UNIVERSIDAD DE PUERTO RICO
RECINTO DE RÍO PIEDRAS

Certificación Núm. 73
Año Académico 2018-2019

Yo, Claribel Cabán Sosa, Secretaria del Senado Académico del Recinto de Río Piedras, Universidad de Puerto Rico, **CERTIFICO QUE**:

El Senado Académico, en la reunión ordinaria celebrada el 21 de marzo de 2019, acordó por consentimiento unánime:

- Aprobar la **Propuesta de Concentración Menor en Seguridad Cibernética** del Departamento de Ciencias de Cómputos de la Facultad de Ciencias Naturales.

- La Propuesta forma parte de esta Certificación.

Y para que así conste, expido la presente Certificación bajo el sello de la Universidad de Puerto Rico, Recinto de Río Piedras, a veinticinco días del mes de marzo del año dos mil diecinueve.

Dra. Claribel Cabán Sosa
Secretaria del Senado

yrs

Certifico correcto:

Dr. Luis A. Ferrao Delgado
Rector Interino

Anejo

Senado Académico
Secretaría

PO Box 21322
San Juan PR, 00931-1322
Tel. 787-763-4970
Fax 787-763-3999

Departamento de Ciencia de Cómputos
Facultad de Ciencias Naturales
Recinto de Río Piedras
Universidad de Puerto Rico

Propuesta de Concentración Menor en Seguridad Cibernética

A tenor con la Certificación Núm. 69, 2013-2014, de la Junta de Gobierno

Aprobado por el Comité de Asuntos Académicos
5 de marzo de 2019

Aprobado por el Senado Académico
21 de marzo de 2019
(Certificación Núm. 73, Año Académico 2018-2019, del Senado Académico)

Propuesta de Concentración Menor en Seguridad Cibernética
A tenor con la Certificación Núm. 69 2013-2014

Departamento de Ciencia de Cómputos
Facultad de Ciencias Naturales
Recinto de Río Piedras
Universidad de Puerto Rico

A. Título de la Concentración Menor: Concentración Menor en Seguridad Cibernética.

El departamento de Ciencia de Cómputos (CCOM) de la Facultad de Ciencia Naturales (CN) del Recinto de Río Piedras de la Universidad de Puerto Rico propone una Concentración Menor en Seguridad Cibernética a tenor con la implantación de la Certificación Núm. 69 2013-2014. La Concentración Menor cumple con los metas y objetivos de la Universidad de Puerto Rico de proveer al estudiante "alternativas curriculares destinadas a enriquecer y diversificar su experiencia y formación sub graduada" y "desarrollar programas innovadores que apoyen y contribuyan a la transformación y progreso de la sociedad puertorriqueña, la economía y calidad de vida".

B. Objetivos y Justificaciones

La seguridad cibernética, también conocida como seguridad en computadoras, ciberseguridad, y seguridad en tecnología de la información es el conjunto de tecnologías, procesos, y prácticas diseñadas para proteger computadoras, redes de computadoras y datos digitales de un ataque, daño, redirección maliciosa de servicios, o acceso no autorizado.

Las redes de computadoras han tocado y avanzado muchos aspectos de la sociedad. Estas se utilizan, entre otras cosas, para avanzar la ciencia y la tecnología, para proveer comunicación entre personas de diferentes culturas e idiomas, y para mejorar la educación y el entretenimiento. Sin embargo, la rápida proliferación de las redes informáticas no ha seguido el ritmo de la seguridad necesaria para proteger a los usuarios individuales, corporaciones, agencias e infraestructura nacional contra los ciberataques. Cada segundo hay una red que está siendo escaneada por vulnerabilidades, y casi todos los días hay una amenaza o ataque contra los EE.UU. La ciberseguridad inadecuada y la pérdida de información han infligido un daño inaceptable a la seguridad nacional y económica. Un ejemplo directo que afectó a nuestra sociedad Puertorriqueña es cuando en Marzo del 2017, el departamento de Hacienda fue víctima de un ataque cibernético que causó pérdida de información y retrasos en la recolección de fondos tributarios que se estima costó 20 millones de dólares en pérdidas según el

secretario de Hacienda, Raúl Maldonado[1]. Una situación parecida fue reportada en el Centro de Recaudaciones de Ingresos Municipales[2].

La revista Forbes[3] estimó en el 2016 que el mercado de la seguridad cibernética aumentará de $75 billones a $200 billones para el 2020 y que la demanda de trabajos alcanzará los 6 millones a nivel global para el 2019. Según la Oficina de Estadísticas Laborales de EEUU[4], la tasa de crecimiento en trabajos relacionados a la seguridad es proyectada a 37% del 2012-2022, más rápido que el promedio de todas las demás ocupaciones.

Con el propósito de satisfacer la demanda de expertos en seguridad cibernética, las agencias federales y la industria han invertido en la creación de nuevos programas de educación en seguridad cibernética, en toda la nación. El mejor ejemplo es nuestro proyecto de seguridad cibernética subvencionado por la NSF "Academics and Training for the Advancement of Cybersecurity Knowledge in Puerto Rico (ATACK-PR)", que surge de una iniciativa de la NSF para construir capacidad para instituir programas de seguridad cibernética en la educación superior[5].

Como parte de los objetivos de la subvención de la NSF "Academics and Training for the Advancement of Cybersecurity Knowledge in Puerto Rico (ATACK-PR)", el departamento de Ciencia de Cómputos de la facultad de Ciencias Naturales del recinto de Río Piedras desarrolló una serie de cursos en seguridad cibernética. Estos cursos han tenido una buena acogida por los estudiantes del departamento y hasta el momento han servido para:

1) Motivar a estudiantes a continuar en Ciencia de Cómputos o transferirse a nuestro programa.
2) Representar al departamento en competencias de seguridad
3) Motivar a estudiantes a hacer investigación subgraduada y divulgar sus trabajos
4) Motivar a estudiantes a participar en internados de verano en el área de seguridad
5) Motivar a estudiantes a continuar estudios graduados en computación con concentración en seguridad.
6) Proponer esta concentración menor a tenor con la Certificación Núm. 69 2013-2014
    a) Con el establecimiento de la concentración menor, aspirar a ser un Centro Nacional de Excelencia Académica en Defensa Cibernética.

---

[1] FBI investigará el hackeo en Hacienda
http://www.primerahora.com/noticias/policia-tribunales/nota/fbiinvestigaraelhackeoenhacienda-1210819/
[2] Los federales invaden Hacienda tras el "hackeo"
https://www.elnuevodia.com/noticias/locales/nota/losfederalesinvadenhaciendatraselhackeo-2298971/
[3]One Million Cybersecurity Job Openings In 2016, Forbes,
https://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#303ef7af27ea
[4] Bureau of Labor Statistics, https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[5] CyberCorps(R) Scholarship for Service (SFS) Defending America's Cyberspace, Capacity Track,
https://www.nsf.gov/pubs/2015/nsf15584/nsf15584.htm

Proponemos una Concentración Menor en Seguridad Cibernética que consiste en la aprobación de 9 créditos en cursos electivos relacionados a ciberseguridad de nuestro programa de Bachillerato en Ciencia de Cómputos. Entendemos que esta concentración menor ampliará las oportunidades de nuestros estudiantes en el mercado laboral y estudios graduados[6]. A nuestro entender, la concentración menor que proponemos sería la primera opción curricular en el campo de la ciberseguridad que se ofrece en la Universidad de Puerto Rico y es cónsona con el desarrollo y proliferación de este tipo de grados en instituciones de los Estados Unidos. Al no contar en el sistema UPR con un programa de seguridad de cibernética como la propuesta, la concentración primaria será aquella de la que provenga el estudiante. Este programa será de impacto inmediato a estudiantes del departamento de Ciencia de Cómputos, al programa de Sistemas de Información de la Facultad de Administración de Empresas, programas relacionados a la computación en otros recintos y estudiantes de cualquier otro programa en el sistema UPR que cumplan con los pre-requisitos de la concentración menor. Varios de estos cursos son actualmente completados por estudiantes interesados en las áreas de seguridad en el departamento, pero su grado es en Ciencia de Cómputos, lo cual no los diferencia de los demás estudiantes y los obliga a evidenciar su experiencia en seguridad a patronos o escuelas graduadas. Este grado menor constará en el expediente académico en beneficio del estudiante.

Resumen de objetivos

Al finalizar el programa el estudiante podrá:

1. Aplicar los conocimientos de la seguridad cibernética con fines prácticos a la prevención y solución de ataques cibernéticos.
2. Describir los componentes del ciberespacio (usuarios, datos, computadoras, redes de computadoras, programas y protocolos) y cómo estos son vulnerables a ataques.
3. Analizar sistemas de información, explicar los resultados o el rendimiento de un sistema de información, y verificar los resultados y diagnosticar fallas.
4. Detectar, describir y corregir prácticas inseguras de implementación de software y sistemas de información.
5. Explicar ataques en sistemas de información, seleccionar y desarrollar herramientas y mitigar ataques.
6. Llevar a cabo reconocimiento, ataque, defensa y análisis forense de sistemas de información.
7. Describir el rol de los usuarios en los sistemas de información. Analizar y explicar cómo los usuarios impactan la seguridad.
8. Reconocer la diferencia entre hacking ético y hacking no ético.

[6]Job Report, Dice, http://media.dice.com/report/may-2015-top-paying-tech-security-jobs/, Monster, The Future of Cybersecurity Jobs, https://www.monster.com/career-advice/article/future-of-cybersecurity-jobs,

C. Evidencia de cumplimiento con los estándares y los requisitos de la acreditación profesional y de las instancias que otorgan las certificaciones o las licencias, según aplique.

El programa de Ciencia de Cómputos está acreditado por la agencia acreditadora de programas de Computación e Ingeniería ABET hasta el año 2022. La adición del grado menor propuesto no afecta la acreditación del programa, por el contrario, lo fortalece ya que le permite al estudiante profundizar en temas de seguridad y sistemas que son parte de los nuevos criterios[7] de evaluación para el próximo ciclo de acreditación.

D. Diseño curricular

Los cursos medulares del bachillerato en Ciencia de Cómputos no son parte de los 9 créditos para completar la concentración menor. La Concentración Menor en Seguridad Cibernética requiere que los estudiantes de CCOM tomen **9 créditos adicionales** para cumplir con los requisitos de la concentración propuesta, los cuales se pueden satisfacer con los cursos electivos libres de la concentración. Los estudiantes de otros programas pueden cumplir con dichos pre-requisitos tomando los cursos ofrecidos por nuestro Departamento o demostrando que cuentan con las destrezas necesarias para tomar el curso de la concentración, e.g. han tomado cursos equivalentes a los pre-requisitos en otros programas o tienen experiencia laboral. (Ver Anejo con Modelos sobre la secuencia curricular actual y la concentración menor).

1. Cursos en Seguridad Cibernética que se ofrecen en el Departamento de Ciencia de Cómputos. Todos los cursos son de 3 créditos.

    CCOM 4088 - Introducción a la Ciberseguridad

    En el curso Introducción a la Ciberseguridad los estudiantes aprenderán la arquitectura física y lógica de Internet y los principios básicos de la seguridad de la información. A través de la interacción con clientes y servidores de red, explorarán por qué los sistemas en red son vulnerables a ataques cibernéticos. Verán cómo los cinco pilares del aseguramiento de la información (disponibilidad, integridad, autenticación, confidencialidad y no repudio) se aplican a los recursos de información en red. Los estudiantes explorarán técnicas básicas de cómo atacar y defender los recursos de Internet. Las técnicas prácticas servirán para motivar a los estudiantes a explorar en profundidad técnicas más avanzadas y los fundamentos matemáticos de la ciberseguridad (matemáticas discretas, criptografía). Al finalizar este curso el estudiante podrá reconocer la diferencia entre un hacker ético y no ético.

[7] CRITERIA FOR ACCREDITING COMPUTING PROGRAMS https://www.abet.org/wp-content/uploads/2018/02/C001-18-19-CAC-Criteria-Version-2.0-updated-02-12-18.pdf

CCOM 4205 - Redes de Computadoras

Este curso ofrece una descripción general de redes de comunicación de computadoras. Se discuten elementos fundamentales de una red, incluyendo protocolos, elementos de diseños y sus características. Se le da un énfasis especial a los protocolos utilizados en el Internet, incluyendo los mecanismos y protocolos de enrutamiento. También se presentan algunas de las aplicaciones fundamentales que se usan en el Internet y sus protocolos.

CCOM 4089 - Seguridad en Sistemas y Redes

En este curso, los estudiantes aprenderán técnicas seguras de administración de sistemas y redes. Los estudiantes tendrán experiencias prácticas de administración de sistemas con servicios clave de Internet, aprenderán sobre temas de seguridad importantes relacionados con tales servicios y estarán expuestos a técnicas y herramientas para analizar, defender y asegurar sistemas y redes.

CCOM 4702 - Ingeniería Inversa de Software

Saber deducir la funcionalidad y las técnicas de desarrollo de un software a partir de su ejecutable, es una destreza esencial para profesionales de seguridad cibernética. Esto les permite inspeccionar software de código cerrado de terceras personas y determinar sus vulnerabilidades y/o comportamientos nocivos. Los estudiantes aprenderán diversas técnicas para deducir el funcionamiento y prácticas de codificación de un programa partiendo de su ejecutable y realizarán ajustes tales como esquivar mecanismos de licencia y hacer cambios o utilizar funcionalidades (dentro de las leyes que protegen la propiedad intelectual del programado). Analizarán malware y aprenderán técnicas reconocidas de prevención de ingeniería inversa y estrategias para contrarrestarlas.

CCOM 50XX - Análisis Forense Digital

Este curso presentará a los estudiantes con la aplicación de los principios de las ciencias forenses y prácticas de recolección, preservación, examinación, análisis y presentación de evidencia digital. El curso incluirá temas de los dominios legales, forense y tecnología de la información y utilizará conferencias, experiencias prácticas de laboratorio y escritos para ilustrar estos temas.

CCOM 50XY - Seguridad en Hardware

Seguridad en hardware es un campo que estudia temas que van desde (a) la implementación de algoritmos de encripción en hardware, (b) las técnicas de diseño para proteger la propiedad intelectual de los circuitos integrados y los sistemas embebidos, y (c) la detección de funcionalidades maliciosas en circuitos integrados. Nos concentraremos en los temas (b) y (c). Su estudio nos llevará a comprender, entre otras cosas, el proceso de diseño de circuitos digitales, su base teórica y tecnológica, y los lenguajes de modelación de hardware. También estudiaremos cómo utilizar dispositivos de lógica programable (FPGAs) para encontrar y aprovechar vulnerabilidades en sistemas embebidos (embedded systems).

La Tabla 1 muestra la oferta de cursos en ciberseguridad de nuestro Departamento. De los 9 créditos para completar la concentración menor, los cursos Introducción a la Ciberseguridad (CCOM4088) y Seguridad en Sistemas y Redes (CCOM4089) son obligatorios. Los restantes 3 créditos pueden ser completados con un curso entre los restantes: Análisis Forense Digital, Introducción a la ingeniería inversa, Seguridad en hardware y otros cursos dirigidos en Ciberseguridad.

Tabla 1 - Oferta de cursos en ciberseguridad del departamento de Ciencia de Cómputos

Concentración menor en seguridad cibernética		
Codificación	**Título**	**Créditos**
CCOM 4088	Introducción a la Ciberseguridad*	3
CCOM 4089	Seguridad en Sistemas y Redes*	3
CCOM 50XX	Análisis Forense Digital	3
CCOM 4702	Introducción a la ingeniería inversa	3
CCOM 50XY	Seguridad en Hardware	3

* Curso obligatorio para la concentración menor.

E. Requisitos generales

Los estudiantes interesados deben haber aprobado el curso CCOM4088 con A o B. Solicitarán admisión a la Concentración Menor en Seguridad Cibernética del Departamento de Ciencia de Cómputos, llenarán la **Declaración de Intención** y llenarán y pagarán la **Solicitud de Concentraciones Múltiples**. Los estudiantes de programas distintos a Ciencia de Cómputos deben observar que los cursos de la concentración menor excepto CCOM4088 tienen como pre-requisitos otros cursos de Ciencia de Cómputos. Para facilitar la participación de estos estudiantes el asesor académico del programa de Ciencia de Cómputos evaluará equivalencias a cursos de otros programas.

La concentración menor que proponemos beneficiará a aquellos estudiantes de Ciencia de Cómputos, Sistemas Computadorizados de Información y otros grados relacionados a la computación que deseen adquirir destrezas y conocimientos en seguridad cibernética, tanto para optar por empleos y/o continuar estudios graduados en el área. El peritaje adquirido por estudiantes y profesores será de gran beneficio al sistema UPR-RP e industrias con presencia en PR. Por ejemplo, los estudiantes pueden realizar proyectos para sus clases de concentración menor en donde evalúan y sugieren mejoras a la seguridad de los sistemas de información de UPR-RP.

F. Criterios de cumplimiento satisfactorio: índices académicos mínimos

Para cumplir satisfactoriamente con los requisitos de esta concentración menor los estudiantes deben aprobar los cursos de ciberseguridad con calificación mínima de C (70%), con excepción del curso CCOM 4088 Introducción a la Ciberseguridad donde se le requerirá una calificación mínima de B (80%).

Plan de avalúo

Dominio	Objetivos	Instrumento	Responsable	Expectativas	Frecuencia
Investigación y creación	Aplicar los conocimientos de la seguridad cibernética con fines prácticos a la prevención y solución de ataques cibernéticos.	CCOM 4088. Ejercicio de laboratorio: Configuración de firewall para proteger una red. CCOM 4089. Ejercicio de laboratorio: Mejorar una aplicación de web utilizando separación de privilegios.	Director del Departamento de Ciencia de Cómputos y/o profesores que dictan el curso.	Más del 66% de los estudiantes tendrán un nivel satisfactorio o mayor	Bienal

Razonamiento lógico matemático	Explicar ataques cibernéticos, seleccionar y desarrollar herramientas para prevenirlos y mitigarlos.	CCOM 4088. Ejercicio de laboratorio: Incorporar medidas de seguridad para corregir las vulnerabilidades de inyección de código (javascript code injection). CCOM 4089. Ejercicio de laboratorio: Incorporar medidas de seguridad para corregir las vulnerabilidades de desbordamiento de búfer en una aplicación web.	Director del Departamento de Ciencia de Cómputos y/o profesores que dictan el curso.	Más del 66% de los estudiantes tendrán un nivel satisfactorio o mayor	Bienal
Contenido de la disciplina	Explicar ataques cibernéticos, seleccionar y desarrollar herramientas para prevenirlos y mitigarlos.	CCOM 4088 y CCOM 4089. Preguntas en examen: Dada la vulnerabilidad o ataque, explique los pasos para detectarla y/o mitigarla. Describa las herramientas que necesitaría para lograr el	Director del Departamento de Ciencia de Cómputos y/o profesores que dictan el curso.	Más del 66% de los estudiantes tendrán un nivel satisfactorio o mayor	Bienal

		análisis y la mitigación.			

A continuación, listamos las actividades de nuestro plan de avalúo. Los resultados esperados para todas las actividades de avalúo es que al menos 70% de los estudiantes obtendrán puntuaciones de 3 o más en una escala de 0 a 5, basado en la rúbrica de la actividad.

Objetivo 1: Aplicar los conocimientos de la seguridad cibernética con fines prácticos a la prevención y solución de ataques cibernéticos.

- CCOM 4088. Ejercicio de laboratorio: Configuración de firewall para proteger una red.
- CCOM 4089. Ejercicio de laboratorio: Mejorar una aplicación de web utilizando separación de privilegios.

Objetivo 2: Describir los componentes del ciberespacio (usuarios, datos, computadoras, redes de computadoras, programas y protocolos) y cómo estos son vulnerables a ataques.

- CCOM 4088. Pregunta de exámen sobre privilegios de archivos y directorios.

Objetivo 3: Analizar sistemas de información, explicar los resultados o el rendimiento de un sistema de información, y verificar los resultados y diagnosticar fallas.

- CCOM 4088. Ejercicio de laboratorio: Utilizando herramientas de código abierto para analizar nodos de una red de computadora.
- CCOM 4089. Ejercicio de laboratorio: Analizar la estructura básica de una aplicación web y usar ataques de desbordamiento de búfer para esquivar su seguridad.

Objetivo 4: Detectar, describir y corregir prácticas inseguras de implementación de software y sistemas de información.

- CCOM 4088. Ejercicio de laboratorio: Incorporar medidas de seguridad para corregir las vulnerabilidades de inyección de código (javascript code injection).
- CCOM 4089. Ejercicio de laboratorio: Incorporar medidas de seguridad para corregir las vulnerabilidades de desbordamiento de búfer en una aplicación web.

Objetivo 5: Explicar ataques cibernéticos, seleccionar y desarrollar herramientas para prevenirlos y mitigarlos.

- CCOM 4088 y CCOM 4089. Preguntas en examen: Dada la vulnerabilidad o ataque, explique los pasos para detectarla y/o mitigarla. Describa las herramientas que necesitaría para lograr el análisis y la mitigación.

Objetivo 6: Llevar a cabo reconocimiento, ataque, defensa y análisis forense de sistemas de información.

- CCOM 4089. Ejercicio de laboratorio: Ataques comunes a navegadores de internet (browsers).

- CCOM 4088. Ejercicio de laboratorio: Rescatando data de dispositivos defectuosos o sospechosos.

Objetivo 7: Describir el rol de los usuarios en los sistemas de información. Analizar y explicar cómo los usuarios impactan la seguridad.

- CCOM 4088. Presentación oral sobre caso reciente relacionado a incumplimiento de seguridad primordialmente debido a usuarios. Explicar cuáles de los pilares de ciberseguridad aplica al caso.

Objetivo 8: Reconocer la diferencia entre hacking ético y hacking no ético.

- CCOM 4088. Ensayo o presentación oral sobre implicaciones éticas en caso de estudio de ciberseguridad.

Recolección de datos

La recolección de datos de avalúo se realizará principalmente en los cursos requisito CCOM 4088 y CCOM 4089. Consistirá mayormente de las evaluaciones de ejercicios de laboratorio, presentaciones orales y ensayos. Además realizaremos un cuestionario de entrada y uno de salida en los que el estudiante auto-evaluará sus actitudes y competencias en temas relacionados a los objetivos de la concentración.

ANEJOS

Modelos sobre la secuencia curricular actual de la concentración en Ciencia de Cómputos y la concentración menor en Seguridad Cibernética

El Modelo 1 contiene la secuencia curricular de nuestro programa de bachillerato de 4 años. Como podrá observar, nuestro programa de bachillerato requiere 9 créditos en electivas libres. Los 9 créditos necesarios para completar la concentración menor en ciberseguridad podrían obtenerse de la siguiente forma: 9 créditos de electivas libres de la secuencia curricular del Bachillerato en Ciencia de Cómputos. De esta forma, un estudiante de nuestro bachillerato si opta por tomar todas sus electivas libres en cursos de ciberseguridad no tendría carga académica adicional para completar la concentración menor. Por lo tanto, los estudiantes podrán completar el bachillerato y concentración menor dentro del 150% del tiempo prescrito para completar el bachillerato en Ciencia de Cómputos, i.e. 6 años.

Modelo 1 - Secuencia curricular actual del bachillerato en Ciencia de Cómputos del departamento de Ciencia de Cómputos de la UPR-RP con Concentración Menor en Seguridad Cibernética.

Currículo bachillerato en Ciencia de Cómputos		
Secuencia Curricular		**Créditos**
Cursos de Educación General		39
Cursos de Ciencias Naturales		14
Cursos de Matemáticas		20
Cursos de Ciencia de Cómputos		39
Electivas dirigidas		9
Electivas libres		9
	Total	127
Codificación	**Cursos de Educación General (39 créditos)**	**Créditos**
ESPA 3101-02	Español I y Español II	6
INGL 3101-02	Inglés I e Inglés II	6
CISO 3121-22	Ciencias Sociales I y Ciencias Sociales II	6
HUMA 3111-12	Humanidades I y Humanidades II	6

CIFI/CIBI 4XXX	Ciencias Fac. Estudios Generales	3
CIFI/CIBI 4XXX	Ciencias Fac. Estudios Generales	3
ESPA32XX	Literatura I	3
ESPA32XX	Literatura II	3
	Arte	3
Codificación	**Cursos de Ciencias Naturales (14 créditos)**	**Créditos**
CINA*	Ciencia I	3
CINA*	Ciencia II	3
CINA**	Ciencia con laboratorio I	4
CINA**	Ciencia con laboratorio II	4
Codificación	**Cursos en Matemáticas (20 créditos)**	**Créditos**
MATE 3151	Cálculo I	4
MATE 3152	Cálculo II	4
MATE 4081	Álgebra Superior I	3
MATE 4080	Álgebra Moderna Aplicada	3
MATE 4031 o 4065	Algebra Lineal o Algebra Lineal Numérica	3
MATE 5001	Probabilidad	3
Codificación	**Cursos en Ciencia de Cómputos (39 créditos)**	**Créditos**
CCOM 3981	Seminario Subg. en Ciencia de Cómputos I	1
CCOM 3982	Seminario Subg. en Ciencia de Cómputos II	2
CCOM 3030	Introducción a la Ciencia de Cómputos	3
CCOM 3020	Matemáticas Discretas	3
CCOM 3033	Introducción a la Programación	3
CCOM 3034	Estructuras de Datos	3
CCOM 4017	Sistemas Operativos	3
CCOM 4027	Introducción al Manejo de Datos	3
CCOM 4029	Lenguajes de Alto Nivel	3
CCOM 4030	Introducción a la Ingeniería de Software	3
CCOM 4086	Arquitectura de Computadoras	3
CCOM 4087	Diseño de Compiladores	3
CCOM 5050	Diseño y Análisis de Algoritmos	3
CCOM 5035	Teoría de la Computabilidad	3
Cursos en Electivas Dirigidas (9 créditos)		
Electiva dirigida (CCOM o MATE)		3
Electiva dirigida (CCOM o MATE)		3
Electiva dirigida (CCOM o MATE)		3
Cursos en Electivas Libres (9 créditos)		
Secuencia curricular bachillerato actual	Secuencia curricular con concentración menor en Seguridad Cibernética	

Electiva libre	Curso de la Secuencia Curricular en Seguridad Cibernética	3
Electiva libre	Curso de la Secuencia Curricular en Seguridad Cibernética	3
Electiva libre	Curso de la Secuencia Curricular en Seguridad Cibernética	3

* Pueden ser cursos de FISI, BIO, QUIM, o cualquier otro curso de ciencia en ciencias naturales.
** Pueden ser FISI 3011, FISI 3012, BIOL 3102, QUIM 3001 o QUIM 3002

El Modelo 2 contiene la secuencia curricular del programa de bachillerato de 4 años en Ciencia e Ingeniería de Computadoras del Recinto de Mayagüez. Como podrá observar, este programa de bachillerato requiere 12 créditos en electivas libres. Los 9 créditos necesarios para completar la concentración menor en ciberseguridad podrían obtenerse de la siguiente forma: 9 créditos de electivas libres de la secuencia curricular del Bachillerato en Ciencia e Ingeniería de Computadoras. De esta forma, un estudiante de nuestro bachillerato si opta por tomar todas sus electivas libres en cursos de ciberseguridad no tendría carga académica adicional para completar la concentración menor. Por lo tanto, los estudiantes podrán completar el bachillerato y concentración menor dentro del 150% del tiempo prescrito para completar el bachillerato en, Ciencia e Ingeniería de Computadoras i.e. 6 años.

Modelo 2 - Secuencia curricular actual del bachillerato en Ciencia e Ingeniería de Computadoras del departamento de Ciencia e Ingeniería de Computadoras de la UPR-Mayagüez con Concentración Menor en Seguridad Cibernética.

Currículo bachillerato en Ciencia e Ingeniería de Computadoras (CIIC)		
Secuencia Curricular		**Créditos**
Cursos de Educación General		32
Cursos de Ciencias Naturales		18
Cursos de Ingeniería		21
Cursos de Matemáticas		14
Cursos de Ciencia e Ingeniería de Computadoras		42
Electivas dirigidas		15
Electivas libres		12
	Total	154
Codificación	**Cursos de Educación General (32 créditos)**	**Créditos**
INGL 3XXX	First year course in English	6
INGL 3XXX	Second Year Course in English	6
ESPA 3101	Basic Spanish I	3

ESPA 3102	Basic Spanish II	3
HUMA XXXX	Socio Humanistic Elective	12
EDFI XXXX	Course in Physical Education	2
Codificación	**Cursos de Ciencias Naturales (18 créditos)**	**Créditos**
QUIM 3131	General Chemistry I	3
QUIM 3133	General Chemistry Lab I	1
QUIM 3132	General Chemistry II	3
QUIM 3134	General Chemistry Lab II	1
FISI 3171	Physics I	4
FISI 3173	Physics Lab I	1
FISI 3172	Physics II	4
FISI 3174	Physics Lab II	1
Codificación	**Cursos de Ingeniería (21 créditos)**	**Créditos**
INGE 3011	Engineering Graphics	2
INEL 3105	Electrical Systems Analysis I	3
INEL 4115	Electrical Measurements Lab	1
INGE 3035	Engineering Mechanics	3
ININ 4010	Probability and Statistics for Engineers	3
INME 4045	General Thermodynamics for Engineers	3
ININ 4015	Engineering Economic Analysis	3
INGE 3045	Materials Science for Electrical Engineers	3
Codificación	**Cursos en Matemáticas (14 créditos)**	**Créditos**
MATE 3031	Cálculo I	4
MATE 3032	Cálculo II	4
MATE 3063	Calculus III	3
MATE 4145	Linear Algebra and Differential Equations	3
Codificación	**Cursos en CIIC (42 créditos)**	**Créditos**
CIIC 3010	Introduction to Computer Programming I	3
CIIC 3075	Foundations of Computing	3
CIIC 4010	Advanced Programming	4
CIIC 4011	Data Structures	4
CIIC 4020	Design and Analysis of Algorithms	3
CIIC 3080	Computer Architecture I	3
CIIC 4030	Programming Languages	3
CIIC 4040	Computer Architecture II	3
CIIC 4050	Operating Systems	4
INSO 4101	Introduction to Software Engineering	3
CIIC 5045	Automata and Formal Languages	3
CIIC 4060	Database Management Systems	3
CIIC 4070	Computer Networks	3

Cursos en Electivas Dirigidas (15 créditos)		
Electiva dirigida (CIIC)		3
Electiva dirigida (CIIC)		3
Electiva dirigida (CIIC)		3
Elective dirigida (CIIC)		3
Elective dirigida (CIIC)		3
Cursos en Electivas Libres (12 créditos)		
Secuencia curricular bachillerato actual	**Secuencia curricular con concentración menor en Seguridad Cibernética**	
Electiva libre	Curso de la Secuencia Curricular en Seguridad Cibernética	3
Electiva libre	Curso de la Secuencia Curricular en Seguridad Cibernética	3
Electiva libre	Curso de la Secuencia Curricular en Seguridad Cibernética	3
Electiva libre		3