**INSTITUTO DE DESARROLLO ECONÓMICO E INNOVACIÓN**
Año: 2021

UNTDF
Universidad Nacional de Tierra del Fuego, Antártida e Islas del Atlántico Sur.

| | |
|---|---|
| **PROGRAMA DE LA ASIGNATURA:** Seminario de Seguridad (IF063) | **CÓDIGO:** IF063<br>**AÑO DE UBICACIÓN EN EL PLAN DE ESTUDIOS:** 5 año<br>**FECHA ULTIMA REVISIÓN DE LA ASIGNATURA:** 2021-03-01<br>**CARRERA/S:** Licenciatura en Sistemas 049/2017, |
| **CARÁCTER:** CUATRIMESTRAL (1ro)<br>**TIPO:** OBLIGATORIA<br>**NIVEL:** GRADO<br>**MODALIDAD DEL DICTADO:** PRESENCIAL (EN LÍNEA)<br>**MODALIDAD PROMOCION DIRECTA:** SI<br>**CARGA HORARIA SEMANAL:** 4 HS<br>**CARGA HORARIA TOTAL:** 60 HS | **EQUIPO DOCENTE** |

| Nombre y Apellido | Cargo | e-mail |
|---|---|---|
| Emilio Izarra | Profesor Adjunto | eizarra@untdf.edu.ar |

## 1. FUNDAMENTACION

En virtud de la pandemia de público conocimiento la modalidad de la materia será en línea combinando la comunicación en forma simétrica y asimétrica. La simetría se refiere al dictado de clases( teóricas y prácticas) mediante video llamadas, brindando una interacción estudiante-docente en vivo, emulando la presencialidad; y utilizando la herramienta de video conferencia Google Meet. En cambio, el contenido estático se refiere al contenido didáctico que se encuentra disponible siempre en la plataforma educativa virtual Moodle (moodle.untdf.edu.ar ) pudiendo el estudiante acceder con libertad de horario.

Las tecnologías de la información y la comunicación (TIC) están ya instaladas en la gestión de las organizaciones y en el uso cotidiano de los individuos, por lo que se hace necesario promover y potenciar la educación en la temática. La gestión de la seguridad de la información hoy en día es una parte fundamental de las organizaciones, con independencia de su tipo, tamaño, sector o localización geográfica. Generalmente las áreas de las organizaciones basan sus operaciones que requieren y consumen información, procesos y servicios de la infraestructura IT. Los servicios y la información que se montan bajo esta infraestructura IT deben estar debidamente protegidos para asegurar su confiabilidad, integridad y disponibilidad, pilares de la seguridad informática.

El incremento de los incidentes de seguridad que afectan la operativa y la continuidad del negocio de las organizaciones, con impactos económicos, legales y de imagen, hacen que sea necesario Gestionar la Seguridad de la Información mediante la elaboración de políticas, desarrollo en mejores prácticas de seguridad y gestión de riesgos.

En el transcurso de este seminario se pasa por los conceptos básicos sobre Seguridad informática, técnicas de hacking ético, estándares para la implementación de Sistemas de Gestión de la Seguridad de la Información (SGSI), metodologías de análisis de riesgo y sistemas criptográficos.

## 2. OBJETIVOS

## a) OBJETIVOS GENERALES

Proporcionar a los alumnos sólidos conocimientos teóricos y prácticos que feliciten la comprensión de los conceptos y los principios de diseño, usados en la construcción de sistemas de gestión de la seguridad de la información. Este conocimiento permitirá visualizar la tecnología actual y futura con una mirada crítica y racional permitiendo aplicar técnicas y herramientas vigentes tanto para la creación de soluciones como para la resolución de problemas específicos. Para ello, la materia se propone analizar los principales temas que conforman el mundo de seguridad informática y de la información, y brindaran al alumno las bases necesarias para enfrentar necesidades de conocimiento especializado o especifico.

## b) OBJETIVOS ESPECIFICOS

1. Introducir al alumno en los fundamentos de la Seguridad de la Información
2. Conocer los distintos tipos de ataques y metodologías de desarrollo
3. Brindar conocimientos sobre los distintos componentes básicos en la protección de la información, ya sean de seguridad informática como de seguridad física (Protección Física. Seguridad Patrimonial. Protección Informática. Seguridad de Redes Teleinformáticas)
4. Introducir los conceptos de criptografía y su aplicación práctica en el campo
5. Introducir los conceptos de Seguridad en Telecomunicaciones
6. Introducir los conceptos de Seguridad Física que permitan al alumno diseñar soluciones acordes a la necesidad de la empresa de proteger sus activos de información
7. Transmitir los conocimientos necesarios para la realización de un Plan de Continuidad de Negocios
8. Dar a conocer la legislación nacional e internacional en materia de delitos informáticos que permita al alumno interactuar y asesorar al área de Legales de la empresa en la que se desempeñe.
9. Generar conciencia sobre los peligros a los que están expuestos los empleados de una compañía a partid de la utilización de las técnicas de Ingeniería Social para obtener información
10. Transmitir los conocimientos básicos sobre la norma ISO/IEC 27002 y su utilidad para el desarrollo del Plan de Seguridad de la Organización.

## 3. CONDICIONES DE REGULARIDAD Y APROBACION DE LA ASIGNATURA

En virtud del aislamiento obligatorio declarado debido a la Pandemia del Covid-19, se han readecuados los contenidos de la asignatura para su dictado en línea. De acuerdo con el Anexo I de la Resolución Rec. Nº 104/2020 el cronograma se ha diagramado de la siguiente forma:

- Dictado presencial del 09/03 al 13/03
- Acompañamiento remoto del 16/03 al 10/04
- Clases en modalidad en línea del 20/04 al fin del cuatrimestre.

En este año 2020 sumamos un desafío, la readecuación del programa de la materia a partir de modificar la modalidad del dictado de clases presencial a clases en línea través de una propuesta para los estudiantes de trabajo obligatorio a través del aula virtual “Moodle” (modo asincrónico), asimismo ofreceremos espacios de consulta y acompañamiento optativos no obligatorios a través de videoconferencia Google Meet (modo sincrónico). La finalidad de este cambio se centra en evitar interrumpir la continuidad pedagógica en esta asignatura en el marco del periodo de aislamiento obligatorio debido a la Pandemia del Covid-19 por la que se encuentra atravesando el mundo entero.

En cumplimiento de la Reso. RO 350/2014 y la Disposición SA 03/2020, se ofrecen las siguientes condiciones de regularidad y aprobación.

Según la RO 350/2014: Art.31 b) Se aprueben las asignaturas sobre la base de un cubrimiento mínimo del 60% de los contenidos y competencias evaluadas.
Según la Disposición 3/2020. Art. 1 c) Las asignaturas serán aprobadas sobre la base de un cubrimiento mínimo del 60% de los contenidos y competencias evaluadas. Es importante aclarar que los docentes tendrán en cuenta el nivel de participación, la calidad de las intervenciones en los diversos foros y la responsabilidad para presentar los trabajos en tiempo y forma.
Regularidad
El cumplimiento de las condiciones de asistencia se obtiene con la realización del 60% de las actividades obligatorias propuestas por el equipo docente (que se realizan de modo asincrónico). Además, es necesario aprobar un mínimo del 60% los contenidos y competencias evaluados a lo largo del cuatrimestre. El 60% corresponde a un 4 (cuatro) de nota Resol. 350 Art. 33 d)
Aprobación de Parciales
Se entiende la evaluación en su doble vertiente formativa continua y sumativa o de síntesis.
En esos términos, se proponen una instancia de evaluación obligatoria: un parcial individual realizados a través de la plataforma Moodle al final del seminario. El parcial se aprueba alcanzando el 60% de los contenidos y competencias evaluados corresponde a un 4 (cuatro) de nota Resol. 350 Art. 33 d).
El parcial tendrá su respectivo recuperatorio con los mismos criterios de aprobación.

Condiciones de aprobación por promoción
Los alumnos que así lo deseen podrán hacer uso del régimen de promoción (sin examen final). Para aprobar la asignatura bajo este régimen el alumno deberá:

1- Aprobar los el parciales con nota equivalente a 8 o superior en su primera instancia (no se tendrán en cuenta los exámenes recuperatorios para la opción de promoción).
2- Haber entregado al 70% de los ejercicios de las guías de prácticas.

Condiciones de aprobación por examen final
Para los alumnos que cursen por régimen con examen final, una vez obtenida la cursada estarán en condiciones de rendir el examen final en algunas de las fechas establecidas en el Calendario Académico.
En el caso de estudiantes regulares, además de cumplir los requisitos de regularidad, deberán aprobar una instancia final de evaluación individual con una calificación igual o superior a 4 (cuatro) puntos, como establece el artículo 33 de la Reso. RO 350/2014
Acreditación
Esta responde a una lógica institucional, explícita en el Reglamento de Estudios de Grado y de Pos Grado de la Universidad, para certificar conocimientos alcanzados.
El criterio utilizado es que el alumno haya alcanzado los objetivos (generales y específicos) citados anteriormente. Para ello se prevén tanto exámenes (parciales y finales), entrega de ejercicios y régimen de promoción sin examen final. Se tendrá en cuenta, además de los resultados cuantitativos, el desempeño y las actitudes que el alumno ha demostrado durante los meses del cursado de la asignatura.

## 4. CONTENIDOS DE LA ASIGNATURA

UNIDAD 1: SEGURIDAD DE LA INFORMACIÓN
Introducción ITIL V3 (Gobierno IT. El ciclo de vida de los servicios IT). Introducción a Seguridad de la Información. Antecedentes. Conceptos de confidencialidad, integridad, autenticidad y disponibilidad. Marco teórico (seguridad informática, principios de seguridad de la información, enfoques de seguridad, servicios de seguridad informática).
UNIDAD 2: SEGURIDAD INFORMÁTICA
Rastreo de sistemas. Enumeración de sistemas. Sniffers. Footprinting y fingerprinting . Tipos de

ataques (ataques a sistemas operativos, ataques a nivel de aplicación, ataques a nivel de red, ataques por configuraciones erróneas o malas configuraciones, ataques de Ingeniería Social). Ataques más comunes. Escaneadores de vulnerabilidades. Denegación de Servicio. Blindaje y protección de sistemas.
UNIDAD 3: SGSI
Sistema de Gestión de la Seguridad de la Información. La Organización Internacional de Normalización (ISO). Normas ISO serie 27000. ISO/IEC 27001:2013. Estructura. Dominios de Seguridad, Clausula, Categorías y Controles ISO/IEC 27001:2013. Políticas de Seguridad de la Información.
UNIDAD 4: GESTIÓN DE RIESGOS
Metodologías existentes. Identificación de activos. Identificación de amenazas y vulnerabilidades. Cálculo del nivel de riesgo. Establecimiento de controles. Implementación de medidas de seguridad. Instalación y configuración de herramientas de seguridad.
UNIDAD 5: FIRMA DIGITAL
Firma Digital. Infraestructura de Firma Digital Argentina. Conceptos básicos. Criptografía. Estructura. Funcionamiento. Certificados digitales, vigencia y revocación. Nociones elementales de Criptografía Simétrica y Asimétrica. Clases de certificados. Autoridades de Certificación. Autoridades de Registro

## 5. RECURSOS NECESARIOS

- Pc
- Laboratorio Informatica

## 6. PROGRAMACIÓN SEMANAL

| Semana | Unidad / Módulo | Descripción | Bibliografía |
|---|---|---|---|
| Semana | Unidad / Módulo | Descripción | Bibliografía |
| Semana 1 | Módulo I | Introducción a la seguridad | |
| Semana 2 | Módulo I | Introducción a la seguridad | |
| Semana 3 | Módulo II | Seguridad Física | |
| Semana 4 | Módulo II | Seguridad Física | |
| Semana 5 | Módulo III | Introducción a la Criptografía y Autenticación | |
| Semana 6 | Módulo III | Introducción a la Criptografía y Autenticación | |
| Semana 7 | Módulo IV | Seguridad en Sistemas Operativos | |
| Semana 8 | Módulo IV | Seguridad en Sistemas Operativos | |
| Semana 9 | Módulo IV | Seguridad en Sistemas Operativos | |
| Semana 10 | Módulo V | Seguridad en Redes | |
| Semana 11 | Módulo V | Seguridad en Redes | |
| Semana 12 | Módulo V | Seguridad en Redes | |
| Semana 13 | Entrega de actividad | Entrega de actividad | |
| Semana 14 | Consultas | Consultas | |
| Semana 15 | Consultas | Consultas | |
| Semana 16 | Entrega de actividad y evaluación | Entrega de actividad y evaluación | |

| | | | |
|---|---|---|---|
| Semana 17 | Informe final de cátedra | Informe final de cátedra | |

## 7. BIBLIOGRAFIA DE LA ASIGNATURA

| Autor | Año | Título | Capítulo/s | Lugar de la Edición | Editor / Sitio Web |
|---|---|---|---|---|---|

Firma del docente-investigador responsable

| VISADO | | |
|---|---|---|
| **COORDINADOR DE LA CARRERA** | **DIRECTOR DEL INSTITUTO** | **SECRETARIO ACADEMICO UNTDF** |
| | | |
| Fecha : | Fecha : | |

**Este programa de estudio tiene una validez de hasta tres años o hasta que otro programa lo reemplace en ese periodo**