# Plan de estudios de la carrera Analista Técnico en Ciberseguridad


## Autor

Área de Seguridad de la Información de Agesic



## Fecha de creación

16/05/2024

## Tipo de publicación

Modelos

# Resumen

La currícula se impulsó en el marco del 10º objetivo de la Agenda Digital Uruguay 2025, en el cual se establece la meta de desarrollar y promocionar trayectorias de formación en ciberseguridad, para el desarrollo de capacidades a través de la educación formal y no formal. Además, se establece la iniciativa de mejorar la empleabilidad de las personas y disminuir la brecha de talento en ciberseguridad.

La propuesta académica impulsada por Agesic y desarrollada con la Facultad de Ingeniería (Instituto de Computación) a través de la Fundación Julio Ricaldoni, con el apoyo del Banco Interamericano de Desarrollo (BID), permite formarse o reconvertirse técnicamente en ciberseguridad a las personas interesadas que hayan culminado segundo grado de enseñanza secundaria. El plan de estudios tiene una duración de 2 años para obtener el título de “Técnico en Ciberseguridad”, con la posibilidad de cursar un tercer año de especialización con materias electivas para adquirir el título de “Analista Técnico en Ciberseguridad”.

La currícula es de acceso libre y flexible para que cualquier institución educativa de Uruguay o el mundo pueda implementarla y complementarla de acuerdo con su propuesta académica y la evolución de las necesidades del mercado. Asimismo, el enfoque de formación fue elaborado para posibilitar la continuidad en estudios de grado y posgrado.

Frente a cualquier duda podrán comunicarse con el área de Seguridad de la información de Agesic a través del correo: ciberseguridad@agesic.gub.uy

# Propuesta de plan curricular e implementación

La presente “Currícula de Ciberseguridad a Nivel Técnico” fue elaborada por un equipo docente del Instituto de Computación en el marco del acuerdo suscrito entre la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y del Conocimiento (Agesic) y la Fundación Julio Ricaldoni (FJR) de la Facultad de Ingeniería de la Universidad de la República, con el fin de ser utilizada como soporte para el desarrollo de programas educativos a nivel técnico orientados a las necesidades de la industria y las capacidades actuales del país. La propiedad intelectual de la currícula corresponde exclusivamente a Agesic.

Se pone a disposición de las entidades educativas públicas y privadas la currícula con la finalidad de ser aplicada a programas educativos en el área de ciberseguridad. Podrán utilizarla y modificarla libremente, citando en todos los casos a Agesic así como el alcance de las modificaciones realizadas, no asumiendo Agesic responsabilidad alguna vinculada a dicha utilización o por eventuales modificaciones. En caso de introducirse modificaciones, deberá remitirse a Agesic las nuevas versiones a efectos de que ésta tome conocimiento.

# Introducción

Palabras claves: Plan de estudios · Ciberseguridad · Formación terciaria técnica · Implementación

Este documento fue desarrollado por Gustavo Betarte, Juan Diego Campo, y Carlos Luna del Instituto de Computación, Facultad de Ingenierĩa, Universidad de la República de Uruguay.

En esta sección se procede a caracterizar brevemente la disciplina de la ciberseguridad, motivar la importancia de generar profesionales con capacidades en este dominio y a describir los objetivos generales del trabajo que se reporta en este documento.

# La ciberseguridad como disciplina

La ciberseguridad es una disciplina basada en las Tecnologías de la Información y la Comunicación (TIC), que involucra tecnología, personas, información y procesos. Se trata de garantizar que los sistemas informáticos funcionen correctamente en presencia de adversarios. Tiene una fuerte componente interdisciplinar, que incorpora aspectos de gestión de riesgos, derecho, psicología y ética, entre otros.

Pese al crecimiento del uso de las TIC, se incrementó la cantidad de amenazas y ataques que se producen a las aplicaciones y los recursos informáticos. Es en este contexto que la información se convierte en un recurso crítico al que hay que proteger. La ciberseguridad se vuelve imprescindible como forma de garantizar la integridad, disponibilidad y confidencialidad de la información. Las organizaciones deben estar preparadas para proteger sus activos de información. Esto implica conocer y aplicar de forma adecuada los conceptos, metodologías, estándares y herramientas propias de la disciplina,

Además, las nuevas normativas existentes en Uruguay y en el mundo, para lograr el objetivo de seguridad, generó un demanda de profesionales especializados en seguridad informática que, tanto a nivel mundial como en Uruguay, está lejos de ser satisfecha. Para satisfacer esta demanda se requiere de recursos humanos debidamente capacitados que puedan aplicar de forma exitosa las metodologías y adaptarse rápidamente a los cambios tecnológicos y las exigencias de un área que está en constante cambio y evolución.

# Una propuesta de formación en ciberseguridad

La propuesta curricular describe una formación necesaria para desempeñarse en ciberseguridad a nivel técnico. Un técnico especializado en ciberseguridad debe ser capaz de aplicar las metodologías, tecnologías y herramientas que provee la disciplina (como, por ejemplo, la criptografía aplicada, los modelos y mecanismos de autenticación y control de acceso, el desarrollo seguro de aplicaciones, el hardening de sistemas operativos y bases de datos, y la arquitectura de redes seguras) en las áreas en las que la ciberseguridad tiene su aplicación. Debe también estar familiarizado con los fundamentos de la seguridad de la información, de forma de poder dar apoyo en la aplicación de normativas y estándares, en la gestión de incidentes y riesgos de seguridad y en garantizar la continuidad del negocio, protegiendo los activos críticos.

El nombre de la carrera que se propone es Analista Técnico en Ciberseguridad. Es una carrera de nivel terciario, o sea que para su cabal aprovechamiento se requiere ingresar con una formación mínima equivalente a la lograda en los estudios de bachillerato (12 años de escolaridad, comprendiendo Primaria y Enseñanza Media). En la Clasificación Internacional Normalizada de Educación (CINE 2011) de UNESCO corresponde al nivel 5 (Educación terciaria de ciclo corto) [UNE13]. Es decir, corresponde a un nivel de enseñanza del primer ciclo del tercer grado que conduce a un certificado no equivalente a un primer título o grado universitario. Según la clasificación, queda comprendida en este nivel toda carrera que tiene una duración mínima de dos años y una duración inferior (aunque no siempre) a tres años (en el caso de los sistemas educativos que tienen programas con organización modular donde las certificaciones se otorgan en base a la acumulación de créditos, se requiere un período comparable de tiempo y similar grado de intensidad). Las carreras de nivel CINE 5 son en general programas terciarios orientados a la práctica profesional que pueden dar eventualmente acceso a otros programas terciarios.

# Generalidades de la propuesta y estructura de este documento

El presente documento describe, en primer lugar y a alto nivel, el mapa curricular de la carrera Analista Técnico en Ciberseguridad, que define aspectos generales de la formación propuesta, como el perfil del egresado, la organización de los estudios y los requerimientos académicos necesarios para la obtención del título. Expresamente no se incluye aquí una lista de asignaturas (cursos), sus programas o sus previas, ni un listado de los recursos necesarios para llevar adelante la carrera, ni ningún otro aspecto relacionado con las especificidades de la implementación y puesta en marcha de la carrera. Se espera que estas cuestiones sean estudiadas y definidas por cada institución al momento de implementar la carrera, dejando bastante flexibilidad para que éstas puedan diseñar una propuesta de implementación acorde con sus objetivos académicos, con los recursos humanos y materiales disponibles, y con las necesidades de la industria, en constante evolución. De esta manera el plan de estudios de la carrera podrá adaptarse sin problemas, contemplando múltiples implementaciones posibles en un momento dado y a lo largo del tiempo.

En segundo lugar, este documento presenta una posible implementación de la carrera de Analista Técnico en Ciberseguridad. Implementaciones son listados de actividades curriculares que permiten cumplir los objetivos expresos del Plan de Estudios de la carrera. Constituyen recorridos curriculares que, aprobados por las autoridades competentes, permiten a quien los complete tener la seguridad de que cumple dichos objetivos y puede, por lo tanto, aspirar a la titulación.

Otras implementaciones posibles, una vez aprobadas por las autoridades, se podrían agregar a la que aquí se propone.

Nota: Las implementaciones no serán rígidas, deberán incluir un mínimo de actividades curriculares electivas, que permitan una especialización o al menos una orientación preferencial de la Carrera en el área de Ciberseguridad.

En consecuencia, este documento está dirigido principalmente a miembros de instituciones educativas que estén interesados en implementar la carrera Analista Técnico en Ciberseguridad, a profesionales de la industria que serán principalmente quienes recibirán a los egresados de estos programas, a miembros de organizaciones gubernamentales, y a otros actores involucrados en el sector de la ciberseguridad.

El resto del documento se estructura como sigue. En la Sección2 se presenta el perfil del egresado, describiendo los conocimientos y habilidades que tendrá un egresado de esta carrera. En la Sección 3 se define la duración total de la carrera. La Sección 4 describe la organización de los estudios y define las áreas de formación. El perfil esperado de ingreso se detalla en la Sección 5, mientras que los requisitos formales para la obtención del título y posibles continuaciones de los estudios se presentan en las Secciones 6 y 7, respectivamente. En la Sección 8 se introducen algunos elementos relevantes relativos a la evaluación y actualización de la carrera. En la Sección 9 se definen algunos supuestos sobre el dictado de la carrera, se define la lista de actividades curriculares a ofrecer, y se muestra una posible distribución de los cursos en 6 semestres lectivos. Finalmente, en la Sección 10 se especifican los recursos necesarios, condicionamientos y se realiza un análisis de factibilidad. En anexos se detallan los programas de algunas actividades curriculares relevantes de la implementación propuesta, incluyendo en cada caso: el nombre de la actividad, el área de formación a la que pertenece, sus créditos, objetivos de aprendizaje, metodología de enseñanza, temario, bibliografía (básica y recomendada), y los conocimientos previos exigidos y recomendados.

# Objetivos de formación y perfil del egresado

La formación recibida durante la carrera le permitirá al Analista Técnico en Ciberseguridad integrarse rápidamente al mercado del trabajo y llevar adelante con solvencia tareas técnicas de seguridad necesarias en los sistemas de la organización en la que se incorpore.

# Competencias técnicas

Los objetivos de aprendizaje específicos en ciberseguridad que habrá adquirido el egresado se pueden clasificar en tres niveles: familiaridad, uso y valoración [Joi13].

El nivel de familiaridad implica que el estudiante conoce un concepto (puede responder la pregunta ¿qué sabes de este concepto?), pero no se espera que lo pueda aplicar. En esta primera categoría, el egresado habrá adquirido familiaridad con: i) las propiedades básicas de la seguridad informática: confidencialidad, integridad y disponibilidad; ii) qué es un riesgo, una vulnerabilidad, una amenaza y un vector de ataque; iii) las distintas formas en las que la criptografía es usada en la comunicación segura de datos; iv) la diferencia entre métodos criptográficos simétricos y asimétricos; v) la importancia de usar un lenguaje de programación type safe para la producción de programas seguros; y vi) los componentes principales de un sistema de gestión de la seguridad y sus funciones.

El nivel de uso implica que el estudiante puede aplicar el concepto en un problema concreto y responder a la pregunta ¿qué sabes hacer con este concepto? En este plano, el egresado habrá adquirido capacidades que le permitirán aplicar: i) los diferentes mecanismos para definir y aplicar procedimientos de identificación, autenticación y autorización en sistemas operativos Unix y Windows; ii) mecanismos de gestión de contraseñas y de definición de principals, sujetos y objetos en sistemas operativos; iii) criptografía de clave pública y privada así como la infraestructura de clave pública (PKI) para incrementar la seguridad de redes TCP/IP; y iv) mecanismos de validación y sanitización de la información para poder hacer frente a la manipulación de canales de entrada por parte de un adversario.

Finalmente, en el nivel valoración el estudiante es capaz de considerar un concepto desde varios puntos de vista, evaluar varias alternativas, y decidir sobre la mejor forma de resolver un problema (responde a la pregunta ¿por qué harías eso?). El egresado podrá identificar, comparar y evaluar los siguientes conceptos: i) qué es un activo de seguridad; ii) en qué consiste un proceso de identificación, un proceso de autenticación y un proceso de autorización; iii) la diferencia entre los procesos de cifrado, de criptoanálisis, algoritmo criptográfico y criptología; iv) los diferentes mecanismos de control de acceso: control de acceso discrecional, control de acceso mandatorio y control de acceso basado en roles; v) el uso de la infraestructuras de clave pública, PKI, para firma digital. Describir y distinguir sus limitaciones y vulnerabilidades; vi) los principios de diseño de seguridad y de seguridad por diseño. Explicar la tensión entre seguridad y usabilidad, y entre seguridad y privacidad; vii) la implementación de mecanismos de control de acceso en sistemas operativos; viii) los mecanismos de auditoría provistos por los sistemas operativos Windows y Unix;

ix) las virtudes y limitaciones de las tecnologías de seguridad en cada capa

de una red de computadores, así como los mecanismos de defensa adecuados y sus limitaciones ante una amenaza de seguridad; x) las diferentes categorías de amenazas y ataques a las redes TCP/IP; xi) la necesidad de gestionar el ciclo de vida de la seguridad de las aplicaciones web; y xii) la importancia de realizar un manejo preciso y claro de condiciones de error y de carrera en la programación de aplicaciones.

Aunque el foco de la carrera está puesto en garantizar la seguridad de sistemas informáticos, la formación también contempla el estudio y puesta en práctica de técnicas y herramientas de seguridad ofensiva, de modo que el estudiante adquiera la mentalidad de atacante necesaria para poder proteger mejor los sistemas.

Esta formación le permitirá a un Analista Técnico en Ciberseguridad colaborar como técnico superior en tareas de concepción, mantenimiento, producción o gestión de complejidad relativa, para el aseguramiento de sistemas computacionales, integrándose al trabajo en equipo para la realización de estas actividades en situaciones de cierta complejidad, tanto por sus características como por su escala.

## Competencias generales

Al egresar de la carrera, el estudiante habrá adquirido, además, una formación básica en las principales áreas de la computación, como programación, arquitectura de computadoras, sistemas operativos y redes, con una profundización en el área de la ciberseguridad. Será capaz de desarrollar sistemas de pequeño porte y contará con la formación necesaria para participar en proyectos de mayor porte. La formación adquirida, unida a la experiencia, se proyectará en un profesional competente en la implementación y el mantenimiento de políticas y controles de aseguramiento de infraestructuras y sistemas informáticos.

El Analista Técnico en Ciberseguridad deberá ser capaz de evaluar soluciones alternativas e integrar distintas tecnologías en la implementación. Deberá poseer habilidades de comunicación, tanto para presentar sus soluciones dentro del área, como para interactuar con profesionales de otras áreas y público en general. Esto incluye la capacidad de trabajar en equipos (tanto de pares como interdisciplinarios) en todos los aspectos de su actividad.

Adicionalmente, la carrera deberá enseñarle al estudiante a mantener una conducta ética y acorde a las responsabilidades propias del trabajo en ciberseguridad. El egresado deberá ser capaz de integrar conocimiento de los procesos de producción vinculados a su área profesional en Uruguay, en sus dimensiones técnica, económica y social, para enfrentarse creativamente a las problemáticas que se le planteen, y tener capacidad de búsqueda y procesamiento de información relevante a su trabajo y de seguir los avances técnicos y metodológicos de las distintas especialidades de la disciplina.

# Especializaciones

Además de haber recibido una formación sólida en las áreas fundamentales de la ciberseguridad, aplicables a todas las especialidades de la disciplina, el egresado deberá haber adquirido las herramientas conceptuales y prácticas básicas de un dominio o perfil de especialización. Algunos perfiles de Analista Técnico en Ciberseguridad podrían ser Ciberinteligencia, Desarrollo seguro de aplicaciones (web) y Administración segura de sistemas. Las instituciones que desarrollen esta carrera deberán definir los perfiles ofrecidos de acuerdo a sus posibilidades, los requerimientos del mercado y los avances de la disciplina.

Está prevista una titulación intermedia, denominada Técnico en Ciberseguridad (descrita en secciones subsiguientes), que abarca las capacidades analíticas y operativas mencionadas pero que no incluye una especialización según perfiles.

# Duración de la carrera

La oferta educativa será presentada en forma de carrera a cursar. Su duración queda definida por la dedicación en horas necesaria para obtener los créditos requeridos para el otorgamiento del título.

El crédito es la unidad de medida, tanto del peso relativo de los distintos cursos o actividades curiculares como del avance de los estudiantes en la carrera. Se entiende por crédito un tiempo de 15 horas dedicado al estudio. Estas horas incluyen aquellas que corresponden a clases y trabajo asistido en aula, laboratorio o campo (tiempo presencial o de enseñanza directa), así como también las de trabajo estrictamente personal (extra- aula) requeridas para el cabal aprovechamiento de los cursos.

En aquellas actividades que requieran tanto tiempo de enseñanza directa como de dedicación extra-aula, la estimación a utilizar será la de 1 crédito por cada 7.5 horas en aula. Este cálculo podrá adoptar otros valores en función de la relación entre dedicación en aula y dedicación adicional extra-aula requerida para su adecuada asimilación. El caso extremo estará dado por los cursos o actividades que requieren nula o casi-nula dedicación extra-aula, en los que la estimación será de 1 crédito por cada 15 horas en aula.

La carrera Analista Técnico en Ciberseguridad requerirá la obtención de al menos 210 créditos, mientras que para el título intermedio Técnico en Ciberseguridad la exigencia es de al menos 140 créditos. Suponiendo un avance promedio de 70 créditos por año (que representa una dedicación aproximada de 30 horas semanales, incluyendo horas de estudio), se espera que la carrera Analista Técnico en Ciberseguridad se pueda realizar en su totalidad en tres años, mientras que la de Técnico en Ciberseguridad en dos años.

Nota: Dado que sería posible revalidar asignaturas o créditos de carreras afines que involucren cursos iniciales de computación y matemática, tanto de carreras de grado como de formaciones terciarias no universitarias, la duración neta de la carrera Analista Técnico en Ciberseguridad y del título intermedio Técnico en Ciberseguridad podría reducirse. En particular, en este último caso sería posible para un estudiante obtener una formación de Técnico en Ciberseguridad en un plazo aproximado de un año siempre que cuente con una formación previa básica adecuada.

# Estructura curricular

Detalle de la estructura curricular.

# Organización de los estudios

La oferta educativa de la carrera incluirá los siguientes tipos de actividades curriculares:

- Cursos o asignaturas;
- Actividades de relacionamiento con el medio laboral en el que presumiblemente se desempeñará el egresado;
- Alguna tarea que implique simultáneamente actividad creativa y uso de conocimientos y formación adquiridos (a modo de pequeño proyecto o tesis).

Los cursos serán principalmente semestrales. Se ofrecerá un conjunto de cursos que permita obtener los créditos necesarios. Habrá un sistema de previaturas, de acuerdo a los conocimientos o la formación requeridos para la realización de cada curso, que fueran impartidos en otro u otros cursos. El sistema de previaturas asegurará la posibilidad académica de cursar con aprovechamiento cada curso.

Este plan deja flexibilidad para que la implementación defina la grilla específica de cursos y previaturas; y también a los estudiantes para realizar una trayectoria curricular adecuada para ellos. Sin embargo, es importante hacer notar que una formación técnica en ciberseguridad requiere de ciertos conocimientos y habilidades básicas en matemática y computación que deberán ser adquiridos sobre el comienzo de la carrera. Es por esto que se visualiza una carrera en donde la formación básica esté concentrada en el primer año y la formación específica en ciberseguridad en el segundo, quedando el tercer año para temas avanzados, pasantías, proyectos y estudios especializados en alguna sub-área de la disciplina.

Dentro de las distintas áreas podrán ofrecerse cursos obligatorios y electivos. Las formas de evaluación serán definidas por cada curso, pudiendo tener éstos pruebas parciales, trabajos obligatorios o exámenes.

Una vez aprobado un curso se entiende que se ha adquirido la cantidad de créditos asignados a éste.

Es deseable que la mayoría de los cursos integren, en la medida de lo posible, teoría y práctica. Para una formación en ciberseguridad es fundamental contar con ambientes de experimentación y entrenamiento en los cuales el estudiante pueda ensayar sobre plataformas que reproduzcan ambientes de producción, incluyendo sus vulnerabilidades, técnicas y herramientas, y reproduciendo problemas reales. En este tipo de ambientes el estudiante podrá tener contacto directo con problemas de seguridad de la vida real, y realizar actividades como montar ataques sobre una infraestructura realista, entrenar las respuestas adecuadas frente a un incidente, investigar las evidencias disponibles en los sistemas atacados, o asegurarlos para que los incidentes no se repitan.

# Áreas de Formación

La carrera se organizará en torno a la siguiente clasificación de áreas de formación (áreas temáticas), que agrupan a las actividades curriculares en concordancia con los objetivos de aprendizaje y el perfil de egreso:

- Matemática Programación
- Arquitectura, Sistemas Operativos y Redes de Computadores Bases de datos
- Seguridad computacional Seguridad de la Información
- Actividades Integradoras: talleres, pasantías y proyectos

**Matemática**

La Matemática constituye una disciplina fundamental de la Computación y la formación en Matemática es importante para un Analista Técnico en Ciberseguridad.

Son objetivos de aprendizaje de esta área de formación tanto la maduración en una forma de razonamiento riguroso como en el manejo de temas específicos que son necesarios para la comprensión de la Computación. Algunos de éstos son: lógica matemática, teoría de conjuntos, definiciones inductivas, recursión, teoría de grafos y estructuras algebraicas.

Se deben incluir cursos de Matemática en, al menos, los siguientes tópicos: Matemática Discreta y Lógica Matemática, que constituyen la base de las ciencias de la computación.

**Programación**

La Programación es una área técnica básica de la carrera Analista Técnico en Ciberseguridad y tiene influencia en casi todas las áreas de la Ciberseguridad. El rol de la Programación en una carrera de este tipo es multidimensional: los estudiantes desarrollan programas durante el diseño de software, modifican programas durante los proyectos, laboratorios, pasantías y talleres, programan y estudian programas en varios cursos de la carrera.

Es objetivo esencial de esta área lograr que un Analista Técnico en Ciberseguridad tenga dominio solvente de lenguajes de programación, conocimiento de paradigmas de programación y lenguajes, manejo de estructuras de datos y algoritmos básicos, y capacidad de diseño y evaluación de algoritmos.

Algunas subáreas dentro del área de formación Programación son: conceptos básicos de Programación, Estructuras de Datos y Algoritmos, Diseño, Implementación y análisis de aplicaciones.

**Arquitectura, Sistemas Operativos y Redes de Computadores**

El estudio de temas en esta área aportan al estudiante conocimientos relativos a la estructura de computadores y el software que permite utilizarlos y conectarlos. Para un profesional en Ciberseguridad resulta fundamental contar con dichos conocimientos ya que son la base de cualquier implementación de un sistema computarizado.

El objetivo de la enseñanza de esta área de formación es que el estudiante tenga conocimientos sólidos en los temas: tipos de procesadores incluyendo manejo de memoria y lenguajes asociados a éstos, estrategias de manejo compartido de recursos del computador, mecanismos de comunicación de datos y de conexión de computadores, incluyendo protocolos y software asociado.

Algunas subáreas dentro de ésta son: Arquitectura de Computadoras, Sistemas Operativos y Redes de Computadoras.

**Bases de Datos**

Esta área de formación trata de la organización de la información así como de los algoritmos que permiten el acceso y modificación eficiente de la información almacenada. También le concierne el estudio de modelos para representar sistemas de información, así como las metodologías utilizables para implementarlos.

Es objetivo de la enseñanza de esta área de formación que el estudiante adquiera conocimientos generales sobre los problemas que surgen en el manejo de grandes cantidades de datos, así como sobre las técnicas propuestas para su resolución. Interesa en particular que el estudiante conozca técnicas de diseño de bases de datos y que sea solvente en la manipulación de modelos de bases de datos existentes. Algunos temas fundamentales involucrados en esta área son: modelos de datos, acceso compartido a datos y diseño de bases de datos.

Algunas subáreas dentro del área Base de Datos son: Tecnología de Gestores de Bases de Datos, y Diseño Conceptual, Lógico y Físico.

**Seguridad Computacional**

El objetivo de esta área de formación es que el estudiante identifique conceptos y propiedades fundamentales de la seguridad informática (confidencialidad, integridad y disponibilidad), así como el concepto de seguridad computacional. Asimismo, que comprenda los conceptos de riesgo, amenaza y vectores de ataque, así como de la seguridad como un concepto que se puede

analizar y aplicar en las distintas capas de la infraestructura de un sistema computacional.

Algunos temas fundamentales contemplados en esta área incluyen: políticas de seguridad, análisis de vulnerabilidades y ataques, técnicas y mecanismos de control de acceso a la información, aplicación de técnicas criptográficas para el aseguramiento del almacenamiento y trasmisión de los datos, análisis de modelos y protocolos de seguridad.

Algunas subáreas dentro del área Seguridad Computacional son: Programación segura, Criptografía aplicada, Seguridad de Sistemas Operativos, Seguridad de Redes.

**Seguridad de la Información**

El objetivo de esta área de formación es que el estudiante adquiera familiaridad con las principales normativas y el marco teórico y práctico necesario para la implementación de Sistemas de Gestión de Seguridad de la Información en todo tipo de organización. Le brindará además las herramientas para aplicar metodologías concretas de gestión de riesgos, incidentes y continuidad del negocio.

Algunos temas fundamentales abarcados en esta área de formación contemplan: metodologías para la gestión de seguridad de la información y la gestión de incidentes, y marco jurídico vigente aplicable a las actividades referentes a la seguridad informática.

Algunas subáreas dentro del área de formación Seguridad de la Información son: Gestión de Seguridad de la Información, Gestión de Incidentes, Protección de Datos Personales, Privacidad y Acceso a la Información Pública.

**Actividades integradoras: talleres, pasantías y proyectos**

Los talleres, proyectos y pasantías, así como los laboratorios asociados a los cursos constituyen una actividad indispensable en la formación de un Analista Técnico en Ciberseguridad. El trabajo práctico en máquina que éstos incluyen se basa en la aplicación de los principios para el diseño, la implementación y la verificación de controles de seguridad en sistemas computarizados. Los laboratorios, por su parte, permiten enfatizar la experimentación de técnicas y métodos descritos en los cursos más teóricos.

En todas las actividades de este tipo, además de los aspectos técnicos específicos, el estudiante deberá desarrollar la capacidad de realización de informes orales o escritos.

En diversas partes de la carrera deberán proponerse actividades de este tipo, basándose en diferentes áreas técnicas, con duración y complejidad acordes.

Como actividad a resaltar en esta área de formación se encuentran las pasantías, cuyo objetivo es la inserción del estudiante en un ambiente de desarrollo o de producción. Se procurará que, dentro de las posibilidades, todos los estudiantes puedan realizar al menos una pasantía.

Dentro de esta área de formación (y especialmente en el marco de las pasantías y los proyectos), será posible instrumentar instancias y experencias de formación dual, donde se incorporen horas de aprendizaje tanto en la institución educativa como en una empresa del rubro, supervisadas por un docente responsable de la Carrera.

# Perfil de ingreso

Como regla general se establece que el requisito mínimo para acceder a la carrera Analista Técnico en Ciberseguridad será la completa aprobación de estudios de enseñanza media a nivel de Bachillerato Diversificado o Bachillerato Tecnológico.

Asimismo, se establece que los desniveles de formación originados por el cursado de diferentes opciones de enseñanza media serán compensados por el esfuerzo personal y por estrategias diseñadas por los docentes de los cursos para lograr el nivel requerido de aprovechamiento.

Por otra parte, será posible revalidar asignaturas o créditos de carreras afines que involucren en particular (aunque no exclusivamente) cursos iniciales, tanto de carreras de grado como de formaciones terciarias no universitarias (como el Tecnólogo en Informática, que corresponde a formación tecnológica terciaria).

# Título otorgado

A continuación se describen los requerimientos de créditos que deben ser obtenidos para titularse.

# Analista Técnico en Ciberseguridad

Para obtener este título se requerirá haber acumulado, al menos, un total de 210 créditos, cumpliendo a su vez con los mínimos por áreas de formación que se indican en el Cuadro 1.

| Área de formación | Mínimo de créditos |
|---|---|
| Matemática | 12 |
| Programación | 24 |
| Arquitectura, Sistemas Operativos y Redes de Computadoras | 24 |
| Bases de Datos | 6 |
| Seguridad Computacional | 90 |
| Seguridad de la Información | 10 |
| Actividades Integradoras | 20 |
| Suma de mínimos por área | 186 |
| Total de la carrera | 210 |

Cuadro 1. Créditos mínimos requeridos para Analista Técnico en Ciberseguridad.

La suma de créditos mínimos requeridos, clasificados por área de formación, es 186. De éstos, 66 corresponden a formación básica en matemática y computación (31 %), mientras que 120 consisten en formación en ciberseguridad propiamente (57 %). El resto de los 210 créditos se consiguen con actividades curriculares electivas o específicas de un perfil.

A quien, teniendo su currículo aprobado por la o las instituciones que administran la carrera, cumpla con los siguientes requisitos:

1. número total de créditos no inferior a 210
2. créditos por área de formación exigidos en el Cuadro1

se le otorgará el título de Analista Técnico en Ciberseguridad.

# Técnico en Ciberseguridad

Se otorgará el título intermedio Técnico en Ciberseguridad a un estudiante de la carrera Analista Técnico en Ciberseguridad que ha completado requisitos mínimos de formación básica y tiene conocimientos específicos en Computación y Ciberseguridad suficientes como para desempeñar tareas técnicas en un equipo de trabajo en el área.

Las condiciones académicas para recibir el título Técnico en Ciberseguridad son reunir al menos 140 créditos y cumplir los mínimos que se se detallan en el Cuadro 2.

| Área de formación | Mínimo de créditos |
|---|---|
| Matemática | 12 |
| Programación | 24 |
| Arquitectura, Sistemas Operativos y Redes de Computadoras | 16 |
| Bases de Datos | 6 |
| Seguridad Computacional | 70 |
| Suma de mínimos por área | 128 |
| Total de la carrera | 140 |

Cuadro 2. Créditos requeridos para título Técnico en Ciberseguridad

La suma de créditos mínimos requeridos, clasificados por área de formación, es 128. El resto de los 140 se consiguen con actividades curriculares electivas de alguna de las áreas de formación.

## Habilitación para otros estudios

El Plan de Estudios de cada implementación de esta carrera preverá la posibilidad de continuar estudios universitarios con posibilidad de aprovechamiento de parte del esfuerzo ya realizado en el nivel tecnológico terciario. En particular, los estudios aprobados a lo largo de la carrera Analista Técnico en Ciberseguridad podrán usarse para revalidar cursos u obtener créditos en carreras de nivel universitario en Computación, según surja del análisis de las implementaciones de los planes de estudio correspondientes por los órganos competentes.

Los Planes de Estudio de las distintas carreras de Analista Técnico en Ciberseguridad deberán prever la posibilidad de movilidad “horizontal”, con aprovechamiento de parte del esfuerzo realizado para cursar estudios correspondientes a otras carreras de este tipo.

# Evaluación y actualización de la carrera

El presente Plan de Estudios fue diseñado para ser flexible y permitir diferentes implementaciones de la carrera, y su evolución a lo largo del tiempo. No obstante, será necesario revisar y posiblemente actualizar tanto el Plan como los contenidos académicos específicos de la carrera, para asegurar que éste se adecúa a la realidad de las instituciones que desarrollan la carrera, a las necesidades en constante evolución del mercado de trabajo y la industria, y a los avances propios de la disciplina.

# Generalidades

Para poder hacer un seguimiento a nivel general de la situación de la carrera se propone un conjunto de indicadores que deberán ser calculados periódicamente (al menos una vez por año). Es importante resaltar que no es suficiente realizar un análisis de cada uno de estos indicadores por separado, si no que es necesario estudiarlos de manera integral, ya que los mismos se complementan. También es muy importante evaluar la evolución de los distintos indicadores a lo largo del tiempo. Este análisis permitirá tener una visión dinámica del estado de la carrera, planificar acciones que tiendan a mejorar la trayectoria de los estudiantes y evaluar los resultados de las mismas.

- Para la elaboración de estos indicadores se definen los siguientes conceptos:
- Egresado: una persona que ha obtenido el título de Analista Técnico en Ciberseguridad.
- Estudiante activo: una persona inscripta a la carrera que registra alguna actividad académica (curso, examen, etc) en los últimos dos años.
- Estudiante inactivo: una persona inscripta a la carrera, pero que no registra ninguna actividad académica en los últimos dos años.
- Generación: Es el año en el que se inscribe un estudiante a la carrera.
- Duración teórica de la carrera: Para la carrera de Analista Técnico en Computación, este valor será de 3 años y se notará DC.

Más allá de los indicadores (abajo) propuestos, será necesario evaluar periódicamente la evolución de la carrera y sus implementaciones considerando el perfil de egreso y los objetivos de la carrera. En particular, será necesario analizar que las diferentes actividades curriculares de una implementación de la carrera cumplen sus objetivos de formación, están actualizadas, siguen la metodología propuesta y contemplan el número de créditos requeridos (se ajustan al número real de horas consideradas).

# Indicadores

Se proponen algunos indicadores básicos, priorizando aplicabilidad y factibilidad, evitando definir medidas que resulten complejas de calcular o no aporten información clave, en una primera instancia:

- Distribución de estudiantes activos: Porcentaje de estudiantes activos de la carrera para una generación.
- Avance por franja de créditos: Indica el porcentaje de estudiantes activos por franja de créditos respecto del total de activos de la carrera. Tasa terminal de la carrera: Indica el porcentaje de estudiantes de cada generación que egresaron hasta ese momento.
- Tasa bruta de eficiencia terminal de la carrera: Cociente entre estudiantes egresados en el año t (con independencia de la generación) y estudiantes inscriptos a la carrera en el año t (DC + 1), expresado en porcentaje.
- Tasa neta terminal de la carrera: Cociente entre estudiantes de la generación t (DC +1) que egresaron en el año t y total de estudiantes inscriptos de esa generación.
- Coeficiente de eficiencia terminal de la carrera: Es el cociente entre la mediana del tiempo de egreso respecto a la duración teórica de la carrera. Se mide la eficiencia de una carrera, mediante la proporción del tiempo teórico previsto por el plan y el tiempo utilizado para la culminación de la carrera. Un coeficiente de 1 significa que la duración mediana de la carrera es igual a la teórica.
- Desvinculación neta: Es la relación entre los estudiantes inactivos de la carrera y los estudiantes inscritos a la carrera para una generación.
- Actividades integradoras vinculadas con el medio: Listado y porcentaje de talleres, pasantías y proyectos realizados con el sector productivo (no exclusivamente dentro de la institución).
- Egresados que trabajan: Porcentaje de egresados que trabajan, distinguiendo en particular si lo hacen en el área de informática en general o en una subárea de seguridad informática.
- Estudiantes que trabajan: Porcentaje de estudiantes de la carrera que trabajan, distinguiendo en particular si lo hacen en el área de informática en general o en una subárea de seguridad informática. Discriminar entre estudiantes activos e inactivos
- Valoración de los egresados: Valoración de los egresados que realizan las empresas que los contratan (considerando encuestas tipo para este fin), distinguiendo el área en la que se desempeñan.

Adicionalmente podrían contemplarse otros indicadores usados para evaluar y realizar el seguimiento de carreras técnicas terciarias, así como indicadores propios considerados por cada institución que implemente la carrera.

Complementariamente, se sugiere considerar instrumentos de evaluación del cuerpo docente y de las actividades curriculares por parte de sus estudiantes, tales como las habituales encuestas estudiantiles, usadas por las instituciones para diversas carreras. Asimismo, se recomienda realizar evaluaciones de los docentes participantes en las actividades curriculares por parte de sus docentes responsables. Finalmente, se sugiere la evaluación periódica de los responsables de las unidades curriculares y el seguimiento de las diferentes evaluaciones planteadas

# Propuesta de implementación de Plan de estudio

En esta sección se definen algunos supuestos sobre el dictado de la carrera, se define la lista de actividades curriculares a ofrecer, y se muestra una posible distribución de los cursos en 6 semestres lectivos.

## Supuestos básicos

Se trata de una carrera terciaria, con orientación al mercado de trabajo. Se considera importante que los estudiantes obtengan formación y resultados (diplomas, cursos específicos) que los capaciten y potencien para ocupar rápidamente posiciones en el mercado de trabajo.

Se ha pensado como referencia en una modalidad presencial (de enseñanza directa) de aproximadamente 4 horas diarias, con un seguimiento más asistido y controlado que lo que es usual en carreras de grado. Asimismo, se consideran en esta propuesta un número significativo de horas de clase por área, lo cual en parte se justifica por el tipo de formación que se persigue (abarcativa, generosa en tiempos) pero que no deja de ser un aspecto a revisar (en particular, en virtud de la relación entre el número de estudiantes y docentes, y de los recursos disponibles). Concretamente, puede discutirse el añadido de actividades curriculares en los distintos semestres.

Deben discutirse los recursos (salones, docentes, laboratorios, carga estudiantil admisible) y considerarse modalidades alternativas (posibilidad de modalidad no presencial o semi-presencial). En particular, el concepto de enseñanza directa podría contemplar tanto clases presenciales, como remotas o híbridas.

# Actividades curriculares por áreas de formación

A continuación se describen, para cada área de formación, algunas actividades curriculares propuestas. Dado que se trata de una carrera técnica específica, se establece como lineamiento general la inclusión, desde el inicio de la formación, de problemáticas vinculadas a la cibserseguridad en, por ejemplo, actividades prácticas, talleres y laboratorios, en las diferentes actividades curriculares, aunque no se trate de cursos específicos de seguridad.

También se sugiere la realización de ponencias como complementos de los cursos, que ejemplifiquen conexiones entre las competencias y los conocimientos desarrollados en las actividades curriculares con habilidades necesarias en el área de la cibserseguridad.

**Matemática**

- Matemática Discreta y Lógica 1 y 2. Estos cursos proveen la formación en los fundamentos matemáticos esenciales de la Informá- tica: lógica matemática, teoría de conjuntos, definiciones inductivas, recursión, teoría básica de grafos y estructuras algebraicas.

Sería posible considerar como alternativa un curso de Matemática Discreta y otro de Lógica.

**Programación**

- Introducción a la Programación. Presenta los fundamentos básicos de la programación estructurada, con aplicaciones de pequeño porte. Se hace énfasis en las buenas prácticas de programación (se podría utilizar el lenguaje C).

- Estructuras de Datos y Algoritmos. Extiende el conjunto de conceptos presentados en Introducción a la Programación y presenta la programación modular, trabajándose con aplicaciones de porte mediano, haciendo uso de estructuras de datos, técnicas de diseño y análisis de algoritmos, y nociones de abstracción (se podría utilizar el lenguaje C/C++).

**Arquitectura, Sistemas Operativos y Redes de Computadoras**

- Arquitectura de Computadoras. Estudia los fundamentos de la arquitectura de computadoras, como los sistemas de representación de datos y de numeración, máquinas de estado, memoria y modelo de Von Neumann. Se estudian los componentes de una computadora: microprocesador, memoria, buses, periféricos, controladores de entrada/salida e interrupciones. Se presentan ejemplos de procesadores CISC y RISC, y conceptos de programación a bajo nivel (como lenguajes de máquina y ensambladores).

- Sistemas Operativos. Presenta la teoría e implementación de los sistemas operativos. Se estudian los diferentes mecanismos de administración de memoria, sistemas de entrada/salida y almacenamiento secundario; y las formas de compartirlos entre diferentes procesos. Se ven además conceptos básicos de programación concurrente, como sincronización, secciones críticas, semáforos, intercambio de mensajes, bloqueos mutuos, etc. Se ilustran los conceptos con implementaciones de los sistemas operativos de mayor difusión (Windows y Linux).

- Redes de computadoras. Provee los conceptos de comunicación de datos en redes de computadoras. Se estudian los modelos de referencia OSI y TCP/IP, y las funcionalidades de cada capa. Se presentan los principales protocolos en la capa de aplicación (DNS, SMTP, HTTP, etc.), en la capa de transporte (TCP y UDP), en la capa de red (IPv4, IPv6, ICMP), y en la capa de enlace (ethernet, arp). Adicionalmente, se presentan conceptos básicos de las redes inalámbricas (WiFi).

**Bases de Datos**

- Bases de Datos. Presenta la teoría y aplicaciones de las bases de datos relacionales. Se estudian modelos de datos, lenguajes de consulta (SQL) y técnicas de diseño e implementación de bases de datos relacionales.

**Seguridad Computacional**

- Desarrollo seguro de aplicaciones. Este curso tiene como objetivo introducir los principales conceptos y metodologías asociadas a la seguridad en el desarrollo de aplicaciones. Se presentan y discuten amenazas específicas al dominio, poniendo especial énfasis en la validación y sanitización de datos de entrada. Se analizan vulnerablidades que posibilitan ataques de race condition y buffer overflow. Se introdu- ce al estudiante al uso de lenguajes para el desarrollo web y a técnicas para el diseño seguro de aplicaciones.

- Taller de programación segura. Este taller tiene como objetivo introducir técnicas y herramientas, metodológicas y tecnológicas, para la verificación de seguridad de aplicaciones. El taller constará de dos módulos donde se ejercitarán prácticas ofensivas y defensivas respectivamente. Las prácticas ofensivas estarán basadas en el uso de métodos y herramientas para la aplicación de tests de penetración y similares propios del enfoque DAST (Dynamic Application Security Testing). Para la parte defensiva se pondrá foco en prácticas que permiten aplicar controles a lo largo de todo el ciclo de desarrollo, en particular para realizar verificaciones tanto con el enfoque DAST como con el enfoque SAST (Static Application Security Testing).

- Seguridad de Sistemas Operativos. El objetivo de este curso es introducir conceptos fundamentales de seguridad en sistemas operativos. Se presentan tanto amenazas específicas y tipos de ataque como mecanismos de identificación y autenticación. Se pone particular énfasis en la gestión de contraseñas y en la implementación de los mecanismos de control de acceso y de auditoría provistos por los sistemas operativos.

- Criptografía aplicada. Este curso busca que el estudiante se familiarice con los fundamentos matemáticos de la criptografía, las principales primitivas criptográficas, identifique conceptos y propiedades funda- mentales de la criptografía aplicada, así como algunas malas prácticas que las hacen vulnerables en el uso.

- Seguridad en redes de computadoras. El objetivo de este curso es introducir al estudiante en los conceptos básicos de la seguridad informática de redes de datos TCP/IP. El curso está orientado a formar técnicos capaces de implantar mecanismos de seguridad en sus organizaciones, con el objetivo de desarrollar, ampliar o mejorar las plataformas de comunicación de datos. Al finalizar el curso el estudiante habrá adquirido los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir una red de datos TCP/IP y establecer los mecanismos de protección adecuados.

- Taller de Técnicas y Procedimientos para el aseguramiento de sistemas informáticos. Esta es una actividad curricular fundamentalmente práctica, basada en el uso de tecnologías sobre las cuales se realizan diferentes laboratorios. En dichos laboratorios los estudiantes pueden aprender y profundizar sobre el uso de herramientas específicas de seguridad. El objetivo principal es llevar a la práctica conceptos básicos de seguridad informática. Consecuentemente, este taller complementa los conceptos teóricos/prácticos que son introducidos en los diferentes cursos de Seguridad Computacional, aportando una visión fuertemente focalizada en el uso de métodos técnicos empleados en el sector profesional.

**Seguridad de la Información**

- Gestión de Seguridad de la Información. Los objetivos de este curso son: introducir a los estudiantes en los principales conceptos y metodologías asociadas a la gestión de seguridad de la información, y en el marco normativo internacional y nacional existente; llevar a la práctica una metodología de rápida aplicación para la implementación de un sistema de gestión de seguridad de la información; y presentar metodologías concretas para la gestión de riesgos y gestión de incidentes. Se abarcarán las principales conceptos de la familia de normas ISO/IEC 27000.

- Marco Jurídico de la Seguridad de la Información. El objetivo de este curso es brindar los conocimientos necesarios sobre el marco jurídico nacional vigente aplicable en la actividad profesional en ciberseguridad, con especial énfasis en aspectos vinculados al derecho administrativo e informático. El curso contempla: consideraciones generales sobre el derecho informático y telemático; documento y firma electrónica; protección de datos personales; acceso a la información pública y accesibilidad; y delitos informáticos.

**Actividades integradoras: talleres, pasantías y proyectos**

- Taller de Introducción a la Seguridad Informática. Esta actividad curricular se concibe como una aproximación inicial a la seguridad informática, para que los estudiantes que comienzan la carrera identifiquen conceptos fundamentales de la ciberseguridad, reconozcan las características principales de esta disciplina y experimenten métodos y herramientas para la resolución de problemas concretos. Tendrá una metodología de enseñanza activa, con sesgo lúdico y énfasis en el trabajo en modalidad de taller en equipos. El curso cubre los fundamentos y propiedades básicas de seguridad informática (como confidencialidad, integridad y disponibilidad), y los principales tipos de ataques de los que puede ser objeto un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar su repercusión.

- Pasantías. Son actividades de inserción del estudiante en un ambiente de desarrollo o de producción, y busca la adquisición directa de experiencia por el estudiante en el mundo laboral. El estudiante podrá familiarizarse con métodos, procedimientos y herramientas comunes de la ciberseguridad, y a su vez podrá aplicar los conocimientos, tanto teóricos como aplicados, adquiridos durante la carrera. Se realizarán tareas como pasante en una empresa, organismo o institución, de acuerdo a un plan de trabajo que deberá ser aprobado por la institución educativa que dicta la carrera.

- Proyecto Final. El objetivo del proyecto final es servir de síntesis de los conocimientos adquiridos durante la carrera, e implica la resolución de un problema real u otra actividad representativa del ejercicio profesional en ciberseguridad. El proyecto podrá ser realizado tanto en forma individual como en equipo, y será dirigido por un docente supervisor que será el encargado de brindar lineamientos a los estudiantes para la concreción de los objetivos del proyecto. El proyecto puede ser propuesto en conjunto con una empresa u otra institución externa, siempre sujeto a la aprobación por parte de la institución educativa que dicta la carrera. Los resultados del trabajo deberán ser documentados en un informe que será presentado y defendido ante un tribunal.

**Actividades curriculares electivas Las electivas se organizarían en base a diferentes perfiles. Ejemplos de perfiles son:**

- Ciberinteligencia. Cursos posibles: Gestión de incidentes de seguridad, Análisis Forense Digital y Análisis predictivo de seguridad usando Aprendizaje Automático.

- Administración segura de sistemas. Cursos posibles: Configuración y administración segura de sistemas e Inteligencia operacional.

## Estructura de la carrera y propuesta de créditos

En el Cuadro 9.3 se presenta la distribución curricular de los contenidos de la implementación propuesta del Plan, siguiendo una estructura de 6 semestres. Se incluyen las actividades curriculares y sus créditos. En anexos se detallan, a modo ilustrativo, los programas de algunas actividades curriculares relevantes de la implementación considerada, incluyendo en cada caso: el nombre de la actividad, el área de formación a la que pertenece, sus créditos, objetivos de aprendizaje, metodología de enseñanza, temario, bibliografía (básica y recomendada), y los conocimientos previos exigidos y recomendados.

# Recursos necesarios, condicionamientos y análisis de factibilidad

Detalle de los recursos necesarios, condicionamientos y análisis de factibilidad

# Organización docente

Director de Estudios
Se sugiere la existencia de un Director de Estudios de la Carrera, que cumpla al menos las siguientes funciones:

- Relacionamiento con los estudiantes (recepción de inquietudes, asesoramiento, seguimiento, etc.).

| Propuesta de implementación | | | | | |
|---|---|---|---|---|---|
| Primer Año | | Segundo Año | | Tercer Año | |
| Introducción a la Programación<br><br>12 créditos | Estructuras de Datos y Algoritmos<br><br>12 créditos | Desarrollo seguro de aplicaciones<br><br>12 créditos | Taller de programación segura<br><br>12 créditos | Pasantía<br><br>10 créditos | Proyecto Final<br><br>20 créditos |
| Arquitectura de Computadoras<br><br>8 créditos | Sistemas Operativos<br><br>8 créditos | Redes de computadoras<br><br>8 créditos | Seguridad en Redes de Computadoras<br><br>12 créditos | Electiva 1<br><br>10 créditos | Electiva 2<br><br>10 créditos |
| Matemática Discreta y Lógica 1<br><br>6 créditos | Matemática Discreta y Lógica 2<br><br>6 créditos | Seguridad de Sistemas Operativos<br><br>12 créditos | Taller de Técnicas y Procedimientos<br><br>6 créditos | Electiva 3<br><br>10 créditos | Electiva 4<br><br>10 créditos |
| Taller de Introducción a la Seguridad Informática<br><br>6 créditos | Introducción a las Bases de Datos<br><br>6 créditos | Criptografía Aplicada<br><br>12 créditos | Gestión de la Seguridad de la Información<br><br>12 créditos | | |
| Técnico en Ciberseguridad | | | | | |
| Analista Técnico en Ciberseguridad | | | | | |

Cuadro 3. Vista tabular de la estructura y los contenidos de la implementación del Plan de Estudios

- Coordinación de las actividades curriculares: horizontal (de un mismo semestre) y vertical (de semestres diferentes).
- Coordinación del Órgano Académico Docente.

Órgano Académico Docente Un miembro por cada Área de Formación definida en el Plan de Estudios (Matemática; Programación; Arquitectura, Sistemas Operativos y Redes de Computadores; Bases de datos; Seguridad computacional; Seguridad de la Información; y Actividades Integradoras), coordinados por el Director de Estudios.

Funciones básicas:

- Actualización del Plan de Estudios.
- Análisis de propuestas y aprobación de actividades curriculares electivas y de actividades integradoras.
- Selección y evaluación del cuerpo docente. Seguimiento y evaluación de la Carrera y sus perfiles. Seguimiento de los estudiantes de la Carrera.

Cuerpo Docente de teórico y de práctico (dependiendo de la actividad curricular) y ayudantes de laboratorio. Cada actividad curricular contará con (al menos) un docente responsable.

# Aparato Administrativo

**Bedelía**

Bedelía Informatizada con acceso a Internet.

**Local**

Un aula por grupo de estudiantes. Espacio de oficinas para docentes y administrativos.

**Infraestructura de Laboratorio**

Para la realización de laboratorios de muchos de los cursos de la carrera (en especial para los cursos de seguridad computacional) es necesario brindarle a los estudiantes un ambiente de experimentación seguro y aislado de otras redes de producción de la institución y de internet. Es imperioso lograr montar ambientes realistas y facilitar su confinamiento, típicamente se utilizan tecnologías de virtualización, ya sea directamente o a través de programas dedicado al despliegue de cyber ranges. Es entonces necesario disponer de los recursos poder desplegar esta infraestructura, idealmente en servidores locales dedicados o en servicios externos del tipo infrastructure as a service (IaaS). El dimensionamiento de estos recursos es muy importante, ya que deberán satisfacer la demanda para todos los estudiantes y todos los cursos que lo requieren.

Adicionalmente los estudiantes deberán contar con computadoras personales o estaciones de trabajo adecuadas al tipo de software a ser utilizada en los cursos (una cada dos estudiantes como máximo), con conexión a Internet.

Debe existir personal de administración de sistemas que se encargue de instalar, mantener y gestionar la infraestructura necesaria.

**Biblioteca**

Acceso a bibliografía necesaria para cada actividad curricular, considerando la indicada y sugerida por cada una en su programa.

# Currículo del personal docente

**Perfil docente**

Cada actividad curricular estará a cargo de un docente con formación y experiencia en los temas contemplados en el programa de la actividad (docente responsable), considerando el nivel técnico terciario de la carrera.

Se valorará el balance entre formación y experiencia acreditables en el área de formación corresponiente.

**Formación requerida**

Se requiere formación terciaria en computación. Se priorizará a egresados de carreras de al menos tres años en computación para ser responsables de una actividad curricular.

Se valorará tener formación acreditable en Ciberseguridad. Para actividades curriculares en las áreas de formación: Seguridad Computacional y Seguridad Informática, será un requisito la formación en Ciberseguridad.

**Experiencia necesaria**

Se requiere experiencia o formación docente y se valorará experiencia laboral profesional para la actividad curricular involucrada. Será necesario acreditar la formación académica y la experiencia referida.

# Bibliografía

[Joi13] Joint Task Force on Computing Curricula. Curriculum Guidelines for Undergraduate Degree Programs in Computer Science. 2013.

[Joi18] Joint Task Force on Cybersecurity Education. Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity. Association for Computing Machinery, New York, NY, USA, 2018.

[UNE13] UNESCO. Clasificación Internacional Normalizada de La Educación. CINE 2011. 2013. Disponible en: http://uis.unesco.org/sites/default/files/documents/isced- 2011-sp.pdf.

# Anexo: Definición de Actividades Curriculares

Definición de Actividades Curriculares a presentarse en el anexo.

# A. Programa de Matemática Discreta y Lógica 1

1. **Datos de la Actividad**

- Curricular Nombre: Matemática Discreta y Lógica 1
- Área de formación: Matemática
- Créditos: 6

2. **Objetivo**

- Reconocer la importancia de la modelización y abstracción en sistemas informáticos.
- Identificar y aplicar los conceptos de conjunto, relación, función y secuencia, y reconocer su relevancia como herramientas de modelización en computación.
- Reconocer, interpretar y aplicar diferentes tipos de pruebas matemáticas.
- Identificar, interpretar y aplicar las ideas de conjunto inductivo, prueba por inducción (estructural) y función recursiva.
- Reconocer y aplicar Máquina de Estados como herramienta de modelización para el análisis de procesos.
- Aplicar definiciones y resultados básicos de combinatoria y teoría de grafos.
- Utilizar las técnicas de la matemática discreta para abordar problemas de conteo, numeración y combinación.
- Reconocer las nociones de conjuntos numerables y no numerables y su importancia en el contexto de la computación.

  El objetivo de esta actividad curricular es que el estudiante comprenda algunos conceptos básicos utilizados en informática para representar elementos de la realidad, pueda razonar y definir funciones sobre éstos. Asimismo, que el estudiante sepa utilizar elementos relevantes de matemática discreta y de lógica matemática, a nivel conceptual.

3. **Metodología de enseñanza**

- Horas clase (práctico y laboratorio): 30
- Horas evaluación: 6
- Horas estudio: 24
- **Total de horas de dedicación del estudiante: 90**
- Horas clase (teórico): 30

4. **Temario**

- Nociones sobre pruebas
  - Nociones de implicación, equivalencia, recíproco, inverso, contrarecíproco, negación y contradicción
  - Estructura de una prueba matemática
  - Pruebas directas, por contraejemplo y por absurdo
- Tipos de datos matemáticos
  - Conjuntos y secuencias
  - Funciones y relaciones binarias
  - Definiciones inductivas y recursivas
  - Definición de conjuntos (lenguajes) inductivos
  - Pruebas por inducción estructural
  - Funciones recursivas
- Máquinas de estado
  - Estados y transiciones
  - Análisis de corrección de algoritmos a través de máquinas de estados
- Grafos dirigidos y órdenes parciales
  - Grados de vértice, caminos
  - matrices de adyacencia, conteo de caminos

        - grafos acíclicos dirigidos, ordenamiento topológico
    - Grafos simples
        - Adyacencia y grados de vértice
        - Grafos bipartitos y emparejamientos
        - Caminos, ciclos y conectividad
        - Bosques y árboles
    - Combinatoria
        - Nociones básicas
        - Progresiones, permutaciones y combinaciones
        - Resolución de relaciones de recurrencia

5. **Bibliografia básica**


- 1. E. Lehman, F. Thomson Leighton, A. R. Meyer: Mathematics for Computer Science, (2017).


| Tema | Básica | Complementaria |
|---|---|---|
| Nociones sobre pruebas | (1) | (1) |
| Tipos de datos matemáticos | (1) | (1) |
| Tipos de datos recursivos | (1) | (1) |
| Máquinas de estado | (1) | (1) |
| Grafos dirigidos y órdenes parciales | (1) | (1,2) |
| Grafos simples | (1) | (1,2) |
| Combinatoria | (1) | (1,2) |

6. **Bibliografia complementaria**


- R. Grimaldi: Matemática discreta y combinatoria: Una introducción con aplicaciones, Addison-Wesley World Student Series, 3rd. Edition, (1998).
- F. Moller, G. Struth: Modelling Computing Systems: Mathematics for Computer Science, (2013).

# B. Programa de Introducción a la Programación

## 1. Datos de la Actividad Curricular

- **Nombre**: Introducción a la Programación
- **Área de formación**: Programación
- **Créditos**: 12

## 2. Objetivos

El objetivo de esta actividad curricular es presentar al estudiante conceptos básicos de programación en el paradigma de la programación imperativa. Luego de introducir elementos básicos de un lenguaje de programación, como C, se trabajará en el diseño, la implementación y el análisis de algoritmos simples (de pequeño porte).

A nivel de los objetivos de aprendizaje, el estudiante será capaz de:

- Utilizar conceptos elementales de la programación imperativa, tales como: identificadores, variables, tipos de datos, estructuras de control y subprogramas (funciones y procedimientos).
- Diseñar algoritmos para resolver problemas no complejos.
- Utilizar estructuras de control adecuadas para distintos problemas. Diseñar algoritmos recursivos simples.
- Utilizar adecuadamente diferentes mecanismos de pasaje de parámetros en funciones y procedimientos.
- Construir programas o subprogramas de pequeño porte utilizando un lenguaje de programación imperativa, como C, contemplando aspectos tal como: codificación, compilación y depuración de errores.
- Identificar mejoras a la calidad de un código, basadas en la aplicación de buenas prácticas de diseño e implementación, y la ejecución de casos de prueba.
- Introducir y aplicar nociones básicas de eficiencia en el diseño de soluciones.

## 3. Metodología de enseñanza

- Horas clase (teórico): 45
- Horas clase (práctico y laboratorio): 75
- Horas evaluación: 6
- Horas estudio: 54

**Total de horas de dedicación del estudiante**: 180

## 4. Temario

1. Introducción a la computación
    1. Noción de algoritmo
    2. Lenguaje de programación: sintaxis y semántica
    3. Compilación y ejecución de programas.
2. Introducción a la programación imperativa
    1. Estructura de un programa
    2. Identificadores, constantes y variables
    3. Tipos de datos básicos *d*) Asignación y expresiones *e*) Entrada y salida
3. Algoritmo y estructuras de control
    1. Secuencia, selección e iteración
    2. Introducción a la recursión
4. Estructuras de datos
    1. Tipos primitivos
    2. Tipos estructurados
5. Descomposición y modularización
    1. Subprogramas (funciones y procedimientos)
    2. Especificación de operaciones mediante pre y post condiciones
    3. Pasajes de parámetro
6. Algoritmos de búsqueda y ordenación
    1. Búsquedas lineal y binaria
    2. Algoritmos de ordenación
    3. Análisis de estos algoritmos

7. Calidad y corrección
    1. Errores. Tipos de errores
    2. Buenas prácticas de diseño e implementación
    3. Nociones básicas de corrección de programas

## 5. Bibliografía Básica

1. B. W. Kernighan, D. M. Ritchie. El lenguaje de programación C.

Prentice-Hall, (1991).

### Complementaria

1. B. W. Kernighan, D. M. Ritchie. El lenguaje de programación C (Spanish Edition), (2021).
2. H. M. Deitel, P. J. Deitel. Cómo programar en C/C++. Prentice-Hall Hispanoamericana, (1998).

| Tema | Básica | Complementaria |
|---|---|---|
| Introducción a la computación | (1) | (1,2) |
| Introducción a la programación imperativa | (1) | (1,2) |
| Algoritmo y estructuras de control | (1) | (1,2) |
| Estructuras de datos | (1) | (1,2) |
| Descomposición y modularización | (1) | (1,2) |
| Algoritmos de búsqueda y ordenación | (1) | (1,2) |
| Calidad | (1) | (1,2) |

## 6. Conocimientos Recomendados Conocimientos Previos Exigidos Ninguno

**Conocimientos Previos Recomendados: s**olo se requieren conocimientos ya contemplados por las condiciones de ingreso a la carrera. Se ubicaría en el primer año de la carrera (en particular en su primer semestre).

# C. Programa de Matemática Discreta y Lógica 2

## 1. Datos de la Actividad Curricular

- **Nombre**: Matemática Discreta y Lógica 2
- **Área de formación**: Matemática
- **Créditos**: 6

## 2. Objetivos

El objetivo de esta actividad curricular es que el estudiante comprenda la Lógica de Predicados desde el punto de vista formal y como mecanismo de especificación y verificación. Asimismo, que sepa utilizar elementos relevantes de matemática discreta y de lógica matemática para formalizar elementos de la realidad.

A nivel de los objetivos de aprendizaje el estudiante será capaz de:

- Reconocer los componentes de un sistema formal.
- Interpretar y distinguir las nociones de verdad, juicio y fórmula lógica en Lógica de Primer Orden.
- Interpretar y distinguir elementos sintácticos de la Lógica de Primer Orden.
- Interpretar la noción de estructura de primer orden.
- Interpretar y diferenciar los juicios que involucran fórmulas, términos y estructuras.
- Construir estructuras y lenguajes de primer orden adecuados para representar una realidad determinada.
- Identificar y probar propiedades sintácticas de los lenguajes de primer orden.
- Identificar y probar propiedades algebraicas de la Lógica de Primer Orden.
- Interpretar las reglas de inferencia de Deducción Natural como esquemas de razonamiento típicos de las matemáticas.
- Construir pruebas usando las reglas de Deducción Natural. Interpretar y aplicar las ideas de axioma, teorema, teoría lógica, consistencia.
- Interpretar las nociones de corrección y completitud de la lógica clásica de primer orden.

## 3. Metodología de enseñanza

- Horas clase (teórico): 30
- Horas clase (práctico y laboratorio): 30
- Horas evaluación: 6
- Horas estudio: 24

**Total de horas de dedicación del estudiante**: 90

## 4. Temario

1. Sintaxis de la Lógica de Primer Orden (LPO)
    1. Definición de estructura de primer orden
    2. Definición recursiva de términos y fórmulas sobre un alfabeto
    3. Definición de variables libres, ligadas, sustituciones
2. Semántica de la LPO
    1. Interpretaciones sobre estructuras. Definición recursiva de funciones de interpretación
    2. Interpretación recursiva de fórmulas proposicionales. Definición de Tautología, Contingencia y Contradicción
    3. Interpretación de fórmulas de primer orden. Clausura Universal. Definición de juicios: Satisfactible, Lógicamente Válido y Consecuencia Lógica
    4. ) Propiedades algebraicas básicas, equivalencia, teoremas de cambios de variables y de sustitución. Identidad
    5. Formalización y análisis de propiedades sobre distintas realidades
3. Deducción Natural en LPO
    1. Reglas de derivación y heurísticas
    2. Definición inductiva del lenguaje de las derivaciones
    3. Análisis de casos de estudio
4. Corrección y Completitud de la LPO
    1. Nociones de corrección y completitud del sistema de pruebas
    2. Corrección del sistema
    3. Conjuntos consistentes e inconsistentes. Definición de teoría
    4. ) Noción de conjunto completo y consistencia maximal

## 5. Bibliografía Básica

1. D. van Dalen: Logic and Structure. Springer London, 5th Edition, (2013).

| Tema | Básica | Complementaria |
|---|---|---|
| Sintaxis de la Lógica de Primer Orden | (1) | (1) |
| Semántica de la Lógica Clásica de Primer Orden | (1) | (1) |
| Deducción Natural en Lógica de Primer Orden | (1) | |
| Corrección y Completitud de la Lógica Clásica de Primer Orden | (1) | (1) |
| Sistema Intuicionista | (1) | (1) |

### Complementaria


1. H. B. Curry: Foundations of mathematical logic. Dover Publications, 2nd Edition, (2010).
2. E. Lehman, F. Thomson Leighton, A. R. Meyer: Mathematics for Computer Science, (2017).


## 6. Conocimientos Recomendados

**Conocimientos Previos Exigidos** Curso Matemática Discreta y Lógica 1 (MDL1)

**Conocimientos Previos Recomendados** Inducción y Recursión (MDL1). Significado intuitivo de los conectivos y cuantificadores de Lógica de Primer Orden (MDL1). De acuerdo a los conocimientos previos necesarios, el curso podría desarrollarse en el segundo semestre.

# D. Programa de Estructuras de Datos y Algoritmos

## 1. Datos de la Actividad Curricular

- **Nombre**: Estructuras de Datos y Algoritmos
- **Área de formación**: Programación
- **Créditos**: 12

## 2. Objetivos

El objetivo de esta actividad curricular es introducir estructuras de datos básicas y sus algoritmos de manipulación, realizar un análisis de su eficiencia, e introducir el concepto de abstracción de datos para el diseño y la evaluación de algoritmos de porte mediano.

A nivel de los objetivos de aprendizaje, el estudiante será capaz de:

- Implementar y analizar algoritmos recursivos.
- Definir y manipular estructuras de datos lineales y arborescentes, tantto estáticas como dinámicas.
- Reconocer los conceptos de modularización, abstracción de datos, en- capsulamiento y Tipo Abstracto de Datos (TAD).
- Explicar la diferencia entre especificación, implementación y uso de TADs.
- Especificar diferentes TADs y ejemplificar su uso. Por ejemplo: Lista, Pila, Cola de Prioridad, Conjunto, Mapping y Grafo.
- Implementar TADs usando estructuras de datos, por ejemplo arreglos, estructuras de datos lineales y arborescentes de memoria dinámica, tablas de dispersión y árboles parcialmente ordenados.
- Elegir estructuras de datos adecuadas para implementar los TADs teniendo en cuenta requerimientos de eficiencia en tiempo de ejecución y espacio de almacenamiento.
- Definir nociones de eficiencia para aplicarlas al análisis de los algoritmos de las estructuras vistas.
- Identificar qué TADs se vinculan con la resolución de ciertos problemas.

## 3. Metodología de enseñanza

- Horas clase (teórico): 45
- Horas clase (práctico y laboratorio): 75
- Horas evaluación: 6
- Horas estudio: 54

**Total de horas de dedicación del estudiante: 180**

## 4. Temario

1. Iteración y recursión
    1. Implementación de invocaciones a procedimientos y funciones
    2. Implementación y uso de esquemas recursivos
    3. Análisis comparativo entre algoritmos recursivos e iterativos
2. Introducción al análisis de algoritmos
    1. Eficiencia en espacio de almacenamiento y tiempo de ejecución
    2. Tiempo de ejecución y orden del peor caso de algoritmos iterativos y recursivos
    3. Introducción al análisis del caso promedio
3. Estructuras de datos estáticas y dinámicas
    1. Estructuras de datos lineales. Distintos tipos de listas
    2. Estructuras de datos arborescentes. En particular, árboles binarios, binarios de búsqueda, árboles balanceados y árboles generales
    3. Tablas de dispersión (hashing)
    4. ) Montículos binarios (binary heap)
    5. Implementación de estructuras múltiples para resolver problemas con restricciones de eficiencia
4. Tipos abstractos de datos (TADs)
    1. El rol de la abstracción en el diseño de sistemas
    2. Especificación e implementación de TADs Distintos tipos de listas, pilas y colas

Conjuntos, multiconjuntos, funciones parciales (mappings, tablas) y colas de prioridad.

Grafos

3. Uso de TADs en la resolución de problemas de porte mediano

## 5. Bibliografía

| Tema | Básica | Complementaria |
|---|---|---|
| Iteración y recursión | (1) | (1,2) |
| Introducción al análisis de algoritmos | (1) | (3) |
| Estructuras de datos estáticas y dinámicas | (1) | (1,2,3) |
| Tipos abstractos de datos (TADs) | (1) | (3) |

### Básica

1. Mark A. Weiss. Data Structures and Algorithm Analysis in C (2nd Edition), (1996).

### Complementaria

1. B. W. Kernighan, D. M. Ritchie. El lenguaje de programación C (Spanish Edition), (2021).
2. H. M. Deitel, P. J. Deitel. Cómo programar en C/C++. Prentice-Hall Hispanoamericana, (1998).
3. G. Brassard, P. Bratley. Fundamentos de Algoritmia. Prentice Hall, (1998).

## 6. Conocimientos Recomendados

**Conocimientos Previos Exigidos** Matemática Discreta y Lógica 1. Introducción a la Programación.

**Conocimientos Previos Recomendados** Solo se requieren conocimientos de los cursos Matemática Discreta y Lógica 1, e Introducción a la Programación. Se ubicaría en el segundo semestre del primer año de la carrera.

# E. Programa de Taller de Introducción a la Seguridad Informática

## 1. Datos de la Actividad Curricular

- **Nombre**: Taller de Introducción a la Seguridad Informática
- **Área de formación**: Actividades integradoras
- **Créditos**: 6

## 2. Objetivos

Este curso se concibe como una aproximación inicial a la seguridad informática, para que los estudiantes que comienzan la carrera adquieran conceptos fundamentales de la ciberseguridad, reconozcan las características principales de esta disciplina y experimenten métodos y herramientas para la resolución de problemas concretos.

El curso cubre los fundamentos y propiedades básicas de seguridad informática (como confidencialidad, integridad y disponibilidad), y los principales tipos de ataques de los que puede ser objeto un sistema informático, así como los posibles métodos de protección, detección y políticas de seguridad que permitan evitar el daño al sistema o minimizar sus consecuencias. Complementando el contenido teórico, se brindarán una serie de talleres durante los cuales los estudiantes realizarán actividades en equipo que ilustren y permitan experimentar técnicas y herramientas de ciberseguridad concretas. Estos talleres tendrán una metodología de enseñanza activa y con sesgo lúdico. Se pueden realizar actividades competitivas, como capturas de bandera en escenarios sencillos, en donde los propios equipos pueden esconder cierta bandera en un ambiente, y a la vez descubrir la de otros grupos, lo que permite desempeñar roles tanto ofensivos como defensivos.

El objetivo principal de este taller es motivar a los estudiantes en el estudio de la ciberseguridad, por lo que se recomienda que las actividades de taller (y por lo tanto los temas que se aborden en esta segunda parte del curso) sean elegidas contemplando en la medida de lo posible los intereses de los estudiantes.

## 3. Metodología de enseñanza

- Horas clase (teórico): 15
- Horas clase (práctico y laboratorio): 40 Horas evaluación: 5
- Horas estudio: 30

**Total de horas de dedicación del estudiante: 90**

## 4. Temario

1. Fundamentos de la Seguridad Informática
    1. Motivación
    2. Definiciones (confidencialidad, integridad y disponibilidad)
    3. Algunos tipos de ataques comunes y mecanismos de protección
    4. ) Introducción a la privacidad y protección de datos personales
2. Talleres. Posibles temas:

Conceptos básicos de criptografía, motivación, definiciones y algunas herramientas.

Manejo elemental de consola y comandos básicos, scripting Programación web básica (HTML, CSS, javascript)

Uso básico de algunas herramientas de seguridad (nmap, tcpdump, ettercap, netcat, curl/wget, john the ripper, zap, etc)

## 5. Bibliografía

| Tema | Básica | Complementaria |
|---|---|---|
| Motivación | (1) | |

| | | |
|---|---|---|
| Definiciones | (1) | |
| Tipos de ataques y protección | (1) | (1) |
| Privacidad | (1) | (1) |

### Básica

1. W. Stallings, L. Brown; Computer Security: Principles and Practice, Pearson, 4th Edition, (2018).

### Complementaria

1. Centro Nacional de Respuesta a Incidentes de Seguridad Informática (CERTuy), AGESIC; Materiales Didácticos (videos, afiches, juegos y otras actividades) de la campaña “Seguro te conectás”; https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/ciudadania

## 6. Conocimientos previos exigidos y recomendados Conocimientos Previos Exigidos Ninguno

**Conocimientos Previos Recomendados** Solo se requieren conocimientos ya contemplados por las condiciones de ingreso a la carrera. Se ubicaría en el primer año de la carrera (en particular en su primer semestre).

# F. Programa de Criptografía Aplicada

## 1. Datos de la Actividad Curricular

- **Nombre**: Criptografía Aplicada
- **Área de formación**: Seguridad Computacional
- **Créditos**: 12

## 2. Objetivos

El objetivo de esta unidad curricular es que el estudiante conozca los fundamentos matemáticos de la criptografía, las principales primitivas criptográficas, identifique conceptos y propiedades fundamentales de la criptografía aplicada así como algunas malas prácticas que las hacen vulnerables en el uso.

A nivel de los objetivos de aprendizaje el estudiante será capaz de:

- Explicar el funcionamiento básico de los algoritmos de cifrado de bloques simétricos.
- Comparar y contrastar el cifrado de bloques y el cifrado de secuencias. Discutir el uso de funciones hash seguras para la autenticación de mensajes.
- Listar otras aplicaciones de funciones hash seguras.
- Explicar el funcionamiento básico de los algoritmos de cifrado de bloques asimétricos.
- Presentar una descripción general del mecanismo de firma digital y explicar el concepto de sobres digitales.
- Explicar la importancia de los números aleatorios y pseudoaleatorios en criptografía.

## 3. Metodología de enseñanza

- Horas clase (teórico): 48
- Horas clase (práctico y laboratorio): 24
- Horas evaluación: 6
- Horas estudio: 48

**Total de horas de dedicación del estudiante:126**

## 4. Temario

1. Confidencialidad con cifrado simétrico
    1. Cifrado simétrico
    2. Algoritmos de cifrado de bloques simétricos
    3. Cifrados de flujo
2. Autenticación de mensajes y funciones hash
    1. Autenticación mediante cifrado simétrico
    2. Autenticación de mensajes sin cifrado de mensajes
    3. Funciones hash seguras
    4. ) Otras aplicaciones de las funciones hash
3. Cifrado de clave pública
    1. Estructura de cifrado de clave pública
    2. Aplicaciones para criptosistemas de clave pública
    3. Requisitos para criptografía de clave pública
    4. ) Algoritmos de cifrado asimétrico
4. Firmas digitales y gestión de claves
    1. Firma digital
    2. Certificados de clave pública
    3. Intercambio de claves simétricas utilizando cifrado de clave pública
    4. ) Sobres digitales
5. Números aleatorios y seudoaleatorios
    1. El uso de números aleatorios
    2. Aleatorio versus pseudoaleatorio

## 5. Bibliografía

| Tema | Básica | Complementaria |
|---|---|---|
| Confidencialidad con cifrado simétrico | (1) | (1) |
| Autenticación de mensajes y funciones hash | (1) | (1) |
| Cifrado de clave pública | (1) | (1,2) |
| Firmas digitales y gestión de claves | (1) | (1) |
| Números aleatorios y seudoaleatorios | (1) | (1) |

### Básica

1. W. Stallings; Criptography and Network Security, Prentice Hall, (2006).

### Complementaria

1. W. Stallings, L. Brown; Computer Security: Principles and Practice, Pearson, 4th Edition, (2018).
2. R. Anderson; Security Engineering: A Guide to Building Dependable Distributed Systems, Ed. Wiley, 3rd. Edition, (2020).

## 6. Conocimientos Recomendados

**Conocimientos Previos Exigidos** Matemática Discreta y Lógica 1 y

2. Introducción a la Programación. Estructuras de Datos y Algoritmos.

**Conocimientos Previos Recomendados** Ninguno.

# G. Programa de Desarrollo Seguro de Aplicaciones

## 1. Datos de la UC

- **Nombre**: Desarrollo Seguro de Aplicaciones
- **Área de formación**: Seguridad Computacional
- **Créditos**: 12

## 2. Objetivos

Introducir los principales conceptos y metodologías asociadas a la seguridad en el desarrollo de aplicaciones. Se presentan y discuten amenazas específicas al dominio, poniendo especial énfasis en técnicas para el diseño seguro de aplicaciones, la validación y sanitización de datos de entrada.

## 3. Metodología de enseñanza

- Horas clase (teórico): 60
- Horas clase (práctico y laboratorio): 60
- Horas evaluación: 6
- Horas estudio: 54

**Total de horas de dedicación del estudiante: 180**

## 4. Temario

Requerimientos y estándares de seguridad Arquitectura y diseño

- Modelado de amenazas
- Características de seguridad y diseño
- Análisis de arquitectura Código
- Revisión de código - automatización
- Gestión de Dependencias
- Testing
  - Testing de seguridad
- Despliegue y mantenimiento
  - Test de penetración
  - Gestión de configuración y vulnerabilidades

| Tema | Básica | Complementaria |
|---|---|---|
| Requerimientos y estándares | (3) | (1) |
| Arquitectura y diseño | (1) (2) | (1-3) |
| Código | (1) (2) | (1-3) |

## 5. Bibliografía Básica

1. D. Fisher, Application Security Program Handbook, 2022.
2. L. Bell, M. Brunton-Spall, R. Smith, J. Bird, Application Security: Enabling Security in a Continuous Delivery Pipeline, 2017.
3. OWASP ASVS, https://github.com/OWASP/ASVS/.

## Complementaria

1. BSIMM Framework, https://www.bsimm.com/content/dam/bsimm/reports/bsimm12-foundations.pdf.
2. NIST, Secure Software Development Framework SSDF, https://csrc.nist.gov/Projects/ssdf.
3. OWASP SAMM, https://owaspsamm.org
4. OWASP Top 10, https://owasp.org/www-project-top-ten/
5. SANS Top 25 software errors, https://www.sans.org/top25-software- errors/

## 6. Conocimientos previos exigidos y recomendados Conocimientos Previos Exigidos Estructuras de Datos y Algoritmos.

**Conocimientos Previos Recomendados** Desarrollo de aplicaciones, en particular aplicaciones web. Conocimientos generales de metodologías de desarrollo.

# H. Programa de Taller de Programación segura

1. **Datos de la UC**

- **Nombre**: Taller de Programación segura
- **Área de formación**: Seguridad Computacional
- **Créditos**: 12

2. **Objetivos**

Introducir técnicas y herramientas, metodológicas y tecnológicas, para la verificación de seguridad de aplicaciones. El taller constará de dos módulos donde se ejercitarán prácticas ofensivas y defensivas respectivamente. Se pretende mediante actividades prácticas que los estudiantes incorporen los conocimientos para la ejecución de análisis de seguridad o test de penetración, así como aprender a utilizar herramientas y tecnologías de seguridad para la identificación de vulnerabilidades durante el desarrollo y despliegue de aplicaciones.

3. **Metodología de enseñanza**

El dictado de la unidad se basa en la presentaciones teóricas donde se introduce un taller o práctica a realizar, luego se realizan clases de consultas con los estudiantes/grupos para evaluar el avance y alcance de la práctica. Finalmente se evalúan los resultados de cada una de las prácticas mediante evaluaciones y/o presentaciones de los trabajos.

4. **Temario**

Práctica ofensiva

- Objetivo: uso de métodos y herramientas para la aplicación de tests de penetración y similares propios del enfoque DAST (Dynamic Application Security Testing)
- Ejemplo de herramientas: OWASP ZAP, Burp Suite, Greenbone OpenVAS

Práctica defensiva

- Objetivo: se pondrá foco en prácticas que permiten aplicar controles a lo largo de todo el ciclo de desarrollo, en particular para realizar verificaciones tanto con el enfoque DAST como con el enfoque SAST (Static Application Security Testing)
- Ejemplo de herramientas: OWASP ZAP, Sonarqube, OWASP Dependency Check, Kube Hunter, Kube Bench

| Tema | Básica | Complementaria |
|---|---|---|
| Práctica ofensiva | (1) (2) | (1-3) |
| Práctica defensiva | (1) (2) | (1-3) |

5. **Bibliografía Básica**


1. D. Fisher, Application Security Program Handbook, 2022.
2. L. Bell, M. Brunton-Spall, R. Smith, J. Bird, Application Security: Enabling Security in a Continuous Delivery Pipeline, 2017.


## Complementaria


1. OWASP WSTG, https://owasp.org/www-project-web-security-testing- guide/.
2. OWASP Top 10, https://owasp.org/www-project-top-ten/.
3. SANS Top 25 software errors, https://www.sans.org/top25-software- errors/.

6. **Conocimientos previos exigidos y recomendados Conocimientos Previos Exigidos Desarrollo Seguro de Aplicaciones.**

**Conocimientos Previos Recomendados** Vulnerabilidades comunes en aplicaciones. Conocimientos de desarrollo de aplicaciones

# I. Programa de Redes de Computadoras

## 1. Datos de la Actividad Curricular Nombre: Redes de Computadoras

- **Área de formación**: Arquitectura, Sistemas Operativos y Redes de Computadoras
- **Créditos**: 8

## 2. Objetivos

El objetivo de este curso es introducir al estudiante en los conceptos de comunicación de datos en redes de computadoras. Se estudian los modelos de referencia OSI y TCP/IP, y las funcionalidades de cada capa. Se presentan los principales protocolos en la capa de aplicación (DNS, SMTP, HTTP, etc.), en la capa de transporte (TCP y UDP), en la capa de red (IPv4, IPv6, ICMP), y en la capa de enlace (ethernet, arp). Adicionalmente, se presentan conceptos básicos de las redes inalámbricas (WiFi).

## 3. Metodología de enseñanza

- Horas clase (teórico): 40
- Horas clase (práctico y laboratorio): 40
- Horas evaluación: 5
- Horas estudio: 35

**Total de horas de dedicación del estudiante**: 120

## 4. Temario

1. Introducción
    1. Introducción general a los temas del curso
    2. Modelos de circuitos virtuales y de datagramas
    3. Presentación del modelo de capas OSI de ISO y TCP-IP
2. Capa de aplicación
    1. Presentación de aplicaciones tradicionales que dan soporte a Inter- net (DNS, SMTP, HTTP, entre otras)
    2. Modelos Cliente-Servidor y Peer-to-Peer
3. Capa de transporte
    1. Servicios ofrecidos a la capa superior
    2. Comunicación extremo a extremo entre procesos, multiplexación, interfaz de programación de*sockets*.
    3. Transporte confiable y no confiable
4. Funcionamiento del User Datagram Protocol (UDP) y del Transport Control Protocol (TCP).
5. Capa de red
    1. Servicios ofrecidos a la capa superior
    2. Comunicación extremo a extremos entre sistemas, enrutamiento y reenvío
    3. Descripción del Internet Protocol (IP)
    4. Subredes y numeración
    5. Algoritmos de enrutamiento de vector-distancia y de estado del enlace
    6. Enrutamiento jerárquico, comunicaciones *broadcast* y *multicast g* ) Protocolo IPv6.
6. Capa de enlace
    1. Servicios ofrecidos a la capa superior
    2. Comunicación entre vecinos, detección y corrección de errores
    3. Medios punto a punto y medios compartidos
    4. ) Direcciones de capa de enlace, redes de área local

## 5. Bibliografía

| Tema | Básica | Complementaria |
|---|---|---|
| Introducción | (1) | (1, 2) |

| | | |
|---|---|---|
| Capa de aplicación | (1) | (1, 2) |
| Capa de transporte | (1) | (1, 2) |
| Capa de red | (1) | (1, 2) |
| Capa de enlace | (1) | (1, 2) |

### Básica

1. J. Kurose, K. Ross; Redes de Computadoras: Un Enfoque Descendente; Ed. Pearson; 7th Edition (2017).

### Complementaria

1. A. Tanenbaum; Computer Networks; 5th Edition (2010).
2. D. Comer; Internetworking with TCP/IP Vol. I: Principles, Protocols, and Architecture; 5th Edition (2005).

## 6. Conocimientos previsos exigidos y recomendados

**Conocimientos Previos Exigidos** Se requieren conocimientos de Arquitectura de Sistemas, Sistemas Operativos y Programación.

**Conocimientos Previos Recomendados** Nociones de física y matemática.

# J.Programa de Seguridad en Sistemas Operativos

## 1. Datos de la Actividad Curricular Nombre: Seguridad en Sistemas Operativos

- **Área de formación**: Seguridad Computacional
- **Créditos**: 12

## 2. Objetivos

El objetivo de este curso es introducir conceptos fundamentales de seguridad en Sistemas Operativos. Se presentan tanto amenazas específicas y tipos de ataque como mecanismos de identificación y autenticación. Se pone particular énfasis en la gestión de contraseñas y en la implementación de los mecanismos de control de acceso y de auditoría provistos por los sistemas operativos. Se presenta el concepto de computación confiable y de seguridad multinivel.

A nivel de los objetivos de aprendizaje el estudiante será capaz de:

- Discutir los cuatro métodos generales para autenticar la identidad de un usuario.
- Explicar el mecanismo mediante el cual se utilizan contraseñas hash para la autenticación de usuarios.
- Presentar una descripción general de la autenticación de usuarios basada en tokens.
- Explicar cómo se ubica el control de acceso en el contexto más amplio que incluye autenticación, autorización y auditoría.
- Distinguir entre sujetos, objetos y derechos de acceso.
- Discutir los conceptos principales del control de acceso basado en roles y el basado en atributos.
- Enumerar los pasos necesarios en el proceso de aseguramiento de un sistema.
- Enumerar los pasos básicos utilizados para asegurar el sistema operativo base.
- Explicar algunos aspectos específicos de la seguridad de los sistemas Unix/Linux.
- Explicar algunos aspectos específicos de la seguridad de los sistemas Windows.
- Enumerar los pasos necesarios para mantener la seguridad en los sistemas virtualizados.
- Explicar el modelo Bell-LaPadula y su relevancia para la computación confiable.

Resumir otros modelos formales de seguridad informática. Comprender el concepto de sistemas confiables.

Enumerar y explicar las propiedades de un monitor de referencia y explicar las relación entre un monitor de referencia y una base de datos del kernel de seguridad.

Presentar una descripción general de la aplicación de la seguridad multinivel al control de acceso basado en funciones.

## 3. Metodología de enseñanza

- Horas clase (teórico): 60
- Horas clase (práctico y laboratorio): 60
- Horas evaluación: 6
- Horas estudio: 54

**Total de horas de dedicación del estudiante: 180**

## 4. Temario

1. Autenticación
    1. Principios de autenticación de usuario
    2. Autenticación de usuarios basada en secretos y en tokens
    3. Mecanismos biométricos
    4. ) Autenticación remota
2. Control de acceso
    1. Principios de control de acceso
    2. Sujetos, objetos y permisos
    3. Control de acceso discrecional (DAC)
    4. ) Control de acceso basado en roles (RBAC)
    5. Control de acceso basado en atributos (ABAC)

*f* ) Gestión de identidades, credenciales y de acceso

3. Seguridad de Sistemas Operativos
    1. Planificación de la seguridad de SO y Hardening
    2. Mantenimiento: Logging y Backup
    3. Seguridad Linux/Unix
    4. ) Seguridad Windows
    5. Seguridad de sistemas de virtualización

4. Computación confiable y Seguridad Multinivel
    1. El modelo Bell-LaPadula para seguridad computacional
    2. Otros modelos
    3. El concepto de modelo confiable
    4. ) Aplicaciones de seguridad multinivel

| Tema | Básica | Complementaria |
|---|---|---|
| Autenticación | (1) | (1) |
| Control de acceso | (1) | (1) |
| Seguridad de Sistemas Operativos | (1) | (1) |
| Computación confiable y Seguridad Multinivel | (1) | (1) |

## 5. Bibliografía Básica

1. W. Stallings, L. Brown; Computer Security: Principles and Practice, Pearson, 4th Edition, (2018).

**Complementaria**

1. Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Editon.

## 6. Conocimientos previsos exigidos y recomendados

**Conocimientos Previos Exigidos** Estructuras de Datos y Algortimos, Arquitectura de Sistemas, Sistemas Operativos.

**Conocimientos Previos Recomendados** Ninguno.

# K. Programa de Seguridad en Redes de Computadoras

## 1. Datos de la Actividad Curricular Nombre: Seguridad en Redes de Computadoras

- **Área de formación**: Seguridad Computacional
- **Créditos**: 12

## 2. Objetivos

El objetivo de este curso es introducir al estudiante en los conceptos básicos de la seguridad informática de redes de datos TCP/IP. El curso está orientado a técnicos encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas, con el objetivo de desarrollar, ampliar o mejorar las plataformas de comunicación de datos. Al finalizar el curso el estudiante habrá adquirido los conceptos básicos necesarios para identificar las posibles amenazas que puede sufrir una red de datos TCP/IP y establecer los mecanismos de protección adecuados.

## 3. Metodología de enseñanza

- Horas clase (teórico): 60
- Horas clase (práctico y laboratorio): 60
- Horas evaluación: 6
- Horas estudio: 54

**Total de horas de dedicación del estudiante**: 180

## 4. Temario

1. Problemas de Seguridad de los protocolos TCP/IP
    1. Autenticación del origen (IP spoofing)
    2. Interacción IP/MAC, ARP spoofing
    3. Ataques a protocolo de ruteo, ICMP *d* ) TCP session Hijacking, SYN Flooding *e*) Capa de Aplicación: Servicio DNS

*f* ) VLAN

2. Redes inalámbricas (WiFi)
    1. Requerimientos de seguridad (autenticación, control de acceso, confidencialidad, integridad)
    2. WEP, WPA, WPA2, EAP, 802.1X
3. Seguridad IP (IPSec)
    1. Asociaciones de Seguridad (SA)

2. Modos de funcionamiento (túnel y transporte)
3. Protocolo AH y ESP (encabezados y servicios que ofrecen)
4. ) IPSec Key Management (IKE)
5. IPsec y filtrado

4. VPN
    1. ¿Qué es una VPN? VPN sobre Internet
    2. Implementación de VPN
5. Firewalls
    1. Definición. ¿Qué puede hacer y qué NO un firewall?
    2. Filtrado de paquetes, con y sin estados. Generando reglas de filtrado
    3. Logging
    4. ) Arquitecturas de Firewall
    5. Tipos de Firewall

*f* ) Servicios Proxy y NAT

6. Sistemas de detección y prevención de intrusiones (IDS/IPS)
    1. Definición
    2. Clasificación y formas de detección
    3. Falsos positivos y negativos
    4. ) ¿Acciones automáticas? Dónde monitorizar (sensar)

    5. Otro tipo de sensores (honeypots)
7. Diseño de un perímetro seguro
    1. Identificación de activos a proteger
    2. Identificación de fronteras
    3. Separación e identificación de zonas de seguridad

## 5. Bibliografía

| Tema | Básica | Complementaria |
|---|---|---|
| Redes TCP/IP | (1) | (1) |
| Problemas de Seguridad de los protocolos TCP/IP | (1) | (1) |
| Redes inalámbricas | (1) | (2) |
| Seguridad IP (IPSec) | (1) | (1) |
| VPN | (1) | (1) |
| Firewalls | (1) | (1, 3) |
| Sistemas de detección y prevención de intrusiones (IDS/IPS) | (1) | (1) |
| Diseño de un perímetro seguro | (1) | (1, 3) |

### Básica

1. Gollman, Dieter (2009), Computer Security, Wiley Computing Publishing, 3rd. Editon.

### Complementaria

1. Garfinkel, S.; Spafford, G. & Schuartz, A. (2003); Practical Unix & Internet Security; Ed. O'Reilly; 3rd Edition.
2. Edney, J.; Arbaugh, W. (2004); Real 802.11 Security - Wi-Fi Protected Access and 802.11i. Addison-Wesley, 2004.
3. Zwicky, E.; Cooper, S. & Chapman, B. (2000); Building Internet Fi- rewalls; Ed. O'Reilly; 2nd Editon.

## 6. Conocimientos previos exigidos y recomendados Conocimientos Previos Exigidos Redes de Computadoras.

**Conocimientos Previos Recomendados** Ninguno.

# L. Programa de Taller de Técnicas y Procedimientos

## 1. Datos de la Actividad Curricular Nombre: Taller de Técnicas y Procedimientos

- **Área de formación**: Actividades integradoras
- **Créditos**: 7

## 2. Objetivos

El Taller de Técnicas y procedimientos es un curso fundamentalmente práctico, basado en el uso de tecnologías sobre las cuales se realizan diferentes laboratorios. En dichos laboratorios los estudiantes pueden aprender y profundizar sobre el uso de herramientas específicas de seguridad. El objetivo principal es llevar a la práctica conceptos básicos de seguridad computacional

En el transcurso del Taller, se implementan servicios y funcionalidades de seguridad, que en general son menospreciados frente a aspectos funcionales del desarrollo de software tradicional, por ejemplo, desarrollando funciones de autenticación, plugins para herramientas de seguridad, modificando y configurando funcionalidades complejas de los sistemas operativos, utilización de criptografía en los canales de comunicación, entre otros.

Este taller representa un complemento esencial a los conceptos teórico/práctico que son introducidos en los distintos cursos del área de formación Seguridad Computacional, aportando además una visión fuertemente focalizada en el uso de métodos técnicos empleados en el sector profesional, convirtiéndose así en un área de especialización cada vez más requerida por diferentes tipos de organizaciones.

## 3. Metodología de enseñanza

La metodología de enseñanza utilizada es la de aprendizaje basado en problemas, donde se presenta una situación que los participantes, en forma individual o grupal, deberán resolver. Se utilizan casos de la vida real, los cuales se deberán estudiar para luego proponer soluciones utilizando diferentes herramientas.

Durante el transcurso de cada laboratorio se realizan distintas tareas, desde la definición del ambiente de trabajo, por ejemplo utilizando máquinas y escenarios virtuales, hasta la implementación de soluciones utilizan- do librerías de seguridad de diferentes lenguajes de programación. Además se pueden utilizar técnicas de juegos de roles, con el objetivo de ampliar la experiencia de los estudiantes y la habilidad para resolver problemas de la vida real.

Dada la modalidad del curso, se requiere un constante y cercano seguimiento por parte de los docentes en cuanto a las soluciones a implementar, ya que las mismas varían entre los diferentes grupos de estudiantes. Es necesario mantener acotado el alcance de cada tarea, sin descuidar el cumplimiento de los requerimientos básicos de cada laboratorio.

- Horas clase (teórico): 10
- Horas clase (práctico y laboratorio): 20
- Horas evaluación: 5
- Horas estudio: 20
- Horas resolución ejercicios/prácticos: 50

**Total de horas de dedicación del estudiante**: 105

## 4. Temario

El temario de base para esta taller lo constituye los conceptos funda- mentales de criptografía aplicada, seguridad de sistemas operativos y de redes, y los principios de desarrollo de código seguro. Los trabajos prácticos o laboratorios podrán varias en diferentes ediciones del taller, pero el objetivo es cubrir aspectos ingenieriles de cada unas de las mencionadas áreas

## 5. Bibliografía

La bibliografía será especificada en cada laboratorio, para guiar al estudiante en la temática objetivo cubierta y en el uso de las herramientas necesarias para el desarrollo de los mismos.

## 6. Conocimientos previos exigidos y recomendados

**Conocimientos Previos Exigidos** Conocimientos de redes de computadoras, sistemas operativos y programación.

**Conocimientos Previos Recomendados** Dadas las características de esta unidad curricular, se recomienda contar con claros fundamentos en relación con la Seguridad Computacional, ya que la dinámica del taller implica aplicarlos a determinadas realidades de laboratorio.

# M. Programa de Gestión de la Seguridad de la Información

## 1. Datos de la UC

- **Nombre**: Gestión de la Seguridad de la Información
- **Área de formación**: Gestión de Seguridad
- **Créditos**: 12
- **Carga horaria semanal**: 6

## 2. Objetivos

Introducir a los participantes en los principales conceptos y metodologías asociadas a la gestión de la ciberseguridad, contemplando el marco normativo internacional y nacional existente. Llevar a la práctica una metodología de rápida aplicación para la implementación de un Sistema de Gestión de Seguridad de la Información. Presentar metodologías y buenas prácticas concretas para la gestión de riesgos, gestión de incidentes, gestión de la continuidad de la seguridad y gestión de vulnerabilidades. Se abarcarán las principales conceptos entorno a la familia de normas ISO/IEC 27000 y el marco de ciberseguridad de NIST.

## 3. Metodología de enseñanza

- Horas clase (teórico-práctico): 80
- Horas estudio: 35
- Horas resolución ejercicios/prácticos: 40
- Horas proyecto final/monografía: 25

**Total de horas de dedicación del estudiante**: 180

## 4. Temario

1. Introducción
    1. Definiciones y conceptos de gestión de ciberseguridad
    2. Confidencialidad, Integridad y Disponibilidad
    3. Marco normativo nacional e internacional
2. Sistema de Gestión de Seguridad de la Información
    1. Metodologías de implantación

2. Principales desafíos a enfrentar
3. c. Herramientas disponibles que faciliten la implantación

3. Gestión de Riesgos
    1. Introducción al proceso de gestión de riesgos
    2. Metodologías de análisis de riesgo
    3. Tratamiento de riesgos
4. Gestión de incidentes
    1. Definición de incidentes
    2. Procesos de clasificación, análisis, tratamiento, resolución y cierre
    3. Control de flujos de información y procesos.
    4. ) Modelos organizacionales de Centros de Respuesta y Centros Ope- rativos de Seguridad
5. Gestión de la continuidad operativa
    1. Componentes del negocio
    2. Tipos de desastres que deben considerarse
    3. Análisis de Impacto del Negocio
    4. ) Desarrollo de estrategias de mitigación

## 5. Bibliografía

| Tema | Básica | Complementaria |
|---|---|---|
| Sistemas de Gestión de SI | (1) | (1,2) |
| Gestión de Riesgos | (3) | (1) |
| Gestión de incidentes | (5) | (3) |
| Gestión de la continuidad operatival | (1) | (1) |

### Básica


1. H. Tipton, M. Krause, Information Security Management Handbook 6th, 2008.
2. Thomas Peltier, Information Security Policies, Procedures and Standards, 2002.
3. L. Hayden, IT Security Metrics. A Practical Framework for Measuring Security and Protecting Data, 2010.
4. Proyecto AMPARO, Manual básico de Gestión de Incidentes de Segu- ridad Informática, 2012
5. Susan Snedaker, Business Continuity and Disaster Recovery for IT professionals, 2007.


### Complementaria


1. NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, 2018
2. AGESIC, Marco de Ciberseguridad, 2019.
3. H. Allen et al, Structuring the Chief Information Security Officer Organization, CERT Division, Software Engineering Institute, Carnegie Mellon University.
4. C. Zimmerman, Ten Strategies of a World-Class Cybersecurity Operations Center, MITRE Corporation.


## 6. Conocimientos previos exigidos y recomendados

**Conocimientos Previos Exigidos** Taller de Introducción a la Seguridad Informática.

**Conocimientos Previos Recomendados** Definición y aplicación de políticas y procedimientos de Seguridad de la Información y computacional.

# N. Programa de Introducción al Análisis Forense Digital

## 1. Datos de la Actividad Curricular Nombre: Introducción al Análisis Forense Digital

- **Área de formación**: Especialización en Ciberinteligencia
- **Créditos**: 10

## 2. Objetivos

El objetivo de este curso es introducir al estudiante en los conceptos básicos del análisis forense informático. El curso está orientado a técnicos encargados de diseñar y/o implantar mecanismos de seguridad en sus empresas. Al finalizar el curso el alumno habrá adquirido los conceptos técnicos básicos necesarios en lo que respecta a las metodologías de análisis y el tratamiento y/o adquisición de la evidencia digital.

## 3. Metodología de enseñanza

- Horas clase (teórico): 60
- Horas clase (práctico y laboratorio): 60
- Horas evaluación: 6
- Horas estudio: 36

**Total de horas de dedicación del estudiante**: 162

## 4. Temario

1. Bases y Motivación
    1. Introducción
    2. Motivación, definiciones y objetivos del análisis forense informático
    3. Principios y usos del análisis informático forense
2. Evidencia digital
    1. Tipos de evidencia
    2. Propiedades
    3. Fuentes de obtención de evidencias
    4. ) Cadena de custodia
3. Tipos de análisis forense
    1. Análisis post-mortem
    2. Live análisis
    3. Análisis On-Sitey en el laboratorio
4. Metodologías para el análisis forense digital
    1. Identificación

2. Preservación
3. Análisis
4. ) Presentación
5. Herramientas de soporte a la metodología

5. Anti-forensia
    1. Problemáticas y desafíos del análisis forense informático
    2. Técnicas anti-forenses
    3. Clasificación de métodos anti-forenses
    4. ) Herramientas anti-forenses

## 5. Bibliografía

| Tema | Básica | Complementaria |
|---|---|---|

| | | |
|---|---|---|
| Bases y Motivación | (1) | (1) |
| Evidencia digital | (1) | (1) |
| Tipos de análisis forense | (1) | (1) |
| Metodologías para el análisis forense digital | (1) | (1) |
| Anti-forensia | (1) | (1) |

### Básica

1. Joakim Kävrestad, Fundamentals of Digital Forensics: Theory, Methods, and Real-Life Applications, Springer London, 2nd Edition, (2020).

### Complementaria

1. Eoghan Casey (Editor), Handbook of Digital Forensics and Investigation, Elsevier, 1st Edition, (2010).

## 6. Conocimientos previstos exigidos y recomendados

**Conocimientos Previos Exigidos** Redes de Computadores, Seguridad en Redes, Seguridad en Sistemas Operativos y Seguridad de Aplicaciones.

**Conocimientos Previos Recomendados** Manejo fluido de conceptos esenciales de arquitectura de computadores y sistemas operativos.

# Ñ. Programa de Configuración y Administración Segura de Sistemas

## Ñ.1. Datos de la Actividad Curricular

- **Nombre**: Configuración y Administración Segura de Sistemas
- **Área de formación**: Electiva del Perfil Administración Segura de Sistemas
- **Créditos**: 10

### Ñ.2. Objetivos

La administración de sistemas se encarga de garantizar la correcta, ininterrumpida y segura operación de los equipos, redes y servicios de una infraestructura de un nivel de complejidad relativamente alto. Las tareas que suelen incluirse en esta disciplina pueden ser: instalación y configura- ción de sistemas de hardware y software (tanto en instalaciones propias de las organización como en la nube); administración de redes; monitoreo de la infraestructura; diagnóstico y solución de problemas; respuesta a incidentes y recuperación ante fallas; auditorías; etc.

Esta actividad curricular profundiza los conocimientos de sistemas operativos, redes y seguridad computacional vistos a lo largo de la carrera, brindándole a los estudiantes capacidades de alto nivel y una visión más global del rol del administrador de sistemas con un foco en operación segura de las infraestructuras. Los objetivos de aprendizaje que el estudiante podrá alcanzar incluyen:

- Entender el rol de un administrador de sistemas en una organización. Estar familiarizado con aspectos de la administración de equipos de hardware, como su adquisición, mantenimiento y aseguramiento físico. Ser capaz realizar el *hardening* de sistemas operativos.
- Conocer diferentes arquitecturas de red y sus efectos en la ciberseguridad.
- Manejar tecnologías de virtualización y ser capaz de desplegar servicios en la nube.
- Estar familiarizado con técnicas y herramientas que garantizan alta disponibilidad.
- Montar sistemas de monitoreo y alerta de la infraestructura.
- Ser capaz de responder frente a fallas o incidentes de seguridad, de modo de garantizar la continuidad del negocio.
- Integrar la ciberseguridad como un aspecto fundamental del correcto mantenimiento y operación de los sistemas de una organización.

### Ñ.3. Metodología de enseñanza

- Horas clase (teórico): 50
- Horas clase (práctico y laboratorio): 40
- Horas evaluación: 5
- Horas estudio: 55

### Total de horas de dedicación del estudiante: 150

### Ñ.4. Temario

1. Fundamentos de la administración de sistemas
    1. Motivación, cometidos y tareas de la administración de sistemas
    2. Consideraciones éticas de la disciplina
    3. Privacidad y protección de datos personales en la administración de sistemas
2. Infraestructura física
    1. Adquisición, instalación y mantenimiento de hardware
    2. Sistemas de inventario
    3. Seguridad física
3. Administración de Sistemas Operativos
    1. Políticas de gestión de usuarios
    2. Servicios de directorio
    3. *Hardening*
4. Administración de Redes
    1. Arquitecturas seguras de redes
    2. Segmentación e identificación de zonas de seguridad
    3. Defensa en profundidad

    4. ) Redes definidas por software, micro-segmentación, arquitecturas

*zero trust*

5. Virtualización y nube
    1. Tecnologías de virtualización y *containers*
    2. *Cloud computing*
    3. *Infrastructure as Code* y DevOps
6. Alta disponibilidad y tolerancia a fallos
    1. Mecanismos y herramientas de redundancia
    2. Diseño y gestión de respaldos
7. Diagnóstico y resolución de problemas
    1. Monitoreo y sistemas de alerta
    2. Auditoría, logging y gestión de eventos e información de seguridad (SIEMs)
    3. Respuesta ante fallas e incidentes de seguridad

| Tema | Básica | Complementaria |
|---|---|---|
| Fundamentos de la administración de sistemas | (1) | (1) |
| Infraestructura física | (1) | (1) |
| Administración de Sistemas Operativos | (1) | (1, 2) |
| Administración de Redes | (1) | (1) |
| Virtualización y nube | (1) | (1, 4) |
| Alta disponibilidad y tolerancia a fallos | (1) | (1) |
| Diagnóstico y resolución de problemas | (1) | (1, 3) |

## Ñ.5. Bibliografía Básica

1. J. Davis; Modern System Administration; 1st Edition (2022).

## Complementaria

1. T. Hein, E. Nemeth, G. Snyder, B. Whaley, D. Mackin; UNIX and Linux System Administration Handbook; 5th Edition (2017).
2. B. Dauti; Windows Server 2022 Administration Fundamentals; 3rd Edition (2022).
3. M. Julian; Practical Monitoring: Effective Strategies for the Real World; 1st Edition (2017).
4. G. Kim, P. Debois, J. Willis, J. Humble; The DevOps Handbook: How to Create World-Class Agility, Reliability, & Security in Technology Organizations; 2nd Edition (2021)

## Ñ.6. Conocimientos previos exigidos y recomendados

**Conocimientos Previos Exigidos** Sistemas Operativos, Seguridad en Sistemas Operativos, Redes de Computadoras, Seguridad en Redes de Computadoras.
**Conocimientos Previos Recomendados** Criptografía Aplicada, Gestión de la Seguridad de la Información.