UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
SANTIAGO - CHILE

"DISEÑO DE UN LÍNEA DE CIBERSEGURIDAD PARA LA CARRERA DE INGENIERÍA CIVIL INFORMÁTICA DE LA UTFSM"

SEBASTIÁN IGNACIO OLIVARES CARRASCO

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: José Luis Martí Lara
Profesor Correferente: Mauricio Olivares Faúndez

Diciembre - 2025

CONSTANCIA DE VALIDACIÓN Y CONFIDENCIALIDAD DE MONOGRAFÍA A REPOSITORIO ACADÉMICO

1.- IDENTIFICACIÓN DEL TRABAJO ACADÉMICO

Tipo de monografía (marcar una opción): ☒ Memoria o trabajo de título ☐ Tesis de Postgrado

Título del trabajo: Diseño de un Línea de Ciberseguridad para la carrera de Ingeniería Civil Informática de la UTFSM

Nombre del candidato(a): Sebastián Ignacio Olivares Carrasco

Carrera / Grado: Ingeniería Civil Informática

Campus: San Joaquín **Departamento:** Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, José Luis Martí Lara, en mi calidad de profesor(a) guía/director(a) del trabajo académico mencionado anteriormente **DEJO CONSTANCIA** que:

- He revisado esta versión del documento y corresponde a la versión final aprobada del trabajo.
- El trabajo cumple con los requisitos académicos y de formato establecidos por la institución.

3.- EVALUACIÓN DE CONFIDENCIALIDAD POR PROPIEDAD INDUSTRIAL (marcar una opción)

☒ El trabajo **NO contiene** información que amerite confidencialidad y puede ser publicado de inmediato en repositorio con acceso abierto.

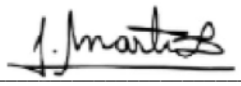
☐ El trabajo **CONTIENE** información con potenciales implicancias de propiedad industrial o intelectual y requiere un periodo de confidencialidad (**embargo**) por **(marcar una opción)**:

☐ 6 meses ☐ 12 meses ☐ 2 años ☐ 3 años ☐ 5 años ☐ 10 años

Fundamentación de la necesidad de confidencialidad (obligatorio si se solicita embargo):

4.- FIRMAS

Profesor(a) guía o director(a) de memoria o tesis:

Fecha: 17 - 12 - 2025 **Firma:** 

Estudiante o Candidato(a):

Fecha: 18 - 12 - 2025 **Firma:** 

Este formulario debe ser insertado como página 2 de la memoria o tesis, completado y firmado por estudiante y profesor(a) antes de la entrega en portal PRISMA de Biblioteca USM.

DEDICATORIA

Dedico este trabajo a mi mamá y mi abuela, que siempre me impulsaron a ser mejor.

AGRADECIMIENTOS

Quiero agradecer a mi familia, amigos y profesores. Esta es la culminación de todas sus contribuciones a mi ser como persona y profesional.

RESUMEN

Resumen— En este trabajo se analizó la formación en ciberseguridad en el contexto de la educación superior chilena, mediante el estudio de la oferta académica existente y su relación con marcos de referencia internacionales. A partir del análisis y comparación de frameworks educativos relevantes, particularmente el NICE y el CSEC2017, se formularon propuestas de líneas curriculares complementarias para la carrera de Ingeniería Civil Informática de la Universidad Técnica Federico Santa María, considerando distintos criterios de organización y priorización de contenidos.

Palabras Clave— Ciberseguridad; Educación en informática; Marcos de referencia; NICE; CSEC2017

ABSTRACT

Abstract— This work analyzes cybersecurity education within the context of Chilean higher education through the study of existing academic offerings and their relationship with international reference frameworks. Based on the analysis and comparison of relevant educational frameworks, particularly NICE and CSEC2017, complementary curricular track proposals were developed for the Computer Engineering program at the Universidad Técnica Federico Santa María, considering different criteria for content organization and prioritization.

Keywords— Cybersecurity; Computer science education; Frameworks; NICE; CSEC2017

GLOSARIO

A

ACM: Association for Computing Machinery (Asociación de Maquinaria Computacional)

AIS SIGSEC: Association for Information Systems – Special Interest Group on Information Security and Privacy (Grupo de Interés Especial en Seguridad de la Información y Privacidad de la Asociación de Sistemas de Información)

ANCI: Agencia Nacional de Ciberseguridad — Chile

B

BERT: Bidirectional Encoder Representations from Transformers — Representaciones de codificación bidireccionales a partir de transformadores

C

CAE-C: Centers of Academic Excellence in Cybersecurity (Centros de Excelencia Académica en Ciberseguridad)

CERT-UA: Computer Emergency Response Team of Ukraine (Equipo de Respuesta ante Emergencias Informáticas de Ucrania)

CSEC2017: Cybersecurity Curricular Guidelines 2017 (Directrices curriculares de ciberseguridad 2017)

CSIRT: Computer Security Incident Response Team (Equipo de Respuesta ante Incidentes de Seguridad Informática)

CyBOK: Cyber Security Body of Knowledge (Cuerpo de conocimiento en ciberseguridad)

D

DDoS: Distributed Denial of Service (Denegación de servicio distribuida)

DoS: Denial of Service (Denegación de servicio)

E

ECSF: European Cybersecurity Skills Framework (Marco Europeo de Competencias en Ciberseguridad)

G

GRU: Glavnoye Razvedyvatel'noye Upravleniye (Dirección Principal de Inteligencia del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia)

I

IEEE-CS: IEEE Computer Society (Sociedad de Computación del IEEE)

IFIP WG 11.8: International Federation for Information Processing, Working Group 11.8 Information Security Education (Federación Internacional para el Procesamiento de la Información, Grupo de Trabajo 11.8 Educación en Seguridad de la Información)

IPST: Instituto Profesional Santo Tomás — Chile

ISC2 / $(ISC)^2$: International Information System Security Certification Consortium (Consorcio Internacional de Certificación en Seguridad de Sistemas de Información)

J

JTF: Joint Task Force on Cybersecurity Education (Fuerza de Tarea Conjunta para la Educación en Ciberseguridad)

K

KA: Knowledge Area (Área de conocimiento)

KD: Knowledge Description (Descripción de conocimiento)

KU: Knowledge Unit (Unidad de conocimiento)

N

NCSI: National Cyber Security Index (Índice Nacional de Ciberseguridad)

NICE: National Initiative for Cybersecurity Education (Iniciativa Nacional para la Educación en Ciberseguridad)

NIST: National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología de EE.UU.)

P

PUCV: Pontificia Universidad Católica de Valparaíso — Chile

S

SCADA: Supervisory Control and Data Acquisition (Control de supervisión y adquisi-

ción de datos)

U

USACH: Universidad de Santiago de Chile

UST: Universidad Santo Tomás - Chile

UTFSM: Universidad Técnica Federico Santa María — Chile

ÍNDICE DE CONTENIDOS

Índice de figuras

ÍNDICE DE TABLAS

INTRODUCCIÓN

El mundo digital en el que se vive hoy ofrece innumerables beneficios, facilitando el acceso a bienes, servicios y conocimiento a través de sistemas tecnológicos presentes en sectores como el comercio, la comunicación y el entretenimiento. Sin embargo, esta misma expansión ha dado lugar a nuevas formas de delincuencia que explotan las vulnerabilidades de dichos sistemas, poniendo en riesgo la privacidad, la integridad de los datos y la estabilidad de operaciones críticas. En este contexto, los profesionales de ciberseguridad se configuran como un componente esencial para garantizar la continuidad de los servicios digitales y la protección de la información sensible.

En consecuencia, se hace necesario formar nuevos profesionales capaces de responder a las exigencias actuales del entorno digital. Con este propósito, en el presente trabajo se formula un conjunto de líneas formativas complementarias para la carrera de Ingeniería Civil Informática de la Universidad Técnica Federico Santa María.

La solución propuesta a esta problemática consiste en la creación de currículos complementarios, mediante la aplicación de metodologías *ad hoc* basadas en estándares y marcos de referencia desarrollados por instituciones especializadas en la disciplina, considerando además el contexto de la oferta académica en la realidad chilena.

El documento se estructura en cinco capítulos. El primero aborda la definición del problema de investigación, así como el contexto en el cual surge, los objetivos planteados, el alcance del estudio y el impacto potencial de la implementación de la solución propuesta. El segundo capítulo desarrolla el marco conceptual, en el cual se describen las herramientas y fuentes de información que sustentan este trabajo, con el fin de proporcionar un marco común de conceptos y conocimientos que permita comprender la propuesta. El tercer capítulo presenta la solución planteada a la problemática, junto con el proceso metodológico utilizado para su formulación. En el cuarto capítulo se evalúa la coherencia y la factibilidad de la solución propuesta. Finalmente, el quinto capítulo expone las conclusiones del trabajo, sus principales aportes, las limitaciones identificadas y las líneas de trabajo futuro.

CAPÍTULO 1
DEFINICIÓN DEL PROBLEMA

"La ciberseguridad es la práctica de proteger a las personas, los sistemas y los datos de los ciberataques mediante el uso de diversas tecnologías, procesos y políticas"[IBM, 2025a].

Es a través de estas prácticas que se preservan la seguridad, la privacidad y el bienestar, tanto en el ámbito digital como en el físico, dentro de un mundo moderno en el cual la tecnología se ha vuelto indispensable para el funcionamiento de la sociedad.

En este contexto, los profesionales en ciberseguridad constituyen un componente crítico para la protección de infraestructuras, información y personas. Sin embargo, el número de profesionales es insuficiente para cubrir la demanda.

En el presente capítulo, se da una visión general del déficit de profesionales en ciberseguridad a nivel mundial y sus consecuencias en distintos sectores. Posteriormente, se examina cómo esta situación se refleja en el contexto nacional, identificando las necesidades y desafíos particulares de Chile. Finalmente, se analizará el caso de la Universidad Técnica Federico Santa María (UTFSM), con el fin de situar la problemática en un entorno académico concreto y establecer la base para las propuestas de solución que se desarrollarán en los capítulos posteriores.

1.1. Problema asociado

Uno de los conceptos fundamentales que debe definirse en primer lugar es el de *ciberataque* o *ataque cibernético*, también conocido coloquialmente como *hackeo*. Este se entiende como cualquier esfuerzo intencional para robar, exponer, alterar, deshabilitar o destruir datos, aplicaciones u otros activos mediante el acceso no autorizado a una red, sistema informático o dispositivo digital [IBM, 2025b].

Los ciberataques, a través de técnicas como el *ransomware*, el acceso no autorizado o la destrucción de información sensible, no solo generan pérdidas financieras significativas, sino que además pueden poner en riesgo la vida de las personas [Cisco, sf].

El aumento de la dependencia en la digitalización ha incrementado la necesidad de garantizar la disponibilidad y seguridad de los sistemas tecnológicos, así como de los datos que estos procesan. No obstante, la cantidad de expertos en ciberseguridad resulta insuficiente para responder a la creciente demanda global.

La organización sin fines de lucro *(ISC)²*, especializada en la formación y certificación de profesionales en ciberseguridad, publica anualmente un informe sobre el estado de la

fuerza laboral en este ámbito. En su edición correspondiente a 2024, el estudio señala que el déficit de profesionales alcanzó los 4 millones, lo que representa un aumento del 19,1 % en comparación con 2023 [ISC2, 2024].

A su vez, las proyecciones de *Statista* advierten que el impacto financiero global del cibercrimen continuará aumentando de manera drástica. Se estimaba que los costos ascendieran a USD 9,22 trillones en 2024 y alcancen los USD 13,82 trillones en 2028, lo que refleja una creciente carga económica sobre gobiernos, empresas y usuarios individuales [Statista, 2024].

Entendiendo que los ciberataques constituyen un fenómeno global en constante evolución, tanto en sus técnicas como en sus objetivos, resulta necesario identificar quiénes están detrás de ellos. En la cultura popular y en los medios de comunicación, suele denominarse a estos actores como *hackers*. Sin embargo, este término originalmente poseía una connotación positiva, aludiendo a "una persona que se deleita en tener íntimo conocimiento del funcionamiento interno de un sistema, computadores o redes de computadores" [Malkin y Parker, 1993]. Con el tiempo, su significado se ha generalizado y distorsionado, utilizándose como sinónimo de cibercriminal, lo cual invisibiliza la diversidad y complejidad de los actores involucrados en este tipo de amenazas.

En realidad, los responsables de los ciberataques conforman un espectro heterogéneo de actores maliciosos, que pueden operar de forma independiente o integrarse en organizaciones estructuradas. Sus motivaciones también son variadas: desde la simple curiosidad técnica, al intentar comprender el funcionamiento de distintos sistemas informáticos; pasando por la obtención de beneficios económicos, mediante la adquisición y venta de información personal a otros actores inescrupulosos; hasta fines políticos o ideológicos, como interferir en gobiernos locales o lanzar ataques contra países rivales.

Una demostración ilustrativa de los ciberataques que ocurren en todo momento es el *Live Threat Map* de Radware [Radware, sf], el cual permite observar en tiempo real cuáles son los países más atacados, cuáles son los principales emisores de ataques y qué tipos de técnicas se utilizan con mayor frecuencia. Este recurso pone en perspectiva la magnitud del problema, evidenciando que se trata de una amenaza constante y generalizada a nivel mundial.

Los cibercriminales logran llevar a cabo sus ataques gracias a su experticia técnica, empleando herramientas y conocimientos avanzados sobre sistemas computacionales para tomar control de dispositivos, generalmente conectados a redes como Internet. Sus objetivos pueden ser variados: desde la extracción de información sensible, hasta el uso de equipos comprometidos para ejecutar acciones maliciosas, como el minado de criptomonedas sin el consentimiento del usuario o como plataforma de lanzamiento para ataques de mayor escala. La diversidad de ciberataques es amplia y depende de factores como la vulnerabilidad explotada, la naturaleza de la víctima u objetivo final, y las herramientas utilizadas en el proceso.

A continuación, se presentan algunos de los ataques más comunes, junto con una breve descripción de en qué consisten:

- ***Malware***: Término genérico que engloba todo software diseñado con la intención de dañar computadores, redes o servidores, generalmente sin el conocimiento o consentimiento del usuario. Es uno de los métodos más comunes de ataque, y puede clasificarse según sus características, como la forma de infección, la función que cumple o su persistencia. Algunos ejemplos son: el *Ransomware*, que encripta información valiosa de la víctima y exige un pago para recuperarla; el *Spyware*, que recolecta información de las actividades del usuario; y el *Keylogger*, que registra silenciosamente lo que el usuario escribe en el teclado.
- ***Denial-of-Service* (DoS)**: Un ataque de denegación de servicio ocurre cuando una fuente inunda una red con solicitudes, sobrepasando la capacidad de los servidores e impidiendo que estos entreguen sus servicios de manera adecuada (por ejemplo, correo electrónico o páginas web). Una variante más avanzada es el *Distributed Denial-of-Service* (DDoS), en el cual se coordina una gran cantidad de dispositivos —muchos de ellos comprometidos mediante *malware*— para enviar solicitudes a un servidor. Este ataque es más veloz y complejo de mitigar, pues resulta difícil identificar y bloquear múltiples orígenes simultáneamente.
- ***Phishing***: Uno de los ataques más comunes que afectan a usuarios individuales. Consiste en engañar a la víctima, generalmente mediante correos electrónicos, llamadas telefónicas o publicaciones en redes sociales, haciéndola creer que interactúa con una fuente confiable (por ejemplo, un ejecutivo bancario o un familiar). El atacante busca inducir a la víctima a realizar acciones como hacer click en un enlace, cambiar contraseñas o instalar aplicaciones, lo que puede otorgar acceso a equipos o exponer información sensible.

Además de los aquí presentados, el espectro de posibilidades para vulnerar sistemas es muy amplio [Baker, 2024]. La creciente sofisticación de estos ataques, junto con los variados propósitos y métodos de entrada que emplean, requiere de conocimientos y habilidades técnicas específicas para su prevención, mitigación y análisis. Esto refuerza la urgencia de formar profesionales capaces de actuar con un nivel de especialización comparable al de los actores maliciosos.

Esta necesidad se vuelve aún más crítica ante la expansión constante del entorno digital, que incrementa la superficie de exposición a posibles ataques. La ubicuidad de los sistemas tecnológicos en las actividades contemporáneas convierte a los ciberataques en una amenaza transversal que afecta a organizaciones de todo tipo. Se proyecta que, para el año 2030, existirán cerca de 40 mil millones de dispositivos conectados a Internet [Sinha, 2024], lo que ampliará significativamente los vectores de ataque disponibles para los actores maliciosos. Sectores estratégicos como el comercio, la salud, la educación y la administración pública pueden verse comprometidos en mayor o menor medida. Cada

uno de estos ámbitos presenta desafíos particulares para los especialistas encargados de su protección, derivados de factores como la sensibilidad de la información gestionada, las características de la infraestructura tecnológica empleada o el nivel de alfabetización digital del personal.

De acuerdo con un estudio reciente de *CheckPoint*, una empresa multinacional que produce *software* y *hardware* para ciberseguridad, el sector educativo se posicionó como el principal objetivo de los ciberataques a nivel mundial durante el primer trimestre de 2025. Las instituciones de este ámbito registraron un promedio de 4.484 ataques semanales por organización, cifra que representa un aumento del 73 % en comparación con el año anterior. El segundo sector más afectado fue el gubernamental, con un promedio de 2.768 ataques por organización por semana, equivalente a un incremento del 51 % respecto de 2024. En tercer lugar, se situó el sector de telecomunicaciones, que experimentó 2.664 ataques semanales por organización y evidenció la mayor variación interanual, con un alza del 94 %.

El análisis regional del informe muestra, además, una marcada disparidad geográfica. África registró el promedio más elevado de ataques, con 3.286 incidentes semanales por organización. En contraste, Latinoamérica, aunque presentó un promedio ligeramente menor (2.640 ataques), exhibió el crecimiento más pronunciado a nivel global, con un incremento del 108 % en relación con el año anterior [Check Point Research, 2025].

Con el avance de las tecnologías de control y automatización, gran parte de la infraestructura de la cual depende la población —como los sistemas de suministro de agua, electricidad y gas— se ha transformado en un frente adicional en los conflictos bélicos contemporáneos. Contar con personal capacitado en el manejo de estas tecnologías constituye una ventaja estratégica, ya que permite afectar los sistemas que regulan los servicios básicos, generando inestabilidad tanto en el adversario como en su población civil. Un ejemplo particularmente ilustrativo corresponde al conflicto entre Ucrania y Rusia, iniciado el 24 de febrero de 2022, en el cual se han desplegado múltiples ciberataques con el objetivo de interrumpir el acceso a dichos servicios por parte del enemigo.

Uno de los primeros ataques documentados durante esta guerra fue reportado el 12 de abril de 2022 por el *Computer Emergency Response Team of Ukraine* (CERT-UA). Este ataque presentaba características similares a otro registrado en 2016, también dirigido contra Ucrania. La empresa eslovaca ESET, especializada en soluciones de ciberseguridad, identificó el uso de un *malware* denominado *Industroyer2*, diseñado para comprometer la red eléctrica del país. Posteriormente, la alianza de inteligencia *Five Eyes*, integrada por Australia, Canadá, Nueva Zelanda, el Reino Unido y Estados Unidos, atribuyó tanto este ataque como el de 2016 al GRU, la agencia de inteligencia militar de Rusia [Cerf, 2024]. Lo distintivo de este episodio radica en que el *malware* tenía como objetivo la infraestructura física, cuando lo habitual es que los ataques se concentren en sistemas computacionales o financieros.

El único antecedente comparable de un *malware* orientado contra infraestructura física es el caso de *Stuxnet*, detectado en junio de 2010. Este ataque comprometió el sistema SCADA (*Supervisory Control and Data Acquisition*), empleado en el control industrial de una planta de enriquecimiento de uranio en Irán [Kushner, 2013].

La realidad contemporánea evidencia que la infraestructura moderna, incluidos los suministros básicos y una amplia gama de servicios, depende de manera ineludible de sistemas computacionales. Esta dependencia es irreversible, dado que las ventajas que tales sistemas ofrecen en términos de monitoreo, velocidad y control superan ampliamente las vulnerabilidades que puedan presentar.

En este contexto, los ataques dirigidos contra sectores críticos ponen de manifiesto la necesidad imperiosa de fortalecer la resiliencia de la infraestructura. Una de las estrategias fundamentales para alcanzar este objetivo radica en la formación de especialistas con las competencias necesarias para garantizar su protección.

Sin embargo, la disponibilidad de este tipo de capital humano no es un fenómeno homogéneo ni garantizado, lo que ha generado preocupación a nivel internacional y ha motivado diversos estudios para dimensionar la magnitud del problema.

1.1.1. Problema a nivel global

En el escenario actual, se reconoce la existencia de un riesgo tangible: los sistemas computacionales de los que depende la sociedad contemporánea se encuentra en un estado de constante amenaza. La primera línea de defensa frente a esta situación la constituyen los profesionales de la ciberseguridad. Sin embargo, surge la interrogante de si su número y capacidades son suficientes para resguardar la totalidad de los sistemas a nivel mundial. La evidencia indica que no es así.

En el informe previamente citado, realizado por la *(ISC)²* correspondiente a la edición 2024, se detalla que la brecha global asciende específicamente a 4.762.963 profesionales adicionales, lo que confirma un incremento del 19,1 % respecto de 2023 [ISC2, 2024].

Dentro de las razones identificadas por los encuestados para explicar la persistencia de esta brecha, destacan las siguientes:

- **Limitaciones presupuestarias como principal causa de la reducción de talento y carencias en habilidades**:

  La mayoría de los encuestados señaló que sus organizaciones carecen de los recursos financieros necesarios para contratar el número suficiente de profesionales que cubran los diversos roles asociados a la seguridad. Este hallazgo contrasta con la tendencia observada en el estudio del año anterior, donde la causa predominante era la dificultad de encontrar personal con las competencias requeridas.

- **Escasez de personal calificado y limitadas oportunidades de capacitación**:

  Muchos equipos de ciberseguridad reportan no contar ni con el número suficiente de integrantes ni con el rango adecuado de habilidades para alcanzar sus objetivos estratégicos. La situación se ha visto agravada por el estado de la economía global, que ha obligado a las organizaciones a reducir personal y restringir presupuestos. Si bien se ha registrado un aumento en la demanda de especialistas capaces de proteger eficazmente a las organizaciones, los empleadores han disminuido las contrataciones y limitado las oportunidades de desarrollo profesional de su personal. Como consecuencia, cerca del 60 % de los encuestados reconoció que estas deficiencias en habilidades han tenido un impacto significativo en su capacidad para resguardar a sus organizaciones, mientras que un 58 % declaró que esta situación las coloca en una posición de riesgo.

- **Cambio en las prioridades de los profesionales**:

  Aunque los especialistas en ciberseguridad continúan manifestando interés por su desarrollo profesional, se observa una creciente tendencia a priorizar el equilibrio entre la vida laboral y personal. Este fenómeno se refleja en el perfil etario de quienes ingresan al campo: una proporción considerable de los nuevos profesionales, aproximadamente un 35 %, corresponde a individuos que comenzaron a trabajar en ciberseguridad entre los 39 y 49 años, lo que sugiere un cambio en las motivaciones y expectativas respecto de la carrera.

El escenario actual evidencia con claridad las dificultades existentes para cubrir la creciente demanda mundial de especialistas en ciberseguridad. Esta problemática responde a múltiples factores, que abarcan tanto las características y limitaciones de los procesos de formación en las distintas instituciones educativas, como las condiciones a las que se enfrentan los profesionales una vez insertos en el campo laboral. Asimismo, influyen de manera decisiva los recursos disponibles para el desempeño de sus funciones, los cuales en muchos casos resultan insuficientes para responder de manera eficaz a las crecientes exigencias del entorno digital.

1.1.2. Problema a nivel local

Esta situación no es exclusiva del contexto internacional. América Latina también enfrenta un déficit considerable de talento especializado en ciberseguridad. De acuerdo con el informe anteriormente citado, la región presenta una necesidad de 328.397 especialistas en el área, lo que, si bien representa una disminución del 5,7 % respecto al déficit estimado en 2023 [ISC2, 2024], continúa evidenciando una brecha significativa.

En cuanto a la fuerza laboral existente, el mismo estudio reporta que en 2024 la región cuenta con 1.273.868 profesionales activos en ciberseguridad, cifra que supone una leve

disminución del 0,9 % en comparación con el año anterior [ISC2, 2024]. Estos datos reflejan que, a pesar de ciertos avances, persisten limitaciones estructurales que dificultan el desarrollo de capacidades suficientes para responder a las crecientes amenazas digitales en el contexto latinoamericano.

Otro estudio relevante sobre el estado del campo de la ciberseguridad fue realizado por *Kaspersky*, una empresa multinacional rusa especializada en soluciones de ciberseguridad y antivirus. La investigación consistió en una encuesta aplicada a 1.012 especialistas de 29 países que trabajan en el área de seguridad de la información (InfoSec), abarcando un rango diverso de niveles de experiencia.

Los resultados muestran que el 48 % de las empresas encuestadas en América Latina describen a sus equipos de ciberseguridad como "algo escasos" o "significativamente escasos"de personal. Comparado al nivel global, el promedio registrado fue de 41 %, siendo las organizaciones rusas las que reportaron la mayor escasez (67 %), mientras que las instituciones de Norteamérica manifestaron la menor (14 %) [Kaspersky, sf].

Si bien los datos sugieren una mejora marginal, dado que la cantidad de especialistas que abandona el área es inferior a la que ingresa, este progreso ocurre a un ritmo considerablemente lento. En consecuencia, la región aún se encuentra lejos de cubrir las necesidades reales de protección cibernética, lo que plantea un escenario de vulnerabilidad que podría derivar en problemáticas de gran escala si no se adoptan medidas correctivas oportunas.

1.1.3. Problema en Chile

En el caso particular de Chile, la situación no difiere del escenario regional y global previamente descrito. La creciente digitalización del país, impulsada por el aumento sostenido de empresas y personas conectadas a Internet, la masificación del comercio electrónico y la digitalización de servicios esenciales ha incrementado significativamente la superficie de ataque para los ciberdelincuentes.

La Asociación de Empresas Chilenas de Tecnología (CHILETEC) advirtió que, durante la primera mitad de 2024, los ciberataques aumentaron en un 30 %, afectando de manera especial a sectores críticos como telecomunicaciones, salud y servicios financieros. Entre las principales amenazas identificadas se encuentra el *ransomware*, situando a Chile en el cuarto lugar de América Latina en cantidad de incidentes reportados. Una cifra que refleja la vulnerabilidad del entorno nacional es que siete de cada diez PYMES carecen de medidas de seguridad adecuadas para proteger sus activos digitales [Chiletec, 2024].

En cuanto al déficit de capital humano especializado, se estima que actualmente en Chile faltan 25.000 profesionales en ciberseguridad, cifra que podría aumentar a 47.000 en 2029 y alcanzar los 76.000 en 2035, siendo las áreas más demandadas la gestión de riesgos, el análisis de vulnerabilidades y la respuesta a incidentes [Chiletec, 2024].

A nivel de volumen de ataques, un reporte de la empresa de ciberseguridad Fortinet indicó que Chile experimentó un alza significativa en los intentos de intrusión, pasando de 6.000 millones en 2023 a 27.600 millones en 2024, lo que refleja la magnitud de la amenaza a nivel nacional [El Mostrador, sf].

Finalmente, de acuerdo con Cristian Bravo, jefe del Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), en el país faltarían más de 28.000 profesionales en ciberseguridad, proyectándose que esta brecha solo podría cerrarse hacia 2033, según lo expuesto en el Seminario Internacional de Ciberseguridad organizado por la Pontificia Universidad Católica de Valparaíso (PUCV) y la Embajada de Israel en Chile [La Tercera, 2023].

Cabe señalar que, si bien la situación nacional refleja una importante brecha en materia de ciberseguridad, no todo el panorama resulta desfavorable. En Chile se han implementado medidas concretas para hacer frente a las crecientes amenazas digitales. Una de las más relevantes es la creación de la Agencia Nacional de Ciberseguridad (ANCI), institución establecida por la Ley Marco de Ciberseguridad y que comenzó a operar el 2 de enero de 2025. Esta agencia tiene como misión fortalecer las capacidades institucionales del país en materia de ciberseguridad, combatir el cibercrimen, fiscalizar y regular a las entidades que prestan servicios esenciales, así como sancionar incumplimientos. Adicionalmente, asesora al Presidente de la República en la formulación de políticas nacionales, administra la red de conectividad segura del Estado y promueve la educación y cultura en ciberseguridad [ANCI, 2025b, ANCI, 2025a].

El impacto de estas medidas ya se ha visto reflejado en indicadores internacionales. De acuerdo con el National Cyber Security Index (NCSI), que evalúa las capacidades de más de 100 países para enfrentar ciberataques, considerando variables como legislación, organismos especializados, estrategias preventivas y capacidad de respuesta, Chile logró un avance significativo: en 2024 se encontraba en la posición 25, y tras la instauración de la ANCI y la entrada en vigor de la Ley Marco de Ciberseguridad, ascendió al puesto 21, consolidándose como el país mejor calificado de América Latina, con un cumplimiento del 83,3 % de los componentes evaluados [NCSI, sf].

En síntesis, aunque en Chile la brecha de profesionales especializados en ciberseguridad continúa siendo un desafío urgente, la creación de instituciones como la ANCI representa un avance significativo en el fortalecimiento de las capacidades nacionales. No obstante, para enfrentar de manera integral las amenazas actuales y futuras, resulta indispensable complementar estas medidas con una estrategia sostenida de formación de capital humano, que permita disponer de profesionales altamente capacitados para resguardar la infraestructura crítica y proteger a la sociedad frente a la creciente actividad cibercriminal.

1.2. Problema específico

Como institución líder en ingeniería, ciencia y tecnología, la UTFSM tiene una responsabilidad fundamental en la formación de profesionales capaces de enfrentar los desafíos de la ciberseguridad. Sin embargo, la carrera de Ingeniería Civil Informática carece de una línea formativa sólida en este ámbito, lo que disminuye su competitividad académica al omitir un área de gran relevancia en la actualidad.

Si bien se han realizado esfuerzos, como la reciente reformulación del plan de estudio que incorpora la asignatura "Redes y Ciberseguridad", se considera que dicha medida resulta insuficiente. La ciberseguridad constituye una disciplina amplia y multidisciplinaria; reducir su estudio únicamente a la defensa de redes computacionales deja de lado aspectos igualmente relevantes, como el desarrollo seguro de software, la protección de datos, la gestión de riesgos o la contratación de personal especializado.

Esta carencia repercute directamente en los egresados, quienes enfrentan desventajas en el mercado laboral frente a profesionales formados en instituciones que han incorporado la ciberseguridad de manera más explícita en sus planes de estudio. Por ejemplo, la Universidad Santo Tomás, en la carrera de Ingeniería Civil en Informática y Sistemas Inteligentes, incluye la asignatura obligatoria "Cyberseguridad" [UST, sf]. De igual manera, la Universidad de Santiago de Chile (USACH), en su carrera de Ingeniería Civil en Informática, no solo contempla la asignatura básica de "Redes de Comunicación", sino que además incorpora asignaturas orientadas a la gestión de servicios, tales como "Gestión de Servicios TI" y "Gobernanza y Gestión TI". Asimismo, el plan curricular incluye una asignatura específica de "Ciberseguridad" en el octavo semestre [USACH, sf]. Incluso a nivel de formación técnica, el Instituto Profesional Santo Tomás, en la carrera de Ingeniería en Informática, contempla unidades de especialización en ciberseguridad, que incluyen las asignaturas obligatorias "*Pentesting*" y "Ciberseguridad" [IPST, sf].

Es importante destacar que, en todos los casos mencionados, las asignaturas de ciberseguridad son de carácter obligatorio para sus respectivos programas de estudios, lo que evidencia la relevancia que otras instituciones otorgan a esta disciplina dentro de la formación profesional. Esta situación contrasta con la realidad de la UTFSM, donde, en ambos planes curriculares vigentes a septiembre de 2025, el plan de estudio 7313 no contempla ninguna asignatura obligatoria en la materia. Por su parte, el nuevo plan de estudio 7310 incluye únicamente la signatura "Redes y Ciberseguridad", lo cual resulta insuficiente si se considera la amplitud y complejidad que caracteriza a ambas áreas. La integración de ambos contenidos en una única asignatura puede derivar en un planteamiento superficial, dejando a una de las áreas —o incluso a ambas— con un tratamiento deficiente en términos de profundidad o alcance conceptual.

En consecuencia, la ausencia de una formación estructurada y progresiva en ciberseguridad dentro del plan formativo de la UTFSM genera una brecha significativa en la preparación de sus egresados frente a las demandas actuales del mercado laboral y los estándares educativos adoptados por otras instituciones. Esta carencia limita las oportunidades de especialización temprana, dificulta el desarrollo de competencias técnicas relevantes para el ejercicio profesional y disminuye la competitividad académica y profesional de los estudiantes. Por tanto, se hace necesaria la incorporación de una línea complementaria de ciberseguridad que permita abordar de manera sistemática y coherente los conocimientos, habilidades y enfoques requeridos en esta disciplina.

1.3. Objetivos del Trabajo

1.3.1. Objetivo general

Diseñar una línea complementaria en ciberseguridad para la carrera de Ingeniería Civil Informática de la UTFSM, con el propósito de ofrecer una trayectoria formativa estructurada que facilite la elaboración de un plan curricular y permita superar las limitaciones actuales de la oferta institucional, la cual resulta insuficiente tanto en cantidad como en profundidad de contenidos.

1.3.2. Objetivos específicos

- Analizar la oferta académica existente en programas de educación superior en Chile relacionados con la ciberseguridad, con el fin de identificar las áreas de la disciplina actualmente abordadas.
- Clasificar las asignaturas identificadas de acuerdo con las áreas y contenidos establecidos en el marco de referencia *CSEC2017*, para poder compararlas con otros marcos existentes en ciberseguridad.
- Elaborar tres propuestas de diseño de currículos considerando distintos escenarios en función del número de asignaturas y áreas a impartir, para sentar las bases de la línea complementaria.
- Validar la propuesta curricular desarrollada mediante la consulta a expertos en el área, con el fin de evaluar su factibilidad tanto en términos de pertinencia y adecuación de los contenidos como en relación con las restricciones académicas y la disponibilidad real de cursos.

1.4. Alcance

El análisis de programas de ciberseguridad se restringe a instituciones chilenas, abarcando todos los niveles de educación superior: programas técnicos, de pregrado, posgrado y diplomados.

La formulación de la línea complementaria de ciberseguridad se circunscribe exclusivamente a la carrera de Ingeniería Civil Informática de la UTFSM. El alcance del trabajo se limita al diseño del contenido y su distribución en cursos coherentes, que se articulen con los conocimientos generales ya presentes en el plan de estudio de la carrera.

La implementación práctica de dicha línea queda fuera del alcance de este estudio, dado que involucra aspectos administrativos, de infraestructura y de gestión institucional que exceden la temática abordada, y cuya materialización dependerá de las condiciones existentes en el momento en que se decida llevarla a cabo.

1.5. Impacto de solucionar el problema

La incorporación de una línea formativa en ciberseguridad en la carrera de Ingeniería Civil Informática de la UTFSM tendría un impacto significativo, tanto a nivel institucional como en la proyección profesional de sus egresados. Por una parte, la universidad fortalecería su posición competitiva frente a otras instituciones de educación superior que no han desarrollado con la misma profundidad esta disciplina, consolidándose como un referente nacional en la formación de especialistas en el área.

Además, los egresados se verían beneficiados al contar con una preparación sólida en un campo altamente demandado y mejor remunerado [IT HUNTERS, 2025], lo que ampliaría sus oportunidades laborales y mejoraría su empleabilidad. Por otra parte, una formación integral en ciberseguridad contribuiría a que los futuros profesionales desarrollen las competencias necesarias para diseñar, implementar y mantener sistemas más seguros, confiables y resilientes, respondiendo así a una necesidad crítica tanto para el sector productivo como para la sociedad en general.

CAPÍTULO 2
MARCO CONCEPTUAL

La ciberseguridad, como disciplina, presenta una problemática interesante al momento de definirla y delimitarla. Si bien es evidente que forma parte del ámbito de las ciencias de la computación y, por lo tanto, se vincula estrechamente con la matemática, la lógica y otras áreas afines, su particularidad radica en la relación que mantiene con otras áreas del quehacer humano. La ciberseguridad se relaciona con disciplinas como las ciencias sociales y humanas, tales como la sociología y la psicología; y al ámbito legislativo, cuando se debe cumplir con regulaciones nacionales e internacionales. En este contexto, diversos esfuerzos se han orientado a precisar los límites de las áreas del conocimiento relacionadas con la ciberseguridad y, de manera más específica, a determinar cuáles de esos conocimientos deben ser impartidos a los estudiantes.

Este capítulo establece las bases conceptuales que sustentan el desarrollo de esta memoria. Su propósito principal es presentar algunos de los intentos más relevantes por estructurar la enseñanza de la ciberseguridad, así como explicar cuáles de ellos fueron considerados para fundamentar nuestra propuesta de solución.

2.1. *Frameworks* de ciberseguridad

Antes de continuar, es necesario aclarar qué se entiende por *framework*. El término proviene del inglés, y la definición que más se ajusta al propósito de este estudio es la ofrecida por el diccionario de Cambridge: *A system or set of rules*. [Cambridge Dictionary, sf], que en español se traduce como "un sistema o conjunto de reglas". Los *frameworks* se utilizan en diversos contextos y cumplen el rol de establecer las bases de un proyecto mayor, ya sea a nivel de contenidos y estructura, como es en el ámbito de la educación, o estableciendo patrones y componentes prehechos en el ámbito tecnológico, como en el desarrollo de software, donde son ampliamente utilizados.

En el contexto de este trabajo, los *frameworks* en ciberseguridad tienen como objetivo delimitar, dentro de los dominios del conocimiento, aquello que resulta relevante para esta disciplina. Esto incluye no solo aspectos técnicos vinculados a la computación como la teoría computacional, criptografía y las redes de computadores, sino también elementos provenientes de la sociología, la psicología, la gestión de organizaciones, entre otros. Los *frameworks* que aquí se analizan están específicamente relacionados con la educación en ciberseguridad; en consecuencia, buscan además establecer objetivos de aprendizaje, tanto prácticos como teóricos, para las personas que deseen desarrollarse en el área.

2.1.1. NICE *Framework*

El *National Institute of Standards and Technology* (NIST) es una institución estatal de Estados Unidos fundada en 1901, cuya misión es impulsar el desarrollo científico y tecnológico del país. Entre sus funciones principales se encuentra la elaboración de estándares en distintas áreas, incluyendo los relacionados con la ciberseguridad.

En el marco de su labor de establecer estándares, el NIST desarrolló el *NICE Workforce Framework for Cybersecurity*, conocido en adelante en este documento como *NICE Framework* o simplemente *NICE* [NIST, 2019]. Este fue publicado en la *NIST Special Publication 800-181* en agosto de 2017. Su primera versión se basó en un trabajo previo iniciado en 2007 por distintas instituciones, con el propósito de evaluar al personal federal en materia de ciberseguridad.

El *NICE* tiene como finalidad proporcionar un lenguaje común para describir el trabajo en ciberseguridad, así como los conocimientos y habilidades necesarios para desempeñarlo. Su público objetivo es amplio: busca servir de guía tanto a empleadores de organizaciones públicas y privadas, como a instituciones educativas, proveedores de servicios y desarrolladores de herramientas vinculadas con la ciberseguridad.

La formulación del *NICE Framework* ofrece una serie de ventajas, entre las que destacan:

- Promueve la movilidad profesional, al visibilizar la diversidad de roles existentes en ciberseguridad.
- Contribuye al desarrollo curricular en instituciones educativas.
- Favorece instancias formativas previas al empleo, como prácticas profesionales, acercándolas a los roles demandados en la industria.
- Facilita la creación de descripciones de cargos y puestos de trabajo, además de proveer mecanismos para evaluar las competencias de los candidatos.
- Permite generar información sobre la fuerza laboral, lo que beneficia investigaciones y análisis de tendencias en la industria.

El *NICE* ha evolucionado a lo largo de los años [NIST, 2025], siendo sus hitos más relevantes los siguientes:

- **Agosto 2017**: Publicación de la primera versión del *framework* en la *NIST Special Publication (SP) 800-181*, conocida como versión 2017.
- **Noviembre 2020**: Publicación de la *SP 800-181 Rev. 1*, que reemplazó a la versión inicial.

- **5 de marzo de 2024**: Publicación de los componentes la primera versión numerada, versión 1.0.0, alineados con la Rev. 1. Esta actualización incluyó:
  - Mapeo de los *Knowledge, Skills, Abilities (KSA)* y *Tasks* de 2017 con los *Tasks, Knowledge y Skills* de la versión 1.0.0.
  - Mapeo de las categorías y roles de trabajo de 2017 con las de la versión 1.0.0.
  - Identificación de áreas de especialidad (*Specialty Areas*) que fueron retiradas, así como la incorporación de nuevas *Competency Areas*.
- **5 de marzo de 2025**: Publicación de la versión 2.0.0 de los componentes del NICE Framework. Esta versión introdujo cambios específicos:
  - Actualización de tres *Work Roles* y una *Competency Area*.
  - Eliminación de dos categorías de roles de trabajo (*Work Role Categories*) junto con los roles asociados.

El *NICE Framework* busca establecer un lenguaje común que permita describir el trabajo en ciberseguridad, así como los conocimientos y habilidades necesarios para desempeñarlo.

Para lograr este objetivo el *framework* define algunos conceptos para poder organizar y estructurar su contenido. A continuación, se definen los siguientes conceptos fundamentales:

- ***Work Role***: Agrupación de tareas y responsabilidades que recaen sobre un individuo o equipo. No son sinónimos de puestos de trabajo u ocupaciones específicas.
- ***Work Role Category***: Agrupación de *Work Roles* en funciones mayores. Son independientes de los títulos de trabajo u otros términos ocupacionales, y se utilizan de manera amplia para reflejar la variedad e interdisciplinariedad del trabajo en ciberseguridad.
- ***Task***: Actividad orientada a lograr un objetivo organizacional específico.
- ***Skill***: Capacidad para ejecutar acciones observables.
- ***Knowledge***: Conjunto de conceptos y principios que pueden recuperarse de la memoria.

Cada uno de los elementos definidos en el *NICE Framework*, *Tasks*, *Skills* y *Knowledge*, se presentan por medio de una frase, un *Statement*, además de esto, existe una descripción asociada que da mayor contexto a la frase inicial. Para los fines de este trabajo, el componente más relevante es el de *Knowledge*, ya que a través de sus descripciones (en adelante, *Knowledge Descriptions* o KD) se especifican los conocimientos que deben ser

adquiridos por los estudiantes. Estos constituyen, por tanto, la base para orientar el diseño de un currículo educativo en ciberseguridad.

Para el desarrollo de este trabajo se optó por utilizar dos versiones del marco NICE: la versión original publicada en 2017 y su primera actualización oficial, la versión 1.0.0 publicada en 2024. Esta decisión responde a que ambas aportan elementos relevantes y complementarios para el análisis, las razones específicas de esta eleccion serán expuestas con mayor detalle en secciones posteriores.

2.1.2. CSEC2017 *Curricular Guidelines*

La *Joint Task Force on Cybersecurity Education* (JTF) fue conformada en septiembre de 2015 como una colaboración entre importantes sociedades internacionales del área de la computación:

- Association for Computing Machinery (ACM).
- IEEE Computer Society (IEEE-CS).
- Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC).
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8).

Esta agrupación se creó con el objetivo de desarrollar guías curriculares comprensivas y flexibles en educación en ciberseguridad, destinadas a apoyar futuros programas en distintos niveles de enseñanza. Además, buscó elaborar un volumen curricular que estructurara la disciplina de la ciberseguridad y que sirviera de guía para instituciones interesadas en desarrollar o actualizar programas y cursos. Todo esto sin restringir el documento a un único tipo de programa académico.

El *Cybersecurity Curricula 2017* (CSEC2017) es un documento publicado en su versión 1.0 el 31 de diciembre de 2017 [ACM, sf]. Este texto ofrece una visión integral de la disciplina de la ciberseguridad desde una perspectiva curricular. Además, presenta un marco de referencia curricular y lineamientos destinados a guiar el desarrollo de contenido académico en esta área.

El CSEC2017 establece un público objetivo primario y uno secundario. El público primario está constituido por miembros de facultades en disciplinas relacionadas con la computación, en instituciones académicas de todo el mundo, que tengan interés en crear programas de ciberseguridad o mejorar los ya existentes.

El público secundario corresponde a actores externos al ámbito académico que necesiten definir o implementar programas vinculados a la ciberseguridad. Entre ellos se incluyen empresas que buscan capacitar a su personal, responsables de políticas públicas que requieren fundamentos para la toma de decisiones, y proveedores de cursos o certificaciones de desarrollo profesional, entre otros.

Para estructurar el conocimiento en ciberseguridad, el CSEC2017 define una serie de conceptos fundamentales que organizan el contenido curricular de manera jerárquica. Estos son los siguientes:

- ***Knowledge Areas* (KA):** Constituyen la base de la organización del contenido de ciberseguridad. Cada área abarca conocimientos críticos de amplia relevancia, que involucran múltiples disciplinas de la computación. No son estructuras rígidas, lo que permite su expansión o contracción según sea necesario. En conjunto, las KA representan la totalidad del conocimiento del campo de la ciberseguridad.
- ***Essentials*:** Se refieren a los conceptos esenciales de cada KA, los cuales representan la competencia mínima que los estudiantes deben alcanzar, independientemente del enfoque particular del programa académico.
- ***Knowledge Units* (KU):** Son agrupaciones temáticas que integran tópicos relacionados dentro de una KA.
- ***Topics*:** Corresponden al contenido curricular específico de cada KU.
- ***Description / Curricular Guidance*:** Cada tópico incluye una descripción o guía curricular, que explicita los conocimientos que deben ser impartidos. Además, se entregan sugerencias sobre los conceptos, cuales sería apropiado enfatizar, en que orden entregarlos o si es posible relacionarlo con otros conceptos.
- ***Learning Outcomes*:** Se trata de descripciones que establecen lo que el estudiante debe saber o ser capaz de hacer al finalizar el aprendizaje. Estos resultados pueden referirse tanto a conocimientos técnicos como a habilidades prácticas.

El CSEC2017 identifica ocho áreas principales de la ciberseguridad, denominadas *Knowledge Areas* (KA):

- ***Data Security***: Se centra en la protección de los datos durante su almacenamiento, procesamiento y transmisión. Esta KA requiere la aplicación de conocimientos matemáticos y de análisis algorítmico.
- ***Software Security***: Aborda el desarrollo y uso de software que preserve de manera confiable las propiedades de seguridad de la información y de los sistemas que protege. Incluye la integración de la seguridad en todo el ciclo de vida del desarrollo de software, así como las consideraciones éticas que puedan surgir en su creación, implementación, uso y retiro.

- ***Component Security***: Orientada a garantizar que los componentes, ya sean desarrollados internamente o adquiridos a terceros, cumplan con los requisitos de seguridad necesarios para no debilitar los sistemas en los que se integran. Comprende el diseño, adquisición, prueba, análisis y mantenimiento de componentes dentro de sistemas más amplios.
- ***Connection Security***: Se enfoca en la seguridad de las conexiones entre componentes, tanto físicas como lógicas. Cubre el conocimiento esencial para asegurar la correcta interconexión entre sistemas y componentes individuales a través de redes, como Internet.
- ***System Security***: Abarca los aspectos de seguridad relacionados con sistemas completos, considerando no solo las interacciones entre sus componentes, sino también la visión integral del sistema en su conjunto.
- ***Human Security***: Dirigida a la protección de los datos y la privacidad de los individuos, tanto en el contexto organizacional (por ejemplo, empleados) como en su vida personal. Además, estudia cómo el comportamiento humano influye en la ciberseguridad.
- ***Organizational Security***: Orientada a la protección de las organizaciones frente a amenazas de ciberseguridad y a la gestión de riesgos con el fin de garantizar el cumplimiento de su misión. Incluye aspectos como la legislación, regulaciones y estándares aplicables, así como la elaboración de políticas internas de seguridad.
- ***Societal Security***: Aborda los aspectos de la ciberseguridad que impactan a la sociedad en su conjunto, tales como el cibercrimen, las leyes, la ética, las políticas públicas y la privacidad.

Este *framework* es el que se trabaja con mayor profundidad en este documento. De él se retoman, para su uso posterior, los conceptos de *Knowledge Areas* (KA), *Knowledge Units* (KU), *Topics* y sus descripciones, los cuales permiten estructurar de manera detallada el contenido curricular en ciberseguridad.

2.1.3. Otros *frameworks* de ciberseguridad

Los marcos de referencia descritos anteriormente no son los únicos existentes. En distintos contextos internacionales, múltiples instituciones y asociaciones vinculadas a la computación y a la seguridad de la información han realizado esfuerzos por definir y estructurar la ciberseguridad desde diversas perspectivas.

European Cybersecurity Skills Framework (ECSF)

La Agencia de la Unión Europea para la Ciberseguridad, conocida por las siglas en inglés de su nombre original, ENISA (*European Network and Information Security Agency*), es la institución encargada de promover y alcanzar un alto nivel de ciberseguridad en toda Europa [ENISA, sf]. En septiembre de 2022 se publicó el *European Cybersecurity Skills Framework* (ECSF). De forma similar al NICE, el ECSF es un *framework* que identifica las tareas, competencias, habilidades y conocimientos asociados a los roles profesionales en ciberseguridad dentro del contexto europeo. Su propósito es establecer una terminología común que facilite el desarrollo de programas de formación, apoyar a los empleadores en la contratación de profesionales de acuerdo con sus necesidades específicas, e incorporar además aspectos diferenciadores como las habilidades blandas y los marcos legislativos propios de la Unión Europea.

El ECSF está compuesto por dos documentos principales:

- *European Cybersecurity Skills Framework Role Profiles*: Propone 12 perfiles profesionales en ciberseguridad. Para cada uno se describen su función, tareas principales, habilidades clave, conocimientos fundamentales y otros atributos relevantes [ENISA, 2022b].
- *European Cybersecurity Skills Framework (ECSF) – User Manual*: Expone los fundamentos del ECSF, sus casos de uso y su aplicación desde distintas perspectivas [ENISA, 2022a]:
  - Organizaciones, que pueden emplearlo para mejorar sus prácticas de ciberseguridad, reclutar profesionales especializados o incluso estructurar departamentos completos en el área.
  - Proveedores de educación, que pueden revisar y adaptar sus currículos para alinearlos mejor con las necesidades tanto de la industria como de los estudiantes.
  - Profesionales individuales, que encuentran en este marco una guía para orientar sus trayectorias profesionales hacia los roles que desean alcanzar.

El ECSF comparte con el NICE un enfoque centrado en la fuerza laboral y los roles de trabajo. Sin embargo, el ECSF posee una fuerte especificidad en el contexto de la Unión Europea, ademáas existe una falta de recursos que lo relacionen directamente con marcos de carácter académico, como el CSEC2017. El NICE, en cambio, sí cuenta con mapeos establecidos hacia este último. Cabe destacar que tanto el ECSF como el NICE no distinguen puestos de trabajos reales; no obstante, existen iniciativas de mapeo hacia bases de datos de empleos: el *ETO-CSET NICE-O*NET Crosswalk* [CSET/ETO, 2024] en el caso del NICE para trabajos en Estados Unidos, y el *Crosswalk between ESCO and ECSF* para el ECSF para trabajos de la Unión Europea [ENISA, 2024].

Cyber Security Body of Knowledge (CyBOK)

Uno de los proyectos más completos que existen para delimitar las áreas de conocimiento de la ciberseguridad es el *Cyber Security Body of Knowledge* (CyBOK) [CyBOK, sf]. El proyecto es financiado por el *National Cyber Security Programme* de Reino Unido y dirigido por Awais Rashid, profesor de la Universidad de Bristol en conjunto con expertos del área de todo el mundo. Este conjunto de especialistas publicó su primera versión, el CyBOK 1.0 el 31 de octubre de 2019 como respuesta a los distintos *frameworks* que surgieron en los años previos, dentro de ellos los ya mencionados. Existía la necesidad de saber cómo estos se comparaban entre sí, que contenidos cubrían, como los distintos énfasis daban forma a los cursos y como estos a su vez resultaban en variados conjuntos de habilidades. La versión más reciente, 1.1.0, identifica 21 áreas de conocimiento (KA) agrupadas en cinco categorías principales: *"Human, Organisational and Regulatory Aspects"*, *"Attacks and Defences"*, *"Systems Security"*, *"Software and Platform Security"* e *"Infrastructure Security"*.

A diferencia de otros *frameworks* utilizados en el área, el CyBOK no busca servir como guía para el desarrollo de programas académicos o profesionales, como es el caso del CSEC2017 o del NICE. Su propósito es distinto: establecer una base de conocimientos de referencia sobre ciberseguridad, es decir, un *body of knowledge*.

Esto lo convierte en una fuente valiosa de carácter académico, ya que ofrece una visión amplia de los temas que constituyen la ciberseguridad, como estos se relacionan y de que manera se pueden impartir. Sin embargo, su utilidad práctica es limitada, pues no establece objetivos de aprendizaje, competencias esenciales ni metodologías de enseñanza. En consecuencia, la responsabilidad de traducir estos conocimientos en currículos, estrategias educativas y resultados de aprendizaje recae en los diseñadores de programas académicos.

Computing Curricula 2020 (CC2020)

Una publicación también relacionada con los esfuerzos en la educación de la ciberseguridad es el *Computing Curricula 2020* (CC2020) [Impagliazzo y Pears, 2018], publicada el 31 de diciembre de 2020. El CC2020 fue desarrollado en conjunto por la *Association for Computing Machinery* (ACM) y la *IEEE Computer Society* (IEEE-CS). Este informe examina las guías curriculares actuales de programas académicos relacionados con las disciplinas de la computación en general, sin restringirse a solo un subconjunto de conocimientos, como resultaba en los trabajos anteriormente presentados que se enfocaban en ciberseguridad.

El CC2020 aborda el contenido de programas de licenciatura (*undergraduate*), consolidando y actualizando, en un documento, los volúmenes previamente elaborados por el ACM y el IEEE-CS en otras áreas de la computación. Estas incluyen: *Computer Engineering*, *Computer Science*, *Cybersecurity*, *Information Systems*, *Information Technology* y *Software Engineering*. Además, incorpora a *Data Science*, cuyo volumen aún se encuentra en desarrollo.

El objetivo principal del CC2020 es proveer un marco conceptual para la educación en computación, identificando los conocimientos, habilidades y disposiciones relevantes en cada área, bajo el enfoque de *Know-what, Know-how, Know-why*. Es decir, no busca detallar contenidos específicos de cada disciplina, sino más bien ofrecer herramientas y lineamientos generales para su enseñanza. En este sentido, el CC2020 cumple el rol de un *metaframework*: un marco de referencia destinado a guiar la creación y desarrollo de otros *frameworks* curriculares más específicos, como ocurre en el caso de la ciberseguridad con el CSEC2017.

El informe está dirigido a estudiantes, a la industria y al gobierno, así como a educadores y organizaciones educativas, con el fin de apoyar la toma de decisiones y el diseño de programas académicos alineados con las necesidades actuales y futuras de la disciplina.

El CC2020 constituye una fuente valiosa, especialmente como referencia para iniciativas académicas de alcance más general. En lugar de profundizar en las áreas y conocimientos particulares de la disciplina, el CC2020 se centra en lineamientos transversales de la educación en computación, tales como la enseñanza basada en competencias, la visión multidisciplinaria y las consideraciones globales y culturales.

2.2. Educación en ciberseguridad

Como se ha evidenciado, los trabajos desarrollados en torno a la educación en ciberseguridad adoptan enfoques diversos. Algunas instituciones privilegian una formación de carácter académico, centrada en el desarrollo de conocimientos técnicos y fundamentos teóricos de la disciplina. Otras, en contraste, orientan sus programas hacia una perspectiva profesional, priorizando el desarrollo de habilidades prácticas y competencias asociadas a roles específicos que desempeñan los profesionales dentro de las organizaciones.

Sin embargo, entre la formulación de *frameworks* y su implementación efectiva persiste una brecha relevante. En este contexto, resulta fundamental analizar los programas ya existentes en distintas instituciones de educación superior y evaluar en qué medida estos se corresponden con los contenidos y lineamientos propuestos por los marcos de referencia internacionales. Asimismo, se hace necesario realizar una comparación sistemática entre dichos programas, con el fin de identificar aquellos que resulten más idóneos para su eventual implementación, así como analizar su desempeño de manera

individual y determinar si su integración conjunta puede aportar beneficios formativos adicionales.

2.2.1. Oferta de programas internacionales

Frente a esta diversidad de enfoques, distintos estudios han intentado articular vínculos entre la formación conceptual y las necesidades del entorno profesional. Un ejemplo representativo es el trabajo de [Hajny *et al.*, 2021], en el cual se analizó el contenido de 89 programas de diversas instituciones a nivel internacional, tanto de pregrado como de posgrado, estableciendo un mapeo entre dichos contenidos y los requerimientos asociados a los *Work Roles* definidos en el tanto de pregrado como de posgrado, realizando un mapeo de dichos contenidos con los requerimientos de los *Work Roles* definidos en el NICE.

Entre sus hallazgos, observaron que no existe un estándar consolidado en la educación en ciberseguridad. Si bien muchos temas se repiten, la intensidad y el énfasis que reciben varía según el país, el continente e incluso entre universidades de una misma región. En instituciones no europeas predomina el enfoque en aspectos técnicos de seguridad, mientras que en Europa las áreas de énfasis varían no solo entre países, sino también entre universidades de un mismo país, mostrando diferencias significativas en sus métodos de enseñanza. Aun así, se observa una predominancia parcial de áreas como la seguridad, ciencias de la computación y privacidad.

Lo anterior refuerza el objetivo de esta investigación de realizar mediciones similares en instituciones chilenas, pues resulta fundamental que la línea de especialización en ciberseguridad que se proponga responda a las necesidades y problemáticas locales. El análisis de los contenidos impartidos en programas nacionales nos entrega una base sólida para asegurar que nuestros esfuerzos se alineen con la realidad que experimentamos en Chile.

Otro aspecto relevante del estudio de [Hajny *et al.*, 2021] es la identificación de áreas deficientes en la enseñanza de la ciberseguridad. Una de las más notorias es la escasa atención otorgada al tema de la privacidad. Este hallazgo resulta especialmente significativo, ya que en 2025 la privacidad, o la falta de ella, se ha convertido en un problema creciente, donde tanto gobiernos como empresas privadas buscan recopilar la mayor cantidad posible de información sobre nuestro comportamiento. La creación de una línea de ciberseguridad en la formación académica ofrece una oportunidad para generar conciencia sobre la relevancia de este tema, establecer los límites que deberían regir su protección y exigir mayores estándares de privacidad en los servicios de software que utilizamos.

2.2.2. Comparación cualitativa entre *frameworks*

Como ya hemos visto, en el ámbito internacional, diversas entidades, asociaciones y sociedades han desarrollado sus propios *frameworks* de ciberseguridad. Conocer cómo estos se diferencian y se comparan resulta crucial en una investigación como la presente.

El trabajo de [Dkaidek y Rashid, 2024] aborda precisamente esta labor, considerando los *frameworks* CyBOK, CSEC2017, NICE y CST, haciendo la consideración de descartar el ECSF de ENISA por su similitud con el NICE en cuanto a su enfoque en la fuerza laboral.

Cabe destacar dentro del análisis la inclusión del *Cybersecurity Taxonomy (CST)*, también denominado *JRC Cybersecurity Taxonomy*. Tal como su nombre lo indica, este corresponde a una taxonomía, es decir, una clasificación sistemática de conceptos y términos relevantes en el ámbito de la ciberseguridad. Por esta razón, no se considera propiamente un framework orientado al diseño curricular o a la estructuración de competencias, motivo por el cual no fue abordado en las secciones anteriores y se menciona aquí únicamente con fines de contextualización.

Los autores evaluaron los *frameworks* en las siguientes categorías: implementación global, conocimientos fundamentales, capacidad de guiar currículos y relevancia.

De su análisis se obtuvieron los siguientes resultados: el NICE es el más comprensivo, ya que incluye explícitamente las competencias y habilidades requeridas por los profesionales, a diferencia del CST que no posee esta característica. El CyBOK destaca en los aspectos de "conocimientos fundamentales", "capacidad de guiar currículos" e "implementación global". El CSEC2017 presenta un desempeño similar en esas mismas dimensiones. Sin embargo, su desventaja radica en la menor frecuencia de sus actualizaciones, lo que afecta a su relevancia. En particular, sobresale la utilidad del NICE en el ámbito profesional, al detallar las competencias necesarias para desempeñar labores específicas. Asimismo, este *framework* resulta valioso para guiar la creación de cursos de especialización, debido a su carácter más prescriptivo.

Este estudio evidencia que ningún *framework* resulta completamente exhaustivo o libre de limitaciones. Cada uno presenta falencias en distintos aspectos, ya sea en su relevancia, en su aplicabilidad para la creación de currículos, en la amplitud y profundidad de los conocimientos que abarca, o en el enfoque —académico o profesional— que adopta. Los hallazgos del trabajo sugieren, por tanto, que la utilización complementaria de múltiples frameworks podría resultar beneficiosa, al permitir mitigar las debilidades individuales de cada uno y favorecer una aproximación más integral al diseño curricular en ciberseguridad.

2.2.3. Comparación cuantitativa entre NICE y CSEC2017

En la creación de frameworks se pueden adoptar distintos enfoques, tanto en relación con el público objetivo como en la forma de enseñar los contenidos o en la selección de los temas a profundizar. Si bien pueden existir similitudes entre ellos, no siempre está garantizada su compatibilidad. La investigación de [Yar *et al.*, 2024] demuestra, para el caso específico de los *frameworks* NICE y CSEC2017, los dos utilizados en esta investigación, que sí existe un alto grado de compatibilidad.

Para verificar esta relación, los investigadores emplearon *Bidirectional Encoder Representations from Transformers* (BERT), una tecnología propia de modelos de lenguaje natural. El procedimiento consistió en tokenizar, por un lado, los *learning outcomes* de cada *Knowledge Area* (KA) del CSEC2017, y por otro, los enunciados de conocimientos, habilidades y destrezas (*KSA statements*) de cada *Specialty Area* descrita en la versión 2017 del NICE. Posteriormente, se aplicó un análisis de *cosine similarity*, técnica que mide el grado de cercanía semántica entre dos representaciones vectoriales.

Con este método, los autores compararon, de manera cuantitativa, la correspondencia entre los dos frameworks. Entre los hallazgos más relevantes, se destaca que la similitud más alta alcanzó un 92.2 % entre la *Specialty Area Knowledge Management* y el KA *Human Security*, mientras que la más baja fue de 84.2 % entre la *Specialty Area Network Security* y el KA *Software Security*. El uso de un framework como guía para estructurar el contenido curricular constituye una estrategia adecuada; sin embargo, como se ha observado, cada enfoque conlleva limitaciones inherentes. Un marco exclusivamente académico, como el CSEC2017, tiende a privilegiar los fundamentos teóricos, pero puede descuidar el desarrollo de competencias prácticas. Por su parte, los marcos orientados al ámbito profesional, como el NICE, fortalecen las habilidades operativas, pero no siempre garantizan una comprensión conceptual profunda.

Los resultados del estudio no solo validan la compatibilidad conceptual entre ambos frameworks, sino que también respaldan su uso conjunto en el diseño curricular, al evidenciar una alta coherencia entre ambos enfoques. La combinación de estos *frameworks* permite equilibrar conocimiento teórico y aplicabilidad profesional, ofreciendo una base más sólida para la formación especializada.

Por lo tanto, en el diseño de planes curriculares en ciberseguridad, se vuelve necesario complementar diversos *frameworks* para alcanzar una formación integral. No obstante, como se evidenciará en el análisis de programas internacionales y nacionales, esta integración no suele materializarse en la práctica, siendo esta una de las deficiencias que existen en la enseñanza en ciberseguridad.

2.3. Enseñanza en Universidades

A nivel internacional, la educación en ciberseguridad presenta ciertas limitaciones. No se trata de una deficiencia en la calidad de la formación de los estudiantes, sino más bien en la estructura institucional de la oferta académica. En muchos países, la ciberseguridad no suele impartirse como una carrera de pregrado independiente, sino como una especialidad o concentración dentro de programas más amplios, tales como Ciencias de la Computación, Ingeniería Informática o Sistemas de Información.

En este contexto, la trayectoria habitual de un estudiante consiste en cursar una carrera base en alguna de estas disciplinas y, posteriormente, optar por una especialización a través de programas de posgrado, diplomas o certificaciones profesionales. Este modelo refleja tanto la naturaleza interdisciplinaria de la ciberseguridad como la percepción, todavía extendida, de que se trata de un campo complementario más que de una disciplina autónoma. En este panorama global, resulta pertinente examinar con mayor detalle la situación de la enseñanza en ciberseguridad en contextos internacionales específicos.

2.3.1. Internacionales

Para este trabajo se optó por considerar el caso de Estados Unidos, ya que, es en este país donde se originan la mayoría de los principales *frameworks* de referencia, entre ellos, los dos utilizados con mayor amplitud en este trabajo (NICE y CSEC2017), y cuyo desarrollo en materia de educación en ciberseguridad ha influido significativamente en las tendencias y estándares adoptados a nivel mundial. Si bien el problema abordado en esta investigación se enmarca principalmente en la realidad chilena, el análisis de otros escenarios permite obtener una perspectiva comparativa valiosa.

Estados Unidos

La situación en Estados Unidos no difiere significativamente de la del resto del mundo. Un estudio realizado por [Crabb *et al.*, 2024] analizó las carreras ofrecidas por cien instituciones con la designación CAE-C, *Centers of Academic Excellence in Cybersecurity*, a lo largo del país. Para su investigación, los autores recopilaron información desde las páginas web de cada institución, considerando, entre otros aspectos: el número y tipo de programas relacionados con ciberseguridad, la cantidad total de créditos requeridos, y si las descripciones de los programas mencionaban marcos de referencia como NICE, CSEC2017, CC2020 o la propia designación CAE-C, ya que estas varían según el nivel académico de los programas que ofrecen, pudiendo ser estas *Cyber Defense* (CAE-CD) para instituciones que ofrezcan programas *bachelor*, *Cyber Research* (CAE-CR) para las que provean doctorados, o *Cyber Operations* (CAE-CO) para programas interdisciplinarios [National Security Agency, sf].

Los resultados entregaron un registro detallado de los tipos de títulos ofrecidos por las instituciones consideradas, lo que permitió identificar los siguientes resultados:

- 50 instituciones ofrecían programas de *bachelor*
- 35 ofrecían certificados
- 32 ofrecían *associate degrees*
- 16 ofrecían *minors*
- 14 ofrecían *concentrations* o *tracks* dentro de programas de *bachelor* o *associate degree* no especializados en ciberseguridad.

Del análisis realizado se desprende que no existe consenso respecto al grado de autonomía que se le otorga a la disciplina de la ciberseguridad. En la mayoría de los casos, esta se concibe como un complemento a otras áreas de las ciencias de la computación, más que como una carrera independiente. Esta decisión institucional no debe interpretarse necesariamente como una deficiencia, sino como una estrategia formativa coherente con la naturaleza interdisciplinaria de la ciberseguridad. Resulta fundamental que el estudiante posea conocimientos generales en computación antes de abordar contenidos especializados; comprender cómo se construye el software y los sistemas que lo ejecutan constituye un requisito indispensable para una formación sólida en el área. Además, es importante señalar que muchos de los frameworks de referencia en ciberseguridad no incorporan en su estructura los conocimientos fundamentales de la computación, por lo que un estudiante que se guíe exclusivamente por ellos sin una base conceptual adecuada podría ver afectado negativamente su proceso de aprendizaje.

Un hallazgo particularmente relevante para esta investigación es el uso de frameworks de referencia, como NICE y CSEC2017, en la educación superior en ciberseguridad. Aunque las instituciones con la designación CAE-C cuentan con requisitos mínimos que las orientan a integrar dichos marcos en sus programas, la evidencia indica que su adopción sigue siendo limitada. Solo un 8 % de los programas analizados incluían referencias explícitas al NICE, mientras que un 20 % mencionaban trayectorias laborales vinculadas a sus lineamientos. En el caso del CSEC2017, únicamente un 2 % de los programas lo citaban, y el CC2020 no fue mencionado en ninguno.

El estudio sostiene que una estrategia eficaz para reducir la brecha de competencias identificada en el sector consiste precisamente en la incorporación sistemática de marcos de referencia como NICE y CSEC2017, complementados con los métodos propuestos en el CC2020 para describir y monitorear currículos. La adopción de estas herramientas permitiría comparar planes de estudio a partir de especificaciones comunes, lo que facilitaría tanto a los estudiantes como a los empleadores la identificación de programas formativos alineados con las demandas del mercado laboral. Asimismo, su uso por parte de instituciones de educación superior generaría un efecto de retroalimentación

positiva: aquellas que las implementen incentivarían a otras a seguir el mismo camino y, al mismo tiempo, contribuirían al perfeccionamiento y evolución de los propios marcos de referencia.

2.3.2. Chile

El panorama nacional de esta disciplina no difiere sustancialmente del contexto internacional, como se evidencia en el caso de Estados Unidos, aunque presenta particularidades derivadas de factores como la menor población, superficie y, en consecuencia, número de instituciones de educación superior. La especialización en ciberseguridad, al igual que en muchos otros países, suele estar asociada principalmente a programas de perfeccionamiento, tales como postítulos, diplomados y certificaciones profesionales, estas últimas otorgadas generalmente por entidades externas y con validez internacional.

Las carreras más comunes vinculadas a la ciberseguridad corresponden a aquellas centradas en las ciencias generales de la computación, como Ingeniería en Informática o Ingeniería en Computación, las cuales suelen incluir un número reducido de asignaturas específicas de ciberseguridad dentro de sus planes de estudio.

Por otra parte, los programas exclusivamente orientados a la ciberseguridad tienden a concentrarse en institutos profesionales más que universidades. Dichos programas destacan, además, por incorporar asignaturas orientadas al uso de tecnologías ampliamente empleadas en la industria y por ofrecer certificaciones reconocidas por proveedores líderes. Por ejemplo, la carrera profesional de Ingeniería en Ciberseguridad del Instituto Profesional AIEP incluye asignaturas que conducen a certificaciones en AWS y Cisco [AIEP, sf], lo cual representa un valor añadido significativo para los estudiantes, dado que este tipo de credenciales refuerzan su perfil profesional y mejoran su empleabilidad.

De manera preliminar, y sobre la base de una revisión general del panorama nacional, no se observa una alineación declarada con *frameworks* internacionales ampliamente reconocidos en el ámbito educativo o profesional de la ciberseguridad, como NICE o CSEC2017. Este punto será abordado con mayor precisión en el análisis específico desarrollado en capítulos posteriores.

En síntesis, la oferta nacional muestra que la formación especializada en ciberseguridad aún se encuentra en proceso de consolidación, con una oferta predominantemente concentrada en programas de posgrado, diplomados y certificaciones externas, mientras que los programas de pregrado presentan una cobertura más limitada y generalista. Este contexto plantea la necesidad de avanzar hacia propuestas curriculares más estructuradas y coherentes con las demandas del sector, lo que respalda la pertinencia de desarrollar una línea complementaria en ciberseguridad dentro del plan de estudios de Ingeniería Civil Informática de la UTFSM.

2.4. Creación de currículos basados en *frameworks*

En esta sección se describen los principios y elementos utilizados para la creación de currículos basados en *frameworks* internacionales de ciberseguridad. En particular, se detallan los componentes específicos que se extraen de cada marco de referencia para la formulación de las propuestas curriculares presentadas en este trabajo. La selección de dichos componentes se realiza procurando mantener coherencia en los niveles de granularidad y especificidad de los contenidos, de modo de facilitar su comparación, integración y posterior traducción a estructuras curriculares concretas.

2.4.1. Selección de componentes de los *frameworks* NICE y CSEC2017

Esta selección se fundamenta en la complementariedad de ambos marcos, donde NICE aporta una visión orientada a roles y funciones profesionales, mientras que CSEC2017 entrega una estructura académica basada en áreas y unidades de conocimiento.

En el caso del **NICE**, se emplean los conceptos de *Work Role*, *Work Role Category* y *Knowledge Description* (KD), así como los elementos *Task, Knowledge* y *Skills* (TKS).

Por otra parte, del **CSEC2017** se utilizan las nociones de *Knowledge Area* (KA), *Knowledge Unit* (KU), *Topics* y *Description / Guidance*. Con el fin de facilitar su uso y referencia a lo largo del documento, se desarrolló un sistema de codificación propio, dado que el CSEC2017 no incluye uno. La codificación funciona de la siguiente manera:

- **KA**: Se asigna un número del 1 al 8, siguiendo el orden en que aparecen en el documento original.
- **KU**: Se representa mediante el número de su KA correspondiente, seguido de un segundo número que indica su posición dentro de esa KA; ambos números separados por un punto.
- **Topic**: Añade un tercer número que indica su posición dentro de la KU respectiva.

De este modo, por ejemplo, se obtiene la siguiente jerarquía:

- 1 DATA SECURITY (KA)
- 1.1 Cryptography (KU)
- 1.1.1 Basic concepts (Topic)

Este sistema de codificación se emplea en el resto del documento y en los apéndices, aclarando que corresponde únicamente al contenido del CSEC2017. En contraste, el NICE ya dispone de una codificación propia para sus TKS, por lo que no fue necesario generar una adicional.

2.4.2. Metodología de Ramezanian et al. (2024) para diseño curricular

Una de las principales fuentes académicas en que se sustenta esta investigación es el trabajo de [Ramezanian y Niemi, 2024], cuyo objetivo fue facilitar la creación de currículos de ciberseguridad en educación superior a partir de los *frameworks* NICE y CSEC2017. En particular, dicho estudio emplea la versión 2017 del NICE, razón por la cual esta investigación también la adopta como referencia.

El artículo realiza diversas contribuciones relevantes, tanto en el plano metodológico como en los resultados obtenidos. A continuación, se destacan aquellas de mayor pertinencia para este trabajo.

En primer lugar, propone un método para calcular **pesos relativos** que permiten determinar la importancia de cada *Knowledge Area* (KA) en función de las necesidades de la fuerza laboral. Con el propósito de garantizar que la ponderación fuese representativa del mercado laboral, los autores se basaron en el estudio de [Lehto y Martti, 2022], el cual identifica los porcentajes de demanda de profesionales en ciberseguridad de Finlandia, distribuyendo esta en siete categorías de competencia:

- Categoría 1: Secure Production (SP) 19 %
- Categoría 2: Operation and Maintenance (OM) 14 %
- Categoría 3: Oversight and Governance (OG) 17 %
- Categoría 4: Protection and Defense (PR) 17 %
- Categoría 5: Analysis (AN) 13 %
- Categoría 6: Data collection & Operation (CO) 10 %
- Categoría 7: Investigation (IN) 10 %

Estas siete categorías corresponden directamente a las *Work Role Categories* del NICE 2017: 1) *Securely Provision* (SP), 2) *Operate and Maintain* (OM), 3) *Oversee and Govern* (OV), *Protect and Defend* (PR), 5) *Analyze* (AN), 6) *Collect and Operate* (CO), y 7) *Investigate* (IN). De esta forma, se establece un mapeo directo entre ambas clasificaciones, lo que permite aproximar la relevancia de cada *Work Role Category* dentro de la fuerza laboral.

Dado que las *Work Role Categories* son conjuntos que agrupan diversos *Work Roles*, el estudio propone calcular el peso relativo de cada *Work Role* X en su categoría mediante la siguiente fórmula:

$$\frac{\text{Porcentaje de la categoría } X}{\text{Número de work roles en la categoría } X} \tag{1}$$

Posteriormente, para obtener la contribución de cada *Knowledge Description* (KD) perteneciente al *Work Role* Y dentro de la categoría X, se utiliza la siguiente expresión:

$$\frac{\frac{\text{Porcentaje de la categoría } X}{\text{Número de work roles en la categoría } X}}{\text{Número de KDs en el work role } Y \text{ de la categoría } X} \tag{2}$$

Otro aporte significativo del trabajo fue establecer un mapeo entre los KDs del NICE y las KA y KU del CSEC2017. Este procedimiento se realizó mediante un análisis cualitativo detallado, en el cual se contrastaron las descripciones del CSEC2017 con los contenidos de los KDs, buscando la correspondencia más adecuada.

De esta manera, al aplicar las fórmulas de ponderación sobre los KDs y proyectar sus valores hacia las KA y KU mediante el mapeo, es posible calcular los pesos relativos de cada KA. A su vez, utilizando el mismo razonamiento en sentido inverso a la fórmula (2), se logra obtener también los pesos correspondientes a cada KU.

A manera de síntesis, los principales aportes del estudio se pueden resumir en el siguiente listado:

- Determinación del peso relativo de cada *Work Role Category* del marco NICE en la fuerza laboral.
- Cálculo del peso específico de cada *Work Role*.
- Obtención del peso de cada *Knowledge Descriptor* (KD).
- Establecimiento de un mapeo entre los KDs del NICE y las KAs y KUs del CSEC2017.
- Determinación del peso de cada KA.
- Determinación del peso de cada KU.

A partir de estas herramientas, el estudio realiza su contribución más significativa, que constituye además la base metodológica utilizada en este trabajo: el uso de estos valores asistiendo en el diseño y desarrollo de currículos académicos.

Para ejemplificar la aplicación práctica, los autores plantean el caso hipotético de un estudiante que, tras finalizar sus estudios de pregrado, desea continuar con un programa de *Master's degree* (equivalente a un Magíster en el contexto nacional). Considerando el total de créditos necesarios para completar dicho programa, se aplican los porcentajes obtenidos para cada KA, lo que permite derivar una distribución proporcional de créditos —y, en consecuencia, de asignaturas— que conformarían un currículo orientado a las necesidades reales de la fuerza laboral en ciberseguridad.

CAPÍTULO 3
PROPUESTA DE SOLUCIÓN

En este capítulo se describe la metodología empleada para el diseño de propuestas curriculares en ciberseguridad. Para ello, se utilizan como base *frameworks* previamente presentados, especificando los conceptos relevantes de cada uno y los criterios que orientan su aplicación. Asimismo, se consideran trabajos previos relacionados con la enseñanza de la ciberseguridad, los cuales sirven de referencia para fundamentar las metodologías propuestas.

3.1. Metodología del análisis

El objetivo principal de este proceso metodológico es establecer lineamientos que permitan articular currículos coherentes y progresivos en torno a la disciplina, adaptados a las características del programa de Ingeniería Civil Informática de la UTFSM.

En este marco, se desarrollan distintas propuestas de línea complementaria en ciberseguridad, diferenciadas por la cantidad de asignaturas y áreas que cubren:

- **Propuesta I-A:** 8 áreas en 8 asignaturas (similar a plan de estudios 7313) con pesos según oferta académica en Chile.
- **Propuesta I-B:** 8 áreas en 8 asignaturas (similar a plan de estudios 7313) con pesos según Leto et al.
- **Propuesta II:** 8 áreas en 4 asignaturas (enfoque similar a un *minor*).
- **Propuesta III:** 8 áreas en 5 asignaturas (solo asignaturas disciplinares en el plan de estudios 7310).
- **Propuesta IV:** Menos de 8 áreas en 5 asignaturas (solo asignaturas disciplinares en el plan de estudios 7310).
- **Propuesta V:** Menos de 8 áreas en 4 asignaturas (enfoque similar a un *minor*).
- **Propuesta VI**: 4 asignaturas *core* y 1 o 2 asignaturas de perfiles especializados.

3.1.1. Elección de *frameworks*

Como ya se ha visto anteriormente, emplear *frameworks* para la confección de planes curriculares es muy beneficioso, sobre todo para tener una primera idea de los contenidos posibles a considerar.

Para establecer una base sólida respecto a las áreas de la ciberseguridad a considerar en este estudio, se tomaron como referencia los *frameworks* NICE del NIST y CSEC2017 del JTF.

Cabe señalar que el NICE, desde su creación, ha tenido múltiples versiones. Para el desarrollo de este trabajo se consideraron en particular dos de ellas: la versión 2017 y la versión v1.0.0, publicada en 2024.

La elección del NICE y el CSEC2017 se basa en los resultados de [Hajny *et al.*, 2021] los cuales validan la decisión de utilizar ambos *frameworks* en la presente investigación, pues demuestran que, pese a provenir de enfoques distintos, sus contenidos presentan un alto nivel de similitud. Esto permite articular un currículo basado en componentes de ambas fuentes de manera sólida y coherente.

Actualmente existen diversas propuestas para guiar la educación en ciberseguridad, algunas con un enfoque más prescriptivo y otras de carácter más informativo. A continuación, se presentan las razones por las cuales ciertos *frameworks* no fueron adoptados en esta investigación:

- **ECSF:** Si bien es una propuesta sólida, resulta muy similar al NICE en su enfoque hacia el ámbito profesional, lo que haría redundante su inclusión. Además, se encuentra altamente condicionado por las normativas y necesidades específicas de la Unión Europea.
- **CyBOK:** A pesar de su amplitud y valor como referencia académica, no resulta práctico desde la perspectiva educativa, ya que no está diseñado para ser implementado como guía curricular. Se trata de un cuerpo de conocimiento y no de un *framework*, por lo que sería necesario un trabajo adicional considerable para suplir los aspectos pedagógicos que carece.
- **CC2020:** Su propósito es servir como un *metaframework* para la educación en ciencias de la computación en general. Aunque es una fuente valiosa, su enfoque es demasiado amplio y transversal. Para los fines de este trabajo se requieren contenidos específicos y concretos sobre ciberseguridad, los cuales no provee con el nivel de detalle necesario.

3.1.2. Procedimiento para la estimación de pesos en Chile

En el trabajo de [Ramezanian y Niemi, 2024], anteriormente descrito, se propone como línea de continuidad la aplicación del procedimiento de diseño curricular en distintas instituciones y contextos geográficos, señalando que basta con contar con los porcentajes iniciales de la fuerza laboral para poder replicar el método.

En el caso de la presente investigación, no se dispone, al menos hasta dónde llega el conocimiento del autor, de un reporte equivalente al de [Lehto y Martti, 2022] en el contexto chileno. Esta carencia representa una primera barrera, ya que impide emplear directamente la metodología sugerida por Ramezanian y colaboradores. En consecuencia, fue necesario desarrollar un procedimiento propio que permitiera aproximar la representación de las KAs en la educación en ciberseguridad en Chile.

Con el objetivo de obtener porcentajes relevantes al contexto local, se realizó el siguiente proceso: se consideró un total de ocho instituciones de educación superior que ofrecieran algún tipo de programa relacionado con la ciberseguridad, ya fuera de pregrado o de postgrado (como magísteres o diplomados). Inicialmente se contempló la posibilidad de incluir programas de áreas afines, tales como Ingeniería en Informática o en Computación; sin embargo, al analizar sus planes de estudio se concluyó que el contenido resultaba excesivamente general en temas de computación. Este resultado, aunque esperable, no se ajusta al objetivo de este trabajo, que es desarrollar una línea de formación complementaria en ciberseguridad, y no la elaboración de un nuevo plan curricular para carreras de informática.

Las carreras analizadas se presentan en la Tabla 1.

Institución	**Tipo de institución**	**Carrera/Programa**	**Nivel (Pre/Postgrado)**
AIEP	Instituto Profesional	Ingeniería en Ciberseguridad	Pregrado
IACC	Instituto Profesional	Ingeniería en Ciberseguridad	Pregrado
INACAP	Instituto Profesional	Ingeniería en Ciberseguridad	Pregrado
Universidad Mayor	Universidad	Ingeniería en Ciberseguridad	Pregrado
PUC	Universidad	Diplomado en Gestión Técnica de Ciberseguridad	Postgrado
PUCV	Universidad	Diplomado en Ciberseguridad	Postgrado
UAI	Universidad	Magíster en Ciberseguridad	Postgrado
USM	Universidad	Diploma en Ciberseguridad	Postgrado

Tabla 1: Programas de Ciberseguridad en Instituciones Chilenas
Fuente: Elaboración propia

Una vez delimitado el conjunto de programas a analizar, se procedió a recopilar la información disponible en los sitios webs oficiales de cada institución. En particular, se extrajeron las mallas curriculares y el listado de asignaturas asociados, los cuales fueron posteriormente organizados y tabulados con el fin de facilitar su análisis.

3.1.3. Análisis de programas en Chile

Reunidos los elementos, el marco CSEC2017 con la codificación propuesta y el conjunto de asignaturas recopiladas, se se efectuó un análisis cualitativo extensivo de cada ítem de las mallas curriculares. El objetivo fue asignar a cada curso uno o más KUs pertinentes, considerando no solo el título del curso, sino también las descripciones y objetivos de aprendizaje disponibles en los programas respectivos.

En una primera etapa se consideró realizar la clasificación de los contenidos de las asignaturas a un nivel más granular, utilizando los *Topics* definidos en el CSEC2017. Sin embargo, este enfoque presentó una consecuencia negativa: en varios casos, las descripciones de las asignaturas eran demasiado amplias, lo que producía una sobre representación de las KUs. Esto ocurría porque, al detallar un curso, resultaba necesario asignarle múltiples *Topics*, aun cuando estos se encontraban estrechamente relacionados y podían ser representados de manera conjunta.

Con el fin de evitar dicha sobre representación, se optó finalmente por emplear la categoría superior, las KU, dado que estas engloban de forma más adecuada los contenidos relacionados y permiten una representación más equilibrada y consistente de los programas analizados.

El resultado del procedimiento aplicado en la presente investigación se encuentra sistematizado en las tablas incluidas en el Anexo A. Cada tabla muestra la estructura que presentada en las páginas web de los programas. Seccionando los programas por módulos, semestres, ciclos. Existen algunas excepciones en las que un módulo podía no contener ítems específicos a este, pero sí contenía una descripción de los aprendizajes del módulo.

Además de la asignación de KUs se empleó tres identificadores extra para casos excepcionales, donde no correspondía asignar KUs.

- X: Ítems que entregan poca información. La mayoría siendo certificados o electivos sin aclarar qué tipo de contenidos podían contemplar, o nexos pedagógicos, como fue el caso del curso denominado “Putting It All Together” en el programa de Diplomado en Gestión Técnica de Ciberseguridad de la Pontificia Universidad Católica de Chile.
- 0: Ítems que estuvieran relacionados con la KA-0. [Ramezanian y Niemi, 2024] emplea un área adicional a las 8 normales del CSEC2017, la KA-0. Esta nueva área contempla temas básicos de computación, matemáticas y redes, así como otros temas ajenos a la disciplina, como leyes, negocios, economía y pedagogía.

  Estos se dan principalmente en las carreras de pregrado, donde se dan casos como el INACAP donde en los primeros semestres tienen las asignaturas “Introducción a la programación” y “Programación orientada al objeto seguro”, pero luego el plan

de estudios conitene también la asignatura “Desarrollo seguro”, donde se puede intuir este sí presenta contenido específico de seguridad. Además de asignaturas no relacionadas con la ciberseguridad como “Inglés inicial I”, “Taller de Marca Personal“ o “Habilidades para la Comunicación”.

- -1: Contenidos que no se encuentra directa ni indirectamente en el CSEC2017. Son conceptos relacionados con ciberseguridad, pero no son parte del *framework*. Se presenta principalmente en las carreras de posgrado. Donde existe contenido muy específico que es difícil de relacionar con el CSEC2017. Por ejemplo, OSINT, que es la recopilación de información libre de internet, lo cual si está relacionado con la ciberseguridad pero no se menciona como tal en el CSEC2017 ni como parte de algún otro contenido.

En el desarrollo de este trabajo se identificó un procedimiento semejante, aunque con fines distintos, en el estudio de [Crabb *et al.*, 2024]. Dicho trabajo realizó un análisis de programas académicos en instituciones de educación superior en Estados Unidos. Sin embargo, el objetivo allí no fue examinar el contenido de las asignaturas ni su relación con los *frameworks* de ciberseguridad, sino más bien verificar si los programas declaraban explícitamente la adopción de algún *framework* reconocido.

A partir de este análisis, haciendo un recuento las KUs, se obtuvo la representación de las KAs correspondientes a cada programa académico, lo que permitió formarse una primera impresión del estado actual de la educación en ciberseguridad en Chile. Con el fin de disponer de una visión más global de la situación, los datos individuales fueron consolidados para calcular la frecuencia total de aparición de cada KA, lo cual se presenta en la Tabla 2.

KA	PUC	PUCV	UAI	USM	IACC	INACAP	UMAYOR	TOTAL KA	PORCENTAJES
DATA SECURITY	44	37	12	40	9	33	18	193	18,4 %
SOFTWARE SECURITY	47	15	27	37	5	62	5	198	18,9 %
COMPONENT SECURITY	7	3	0	1	3	7	1	22	2,1 %
CONNECTION SECURITY	74	16	4	38	20	46	22	220	21,0 %
SYSTEM SECURITY	72	18	5	19	13	33	18	178	17,0 %
HUMAN SECURITY	10	0	0	8	1	0	2	21	2,0 %
ORGANIZATIONAL SECURITY	52	16	10	19	11	30	10	148	14,1 %
SOCIETAL SECURITY	20	6	1	13	10	11	9	70	6,7 %
Total	326	111	59	175	72	222	85	1.050	100 %

Tabla 2: Distribución de KAs en programas de Ciberseguridad en Chile
Fuente: Elaboración propia

De esta manera, se obtienen los porcentajes que representan de forma más fiel la situación de la educación en ciberseguridad a nivel local. A partir de estos resultados, se procede a presentar la primera propuesta de currículo.

3.2. Propuestas

Dado que el problema identificado corresponde específicamente a la ausencia de una línea de formación en ciberseguridad dentro de la carrera de Ingeniería Civil Informática en la UTFSM, se decidió estructurar la propuesta considerando los parámetros institucionales ya existentes. En este sentido, se tomaron como referencia los dos planes de estudios vigentes a septiembre de 2025: el plan de estudio 7313, correspondiente al plan antiguo, y el plan de estudio 7310, correspondiente al plan nuevo.

La solución planteada busca complementar los contenidos fundamentales de ciencias de la computación que ya se imparten en ambos planes. Por ello, se optó por utilizar como base las asignaturas de carácter electivo. En adelante, se hará referencia a las asignaturas obligatorias como asignaturas "generales" o como la parte "general" del plan. Estas asignaturas constituyen un componente esencial para la propuesta, en la medida en que entregan los conocimientos básicos sobre los cuales se profundizará y extenderá la formación en ciberseguridad.

Es posible que algunos de los contenidos tratados en las asignaturas generales coincidan con los de la línea complementaria propuesta. Sin embargo, esta superposición no se considera una desventaja; por el contrario, se valora como una oportunidad pedagógica. La reiteración de conceptos, abordados desde nuevas perspectivas y en contextos aplicados, permite reforzar el aprendizaje y evidenciar cómo dichos fundamentos se relacionan con problemáticas concretas de la disciplina, como es el caso de la ciberseguridad.

Al analizar ambos planes, se observa que en el plan 7313 (plan antiguo) existen cuatro asignaturas electivas de informática (INF305, INF306, INF307, INF309) y cuatro asignaturas electivas generales (INF311, INF312, INF313, INF314), cada una con un valor de 5 créditos SCT. Por su parte, en el plan 7310 (plan nuevo) se identifican dos asignaturas electivas generales (AUX219 y AUX222), cada uno con 5 créditos SCT, y cinco asignaturas electivas disciplinares (INF169, INF170, INF171, INF540, INF541), cada uno con 6 créditos SCT.

Ambos planes curriculares permiten disponer de un total de 40 créditos SCT, lo cual constituye un elemento clave para el diseño de la propuesta. Esta cantidad de créditos es emplea como valor de referencia, a manera de tener un total representativo de las asignaturas. Este puede ser fraccionado según los pesos obtenidos en el análisis de la oferta académica en Chile. Además, nos facilita poder determinar si se requiere una, más o menos asignaturas por área.

3.2.1. Propuestas basadas en pesos

PROPUESTAS I-A y I-B La primera propuesta basada en pesos se construye a partir de los valores obtenidos en el análisis de los programas de ciberseguridad en Chile. Para su elaboración, se asume que cada curso equivale a 5 créditos SCT, disponiendo así de un total de 40 SCT para la conformación completa de la línea complementaria en ciberseguridad.

Con el fin de determinar la cantidad de créditos que corresponde a cada KA, se aplica la siguiente fórmula:

$$\lfloor \text{Porcentaje de KA} \cdot 40 \rfloor \tag{1}$$

Posteriormente, para calcular el número de asignaturas completas que corresponde impartir según los créditos obtenidos, se divide la cantidad de créditos por 5. La parte entera del resultado indica el número de asignaturas completas, mientras que la parte decimal representa la fracción de una asignatura adicional a impartir.

Los datos obtenidos se presentan en la Tabla 3. En esta se observa que algunas KAs deben impartirse de manera individual, requiriendo la extensión de una asignatura completa, e incluso, en ciertos casos, más de una. De forma complementaria, se identifican áreas cuya extensión no justifica por sí sola la creación de una asignatura completa.

KA	**PORCENTAJES**	**Aprox. créditos**	**Proporcion de asignatura**
DATA SECURITY	18,38 %	7	1,4
SOFTWARE SECURITY	18,86 %	8	1,6
COMPONENT SECURITY	2,10 %	1	0,2
CONNECTION SECURITY	20,95 %	8	1,6
SYSTEM SECURITY	16,95 %	7	1,4
HUMAN SECURITY	2,00 %	1	0,2
ORGANIZATIONAL SECURITY	14,10 %	6	1,2
SOCIETAL SECURITY	6,67 %	3	0,6
Total	100,01 %	41	8,2

Tabla 3: Distribución de créditos y asignaturas según pesos en Chile
Fuente: Elaboración propia

Considerando dicha situación, se adopta la siguiente decisión de diseño curricular: se establecen asignaturas dedicadas exclusivamente a aquellas KA que ameritan una asignatura completa. Por su parte, las áreas que representan una fracción menor, así como aquellas que exceden una asignatura completa (parte entera igual a 1 y parte decimal mayor a 0), se integran en asignaturas conjuntas que abordan múltiples KA de manera simultánea.

Por ejemplo, en el caso de las áreas *DATA SECURITY* y *SOFTWARE SOFTWARE*, cuyos valores corresponden a 1,4 y 1,6, respectivamente, se proponen las asignaturas **Seguridad de Datos** y **Seguridad del Software**. Los contenidos restantes se complementan en una asignatura conjunta denominada **Seguridad de Datos orientado al Software**.

De esta manera, se configuran las ocho asignaturas que conforman la propuesta, combinando asignaturas dedicadas a un único ámbito con otras de carácter integrador. La selección de las áreas que se imparten de manera conjunta se fundamenta en su relación temática, de forma que el contexto compartido actúe como un nexo pedagógico que favorezca la comprensión integral de los contenidos.

Esta distribución permite un enfoque integrador, en el que las áreas se presentan de manera simultánea. Por ejemplo, los contenidos de *DATA SECURITY*, como algoritmos criptográficos y sus características, pueden enseñarse en paralelo con aspectos de *SOFTWARE SECURITY*, como el almacenamiento seguro de contraseñas. Esto permite enfatizar las buenas prácticas y analizar cuáles algoritmos resultan más adecuados en contextos de desarrollo de software.

La elección de nombres de los asignaturas formadas se realizó de manera que fuesen descriptivos de las áreas que contienen, especialmente de aquellos que integran más de una.

A partir de este criterio de diseño, se procedió a estructurar la siguiente propuesta de asignaturas presentada en la Tabla 4:

Asignatura	**Fracciones**	**Créditos SCT**
Seguridad de Datos	1	5
Seguridad del Software	1	5
Seguridad en Redes	1	5
Seguridad de Sistemas	1	5
Seguridad Organizacional	1	5
Seguridad Humana, Social y Organizacional	0,2 + 0,2 + 0,6	5
Seguridad de Datos orientado al Software	0,4 + 0,6	5
Seguridad de Componentes, Redes y Sistemas	0,2 + 0,4 + 0,6	6
Total	8,2	41

Tabla 4: Propuesta I-A: Distribución de asignaturas y créditos
Fuente: Elaboración propia

Se observa que el total de créditos SCT es 41, superando levemente los 40 inicialmente considerados. Esta diferencia se produce debido al redondeo de los valores obtenidos a partir de los porcentajes, lo que genera un exceso de un crédito. En la práctica, esta variación resulta irrelevante, ya que la diferencia de un crédito no es significativa. Si

bien sería posible ajustar la suma para mantener estrictamente los 40 créditos, se optó por conservar los 41 con el fin de respetar de manera fiel los cálculos realizados.

Con las asignaturas propuestas, se denomina a esta primera propuesta como **PROPUESTA I-A**. La subdenominación "A" se justifica porque es posible generar una propuesta adicional empleando el mismo procedimiento, pero utilizando valores distintos para los porcentajes de las KAs.

Para la segunda propuesta, se emplearon los porcentajes obtenidos en [Ramezanian y Niemi, 2024] para las distintas KAs. La razón de generar esta propuesta adicional es que dichos porcentajes resultan más representativos de las necesidades de la fuerza laboral, mientras que los porcentajes utilizados en la primera propuesta reflejan la situación de la educación en ciberseguridad en Chile. De esta manera, se presentan dos perspectivas diferentes de forma sencilla.

Es importante mencionar que no se pueden aplicar los valores de manera directa, ya que [Ramezanian y Niemi, 2024] incluye el área adicional KA-0, la que, como mencionamos anteriormente, aglomera contenido distinto a las ocho KAs presentadas en CSEC2017.

Dado que el enfoque del presente trabajo se centra exclusivamente en las áreas específicas de ciberseguridad, es necesario recomputar los porcentajes de las KAs. Para ello, se procede de la siguiente manera: se descarta el porcentaje correspondiente al aporte correspondiente a la KA-0.

El total resultante se toma como el nuevo 100 %, y a partir de este se recalculan los porcentajes relativos de cada KA.

A continuación, se aplica el mismo procedimiento descrito en la **PROPUESTA I-A**, consistente en convertir los porcentajes en créditos y, posteriormente, sus proporciones de asignaturas completas.

Los nuevos porcentajes, junto con los otros datos correspondientes, se presentan en la Tabla 5.

KA	**Porcentaje incluyendo KA-0)**	**Nuevo porcentaje**	**Aprox. créditos**	**Proporción de curso**
DATA SECURITY	7,80 %	9,97 %	4	0,8
SOFTWARE SECURITY	5,40 %	6,91 %	3	0,6
COMPONENT SECURITY	3,30 %	4,22 %	2	0,4
CONNECTION SECURITY	20,30 %	25,96 %	10	2
SYSTEM SECURITY	9,60 %	12,28 %	5	1
HUMAN SECURITY	1,00 %	1,28 %	1	0,2
ORGANIZATIONAL SECURITY	24,20 %	30,95 %	12	2,4
SOCIETAL SECURITY	6,60 %	8,44 %	3	0,6
Total	78,20 %	100,00 %	40	8

Tabla 5: Distribución de créditos y asignaturas según valores de fuerza laboral
Fuente: Elaboración propia

A partir de los porcentajes recalculados, se construye la segunda propuesta de currículo, denominada **PROPUESTA I-B**. Esta propuesta se presenta en la Tabla 6, mostrando la asignación de créditos y la distribución de asignaturas correspondiente a cada área de ciberseguridad.

Asignatura	**Fracciones**	**Créditos SCT**
Seguridad en Redes I	1	5
Seguridad en Redes II	1	5
Seguridad de Sistemas	1	5
Seguridad Organizacional I	1	5
Seguridad Organizacional II	1	5
Seguridad Humana, Social y Organizacional	0,2 + 0,4 + 0,6	6
Seguridad de Software orientado al Componente	0,4 + 0,6	5
Seguridad de Datos	0,8	4
Total	8	40

Tabla 6: Propuesta I-B: Distribución de asignaturas y créditos
Fuente: Elaboración propia

Con estas dos propuestas se observa cómo se puede emplear el método de pesos como una de las estrategias para determinar las asignaturas que conformarán la línea de ciberseguridad. Esta opción tiene la particularidad de proporciona un menor nivel de detalle en cuanto al contenido específico a impartir, ofreciendo libertad al instructor para seleccionar los temas más relevantes extraídos del CSEC2017. Estas dos primeras propuestas pueden considerarse como un punto inicial para el desarrollo posterior en detalle del currículo.

3.2.2. Propuestas basadas en importancia

En la propuesta anterior se seleccionaron las áreas a un nivel general; sin embargo, en la práctica, el tiempo disponible para la enseñanza puede ser limitado, lo que obliga a priorizar los contenidos. En este sentido, uno de los criterios posibles consiste en identificar con claridad el público objetivo, es decir, determinar qué tipo de estudiante optaría por especializarse en ciberseguridad.

Adicionalmente, el instructor puede recurrir a su conocimiento experto del área y a la comprensión de cómo se interrelacionan los distintos conceptos, con el fin de evitar reiterar una idea que tenga matices distintos según su implementación y en su lugar identificar la idea transversal, que luego puede ser enseñada de manera tal que los estudiantes, por su propia cuenta, logren aplicar lo aprendido a situaciones diversas, aunque no idénticas a las vistas en el aula.

Bajo este enfoque, la **PROPUESTA II** contempla la integración de las 8 áreas en 4 asignaturas. Para lograr abarcar todas las áreas en una cantidad reducida de asignaturas, se emplean distintos criterios tanto para la selección de los temas como para la distribución de los contenidos. A continuación, se detallan los métodos empleados en dicha organización.

Modelo de estudiante

Para las siguientes propuestas se define un "Modelo de Estudiante", el cual describe las características deseables de un alumno que opta por especializarse en ciberseguridad. Este modelo se utiliza con el fin de acotar el dominio del conocimiento que se busca impartir y adaptarlo al contexto particular de un estudiante de la UTFSM.

A continuación, se detallan las características del modelo:

- Estudiante de Informática de la UTFSM, con grado de licenciado, que está próximo a inscribir sus primeras asignaturas electivas.
- Su interés se orienta principalmente hacia la seguridad en software, más que en hardware, debido al énfasis de la carrera en temas relacionados con el desarrollo y las aplicaciones de software.
- Posee conocimientos previos en matemáticas, teoría computacional, fundamentos de redes, arquitectura de computadores y nociones básicas de desarrollo de software; es decir, los aprendizajes esperados de las asignaturas previos a la elección de electivos.
- Presenta una preferencia por contenidos técnicos y científicos, relegando a un segundo plano aspectos como legislación, ética u otras áreas humanísticas relacionadas con la disciplina.
- No ha decidido si desea especializarse en defensa o ataque, por lo que busca adquirir una visión amplia y equilibrada que le permita tomar esta decisión posteriormente.
- Requiere adquirir conocimientos prácticos y técnicos en seguridad de sistemas, incluyendo redes, software y protección de datos, dado que ingresará a la empresa en un rol de nivel inicial (*junior*).
- Para poder escalar profesionalmente dentro de la organización, necesitará competencias en aspectos gerenciales de la seguridad interna, tales como la gestión segura de personal, definición de políticas de seguridad y administración de riesgos dentro de la propia empresa.
- Algunas funciones gerenciales más amplias, como la gestión de la seguridad de la cadena de suministro o de componentes de software de terceros, se consideran

responsabilidad de áreas especializadas o de terceros, y por lo tanto se encuentran fuera del alcance del estudiante en esta línea de especialización.

- No tiene claridad sobre el rol específico que desempeñará, y reconoce que podría asumir múltiples funciones en paralelo. En una empresa mediana o pequeña, podría encargarse simultáneamente de tareas como desarrollo y pruebas de software, frontend y diseño, backend y administración de bases de datos, o incluso redes y DevOps.

Un ejemplo de omisión, basado en este modelo de estudiante, se observa en los contenidos relacionados con seguridad de hardware. En particular, dentro del KA *COMPONENT SECURITY*, los KU 3.1.5 *Side-channel attack mitigation*, 3.1.6 *Anti-tamper technologies* y 3.4.2 *Hardware reverse engineering* no se incluyen en las propuestas finales. Esto se debe a que dichos tópicos están directamente relacionados con hardware, mientras que el modelo de estudiante establece un enfoque prioritario en la seguridad de software, por lo que se considera más pertinente omitirlos en la planificación curricular.

Criterio de ideas transversales

En el ámbito de la computación existen numerosas ideas que son independientes de la tecnología, el lenguaje de programación o el tipo de sistema. Por esta razón, otro criterio utilizado para la selección de contenidos fue omitir tópicos que presentaran ideas transversales, conservando únicamente uno representativo. Por ejemplo, conceptos como la encriptación, aplicables tanto a software como a hardware, se incluyen solo desde la perspectiva del software. De igual manera, conceptos generales de diseño de sistemas se ejemplifican mediante sistemas de software, con el objetivo de minimizar la redundancia presente en el CSEC2017, donde en ocasiones se expresa la misma idea para distintas implementaciones. En la elección de tópicos se da siempre preferencia al contexto de software.

Criterio de similitud

Dada la reducida cantidad de asignaturas en esta propuesta, se consideró la posibilidad de impartir áreas afines dentro de una misma asignatura. Esta estrategia, junto con la selección de los tópicos más relevantes, permite formar unidades temáticas dentro de un ramo, donde se agrupan conceptos similares y se explican desde diferentes perspectivas. Por ejemplo, en un mismo ítem se pueden agrupar los tópicos 5.3.1 *Authentication methods* y 1.4.1 *Physical data security*, relacionándolos en un contexto común, como la seguridad de un *data center*, y explicando los métodos de autenticación tanto lógicos como físicos. De esta manera, ambos tópicos se cubren de manera complementaria, pudiendo uno ser tratado parcialmente, mientras que se refuerza con el otro afín.

Siguiendo estos criterios de selección y considerando el modelo de estudiante previamente definido, se procedió a un análisis minucioso y exhaustivo del CSEC2017. Este análisis implicó la revisión detallada de los KUs, los *Topics* y sus descripciones, con el

objetivo de formar cuatro asignaturas según la **PROPUESTA II**, cada uno siguiendo una línea conceptual lógica y abarcando en conjunto las ocho KAs.

Las asignaturas obtenidas y las KAs que contienen se presentan a continuación:

Asignatura	**Áreas (KA)**
Introducción a la Ciberseguridad	HUMAN SECURITY SOCIETAL SECURITY
Seguridad de Software	COMPONENT SECURITY SOFTWARE SECURITY
Administración de Sistemas	SYSTEM SECURITY ORGANIZATIONAL SECURITY
Seguridad de Datos y Redes	DATA SECURITY CONNECTION SECURITY

Tabla 7: Propuesta II: 8 áreas distribuidos en 4 asignaturas
Fuente: Elaboración propia

PROPUESTA II
A diferencia de las propuestas anteriores, en las cuales las asignaturas se definían a un nivel general según sus KAs, en esta, dada la reducida cantidad de asignaturas, se utiliza la unidad de contenido más pequeña que considera el CSEC2017, es decir, el nivel de *Topics*. Esto permite realizar una selección más precisa de los contenidos de cada curso.

Se presenta un resumen de los contenidos por curso:

- **Introducción a la Ciberseguridad**: Incluye temas de carácter no técnico, como ciber-higiene, privacidad, leyes y el impacto de los ciberataques.
- **Seguridad de Software**: Abarca el desarrollo de software seguro, los fundamentos de seguridad en el software, la gestión de un ciclo de vida seguro, así como aspectos de *reverse engineering*.
- **Administración de Sistemas**: Contempla la puesta en marcha, operación y mantención de distintos tipos de sistemas computacionales, además de caracterizar la organización como un ejemplo de sistema y sus desafíos particulares, como lo son la formulación de políticas de seguridad y la gestión segura del personal.
- **Seguridad de Datos y Redes**: Abarca los aspectos necesarios para desplegar, gestionar y proteger sistemas de redes, así como los fundamentos criptográficos aplicables a las transacciones de red y al almacenamiento seguro de datos.

El contenido completo de las asignaturas se presenta en los Anexo C.

Este método de selección de un subconjunto de temas permite adaptarse a situaciones donde el número de asignaturas disponibles es limitado. En caso de necesidad, se podría focalizar aún más la línea de especialización, cubriendo únicamente 5 o incluso 4 KAs, reduciendo así la cantidad de asignaturas requeridas.

De esta manera, mediante la selección de temas y la realización de los ajustes necesarios, es posible generar propuestas adicionales siguiendo la misma metodología presentada. Se presentan tres propuestas más donde se varían la cantidad de áreas y asignaturas.

- PROPUESTA III: 8 áreas en 5 asignaturas
- PROPUESTA IV: Menos de 8 áreas en 5 asignaturas
- PROPUESTA V: Menos de 8 áreas en 4 asignaturas

PROPUESTA III

Esta propuesta constituye una extensión de la propuesta previamente planteada, la cual consideraba cuatro asignaturas. La ampliación a cinco asignaturas se logra de manera relativamente sencilla mediante la división de uno de los asignaturas existentes. Por ejemplo, el curso **Seguridad de Datos y Redes** de la PROPUESTA II puede desglosarse en dos asignaturas independientes: **Seguridad de Datos** y **Seguridad de Redes**.

Esta división permite no solo distribuir los contenidos de manera más equilibrada, sino también incorporar aquellos tópicos que fueron omitidos durante el proceso de selección inicial, asegurando así una cobertura más completa de los KAs correspondientes.

Asignatura	**Áreas (KA)**
Introducción a la Ciberseguridad	HUMAN SECURITY SOCIETAL SECURITY
Seguridad de Software	COMPONENT SECURITY SOFTWARE SECURITY
Administración de Sistemas	SYSTEM SECURITY ORGANIZATIONAL SECURITY
Seguridad de Datos	DATA SECURITY
Seguridad de Redes	CONNECTION SECURITY

Tabla 8: Propuesta III: 8 áreas distribuidas en 5 asignaturas
Fuente: Elaboración propia

PROPUESTA IV

Para la formulación de esta propuesta, se consideraron las áreas más importantes, es decir, aquellas que se alínean con los contenidos centrales que se pretenden impartir, siguiendo el *Modelo de Estudiante*. Se priorizó excluir aquellas áreas que, por su naturaleza, aportan relativamente poco al perfil formativo buscado o cuyo contenido consiste principalmente en ideas transversales que podrían abordarse en otras áreas.

Asignatura	**Áreas (KA)**
Seguridad de Software	SOFTWARE SECURITY
Seguridad de Datos	DATA SECURITY
Seguridad de Redes	CONNECTION SECURITY
Seguridad de la Organización	ORGANIZATIONAL SECURITY
Seguridad Humana	HUMAN SECURITY

Tabla 9: Propuesta IV: Menos de 8 áreas distribuidas en 5 asignaturas
Fuente: Elaboración propia

En este contexto, se identificaron las siguientes KAs como prescindibles: *COMPONENT SECURITY*, *SYSTEM SECURITY* y *SOCIETAL SECURITY*. A continuación, se analiza cada una de ellas de manera detallada.

- *COMPONENT SECURITY*: Aplicando el *Modelo de Estudiante*, se pueden descartar todos los tópicos relacionados con hardware, así como aquellos vinculados a roles de nivel superior, como la gestión de proveedores y la seguridad de la cadena de suministro. Esta área también incluye conceptos de *testing*, que son transversales y podrían abordarse en el módulo de desarrollo de software seguro. Los únicos temas que no son transversales y podrían considerarse relevantes para el perfil del estudiante son aquellos relacionados con *reverse engineering*, dado que resultan pertinentes para quienes desarrollan software. No obstante, dado que se busca reducir al mínimo las áreas, estos contenidos también se omiten en esta propuesta por ser conocimientos que consideramos muy especializados y menos probables que el estudiante requiera en primera instancia.
- *SOCIETAL SECURITY*: Los contenidos de esta área son, sin duda, importantes, ya que cualquier actividad profesional debe regirse por normas legales y principios éticos. Sin embargo, para fines de esta propuesta, se opta por centrarse únicamente en los temas de carácter técnico, delegando los aspectos legales o de ética a profesionales especializados, como abogados en ciberseguridad. Además, esta área incluye temas de ciberseguridad internacional, los cuales no corresponden al perfil de un estudiante que optara a un trabajo *entry-level*.
- *SYSTEM SECURITY*: Esta área abarca principalmente conceptos generales aplicables a cualquier tipo de sistema, muchos de los cuales ya se encuentran cubiertos en los módulos de software, redes y organización. Por ejemplo, temas

de ataque y defensa se abordan dentro de los tópicos de redes, las políticas de seguridad se incluyen en el área organizacional, y otros conceptos como *testing* o arquitecturas ya se tratan en módulos previos. Por ello, su inclusión en esta propuesta se considera redundante y se omite.

PROPUESTA V

Esta propuesta constituye una reducción respecto de la PROPUESTA IV, considerando únicamente las áreas que se mantienen tras la eliminación de ciertas unidades. En este caso, el área seleccionada para suprimir es *HUMAN SECURITY*.

La decisión de excluir dicha área no se toma a la ligera, dado que los conocimientos que aporta son fundamentales: incluso si se dispone de software seguro, sistemas robustos y redes resilientes, un error humano, como la entrega inadvertida de credenciales a agentes maliciosos, puede comprometer toda la seguridad implementada. Por ello, un especialista en ciberseguridad requiere un mínimo de ciber-higiene personal, habilidades para instruir a usuarios con menos conocimientos técnicos y criterios de diseño de software que consideren la falta de preparación del usuario final.

Sin embargo, dada la necesidad de reducir al máximo la cantidad de áreas, se decidió descartar *HUMAN SECURITY*. Esta exclusión se justifica considerando que existen roles específicos donde la interacción con el factor humano es mínima, como desarrolladores de *kernel* o *drivers*, o administradores de servidores y *data centers*, en los cuales los conocimientos de ciber-higiene y educación del usuario no resultan críticos. En contraste, roles orientados al desarrollo de software con interacción directa con usuarios, como frontend o aplicaciones de uso general, sí requerirían mantener estos conocimientos.

Asignatura	**Áreas (KA)**
Seguridad de Software	SOFTWARE SECURITY
Seguridad de Datos	DATA SECURITY
Seguridad de Redes	CONNECTION SECURITY
Seguridad de la Organización	ORGANIZATIONAL SECURITY

Tabla 10: Propuesta V: Menos de 8 áreas distribuidas en 4 asignaturas
Fuente: Elaboración propia

Si bien en estas últimas dos propuestas se plantea una reducción significativa en la cantidad de áreas, se recomienda a los instructores priorizar la reducción de contenidos dentro de cada área, en lugar de eliminar áreas completas. Áreas como *HUMAN SECURITY* y *SOCIETAL SECURITY* resultan fundamentales para la formación de especialistas en ciberseguridad. La instrucción debe asegurar que los profesionales consideren el factor humano y el impacto ético de sus decisiones en el desarrollo de software y la gestión de sistemas, promoviendo la responsabilidad y la protección de la privacidad de los usuarios.

3.2.3. Propuesta basada en perfiles

La creación de currículos académicos es una tarea compleja, dado que pueden existir múltiples perspectivas, contenidos y formas de organización para estructurarlos. Una de las metodologías consideradas en este trabajo consiste en diseñar el currículo a partir de perfiles de especialización, de modo que el estudiante adquiera un conocimiento más específico según el tipo de labor al que aspire en su futuro profesional.

Para formular la propuesta denominada **PROPUESTA VI**, se requiere una guía fundamentada en el mercado laboral y en las funciones reales que desempeñan los especialistas en ciberseguridad. Con este propósito, es necesario primero contextualizar las fuentes de información utilizadas.

La base de datos *O*NET* [National Center for O*NET Development, sf], desarrollada por el *U.S. Department of Labor*, describe diversas profesiones en términos de los conocimientos, habilidades, tareas y actividades que estas requieren, además de aportar información complementaria como tendencias de empleo y niveles de remuneración. La fuente principal empleada en este desarrollo es el *ETO-CSET NICE-O*NET Crosswalk* [CSET/ETO, 2024], en adelante *Crosswalk*, creado por el *Emerging Technology Observatory* (ETO). Esta base de datos establece un mapeo entre las ocupaciones descritas por *O*NET*, relacionadas con la ciberseguridad, y los *Work Roles* definidos por el marco NICE, a partir de las tareas, habilidades y conocimientos descritos para cada profesión.

Algunas de las profesiones consideradas en este cruce incluyen *Database Administrators*, *Network and Computer Systems Administrators*, *Software and Quality Assurance Engineers and Testers*, *Penetration Testers* y *Digital Forensics Analysts*. El uso del *Crosswalk* se justifica en el hecho de que NICE no define ocupaciones específicas, sino más bien roles que un especialista en ciberseguridad puede desempeñar en una organización. En la práctica, un mismo profesional puede asumir múltiples roles de manera simultánea, lo que dificulta basar el diseño curricular en una selección aislada de estos. En consecuencia, se adopta el *Crosswalk* por ser una fuente que describe ocupaciones reales y que integra de forma coherente los distintos roles que puede desempeñar un profesional en el ámbito de la ciberseguridad.

Otro de los recursos empleados es el mapeo entre KDs y KUs presentado en [Ramezanian y Niemi, 2024], el cual resulta útil para identificar los conocimientos específicos requeridos en los distintos trabajos asociados a la ciberseguridad. No obstante, esta fuente presenta una primera dificultad: existe una disparidad entre las versiones de los marcos utilizados en los mapeos. Mientras que el *Crosswalk* se basa en la versión 1.0.0 del NICE, el trabajo de Ramezanian emplea la versión original del documento (2017).

Esta diferencia no es menor, dado que en la versión 1.0.0 las 635 KDs originales fueron reformuladas, dividiéndose en algunos casos, o transformándose en *Skills*, *Tasks*, o

combinaciones de ellas. Afortunadamente, esta reformulación se realizó de manera correlativa: al eliminar una KD, la enumeración continuó a partir del último identificador existente. Por ejemplo, la K0001 pasó a convertirse en K0674, K0983 y K1014. Esto implica que no existe coincidencia de identificadores entre la versión 2017 y la versión 1.0.0, salvo en aquellos casos donde los elementos se mantuvieron sin modificación.

Para resolver este conflicto, se emplea el mapeo provisto por los creadores del NICE [NIST, 2025], el cual detalla las correspondencias entre los KSATs (*Knowledge, Skills, Abilities, Tasks*) definidos en la versión 2017 y los TKS (*Tasks, Knowledge, Skills*) de la versión 1.0.0.

Con estos tres recursos detallados, se procedió a realizar los reemplazos necesarios para obtener como resultado un mapeo entre los trabajos descritos en *O*NET* y los KUs del CSEC2017. Para ello, se desarrollaron *scripts* en lenguaje *Python* con el objetivo de limpiar las bases de datos y establecer las correspondencias entre los distintos mapeos. Cabe señalar que se eliminaron los *Skills* y *Tasks* surgidos de la transición del NICE 2017 a la versión 1.0.0, ya que no resultan relevantes en este estudio, el cual se centra en los conocimientos específicos (KDs) y no en las habilidades o tareas que pueden desempeñarse en la disciplina.

El resultado del procedimiento, consiguió el mapeo entre códigos de trabajos descritos en *O*NET* con los KUs relacionados. Este se presenta en las tablas del Anexo F.

Apartir del mapeo final se pudo calcular la frecuencia de aparición de cada KU en el conjunto total de trabajos considerados en el *Crosswalk* (23 en total). Posteriormente, los KUs se clasificaron en tres categorías según dicha frecuencia: *fundamentales* (frecuencia ≥ 20), *optativos* (frecuencia entre 15 y 19) y de *nicho* (frecuencia < 15). Esta clasificación se presenta en la Tabla C.1.

Los resultados muestran que la mayoría de los KUs identificados se concentran en la categoría de fundamentales. Este hallazgo resulta consistente con lo esperado, dado que todas las profesiones incluidas en el *Crosswalk* son adyacentes a la ciberseguridad. Por lo tanto, comparten un conjunto común de conocimientos esenciales que todo especialista debe poseer como base, tales como redes, criptografía y desarrollo de software.

A partir de este análisis, se concluye que para la construcción de perfiles debe considerarse la existencia de un núcleo (*core*) de contenidos que sea transversal a todos ellos, donde el factor diferenciador entre perfiles estará determinado por los contenidos clasificados como optativos o de nicho.

Dado lo anterior, se propuso la siguiente configuración general para la estructuración de perfiles de especialización.

PROPUESTA VI: 4 asignaturas *core* y 1 o 2 asignaturas especializadas.

A partir de la identificación de los KUs fundamentales, se diseñaron cuatro asignaturas

que constituyen el núcleo común de formación para todos los perfiles de especialización. De este modo, independientemente del perfil que el estudiante elija seguir, contará con una base sólida e indispensable para su desarrollo profesional en el ámbito de la ciberseguridad.

Al igual que en las propuestas anteriores, la conformación de las asignaturas se realizó agrupando contenidos afines y temáticamente coherentes. Sin embargo, se observa una diferencia significativa respecto a las propuestas previas: en esta ocasión, los contenidos relacionados con datos y software se integran en una misma asignatura, al igual que los de redes y sistemas, y se otorga un mayor énfasis a los aspectos sociales de la ciberseguridad. Esta variación puede considerarse una ventaja, ya que brinda al cuerpo docente la posibilidad de adoptar estas asignaturas fundamentales como base para su desarrollo curricular, incorporando un enfoque alternativo en la organización y enseñanza de los contenidos.

Las asignaturas *core* propuestas son los siguientes:

- Fundamentos técnicos de la ciberseguridad
- Arquitecturas de redes y sistemas seguros
- Gestión, gobernanza y respuesta ante incidentes
- Ciberseguridad y sociedad

Las asignaturas junto con los KUs que los componen se presentan en las Tablas 11, 12, 13 y 14.

Asignatura	**KUs**
Fundamentos técnicos de la ciberseguridad	1.1 Cryptography 1.3 Data Integrity and Authentication 1.4 Access Control 1.5 Secure Communication Protocols 1.8 Information Storage Security 2.1 Fundamental Principles 2.2 Design 2.4 Analysis and Testing

Tabla 11: Asignatura 1: Fundamentos técnicos de la ciberseguridad
Fuente: Elaboración propia

Asignatura	**KUs**
Arquitecturas de redes como sistemas seguros	3.1 Component Design 3.2 Component Procurement 4.1 Physical Media 4.3 Hardware Architecture 4.4 Distributed Systems Architecture 4.5 Network Architecture 4.7 Network Services 4.8 Network Defense 5.3 System Access 5.4 System Control 5.7 Common System Architectures 6.1 Identity Management

Tabla 12: Asignatura 2: Arquitecturas de redes como sistemas seguros
Fuente: Elaboración propia

Asignatura	**KUs**
Gestión, Gobernanza y Respuesta ante Incidentes	5.1 System Thinking 5.2 System Management 7.1 Risk Management 7.2 Security Governance & Policy 7.3 Analytical Tools 7.4 Systems Administration 7.5 Cybersecurity Planning 7.6 Business Continuity Disaster Recovery and Incident Management 7.7 Security Program Management 7.9 Security Operations 1.2 Digital Forensics

Tabla 13: Asignatura 3: Gestión, Gobernanza y Respuesta ante Incidentes
Fuente: Elaboración propia

Asignatura	**KUs**
Ciberseguridad y Sociedad	8.2 Cyber Law 8.3 Cyber Ethics 8.4 Cyber Policy 8.5 Privacy

Tabla 14: Asignatura 4: Ciberseguridad y Sociedad
Fuente: Elaboración propia

Para la construcción de los perfiles de especialización, se consideraron los KUs clasificados como optativos y de nicho en el análisis previo. A partir de ellos, se diseñaron cuatro perfiles diferenciados que permiten orientar la formación del estudiante hacia áreas específicas de la disciplina, en función de sus intereses profesionales y del rol que aspire a desempeñar en el mercado laboral. Estos perfiles representan trayectorias de especialización complementarias a las asignaturas fundamentales, y responden a las demandas identificadas en el análisis del *Crosswalk*.

Los perfiles definidos son los siguientes:

- Perfil 1: Especialista en Desarrollo Seguro y DevOps
- Perfil 2: Especialista en Aseguramiento de la Calidad y Análisis de Sistemas
- Perfil 3: Especialista en Dimensiones Sociales de la Ciberseguridad
- Perfil 4: Especialista en Gobernanza y Legalidad

La cantidad de KUs no pertenecientes al núcleo común es limitada, apenas diez; sin embargo, es posible agruparlos de manera coherente para conformar perfiles de especialización con sentido pedagógico y profesional. Asimismo, se observa una diferencia en la cantidad y profundidad del contenido disponible al analizar el nivel de los *Topics*. Por esta razón, se optó por dividir en dos asignaturas aquellos conjuntos de KUs que lo permitían, manteniendo en una única asignatura aquellos cuyo contenido resultaba más acotado.

Lejos de considerarse una limitación, esta situación puede interpretarse como una oportunidad. En escenarios donde los estudiantes dispongan de ocho asignaturas electivas, podrían elegir entre dos o tres asignaturas adicionales según el caso. Esto abre la posibilidad de que exploren otros intereses académicos, dado que la UTFSM ofrece múltiples alternativas para la convalidación de asignaturas electivas.

A continuación, se presentan las asignaturas conformadas y los KUs que los componen.

Perfil 1: Especialista en Desarrollo Seguro y DevOps

- Asignatura 1: Implementación de Software Seguro (KU 2.3 *Implementation*)
- Asignatura 2: Despliegue y Mantenimiento en Entornos DevOps (KU 2.5 *Deployment and Maintenance*)

Perfil 2: Especialista en Aseguramiento de la Calidad y Análisis de Sistemas

- Asignatura 1: Pruebas de Software y Sistemas (KU 3.3 *Component Testing*, 5.6 *System Testing*)
- Asignatura 2: Ingeniería Inversa de Componentes (KU 3.4 *Component Reverse Engineering*)

Perfil 3: Especialista en Dimensiones Sociales de la Ciberseguridad

- Asignatura: Privacidad y Comportamiento Humano en Ciberseguridad (KU 6.5 *Social and Behavioral Privacy*, 8.1 *Cybercrime*)

Perfil 4: Especialista en Gobernanza y Legalidad

- Asignatura: Seguridad del Personal y Cumplimiento Organizacional (KU 7.8 *Personnel Security*, 6.3 *Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms*)

Dentro del conjunto de KUs no pertenecientes al núcleo común, se observa la ausencia del KU 4.6 *Network Implementations*. Este fue excluido del diseño final por dos razones principales. En primer lugar, se buscó mantener la coherencia temática en la conformación de los perfiles, y este KU en particular no presentaba una relación directa con los demás contenidos técnicos seleccionados. Su inclusión habría introducido un nivel de especificidad que rompía con la estructura conceptual propuesta.

En segundo lugar, el contenido que aborda este KU es altamente especializado y orientado a niveles muy bajos de implementación de redes, abarcando temáticas como *IEEE 802/ISO networks*, *IETF networks and TCP/IP*, y *Practical integration and Glue protocols*. Si bien estos temas son relevantes para comprender la seguridad de redes en profundidad, la mayoría de los especialistas en ciberseguridad no trabajan directamente en estos niveles, dado que dichos componentes suelen estar ya implementados y se utilizan como bloques funcionales confiables. Además, la mayor parte de las vulnerabilidades explotadas actualmente se concentra en capas superiores, como la capa de aplicación o en errores atribuibles al factor humano.

No obstante, con el fin de no excluir completamente estos contenidos, se sugiere que, si se considera pertinente su inclusión, el KU 4.6 podría incorporarse dentro de la asignatura **Arquitecturas de Redes como Sistemas Seguros**, en el que ya se abordan temáticas de redes. De esta manera, se preservaría la coherencia temática sin comprometer la estructura general de los perfiles.

Otro aspecto que se considera relevante destacar es el relacionado con el *reverse engineering*. Si bien esta técnica puede emplearse con fines ofensivos —por ejemplo, para identificar vulnerabilidades y desarrollar código malicioso que las explote—, en el contexto de esta propuesta se le otorga un enfoque distinto. Su incorporación dentro de la asignatura **Aseguramiento y Pruebas de Software y Sistemas** responde a su utilidad como herramienta defensiva, ya que el *reverse engineering* permite realizar análisis y pruebas más exhaustivas sobre el software, especialmente en sistemas críticos en los que la existencia de vulnerabilidades o la presencia de casos de borde no contemplados representa un riesgo significativo. En estos escenarios, la capacidad de desensamblar, examinar y comprender el comportamiento interno del software constituye un complemento valioso a las metodologías tradicionales de prueba, contribuyendo así a garantizar un mayor nivel de confiabilidad y seguridad en el producto final.

3.3. Síntesis de la propuesta

El presente capítulo desarrolló la propuesta de solución al problema identificado en esta investigación: la ausencia de una línea formativa estructurada en ciberseguridad dentro del plan de estudios de Ingeniería Civil Informática de la UTFSM. Para ello, se diseñó un marco metodológico que combina el uso de los principales frameworks internacionales (NICE y CSEC2017) con el análisis del estado actual de la oferta académica en Chile, integrando además aportes metodológicos de trabajos previos y datos provenientes del mercado laboral global.

Este proceso permitió no solo caracterizar las áreas del conocimiento más relevantes en el ámbito de la ciberseguridad, sino también adaptar dicha caracterización a la realidad institucional y nacional. Sobre esta base, se formularon múltiples propuestas curriculares que exploran distintas estrategias de diseño:

Las propuestas basadas en pesos traducen la representación actual de las áreas en la educación chilena y en la fuerza laboral en distribuciones proporcionales de asignaturas y créditos.

Las propuestas basadas en importancia priorizan contenidos esenciales en escenarios con restricciones de tiempo y carga académica, adaptándose al perfil del estudiante de la UTFSM.

Finalmente, las propuestas basadas en perfiles abordan la formación desde una perspectiva profesional, estableciendo un núcleo común y trayectorias de especialización vinculadas a ocupaciones reales en el mercado laboral.

La coexistencia de estas estrategias no representa una dispersión metodológica, sino una fortaleza de la propuesta: permite que la línea complementaria en ciberseguridad sea flexible y ajustable a diferentes contextos institucionales, necesidades curriculares y

recursos disponibles. Asimismo, ofrece al cuerpo docente un conjunto de herramientas y alternativas para diseñar programas de formación más alineados con la demanda profesional y las tendencias internacionales en la disciplina.

CAPÍTULO 4
VALIDACIÓN DE EXPERTOS

Si bien las propuestas formuladas en este trabajo se sustentan en datos objetivos y en referentes desarrollados por instituciones internacionales, tales como los *frameworks* NICE y CSEC2017 ya mencionados, es importante reconocer la existencia de un inevitable grado de subjetividad en el proceso de toma de decisiones asociado a la configuración curricular. Esta condición resulta particularmente relevante en una disciplina tan amplia y heterogénea como la ciberseguridad, en la que los distintos profesionales involucrados pueden otorgar mayor relevancia a determinadas áreas según su campo de especialización, experiencia o enfoque conceptual respecto de la protección de la información y los sistemas.

En el caso específico de la formulación de las asignaturas propuestas en este trabajo, dicha subjetividad se manifiesta principalmente en la priorización de las áreas temáticas, en su agrupación conceptual y en la selección de los contenidos individuales que se consideran pertinentes de impartir. En virtud de ello, se optó por incorporar una segunda instancia de validación mediante la consulta a expertos que se desempeñan en áreas afines a la ciberseguridad, con el propósito de complementar y contrastar los criterios adoptados.

En este capítulo se examina el procedimiento empleado para la obtención de las apreciaciones de estos expertos, así como la forma en que dichas valoraciones se vinculan con las propuestas curriculares formuladas en el presente estudio.

4.1. Metodología de la consulta experta

Con el propósito de validar el trabajo realizado en la formulación de las distintas propuestas de planes complementarios para la carrera de Ingeniería Civil en Informática de la UTFSM, se optó por recurrir a la consulta de expertos pertenecientes al entorno académico cercano, específicamente docentes con desempeño en disciplinas vinculadas a la ciberseguridad. En particular, se consultó a profesores de la UTFSM con el fin de evaluar tanto la viabilidad de las propuestas como su coherencia interna, considerando su conocimiento en la disciplina y su experiencia en labores propias de la docencia universitaria, tales como la planificación de asignaturas, el diseño de planes de estudio y la gestión académica.

El tamaño de la muestra resultó reducido, ya que solo dos profesores respondieron el cuestionario de un total de cinco académicos contactados. Esta situación se explica, en parte, por la limitada disponibilidad de docentes con formación específica en ciberseguridad, dado que la mayoría del cuerpo académico se especializa en otras áreas de la

computación, tales como teoría computacional, bases de datos o desarrollo de software. Los profesores seleccionados para la consulta presentaban especialización en ámbitos como redes, criptografía o seguridad de la información, áreas directamente relacionadas con la temática abordada, las cuales no cuentan con una alta representación dentro de la planta docente.

Dado que los términos utilizados para describir los roles u ocupaciones en el ámbito de la ciberseguridad no son uniformes, y considerando además la amplia diversidad de especialidades que la conforman —al tratarse de una disciplina que integra y articula múltiples campos relacionados—, se permitió a los encuestados describir brevemente el área en la cual se desempeñan profesionalmente. A partir de ello, se obtuvieron los siguientes datos:

- Experto 1: Networking, Information Security, Cyber Architecture.
- Experto 2: Diseño de Protocolos Criptográficos.

Durante el proceso de formulación de propuestas fue necesario adoptar diversas decisiones de diseño que influyeron directamente en su configuración final. Entre estas se incluyen la selección de los temas específicos a impartir, la eventual agrupación de áreas afines, la determinación de contenidos considerados fundamentales para la formación de los estudiantes, entre otros aspectos relevantes. Con el fin de evaluar la pertinencia de dichas decisiones, se optó por un procedimiento de validación indirecto: en lugar de solicitar a los expertos una evaluación directa de las propuestas curriculares resultantes, se les permitió tomar sus propias decisiones, replicando de manera aproximada el proceso de formulación utilizado en este trabajo a través de un cuestionario estructurado.

El cuestionario fue organizado en función de las ocho KAs definidas por el CSEC2017. Cada sección contempló cuatro preguntas obligatorias y una adicional de carácter opcional. Su objetivo fue recoger la opinión de los expertos respecto de cada área de conocimiento de manera individual, específicamente en relación con el grado de relevancia que le atribuyen dentro del contexto de la construcción de planes de estudio en ciberseguridad. Las cuatro primeras preguntas estuvieron orientadas a la evaluación general de la KA correspondiente, mientras que la quinta pregunta se enfocó en la valoración específica de sus respectivas KUs.

En lo que sigue, se detallan las preguntas formuladas y se analiza su relación con el proceso de diseño de asignaturas desarrollado en este trabajo.

4.2. Preguntas de la consulta experta

Dentro de las propuestas formuladas en este trabajo, aquellas basadas en pesos se caracterizan por generar asignaturas a un nivel de abstracción elevado, en las cuales las KAs se asignan sin detallar explícitamente los contenidos específicos a tratar, priorizando en cambio la distribución de las áreas en asignaturas individuales o bien su agrupación cuando resulta pertinente.

Con el propósito de simular este proceso de toma de decisiones a nivel macro-curricular, el cuestionario incluyó una serie de preguntas diseñadas para emular dicha lógica de selección. A continuación, se presentan estas preguntas ejemplificadas mediante la KA-1, entendiendo que su estructura y formulación fueron idénticas para todas las áreas consideradas. Cabe destacar que, con el fin de proporcionar un mayor contexto y facilitar la correcta interpretación por parte de los encuestados, se incluyó una breve descripción introductoria de cada área, permitiendo así familiarizar a los expertos con el alcance conceptual de cada KA antes de proceder a su evaluación.

- Qué importancia le daría a KA-1 (Indispensable, Importante, Opcional, Nicho)
- Con qué nivel de profundidad impartiría KA-1 (Introductorio, Intermedio, Avanzado)
- ¿Considera que KA-1 debería ser el único contenido de una asignatura? (Sí, No)
- Si contesto ”No”. Con cuales KAs es razonable agruparla. Omitir si contesto ”Si”(Con opción de elegir una de las KA distintas a las que se está evaluando)

Las preguntas planteadas replican el proceso empleado para la distribución de las KAs en asignaturas dentro de las propuestas basadas en pesos, donde los criterios de prioridad y profundidad permiten inferir la extensión y el tratamiento curricular requerido para cada área. En este sentido, aquellas áreas consideradas indispensables o que debían ser abordadas en niveles intermedios o avanzados podían justificar la asignación de una asignatura completa de manera independiente. En contraste, las áreas definidas como optativas, de nicho o de nivel introductorio ofrecían la posibilidad de ser fraccionadas e integradas conjuntamente en asignaturas que agruparan múltiples KA.

Por otra parte, las propuestas basadas en importancia y aquellas basadas en perfiles requieren un mayor nivel de granularidad que el contemplado en las preguntas anteriores, dado que su formulación depende de la priorización de contenidos específicos dentro de cada área. Con el fin de recoger la opinión de los expertos bajo este nivel de detalle, se solicitó que evaluaran individualmente todos los KUs asociados a cada KA, asignándoles una calificación en una escala de 1 a 5 en el contexto de un plan de estudios, donde 1 representa la mínima importancia y 5 la máxima.

- Califique los temas del KA-1 según su nivel de importancia para ser abordado con mayor profundidad en un plan de estudios. Con 1 siendo menos importante y 5 más importante. (Se presentan los KUs del área con la opción de calificarlos entre 1 a 5)

Esta calificación reproduce, en términos metodológicos, el proceso seguido para la selección de contenidos específicos en aquellas propuestas que requerían un mayor nivel de detalle. Cabe destacar que, en el caso de las propuestas basadas en importancia y basadas en perfiles, el trabajo desarrollado en este estudio alcanzó un grado de especificidad superior, llegando al nivel de *Topics* del CSEC2017, mientras que la consulta a expertos se realizó únicamente hasta el nivel de KUs.

Esta decisión respondió a criterios de factibilidad, dado el elevado número de *Topics* existentes, lo que habría hecho inviable solicitar a los expertos una evaluación tan exhaustiva. No obstante, la selección a nivel de KUs resulta metodológicamente adecuada, puesto que estas unidades mantienen una relación directa y estructural con los *Topics* que las componen, permitiendo capturar de manera representativa las prioridades temáticas de cada área.

Adicionalmente, se proporcionó a los expertos una versión acotada del CSEC2017 que incluía las descripciones oficiales de las KUs, las cuales ofrecen una caracterización suficientemente amplia de los contenidos que estas abarcan. Esto permitió que los participantes tomaran decisiones informadas, reduciendo al mismo tiempo la carga cognitiva asociada al exceso de información y evitando un nivel de detalle innecesariamente complejo para los fines de la consulta.

Los resultados del proceso se presentan en las tablas en el Anexo D.

4.3. Análisis de los resultados

En esta sección se presentan y analizan los resultados obtenidos a partir de la consulta experta, con el objetivo de contrastarlos con las distintas propuestas curriculares formuladas en este trabajo. En particular, se examina el grado de coherencia entre la valoración entregada por los expertos y las propuestas basadas en pesos, en importancia y en perfiles, considerando tanto la priorización de las áreas de conocimiento como la representación de sus unidades constitutivas. Este análisis permite evaluar el nivel de alineación entre los criterios definidos en las propuestas y la percepción experta respecto de la relevancia formativa de los contenidos, aportando evidencia para la discusión sobre la solidez y consistencia de las soluciones planteadas.

4.3.1. Respuestas para propuestas basadas en pesos

El primer conjunto de preguntas, orientado a evaluar las propuestas basadas en pesos, tuvo como objetivo analizar las KAs de manera individual y, en caso pertinente, explorar posibles criterios de agrupación entre ellas. Para este propósito se consideraron dos criterios fundamentales: importancia y profundidad.

El criterio de importancia permite discriminar qué áreas deben ser consideradas dentro del currículo, en función de su relevancia formativa. Por su parte, la profundidad aporta una dimensión más operativa al proceso de formulación curricular, pues el nivel al cual se imparte una asignatura está estrechamente vinculado al tiempo disponible, ya sea medido en semestres o meses. Este criterio, además, entrega indicios sobre la posible necesidad de segmentar una misma área en más de una asignatura, por ejemplo, distinguiendo entre una instancia introductoria y otra avanzada, o bien entre una asignatura de carácter teórico y una posterior de enfoque predominantemente práctico.

Dado que el interés principal de esta etapa se centra en la definición y priorización de las áreas más que en su nivel específico de desarrollo —el cual depende de factores adicionales—, se otorgó una mayor ponderación al criterio de importancia. En consecuencia, se asignó un multiplicador de 0,6 a la importancia y de 0,4 a la profundidad. Las categorías de importancia (Indispensable, Importante, Opcional, Nicho) fueron valoradas con puntajes decrecientes desde 4 hasta 1, respectivamente, mientras que las categorías de profundidad (Avanzado, Intermedio, Introductorio) fueron valoradas de 3 a 1 punto, respectivamente. El puntaje final de cada KA se obtuvo a partir de la suma ponderada de ambos criterios.

Los valores resultantes de este proceso se presentan en la Tabla 15.

KA	**Puntaje final**
KA-1	3,6
KA-2	2,4
KA-3	2,6
KA-4	2,9
KA-5	2,9
KA-6	3,1
KA-7	2,4
KA-8	2,4
Total	22,3

Tabla 15: Puntuaciones finales asignadas por expertos a las KAs
Fuente: Elaboración propia

Para analizar de mejor forma los valores, se calcularon los porcentajes relativos de cada área respecto del total de puntos obtenidos. Estos se muestran en la Tabla 16.

KA	**Porcentaje parcial**
KA-1	16,14 %
KA-2	10,76 %
KA-3	11,66 %
KA-4	13,00 %
KA-5	13,00 %
KA-6	13,90 %
KA-7	10,76 %
KA-8	10,76 %
Total	100,00 %

Tabla 16: Porcentajes relativos asignados por expertos a las KAs
Fuente: Elaboración propia

Analizando los porcentajes obtenidos en la valoración de las KA, se desprenden las siguientes conclusiones:

- Los expertos evidencian una tendencia a favorecer una cobertura más amplia de áreas, en lugar de concentrar la formación en unas pocas. Esta postura contrasta con la realidad observada en el análisis de los programas chilenos de ciberseguridad, donde se aprecia una mayor focalización en ciertas áreas, relegando otras a un segundo plano.
- La mayoría de las áreas fue calificada por los expertos como “Importantes” o “Indispensables”. Solo una fue considerada “Opcional”, y por uno expertos, mientras que ninguna fue categorizada como “Nicho”, lo que refleja una valoración generalizada de la relevancia dentro de la formación en ciberseguridad.
- En términos de profundidad, los expertos situaron mayoritariamente a las áreas en un nivel intermedio. Coincidieron en que la seguridad de los datos debe ser impartida con mayor profundidad. Asimismo, reconocieron que existen áreas para las cuales un nivel introductorio sería suficiente; no obstante, no se alcanzó consenso respecto a cuáles deberían asignarse a dicho nivel.

Cabe señalar que, debido a una limitación del cuestionario aplicado, los expertos, al momento de seleccionar agrupaciones de áreas, solo podían optar por una única alternativa, es decir, agrupar el área evaluada con una sola área adicional. Esta restricción difiere del proceso empleado en la formulación de asignaturas, donde existía la posibilidad de agrupar un mayor número de áreas, otorgando así mayor flexibilidad en la configuración de las propuestas.

Esta restricción implicó que los expertos debieran establecer relaciones más específicas entre pares de áreas, priorizando aquellas que consideraban más directamente vinculadas. En este sentido, las agrupaciones resultantes reflejan asociaciones más focalizadas,

lo que permite identificar con mayor claridad los vínculos percibidos entre las distintas áreas evaluadas.

Para efectos del análisis, se consideraron como equivalentes aquellas agrupaciones conformadas por las mismas dos áreas, independientemente del orden en que estas aparecieran. Asimismo, en el caso de las agrupaciones de tres áreas presentes en las propuestas, estas fueron descompuestas en los tres pares posibles derivados de la permutación de dichas áreas, con el fin de homologar el tratamiento de los datos y mitigar la limitación impuesta por el diseño del cuestionario.

Al comparar las agrupaciones obtenidas, se observa que los expertos tendieron a reducir la cantidad de áreas no agrupadas, mientras que en las propuestas de asignaturas elaboradas en este trabajo predominan las áreas presentadas de forma individual. Esta diferencia sugiere que los expertos conciben la ciberseguridad como un dominio de carácter transversal, en el cual las distintas áreas deben articularse de manera integrada, más que abordarse de forma aislada. Asimismo, esta preferencia podría interpretarse como reflejo de su experiencia en procesos de diseño curricular, donde las restricciones de tiempo y carga académica conducen a privilegiar estructuras que permitan abordar múltiples competencias de manera simultánea, favoreciendo un enfoque más holístico del aprendizaje.

En la propuesta I-A se identificaron cuatro coincidencias, dos con cada experto, mientras que en la propuesta I-B se registró una única coincidencia con el Experto 1. Estos resultados sugieren que la propuesta I-A presenta un mayor grado de concordancia con las agrupaciones realizadas por los expertos, en comparación con la propuesta I-B, la cual se configuró a partir de los valores empleados en [Lehto y Martti, 2022], cuyos criterios responden principalmente a tendencias del mercado laboral.

Cabe destacar que la propuesta I-B, posee una mayor presencia de áreas abordadas de forma individual, sin ser integradas con otras. Esta diferencia podría interpretarse como una manifestación del contraste entre un enfoque de carácter más académico, orientado a la articulación conceptual e integración de contenidos, y un enfoque más fragmentado, vinculado a la especialización profesional en áreas específicas, coherente con las demandas del entorno laboral.

4.3.2. Respuestas para propuestas basadas en importancia

El segundo conjunto de preguntas tuvo por objetivo calificar las KUs de cada KA de manera individual, permitiendo alcanzar un mayor nivel de especificidad respecto al valor atribuido a los contenidos que pueden ser considerados dentro del currículo. Este enfoque posibilita identificar con mayor precisión qué unidades de conocimiento son percibidas como más relevantes en el contexto de la formación en ciberseguridad.

Para llevar a cabo este análisis se contó con las calificaciones asignadas por los expertos a cada KU. El paso siguiente consistió en vincular estos resultados con las propuestas curriculares desarrolladas en este trabajo. Para ello, se sumó el total de puntos otorgados a cada KU por los encuestados y posteriormente se normalizó el resultado, con el fin de obtener un porcentaje representativo de su valoración relativa.

La normalización se realizó mediante la siguiente expresión:

$$A = \frac{\sum(\text{calificación experta}) \cdot 100}{10} \tag{2}$$

donde A corresponde al porcentaje de importancia asignado a cada KU en función de las evaluaciones emitidas por los expertos.

La segunda etapa del proceso consistió en transformar las propuestas formuladas en valores cuantificables y directamente comparables con las calificaciones otorgadas por los expertos. Para ello, se contabilizó la aparición de los *Topics* que conformaban las cuatro asignaturas propuestas. Posteriormente, estos conteos se agregaron a nivel de KU; así, por ejemplo, si se incluían los *Topics* 1.1.2, 1.1.4 y 1.1.5, se asignaba una frecuencia de 3 a la KU 1.1.

Cabe destacar que cada *Topic* fue considerado una única vez, aun cuando apareciera en más de una asignatura, con el fin de evitar una sobre-representación artificial de una KU particular. Finalmente, se calculó el porcentaje de *Topics* utilizados respecto del total de aquellos definidos para cada KU, lo que permitió estimar el nivel de representación de dicha unidad dentro de las asignaturas propuestas, entendido como un indicador de su importancia relativa en el diseño curricular.

La cuantificación de este valor se obtuvo mediante la siguiente expresión:

$$B = \frac{\sum(\text{Topics utilizados del KU}_X) \cdot 100}{\text{Total de Topics del KU}_X} \tag{3}$$

donde B corresponde al porcentaje de importancia individual asignado a cada KU según su aparición en las asignaturas propuestas.

El conjunto completo de datos resultantes se presenta en las tablas incluidas en el Anexo E. De los datos obtenidos se desprende que los expertos tienden a asignar altos niveles de relevancia a la mayoría de las áreas, concentrándose principalmente en rangos elevados (70–100 %). En contraste, las propuestas formuladas presentan una menor homogeneidad, evidenciando una distribución más dispar, en la que ciertos KUs alcanzan valores de relevancia máxima, mientras que otros son omitidos.

Esta situación da cuenta de una desalineación parcial entre ambas perspectivas, en tanto las propuestas no reproducen estrictamente la jerarquía de importancia establecida por los expertos, sino que responden a una lógica propia derivada del análisis detallado de los *Topics*, priorizando ciertos contenidos en función de su especificidad y coherencia interna.

A partir de esta comparación, los resultados pueden clasificarse en cuatro categorías generales, según la relación entre la relevancia asignada por las propuestas y aquella otorgada por los expertos:

- **Alta en propuesta – Alta según expertos**
- **Alta en propuesta – Baja según expertos**
- **Baja en propuesta – Alta según expertos**
- **Baja en propuesta – Baja según expertos**

En relación con la categoría *Alta en propuesta – Alta segun expertos*, esta refleja que los contenidos seleccionados corresponden a núcleos conceptuales de alta relevancia formativa, evidenciando una adecuada identificación de su importancia por parte de quienes elaboraron las propuestas. Por su parte, la categoría *Alta en propuesta – Baja según expertos* pone de manifiesto una diferencia de enfoque, atribuible al modelo adoptado durante el proceso de formulación, en el cual se privilegió la selección de contenidos vinculados al ámbito del software, asumiendo implícitamente que otros conocimientos podían considerarse previamente adquiridos o menos prioritarios.

En el caso de la categoría *Baja en propuesta – Alta según expertos*, la brecha observada puede explicarse nuevamente por el carácter acotado del enfoque aplicado, que, al centrarse en contenidos específicos del software, deja fuera otros temas que los expertos consideran relevantes desde una perspectiva más integral de la ciberseguridad. Tanto esta situación como la anterior representan una oportunidad para revisar y ampliar el enfoque adoptado, incorporando contenidos valorados por los expertos y evitando una sobre-focalización en aquellos ya presentes en las propuestas.

Finalmente, la categoría *Baja en propuesta – Baja según expertos* evidencia una coincidencia en la valoración reducida de ciertos temas, lo que sugiere una correcta identificación, por parte de los autores de las propuestas, de contenidos con menor peso formativo, ya sea por su carácter secundario o por estar asociados a roles profesionales altamente especializados o de nicho.

Los resultados del proceso se presentan en las tablas en el Anexo E.

Otro análisis se concentró específicamente en la segunda y tercera categoría, correspondientes a los casos en que hay diferencia entre la calificación asignada por los expertos

y la relevancia de los KUs. Para esto, se calculó la diferencia en puntos porcentuales entre ambos valores y se estableció un umbral del 50 % de manera arbitraria con el fin de identificar discrepancias consideradas significativas.

Bajo este criterio, se observó que el 24,07 % de los KUs presentó diferencias superiores a dicho umbral, lo que indica que, si bien existe una alineación general entre la opinión experta y las propuestas formuladas, persisten divergencias relevantes que podrían constituir focos prioritarios de revisión y ajuste en futuras iteraciones del diseño curricular.

Cabe destacar que la mayoría de los casos que superan este umbral corresponden a KUs cuya representación en las propuestas es nula, es decir, contenidos que, bajo la lógica de selección empleada, quedan completamente excluidos.

Esta situación pone de manifiesto una posible subvaloración estructural de ciertos conocimientos que, desde la perspectiva experta, resultan pertinentes, evidenciando así una distancia entre el modelo de selección adoptado y una visión más integral del dominio formativo.

Al examinar los KUs en los que se concentran estas discrepancias, es posible agruparlas en tres categorías generales según la razón que explica su aparición:

- **Enfoque distinto:** Algunos KUs, tales como *Data Forensics*, *Component Procurement* y *Cyber Law*, quedan fuera del modelo empleado para la selección de contenidos. Esto se debe a que dichos ámbitos se asocian a perfiles profesionales con mayor nivel de especialización o experiencia, o bien a roles que trascienden el quehacer técnico directo, como aquellos vinculados a la gestión organizacional o al asesoramiento jurídico, los cuales no constituyen el foco principal del currículo propuesto.
- **Conocimientos previos asumidos:** KUs como *Documentation* y *Network Architecture* fueron excluidos en la formulación de las propuestas debido a que el currículo se concibe como complementario, asumiendo la existencia de conocimientos base en computación general por parte del estudiantado. Dichos conocimientos se adquieren previamente en asignaturas como desarrollo de software o introducción a las redes de computadores, lo que justifica su exclusión como contenidos específicos de ciberseguridad.
- **Ideas transversales:** Con el objetivo de reducir la sobrecarga temática y evitar redundancias, la lógica empleada en la confección de las propuestas priorizó la minimización de ideas aplicables de manera transversal a múltiples ámbitos de la computación. En este contexto, KUs como *Component Design* y *System Testing* fueron descartados, privilegiándose contenidos similares en el marco del desarrollo de software, donde se abordan conceptos equivalentes como *Analysis and Testing* y *Design*, adaptados al enfoque específico del plan propuesto.

En conjunto, los resultados obtenidos permiten concluir que las discrepancias observadas entre la valoración experta y la representación de las KUs en las propuestas no deben interpretarse necesariamente como deficiencias del diseño curricular, sino como la manifestación de criterios de priorización distintos, sustentados en enfoques conceptuales y objetivos formativos diferenciados. Mientras la opinión experta tiende a reflejar una visión amplia e integral del dominio de la ciberseguridad, las propuestas formuladas responden a una lógica de selección más acotada, orientada por la coherencia interna del currículo y por la focalización en determinados ejes temáticos.

En este sentido, el análisis pone de relieve la existencia de múltiples alternativas legítimas para la toma de decisiones curriculares: mantener la estructura propuesta, privilegiando su consistencia conceptual; ajustar los contenidos para aproximarse en mayor medida a la visión amplia planteada por los expertos; o bien incorporar criterios externos adicionales, tales como las demandas del mercado laboral u orientaciones institucionales específicas. Cada una de estas alternativas conlleva compromisos distintos entre amplitud, profundidad y especialización, los cuales deben ser evaluados en función del propósito formativo del programa y comprendidos como parte de un proceso de diseño curricular de carácter iterativo, susceptible de ajustes y refinamientos sucesivos en función de nuevos antecedentes y contextos de aplicación.

4.3.3. Respuestas para propuestas basadas en perfiles

Finalmente, se analizan las propuestas basadas en perfiles, las cuales, al igual que las anteriores, presentan una estrecha relación con el nivel de especificidad de las KUs. No obstante, dado que la elaboración de asignaturas desde este enfoque se fundamentó principalmente en el análisis de las funciones profesionales descritas en el *O*NET Crosswalk* [CSET/ETO, 2024], y en su mapeo directo hacia las KUs, más que en un ejercicio interpretativo por parte del investigador, se optó por utilizar la valoración experta de estas últimas como principal criterio de contraste.

En primera instancia, los valores porcentuales previamente obtenidos a partir de la calificación experta fueron asignados a las asignaturas de los perfiles de especialización, incluyendo tanto las asignaturas *core* como las especializadas.

Como se señaló anteriormente, la calificación experta no presentó valores inferiores al 70 % para ningún KU. En función de ello, se estableció una categorización operativa de relevancia, definida en cuatro niveles: muy alta, alta, media y baja, correspondientes a los valores de 100, 90, 80 y 70, respectivamente.

De los 35 KUs asociados a las asignaturas *core*, 29 (82,86 %) se sitúan en los niveles de relevancia 80–100, y 18 de ellos (51,43 %) en los niveles más altos (90–100). Esta distribución evidencia una alineación sólida entre la estructura central propuesta y la valoración experta, lo que sugiere que los contenidos fundamentales del plan se corres-

ponden mayoritariamente con conocimientos considerados altamente relevantes en el ámbito profesional.

Si bien se observa una concentración significativa en los niveles superiores de relevancia, la presencia de KUs en el nivel 70 indica que el plan también incorpora contenidos necesarios, aunque de menor prioridad relativa. Esto sugiere una combinación equilibrada entre saberes estructurales altamente prioritarios y otros que, aun siendo secundarios, contribuyen a una formación integral del perfil base.

En cuanto a las asignaturas especializadas, 8 de los 9 KUs (88,89 %) se concentran igualmente en los rangos 80–100, aunque con menor presencia en los valores extremos. Esta distribución indica que, si bien estas asignaturas cumplen una función de profundización temática, mantienen una alta coherencia con las prioridades definidas por la opinión experta, reforzando su pertinencia dentro del modelo formativo propuesto.

A diferencia de las asignaturas *core*, cuya concentración se observa ligeramente mayor en los niveles máximos de relevancia, las asignaturas especializadas presentan una dispersión más equilibrada dentro de los rangos altos. Este comportamiento resulta coherente con su función de profundización temática, ya que permite ampliar el espectro de contenidos sin comprometer su pertinencia dentro de la disciplina.

Otro aspecto relevante dentro de este análisis corresponde a la relación con la clasificación inicial realizada por los expertos respecto de las áreas de conocimiento (KAs). Ninguna de estas fue calificada con una importancia baja y solo una fue considerada como opcional por uno de los evaluadores. Este resultado sugiere que, incluso tratándose de perfiles más especializados, estos se estructuran a partir de áreas que continúan siendo significativas para la disciplina, evitando una excesiva especificidad asociada a contenidos excesivamente emergentes o de carácter altamente especializado, tales como aquellos propios de niveles de posgrado avanzado o investigación doctoral.

Finalmente, se observa que el área *Societal Security* adquiere una mayor presencia en comparación con las propuestas basadas en importancia o en pesos. Este fortalecimiento resulta consistente con la valoración experta, en la que dicha área es clasificada con altos niveles de relevancia, reforzando así su posicionamiento dentro del modelo curricular propuesto.

El conjunto de asignaturas *core* se configura como una base sólida y flexible para la formación del estudiantado, dado que se orienta hacia conocimientos de alta relevancia profesional según la valoración experta. Esta estructura permite el desarrollo de fundamentos robustos, al tiempo que habilita la posibilidad de especialización mediante la elección de perfiles específicos o trayectorias de profundización futura, favoreciendo así una formación adaptable y progresiva.

Asimismo, se observa un énfasis en áreas que no habían adquirido la misma centralidad en propuestas previas, como es el caso de *Societal Security*, la cual, en este conjunto de asignaturas, adquiere mayor protagonismo al materializarse en una asignatura individual. Este hecho refleja una ampliación del enfoque formativo hacia dimensiones sociales y contextuales de la disciplina.

En este marco, la propuesta curricular basada en perfiles no solo responde a las demandas profesionales previamente identificadas, sino que además promueve una formación equilibrada entre competencias técnicas, organizacionales y sociales. Lo anterior contribuye a la configuración de un perfil profesional integral, pertinente y capaz de adaptarse a diversos contextos laborales y escenarios de desempeño.

CONCLUSIONES

El presente trabajo abordó la problemática de la incorporación de la ciberseguridad en la formación de pregrado en la carrera de Ingeniería Civil Informática en la UTFSM, proponiendo un conjunto de lineamientos curriculares complementarios fundamentados en marcos de referencia internacionales y en el análisis del contexto académico nacional. A partir de este enfoque, se desarrollaron diversas metodologías de formulación curricular que permiten aproximarse al diseño de planes de estudio desde perspectivas complementarias.

Entre los principales aportes de este trabajo se encuentra, en primer lugar, el análisis de la oferta académica en ciberseguridad existente en Chile, lo que permitió identificar tendencias, vacíos formativos y patrones de focalización en determinadas áreas del conocimiento. En segundo lugar, se propone una equivalencia entre los pesos observados en los programas nacionales y las *Knowledge Areas* del CSEC2017, inspirada en enfoques similares al planteado por [Ramezanian y Niemi, 2024], lo que posibilita una lectura estructurada y comparable de la relevancia otorgada a cada área. Asimismo, se formuló un conjunto de propuestas curriculares ad hoc basadas en tres metodologías diferenciadas —pesos, importancia y perfiles—, las cuales ofrecen alternativas flexibles para la construcción de currículos complementarios según distintos criterios de priorización. Finalmente, se establece una relación explícita entre el *O*NET Crosswalk* y el CSEC2017, permitiendo traducir funciones profesionales reales en términos de *Knowledge Units*, lo que contribuye a vincular de manera más directa los marcos académicos con el ejercicio profesional de la ciberseguridad.

No obstante, el trabajo presenta una serie de limitaciones que deben ser consideradas al interpretar sus resultados. En particular, la opinión experta no fue incorporada directamente en la etapa de confección de las propuestas, sino utilizada posteriormente como mecanismo de contraste y validación, lo que limita su influencia en las decisiones iniciales de diseño. La metodología basada en pesos, si bien resulta útil como aproximación de alto nivel, carece de la granularidad necesaria para definir contenidos específicos de manera autónoma. Por su parte, la metodología basada en importancia presenta un componente inevitable de subjetividad, que podría atenuarse mediante la integración de evaluaciones expertas. Finalmente, la metodología basada en perfiles, al apoyarse en el *O*NET*, adopta una estructura relativamente rígida y dependiente del contexto laboral estadounidense, lo que puede generar desajustes respecto de las necesidades y realidades del entorno local.

En cuanto a las proyecciones de trabajo futuro, este estudio puede entenderse como una primera base sobre la cual desarrollar procesos iterativos de refinamiento curricular. Una línea natural de continuación consiste en utilizar las metodologías propuestas como marcos de apoyo, equilibrando sus resultados con la opinión experta, la oferta académica de instituciones locales, las demandas del mercado laboral y el enfoque for-

mativo particular de cada institución. En este sentido, una ampliación del proceso de evaluación experta, con una mayor participación y diversidad de perfiles, permitiría ajustar las propuestas, especialmente en los casos donde se observan discrepancias significativas entre la valoración experta y la selección de contenidos. Dichas discrepancias podrían abordarse mediante procesos de consenso que permitan reformular las propuestas, manteniendo el énfasis original —particularmente en los contenidos de software— sin perder coherencia con la experiencia profesional del dominio.

Finalmente, un ámbito relevante para trabajos posteriores corresponde al desarrollo del componente pedagógico del currículo, profundizando en la definición de objetivos de aprendizaje, metodologías de evaluación y estrategias didácticas específicas. En particular, resulta pertinente explorar el uso de entornos prácticos como *Hack The Box* [HackTheBox, sf] o *TryHackMe* [TryHackMe, sf], así como la selección y articulación de herramientas especializadas —por ejemplo, *Metasploit* [Metasploit, sf] —, con el fin de fortalecer la dimensión aplicada de la formación en ciberseguridad y asegurar una adecuada integración entre teoría y práctica.

ANEXOS

Anexo A: Tabla de análisis de asignaturas/módulos

	KU
MÓDULO 1: GESTIÓN DE LA CIBERSEGURIDAD EN LA ORGANIZACIÓN	
Introducción. Conceptos de la Ciberseguridad.	X
Dominios de la Seguridad de la Información.	X
Rol de los diferentes actores involucrados.	6.3;7.8
Aspectos Legales en ciberseguridad.	8.2;7.2;1.8
Gobierno Corporativo de la Ciberseguridad.	7.2
Gobierno y gestión de la Ciberseguridad.	7.2;7.5;7.7
Visión ejecutiva e impactos del gobierno corporativo de la Ciberseguridad.	7.2
MÓDULO 2: DESARROLLO DE APLICACIONES SEGURAS	
Ciclo de Vida del desarrollo de sistemas seguros	2.2;2.3;2.4;2.5
Modelamiento de amenazas	5.1
Mitigación de Riesgos	7.1
Arquitectura de seguridad	1.4
Modelos de seguridad	5.2
Requerimientos legales	1.8;.2.7;7.2;8.2
Testing	2.4;5.6;3.3
Buenas prácticas de seguridad	2.1;2.3
Diseño web seguro	1.5;2.1;2.2;2.3;4.7
MÓDULO 3: PENETRATION TESTING	
Logística, comercial y técnica, de una Prueba de Penetración.	5.4;8.2
Recopilación de información y detección de sistemas.	4.8
Enumeración.	4.8
Evaluación de vulnerabilidades automatizada.	5.4
Explotación de sistemas operativos.	5.4
Evaluación avanzada y técnicas de explotación.	1.6;3.4;5.4
Redes, Sniffing e IPS.	4.8
Evaluación y explotación de tecnologías web.	1.5;4.7
Redacción de informes.	-1
MÓDULO 4: INVESTIGACIÓN FORENSE	
La computación forense, una perspectiva de tres roles.	1.2;5.4;8.2
El Intruso y sus técnicas.	5.4;8.1
Para profundizar práctica de asalto a una sesión tcp.	4.6;4.8
El administrador y la infraestructura de la seguridad informática.	5.2;7.4
El investigador y la criminalística digital.	1.2;8.2
Retos y riesgos emergentes para la computación forense.	1.2;8.2
Técnicas informáticas de procesamiento forense.	1.2
Informes forenses.	1.2

Tabla A.1: Análisis del Diplomado en Ciberseguridad de la PUCV
Fuente: Elaboración propia

	KU
CURSO 1: Seminario de preparación para la certificación internacional CISSP: Parte I	
Introducción al Seminar review	X
The Information Security Environment	X
Information Asset Security	6.1
Identity and Access Management	6.1;1.4;5.3
Security Architecture and Engineering	5.1;1.4;3.1
CURSO 2: Seminario de preparación para la certificación internacional CISSP: Parte II	
Communication and Network Security	4.8;1.5
Software Development Security	2.1;2.2;2.3;2.4;2.5;2.6
Security Assessment and Testing	2.4;3.3;5.6
Security Operations	5.4;7.3;7.6;7.9
Putting It All Together	X
CISSP Certification Information	X
CURSO 3: Planificación y monitoreo continuo de la ciberseguridad	
¿Dónde nos estamos moviendo?	X
Quien está detrás del Cibercriminal	8.1
El Juego Infinito	5.4;7.5;7.6;8.1
Negocio – Cultura	X
Modelo y Marco NIST CSF / GDPR	1.7;2.7;6.5;6.6;6.7;7.2;7.5;7.8;8.2;8.5
Mitre ATT&CK	4.8;5.4;7.3;5.6;2.4
Modelo y Marco CIS Taller CIS Material CIS: Version 8	4.8;1.3;2.1;5.4;7.3;1.4;5.3;3.2;7.8;7.4;2.4;6.2;6.1;7.6;6.4;2.6;2.3;2.2
Modelo y Marco CIS Taller CIS Material CIS: Comunity Defense Model	-1
Modelo y Marco CIS Taller CIS Material CIS: Informe DBIR	6.4;6.2;8.1;8.2;7.2
Taller “Controles CIS”	4.8;1.3;2.1;5.4;7.3;1.4;5.3;3.2;7.8;7.4;2.4;6.2;6.1;7.6;6.4;2.6;2.3;2.2
Seguridad Modelo tradicional	1.4;4.8;5.3;
Servicios dentro de un SOC	5.4;7.3;7.6;7.9
Modelo SOC	5.4;7.3;7.6;7.9
Ciclo de Vida Respuesta Incidentes	1.2;5.4;7.6
NIST/SANS y FIRST CSIRT	7.1;7.2;7.3;7.4;7.6
Seguridad Cloud: Ciberseguridad Hibrida	4.8;7.4
Seguridad Cloud: Ruta de una organización	X
OWASP10	2.1;2.2;2.3;2.4
Análisis de Ransomware	5.4;7.6;8.1
Sase	7.4;4.8
Taller “Hardening de Sistemas”	4.8;7.4
CURSO 4: Técnicas y herramientas de ciberseguridad avanzada: Parte I	
Vectores de ataque	1.6;5.4;8.1
Conceptos básicos de hacking ético y pentesting	5.4;8.3
Metodologías de hacking ético y pentesting	2.4;4.8;5.4;7.3
Evaluación de vulnerabilidades	2.4;5.4;7.4
Uso de herramientas en diversas fases de un ataque (reconocimiento, escaneo, obtención y mantención de acceso y eliminación de huellas).	4.8;5.4
Ejercicios simulados de un hacking ético	5.4
Desarrollo de reportes para la mitigación de vulnerabilidades	1.2;2.5;5.6;7.2
CURSO 5: Técnicas y herramientas de ciberseguridad avanzada: Parte II	
Threat Intelligence	7.1;7.2;
Threat Hunting	4.8;5.4;7.3
Framework Mitre	4.8;5.4;7.3;5.6;2.4
OSINT	-1
SOCMINT	8.2;1.7;6.5;
Análisis de Malware	3.4;5.4
Ingeniería Reversa.	3.1;3.4
Detección Avanzada y análisis de intrusiones en la red	4.8;5.4;7.3
CURSO 6: Técnicas y herramientas de ciberseguridad avanzada: Parte III	
Uso de ATT&CK Framework, Parte I (Adversary Emulation)	4.8;5.4;7.3;5.6;2.4
Uso de ATT&CK Framework, Parte II (SOC Assessment)	5.4;7.3;7.6
Respuesta a incidentes	1.2;7.6
Análisis de Malware	2.4;5.6;3.4;5.4
Ingeniería Reversa	3.1;3.4
Uso y configuración de Yara Rules	2.4;5.4;
Automatización de fuentes de información	4.8;5.2;7.3
CURSO 7: Taller Convergencia IT/OT	
Revisión de arquitecturas y estándares de seguridad y ciberseguridad tanto para IT/OT	5.4;4.8;3.1;7.4;5.7;7.2
Revisión de convergencia IT-OT	7.9
Aplicabilidad de isa/iec 6244	7.5;7.2;7.7
Herramientas tecnológicas para ciberseguridad OT	5.4;4.8;3.1;7.4;5.7

Tabla A.2: Análisis del Diplomado en Gestión Técnica de Ciberseguridad de la PUC
Fuente: Elaboración propia

	KU
Módulo I	
Aspectos estratégicos de la ciberseguridad	7.1;7.2;7.5;7.7
Módulo II	
Aspectos legales de la ciberseguridad	8.2;7.2;1.8
Módulo III	
Alineamiento estratégico y plan director de ciberseguridad	7.2;7.5;7.7
Módulo IV	
Gestión integral de riesgos y controles	7.1;7.2;7.5;7.7
Módulo V	
Implementación y gestión de un programa de seguridad de la información	1.8
Módulo VI	
Implementación y gestión de un sistema de Cyber Defense	5.2;7.3;7.6;7.9
Módulo VII	
Respuesta ante incidentes y recuperación ante crisis	1.2;7.6
Módulo VIII	
Gestión ágil y desarrollo seguro de software	2.5;2.3;2.1;2.2;2.6;2.4
Módulo IX	
Criptografía y Blockchain	1.1;1.3;1.6
Módulo X	
Privacidad de datos en la era digital	6.4;8.5;1.7;7.2;6.7;6.6;8.2;1.5;6.5
Módulo XI	
Seguridad de redes de datos	4.4;4.6;4.7;4.8
Módulo XII	
Seguridad de sistemas operativos y bases de datos	1.8;7.4
Módulo XIII	
Seguridad de aplicaciones web y aplicaciones móviles	1.2;4.4;5.7
Módulo XIV	
Seguridad de Cloud computing e Internet de las cosas (IoT)	4.4;5.7;7.4
Módulo XV	
Taller de Hacking ético	5.4;8.3

Tabla A.3: Análisis del Magíster en Ciberseguridad de la UAI
Fuente: Elaboración propia

	KU
Módulo I : Fundamentos de Ciberseguridad	
Definición de la ciberseguridad y del ciberespacio.	X
La ciberseguridad en el ámbito de una empresa u organización.	7.1;7.8;7.2;7.5;7.7;7.9
Gestión de recursos humanos y de los comportamientos.	6.2;6.3;6.4;7.8
Bases de seguridad de datos: Nociones básicas de criptografía aplicada	1.1
Bases de seguridad de datos: Algoritmos de cifrado simétricos y asimétricos	1.1
Bases de seguridad de datos: Funciones de Hash seguras	1.2;1.3
Bases de seguridad de datos: Distribución de claves	1.1;1.5
Módulo II : Aspectos Legales y Organizaciones de la Ciberseguridad	
Uso de las tecnologías en el trabajo	X
Delitos informáticos	8.1;8.2
Protección de datos, contratos y propiedad intelectual	6.2;7.2;7.5;8.2;1.8
Módulo III : Análisis de Riesgos y Generación de Políticas de Ciberseguridad	7.1;7.2;7.5
Módulo IV : Administración y configuración de Infraestructura	
Seguridad de los Sistemas Operativos: Instalación y configuración segura de sistemas operativos	7.4
Seguridad de los Sistemas Operativos: Sistemas de archivos seguros	1.8;7.4
Seguridad de los Sistemas Operativos: Instalación de herramientas de seguridad	7.4
Seguridad de los Sistemas Operativos: Seguridad en Máquinas Virtuales y Contenedores	4.5;4.7;5.7
Seguridad de los Sistemas Operativos: Sistemas de Respaldo de datos.	1.8;7.4;7.6
Seguridad de los Sistemas Operativos: Antivirus, Anti-Malware, etc.	4.8;5.4
Seguridad de los Equipos de Redes: Instalación y configuración de Firewalls	4.8
Seguridad de los Equipos de Redes: IDS (Intrusion Detection System)	4.8;7.4
Seguridad de los Equipos de Redes: IPS (Intrusion Prevention System)	4.8;7.4
Seguridad de los Equipos de Redes: Cifrado de la red y Monitoreo	1.5;4.8;7.3
Seguridad Física: Control de acceso	1.4;5.3
Seguridad Física: Control de incendios	-1
Seguridad Física: Respaldo de energía	-1
Módulo V : Programación Segura	
Amenazas actuales al software: ¿Quiénes son los atacantes?	8.1
Amenazas actuales al software: Vulnerabilidades de software correspondientes a cada etapa del SDLC: Inyecciones, XSS, configuraciones inseguras, autentificación débil, etc.	2.1;2.2;2.3;2.4;2.5
Programación segura: Necesaria pero difícil: ¿Cuáles son las consecuencias de un ataque exitoso a software?	5.4;7.6
Programación segura: Necesaria pero difícil: ¿Por qué es difícil programar en forma segura?	2.1;2.3;6.7
Cómo asegurar software: Buenas prácticas de programación segura	2.1;2.3
Cómo asegurar software: Herramientas de desarrollo seguro	2.4
Cómo asegurar software: Taller/demostración de programación segura	2.1;2.2;2.3;2.4;2.5
Módulo VI : Penetration Testing & Ethical Hacking	
Introducción: Conceptos básicos del Hacking Ético	5.4;8.3
Técnicas y herramientas de reconocimiento	2.4;4.8;5.4;7.3
Uso de herramientas de escaneo y enumeración de servicios	2.4;4.8;5.4;7.3
Análisis de vulnerabilidades	2.4;4.4;4.6;4.7;5.4
Explotación de vulnerabilidades	4.4;4.6;4.7;4.8
Módulo VII : Respuesta a Incidentes	
Explicación y uso de herramientas de respuesta de incidentes	1.2;7.6
Procesos de KillChain	7.6;7.3
Mitre ATT&CK	4.8;5.4;7.3;5.6;2.4
Módulo VIII : Análisis Forense	
Concepto de Evidencia Digital y aspectos legales relacionados.	1.2;8.2
Gestión de Evidencia Digital	1.2
Cadena de Custodia y preservación de evidencia digital	1.2;8.2
Etapas de Informática Forense: Identificación, Recopilación, Adquisición, Examen, Análisis y Presentación.	1.2
Laboratorio de Adquisición de Evidencia Digital.	1.2
Laboratorio de Examen y Análisis de Evidencia Digital.	1.2
Módulo IX: Seminarios sobre Ciberseguridad	
Presentación de casos	X
Procedimientos en casos de ataques y respuestas	7.6
Fuentes y origen de los ataques.Trabajo Personal	X
Módulo X: Análisis de casos sobre Ciberseguridad	
Incluye discusiones y trabajo personal de análisis para la producción de un informe final.	X

Tabla A.4: Análisis del Diploma en Ciberseguridad de la USM
Fuente: Elaboración propia

	KU
1er Semestre	
Taller de Networking	4.1;4.2;4.3;4.4;4.5;4.6
Taller de Cableado y Datacenter	4.1;4.2;4.3
Matematica para la Educacion Superior	0
Herramientas para la Empleabilidad	0
Habilidades para la Comunicacion	0
Taller Aplicado para Ciberseguridad	X
2do Semestre	
Seguridad de Cableado y Datacenter	4.1;4.2;4.3
Seguridad en Networking	4.8
Taller aplicado de seguridad de la informacion	1.1;1.3;1.4;1.8
Herramientas para la innovacion	0
Gestion y soporte de seguridad en hardware y software	2.5;5.2;7.4
Herramientas de inteligencia artificial	0
3er Semestre	
Taller de sistemas operativos	7.4
Taller de plataformas web	0
Ingles inicial I	0
Sostenibilidad organizacional	0
Redes inalambricas	4.1
Certificado de especialidad I	X
4to Semestre	
Seguridad con herramientas opensource	3.2;3.3
Seguridad para plataforma web	1.2;2.3;4.7
Ingles inicial II	0
Certificado de especialidad II	X
Taller de Proyecto de Especialidad	X
Taller de Marca Personal	0
5to Semestre	
Gestion de Riesgos en Seguridad TI	7.1
Ingenieria de Requisitos de Seguridad	2.2;5.6;5.1
IA para la Gestion Profesional	0
Taller de Hacking Etico	5.4;8.3
Gestion de Incidentes de Seguridad	7.6;1.2
Ingles Pre Intermedio I	0
6to Semestre	
Procesos de Continuidad de Negocios	7.6
Arquitectura de Redes	4.4;4.5;7.4
Legislacion informatica	8.2;7.2;1.8
Gestion de Servicios de TI	7.4
Ingles Pre Intermedio II	0
Certificado de Especialidad III	X
7mo Semestre	
Taller de analisis forense digital	1.2
Seguridad de Arquitectura de Redes	4.8
Ingles de Especialidad	0
Taller de Monitoreo de Redes	4.8;7.3
Certificado de Especialidad IV	X
Gestion de Proyectos de Ciberseguridad	7.7
8vo Semestres	
Taller de Amenazas Ciberneticas	5.4;4.4;4.6;4.7;4.8
Organizacion y Gobernabilidad en TI	7.2
Evaluacion de Seguridad en Compra de Servicios TI	7.5;3.2
Proyecto de Especialidad Profesional	X
Coaching laboral	0

Tabla A.5: Análisis de la carrera de Ingeniería en Ciberseguridad del AIEP
Fuente: Elaboración propia

	KU
Ciclo I	
Fundamentos de Hardware y Software	0
Transversal I: Habilidades para el Aprendizaje	0
Ciclo II	
Introducción a la Programación	0
Matemática y Lógica	0
Ciclo III	
Programación	0
Transversal II: Herramientas para la Comunicación Social	0
Ciclo IV	
Introducción a la Ciberseguridad	1.1;1.4;5.1
Redes Inalámbricas	4.1
Ciclo V	
Ciberseguridad	X
Seguridad con Herramientas Opensource	3.2;3.3
Ciclo VI	
Marco Legal	1.8;.2.7;7.2;8.2
Criptografía y Gestión de Certificados	1.1;1.5
Ciclo VII	
Redes	4.1;4.2;4.3;4.4;4.5;4.7
Gestión de la Seguridad y de Incidentes	1.2;7.6;7.5;7.1;7.9
Ciclo VIII	
Hacking Ético	5.4;8.3
Tecnologías y Componentes Computacionales	X
Ciclo IX	
Hardening	7.4;4.8
Análisis Forense Digital	1.2;8.2
Ciclo X	
Transversal III: Ética	0
Taller de Integración en Seguridad de Datos	1.3;1.8;1.5
Ciclo XI	
IOT	5.7;7.4
CyberOps	5.4;7.3;7.6;7.9
Ciclo XII	
Seguridad IOT	5.7;7.4
Administración de Sistemas Operativos de Red	7.4;1.4;5.3
Ciclo XIII	
Plataformas Web	4.7
Seguridad en Sistemas Operativos de Red	7.4;4.8;1.4;5.3
Ciclo XIV	
Seguridad para Plataformas Web	1.5;2.3
Seguridad de la Red	4.8
Ciclo XV	
Seguridad Cloud	4.8;7.4
Gestión de Incidentes de Seguridad	7.6;1.2
Ciclo XVI	
Gestión de Redes	4.5;4.7;4.8
Hardening e Identidad Digital	6.1;7.4;4.8
Ciclo XVII	
Continuidad de Negocios	7.6
Liderazgo y Gestión de Proyectos	0
Ciclo XVIII	
Organización y Gobernabilidad en TI	7.2
Metodologías para la Gestión de Proyectos	0
Ciclo XIX	
Innovación en Proyectos Tecnológicos	0
Taller de Amenazas Cibernéticas	5.1;5.4
Ciclo XX	
Emprendimiento Tecnológico	0
Taller Integrado de Proyectos en Ciberseguridad	X

Tabla A.6: Análisis de la carrera de Ingeniería en Ciberseguridad del IACC
Fuente: Elaboración propia

	KU
Semestre 1	
Introducción a la Programación Segura	0
Fundamentos de Base de Datos	0
Fundamentos de Hardware y Software	0
Resolución de Problemas en Álgebra	0
Formación Ciudadana	0
Semestre 2	
Metodología de Desarrollo Ágil	2.2
Programación Orientada a Objeto Seguro	0
Bases de Datos Estructuradas	0
Modelamiento de Soluciones Informáticas	0
Funciones y Matrices	0
Administración	0
Semestre 3	
Sistemas Operativos	7.4
Bases de Datos No Estructuradas	0
Programación Front End	0
Fundamentos de Seguridad de la Información	1.1;1.4;5.1
Electivo de Tendencias del Sector Productivo y de Servicios I	0
Innovación y Emprendimiento I	0
Semestre 4	
Ingeniería de Software	2.2
Aplicaciones Móviles para IoT	0
Programación Back End	0
Electivo de Tendencias del Sector Productivo y de Servicios II	0
Inglés Inicial	0
Proyecto Integrado	X
Semestre 5	
Arquitectura On-Premise y On-Cloud	4.4;7.4
Gestión de la Ciberseguridad	7.5;7.1;7.9
Redes de Datos	4.1;4.2;4.3;4.4;4.5;4.7
Cálculo Diferencial	0
Gestión de Personas	7.8
Innovación y Emprendimiento II	0
Semestre 6	
Diseño de Arquitecturas de Seguridad TI	7.1;7.2;7.5;7.7;7.9
Seguridad en Redes	4.4;4.6;4.7;4.8
Seguridad IoT	5.7;7.4
Desarrollo Seguro	2.2;2.3;2.4;2.5
Finanzas	0
Inglés Habilitante	0
Semestre 7	
Hacking Ético	5.4;8.3
Análisis Forense	1.2;8.2
Auditoria IT/OT	5.7;7.4
Legislación	8.2;7.2;1.8
Formulación y Gestión de Proyectos	0
Inglés Intermedio	0
Semestre 8	
Gestión de Proyectos de Ciberseguridad	7.7
Gobierno de Seguridad de la Información	7.2
Electivo de Tendencias del Sector Productivo y de Servicios III	0
Electivo de Tendencias del Sector Productivo y de Servicios IV	0
Innovación y Emprendimiento III	0
Proyecto de Título	0

Tabla A.7: Análisis de la carrera de Ingeniería en Ciberseguridad del INACAP
Fuente: Elaboración propia

	KU
Trimestre 1	
Programación para ciberseguridad	2.1;2.2;2.3
Factores humanos y ciberseguridad	6.2;6.3;6.4;6.7
Redes y administración de sistemas operativos	7.4;4.4;4.5
Álgebra	0
Trimestre 2	
Fundamentos de seguridad de la información	1.1;1.4;5.1
Taller bootcamp en ciberseguridad	X
Criptografía	1.1;1.6
Cálculo	0
Trimestre 3	
Hardening y seguridad en sistemas operativos	7.4;5.4
Gobierno y gestión de la ciberseguridad	7.2;7.5
Seguridad en base de datos	1.8;7.4
Certificación 1	X
Trimestre 4	
Hacking ético	5.4;8.3
Legislación y normativas de seguridad	7.2;8.2
Estadística	0
Certificación 2	X
Trimestre 5	
DevSecOps	2.5;7.4
Seguridad en redes y comunicaciones	4.8;1.5
Red team: técnicas ofensivas	1.6;5.4;3.4;4.8
Ciberseguridad en tecnologías emergentes	X
Trimestre 6	
Blue team: técnicas defensivas	4.8;5.4;7.6;7.3
Análisis de malware	3.4;5.4
Gestión de incidentes	1.2;7.6
Certificación 3	X
Trimestre 7	
Pentesting (móvil & web)	4.7;1.2;5.4
Teoría forense	1.2;8.2
Seguridad en ambientes cloud	4.4;4.8;7.4
Proyecto de ingeniería	0
Trimestre 8	
Proyecto de título I	0
Taller de implementación de herramientas para ciberseguridad	X
Trimestre 9	
Proyecto de título II	0
Threat hunting	4.8;7.3;5.4

Tabla A.8: Análisis de la carrera de Ingeniería en Ciberseguridad de la UMAYOR
Fuente: Elaboración propia

Anexo B: Asignaturas basadas en importancia

Introducción a la Ciberseguridad

Tema 1: Introducción a la Ciberseguridad

1. Concepto y alcance de la ciberseguridad
   - Definiciones fundamentales y terminología básica.
   - Principios de la ciberseguridad: confidencialidad, integridad, disponibilidad, autenticidad y no repudio.
   - Diferencias entre seguridad informática, seguridad de la información y ciberseguridad.
2. Naturaleza interdisciplinaria de la ciberseguridad
   - Relación con las ciencias de la computación, la ingeniería y las matemáticas.
   - Conexiones con disciplinas sociales y jurídicas: derecho, ética, psicología y sociología.
   - Importancia del enfoque sistémico y humano en la protección digital.
3. Impacto económico y social de la ciberseguridad
   `Topics: (8.1.4)`
   - Sectores productivos afectados por amenazas y vulnerabilidades.
   - Costos económicos y reputacionales de los incidentes de seguridad.
   - Rol estratégico de la ciberseguridad en la economía digital y en la sociedad moderna.

Tema 2: Hacking Ético

1. Conceptos fundamentales del hacking
   - Definición y evolución del término hacking.
   - Diferencias entre hacking y cracking.
   - Cultura hacker y su contribución al desarrollo tecnológico.
2. Clasificación de los hackers y sus motivaciones
   `Topics: (8.1.1, 8.1.2, 8.1.4, 8.3.6)`

- White hat hackers: propósitos éticos y aplicaciones legítimas (bug hunting, auditorías de seguridad).
- Grey hat y black hat hackers: actividades ilícitas y zonas grises.
- Cibercriminalidad y sus manifestaciones: cibercrimen, ciberterrorismo, ciberactivismo y uso de criptomonedas en el ámbito delictivo.

3. Principios del hacking ético
   `Topics: (8.3.2, 8.3.7, 8.3.8)`

   - Concepto de ethical hacking y su marco ético-legal.
   - Responsabilidad profesional y límites de la actuación ética.
   - Importancia del consentimiento, la autorización y la divulgación responsable de vulnerabilidades.

4. Penetration Testing
   `Topics: (5.4.9)`

   - Objetivos y alcance del penetration testing.
   - Fases del proceso de prueba de penetración:
     a) Planificación y reconocimiento (Planning and Reconnaissance)
     b) Escaneo y mapeo de objetivos (Scanning)
     c) Obtención de acceso (Gaining Access)
     d) Mantenimiento de acceso (Maintaining Access)
     e) Análisis y reporte de resultados (Analysis and Reporting)
   - Herramientas y metodologías utilizadas en pruebas de penetración.

Tema 3: Social Engineering y Ciberhigiene

1. Ingeniería Social
   `Topics: (6.2.1, 6.2.2, 6.2.3, 6.2.4, 6.4.1)`

   - Concepto y fundamentos de la ingeniería social.
   - Factores psicológicos y conductuales explotados por los atacantes.
   - Tipos de ataques de ingeniería social:
   - Detección y mitigación de ataques de ingeniería social.

2. Ciberhigiene
   `Topics: (6.4.2, 6.4.4)`

   - Definición de ciberhigiene y su rol en la seguridad digital.
   - Buenas prácticas y hábitos seguros en el uso de tecnologías.

- Mantenimiento preventivo de la seguridad personal y organizacional.
- Herramientas de apoyo a la ciberhigiene.

Tema 4: Privacidad

1. Concepto y fundamentos de la privacidad
   `Topics: (8.5.1)`
   - Definición de privacidad: distinción entre confidencialidad, anonimato y privacidad.
   - Trade-offs: balance entre privacidad, seguridad y usabilidad.
   - Modelos de privacidad (contextual integrity, privacy by design, privacy as control).
2. Privacidad como derecho universal
   `Topics: (6.7.4, 8.2.9, 8.5.2)`
   - La privacidad en marcos legales internacionales.
   - Recolección y uso de datos desde la perspectiva del usuario.
   - Políticas de privacidad, consentimiento informado y "dark patterns".
3. Privacidad en sociedades modernas
   `Topics: (6.5.2, 8.5.7)`
   - Impacto de la vigilancia masiva, publicidad dirigida y redes sociales.
   - Relación entre privacidad, democracia y poder.
   - Privacidad colectiva vs. individual.
4. Qué se busca proteger
   `Topics: (6.6.1, 6.6.2)`
   - Tipos de datos personales: PII (Personally Identifiable Information), SPD (Sensitive Personal Data).
   - Huella digital y seguimiento personal.
   - Rastreo en línea: cookies, fingerprinting, geolocalización, redes sociales.
   - Concepto de "digital footprint" y prácticas de autogestión de identidad digital.
5. Cómo proteger la privacidad
   `Topics: (8.5.3)`
   - Buenas prácticas del usuario: configuración de privacidad, contraseñas, uso consciente de aplicaciones y permisos.

- Privacidad operacional (OPSEC) a nivel individual.
- Uso de tecnologías de preservación de privacidad (Privacy Enhancing Technologies, PETs)

Administración de Sistemas

Tema 1: Sistemas y Seguridad

1. Conceptos fundamentales de sistemas
   `Topics: (5.1.2, 5.1.3, 5.5.1)`
   - Definición y componentes de un sistema.
   - Principios de diseño y visión holística en la construcción de sistemas.
   - Procesos de desarrollo y enfoques de modelado sistémico.
   - Interacción entre subsistemas y dependencias funcionales.
2. Arquitecturas y tipos de sistemas
   `Topics: (5.7.1, 5.7.5, 5.7.6, 5.7.7)`
   - Sistemas de propósito general (*general-purpose systems*).
   - Máquinas virtuales y entornos de virtualización.
   - Sistemas móviles y distribuidos.
   - Sistemas autónomos e inteligentes.
3. Vulnerabilidades en sistemas
   `Topics: (5.1.4, 5.1.5, 5.1.6)`
   - Modelos de amenazas y evaluación de riesgos en sistemas computacionales.
   - Relación entre arquitectura del sistema y vulnerabilidades de seguridad.
   - Ejemplos comparativos entre sistemas de propósito general y especializado.

Tema 2: Administración de Sistemas

1. Ciclo de vida del sistema
   `Topics: (2.5.5, 5.2.5, 5.2.6, 5.2.8, 5.2.9, 5.5.1)`
   - Instalación y puesta en marcha de sistemas.
   - Documentación técnica y operativa de sistemas.
   - Operación y monitoreo de sistemas en producción.

- Gestión y administración durante el ciclo de vida del sistema.
- Retiro, desmantelamiento y *decommissioning* de sistemas.

2. Administración general de sistemas
   `Topics: (1.8.4, 5.4.11, 7.3.1, 7.4.1, 7.4.2, 7.4.3, 7.4.4, 7.4.7, 7.6.3)`

   - Principios de gestión y configuración de sistemas operativos.
   - Administración de bases de datos y su integración en entornos productivos.
   - Gestión de redes de computadores y su infraestructura asociada.
   - Administración de entornos en la nube y servicios cloud.
   - Evaluación del desempeño mediante métricas de rendimiento.
   - Continuidad operacional, alta disponibilidad y planes de continuidad de negocio.

3. Protección y seguridad de sistemas
   `Topics: (5.2.4, 5.4.3, 5.4.4, 5.4.5, 5.4.6, 5.4.7, 5.4.8, 7.3.2, 7.4.6, 7.6.1, 7.6.2)`

   - Modelos de vulnerabilidades.
   - Tipología de ataques y clasificación de malware.
   - Detección de intrusiones mediante técnicas de monitoreo y supervisión.
   - Auditorías de seguridad y análisis de datos para la identificación de anomalías.
   - Respuesta ante incidentes y estrategias de defensa de sistemas.
   - Recuperación ante desastres y planes de contingencia.
   - Gestión de parches y ciclo de vida de vulnerabilidades.
   - Endurecimiento de sistemas y aplicación de buenas prácticas de seguridad (*hardening*).

Tema 3: La organización como sistema

1. La organización como sistema
   `Topics: (7.2.1)`

   - Definición de organización desde una perspectiva sistémica.
   - Análisis de la variabilidad organizacional según su contexto y entorno operativo.

2. Planificación de la seguridad organizacional
   `Topics: (5.2.1, 5.2.2, 7.2.4, 7.2.5, 7.2.6, 7.5.1, 7.7.1, 7.7.2, 7.7.3, 7.7.4)`

- Ciclo de vida de las políticas de seguridad de la información.
- Modelos y enfoques para la formulación de políticas de seguridad.
- Estructura y composición de políticas organizacionales de seguridad.
- Estrategias para la comunicación y difusión de políticas hacia directivos y responsables.
- La seguridad como proyecto y como gestionarlo.
- Cómo validar el proyecto de seguridad.

3. Gestión del riesgo en la organización
   `Topics: (7.1.1, 7.1.2, 7.1.4, 7.1.5)`

   - Identificación, análisis y evaluación de riesgos.
   - Modelos y metodologías de gestión de riesgos.
   - Estrategias de mitigación y tratamiento del riesgo.
   - Seguimiento y control de riesgos residuales.

4. Gestión segura del recurso humano
   `Topics: (1.4.4, 5.2.7, 6.7.3, 7.1.3, 7.8.1, 7.8.2, 7.8.3, 7.8.5)`

   - Procesos de adquisición de personal y prevención de amenazas internas (*insider threats*).
   - Formación y concientización en seguridad de la información (*security awareness*).
   - Prevención de fuga de información (*Data Leak Prevention*).
   - Evaluación y verificación permanente del cumplimiento de prácticas seguras.
   - Terminación segura de la relación laboral y revocación de accesos y activos.

Software Seguro

Tema 1: Fundamentos del Software Seguro

1. Principios conceptuales del diseño seguro
   `Topics: (2.1.1, 2.1.5, 2.1.8, 2.1.9)`

   - Principio de mínimo privilegio (*Least Privilege*).
   - Minimización de confianza implícita (*Minimize Trust*).
   - Diseño abierto como principio de transparencia (*Open Design*).
   - Principio de mínima sorpresa (*Least Astonishment*).

2. Principios estructurales y arquitectónicos
   `Topics: (2.1.4, 2.1.6, 2.1.7, 2.1.10, 2.1.11, 2.1.12)`
   - Separación de responsabilidades y privilegios (*Separation*).
   - Diseño en capas como mecanismo de contención (*Layering*).
   - Modularidad aplicada a la seguridad (*Modularity*).
   - Abstracción como mecanismo de protección de detalles críticos.
   - Economía de mecanismos de seguridad (*Economy of Mechanism*).
   - Minimización de mecanismos compartidos (*Minimize Common Mechanism*).
3. Principios de control, validación y verificación
   `Topics: (2.1.2, 2.1.3, 2.1.13)`
   - Mediación completa de accesos (*Complete Mediation*).
   - Enlace completo de dependencias y relaciones (*Complete Linkage*).
   - Valores por defecto seguros (*Fail-safe Defaults*).

Tema 2: Aseguramiento del Ciclo de Vida del Software

1. Diseño e implementación segura
   `Topics: (2.2.1, 2.2.2, 2.2.4, 2.3.1, 2.3.2, 2.3.3, 2.3.4, 2.3.5, 2.3.6, 2.3.7, 2.3.8, 2.7.2, 6.7.5)`
   - Definición y especificación de requerimientos de seguridad.
   - Consideraciones de seguridad en lenguajes de programación.
   - Prácticas seguras de implementación:
     - Validación de entradas y verificación de su representación.
     - Uso correcto de APIs.
     - Uso adecuado de funcionalidades de seguridad.
     - Control de relaciones de tiempo y estado.
     - Manejo seguro de excepciones y errores.
     - Programación robusta.
     - Encapsulamiento de estructuras y módulos.
     - Consideración del entorno de ejecución.
     - Configuración de valores por defecto seguros.
   - Aspectos de seguridad durante el desarrollo.
2. Despliegue y mantenimiento seguro del software
   `Topics: (2.5.1, 2.5.2, 2.5.3, 2.5.4)`

- Configuración segura de sistemas y aplicaciones.
- Gestión de parches y ciclo de vida de vulnerabilidades en software.
- Verificación del entorno de operación.
- Integración de prácticas DevOps con consideraciones de seguridad.

Tema 3: Testing y Evaluación de Seguridad en Software

1. Enfoques generales de análisis y evaluación
   `Topics: (2.4.1)`
   - Análisis estático y dinámico del software.
2. Testing funcional del software
   `Topics: (2.4.2, 2.4.3, 2.4.4, 3.3.1)`
   - Pruebas unitarias (*Unit Testing*).
   - Pruebas de integración (*Integration Testing*).
   - Pruebas generales de software (*Software Testing*).
3. Testing orientado a la seguridad
   `Topics: (3.3.2)`
   - Pruebas de seguridad del software (*Security Testing*).

Tema 4: *Reverse Engineering*

1. Fundamentos del *Reverse Engineering*
   - Definición y alcance del proceso de ingeniería inversa.
   - Contextos de aplicación: usos defensivos y ofensivos.
2. Técnicas y herramientas para ingeniería inversa
   `Topics: (3.4.1, 3.4.3)`
   - Metodologías y técnicas de análisis de software.
   - Herramientas empleadas en procesos de *reverse engineering*.
3. Mecanismos de *anti-reverse engineering*
   `Topics: (3.1.4)`
   - Técnicas de protección y ofuscación contra análisis inverso.
   - Estrategias de detección y mitigación de ingeniería inversa.

Seguridad de Datos y Redes

Tema 1: Criptografía y Criptoanálisis

1. Fundamentos, clasificación y evolución de los sistemas criptográficos
   `Topics: (1.1.1, 1.1.1, 1.1.4, 1.1.5, 1.1.6 1.6.3, 1.6.4, 1.6.6)`
   - Definición de criptografía y conceptos fundamentales.
   - Origen y evolución histórica de la criptografía: cifrados clásicos.
   - Criptografía moderna: visión general conceptual.
   - Mecanismos de cifrado: implementación en software versus hardware.
   - Fundamentos matemáticos aplicados a la criptografía.
   - Sistemas criptográficos simétricos y asimétricos.
2. Conceptos criptográficos avanzados:
   `Topics: (1.1.2)`
   - Pruebas y protocolos de conocimiento cero (*Zero-knowledge proofs*).
   - Esquemas de compartición de secretos (*Secret sharing*).
   - Compromisos criptográficos.
   - Transferencia inconsciente (*Oblivious transfer*).
   - Computación segura multiparte (*Secure multi-party computation*).
3. Limitaciones inherentes y ataques contra los criptosistemas
   `Topics: (1.6.1, 1.6.3, 1.6.4, 1.6.5, 1.6.6)`
4. Desarrollos recientes y tendencias avanzadas: cifrado homomórfico, ofuscación, criptografía cuántica y esquema KLJN
   `Topics: (1.1.2)`

Tema 2: Autenticación y Comunicacion Segura

1. Mecanismos de autenticación y gestión de credenciales
   `Topics: (1.3.1, 1.3.3)`
   - Modelos de autenticación: multifactor, tokens criptográficos, dispositivos criptográficos y biometría.
   - Técnicas de protección de credenciales: *hashing*, *salting* y *password-based key derivation*.

2. Amenazas y validación en procesos de autenticación
   `Topics: (1.3.2, 1.3.4)`
   - Ataques contra mecanismos de autenticación basados en contraseñas.
   - Relación entre la autenticación del emisor y la verificación de la integridad de los datos en sistemas seguros.

3. Control de acceso
   `Topics: (5.3.1, 5.3.2, 6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5)`
   - Métodos de autenticación y gestión de identidad.
   - Control de acceso físico y lógico en entornos computacionales.
   - Identificación y validación de personal y dispositivos.
   - Servicios de identidad externalizados (*Identity as a Service*) y soluciones de terceros.
   - Ataques y vulnerabilidades asociados a los mecanismos de control de acceso.

4. Protocolos de comunicación segura
   `Topics: (1.5.1, 1.5.2, 1.5.3, 1.5.4, 1.5.5)`
   - Protocolos seguros en las capas de aplicación y transporte para la protección de las comunicaciones.
   - Principales ataques y debilidades asociados a TLS y canales cifrados.
   - Mecanismos de seguridad en la capa de red y su relevancia en la transmisión de datos.
   - Protocolos orientados a la preservación de la privacidad en entornos de comunicación.
   - Seguridad en la capa de enlace y su relación con ataques de proximidad.

Tema 3: Reforzamiento de Redes de Computadores

1. Fundamentos físicos y arquitectura de las redes
   `Topics: (4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.2.3, 4.3.1, 4.3.2, 4.3.3)`
   - Medios físicos de transmisión y sus características de comunicación.
   - Interfaces, conectores y arquitectura de hardware de red.
   - Análisis general de vulnerabilidades asociadas al hardware y a las interfaces físicas.

2. Modelos de comunicación y sistemas en red
   `Topics: (4.1.3, 4.1.4, 4.4.1, 4.4.2, 4.4.3, 4.4.4)`

- Modelos de compartición de recursos y mecanismos de acceso.
- Procesos y comunicación entre ellos.
- Introducción a sistemas distribuidos y sus principios generales.
- Arquitectura por capas y organización de protocolos.

3. Virtualización y tendencias emergentes en redes
   `Topics: (4.5.6, 4.5.7)`

   - Virtualización de infraestructura y abstracción de recursos de red.
   - Nuevos paradigmas y tecnologías emergentes, con énfasis en *Software Defined Networking* (SDN).

Tema 4: Seguridad en Redes

1. Ataques en redes de computadores
   `Topics: (4.4.7, 4.6.2, 4.6.3, 4.6.4, 4.7.1, 4.7.2, 4.7.3, 4.7.4, 4.7.5, 4.7.6, 4.8.13)`

   - Análisis de implementaciones de redes y su superficie de exposición.
   - Protocolos de integración práctica y protocolos de enlace (ej.: ARP) y su relevancia en escenarios de ataque.
   - Origen de vulnerabilidades en las implementaciones de red, considerando diferentes capas del modelo de comunicación.
   - Modelos de servicios de red y generación de vulnerabilidades asociadas a su diseño y operación.
   - Tipología y caracterización general de ataques en redes.

2. Mecanismos de defensa y protección en infraestructuras de red
   `Topics: (4.8.1, 4.8.2, 4.8.3, 4.8.5, 4.8.6, 4.8.7, 4.8.8, 4.8.10)`

   - Estrategias de endurecimiento de red (network hardening) y reducción de superficie de exposición.
   - Sistemas de detección y prevención de intrusiones (IDS/IPS), *firewalls* y redes privadas virtuales (VPN).
   - Monitoreo y análisis de tráfico de red.
   - Implementación de entornos de contención: *honeypots*, *honeynets* y zonas desmilitarizadas (DMZ).

Anexo C: Frecuencia de KUs en O*NET *Crosswalk*

KU	**Frecuencia**
1.1 Cryptography	23
1.3 Data Integrity and Authentication	23
2.1 Fundamental Principles	23
2.2 Design	23
3.1 Component Design	23
4.5 Network Architecture	23
4.7 Network Services	23
4.8 Network Defense	23
5.1 System Thinking	23
5.2 System Management	23
7.1 Risk Management	23
7.2 Security Governance & Policy	23
7.3 Analytical Tools	23
7.4 Systems Administration	23
7.5 Cybersecurity Planning	23
7.6 Business Continuity Disaster Recovery and Incident Management	23
7.7 Security Program Management	23
7.9 Security Operations	23
8.2 Cyber Law	23
8.3 Cyber Ethics	23
8.4 Cyber Policy	23
8.5 Privacy	23
1.2 Digital Forensics	22
1.4 Access Control	22
1.8 Information Storage Security	22
4.4 Distributed Systems Architecture	22
5.3 System Access	22
5.4 System Control	22
6.1 Identity Management	22
1.5 Secure Communication Protocols	21
5.7 Common System Architectures	21
4.3 Hardware Architecture	20
2.4 Analysis and Testing	20
3.2 Component Procurement	20
4.1 Physical Media	20
3.4 Component Reverse Engineering	19
4.6 Network Implementations	19
2.5 Deployment and Maintenance	15
3.3 Component Testing	14
5.6 System Testing	13
2.3 Implementation	12
6.3 Personal Compliance with Cybersecurity RulesPolicyEthical Norms	4
8.1 Cybercrime	4
7.8 Personnel Security	1
6.5 Social and Behavioral Privacy	1

Tabla C.1: Frecuencias de KUs en O*NET *Crosswalk*
Fuente: Elaboración propia

Anexo D: Respuestas a cuestionario aplicado a expertos

Prioridad / Experto	KA-1	KA-2	KA-3	KA-4	KA-5	KA-6	KA-7	KA-8
Experto 1	Indispensable	Importante	Importante	Indispensable	Importante	Indispensable	Importante	Indispensable
Experto 2	Indispensable	Importante	Importante	Importante	Indispensable	Importante	Importante	Opcional

Tabla D.1: Prioridad asignada a cada área de conocimiento (KA) por los expertos
Fuente: Elaboración propia

Profundidad / Experto	KA-1	KA-2	KA-3	KA-4	KA-5	KA-6	KA-7	KA-8
Experto 1	Avanzado	Intermedio	Intermedio	Intermedio	Intermedio	Avanzado	Introductorio	Intermedio
Experto 2	Avanzado	Introductorio	Intermedio	Intermedio	Intermedio	Intermedio	Intermedio	Introductorio

Tabla D.2: Nivel de profundidad asignado a cada área de conocimiento (KA) por los expertos
Fuente: Elaboración propia

Agrupar / Experto	KA-1 con	KA-2 con	KA-3 con	KA-4 con	KA-5 con	KA-6 con	KA-7 con	KA-8 con
Experto 1	KA-6 Human Security	KA-4 Connection Security	KA-4 Connection Security	KA-3 Component Security	KA-6 Human Security	Nada	KA-8 Societal Security	Nada
Experto 2	KA-5 System Security	KA-1 Data Security	KA-1 Data Security	KA-5 System Security	KA-1 Data Security	KA-1 Data Security	KA-1 Data Security	KA-1 Data Security

Tabla D.3: Agrupaciones propuestas entre áreas de conocimiento (KA) según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
1.1 Cryptography	4	5
1.2 Digital Forensics	4	3
1.3 Data Integrity and Authentication	4	4
1.4 Access Control	4	3
1.5 Secure Communication Protocols	5	5
1.6 Cryptanalysis	4	3
1.7 Data Privacy	5	3
1.8 Information Storage Security	4	4

Tabla D.4: Calificación de las unidades de conocmiento (KU) del área *Data Security* según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
2.1 Fundamental Principles	5	5
2.2 Design	3	5
2.3 Implementation	3	5
2.4 Analysis and Testing	3	4
2.5 Deployment and Maintenance	3	4
2.6 Documentation	3	4
2.7 Ethics	5	4

Tabla D.5: Calificación de las unidades de conocmiento (KU) del área *Software Security* según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
3.1 Component Design	4	5
3.2 Component Procurement	4	4
3.3 Component Testing	4	4
3.4 Component Reverse Engineering	4	4

Tabla D.6: Calificación de las unidades de conocmiento (KU) del área *Component Security* según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
4.1 Physical Media	4	5
4.2 Physical Interfaces and Connectors	4	4
4.3 Hardware Architecture	4	4
4.4 Distributed Systems Architecture	5	4
4.5 Network Architecture	5	5
4.6 Network Implementations	5	4
4.7 Network Services	4	4
4.8 Network Defense	5	4

Tabla D.7: Calificación de las unidades de conocmiento (KU) del área *Connection Security* según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
5.1 System Thinking	4	4
5.2 System Management	3	4
5.3 System Access	4	5
5.4 System Control	4	5
5.5 System Retirement	4	4
5.6 System Testing	4	4
5.7 Common System Architectures	3	5

Tabla D.8: Calificación de las unidades de conocmiento (KU) del área *System Security* según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
6.1 Identity Management	5	5
6.2 Social Engineering	5	5
6.3 Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	5	5
6.4 Awareness and Understanding	5	4
6.5 Social and Behavioral Privacy	5	4
6.6 Personal Data Privacy and Security	5	5
6.7 Usable Security and Privacy	5	4

Tabla D.9: Calificación de las unidades de conocmiento (KU) del área *Human Security* según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
7.1 Risk Management	4	4
7.2 Security Governance & Policy	4	4
7.3 Analytical Tools	3	4
7.4 Systems Administration	3	4
7.5 Cybersecurity Planning	4	5
7.6 Business Continuity, Disaster Recovery, and Incident Management	5	4
7.7 Security Program Management	4	4
7.8 Personnel Security	5	4
7.9 Security Operations	5	4

Tabla D.10: Calificación de las unidades de conocmiento (KU) del área *Organizational Security* según los expertos
Fuente: Elaboración propia

KU	**Experto 1**	**Experto 2**
8.1 Cybercrime	4	5
8.2 Cyber Law	4	5
8.3 Cyber Ethics	5	4
8.4 Cyber Policy	5	4
8.5 Privacy	5	5

Tabla D.11: Calificación de las unidades de conocmiento (KU) del área *Societal Security* según los expertos
Fuente: Elaboración propia

Anexo E: Tablas de análisis de opinión experta

KU	**Presencia en propuestas**	**Calificación experta**
1.1 Cryptography	83,33	90,00
1.2 Digital Forensics	0,00	70,00
1.3 Data Integrity and Authentication	100,00	80,00
1.4 Access Control	25,00	70,00
1.5 Secure Communication Protocols	100,00	100,00
1.6 Cryptanalysis	83,33	70,00
1.7 Data Privacy	0,00	80,00
1.8 Information Storage Security	20,00	80,00

Tabla E.1: Comparación entre la relevancia de los KU de KA *Data Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

KU	**Presencia en propuestas**	**Calificación experta**
2.1 Fundamental Principles	92,86	100,00
2.2 Design	75,00	80,00
2.3 Implementation	100,00	80,00
2.4 Analysis and Testing	100,00	70,00
2.5 Deployment and Maintenance	100,00	70,00
2.6 Documentation	0,00	70,00
2.7 Ethics	20,00	90,00

Tabla E.2: Comparación entre la relevancia de los KU de KA *Software Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

KU	**Presencia en propuestas**	**Calificación experta**
3.1 Component Design	16,67	90,00
3.2 Component Procurement	0,00	80,00
3.3 Component Testing	100,00	80,00
3.4 Component Reverse Engineering	66,67	80,00

Tabla E.3: Comparación entre la relevancia de los KU de KA *Component Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

KU	**Presencia en propuestas**	**Calificación experta**
4.1 Physical Media	100,00	90,00
4.2 Physical Interfaces and Connectors	100,00	80,00
4.3 Hardware Architecture	100,00	80,00
4.4 Distributed Systems Architecture	71,43	90,00
4.5 Network Architecture	28,57	100,00
4.6 Network Implementations	75,00	90,00
4.7 Network Services	100,00	80,00
4.8 Network Defense	64,29	90,00

Tabla E.4: Comparación entre la relevancia de los KU de KA *Connection Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

KU	**Presencia en propuestas**	**Calificación experta**
5.1 System Thinking	55,56	80,00
5.2 System Management	88,89	70,00
5.3 System Access	100,00	90,00
5.4 System Control	72,73	90,00
5.5 System Retirement	50,00	80,00
5.6 System Testing	0,00	80,00
5.7 Common System Architectures	57,14	80,00

Tabla E.5: Comparación entre la relevancia de los KU de KA *System Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

KU	**Presencia en propuestas**	**Calificación experta**
6.1 Identity Management	100,00	100,00
6.2 Social Engineering	100,00	100,00
6.3 Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	0,00	100,00
6.4 Awareness and Understanding	75,00	90,00
6.5 Social and Behavioral Privacy	50,00	90,00
6.6 Personal Data Privacy and Security	100,00	100,00
6.7 Usable Security and Privacy	60,00	90,00

Tabla E.6: Comparación entre la relevancia de los KU de KA *Human Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

KU	**Presencia en propuestas**	**Calificación experta**
7.1 Risk Management	100,00	80,00
7.2 Security Governance & Policy	66,67	80,00
7.3 Analytical Tools	66,67	70,00
7.4 Systems Administration	85,71	70,00
7.5 Cybersecurity Planning	50,00	90,00
7.6 Business Continuity, Disaster Recovery, and Incident Management	100,00	90,00
7.7 Security Program Management	100,00	80,00
7.8 Personnel Security	66,67	90,00
7.9 Security Operations	0,00	90,00

Tabla E.7: Comparación entre la relevancia de los KU de KA *Organizational Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

KU	**Presencia en propuestas**	**Calificación experta**
8.1 Cybercrime	75,00	90,00
8.2 Cyber Law	11,11	90,00
8.3 Cyber Ethics	50,00	90,00
8.4 Cyber Policy	0,00	90,00
8.5 Privacy	66,67	100,00

Tabla E.8: Comparación entre la relevancia de los KU de KA *Societal Security* según expertos y su representación en la propuesta curricular
Fuente: Elaboración propia

Anexo F: Mapeo de códigos O*NET hacia KUs de CSEC2017

Código O*NET	**KUs**
11-3021.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.1, 8.2, 8.3, 8.4, 8.5
13-2099.04	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.7, 3.1, 3.2, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1211.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 6.3, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1212.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1221.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1231.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.7, 3.1, 3.2, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1232.00	1.1, 1.2, 1.3, 1.4, 1.8, 2.1, 2.2, 2.7, 3.1, 4.3, 4.4, 4.5, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1241.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5

Tabla F.1: Mapeo códigos de O*NET con KUs del CSEC2017
Fuente: Elaboración propia

Código O*NET	**KUs**
15-1242.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 6.3, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1243.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 6.3, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1244.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1253.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.4, 4.5, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1299.01	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.7, 3.1, 3.2, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1299.02	1.1, 1.2, 1.3, 1.4, 1.8, 2.1, 2.2, 2.3, 2.4, 2.7, 3.1, 4.5, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 6.1, 6.3, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1299.03	1.1, 1.3, 2.1, 2.2, 2.7, 3.1, 4.5, 4.7, 4.8, 5.1, 5.2, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1299.04	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5

Tabla F.2: Mapeo códigos de O*NET con KUs del CSEC2017 parte 2
Fuente: Elaboración propia

Código O*NET	**KUs**
15-1299.05	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1299.06	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 6.5, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1299.08	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
15-1299.09	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.4, 4.1, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
19-4092.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.3, 2.4, 2.5, 2.7, 3.1, 3.2, 3.3, 3.4, 4.1, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.6, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
33-3021.00	1.1, 1.2, 1.3, 1.4, 1.5, 1.8, 2.1, 2.2, 2.4, 2.7, 3.1, 3.4, 4.1, 4.3, 4.4, 4.5, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 5.7, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5
33-3021.06	1.1, 1.2, 1.3, 1.4, 1.8, 2.1, 2.2, 2.7, 3.1, 4.5, 4.7, 4.8, 5.1, 5.2, 5.3, 5.4, 6.1, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.9, 8.2, 8.3, 8.4, 8.5

Tabla F.3: Mapeo códigos de O*NET con KUs del CSEC2017 parte 3
Fuente: Elaboración propia

REFERENCIAS BIBLIOGRÁFICAS

[ACM, sf] ACM (s.f.). Cybersecurity Curricular Guidelines | CSEC 2017. https://cybered.hosting.acm.org/wp. Recuperado el 2025-11-12.

[AIEP, sf] AIEP (s.f.). Ingeniería en ciberseguridad. https://www.aiep.cl/admision/carrera/ingenieria-en-ciberseguridad. Recuperado el 2025-10-01.

[ANCI, 2025a] ANCI (2025a). Anci mision y vision. https://anci.gob.cl/quienes-somos/mision-y-objetivos. Recuperado el 2025-10-01.

[ANCI, 2025b] ANCI (2025b). Subsecretaría del Interior – Ministerio del Interior – Gobierno de Chile. https://www.subinterior.gob.cl/noticias/2025/01/02/este-jueves-2-de-enero-comenzo-a-funcionar-la-agencia-nacional-de-ciberseguridad. Recuperado el 2025-10-01.

[Baker, 2024] Baker, K. (2024). Types of cyberattacks. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks. Recuperado el 2025-10-01.

[Cambridge Dictionary, sf] Cambridge Dictionary (s.f.). framework. Recuperado el 2025-10-01.

[Cerf, 2024] Cerf, E. (2024). Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world - news. https://news.ucsc.edu/2024/05/ukraine-cybersecurity. Recuperado el 2025-10-01.

[Check Point Research, 2025] Check Point Research (2025). Q1 2025 Global Cyber Attack Report from Check Point Software: An Almost 50 % Surge in Cyber Threats Worldwide, with a Rise of 126 % in Ransomware Attacks. https://blog.checkpoint.com/research/q1-2025-global-cyber-attack-report-from-check-point-software-an-almost-50-surge-in- Recuperado el 2025-10-01].

[Chiletec, 2024] Chiletec (2024). Mes de la ciberseguridad: Ciberataques en chile crecieron un 30 % durante el primer semestre. https://chiletec.org/noticias/mes-de-la-ciberseguridad-ciberataques-en-chile-crecieron-un-30-durante-el-primer-se Recuperado el 2025-10-01.

[Cisco, sf] Cisco (s.f.). What is cybersecurity? https://www.cisco.com/site/us/en/learn/topics/security/what-is-cybersecurity.html. Recuperado el 2025-10-01.

[Crabb *et al.*, 2024] Crabb, J., Hundhausen, C., y Gebremedhin, A. (2024). A critical review of cybersecurity education in the united states. En *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, pp. 241–247.

[CSET/ETO, 2024] CSET/ETO (2024). Eto-cset nice-o*net crosswalk. https://eto.tech/dataset-docs/nice-onet-crosswalk/. Recuperado el 2025-10-01.

[CyBOK, sf] CyBOK (s.f.). Cybok – the cyber security body of knowledge. https://www.cybok.org. Recuperado el 2025-11-12.

[Dkaidek y Rashid, 2024] Dkaidek, Z. y Rashid, A. (2024). Bridging the cybersecurity skills gap: Knowledge framework comparative study. *IEEE Security & Privacy*, 22(5):88–95.

[El Mostrador, sf] El Mostrador (s.f.). Informe de ciberseguridad: Chile sufrió 27.600 millones de intentos de ciberataques en 2024. https://www.elmostrador.cl/noticias/pais/2025/04/30/informe-de-ciberseguridad-chile-sufrio-27-600-millones-de-intentos-de-ciberataques- Recuperado el 2025-10-01.

[ENISA, 2022a] ENISA (2022a). European cybersecurity skills framework (ecsf) - user manual. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-ecsf. Publication date: September 19, 2022.

[ENISA, 2022b] ENISA (2022b). European cybersecurity skills framework role profiles. https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles. Publication date: September 19, 2022.

[ENISA, 2024] ENISA (2024). Crosswalk between esco and ecsf. https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf/crosswalk-between-esco-and-ecsf. Recuperado el 2025-11-12.

[ENISA, sf] ENISA (s.f.). What we do | ENISA. https://www.enisa.europa.eu/about-enisa/what-we-do. Recuperado el 2025-10-01.

[HackTheBox, sf] HackTheBox (s.f.). Cyber Mastery: Community Inspired. Enterprise Trusted. — hackthebox.com. https://www.hackthebox.com/. Recuperado 14-12-2025.

[Hajny *et al.*, 2021] Hajny, J., Ricci, S., Piesarskas, E., Levillain, O., Galletta, L., y De Nicola, R. (2021). Framework, tools and good practices for cybersecurity curricula. *IEEE Access*, 9:94723–94747.

[IBM, 2025a] IBM (2025a). ¿Qué es la ciberseguridad? https://www.ibm.com/mx-es/think/topics/cybersecurity. Recuperado el 2025-12-01.

[IBM, 2025b] IBM (2025b). ¿Qué es un ataque cibernético? https://www.ibm.com/mx-es/topics/cyber-attack. Recuperado el 2025-10-01.

[Impagliazzo y Pears, 2018] Impagliazzo, J. y Pears, A. N. (2018). The CC2020 project — computing curricula guidelines for the 2020s. pp. 2021–2024.

[IPST, sf] IPST (s.f.). Ingeniería en informática. https://www.ipsantotomas.cl/carreras/ingenieria-en-informatica/. Recuperado el 2025-10-01.

[ISC2, 2024] ISC2 (2024). ISC2 Cybersecurity Workforce Study 2024. https://www.isc2.org/research/workforce-study. Recuperado el 2025-10-01.

[IT HUNTERS, 2025] IT HUNTERS (2025). Los cargos más solicitados en la primera mitad del año en chile en las áreas ti.

[Kaspersky, sf] Kaspersky (s.f.). The portrait of modern infosec professional. https://www.kaspersky.com/blog/portrait-of-infosec-professional-report-2024. Recuperado el 2025-10-01.

[Kushner, 2013] Kushner, D. (2013). The real story of stuxnet. *ieee Spectrum*, 50(3):48–53.

[La Tercera, 2023] La Tercera (2023). Ciberseguridad: expertos estiman que chile necesita más de 28 mil profesionales vinculados a esta área. https://www.latercera.com/ediciones-especiales/noticia/ciberseguridad-expertos-estiman-que-chile-necesita-mas-de-28-mil-profesionales-vinc
JHMZ5KNXMZDULPFWIDUPWLRASQ. Recuperado el 2025-10-01.

[Lehto y Martti, 2022] Lehto y Martti (2022). Development needs in cybersecurity education: Final report of the project. *Informaatioteknologian tiedekunnan julkaisuja*, 96.

[Malkin y Parker, 1993] Malkin, G. S. y Parker, T. L. (1993). Internet Users' Glossary. RFC 1392.

[Metasploit, sf] Metasploit (s.f.). Metasploit | Penetration Testing Software, Pen Testing Security | Metasploit — metasploit.com. https://www.metasploit.com/. Recuperado 14-12-2025.

[National Center for O*NET Development, sf] National Center for O*NET Development (s.f.). O*net online. https://www.onetonline.org/. Recuperado el 2025-10-01.

[National Security Agency, sf] National Security Agency (s.f.). National centers of academic excellence in cybersecurity. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence. Recuperado el 2025-10-01.

[NCSI, sf] NCSI (s.f.). NCSI :: Chile. https://ncsi.ega.ee/country/cl. Recuperado el 2025-10-01.

[NIST, 2019] NIST (2019). Nice framework resource center. https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center. Recuperado el 2025-11-12.

[NIST, 2025] NIST (2025). Nice framework history — nist.gov. Recuperado el 2025-10-01.

[Radware, sf] Radware (s.f.). Live cyber threat map. https://livethreatmap.radware.com. Recuperado el 2025-10-01.

[Ramezanian y Niemi, 2024] Ramezanian, S. y Niemi, V. (2024). Cybersecurity education in universities: a comprehensive guide to curriculum development. *Ieee Access*, 12:61741–61766.

[Sinha, 2024] Sinha, S. (2024). Number of connected iot devices growing 13 % to 18.8 billion. https://iot-analytics.com/number-connected-iot-devices. Recuperado el 2025-10-20.

[Statista, 2024] Statista (2024). Cybercrime expected to skyrocket in coming years. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/. Accessed 2025-10-21.

[TryHackMe, sf] TryHackMe (s.f.). TryHackMe | Cyber Security Training — tryhackme.com. https://tryhackme.com/. Recuperado 14-12-2025.

[USACH, sf] USACH (s.f.). Ingeniería civil en informática. https://admision.usach.cl/carreras/ingenieria-civil-en-informatica/. Recuperado el 2025-10-01.

[UST, sf] UST (s.f.). Ingeniería civil informática y sistemas inteligentes. https://www.ust.cl/carreras/ingenieria-civil-informatica-y-sistemas-inteligentes. Recuperado el 2025-10-01.

[Yar *et al.*, 2024] Yar, M. A., Goh, H. G., Adnan, K., Gan, M. L., y Ponnusamy, V. (2024). Bridging cybersecurity education and industry demands: mapping and prioritizing curriculum guidelines. En *2024 International Conference on Future Technologies for Smart Society (ICFTSS)*, pp. 188–193. IEEE.