Síntesis del Plan de Estudios de la Carrera Analista Técnico en Ciberseguridad

Autor

Área de Seguridad de la información de Agesic

Fecha de creación

23/01/2023

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 e impulsar 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, que actualmente se presenta en el sector.

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 del país 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.

Las instituciones de educación públicas y privadas interesadas en implementar una tecnicatura de Ciberseguridad en base a esta currícula, podrán comunicarse con el área de Seguridad de la información de Agesic a través del siguiente correo:

ciberseguridad@agesic.gub.uy

Introducción

Keywords: 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 Ingeniería, Universidad de la República, Uruguay

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

La ciberseguridad como disciplina

La ciberseguridad [Joi18] es una disciplina basada en las tecnologías de la información y la comunicación (TIC), que involucra tecnología, personas, información y procesos, en la que se trata de garantizar que los sis- temas 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.

Asociado al enorme crecimiento en los últimos años del uso de las TIC, es también cada vez mayor 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 de las nuevas normativas existentes en nuestro país y en el mundo, para lograr el objetivo de seguridad. Esto ha generado un aumento en la demanda de profesionales especializados en seguridad informática que, tanto a nivel mundial como en nuestro país, está lejos de ser satisfecha. Para comenzar a 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 presente 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 es- tar 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 Sección 2 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 dicta- do 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 *typesafe* 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 principales, 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 adecua- dos 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

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 re- quiere 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 Inciden- tes, 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 mînimo 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.

6.1. 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 for- mación, es 186. De éstos, 66 corresponden a formación básica en matemá- tica y computación (31 %), mientras que 120 consisten en formación en ciberseguridad propiamente (57 %). El resto de los 210 créditos se consi- guen 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 Cuadro 1

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 completa- do 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 calcula- dos 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 intrumentos de evalua- ción 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 resposnables 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 introduce 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 apli- car 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 familia- rice con 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.

- 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 for- mar 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 estudian- te 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 ci- berseguridad, con especial énfasis en aspectos vinculados al derecho administrativo e informático. El curso contempla: consideraciones ge- nerales 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 iden- tifiquen 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 traba- jo 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 mé- todos 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 am- biente 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 co- munes 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 ins- titución 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 estu-diantes 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 seguri- dad, Análisis Forense Digital y Análisis predictivo de seguridad usando Aprendizaje Automático.

- Administración segura de sistemas: Cursos posibles: Configura- ción 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 conte- nidos 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 activida- des curriculares relevantes de la implementación considerada, incluyendo en cada caso: el nombre de la actividad, el área de formación a la que per- tenece, 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

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 12 créditos	Estructuras de Datos y Algoritmos 12 créditos	Desarrollo seguro de aplicaciones 12 créditos	Taller de programación segura 12 créditos	Pasantía 10 créditos	Proyecto Final 20 créditos
Arquitectura de Computadoras 8 créditos	Sistemas Operativos 8 créditos	Redes de computadoras 8 créditos	Seguridad en Redes de Computadoras 12 créditos	Electiva 1 10 créditos	Electiva 2 10 créditos
Matemática Discreta y Lógica 1 6 créditos	Matemática Discreta y Lógica 2 6 créditos	Seguridad de Sistemas Operativos 12 créditos	Taller de Técnicas y Procedimientos 6 créditos	Electiva 3 10 créditos	Electiva 4 10 créditos
Taller de Introducción a la Seguridad Informática 6 créditos	Introducción a las Bases de Datos 6 créditos	Criptografía Aplicada 12 créditos	Gestión de la Seguridad de la Información 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 seguri- dad 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 realis- tas 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 de- dicados 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 invo- lucrada. 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 Machi- nery, 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.