje a promover en el desarrollo de la asignatura son 26 (veintiséis) agrupados en 8 (ocho) categorías, en relación con el descriptor "**Conceptos de Seguridad Informática**" dentro del bloque de "**Tecnologías Aplicadas**".

1. Conceptos básicos de criptografía

    1.1. Describir el propósito de la criptografía y enumerar las formas en que se utiliza en las comunicaciones de datos.
    1.2. Describir los siguientes términos: cifrado, criptoanálisis, algoritmo criptográfico y criptología, y describir los dos métodos básicos (cifrados) para transformar texto sin formato en texto cifrado.
    1.3. Explicar cómo la infraestructura de clave pública admite la firma y el cifrado digitales y analizar limitaciones y vulnerabilidades.
    1.4. Discutir los peligros de inventar sus propios métodos criptográficos. Describir qué protocolos, herramientas y técnicas criptográficas son apropiados para una situación determinada.

2. Integridad y autenticación de datos

    2.1. Explicar los conceptos de autenticación, autorización, control de acceso e integridad de datos.
    2.2. Explicar las diversas técnicas de autenticación con sus fortalezas y debilidades.
    2.3. Explicar ataques posibles a contraseñas.

3. Requerimientos de seguridad y el papel que desempeñan en el diseño.

    3.1. Explicar por qué los requerimientos de seguridad son importantes.
    3.2. Identificar vectores de ataque comunes.
    3.3. Describir la importancia de escribir programas seguros y robustos.
    3.4. Describir el concepto de privacidad, incluida la información de identificación personal.

4. Problemas de implementación de software

    4.1. Diferenciar entre codificación segura y parcheo y explicar la ventaja de utilizar técnicas de codificación segura.
    4.2. Describir un desbordamiento de búfer y por qué es un posible problema de seguridad.

5. Configurar y parchear software

5.1. Analizar la necesidad de actualizar el software para corregir vulnerabilidades de seguridad.
5.2. Explicar la necesidad de probar el software después de una actualización pero antes de distribuir el parche.
5.3. Explicar la importancia de configurar correctamente el software.

6. Ética, especialmente en el desarrollo, las pruebas y la divulgación de vulnerabilidades

6.1. Explicar el concepto de que el hecho de que pueda hacerlo no significa que deba hacerlo.
6.2. Discutir las cuestiones éticas al revelar vulnerabilidades.
6.3. Analizar la ética de las pruebas exhaustivas, especialmente los casos extremos.
6.4. Identificar los efectos e impactos éticos de las decisiones de diseño.

7. Monitoreo de tráfico

7.1. Analizar cómo los sistemas de detección de intrusos contribuyen a la seguridad.
7.2. Describir los límites del software antimalware, como los programas antivirus.
7.3. Analizar los usos de sistemas de monitoreo.

8. Pruebas de sistemas

8.1. Describir qué es una prueba de penetración y por qué es valiosa.
8.2. Analizar cómo documentar una prueba que revele una vulnerabilidad.
8.3. Discutir la importancia de validar requerimientos.

A continuación, se muestra en la Tabla 1, las competencias específicas desagregadas y los resultados de aprendizaje relacionados.

Desagregación de Competencias Específicas	Resultados de Aprendizaje
CE10.3_A Proyectar y diseñar la Seguridad Informática. (A)	(1) (2) (3)
CE10.3_B Dirigir e implementar la Seguridad Informática. (A)	(4) (5) (6)
CE10.3_C Asegurar y garantizar la Seguridad Informática. (A)	(7)(8)

Tabla 1: Desagregación de competencias y resultados de aprendizaje

Las competencias genéricas CG2, CG4 y CG8 se encuentran cubiertas por los resultados de aprendizaje propuestos anteriormente.

Para las competencias CG6 y CG7 se proponen los siguientes resultados de aprendizaje:

1. Redacta informes técnicos precisos y con lenguaje claro.
2. Interpreta correctamente una consigna compleja.
3. Respeta y se desempeña adecuadamente en el rol asignado dentro de su equipo.

Bibliografía

- Chapple M., Stewart J., Gibson D., Seidl D., (ISC)2 CISSP Certified Information Systems Security Professional Official Study Guide & Practice Tests Bundle 3rd Edición. Editorial Sybex 2021. ISBN 978-1119790020.
- CyberOps Associate, 2020, Academia Cisco UNC.
- Brooks C., Grow C., Craig P.Jr., Short D., Cybersecurity Essentials 1st Edición, Editorial Sybex 2018. ISBN 978-1119362395.
- https://www.cybok.org/