000027

Seguridad de la Información

INSTITUTOS/S: **INSTITUTO DE TECNOLOGÍA E INGENIERÍA**

CARRERA/S: **Licenciatura en Informática**

RESPONSABLE DE LA ASIGNATURA Y EQUIPO DOCENTE:
Felipe Ortiz
Alejandro Pujol

AÑO: 2025

CRÉDITOS: 5

CARGA HORARIA DE INTERACCIÓN PEDAGÓGICA: 64

CARGA HORARIA TOTAL: 125

CÓDIGO DE LA MATERIA EN SIU:

000027

UNAHUR
UNIVERSIDAD NACIONAL DE HURLINGHAM

1. Fundamentación

La información es un recurso que, como el resto de los activos, tiene valor para las organizaciones y por consiguiente debe ser debidamente protegida de una amplia gama de amenazas (internas o externas, deliberadas o accidentales), a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos.

Con el surgimiento y la apertura mundial del internet se perdió esta idea de las redes internas como exclusivas para colaboradores de una organización. Su utilización implicó la expansión a millones de personas, la mayoría de ellas anónimas, alrededor del mundo.

Las empresas se vieron obligadas a redefinir la forma en que implementan una política de Seguridad de la información. Ya no solo hay que cuidar la infraestructura, sino además la información en sí, desde bases de datos hasta usuarios y contraseñas.

En la actualidad, para que exista una correcta seguridad de la información en las empresas, se debe contar con personal experto en tecnologías informáticas capaces, sobre todo, de predecir dichas amenazas y riesgos.

2. Propósitos y/u objetivos

- *Interiorizar a los/as alumnos/as en principios, tecnologías, metodologías y estándares empleados para asegurar y controlar la disponibilidad, integridad y confidencialidad de sistemas, equipos, redes y la información contenida o transmitida a través de estos.*

- *Dar a conocer los fundamentos de la seguridad de la información y su relación con las organizaciones y el ambiente laboral.*

3. Contenidos mínimos:

Introducción a la Seguridad de la Información. Conceptos fundamentales y objetivos. Gestión de la Seguridad de la Información. Riesgo: análisis y tratamiento. Seguridad en Redes, elementos de criptografía. Criptografía Simétrica y Asimétrica. Algoritmos de Hash.

Infraestructura de Clave Pública. Certificados digitales. Seguridad en Redes. Objetivos. Ataques, Servicios y Mecanismos de Seguridad. Seguridad en Redes Inalámbricas. Control de Acceso Lógico. Controles físicos de seguridad: seguridad en el centro de cómputos. Seguridad en las operaciones. Gestión de usuarios. Control de cambios. Métodos de Evaluación de seguridad: Auditorías, Evaluaciones funcionales, Vulnerability Assessment y Penetration Test. Gestión de Incidentes. Seguridad en Aplicaciones. Vulnerabilidades. Software malicioso. Problemática de las aplicaciones WEB. Leyes, Regulaciones y Estándares. Marcos legales nacional e internacional. Privacidad, Integridad y seguridad en sistemas de información.

4. Carga horaria

Créditos	*Interacción pedagógica*		*Trabajo Autónomo*	*Total*
5	*Teoría: 32*	*Práctica: 32*	*61*	*125*

4.1. Trabajo autónomo de la/el estudiante

Actividad	*Carga horaria*
Desarrollo del trabajo práctico integrador	*31*
Investigar herramientas	*30*

5. Programa analítico

UNIDAD 1: *Introducción a la seguridad de la información.*

Introducción a la Seguridad de la Información. Confidencialidad, Integridad y Disponibilidad. Identificación, Autenticación, Autorización y Accountability. Definición de Activo de información, Vulnerabilidad, Amenazas y Riesgos.

UNIDAD 2: *Sistemas de Gestión de la Seguridad de la Información (SGSI).*

Introducción a los Sistemas de Gestión. Modelo PDCA. Enfoque Top Down Vs. Enfoque Bottom Up. Familia ISO/IEC 27.00X. Clasificación de la Información. Análisis de Riesgos como base de los SGSI.

UNIDAD 3: *Seguridad en Redes.*

Objetivos. Modelo OSI. Ataques, Servicios y Mecanismos de Seguridad. Modelo TCP/IP. Controles y dispositivos de seguridad. Seguridad en el perímetro. Firewalls y proxies. Redes Virtuales (VLANs). Redes Privadas Virtuales (VPNs). IPSec. Seguridad en redes inalámbricas. Seguridad en redes Wifi.

UNIDAD 4: *Unidad 4: Control de acceso físico y lógico.*

Tipos de amenazas. Selección de la ubicación del datacenter. Protección en capas. Seguridad perimetral. Control de acceso lógico. Metodologías de control de acceso. Identificación, autenticación y autorización. Tipos de factores de autenticación. Gestión de identidades. SSO.

UNIDAD 5: *Detección y análisis de vulnerabilidades.*

Métodos de Evaluación de Seguridad. Tipos de análisis de vulnerabilidades. Aspectos legales. CVSS (common vulnerability scoring system). Escaneo de vulnerabilidades. Vulnerability Assessment y Test de Intrusiones. Tipos de hackers. Fases del hacking ético. Gestión del hacking ético.

UNIDAD 6*: Legislación de la Seguridad de la Información.*

Marco normativo. Leyes, regulaciones y estándares en materia de seguridad de la información. Marcos legales nacional e internacional.

UNIDAD 7*: Auditoría y análisis forense.*

Clasificación de los riesgos de auditoría. Procesos de auditoría. Tipo de auditoría. Protección de datos personales. Introducción al análisis forense. Puntos de pericia. Manejo de la evidencia. Cadena de custodia. Procedimiento forense.

UNIDAD 8: *Criptografía.*

Requerimientos de la criptografía. Tipos de cifrados. Hitos de la criptografía. Cifrado Simétrico. Algoritmos estándares. Problemas de los algoritmos simétricos o de clave pública/privada. Cifrado Asimétrico. Funciones unidireccionales con trampa y problemas matemáticos. Criptografía híbrida. Introducción a PKI. Componentes. PGP. Autoridades de certificación internacionales. Firma electrónica y firma digital.

UNIDAD 9*: Seguridad en Aplicaciones.*

Introducción a la seguridad en el software. Problemática del desarrollo de aplicaciones. Ciclo de vida del desarrollo del software. Software malicioso: Troyanos, backdoors, virus y gusanos. Otros tipos de malware. Niveles de maduración. Problemática de las aplicaciones WEB. OWASP Top 10.

6. Ejes y enunciados Multidimensionales y transversales

Eje	*Nivel de logro de Aprendizaje*	*Acciones de enseñanza*
C1. Identificación, formulación y resolución de problemas de informática	*Alto*	*Clase expositiva dialogada.*
C2. Concepción, diseño y desarrollo de proyectos de informática	*Alto*	*Ilustraciones.*
C3. Gestión, planificación, ejecución y control de proyectos de informática	*Alto*	*Ilustraciones.*
C4. Utilización de técnicas y herramientas de aplicación en la informática	*Alto*	*Ilustraciones.*
C5. Generación de desarrollos tecnológicos y/o innovaciones tecnológicas	*Alto*	*Clases prácticas.*
C6. Fundamentos para el desempeño en equipos de trabajo	*Alto*	*Clases prácticas.*
C7. Fundamentos para la comunicación efectiva	*Alto*	*Clases prácticas.*
C8. Fundamentos para la acción ética y responsable	*No aporta*	*N/A*
C9. Fundamentos para evaluar y actuar en relación con el impacto	*No aporta*	*N/A*

social de su actividad en el contexto global y local		
C10.Fundamentos para el aprendizaje continuo	*No aporta*	*N/A*
C11.Fundamentos para la acción emprendedora	*Alto*	*Resolución de ejercicios y problemas.*

7. Bibliografía y recursos

7.1 Bibliografía obligatoria

Mike Chapple ,James Michae l Stewart ,Darril Gibson. (2024) "ISC2 CISSP Certified Information Systems Security Professional Official Study Guide (Sybex Study Guide)" 10th Edición.

Alexander, A.G. (2007). "Diseño de un Sistema de Gestión de Seguridad de Información". Óptica ISO 27001:2005. Bogotá; Colombia: Alfaomega.

Stallings, W. (2004). "Fundamentos de seguridad en Redes. Aplicaciones y estándares". 2da Edición Madrid: Pearson.

7.2 Bibliografía optativa

Albakri, Sameer-Hasan; Shanmugam, Bharanidharan; Samy, Ganthan-Narayana; Idris, Norbik-Bashah; Ahmed, Azuan (2014). "Security risk assessment framework for cloud computing environments". Security and communication networks, v. 7, n. 11, pp. 2114-2124. https://doi.org/10.1002/sec.923

Mesquida, Antoni-Lluís; Mas, Antonia (2015). "Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 security extension". Computers and security, v. 48, pp. 19-34. https://goo.gl/BZt89n https://doi.org/10.1016/j.cose.2014.09.003

7.3 Recursos

Como recursos al dictado de la materia se utilizarán diapositivas, campus virtual, guías de trabajos prácticos y guías de desafíos. Además, se ilustrará con ejemplos de la aplicación de las soluciones en la industria.

En el campus virtual se propondrá material educativo y bibliografía, así como también el programa y cronograma de la asignatura y las guías de Trabajos Prácticos y ejercicios.

Dentro de las aplicaciones que se utilizan para el desarrollo de las actividades prácticas se encuentran las siguientes:
OWASP top 10 - https://owasp.org/www-project-top-ten/
Kali Linux - https://www.kali.org/

8. Metodología de enseñanza

8.1 Modalidades u opciones pedagógicas

Durante la cursada se combinarán distintas modalidades: clases teóricas desarrolladas en base a presentaciones de los contenidos base, clases demostrativas donde se muestra el uso de aplicaciones y software especializado.

Trabajos de laboratorio en los cuales se desarrollan actividades técnicas con consigna.

Las actividades prácticas se realizan sobre la base de "desafíos".

8.2 Formación Práctica

Se realiza un trabajo práctico integrador en el cual se desarrolla un plan de seguridad de la información a fin de implementarlo en una Pyme, para el armado de este, los alumnos deben investigar sobre las herramientas más utilizadas en la industria tanto open source como licenciadas.

Además, se realiza un trabajo práctico de hacking utilizando las herramientas que se mencionan en la sección recursos. Durante esta actividad, los alumnos aprenden a detectar y resolver vulnerabilidades.

9. Evaluación y régimen de aprobación

9.1 Modalidad de evaluación

Se organiza a partir de 2 evaluaciones que permitan determinar el grado de aprendizaje del alumno/a.

El sistema normal de evaluación consistirá en 2 (dos) exámenes parciales con recuperatorios, según el cronograma previsto, de la totalidad de la materia descripta en el programa. Los mismos se realizarán en las fechas que, a tal efecto, se establezcan en el cronograma. El primer parcial es teórico-práctico e individual y el segundo parcial es un trabajo integrador desarrollado por los alumnos de manera grupal y se debe defender por todos los integrantes del grupo de manera oral. Además, se considera como parte de la evaluación de la cursada el desarrollo de la guía de trabajos prácticos que los alumnos deben presentar de manera grupal al final de la cursada de la asignatura.
El alumno deberá poseer una asistencia no inferior al 75% en las clases presenciales.

La materia podrá aprobarse mediante: régimen de promoción directa, exámenes finales regulares y exámenes libres.

9.2 Aprobación de la cursada

Para aprobar la cursada y obtener la condición de regular, el régimen académico establece que debe obtenerse una nota no inferior a cuatro (4) puntos. Todas las instancias evaluativas deberán tener una instancia de recuperatorio. Podrán acceder a la administración de esta modalidad solo aquellos y aquellas estudiantes que hayan obtenido una nota inferior o igual a 6 (seis) puntos en el examen parcial.

Siempre que se realice una evaluación de carácter recuperatorio, la calificación que los/as estudiantes obtengan reemplazará la calificación obtenida en el examen que se ha recuperado y será la considerada definitiva a los efectos de la aprobación.

9.3 Acreditación de la materia

La materia puede aprobarse por promoción, evaluación integradora, examen final o libre.

***Promoción directa:** tal como lo establece el art°17 del Régimen Académico, para acceder a esta modalidad, el/la estudiante deberá aprobar la cursada de la materia con una nota no inferior a siete (7) puntos, no obteniendo en ninguna de las instancias de evaluación parcial menos de seis (6) puntos, sean evaluaciones parciales o recuperatorios. El*

promedio estricto resultante deberá ser una nota igual o superior a siete (7) sin mediar ningún redondeo.

Evaluación integradora: *tal como lo establece el art°18 del Régimen Académico, podrán acceder a esta evaluación aquellos estudiantes que hayan aprobado lo cursado con una nota de entre cuatro (4) y seis (6) puntos.*
La evaluación integradora tendrá lugar por única vez en el primer llamado a exámenes finales posterior al término de la cursada. Deberá tener lugar en el mismo día y horario de la cursada y será administrada, preferentemente, por el/la docente a cargo de la comisión.
Se aprobará tal instancia con una nota igual o superior a cuatro (4) puntos, significando la aprobación de la materia.
La nota obtenida se promediará con la nota de la cursada.

Examen final*: Instancia destinada a quienes opten por no rendir la evaluación integradora o hayan regularizado la materia en cuatrimestres anteriores. Se evalúa la totalidad de los contenidos del programa de la materia y se aprueba con una calificación igual o superior a cuatro (4) puntos. Esta nota no se promedia con la cursada.*