UNIVERSIDAD NACIONAL DE PIURA
FACULTAD DE INGENIERÍA INDUSTRIAL
DEPARTAMENTO ACADÉMICO DE INGENIERÍA INFORMÁTICA

Syllabus

Seguridad de la Información

1. DATOS GENERALES

1. Nombre de la asignatura: Seguridad de la Información
2. Código de la asignatura: SI 5496
3. Facultad: Ingeniería Industrial
4. Escuela profesional: Ingeniería Informática
5. Nivel de estudios: Quinto
6. Ciclo de estudios: Noveno
7. Requisito: Redes
8. Número lectivas semanales: Teoría: 03, Práctica: 02
9. Número lectivas semestrales: Teoría: 48, Práctica: 32
10. Duración: Inicio: / /2024 - Termino: / /2024
11. Condición: Obligatorio
12. Plan de Estudios: 2018
13. Número de Créditos: Cuatro (04)
14. Semestre Académico: 2024-I
15. Docente: Ing. Wilfredo Cruz Yarlequé - wcruzy@unp.edu.pe

2. SUMILLA

La asignatura de Seguridad de la Información corresponde al área de Formación Especializada, siendo de carácter teórico práctico. Tiene como propósito brindar al estudiante recursos cognitivos y habilidades instrumentales que le permitan conocer los principios para planificar e implementar la Seguridad de la Información en cualquier tipo de organización y garantizar el logro de sus objetivos. Comprende las unidades temáticas de: Gestión de la Seguridad de la Información, Implementación del modelo de Seguridad de la Información, Seguridad de la Información y Tecnología, Diseño de sistemas seguros, Seguridad física y otros aspectos.

3. COMPETENCIAS GENÉRICAS

1. Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.
2. Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.
3. Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.

4. PROGRAMACIÓN ACADÉMICA

4.1. Contenido de la asignatura

UNIDAD DE APRENDIZAJE I: Fundamentos de la seguridad de la información			
Duración: 25 horas / 05 semanas			
Resultados del aprendizaje: Identifica y evalúa riesgos en materia de seguridad de la información en diferentes tipos de entidades			
Semana	Contenidos de aprendizaje	Actividades de aprendizaje	Evidencia de aprendizaje
1	Introducción. Conceptos básicos, amenazas y vulnerabilidades, activos de información, triángulo de la Confidencialidad, Integridad, Disponibilidad	Observa, reconoce, identifica posibles riesgos y vulnerabilidades	Identifica posibles riesgos y vulnerabilidades que encuentra en una entidad.
2	Criptografía: Algoritmos de cifrado, criptografía simétrica y asimétrica, firma digital, funciones hash	Conoce las bases de la criptografía, simétrica y asimétrica. Utiliza funciones hash	Hace uso de la criptografía, simétrica y asimétrica. Usa funciones hash
3	Seguridad de redes: Protocolos de seguridad, firewalls, VPNs, detección de intrusiones, análisis de tráfico de red	Conoce los fundamentos de la seguridad de redes, accesos no autorizados y análisis de tráfico	Propone la implementación del protocolos de seguridad en una entidad
4	Seguridad de aplicaciones: Vulnerabilidades web, inyección de código, XSS, CSRF, OWASP Top 10	Conoce el tipo de vulnerabilidades que podría encontrar en aplicaciones web	Propone correcciones a aplicaciones web con vulnerabilidades detectadas
5	Seguridad del sistema operativo: Hardening de sistemas, control de acceso, gestión de parches, seguridad de dispositivos	Conoce como hacer seguro un sistema operativo.	Aplica medidas de seguridad para hacer su sistema operativo más seguro

UNIDAD DE APRENDIZAJE II: Gestión de la seguridad de la información			
Duración: 20 horas / 04 semanas			
Resultados del aprendizaje: Diseña, implementa y gestiona medidas de seguridad de la información bajo las normativas al respecto			
Semana	Contenidos de aprendizaje	Actividades de aprendizaje	Evidencia de aprendizaje
6	Marco de gestión de riesgos: ISO 27001, NIST Cybersecurity Framework, identificación, análisis y tratamiento de riesgos	Conoce cómo gestionar la seguridad de la información en entidades públicas, privadas	Diseña e implementa la seguridad de la información en una entidad
7	Auditoría de seguridad: Tipos de auditorías, pruebas de penetración, análisis de vulnerabilidades, gestión de incidentes	Conoce como ejecutar una auditoría, a leer resultados de análisis de vulnerabilidades y gestión de incidentes.	Reconoce una vulnerabilidad en un sistema informático al leer informes de auditorías.
8	Legislación y normativa: Ley de Protección de Datos, GDPR, CCPA, ciberseguridad industrial. **Examen Parcial**	Conoce la legislación y normativas en materia de seguridad de la información	Identifica claramente las normativas en materia de seguridad de la información
9	Concienciación en seguridad: Formación en seguridad para usuarios, phishing, ingeniería social, mejores prácticas	Conoce como implementar un plan de formación en seguridad para usuarios, conceptos como phishing, ingeniería social, mejores prácticas	Implementa un plan de formación en seguridad para usuarios, con conceptos como phishing, ingeniería social, mejores prácticas

UNIDAD DE APRENDIZAJE III: Tecnologías de seguridad			
Duración: 35 horas / 07 semanas			
Resultados del aprendizaje: Capacidad para implementar y gestionar soluciones de seguridad basadas en sistemas de prevención de intrusiones, análisis de vulnerabilidades haciendo uso de antivirus, anti-malware, gestión de parches			
Semana	Contenidos de aprendizaje	Actividades de aprendizaje	Evidencia de aprendizaje
10	Firewalls y sistemas de detección de intrusiones (IDS/IPS): Funciones, configuración, gestión	Conoce de seguridad perimetral, sistemas de detección de intrusos	Elabora un plan de seguridad perimetral y de detección de intrusos
11	Sistemas de prevención de intrusiones (IPS): Tipos de IPS, prevención de ataques	Conoce como prevenir la intrusión de externos a la institución.	Implementa una solución para prevenir la presencia de intrusos
12 13	Antivirus y antimalware: Protección contra malware, análisis de comportamiento, sandboxing	Conoce la tecnología usada por herramientas anti virus, malware, etc	Implementa cuarentenas para archivos infectados
14 15	Herramientas de análisis de vulnerabilidades: Escáneres de vulnerabilidades, gestión de parches	Conoce herramientas de análisis de vulnerabilidades y gestión de parches para los sistemas informáticos	Gestiona el manejo de herramientas de análisis de vulnerabilidades y actualizaciones de sistemas informáticos
16	**Examen final**		

4.2. Actitudes

Las actitudes que se trabajarán en el desarrollo de la asignatura son:

- Creatividad en la propuesta de soluciones para la empresa o entidad
- Dominio de habilidades cognitivas
- Actitud colaborativa y trabajo en equipo
- Calidad en la producción de soluciones a problemas
- Iniciativa para encontrar soluciones a problemas detectados
- Liderazgo para conducir al equipo a obtener resultados de calidad.

5. ESTRATEGIAS METODOLÓGICAS

- El proceso educativo de la UNP requiere para su cumplimiento de estrategias metodológicas activas, globales e integrales que permitan alcanzar logros y resultados pertinentes al desarrollo de competencias (Modelo Educativo UNP, 2015)
- El desarrollo de las sesiones de enseñanza-aprendizaje se realizan mediante:
    - Conferencia o clase magistral
    - Seminario-talleres
    - Dinámicas grupales
    - Proyectos
    - Investigación formativa
    - Estudios de casos, ABP, etc.

6. MATERIALES EDUCATIVOS Y RECURSOS DIDÁCTICOS

- Seminarios en el aula con participación de los estudiantes
- Materiales educativos: Guías de laboratorio, notas técnicas, ppt, etc.
- Recursos didácticos: PC con video y audio o laptop
- Plataforma Google Meet para reuniones de asesoría académica
- Plataforma Google Classroom para subir y consultar material, desarrollo de tareas, así como la retroalimentación.

7. ACTIVIDAD DE INVESTIGACIÓN FORMATIVA

Elaboración de un informe académico elaborado por grupos de tres estudiantes que cubra el tema:

Problema:	El uso frecuente de aplicaciones informáticas ha devenido en una cultura de uso masivo y espontáneo de datos personales, sin el correcto uso de los mecanismos de protección
Tema:	Seguridad en sistemas de información que usan datos sensibles del usuario
Título de la investigación:	Parámetros mínimos de seguridad de la información aplicados a datos personales en aplicaciones informáticas de uso abierto.

8. EVALUACIÓN DEL APRENDIZAJE

8.1. INSTRUMENTOS DE EVALUACIÓN

La evaluación constituye un proceso integral, continúo y sistémico que abarca el progreso académico del estudiante. Para medir dicho avance y el logro de las competencias y capacidades diseñadas para esta asignatura, se aplicarán Prácticas Calificadas en un número de tres (03), Trabajos Encargados a ser desarrollado en equipos de tres estudiantes, que serán dos (02), un Examen Parcial a mitad de curso, y un Examen Final al término del mismo.

El sistema de evaluación de esta asignatura es de carácter cualitativo y cuantitativo.

Tipo de evaluación	Criterios a evaluar	Instrumento	Peso ponderado	Semana aplicación
Práctica Calificada	Dominio cognitivo de conceptos y su aplicación para la solución de problemas y casos de estudio, de acuerdo a las competencias de las unidades académicas	Cuestionario	30 %	5a, 11a, 15a
Trabajo Encargado	Dominio cognitivo de los conceptos, su aplicación y trabaja en equipo para la solución de casos de estudio.	Informes	25 %	7a, 14a
Examen Parcial	Aplica los conceptos y procedimientos a la resolución de problemas y casos.	Cuestionario	20 %	8a
Examen Final	Aplica los conceptos y procedimientos a la resolución de problemas y casos.	Cuestionario	20 %	16a

La nota promedio (NP) de la asignatura será calculada de la siguiente manera:

$$NP = PPC * 0.30 + PTE * 0.25 + EP * 0.20 + EF * 0.25$$

Donde:

- PPC: Promedio de prácticas calificadas
- PTE: Promedio de trabajos encargados

- EP: Examen Parcial
- EF: Examen Final

Además se considerará lo estipulado en el Reglamento Académico de la UNP

8.2. REQUISITOS DE APROBACIÓN DE ASIGNATURA

- Los requisitos para la aprobación de la asignatura se encuentran estipulados en el Reglamento Académico de la UNP y demás normas complementarias.
- El sistema de calificación en la universidad Nacional de Piura, es vigesimal (0 a 20).
- La nota mínima promocional para aprobar un curso es 11 (Art. 66 del Reglamento Académico).
- La nota promocional mínima desaprobatoria para rendir un examen sustitutorio es ocho (08) (Art. 85 del Reglamento Académico).

9. ASESORÍA ACADÉMICA

- Lugar de atención: Departamento Académico de Ingeniería Informática, o Plataforma digital Classroom (cuenta institucional de la UNP)
- Horario: miércoles de 4:00 pm a 5:00 pm

10. BIBLIOGRAFÍA

- ABAD P, CAÑARTE T, et al: "*La ciberseguridad práctica aplicada a las redes, servidores y navegadores web*"; Ed. Área de Innovación y Desarrollo S.L, Alicante, España, 2019
- ACISSI: "*Seguridad Informática. Hacking Ético*"; ENI Ediciones, España, 2015
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2012). "*Metodología de análisis y gestión de riesgos de los sistemas de información versión 3.0.*" España: Ministerio de Hacienda y Administraciones Públicas
- DOMÍNGUEZ J. "*Seguridad Informática Personal y Corporativa (Primera parte)*" Ed. IEASS, Venezuela, 2015
- GREENWALD G. "*Snowden: sin un lugar para esconderse*". Barcelona: Ediciones B. 2014
- HODEGHATTA U, NAYAK U. "*The InfoSec Handbook*", Ed. Apress Media. USA 2014
- ISO International organization for standardization. (2013). "*ISO/IEC 27002:2013. Information technology – Code of Practice for Information Security Management. ISO/IEC*". Isaca. (2014). CISM Review Manual. (13° ed.). EEUU: ISACA.
- McCLURE S, SCAMBLAY J, KURTZ G "*HACKERS. Secretos y soluciones para la seguridad de redes*"; 8a ed. Ed. McGraw-Hill. 2010
- MCCARTHY M, BROWNSTEINN R, CAMPBELL S "*Seguridad digital estrategias de defensa digital para proteger la reputación y la cuota de mercado de su compañía*". Mc. Graw-Hill, España, 2002.
- McNAB, Chris "*Seguridad de redes*"; Primera edición. Ed. Anaya Multimedia, España. 2008
- MITNICK K, WOZNIAK S. "*Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*". USA: Little, Brown and Company. 2012
- ROMERO M, FIGUEROA G, et al "*Introducción a la seguridad informática y el análisis de vulnerabilidades*" Ed. Área de Innovación y Desarrollo S.L. Alicante, España, 2018
- TENENBAUM Andrew "*Redes de computadoras*"; 5a. Edición. de. Prentice Hall, 2012, México

Castilla, abril del 2024