INSTITUTO/S: Tecnología e Ingeniería

CARRERA/S: Licenciatura en Informática

MATERIA: Seguridad de la Información

NOMBRE DEL RESPONSABLE DE LA ASIGNATURA: Mg. Felipe David Ortiz

EQUIPO DOCENTE: ------

CUATRIMESTRE: 1°

AÑO: 3

PROGRAMA N°: 21 **(Aprob. Por Cons.Directivo fecha XX)**

Instituto/s: Instituto de Tecnología e Ingeniería

Carrera/s: Licenciatura en Informática

Nombre de la materia: Seguridad de la Información

Responsable de la asignatura y equipo docente: Mg. Felipe David Ortiz

Cuatrimestre y año: 1ro del 3er año

Carga horaria semanal: 4 hs

Programa N°: 21

Código de la materia en SIU: 771

Seguridad de la Información

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.

En este sentido, en la catedra se plantean los siguientes propósitos y objetivos:

2. Propósitos y/u objetivos

Propósitos

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

Objetivos

Que los/as alumnos/as logren:

- Aplicar los conceptos técnicos de la seguridad a través del uso de herramientas de software destinadas a tal fin.
- Vincular los conocimientos adquiridos en informática y programación, con los distintos aspectos de la seguridad informática.
- Conocer las estrategias para la identificación de los activos de información y la implementación de políticas, estándares, procedimientos y guías de acuerdo con su nivel de riesgo.

3. Programa sintético:

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. Programa analítico

4.1 Organización del contenido:

Unidad 1: Introducción

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: 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: 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.

4.2 Bibliografía y recursos obligatorios:

Stallings, W. (2002). *Cryptography and Network Security, 3rd. Ed*. Lebanon, Indiana, U.S.A.: Prentice Hall.

Stallings, W. (2004). *Fundamentos de Seguridad en Redes*, *2da. Ed*. Madrid, España: Pearson Educacion.

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

4.3 Bibliografía optativa:

Schneier, B. (1996). *Applied Cryptography*. Ed. Wiley.

Kaufman,C., Perlman,R. y Speciner,M. (2002). *Network Security, 2nd. Ed*. Prentice Hall.

Jara, H y Pacheco, F. (2009). *Hackers al Descubierto.* MP Ediciones.

Jara, H y Pacheco, F. (2012). *Ethical Hacking 2.0*. MP Ediciones.

5. Metodologías de enseñanza:

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”.

Como recursos al dictado de la materia se utilizarán diapositivas, campus virtual, guías de trabajos prácticos, PC, un “live CD” con herramientas open source y guías de desafíos.

Plan de trabajo en el campus:

El Campus Virtual es un espacio fundamental para el desarrollo de la asignatura. En el aula virtual se propondrá material educativo, apuntes de clase, bibliografía, así como también el programa y cronograma de la asignatura y las guías de Trabajos Prácticos y ejercicios.

6. Actividades de investigación y extensión (si hubiera)

7. Evaluación y régimen de aprobación

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

La calificación de cada evaluación se determinará en la escala 0 a 10, con los siguientes valores: 0, 1, 2 y 3: insuficientes; 4 y 5 regular; 6 y 7 bueno; 8 y 9 distinguido; 10 sobresaliente. La materia podrá aprobarse mediante: régimen de promoción directa, exámenes finales regulares y exámenes libres.

7.1 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.

Los alumnos y alumnas deberán poseer una asistencia no inferior al 75% en las clases bajo la modalidad híbrida, esto contempla las clases presenciales y las clases que se dictarán de manera sincrónica de manera virtual.

7.2 Aprobación 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 y aquellas estudiantes que hayan aprobado la 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 administrado, 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.

7.3 Criterios de calificación

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 y las alumnas de manera grupal y se debe defender por todos los integrantes del grupo. Además, se considera como parte de la evaluación de la cursada el desarrollo de la guía de trabajos prácticos que los alumnos y las alumnas deben presentar de manera grupal al final de la cursada de la asignatura.

8. Cronograma

CRONOGRAMA DE CLASES, PARCIALES Y RECUPERATORIOS

CLASE	FECHA	TEMAS A DESARROLLAR	PRESENTACIÓN	OBSERVACIONES	ACTIVIDADES	MODALIDAD
1	29/3	• Introducción a la Seguridad de la Información. Conceptos fundamentales y objetivos • Privacidad, Integridad y seguridad en sistemas de información. • Activos de información.	Introducción a la seguridad de la información	Presentación: Pautas de la materia. Guía de TPs. Trabajo Grupal Integrador.	Presentación de la materia y armado de grupos de trabajo integrador.	Presencial
2	5/4	• Gestión de la Seguridad de la Información (SGSI)	Gestión de la seguridad de la información		Desarrollo del TP	Virtual
3	12/4	• Seguridad en Redes.	Seguridad en redes de información			Virtual
4	19/4	• Seguridad en el uso de correo electrónico e Internet. • Seguridad en dispositivos móviles. • Copias de seguridad.	Seguridad en redes de información		Desarrollo del TP	Presencial
5	26/4	• Controles físicos de seguridad • seguridad en el centro de cómputos. • Control de Acceso Lógico. • Gestion de usuarios y contraseñas. • Biometría, SSO y doble factor de autenticación.			**Punto de Control # 1**	Virtual
6	3/5	• Objetivos, Ataques, Servicios y Mecanismos de Seguridad • Métodos de Evaluación de seguridad. Auditorías • Evaluaciones funcionales • Vulnerability Assessment • Penetration Test.			Consultas para el parcial	Presencial
7	10/5	**Examen - Primer Parcial**		Parcial - Duración: 2 hs		Virtual
8	17/5	Punto de control – Devolución de parciales		.		Presencial
9	24/5	• Vulnerabilidades.				Virtual

		Problemática de las aplicaciones WEB. Desarrollo seguro.				
10	31/5	Leyes, Regulaciones y Estándares. Marcos legales nacional e internacional.			**Punto de Control # 2**	Virtual
11	7/6	Laboratorio de hacking				Presencial
12	14/6	Gestion de Riesgos: análisis y tratamiento. Respuesta ante incidentes de seguridad en las Organizaciones.				Virtual
13	21/6	● Elementos de criptografía. ● Criptografía Simétrica y Asimétrica. ● Algoritmos de Hash. ● Infraestructura de Clave Pública. ● Certificados digitales				Presencial
14	28/6	Desarrollo del TP integrador			Revisión de correcciones del Trabajo Práctico integrador y de la Guía de Trabajos Prácticos por grupo.	Presencial
15	5/7	**Exposición del TP – Defensa oral**				Presencial
16	**12/7**	**Examen recuperatorio**			Finalización del cuatrimestre. Indicaciones para la evaluación integradora	Virtual