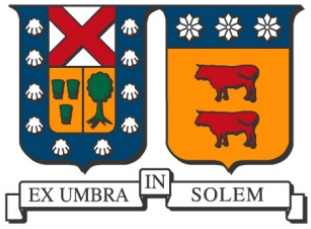
UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
SANTIAGO - CHILE



“DISEÑO DE UN MARCO DE REFERENCIA PARA LA INTEGRACIÓN DE COMPETENCIAS TRANSVERSALES EN CIBERSEGURIDAD EN LA FORMACIÓN DE INGENIEROS DE PREGRADO EN LA UTFSM”

MATÍAS IGNACIO HERRERA CIFUENTES

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: Berioska Contreras
Profesor Correferente: Claudio Lobos

Julio - 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 marco de referencia para la integración de competencias transversales en ciberseguridad en la formación de ingenierps de pregrado en la UTFSM

Nombre del candidato(a): Matias Ignacio Herrera Cifuentes

Carrera / Grado: Ingeniería Civil en Informática

Campus: Santiago San Joaquin **;** **Departamento**: Departamento de Informática

2.- VALIDACIÓN DEL PROFESOR GUÍA/DIRECTOR DE TESIS

Yo, Berioska Maureen Contreras Vargas, 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

☒ 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:

☐ 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: 21-08-2025 ; **Firma:** 

Estudiante o Candidato(a):

Fecha: 21-08-2025 ; **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.

AGRADECIMIENTOS

En primer lugar quisiera agradecer a mi familia, en especial a mis padres Rusty Herrera y Jeannette Cifuentes y mis hermanos Rusty y Darling, los que siempre han estado presentes para brindarme su apoyo durante toda mi vida, en especial en esta última etapa de mi formación académica y a quienes quiero dedicar este deseado logro personal.

También nombrar a mis amigos, quienes desde el primer día me han acompañado en este proceso en el que hemos vivido tantos buenos momentos, una mención especial a Sebastián, Benjamín, Simón, Julio, Mauricio, Jeremmy, Claudio, Iván, Leonardo y Juan Carlos, sin ustedes no hubiese logrado tanto en tan poco tiempo.

Finalmente me gustaría agradecer a mi profesora guía Berioska Contreras, quien desde el primer día confió en mí y me brindó su conocimiento en este tema, paciencia, apoyo y comprensión en momentos difíciles. Sin todo esto el desarrollo de mi memoria no hubiese sido posible.

RESUMEN

Resumen— La presente memoria desarrolla un estudio descriptivo y exploratorio, el que propone un marco de referencia integral de competencias en ciberseguridad orientado transversalmente a la formación de ingenieros de diversas especialidades en la Universidad Técnica Federico Santa María (UTFSM). El objetivo principal fue identificar, estructurar y priorizar las habilidades, conocimientos y competencias digitales fundamentales que todo ingeniero debería adquirir durante su formación inicial, independientemente de su disciplina. Para ello, se diseñó una metodología en cuatro etapas: recopilación de antecedentes mediante una encuesta de percepción a estudiantes, alineación con los objetivos formativos institucionales, análisis de brechas de conocimiento e interés, y formulación de un plan de acción basado en estándares internacionales como el NIST, ENISA y objetivos del Gobierno de Chile. Los resultados mostraron que entre los 214 encuestados, un 63,6 % afirma no haber recibido formación en ciberseguridad, contrastado con un alto interés en adquirir un curso introductorio de ciberseguridad como parte del plan común de Ingeniería con un 77,6 %. El marco de referencia propuesto permite identificar e integrar contenidos esenciales en cursos lectivos facilitando su adopción en mallas curriculares universitarias. Su implementación busca promover una cultura de ciberseguridad en la educación superior y responder a las crecientes necesidades detectadas en el trato de las personas con la seguridad de la información.

Palabras Clave—
• **Seguridad y privacidad → Aspectos sociales de la seguridad y la privacidad**;
• **Computación aplicada → Educación**;
• **Ingeniería del software → Creación y gestión de software**;

ABSTRACT

***Abstract*—**

This paper develops a descriptive and exploratory study that proposes a comprehensive cybersecurity competency framework aimed at training engineers of various specialties at the Federico Santa María Technical University (UTFSM). The main objective was to identify, structure, and prioritize the fundamental digital skills, knowledge, and competencies that every engineer should acquire during their initial training, regardless of their discipline. To this end, a four-stage methodology was designed: gathering background information through a student perception survey, alignment with institutional training objectives, analysis of knowledge and interest gaps, and formulation of an action plan based on international standards such as NIST, ENISA, and objectives of the Chilean Government. The results showed that among the 214 respondents, 63.6 % reported having received no cybersecurity training, contrasting with a high interest in enrolling an introductory cybersecurity course as part of the common engineering program (77.6 %). The proposed framework allows for the identification and integration of essential content into courses, facilitating their adoption in university curricula. Its implementation seeks to promote a culture of cybersecurity in higher education and respond to the growing needs identified in people's interactions with information security.

***Keywords*—**

- **Security and privacy → Social aspects of security and privacy**;
- **Applied computing → Education;**
- **Software and its engineering → Software creations and managements;**

GLOSARIO

DI: Departamento de Informática.

UTFSM: Universidad Técnica Federico Santa María.

NICE: National Initiative for Cybersecurity Education

NIST: National Institute of Standards and Technology

NCSI: National Cyber Security Index

ENISA: European Union Agency for Cybersecurity

ECSF: European Cybersecurity Skills Framework

MFA: Multi-factor authentication

2FA: Two-factor authentication

SCT: Sistema de Créditos Transferibles, busca medir, racionalizar y distribuir el trabajo académico en sus planes de estudio.

Competencias: Aptitud de una persona con capacidades, habilidades clave y destrezas que le permiten realizar una actividad o cumplir un objetivo dentro del ámbito laboral o académico.

Competencia Digital: Uso seguro, saludable, sostenible, crítico y responsable de las tecnologías digitales para el aprendizaje, el trabajo y la participación social MINEDUC (2025).

IES: Instituciones de Educación Superior, tanto públicas como privadas.

IMC: Índice de Madurez en Ciberseguridad.

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1
INTRODUCCIÓN

En las últimas décadas, el avance de tecnologías digitales ha incrementado exponencialmente los riesgos asociados a la ciberseguridad. Esta situación ha generado una demanda de personas digitalmente capacitadas no solo en sectores de tecnologías de la información, sino también en otras disciplinas de la ingeniería, que comprendan los principios fundamentales de la ciberseguridad y puedan aplicarlos de forma transversal en sus respectivos contextos laborales y más importantemente aún, sus vidas diarias. En este escenario, la formación en competencias digitales se ha convertido en una prioridad para instituciones académicas no solo en Chile, sino en todo el mundo.

La Universidad Técnica Federico Santa María (UTFSM), reconocida por su excelencia en la formación de ingenieros, enfrenta el desafío de incorporar de estas competencias en sus mallas curriculares. Dentro de su Modelo Educativo Institucional (UTFSM, 2016), declara la Responsabilidad Social y Ética como una competencia que apunta a que los alumnos pongan sus conocimientos y habilidades al servicio y bien común de la comunidad, sin embargo, actualmente no existe un enfoque transversal que asegure que todos los egresados, independientemente de su especialidad, tengan un conocimiento básico sobre ciberseguridad en sus mallas laborales. Esta problemática genera una brecha entre las competencias adquiridas durante la formación académica y las necesidades de sus respectivos entornos laborales.

En este contexto, la presente memoria propone la implementación de un marco de referencia integral de competencias en ciberseguridad con enfoque transversal, aplicado a estudiantes de ingeniería de pregrado la UTFSM en sus dos primeros años. Este marco de referencia busca ser una base de investigación, que al aplicarse en un contexto universitario, permita identificar los conocimientos y habilidades que todo futuro ingeniero debería adquirir durante su formación universitaria, permitiendo fortalecer su perfil profesional.

La propuesta se estructura en cuatro etapas metodológicas: (1) análisis de los objetivos formativos de la universidad y su relación con competencias digitales fundamentales de la ciberseguridad, (2) diagnóstico del nivel de conocimiento y percepción de los estudiantes sobre ciberseguridad mediante encuestas (3) identificación de brechas y áreas prioritarias de intervención, y (4) diseño de un plan de acción que consolide estas competencias dentro del perfil de egreso, considerando literatura relevante y la realidad de la industria.

CAPÍTULO 2
DEFINICIÓN DEL PROBLEMA

2.1. Contexto y Situación Actual

El Índice Nacional de Ciberseguridad desarrollado por Estonia, mide la preparación en ciberseguridad de los países en relación con otros mediante doce indicadores principales, posiciona a Chile en la posición número 42 dentro de un ranking de 175 países (NCSI, 2025). Dentro de sus indicadores se encuentra el *awareness* en el que Chile representa un 25 % de cumplimiento en temáticas como concienciación sobre ciberseguridad y análisis de ciberamenazas. Mientras que, existen cinco universidades en Chile que ofrecen programas de formación en ciberseguridad, de las cuales, tres se dictan de manera online.

Por otro lado, el Índice de Madurez en Ciberseguridad (IMC) es un marco de referencia diseñado para evaluar el estado de la ciberseguridad en universidades e instituciones de educación superior (IES). Según MetaRed (2024), el 62 % de las IES participantes incluyen cursos relacionados con ciberseguridad en sus planes de estudio, distribuidos en un 27,6 % a nivel de pregrado y un 35,5 % en programas de postgrado. Este índice clasifica la madurez institucional en cuatro niveles: inicial (L0), básico (L1), intermedio (L2) y avanzado (L3). Actualmente, las instituciones chilenas se sitúan en el nivel básico (L1), aunque próximas al nivel intermedio (L2), superando en promedio al IMC iberoamericano. A pesar de esto, se observa una brecha entre instituciones públicas y privadas, donde las primeras se mantienen en un nivel básico, mientras que las privadas alcanzan un nivel intermedio. La principal diferencia entre ambas radica en la existencia y cantidad de personal dedicado específicamente a la gestión de ciberseguridad dentro de las instituciones.

En cuanto al número de incidentes reportado por el IMC, se advierte que 6 de cada 10 Instituciones en Chile han sufrido incidentes relacionados en ciberseguridad, mostrando una relación directa entre el nivel de madurez mostrado y el número de ciberincidentes registrados, por lo que, instituciones que figuran con más incidentes tienden a destinar un mayor presupuesto en el sector de ciberseguridad que aumentan su Índice de Madurez.

En relación a este estancamiento, la Política Nacional de Ciberseguridad de Chile para el período 2023-2028 identifica deficiencias significativas en el ámbito nacional (ANCI, 2023). Entre estas, se destaca la escasez de aproximadamente 28.000 especialistas en ciberseguridad necesarios para los sectores público y privado. Adicionalmente, se observa un déficit en la cultura de ciberseguridad en los niveles de educación básica y media, incluyendo las instituciones privadas.

En respuesta a estos desafíos, la política propone cinco objetivos estratégicos, siendo uno de los principales el desarrollo de una cultura de ciberseguridad. Este objetivo enfatiza la importancia de la educación en ciberhigiene y ciberseguridad desde una edad temprana, promoviendo buenas prácticas y la responsabilidad en el manejo de tecnologías digitales.

Tomando en consideración estos objetivos planteados para los próximos años y la creciente relevancia de la ciberseguridad en la industria tecnológica de nuestro país, se llevó a cabo un análisis de las mallas curriculares del semestre 2024-1 de las diversas ramas de Ingeniería civil impartidas por la Universidad Técnica Federico Santa María (UTFSM). Posteriormente en la actualización de mallas a 2025 se redujeron la cantidad de semestres para la utilización de planes de estudio de cinco años, las mallas cuentan con distintos ciclos para denotar la cantidad de semestres cursados y relación en torno a la carrera específica, el ciclo de bachillerato corresponde a los cuatro primeros semestres lectivos y el ciclo profesional a los últimos dos.

Se tomará en cuenta dos carreras de la UTFSM que tienen una implicación significativa en áreas relacionadas con la ciberseguridad para un análisis de sus mallas no incluyendo sus asignaturas electivas: Ingeniería Civil Informática e Ingeniería Civil Telemática.

La revisión de la malla curricular de Ingeniería Civil Informática (ver Figura 26) revela que, a pesar de su estrecha vinculación con el desarrollo de software y sistemas de información, no existe un curso formal obligatorio que aborde específicamente temas de ciberseguridad en sus ciclos de formación de bachillerato, que contempla los primeros dos años del estudiante. Esta ausencia implica que los estudiantes pueden llegar a graduarse sin haber recibido una formación estructurada en principios y prácticas fundamentales de seguridad informática, lo que es crucial tanto para su desempeño profesional como personal.

Por otro lado, la malla curricular de Ingeniería Civil Telemática (ver Figura 27) incluye dos cursos específicos, Criptografía y Seguridad de la Información (TEL-252) y Seguridad en Redes de Computadores (TEL-312), que se enfocan en temas avanzados de ciberseguridad. Sin embargo, estos cursos no cuentan con otros ramos como prerrequisito que aborden los aspectos básicos y fundamentales del campo, limitando así la preparación de los estudiantes en competencias esenciales que son necesarias para entender y mitigar amenazas cibernéticas en niveles iniciales de su carrera profesional. Para su actualización en 2025, incluye la asignatura de Ingeniería en Ciberseguridad, sin embargo, se encuentra en el ciclo de licenciatura, el que corresponde entre el quinto y octavo semestre de las nuevas mallas de cinco años.

2.2. Objetivos e Impacto

2.2.1. Objetivo General

Desarrollar un marco de referencia que permita especificar descriptores concretos y medibles de las habilidades o conocimientos esenciales que los estudiantes de ingeniería civil de la UTFSM deben adquirir durante el ciclo de bachillerato en el área de ciberseguridad para su desarrollo personal y profesional, tal que contribuya a la creación de cursos orientados a fomentar una cultura de alfabetización digital segura alineada con la política pública de nuestro país.

2.2.2. Objetivos Específicos

1. **Examinar el conocimiento actual:** Especificar descriptores que permitan evaluar de manera consistente la percepción de los estudiantes de ingeniería de la UTFSM respecto a sus habilidades o conocimientos en el área de ciberseguridad.
2. **Establecer las habilidades o conocimientos esenciales:** Determinar el nivel deseado de conocimientos y competencias básicas de ciberseguridad basándose en un estudio exploratorio de fuentes formales.
3. **Diseñar un marco de referencia:** Construir un modelo adaptado al contexto educativo de pregrado, del ciclo de bachillerato, de la UTFSM que integre descriptores esenciales de ciberseguridad cuantificables a través de una encuesta de percepción para identificar eventuales brechas, reconociendo las competencias digitales necesarias para una educación de calidad.
4. **Documentación y difusión:** Elaborar un informe que documente el proceso de investigación, el desarrollo del marco de referencia, los resultados de la implementación y las recomendaciones para futuras iniciativas.

2.2.3. Impacto de la Solución

La Universidad establece un conjunto de Competencias Transversales-Sello, las cuales fueron seleccionadas en base a los valores fundacionales y consultas en conjunto entre estudiantes y profesorado. Estas tienen como objetivo cubrir tanto las competencias planteadas por la institución como también dar respuesta a las constantes necesidades detectadas por el entorno. Entre ellas se encuentra el Compromiso con la calidad, que implica enfrentar retos actuales y futuros, como también buscar un aprendizaje continuo y una consolidación de una cultura de calidad dentro de su alumnado y también el Manejo de las Tecnologías de Información y Comunicaciones, que propone el uso de herramientas para la resolución de problemas en contextos de alfabetización digital, contribuyendo al cumplimiento del objetivo 4; Calidad de la Educación, de los Objetivos de Desarrollo Sostenible, que busca aumentar el número de estudiantes que cuentan con competencias técnicas y digitales para facilitar su acceso a empleos decentes (United Nations, 2025).

El marco de referencia propuesto como solución apunta a ser un punto de partida que para impactar directamente en las Competencias Transversales-Sello, promoviendo una formación integral y de calidad en todas sus carreras. De igual manera, en pos de cumplir los objetivos Nacionales, permite ser aplicada a cualquier Institución de educación superior que requiera de una base para definir y establecer su propio conjunto de competencias en ciberseguridad.

CAPÍTULO 3
MARCO CONCEPTUAL

3.1. Marcos de referencia existentes

Un framework, por sí solo, se entiende como un esquema o patrón estructurado que sirve de guía para la creación de un determinado elemento. Su propósito principal es facilitar el proceso de diseño y desarrollo, proporcionando una base predefinida que optimiza la implementación. Esto permite al usuario enfocarse en la resolución del problema específico que busca abordar, en lugar de dedicar tiempo y esfuerzo a la construcción desde cero de la infraestructura necesaria para su implementación.

El marco de referencia más prominente en la actualidad para la formación en ciberseguridad es el ”Workforce Framework for Cybersecurity (NICE)”(Petersen et al., 2020). Este framework tiene como propósito principal proveer una estructura organizativa que clasifica y define las tareas y competencias esenciales en el ámbito de la ciberseguridad. Además, estandariza roles y habilidades requeridas en la industria. La adopción de este marco por parte de estudiantes de enseñanza media y superior facilita el desarrollo de habilidades de manera progresiva a través de su formación escolar. Asimismo, sirve como un punto de referencia esencial para que las organizaciones diseñen y preparen recursos adecuados que atiendan las necesidades en diversos aspectos de la educación, la capacitación y el desarrollo profesional en el campo de la ciberseguridad y ciberhigiene.

El documento del NIST define siete categorías principales, cada una de las cuales agrupa funciones comunes relacionadas con la ciberseguridad. Dentro de estas categorías, se especifican 33 áreas de especialidad. Además, se identifican 52 roles laborales o competencias distintas, que engloban los conocimientos, habilidades y capacidades específicas requeridas para desempeñar eficazmente las tareas asociadas a cada puesto de trabajo en el ámbito de la ciberseguridad.

Competencias destacadas de tipo técnico

1. **Lenguajes informáticos:** Competencia que describe las capacidades de un aprendiz relacionadas con los lenguajes informáticos y sus aplicaciones para permitir que un sistema realice funciones específicas.

2. **Seguridad de datos:** Competencia que describe las capacidades de un aprendiz relacionadas con los métodos y procedimientos que protegen los datos y los sistemas de información asegurando su confidencialidad, integridad y disponibilidad.

3. **Impartición de educación y formación:** Competencia que describe las capacidades de un aprendiz relacionadas con ayudar a otros a adquirir conocimientos o desarrollar habilidades. Incluyendo la concienciación sobre ciberseguridad para usuarios de computadoras y otros dispositivos electrónicos.

4. **Gestión de incidentes:** Competencia que describe las capacidades de un aprendiz relacionadas con las tácticas, tecnologías, principios y procesos para analizar, priorizar y manejar incidentes de ciberseguridad.

5. **Derecho, políticas y ética:** Competencia que describe las capacidades de un aprendiz relacionadas con el conocimiento y cumplimiento de leyes, regulaciones, políticas y ética que pueden impactar las actividades organizacionales y personales.

De acuerdo a lo planteado por (ANCI, 2023) la falta de cultura de las organizaciones sobre la importancia de la ciberseguridad conlleva a no tomar en cuenta estas competencias a la hora de formar profesionales no solo en áreas de tecnología, sino de manera transversal. De igual manera (Tsado, 2019) recalca que un enfoque multidisciplinario tanto en disciplinas técnicas como no técnicas, en todos los niveles de estudio es el más adecuado para planificar e implementar un programa educativo de ciberseguridad exitoso.

Mientras tanto, (Dupuis, 2017) utilizó una adaptación de la taxonomía de Bloom Bloom et al. (1964) para desarrollar un marco de trabajo destinado a cursos introductorios de ciberseguridad donde destacan una gran aprobación por parte del público objetivo luego de dos iteraciones en estudiantes sin conocimientos previos.

Un estudio complementario a (Thompson et al., 2018), aplica técnicas de enseñanza dirigidas a un público amplio interesado en la ciberseguridad, independientemente de su nivel de conocimiento previo. Este enfoque introduce y aclara conceptos a través de escenarios prácticos y casos de estudio tomados de situaciones reales, motivando a los estudiantes a profundizar en esta área y a comprender mejor las situaciones cotidianas relacionadas con la ciberseguridad Sherman et al. (2017).

La National Institute of Standards and Technology (NIST) publicó la guía Special Publication 800-50r1 Merritt et al. (2024) con el propósito de asistir a organizaciones en el diseño e implementación de programas de concientización, capacitación y educación en ciberseguridad. En este documento, se introduce el concepto de continuo de aprendizaje (learning continuum), el cual estructura la formación en ciberseguridad en tres niveles progresivos:

1. **Concientización (*Awareness*)**: Enfocada en sensibilizar a los usuarios respecto a qué es la ciberseguridad y por qué es importante. Su objetivo es promover buenas prácticas y actitudes responsables frente a amenazas comunes, sin requerir conocimientos técnicos. Busca generar cambios de comportamiento mediante la identificación de riesgos y la adopción de medidas básicas de protección. *Dirigida a todo tipo de usuarios.*
2. **Capacitación (*Training*)**: Proporciona habilidades prácticas que permiten a los usuarios aplicar principios de ciberseguridad en sus roles específicos. A diferencia de la concientización, que busca generar atención y actitud, la capacitación está orientada al desarrollo de competencias operativas vinculadas a tareas concretas dentro de los sistemas de información. *Enfocada en usuarios que interactúan directamente con tecnologías de la información.*
3. **Educación (*Education*)**: Aborda en profundidad los fundamentos teóricos y técnicos de la ciberseguridad desde una perspectiva multidisciplinaria. Este nivel se asocia con la formación académica especializada, como programas universitarios, diplomados o especializaciones profesionales. *Dirigida a quienes buscan una carrera o especialización en ciberseguridad.*

La European Union Agency for Cybersecurity (ENISA) publicó el Cybersecurity Skills Framework (ENISA, 2022) con el propósito de establecer un lenguaje común para describir los perfiles, funciones y competencias requeridas en el ámbito de la ciberseguridad dentro de la Unión Europea. Este marco busca servir de guía tanto para la formación profesional como para el diseño de políticas públicas, programas académicos y estrategias de desarrollo de talento en el sector.

A diferencia del enfoque progresivo por niveles del NIST SP 800-50r1, el ECSF de ENISA se basa en la identificación y caracterización de doce perfiles profesionales clave en ciberseguridad (ver Figura 1). Cada perfil se describe mediante un conjunto estructurado de tareas, conocimientos, habilidades y competencias, lo que permite obtener un panorama de las necesidades del mercado laboral.

Figura 1: Perfiles ECSF
Fuente: European Cybersecurity Skills Framework Role Profiles

El ECSF no está orientado a la formación de usuarios generales, sino que define las competencias esperadas para quienes postulan a cargos específicos en ciberseguridad. Esta perspectiva permite identificar con mayor precisión las expectativas de la industria en cuanto a la preparación y formación de los profesionales del área, ofreciendo una guía útil para delimitar los contenidos transversales más relevantes, incluso en etapas educativas tempranas.

Algunas habilidades claves y tareas de los perfiles más destacables se detallan de la siguiente manera:

1. **Educador en Ciberseguridad**: Diseña, desarrolla e implementa programas de concienciación, formación y educación en temas de ciberseguridad y protección de los datos. Fortalece la cultura, capacidades y conocimientos claves promoviendo la importancia de la ciberseguridad en el aspecto personal y organizacional.
    - **Habilidades y tareas destacadas:** Identificar las necesidades de concienciación y formación en ciberseguridad - Impartir programas de aprendizaje para cubrir las necesidades - Desarrollar simulaciones en entornos de ciberseguridad - Impartir formación para obtener certificaciones - Fomentar el interés por los temas de ciberseguridad.
2. **Protector de datos:** Supervisa y garantiza el cumplimiento de los marcos legales regulatorios en materia de ciberseguridad y protección de datos, recomendando estrategias y soluciones para garantizar cumplimiento ético y normativo.
    - **Habilidades y tareas destacadas:** Comprensión y adhesión a los estándares éticos - Realizar evaluaciones de impacto en la privacidad al utilizar estándares reconocidos - Difusión de políticas y prácticas recomendadas - Garantizar que las personas estén informados sobre sus derechos y obligaciones en materia de protección de datos.
3. **Respondedor a incidentes cibernéticos:** Especialista en el análisis, evaluación y mitigación de incidentes de seguridad. Este perfil requiere conocimientos técnicos sobre amenazas, vulnerabilidades y gestión de crisis.
    - **Habilidades y tareas destacadas:** Conocimiento plan de respuesta a incidentes - Conocimiento de ciberamenazas - Conocimiento vulnerabilidades - Trabajo en ambientes controlados.

El Global Forum on Cyber Expertice (GFCE) (on Cyber Expertise, 2023) es una plataforma que está centrada en promover políticas y habilidades en ciberseguridad, programas de formación y marcos de competencias, impulsando la creación de frameworks adaptados a contextos nacionales, utilizando estándares internacionales reconocidos como ENISA y NICE. Dentro de sus objetivos destacan promover la concienciación integral sobre amenazas y vulnerabilidades relacionadas con ciberseguridad y empoderarlas con el conocimiento, habilidades y sentido de responsabilidad para practicar comportamientos seguros en la industria, como también poner especial atención en la educación y capacitación en el desarrollo de la fuerza laboral.

El articulo publicado por (Microsoft, 2022) presenta su estrategia para reducir la brecha de habilidades en ciberseguridad mediante capacitación de estudiantes y trabajadores en 23 países, incluyendo alianzas con universidades y certificaciones, analizando las brechas en cada país y desarrollando un framework que se adapte a las necesidades encontradas en cada uno.

(CyberSeek, 2024) es una iniciativa respaldada por el National Initiative for Cyber security Education (NICE) y CompTIA que permite comprender, visualizar y encontrar recursos para la realización de trayectorias laborales en ciberseguridad en Estados Unidos, también destacan que un 10 % de las ofertas de empleo relacionadas a ciberseguridad referencian a la necesidad de conocimientos en Inteligencia Artificial como una de las habilidades de requerimiento mínimo para la aplicación al trabajo.

3.2. Estudios relevantes

3.2.1. Estudio sobre la fuerza laboral en ciberseguridad - ISC2

El estudio anual desarrollado por el (ISC2, 2024), estima la existencia de una brecha laboral en ciberseguridad, lo que significa la diferencia entre el número de profesionales que las organizaciones necesitan para protegerse adecuadamente y el número de profesionales de ciberseguridad activos.

A nivel mundial la estimación identifica una brecha de más de 4 millones de profesionales en el mundo, mientras que en Latinoamerica experimenta una disminución en el gap necesario en comparación con años anteriores y el resto del mundo.

El estudio también destaca en su encuesta realizada que las carreras relacionadas a las Tecnologías de la información corresponden a la vía más popular para acceder a la ciberseguridad (70 %). Si bien es un número elevado, cada vez más profesionales provienen de diferentes ámbitos y profesiones, destacando que aunque provengan de un área diferente, el desarrollo profesional y certificaciones pueden ayudar a mejorar sus competencias una vez asumen el puesto, colaborando a disminuir la brecha de trabajadores identificada.

3.2.2. Informe de investigación global sobre la brecha de competencias en ciberseguridad - Fortinet

El informe publicado por (Fortinet, 2022) reporta que en el mundo, un 80 % de las organizaciones sufrieron una o más vulnerabilidades que podrían atribuirse a la falta de habilidades o conocimientos en ciberseguridad. En su encuesta realizada a 1223 profesionales del área en distintos países del mundo identifican cinco puntos claves que explican la situación:

- La ciberseguridad afecta a todas las organizaciones.
- Reclutamiento y retención de talentos es un problema.
- Las organizaciones buscan trabajadores con certificaciones.
- Las organizaciones buscan diversidad.
- Aumentar concientización en ciberseguridad es un desafío.

3.2.3. Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad - OEA

El reporte realizado por la (OEA, 2022) identifica que el mercado laboral en ciberseguridad en América Latina y el Caribe necesita más tiempo para la capacitación y la educación para generar el equilibrio necesario, estimando un déficit entre 515.000 y 701.000 profesionales para la región.

De igual manera, declaran que los puntos a mejorar desde el lado de la oferta laboral se inclinan por conectar la educación con la formación y la industria promoviendo acceso a rutas de aprendizaje, aclarar y definir las profesiones en ciberseguridad, incrementar vocaciones científicas en la población infantil de la región y concientizar en ciberseguridad desde una edad temprana.

3.2.4. Modelo Educativo Institucional - UTFSM

El punto 6.2 del Modelo Educativo Institucional UTFSM (2016) declara que las unidades académicas y docentes que administran el programa y la Dirección de Enseñanza y Aprendizaje son las responsables del diseño curricular y su futura actualización. De ésta manera, los talleres de empleadores permiten mantener al día tanto la malla curricular como el perfil de egreso del estudiante, centrándose en un modelo basado en competencias, ajustado por la carga máxima de créditos SCT-Chile.

3.2.5. Marco orientador de competencias digitales docentes - MINEDUC

En respuesta a la necesidad de adherirse a los constantes cambios en las tecnologías digitales, (MINEDUC, 2025) presenta su marco para constituirse como una herramienta para integrar competencias digitales en la formación docente, utilizando referencias internacionales tales como ISTE, UNESCO, y el Marco Europeo para la Compentecia Digital de los Educadores.

El documento busca abordar los desafíos en torno a lo digital que enfrentan los docentes, en las que identifican competencias digitales que aportan a cumplir con los estándares asociados a el marco para la buena enseñanza presentado por el Centro de perfeccionamiento, experimentación e investigaciones pedagógicas CPEIP (2021). Para su desarrollo, cuenta de 3 dimensiones principales:

- **Compromiso profesional:** Insta a los docentes a actuar éticamente y en compromiso con el proceso de aprendizaje y desarrollo profesional de sus alumnos, en busca de la mejora continua en los procesos de enseñanza.
- **Competencias pedagógicas:** Busca abordar las competencias que incorporan el uso de las tecnologías digitales adaptados a las distintas disciplinas de los estudiantes.

- **Desarrollo de la ciudadanía digital de las y los estudiantes:** Centrado en desarrollar a los docentes para que sus estudiantes aprendan las competencias necesarias que comprende una ciudadanía digital, en complemento, busca la promoción de la alfabetización digital, participación ciudadana y el cuidado y responsabilidades digitales de las personas.

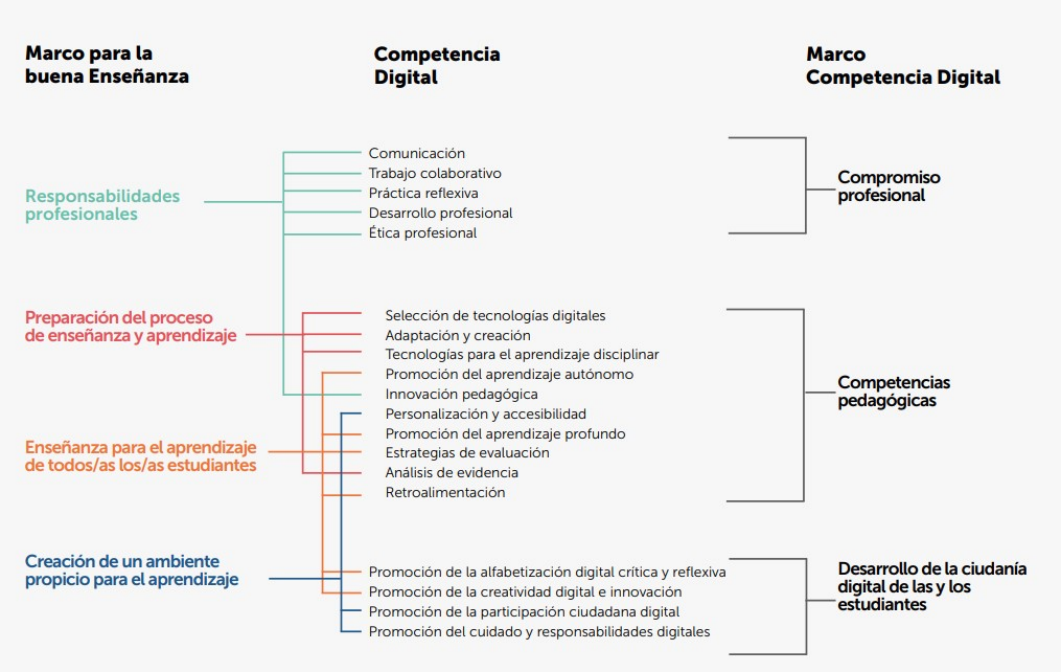


Figura 2: Competencias digitales identificadas
Fuente: Marco Orientador de Competencias Digitales Docentes MINEDUC.

La implementación de este marco en la formación inicial docente plantea la incorporación de las competencias en el uso de las tecnologías digitales de manera integral durante su formación, adheriendo cursos y talleres en mallas curriculares, reconociendo los avances en tales tecnologías (awareness), comprendiendo su importancia en el marco educativo actual y su aplicación en contextos de enseñanza. De igual manera, destaca la importancia de desarrollar diagnósticos de entrada para reconocer las competencias digitales de los docentes y así abordarlos en su formación inicial.

3.2.6. Índice de Madurez en Ciberseguridad Iberoamerica - Metared

El informe destaca, entre sus conclusiones, la relevancia de evaluar constantemente el estado y la madurez en ciberseguridad de las instituciones de educación superior como herramienta clave para identificar brechas, espacios de mejora y mitigar riesgos MetaRed (2024), destacando la medición como aspecto primario necesario para la mejora continua y fortalecimiento de las capacidades institucionales en seguridad digital. Si bien el índice sitúa a las IES Iberoamericanas en un nivel de madurez básico, destaca los esfuerzos colaborativos y las redes de apoyo entre países, los cuales contribuyen a promover la concientización, integración y distribución de recursos destinados al desarrollo de las competencias digitales y a la gestión de la ciberseguridad en el ámbito universitario.

3.2.7. Estrategia Nacional de Educación y Fuerza Laboral Cibernética - La Casa Blanca

El documento publicado por The White House (2023) destaca cuatro pilares fundamentales para que todas las personas de Estados Unidos tengan las oportunidades de adquirir competencias en ciberseguridad en todos los niveles de educación, algunos de los puntos más destacados de los pilares son los siguientes:

1. **Hacer que cada ciudadano cuente con habilidades cibernéticas**: Promover a los educadores en implementar estas competencias en sus enseñanzas, incluir habilidades digitales fundamentales en marcos, programas y actividades educativas existentes, incorporar conocimientos en ciberseguridad como una responsabilidad social, desarrollar campañas relacionadas para impulsar carreras de ciberseguridad, compartir las habilidades cibernéticas con aliados internacionales y promover el desarrollo de estándares y marcos internacionales relacionados con las habilidades cibernéticas fundamentales.
2. **Transformar la educación cibernética** : Transformar la educación es el primer paso para lograr una fuerza laboral diversa y cualificada, fomentando el aprendizaje «competency based». Integrar la ciberseguridad en todas las disciplinas para preparar a la fuerza laboral y construir sistemas que sean seguros desde el diseño, aumentar la disponibilidad de planes de estudio para programas de educación cibernética, alentar a las universidades a colaborar en crear programas innovadores con apoyo de expertos para aumentar el número de educadores que enseñan habilidades cibernéticas, fomentar enfoques interdisciplinarios para la enseñanza, incorporar la educación y la capacitación en las iniciativas de trayectoria profesional y lograr la accesibilidad a estos programas a la mayor cantidad de personas.
3. **Expandir y mejorar las oportunidades de capacitación laboral:** Ampliar la disponibilidad de acreditaciones de competencias en ciberseguridad a bajo o costo cero.

CAPÍTULO 4
PROPUESTA DE SOLUCIÓN

Ante el creciente impacto de las tecnologías de la información en todos los ámbitos de la ingeniería, y considerando los desafíos asociados a la seguridad de la información planteados tanto para Chile como a nivel mundial, se ha identificado la necesidad de fortalecer la formación en ciberseguridad en el contexto universitario.

4.1. Marco de referencia basado en Descriptores

El presente marco presenta un conjunto de áreas de competencia que agrupan descriptores concretos y medibles, permitiendo evaluar las habilidades y conocimientos en el área de ciberseguridad. Estos descriptores serán creados a partir de una propuesta preliminar de competencias inspirados en marcos de referencia, documentos y recomendaciones estudiadas en el marco conceptual. Luego serán evaluados y relacionados a través de una encuesta de percepción a los estudiantes, la que permitirá evaluar el conocimiento e interés en las competencias descritas.

4.2. Competencias

La propuesta presenta cinco áreas de competencias, que serán una base preliminar sobre los temas que deben ser abordados transversalmente.

Competencias

Conciencia de amenazas y comportamiento seguro

- **Reconocer los principales tipos de amenazas cibernéticas**, como phishing, malware, ingeniería social y ransomware.
- **Identificar vulnerabilidades humanas**, en el contexto de ataques digitales en entornos laborales o académicos.
- **Comprender importancia de la respuesta a incidentes** conociendo pasos básicos de acción frente a los ataques más comunes.

Identidad digital segura

- **Uso de buenas prácticas en creación, almacenamiento y gestión de contraseñas** incluyendo autenticación segura.
- **Reconocer importancia de canales seguros de comunicación**, como uso de VPN, HTTPS y cifrado E2EE en contextos de teletrabajo.

Protección de la información

- **Ser capaz de identificar información personal, sensible y confidencial** en contextos académicos y laborales.
- **Comprender conceptos básicos de cifrado, almacenamiento seguro y respaldo de información**.
- **Distinguir correctamente entre sitios seguros y no seguros**, entendiendo el uso de cookies, rastreadores web y otros.

Ética digital y uso responsable

- **Comprender principios éticos en el uso de datos**, públicos y privados.
- **Utilización responsable de los recursos digitales proporcionados por empresas o empleadores**, respetando políticas de seguridad física y lógica.

Cultura de ciberseguridad y mejora continua

- **Adaptar comportamientos seguros**, fomentando buenas prácticas y una cultura de seguridad y mejora continua entre iguales.
- **Reconocimiento y conocimiento de la importancia de normas y estándares internacionales relacionados a la ciberseguridad**, tales como la familia de normas ISO-IEC 27000 .

4.3. Descriptores

A continuación se definen un listado de descriptores agrupados por áreas que representan las competencias transversales en ciberseguridad, cada uno de ellos permite ser evaluado a través de una o más preguntas de percepción.

Tabla 1: Área 1: Conciencia de amenazas y comportamiento seguro

Descriptor	**Pregunta asociada**
Reconoce amenazas frecuentes como phishing, malware o ingeniería social.	¿Sabes qué es el phishing y cómo identificarlo?
Identifica conductas de riesgo en el entorno digital académico o laboral.	¿Con qué frecuencia tomas medidas de seguridad al navegar por internet?
Comprende la importancia de responder adecuadamente ante incidentes comunes.	¿Qué temas te parecería útil aprender en un curso de ciberseguridad? (ítem: respuesta a incidentes o hackeos)

Tabla 2: Área 2: Identidad digital segura

Descriptor	**Pregunta asociada**
Aplica buenas prácticas en la creación y uso de contraseñas seguras.	¿Con qué frecuencia usas contraseñas seguras (largas, únicas, con caracteres variados)?
Utiliza mecanismos de autenticación robustos, como la verificación en dos pasos.	¿Utilizas verificación en dos pasos (MFA/2FA) en dos o más de tus cuentas digitales?
Reconoce la importancia de canales seguros de comunicación.	¿Qué temas te parecería útil aprender? (ítem: navegación segura, configuración de navegadores, redes Wi-Fi seguras)

Tabla 3: Área 3: Protección de la información

Descriptor	**Pregunta asociada**
Identifica información personal, sensible y confidencial.	¿Crees que deberías aprender sobre cómo proteger tu información personal y profesional?
Conoce y comprende conceptos básicos de cifrado y respaldo de datos.	¿Qué tan familiarizado/a estás con (ítems: cifrado de información, protección de datos personales)?
Distingue sitios web seguros y comprende el uso de cookies y rastreadores.	¿Qué temas te parecería útil aprender? (ítem: navegación segura, configuración de navegadores)

Tabla 4: Área 4: Ética digital y uso responsable

Descriptor	**Pregunta asociada**
Comprende los principios éticos asociados al uso y tratamiento de datos.	¿Qué temas te parecería útil aprender? (ítem: ética digital y uso responsable de la tecnología)
Reconoce la importancia de respetar normas y políticas institucionales.	¿Qué tan familiarizado/a estás con (ítem: uso responsable de dispositivos en ambientes laborales)?

Tabla 5: Área 5: Cultura de ciberseguridad y mejora continua

Descriptor	**Pregunta asociada**
Fomenta buenas prácticas de seguridad entre sus pares.	¿Qué tan importante consideras que es la ciberseguridad para un profesional de ingeniería?
Reconoce el valor de normas y estándares internacionales.	¿Qué tan familiarizado/a estás con (ítem: normas como la ISO 27001)?
Demuestra interés en formarse continuamente en temas de ciberseguridad.	¿Estarías interesado/a en tomar un curso introductorio de ciberseguridad?

4.4. Encuesta de percepción para la medición de Descriptores

La encuesta de percepción fue diseñada a partir de los descriptores con el objetivo de identificar brechas, reconociendo las competencias digitales necesarias para una educación de calidad. En combinación con la información obtenida en los puntos anteriores se listan las preguntas a continuación:

Esta encuesta forma parte de una memoria para diseñar un curso introductorio de ciberseguridad transversal para estudiantes de Ingeniería civil y sus especialidades. Tus respuestas son anónimas y serán utilizadas con fines académicos.

1. **¿Con qué género te identificas?**
    - *Respuesta esperada:* Masculino — Femenino — Otro
    - *Justificación aplicación de la pregunta:* Permite analizar posibles diferencias en interés, percepción o brechas de conocimientos en ciberseguridad según género.
2. **¿A qué campus perteneces?**
    - *Respuesta esperada:* Campus San Joaquín—Campus Casa Central
    - *Justificación aplicación de la pregunta:* Permite identificar diferencias entre campus que puedan influir en el interés o el acceso a formación en ciberseguridad.
3. **¿Qué carrera estás cursando?**
    - *Respuesta esperada:* Ing Civil: Ambiental — en Minas — Eléctrica — Electrónica — Física — Industrial — Informática — Matemática — Mecánica — Metalúrgica — Plan Común— Química — Telemática — Comercial
    - *Justificación aplicación de la pregunta:* Permite diferenciar las respuestas según especialidad y grado de acercamiento a temáticas relacionadas a ciberseguridad, identificando brechas en conocimientos previos, necesidades generales y niveles de interés, contrastando con carreras que abordan ciberseguridad con mayor profundidad.

4. **¿En qué semestre lectivo te encuentras actualmente?**
    - *Respuesta esperada:* Rango [2-11]
    - *Justificación aplicación de la pregunta:* Permite relacionar el avance académico con el interés y exposición de los estudiantes a contenidos en ciberseguridad en su ciclo formativo.
5. **¿Has recibido alguna formación en ciberseguridad durante tu carrera universitaria?**
    - *Respuesta esperada:* Sí, en un ramo obligatorio — Sí, en un curso o taller optativo — No
    - *Justificación aplicación de la pregunta:* Permite conocer el grado de formación previa de los estudiantes directamente, con el objetivo de evitar redundancias en contenidos propuestos.
6. **¿Con qué frecuencia tomas medidas de seguridad al navegar por internet?**
    - *Respuesta esperada:* Siempre — Frecuentemente — A veces — Raramente — Nunca
    - *Justificación aplicación de la pregunta:* Permite evaluar hábitos de los estudiantes en relación a comportamientos seguros, permitiendo abrir posibles áreas de mejora.
7. **¿Sabes qué es el phishing y cómo identificarlo?**
    - *Respuesta esperada:* Sí, completamente — Lo he escuchado, pero no estoy seguro(a) — No
    - *Justificación aplicación de la pregunta:* Evalúa nivel de conocimiento sobre una de las amenazas más comunes, conocidas y relevantes en ciberseguridad, vinculada a la competencia «Conciencia de amenazas y comportamiento seguro».

8. **¿Con qué frecuencia usas contraseñas seguras (largas, únicas, con caracteres variados)?**
    - *Respuesta esperada:* Siempre — Casi siempre — Algunas veces — Nunca
    - *Justificación aplicación de la pregunta:* Permite medir conocimientos sobre contraseñas, incluido en competencia «Identidad digital segura».
9. **¿Utilizas verificación en dos pasos (MFA/2FA) en dos o más de tus cuentas digitales?**
    - *Respuesta esperada:* Sí — No — No sé qué es
    - *Justificación aplicación de la pregunta:* Permite medir conocimientos sobre contraseñas, incluido en competencia «Identidad digital segura».
10. **¿Qué tan importante consideras que es la ciberseguridad para un profesional de ingeniería, independientemente de su especialidad?**
    - *Respuesta esperada:* Muy importante — Importante — Poco importante — Nada importante
    - *Justificación aplicación de la pregunta:* Permite medir la percepción general de la relevancia en ciberseguridad en el ámbito laboral, lo cual es crucial para justificar la necesidad de la aplicación de competencias transversales en etapas formativas.
11. **¿Estarías interesado/a en tomar un curso introductorio de ciberseguridad como parte del plan común de ingeniería?**
    - *Respuesta esperada:* Sí — No — Tal vez
    - *Justificación aplicación de la pregunta:* Evalúa disposición del público objetivo a participar en un curso transversal, permitiendo anticipar su interés en la iniciativa propuesta.
12. **¿Crees que deberías aprender sobre cómo proteger tu información personal y profesional como parte de tu formación?**
    - *Respuesta esperada:* Totalmente de acuerdo — De acuerdo — En desacuerdo — Totalmente en desacuerdo
    - *Justificación aplicación de la pregunta:* Permite medir el nivel de acuerdo respecto a la inclusión de estos temas en la formación académica, perteneciente a la competencia «Protección de la información».

13. **¿Qué tan familiarizado/a estás con los siguientes temas?**

    - *Respuesta esperada:* Escala de 1 (nada familiarizado) a 5 (completamente familiarizado), aplicada a los siguientes ítems:
        - Buenas prácticas con contraseñas
        - Privacidad en redes sociales
        - Cifrado de información
        - Reconocimiento de amenazas como malware o ransomware
        - Uso responsable de dispositivos en ambientes laborales
        - Normas como la ISO 27001
    - *Justificación aplicación de la pregunta:* Permite identificar grado de familiaridad previa de los estudiantes vinculados directamente a las competencias propuestas.

14. **¿Qué temas te parecería útil aprender en un curso de ciberseguridad?**

    - *Respuesta esperada:* (Pregunta de opción múltiple)
        - Cómo detectar fraudes y estafas digitales (phishing, suplantación de identidad)
        - Protección de datos personales y privacidad en línea
        - Ética digital y uso responsable de la tecnología
        - Uso seguro de redes Wi-Fi, navegación segura, y configuración de navegadores
        - Manejo seguro de dispositivos personales y laborales (USB, laptops, móviles)
        - Respuesta a incidentes o hackeos (qué hacer y cómo reportar)
        - Fundamentos de cifrado de datos y cómo se usa en la vida cotidiana
        - Gestión de la identidad digital y autenticación multifactor
        - Introducción a normas y estándares de seguridad como ISO/IEC 27001
        - Principios de seguridad en teletrabajo y acceso remoto
        - Seguridad en redes sociales y control de huella digital
        - Introducción al hacking ético y análisis básico de vulnerabilidades
        - Principios básicos de arquitectura de ciberseguridad en empresas
        - Tecnología Blockchain
        - Inteligencia Artificial aplicada a ciberseguridad
        - Otros (especificar): _____
    - *Justificación aplicación de la pregunta:* Identifica los intereses específicos del público objetivo, permitiendo priorizar los contenidos más valorados y alinear competencias con las expectativas de los estudiantes.

15. **¿Has vivido alguna situación personal o académica relacionada con un incidente de ciberseguridad?**
    - *Respuesta esperada:* Sí (opcional: describir brevemente) — No
    - *Justificación aplicación de la pregunta:* Permite contextualizar la recurrencia de casos en vida cotidiana.
16. **Casilla opcional para adjuntar cualquier comentario**
    - *Respuesta esperada:* (Respuesta abierta)
    - *Justificación aplicación de la pregunta:* Permite recibir comentarios adicionales relevantes a la investigación.

4.5. Diagrama conceptual del Marco de Referencia

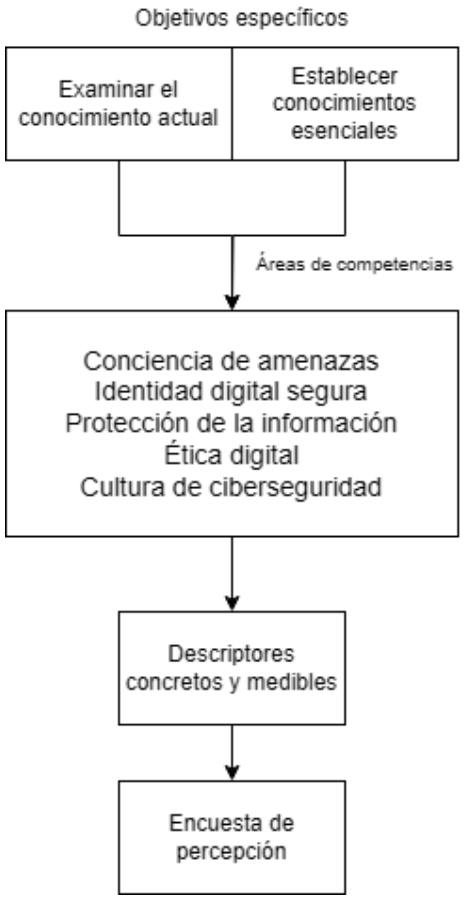


Figura 3: Diagrama conceptual del Marco de Referencia
Fuente: Elaboración propia

4.6. Estructura del Marco de Referencia

La estructura del Marco de Referencia se compone de cuatro elementos, los que permiten su aplicación y evaluación en contextos educativos.

- **Definición de competencias clave:** Identificación de conocimientos de ciberseguridad que deben abordarse transversalmente.
- **Definición de Descriptores observables y medibles:** Competencias definidas como descriptores que permitan ser evaluadas a través de encuestas.
- **Agrupación de Descriptores:** Agrupación de descriptores en áreas de conocimiento dentro de la ciberseguridad.
- **Medición de Descriptores:** Preguntas que permiten medir y evaluar descriptores de manera precisa.

CAPÍTULO 5
VALIDACIÓN DE LA SOLUCIÓN

5.1. Caso de uso aplicado a la UTFSM

El marco de referencia propuesto tiene como objetivo ser una base para la identificación de competencias digitales necesarias para estudiantes de educación superior, a modo de encontrar la validación a el esquema propuesto anteriormente, se aplican todos los puntos del marco al contexto actual semestre 2025-1 de la Universidad Técnica Federico Santa María.

5.2. Definición del Objetivo y Público Objetivo

Esta investigación y propuesta están dirigidas a fortalecer la formación básica en conocimientos de ciberseguridad dentro de la Universidad Técnica Federico Santa María (UTFSM), una institución con una sólida tradición en educación en ingeniería en Chile. La UTFSM cuenta con tres campus principales en Valparaíso (Casa Central) y Santiago (San Joaquín y Vitacura), además de dos sedes en Viña del Mar y Concepción.

El objetivo de la aplicación del marco de referencia en el contexto de la UTFSM es evaluar las habilidades o conocimientos esenciales establecidos por los descriptores propuestos, que demuestra la necesidad de un aprendizaje temprano y transversal en ciberseguridad, complementándolas con el planteamiento de un curso exploratorio que aborde de manera transversal en las distintas carreras las competencias identificadas tras la aplicación del marco incorporado. Buscando garantizar que los estudiantes adquieran competencias esenciales en ciberseguridad, independientemente de su área específica dentro de la ingeniería. Integrando conocimientos actualizados en seguridad digital, alineados con las necesidades actuales y tendencias tecnológicas emergentes.

5.3. Muestra de Estudio

El público objetivo de la aplicación del marco de referencia está compuesto por estudiantes de Ingeniería Civil y sus especialidades, carreras que tienen una duración de diez semestres o más. La selección de este grupo responde a la necesidad de garantizar una aplicación transversal dentro de las distintas ramas de la Ingeniería Civil, asegurando que la ciberseguridad sea vista como una competencia clave en su desarrollo profesional y académico.

5.4. Resultados

Con el objetivo de recabar información sobre la opinión de alumnos de Ingeniería Civil y sus especialidades, se presentan los resultados de la encuesta de percepción dirigida a los campus San Joaquín y Casa Central, que anteriormente fueron seleccionados como caso de estudio. Las respuestas obtenidas permitirán evaluar la pertinencia de agregar, eliminar o modificar competencias en el curso propuesto como solución.

La encuesta se realizó entre el 04-06-2025 hasta el 03-07-2025, contando con un total de **214 participantes** entre los campus San Joaquín y Casa Central, con petición dedicada de difusión a departamentos de Ingeniería Civil Informática e Ingeniería Civil Telemática y participación activa del memorista en obtener respuestas de otras carreras parte del estudio.

5.4.1. Pregunta 1 - Identificación de género

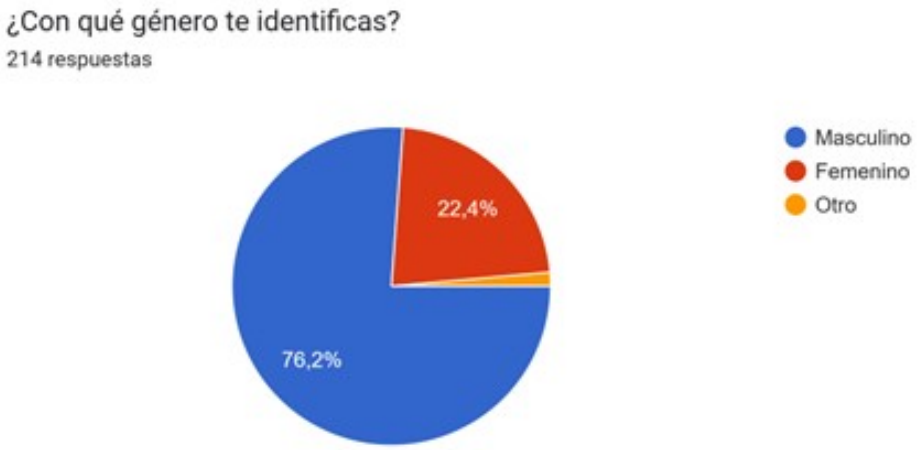


Figura 4: Distribución de géneros en la encuesta
Fuente: Elaboración propia

En la Figura 4 se observa una participación femenina significativa a nivel general que permiten validar su participación en la encuesta. Durante el año 2024, las mujeres representaron el 34 % de los estudiantes admitidos, mientras que a nivel institucional alcanzaron un 28 % UTFSM (2024).

5.4.2. Pregunta 2 - Campus de pertenencia

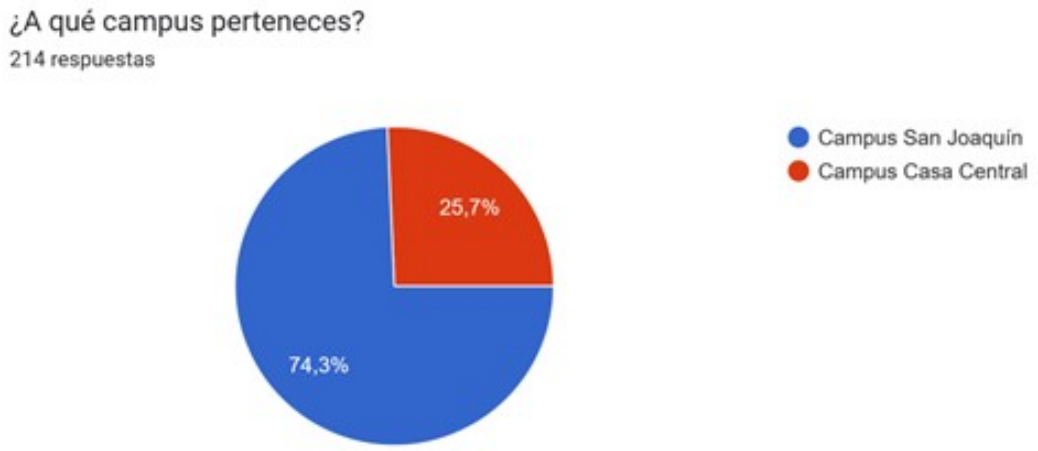


Figura 5: Cantidad de respuestas Casa Central vs San Joaquín
Fuente: Elaboración propia

En la Figura 5 la participación mayoritaria de la encuesta mostrada pertenece a el Campus San Joaquín con 159 respuestas correspondientes a un 74,3 % del total de estudio, la diferencia corresponde a la campaña activa del memorista para obtener respuestas en espacios públicos de la universidad.

5.4.3. Pregunta 3 - Distribución de carreras

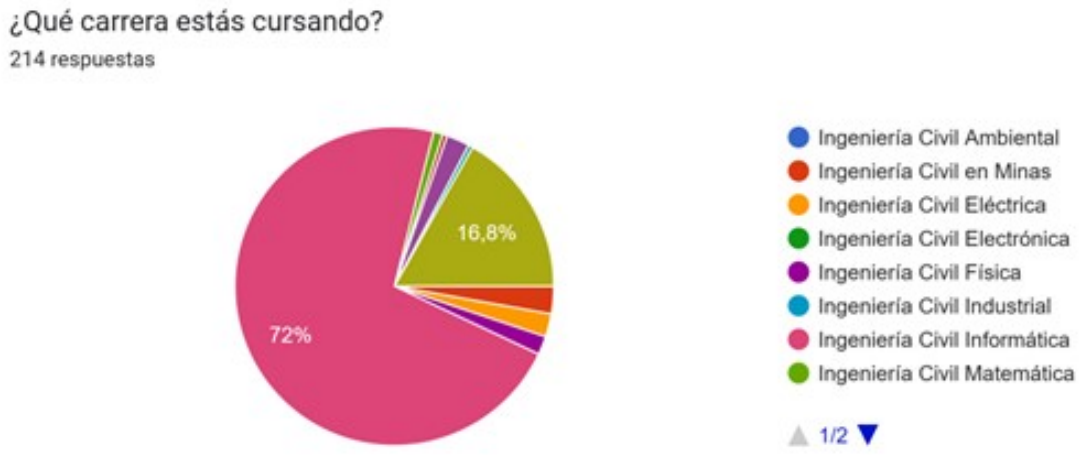


Figura 6: Distribución de alumnos según carreras
Fuente: Elaboración propia

La siguiente Figura 6 contempla una participación mayoritariamente compuesta por estudiantes de Ingeniería Civil Informática (72 %) e Ingeniería Civil Telemática (16,8 %), el porcentaje restante se divide en las Ingenierías Civiles objetivo de estudio. La mayor participación de ambas carreras se debe a petición directa del memorista a los departamentos correspondientes para difusión de encuesta.

▪ 5.4.4. Pregunta 4 - Semestre lectivo actual del estudiante

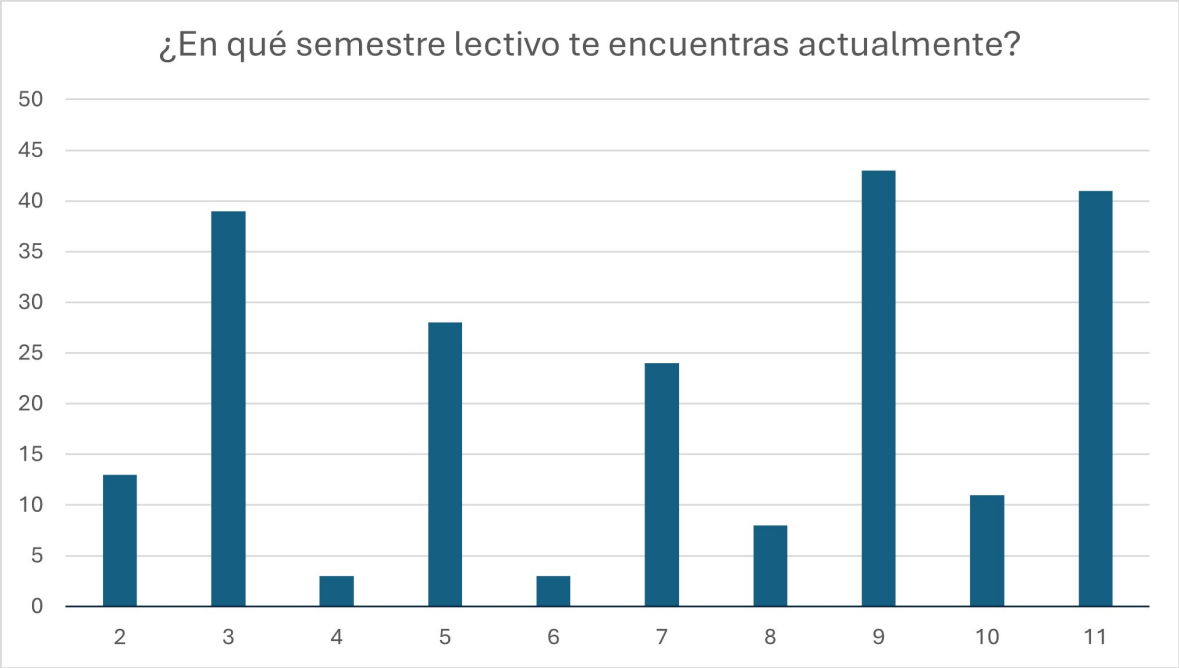


Figura 7: Distribución de semestres
Fuente: Elaboración propia

Se observa en la Figura 7 una participación equilibrada entre todos los ciclos, con mayor cantidad de participantes en semestres impares, esto se debe a que la encuesta se realizó en el semestre 2025-1, todas las respuestas correspondientes a los semestres 3-5-7-9-11 son estudiantes que están al día en sus mallas curriculares o atrasos en cantidad de semestres pares, mientras que los semestres pares tienen atraso en al menos 1 ramo.

5.4.5. Pregunta 5 - Formación previa en ciberseguridad

Figura 8: Formación previa en ciberseguridad
Fuente: Elaboración propia

A continuación, la Figura 8 muestra que, del total de encuestados, un 63,6 % afirma no haber recibido formación en ciberseguridad dentro de su malla curricular, mientras que solo un 16,4 % indica haber cursado un ramo obligatorio relacionado.

Al analizar únicamente las respuestas de estudiantes de Ingeniería Civil Informática, se observa que un 28,38 % ha recibido formación en ciberseguridad de manera optativa y un 9,46 % de forma obligatoria. En contraste, entre los estudiantes de Ingeniería Civil Telemática, un 64,86 % señala haber tenido formación obligatoria en esta materia.

Entre los estudiantes de las demás carreras (excluyendo las ya mencionadas), un 93,75 % declara no haber recibido ningún tipo de formación en ciberseguridad, mientras que el 6,25 % restante indica haberla cursado en un taller o curso optativo.

Con base en los estudios revisados en la sección de Marco Conceptual, los resultados presentan una brecha significativa en el acceso formal a contenidos de ciberseguridad, especialmente en las carreras menos vinculadas a las tecnologías de la información. Esto refuerza tanto el planteo inicial objetivo de la memoria presente como la necesidad de tomar medidas para avanzar en el cumplimiento de los objetivos nacionales establecidos.

5.4.6. Pregunta 6 - Frecuencia de prácticas seguras en ciberseguridad

Figura 9: Frecuencia de prácticas seguras en navegación web
Fuente: Elaboración propia

Tal como se muestra en la Figura 9, gran parte de los encuestados ya posee los conocimientos y el nivel de conciencia necesarios en este ámbito. Por lo que, si bien, se considera importante que los estudiantes mantengan este conocimiento como parte de su cultura digital general, no se estima necesario incluirla como un objetivo específico dentro de las competencias a desarrollar en el curso formativo.

El propósito de esta pregunta es evaluar la pertinencia de integrar la competencia «Protección de la información: Distinguir correctamente entre sitios seguros y no seguros, entendiendo el uso de cookies, rastreadores web y otros» dentro del curso propuesto.

5.4.7. Pregunta 7 - Conocimiento sobre pishing

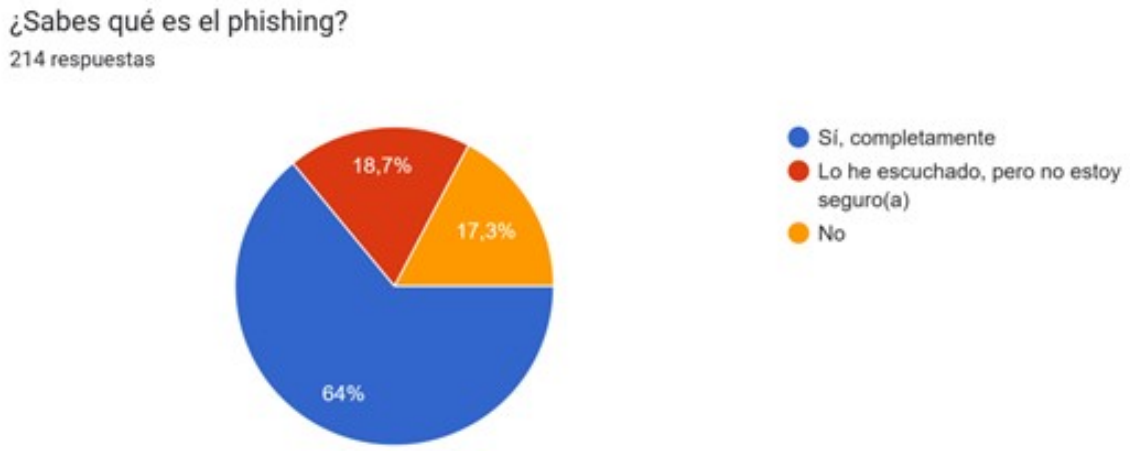


Figura 10: Conocimiento sobre phishing
Fuente: Elaboración propia

La siguiente Figura 10 relacionada con el phishing, evalúa el nivel de conocimiento general sobre este tipo de ataque, considerando que se trata de una de las amenazas más conocidas y que, además, ya ha afectado previamente a la universidad. Los resultados revelan un moderado nivel de conciencia entre los estudiantes, con un 64 % que declara tener un conocimiento completo sobre este tipo de ataque.

5.4.8. Pregunta 8 - Utilización correcta de contraseñas

Figura 11: Utilización correcta de contraseñas
Fuente: Elaboración propia

A continuación, la Figura 11 refleja que los estudiantes poseen un conocimiento suficiente en esta temática, lo que sugiere que dicha competencia no requiere ser abordada desde niveles básicos, sino más bien en un nivel avanzado o complementario. Esta pregunta fue diseñada para evaluar la pertinencia de incluir la competencia «Identidad digital segura» como parte de la formación del curso, considerando su enfoque desde un nivel básico.

5.4.9. Pregunta 9 - Utilización de autenticadores

Figura 12: Uso de verificación en dos pasos (MFA/2FA)
Fuente: Elaboración propia

Al igual que en preguntas anteriores, en la Figura 12 al contar con una gran adhesión por parte de los estudiantes, no se considera pertinente agregar esta competencia para el curso formativo planteado posteriormente.

- **5.4.10. Pregunta 10 - Percepción de la importancia de la ciberseguridad en ingeniería**

Figura 13: Percepción de la importancia de la ciberseguridad en ingeniería
Fuente: Elaboración propia

Los resultados de la Figura 13 reflejan un alto nivel de conciencia sobre la transversalidad de la ciberseguridad incluso en disciplinas alejadas de ella en los futuros ingenieros de la UTFSM, con solo una pequeña fracción que lo percibe como poco relevante.

▪ 5.4.11. Pregunta 11 - Interés del alumnado en recibir formación en ciberseguridad

Figura 14: Interés en cursar formación introductoria en ciberseguridad
Fuente: Elaboración propia

La relevancia analizada en la Figura 14 es dimensionar el interés por cursar un ramo introductorio de ciberseguridad dentro del plan común de ingeniería, considerando que este plan abarca los dos primeros años de formación de los estudiantes de las Ingenierías Civiles en la UTFSM. En este período gran parte de las mallas curriculares comparten asignaturas, incluyendo ramos con enfoque en Competencias Transversales-Sello, como es el caso de programación.

Los resultados entregan una alta aceptación, un 77,6 % del total de encuestados está de acuerdo con incorporar un curso introductorio de ciberseguridad durante su etapa inicial de formación. Segmentando los datos y considerando solo a los estudiantes de cursos superiores (aquellos con 7 o más semestres cursados), el interés se mantiene elevado, con un 74,42 % que estaría dispuesto a tomarlo, mientras que un 21,71 % respondió «tal vez».

Estos resultados sugieren que tanto entre estudiantes que recién inician su carrera como aquellos con mayor experiencia académica, existe una disposición a adquirir competencias en ciberseguridad desde etapas tempranas de la formación profesional. Esto refuerza la pertinencia de integrar un curso de estas características como parte del plan común, siguiendo el enfoque de competencias transversales que plantea la formación inicial de la UTFSM.

- **5.4.12. Pregunta 12 - Percepción sobre la necesidad de formación en protección de la información**

Figura 15: Percepción sobre la protección de la información como parte de la formación
Fuente: Elaboración propia

La Figura 15 demuestra una alta aceptación y permite ser mantenida como un componente a tratar dentro del curso lectivo. Esta pregunta fue diseñada con el objetivo de evaluar el nivel de interés tanto en su etapa estudiantil como profesional, tiene relación con la competencia «Ser capaz de identificar información personal, sensible y confidencial», la que forma parte del ámbito de Identidad Digital Segura.

- **5.4.13. Pregunta 13 - Nivel de familiaridad con temáticas específicas [1 nada familiarizado - 5 completamente familiarizado]**

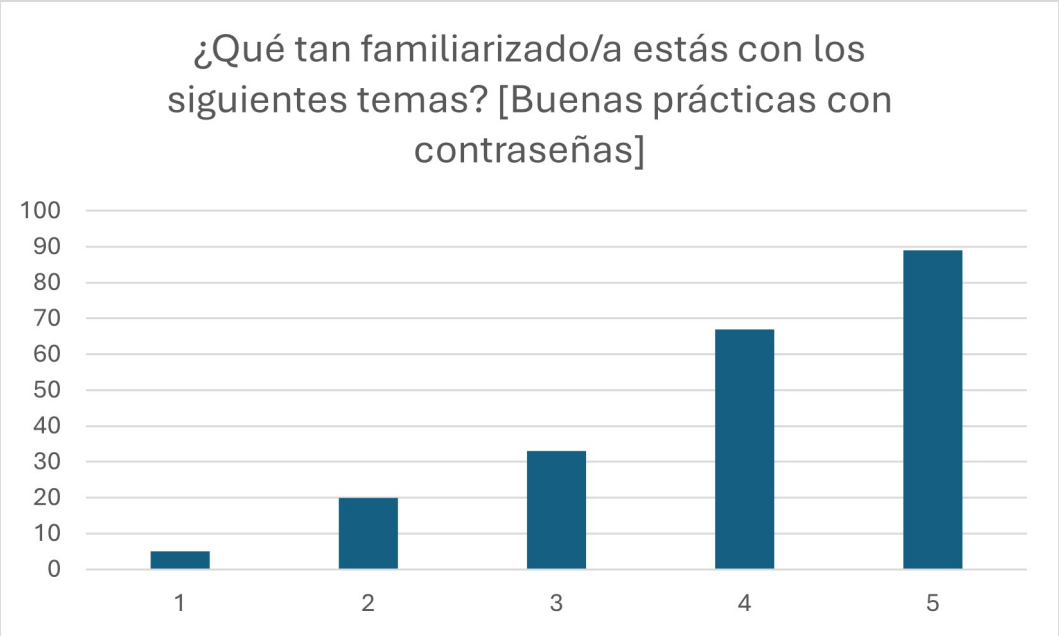


Figura 16: Nivel de familiaridad con conceptos de buenas prácticas con contraseñas
Fuente: Elaboración propia

La Figura 16 demuestra que es un concepto ampliamente conocido por los estudiantes, no justifica aplicación a curso lectivo.

Figura 17: Nivel de familiaridad con conceptos de privacidad en redes sociales
Fuente: Elaboración propia

La Figura 17 demuestra que es un concepto ampliamente conocido por los estudiantes, no justifica aplicación a curso lectivo.

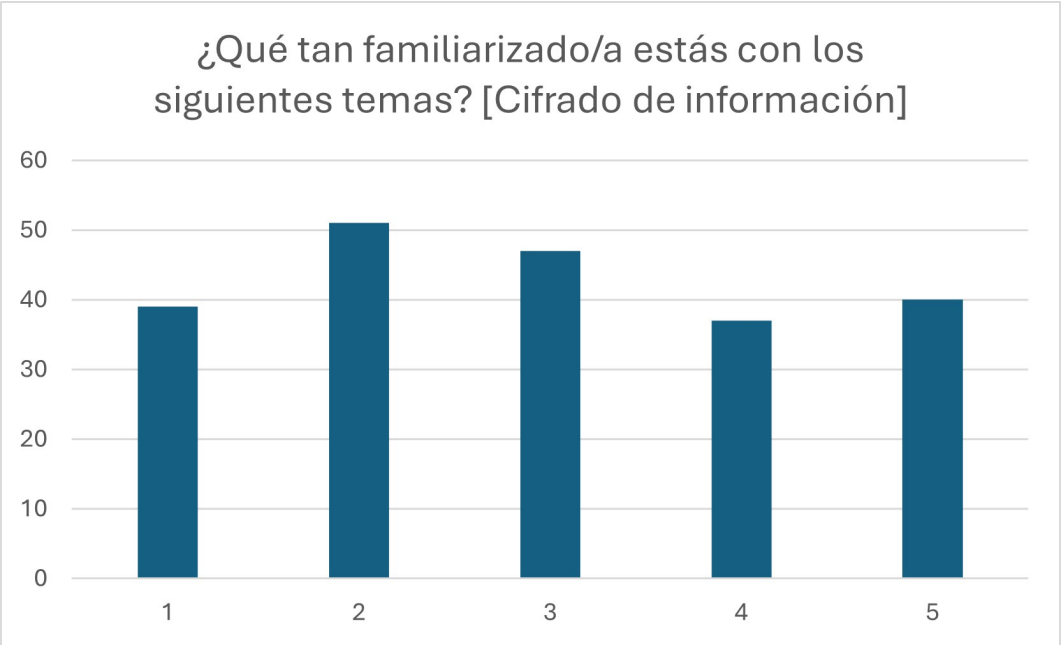


Figura 18: Nivel de familiaridad con conceptos de cifrado de información
Fuente: Elaboración propia

Puede apreciarse en la Figura 18 un equilibrio en las respuestas, reflejando variados grados de conocimiento previo entre los encuestados. Considerando que la mayoría de los estudiantes participantes tienen un alto acercamiento a tecnologías digitales (Ing Telemática e Informática), estos resultados respaldan la incorporación de esta temática en el curso propuesto, aunque con un enfoque introductorio y básico.

La temática cifrado de información es un tema amplio que requiere conocimientos técnicos avanzados en ciertas áreas, aún así, se considera pertinente abordarlo de forma superficial. El objetivo es que los estudiantes logren comprender sus fundamentos, identificar sus aplicaciones prácticas y reconocer los componentes clave que permiten su implementación, de esta manera permite al alumno tener un aprendizaje más familiar y profundo en el futuro.

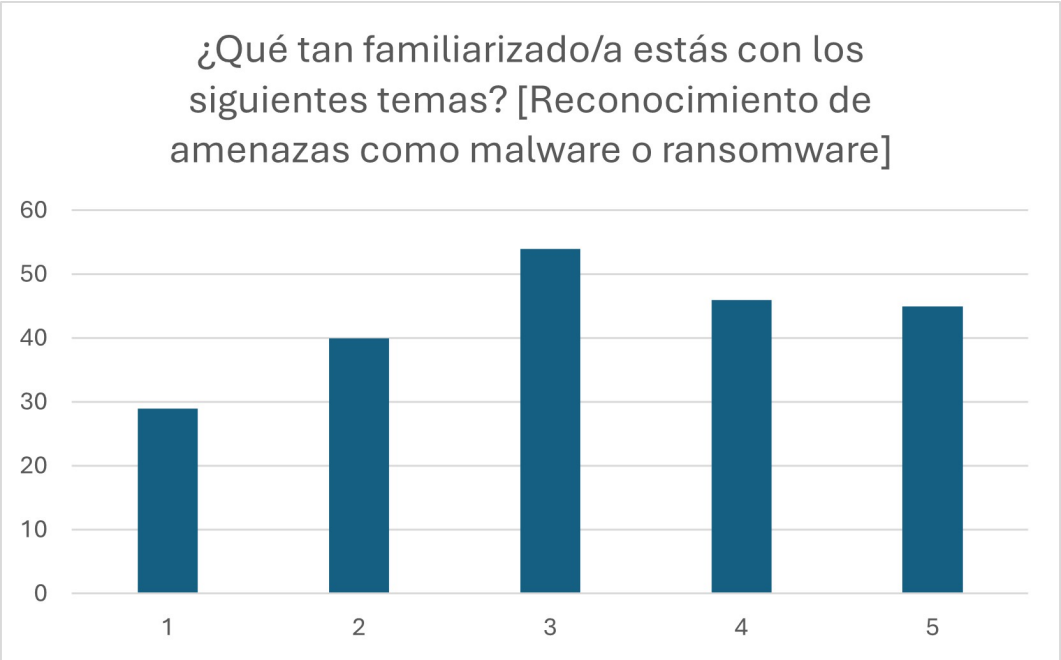


Figura 19: Nivel de familiaridad con conceptos de reconocimiento de amenazas
Fuente: Elaboración propia

A partir de los resultados de la Figura 19, y considerando que se trata de un aspecto básico esencial para la respuesta a incidentes, se confirma la necesidad de integrar este contenido dentro del curso propuesto. El enfoque estará orientado a proporcionar los conocimientos básicos necesarios para identificar amenazas y comprender su impacto, habilitando así una progresión de contenidos natural dentro del curso.

El reconocimiento de amenazas es parte fundamental del «awareness» en ciberseguridad, y se considera como una competencia que los estudiantes deben dominar como parte de su formación, ya que se relaciona directamente con la capacidad de respuesta ante incidentes de seguridad. Las respuestas obtenidas reflejan un nivel de familiaridad medio entre los encuestados.

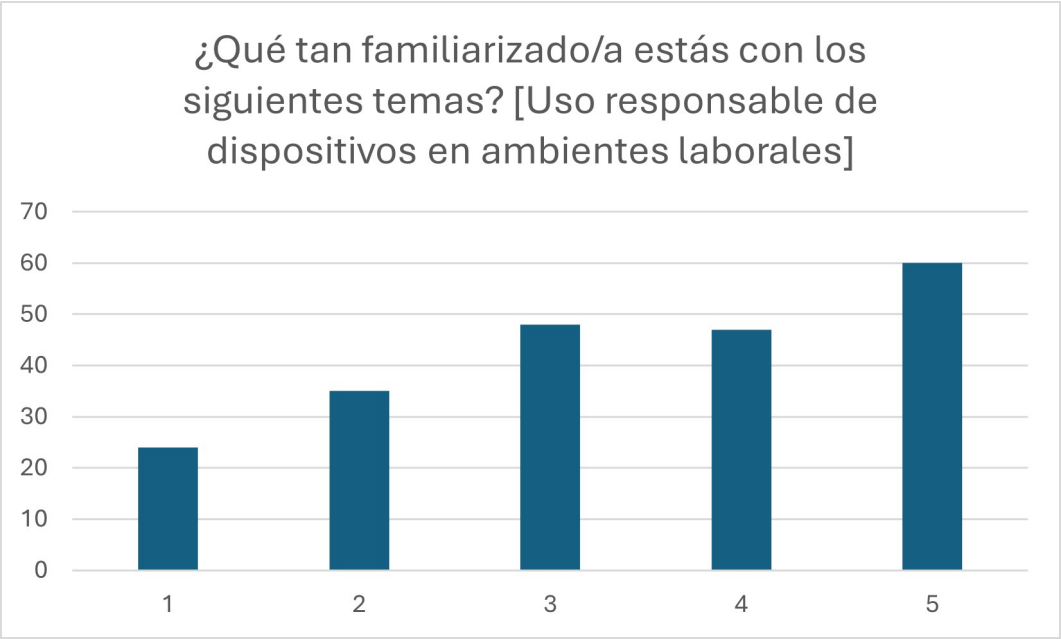


Figura 20: Nivel de familiaridad con conceptos de uso responsable de dispositivos en ambientes laborales

Fuente: Elaboración propia

La Figura 20 presenta un nivel de familiaridad medio-alto entre los encuestados respecto al uso responsable de dispositivos. Sin embargo, destaca que cerca de un 25 % de los participantes manifestó no tener conocimientos al respecto, esto, considerando que la cantidad de encuestados no relacionados a tecnologías digitales es baja, refuerza la inclusión de esta temática dentro del curso propuesto, con el fin de garantizar que todos los estudiantes adquieran una comprensión adecuada de las prácticas seguras en el uso de dispositivos y redes.

El uso responsable de dispositivos en entornos laborales se encuentra vinculado a las competencias de «Adaptar comportamientos seguros» e «Identidad digital segura», abarcando temas como el uso seguro de dispositivos y redes privadas virtuales (VPN). La importancia de reforzar esta temática durante la formación de los futuros profesionales radica en que establece una base para que los estudiantes cuenten con los conocimientos mínimos necesarios al momento de enfrentar sus prácticas industriales y profesionales. Esto resulta particularmente relevante en el contexto actual, donde gran parte de los trabajos ofrecidos contienen teletrabajo a tiempo completo o híbridos.

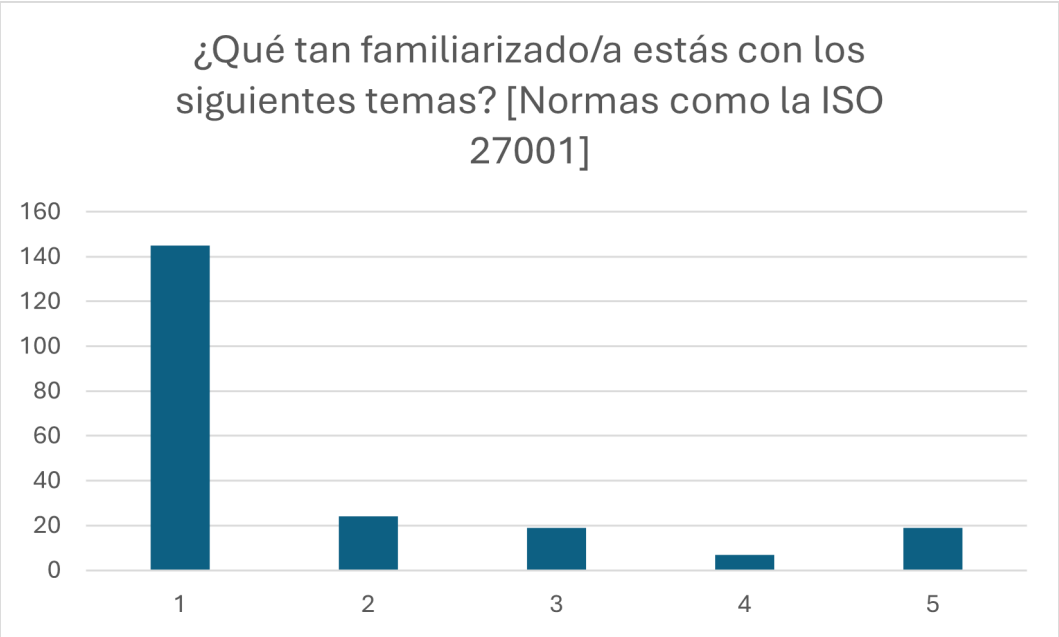


Figura 21: Nivel de familiaridad con conceptos de normativas ISO
Fuente: Elaboración propia

Los resultados obtenidos en la Figura 21 muestran que cerca de la totalidad de los encuestados no posee familiaridad con las normas ISO ni con marcos normativos relacionados. Respaldando la incorporación de esta temática en el curso propuesto, con un enfoque introductorio que permita a los estudiantes identificar las principales normativas y entender su rol en la cultura de ciberseguridad.

La implementación detallada de normas como la ISO 27001 no forma parte de las competencias específicas que se espera desarrollar en la formación de un ingeniero, ya que existen certificaciones profesionales especializadas para ello, pero es fundamental que los estudiantes reconozcan las principales normas de referencia en el ámbito de la ciberseguridad. El objetivo es que comprendan su importancia y adquieran una visión general de su aplicación en entornos profesionales, especialmente en los relacionados con la protección de la información y la gestión de riesgos.

5.4.14. Pregunta 14 - Percepción de temas de interés en ciberseguridad

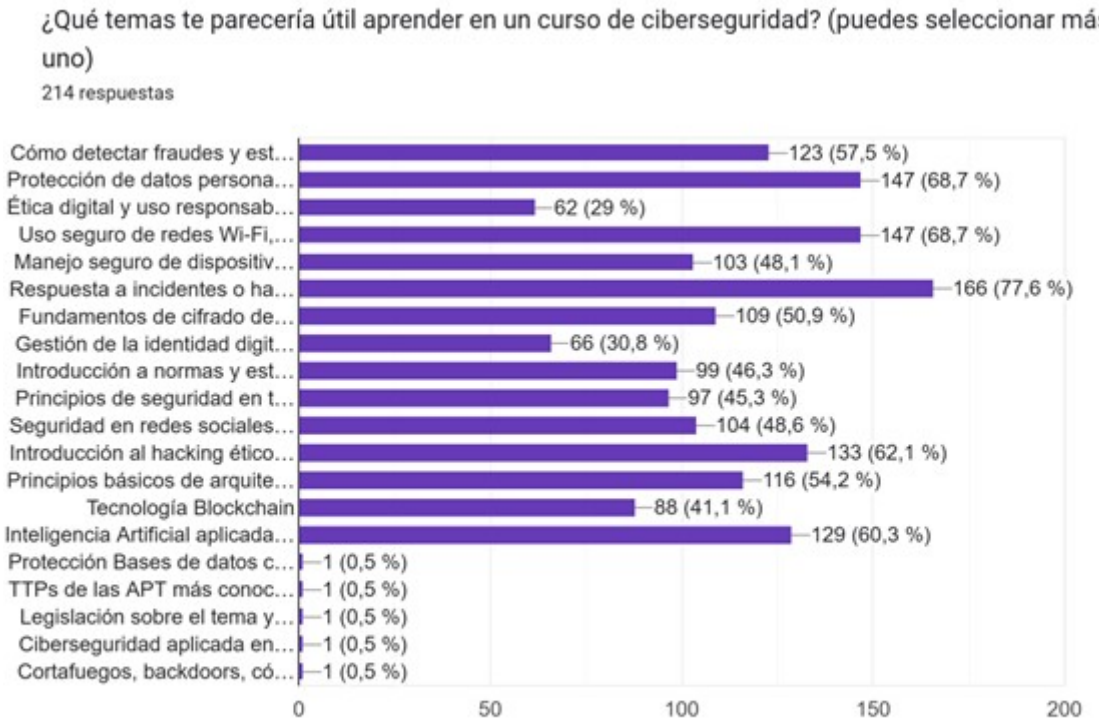


Figura 22: Temáticas que los estudiantes consideran útiles en un curso de ciberseguridad
Fuente: Elaboración propia

En la Figura 22 las opciones que cuentan con un porcentaje menor o igual a 45 % se clasifican como aquellas que no cuentan con el interés general del alumnado y tienen baja prioridad de inclusión. Las que corresponden a:

- Ética digital y uso responsable de las tecnologías
- Gestión de la identidad digital y autenticación multifactor
- Tecnología Blockchain
- Principios de seguridad en teletrabajo y acceso remoto

Las opciones que cuentan con un 0,5 % corresponden a temáticas propuestas por encuestados, las que no serán seleccionadas por los siguientes motivos:

- **Protección Bases de datos contra DDos o parecidos**: Implica conocimiento en una temática no abordada por la totalidad de las ingenierías, pero es integrado en el entendimiento sobre ataques de denegación de servicios.
- **Legislación y desarrollo seguro de aplicaciones**: No aplica al contexto en el que se quiere aplicar de manera introductoria, ya que el desarrollo de software solamente está presente en carreras específicas y en cursos más avanzados.
- **Ciberseguridad aplicada al desarrollo seguro de aplicaciones**: Descartada por el motivo anterior.
- **Cortafuegos, backdoors, como defenderse contra amenazas en desarrollo de software**: Cortafuego y backdoors son consideradas en otras competencias ya aplicadas al curso, mientras que las amenazas en desarrollo son una temática que deben tratarse en desarrollo seguro no aplicable al entendimiento de este curso general.

Las temáticas que se encuentran en el rango de 45 % a 60 % se clasifican como temas complementarios relevantes para los alumnos y pueden llegar a tener inclusión, se detallan a continuación:

- **Cómo detectar fraudes y estafas digitales**
- **Manejo seguro de dispositivos personales y laborales**
- **Fundamento de cifrado de datos**
- **Introducción de normas y estándares de seguridad**: Tema anteriormente relacionado como desconocido a los estudiantes que muestran interés en abordar.
- **Principios de seguridad en teletrabajo**
- **Seguridad en redes sociales y control de huella digital**
- **Principios básicos de arquitectura de ciberseguridad en empresas**

Las temáticas que lograron 60 % o más cuentan con la mayor aceptación e interés entre los alumnos y serán añadidas al curso lectivo, corresponden a las siguientes:

- **Protección de datos personales y privacidad en línea**
- **Uso seguro de redes y navegación segura**
- **Respuesta a incidentes**
- **Introducción al hacking ético y análisis de vulnerabilidades**
- **Inteligencia artificial aplicada a ciberseguridad**: con un 60,3 % de apoyo y considerando que en el estudio de memorias en San Joaquín refleja una alta afinidad a temas relacionadas a inteligencia artificial, demuestra un interés mayor en sus nuevas aplicaciones.
- **TTPs de las APT más conocidas**: Temática aportada por un alumno, las TTPs corresponden a las Tácticas, Técnicas y Procedimientos que utilizan los grupos «Advanced Persistent Threats» para llevar a cabo ataques, dicho de otra manera, introducir la matriz de MITRE ATT&CK para dar a conocer las TTPs más comunes. Esta temática se relaciona a la introducción al hacking ético y análisis de vulnerabilidades.

5.4.15. Pregunta 15 - Experiencias previas con incidentes de ciberseguridad

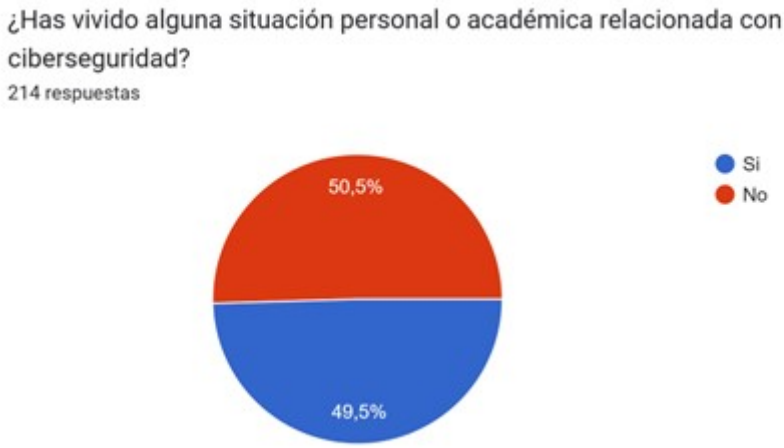


Figura 23: Experiencias previas con incidentes de ciberseguridad
Fuente: Elaboración propia

En la figura 23, notamos que la mitad de los estudiantes declara ya haber experimentado problemas relacionados a la ciberseguridad, confirmando que no es un tema ajeno a la realidad de la universidad. Además, un 50 % revela que existe un nivel considerable de exposición a riesgos digitales que necesitan ser prevenidos o mitigados en futuros incidentes.

5.4.16. Categorización de Competencias Actualizadas

En esta sección se presentan **todas las competencias** consideradas en este estudio como esenciales para el conocimiento transversal de estudiantes de Ingeniería Civil de la UTFSM, junto con su respectiva descripción detallada. A partir de este conjunto, se seleccionarán aquellas competencias y sus respectivos desgloses de temáticas que resulten más relevantes para el contexto actual nacional y de la universidad, según los criterios de análisis y las investigaciones expuestas en las secciones anteriores. Estas competencias seleccionadas constituirán la base para el diseño de los contenidos del curso lectivo propuesto.

1. **Competencia:** *Conciencia de amenazas y comportamiento seguro*
    - **Descripción General:** *Reconoce los principales tipos de amenazas cibernéticas, comprendiendo los riesgos que representan para el entorno académico y laboral. Fomenta un comportamiento preventivo y proactivo ante posibles incidentes digitales.*
    - **Objetivo de aprendizaje:** *Ser capaz de identificar amenazas digitales comunes como phishing, malware, ingeniería social y ransomware.*
    - **Aplicación en área de Ingeniería:** *Prevención de riesgos en el ámbito universitario y laboral.*
    - **Nivel de profundidad:** *Medio – Obligatorio para todos los estudiantes en su formación inicial.*
2. **Competencia:** *Identidad digital segura*
    - **Descripción General:** *Promueve la protección de la identidad digital mediante el uso responsable de contraseñas, autenticación y canales seguros de comunicación.*
    - **Objetivo de aprendizaje:** *Aplicar buenas prácticas en la gestión de contraseñas y reconocer la importancia de utilizar medios seguros como VPN, HTTPS y cifrado extremo a extremo (E2EE).*
    - **Aplicación en área de Ingeniería:** *Protección de cuentas institucionales, proyectos, entornos de trabajo y redes sociales.*
    - **Nivel de profundidad:** *Básico – Obligatorio para todos los estudiantes en su formación inicial, mencionado para aumentar «awareness».*

3. **Competencia:** *Protección de la información*
    - **Descripción General:** *Practica activamente el resguardo de la información personal, académica y laboral mediante el uso común de técnicas de cifrado, almacenamiento y navegación seguras en su vida diaria.*
    - **Objetivo de aprendizaje:** *Ser capaz de distinguir información sensible, utilizar técnicas básicas de cifrado en la vida diaria y reconocer sitios web seguros, entendiendo conceptos de cookies y rastreadores.*
    - **Aplicación en área de Ingeniería:** *Protección de datos personales e institucionales en contextos laborales.*
    - **Nivel de profundidad:** *Básico – No necesario de implementar para todos los estudiantes en su formación, ya que cuenta con gran adopción inicial.*
4. **Competencia:** *Ética digital y uso responsable*
    - **Descripción General:** *Comprende y aplica principios éticos en el uso y gestión de datos digitales, con énfasis en el respeto por la privacidad y los recursos institucionales.*
    - **Objetivo de aprendizaje:** *Reconocer y aplicar el uso responsable de los datos, respetando las normas establecidas en los ámbitos académicos y profesionales.*
    - **Aplicación en área de Ingeniería:** *Proyectos con datos sensibles, prácticas profesionales, uso de software y sistemas institucionales.*
    - **Nivel de profundidad:** *Básico – No necesario de implementar para todos los estudiantes en su formación, ya que cuenta con gran adopción inicial.*
5. **Competencia:** *Cultura de ciberseguridad y mejora continua*
    - **Descripción General:** *Fomenta la incorporación de la ciberseguridad como parte de la cultura organizacional y personal, en busca de actualización constante frente a nuevas amenazas.*
    - **Objetivo de aprendizaje:** *Adoptar comportamientos seguros, reconocer la importancia de las normativas internacionales y mantener una actitud en busca de la mejora continua en ciberseguridad.*
    - **Aplicación en área de Ingeniería:** *Participación en equipos de trabajo, conciencia de estándares ISO.*
    - **Nivel de profundidad:** *Básico – Obligatorio para todos los estudiantes en su formación inicial.*

6. **Competencia:** *Principios básicos de arquitectura de ciberseguridad en empresas*
    - **Descripción General:** *Comprende los principios fundamentales sobre la organización de sistemas y redes seguras en entornos laborales, considerando controles de acceso y medidas de protección, lo que le permite analizar e identificar infraestructuras seguras en entornos de trabajo.*
    - **Objetivo de aprendizaje:** *Comprender el diseño básico de redes seguras, el acceso basado en roles y los mecanismos de control de identidad.*
    - **Aplicación en área de Ingeniería:** *Comprensión de los sistemas de ciberseguridad implantados en distintos entornos de trabajo*
    - **Nivel de profundidad:** *Introductorio - Recomendado mencionar como conocimiento adicional.*
7. **Competencia:** *Respuesta a incidentes de ciberseguridad*
    - **Descripción General:** *Presenta los conocimientos básicos y conoce herramientas que permitan ayudar a la respuesta efectiva a incidentes de ciberseguridad, con el fin de mitigar el impacto de amenazas digitales en entornos académicos y profesionales.*
    - **Objetivo de aprendizaje:** *Conocer conceptos básicos de análisis y recuperación ante incidentes.*
    - **Aplicación en área de Ingeniería:** *Participar en el desarrollo de cultura en ciberseguridad.*
    - **Nivel de profundidad:** *Medio - Obligatorio, requiere conocimientos de amenazas.*
8. **Competencia:** *Introducción al hacking ético y análisis de vulnerabilidades*
    - **Descripción General:** *Comprende y conoce las técnicas de análisis de vulnerabilidades, como también trabajos, roles y herramientas de hacking ético utilizadas frecuentemente en contextos de aprendizaje.*
    - **Objetivo de aprendizaje:** *Comprender el rol del hacking ético, conocer herramientas básicas (como Kali Linux, Wireshark, OWASP ZAP, MITRE ATT&CK), roles de pentesting y metodología básica de pruebas de seguridad.*
    - **Aplicación en área de Ingeniería:** *Evaluación básica de seguridad en proyectos y análisis de riesgos.*
    - **Nivel de profundidad:** *Medio - Recomendado para integrar conocimientos en distintas áreas de la ingeniería.*

9. **Competencia:** *Inteligencia artificial aplicada a la ciberseguridad*
    - **Descripción General:** *Comprende la utilidad y los riesgos del uso de la inteligencia artificial en ciberseguridad, conociendo cómo estas tecnologías pueden apoyar la detección de amenazas y el análisis de comportamientos sospechosos.*
    - **Objetivo de aprendizaje:** *Reconocer casos existentes de aplicación de IA en casos reales de ciberseguridad, como sistemas de detección de anomalías o análisis de comportamiento.*
    - **Aplicación en área de Ingeniería:** *Comprensión de utilización de soluciones basadas en IA para ciberseguridad en contextos empresariales.*
    - **Nivel de profundidad:** *Básico - Recomendado mencionar brevemente para visibilizar la utilización constante de nuevas tecnologías en ciberseguridad.*

5.4.17. Ordenamiento y Adaptación

En esta sección se presenta la propuesta de un curso introductorio de ciberseguridad, diseñado para ser implementado como curso lectivo obligatorio durante los primeros dos años en las carreras del área civil de las ingenierías presentadas como objetivo. Este curso busca ser reconocido como una Competencia Transversal-Sello, conforme a lo establecido por la Universidad Técnica Federico Santa María (UTFSM).

En el apartado anterior fueron definidas las nueve competencias transversales para los estudiantes de ingeniería de la UTFSM. A continuación, se presenta la propuesta de un curso que aborda los componentes más relevantes de dichas competencias. Aquellas competencias que no se incluyen en esta propuesta han sido excluidas por su simplicidad al no requerir un tratamiento formal en un curso introductorio o bien para facilitar la integración y adaptación del curso a las distintas disciplinas de la ingeniería a las que está dirigido. De manera que cubran las temáticas más demandadas y que cuentan con mayor interés entre los estudiantes.

Curso lectivo

La duración propuesta para el curso corresponde a un semestre académico, contemplando el desarrollo de todos los contenidos en un plazo de 14 semanas. Durante este periodo, se espera integrar tres evaluaciones, cada uno enfocado en medir los conocimientos adquiridos en los tres ejes principales a tratar que compondrán el curso y sus respectivos desgloses, los cuales son los siguientes:

1. **Seguridad de la información**

    - Introducción al ramo, fundamentos de la seguridad de la información e importancia de su implementación en la UTFSM como competencia transversal.
    - Uso, justificación y funcionamiento de VPNs en redes de trabajo.
    - Principales normativas y estándares internacionales aplicables a ciberseguridad (NIST, normas ISO), concepto CIA triad y Ley de protección de datos.
    - Fundamentos básicos de criptografía y cifrado de la información.
    - Cultura organizacional y ética digital en ciberseguridad.

    Competencias transversales asociadas: Identidad digital segura - Protección de la información - Cultura de ciberseguridad y mejora continua - Ética digital y uso responsable.

2. **Amenazas, Análisis de Vulnerabilidades y Respuesta a Incidentes**

    - Clasificación y reconocimiento de amenazas, ataques más comunes con sus respectivas consecuencias.
    - Casos de estudio de ciberataques reales, su impacto y análisis forense.
    - Herramientas, metodologías de análisis, respuesta a incidentes, detección de intrusiones (IDS/IPS, SIEM).
    - Arquitectura básica de redes seguras (conceptos de segmentación de redes y control de acceso).
    - Estrategias de mitigación y respuesta a incidentes para las amenazas más comunes.

    Competencias transversales asociadas: Conciencia de amenazas y comportamiento seguro - Principios básicos de arquitectura de ciberseguridad - Respuesta a incidentes.

3. **Hacking ético, Pentesting e Inteligencia Artificial en Ciberseguridad**

    - Fundamentos del hacking ético y malicioso, roles y metodologías en pruebas de seguridad.
    - Herramientas de pentesting: Kali Linux, Wireshark, OWASP ZAP, MITRE ATT&CK, entre otras.
    - Simulaciones guiadas en entornos controlados.
    - Aplicación de IA para la detección y análisis de amenazas.

    Competencias transversales asociadas: Introducción al hacking ético y análisis de vulnerabilidades - Inteligencia artificial aplicada a la ciberseguridad.

5.4.18. Evaluación y Retroalimentación

Para finalizar la aplicación del marco, se espera proponer una metodología de seguimiento y mejora continua orientada a la actualización de competencias y la adaptación progresiva del curso lectivo. En el caso aplicado a modo de validación del marco de referencia en el contexto de la UTFSM, este proceso ya cuenta con un mecanismo para este punto. Las evaluaciones docentes, realizadas al finalizar cada semestre, recopilan opiniones por parte de los estudiantes facilitando la revisión constante de los contenidos, el desempeño docente y el fortalecimiento de las competencias adquiridas por los alumnos.

Por este motivo, no se considera necesario aplicar de forma recurrente el marco de referencia propuesto en cada semestre. Su utilización en el contexto de la UTFSM se plantea únicamente como un punto de partida, el que se encuentra estrechamente ligado a la evolución del contexto nacional e institucional en materia de ciberseguridad y la eventual identificación de nuevas competencias que requieran ser incorporadas en el curso con el paso del tiempo.

5.5. Análisis de resultados

Una vez terminada la implementación del marco de referencia propuesto para el contexto educativo de la UTFSM, es posible definir un gran listado de temas que los estudiantes perciben como prioritarios pero que no dominan del todo y temáticas que generan mayor interés pero que no se consideran del todo esenciales en marcos de referencia internacionales.

En el entorno del marco de referencia del NICE (Petersen et al., 2020), los resultados obtenidos de la encuesta en estudiantes de la UTFSM revela que las competencias de tipo técnico con menor interés son las leyes, regulaciones, éticas y políticas relacionadas, como también la gestión de la identidad digital como parte importante de su formación, la utilización de este marco de referencia permitió el análisis y posterior inclusión de competencias relacionadas a las capacidades de manejar incidentes de ciberseguridad de las cuales los estudiantes se encontraron mayormente dispuestos a aprender en sus ciclos formativos. Tales competencias más específicas relacionadas a lenguajes de programación no fueron de gran prioridad para la investigación, ya que su inclusión no cubre la premisa de buscar transversalmente el conocimiento en distintas áreas, sino en sectores relacionados con tecnologías de información y no son parte del objetivo planteado inicialmente.

Mientras tanto el marco de roles profesionales (ENISA, 2022) describe principalmente la importancia de la implementación de programas formativos y concienciación en competencias digitales, la formación del marco de referencia nace de la necesidad de fomentar la educación y awareness en personas independiente de su especialidad. Los resultados de la encuesta mostraron una alta adhesión y disposición a ser parte de programas que permitan la inclusión de roles tales como «Cybersecurity Educator», apreciando la implementación de estos roles como necesarios y útiles para su educación.

Nuevamente nombrando el documento publicado por (The White House, 2023), los estudiantes se mostraron de acuerdo en la métodos de aprendizaje por competencias más que los basados en títulos, valorando la transversalidad del programa que ofrece oportunidades para el conocimiento fuera de las barreras establecidas en cada especialidad de ingeniería. De igual manera, la valoración e importancia del rol ciudadano en formarse adecuadamente y formar a ser parte de la ciberseguridad social más allá de lo técnico permiten valorizar la propuesta de la memoria presente en alinearse con los estándares internacionales propuestos en educación digital.

CAPÍTULO 6
CONCLUSIONES Y TRABAJO FUTURO

La presente memoria ha permitido ofrecer un diagnóstico respecto al nivel de conocimiento, interés y percepción que tienen los estudiantes de ingeniería de la UTFSM en torno a la ciberseguridad, así como diseñar y proponer un marco de referencia que mide las competencias transversales para las necesidades actuales y desafíos futuros de la formación profesional. A través de la integración del marco de referencia propuesto en el diseño de la encuesta y el posterior análisis de sus resultados, fue posible evidenciar que, si bien existe un reconocimiento general sobre la importancia de la ciberseguridad en el desarrollo de la ingeniería, también existen vacíos en percepción de la importancia en carreras no directamente asociadas a la informática.

Los objetivos formulados al inicio del trabajo fueron alcanzados. Se diseñó un marco de referencia basado en descriptores concretos y medibles que nos permitieron evaluar el estado actual de las habilidades y conocimientos esenciales en ciberseguridad, con búsqueda de cumplimiento de objetivos provenientes de marcos internacionales reconocidos como el *NIST NICE Framework*, el *ENISA Cybersecurity Skills Framework*, la estrategia estadounidense *National Cyber Workforce and Education Strategy (NCWES)*, *Índices de madurez de Metared*, *competencias digitales del Mineduc*, entre otros. La utilización de la encuesta de percepción logró identificar puntos de coincidencia, discrepancia y oportunidades de mejora. De este modo, se logró establecer una conexión entre la realidad de un caso de uso nacional y recomendaciones globales, de manera que la solución propuesta adapte buenas prácticas internacionales al contexto chileno.

La contribución más importante de esta memoria es la «propuesta de competencias transversales en ciberseguridad», las que fueron clave para crear un curso abordando competencias básicas comunes, fomentando la conciencia digital y preparando a los futuros ingenieros para enfrentar desafíos reales en un entorno expuesto a riesgos. La implementación del curso no responde solamente a necesidades detectadas en los estudiantes, sino que también busca alinearse con los objetivos nacionales establecidos por el Gobierno de Chile y el MINEDUC en su búsqueda por fortalecer las competencias digitales en la educación superior y avanzar hacia una ciudadanía digitalmente preparada.

De igual manera la solución planteada y llevada a cabo en esta memoria cubre gran parte de los objetivos propuestos por el NCSWES (The White House, 2023), una posible implementación de este estudio permitiría probar que no es necesario contar con conocimientos específicos en ciberseguridad para lograr una educación que democratice estos conocimientos en edades aún más tempranas de formación. Como bien destacan los marcos de referencia utilizados, la transformación de la educación es el primer paso para lograr una cultura de la sociedad en competencias digitales, fortaleciendo la fuerza laboral y alentando a más instituciones a crear planes de estudios para programas de formación en seguridad digital, permitiendo el acceso de más personas a la educación basada en competencias.

Respecto a los trabajos futuros, se buscan mejorar e implementar los siguientes aspectos:

- **Implementación del curso lectivo propuesto dentro de las mallas curriculares de Ingeniería Civil y sus derivados:** El propósito de la presente memoria fue plantear un cambio en la UTFSM que permita alinearse con los estándares y objetivos deseados tanto nacional como internacionalmente. Una futura implementación del curso como el propuesto permitiría sentar una base para que la universidad diera el primer paso en generar el cambio.
- **Validar la base del marco de referencia propuesto:** El marco de referencia permite ser flexible para que pueda ser aplicado en distintas áreas de conocimiento e instituciones educacionales, su adopción por parte de ellas permitiría evidenciar el estado actual de cada una y descubrir sus falencias. Al utilizarse en más instituciones, lograría validar la solución como una herramienta robusta y adaptable.
- **Aumentar base de encuestados:** Si bien se logró una gran cantidad de respuestas en la encuesta, por problemas de factibilidad no fue posible obtener una base mínima representativa de respuestas de cada una de las carreras definidas como objetivo. Al obtener estos nuevos puntos de vista e integrar más opiniones de distintos sectores de la industria permitirían lograr determinar de manera más exacta las competencias digitales deseadas y los temas de interés de los alumnos. Así mismo, aumentar la participación de estudiantes de distintos campus, ya que como se evidenció en los resultados de la encuesta, existen diferencias significativas de intereses y conocimientos entre Santiago y Valparaíso.

REFERENCIAS

ANCI, G. d. C. (2023). Política nacional de ciberseguridad.

Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H., and Krathwohl, D. R. (1964). *Taxonomy of educational objectives*, volume 2. Longmans, Green New York.

CPEIP (2021). Marco para la buena enseñanza.

CyberSeek (2024). Cybersecurity career pathways and training. https://https://www.cyberseek.org/index.html.

Dupuis, M. J. (2017). Cyber security for everyone: An introductory course for non-technical majors.

ENISA (2022). European cybersecurity skills framework – role profiles. Technical report, ENISA, Heraklion, Greece.

Fortinet (2022). 2022 cybersecurity skills gap report.

ISC2 (2024). Cybersecurity workforce study 2024.

Merritt, M., Hansche, S., Ellis, B., Sanchez-Cherry, K., Nethery Snyder, J., and Walden, D. (2024). Building a Cybersecurity and Privacy Learning Program. NIST Special Publication SP 800-50r1, National Institute of Standards and Technology.

MetaRed (2024). Índice de Madurez en Ciberseguridad de las IES Iberoamericanas (IMC 2024). https://www.metared.org/global/imc2024.html.

Microsoft (2022). Closing the cybersecurity skills gap: Microsoft expands efforts to 23 countries. https://blogs.microsoft.com/blog/2022/03/23/closing-the-cybersecurity-skills-gap-microsoft-expands-efforts-to-23-countries/.

MINEDUC (2025). Marco orientador de competencias digitales docentes. https://www.mineduc.cl/wp-content/uploads/sites/19/2025/06/Marco-Orientador-de-Competencias-Digitales-Docentes.pdf.

NCSI (2025). ncsi.ega.ee/country/cl/.

OEA (2022). Reporte sobre el desarrollo de la fuerza laboral de ciberseguridad en una era de escasez de talento y habilidades.

on Cyber Expertise, G. F. (2023). About gfce: Global forum on cyber expertise. https://thegfce.org/.

Petersen, R., Santos, D., C, M., Smith, Wetzel, K. A., and Witte, G. (2020). Workforce framework for cybersecurity (nice framework).

Sherman, A., DeLatte, D., Neary, M., Oliva, L., Phatak, D., Scheponik, T., Herman, G., and Thompson, J. (2017). Cybersecurity: Exploring core concepts through six scenarios. *Cryptologia*, 42:1–42.

The White House (2023). National cyber workforce and education strategy. Tech. report.

Thompson, J. D., Herman, G. L., Scheponik, T., Oliva, L., Sherman, A., Golaszewski, E., Phatak, D., and Patsourakos, K. (2018). Student misconceptions about cybersecurity concepts: Analysis of think-aloud interviews. *Journal of Cybersecurity Education, Research and Practice*, 2018(1):5.

Tsado, L. (2019). Cybersecurity education: The need for a top-driven, multidisciplinary, school-wide approach.

United Nations (2025). Sustainable development goals. `https://sdgs.un.org/es/goals`.

UTFSM (2016). Modelo educativo institucional.

UTFSM (2024). Presentan avances y desafíos de la usm en cuenta pública institucional 2024. `https://usm.cl/noticias/presentan-avances-y-desafios-de-la-usm-en-cuenta-publica-institucional-2024/`.

ANEXOS

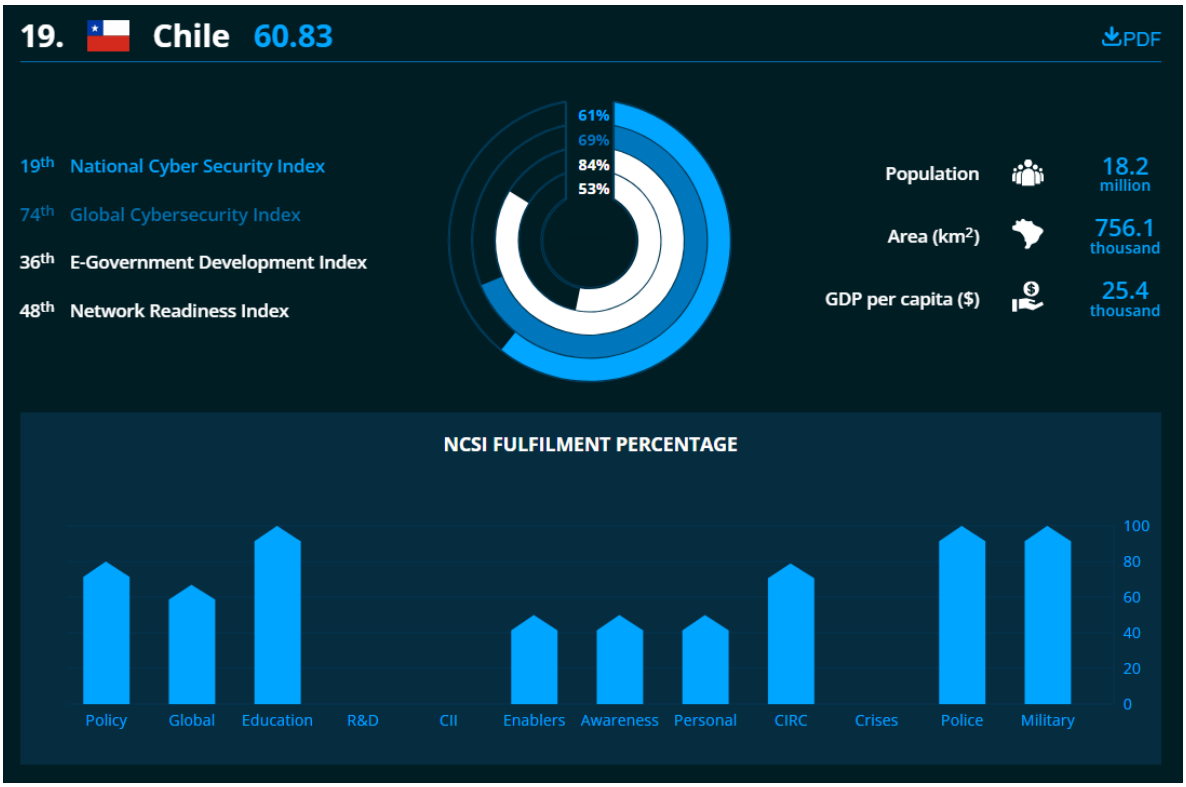


Figura 24: Porcentaje de cumplimiento de Chile Abril 2024
Fuente: National Cyber Security Index

Figura 25: Porcentaje de cumplimiento de Chile Junio 2025
Fuente: National Cyber Security Index

Figura 26: Malla Curricular Ingeniería Civil Informática 2024-1.
Fuente: mallas.labcomp.cl

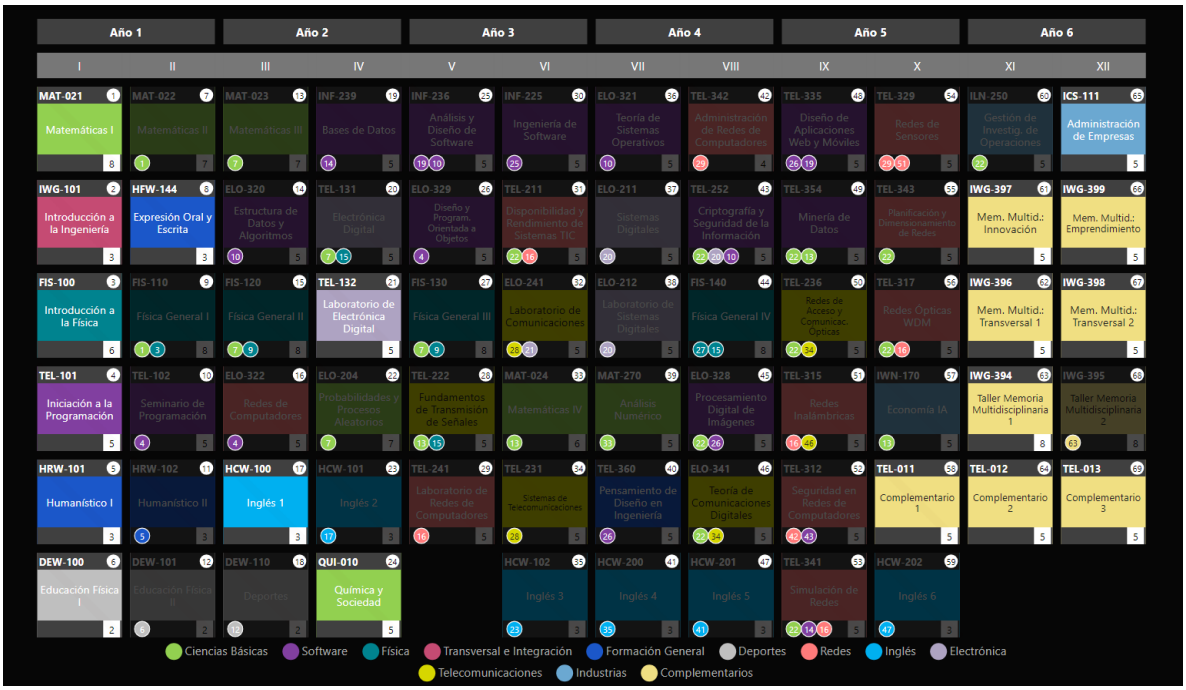


Figura 27: Malla Curricular Ingeniería Civil Telemática 2024-1.
Fuente: mallas.labcomp.cl

Casilla opcional de comentarios recibidos en encuesta

A continuación se presentan algunos de los comentarios más relevantes entregados en la encuesta:

- 'Creo que en este momento de la tecnología, el conocimiento de ciberseguridad debería ser parte base del conocimiento de cualquier profesional competente.'
- 'Sería interesante tener una introducción a la ciberseguridad, al menos dentro de los dos primeros años.'
- 'La verdad es que ciberseguridad es el área de interés en mi estudio, en especial la gestión, normativa y políticas de seguridad, y la ingeniería social, estoy cursando el CEH y tuve acceso al libro CISSP de la ISC2. Aparte de mucha lectura en psicología.'
- 'Me parece súper interesante la iniciativa de un curso de introducción a la ciberseguridad en la malla, así como me llama la atención que existan electivos que profundicen más en el área ya que creo que es algo que tiene mucha importancia sea cual sea el campo en el que uno se especialice luego.'
- 'Creo que es importante enseñar más de la ciberseguridad, pero a un nivel más profesional. Me refiero a algo más que el típico curso que te enseña cosas súper básicas como no hacer click en enlaces extraños. Sería una oportunidad que además nos daría más valor como profesionales en el futuro.'
- 'Súper importante el tema y dentro de la carrera de manera obligatoria es casi nulo el tiempo que se le da.'
- 'Me parecería muy interesante que se lleve a cabo. De no lograrse, seria muy útil que se dicte como electivo o ramo libre.'
- 'Se necesita con urgencia una ramo (o mejor aún, un taller para hacerlo más accesible) de ciberseguridad en la carrera de Ingeniería Civil Informática. Este tema es cada vez más relevante a medida que pasan los años, por lo que será imprescindible saber de éste.'
- 'Considero que el planteamiento de una asignatura de plan común asociada a la ciberseguridad es muy importante, dado que suelen existir casos de personas no relacionadas con el área informática que son víctimas de fraudes y no suelen tener una formación para poder reaccionar correctamente.'
- 'Yo estoy super interesado en talleres de ciberseguridad, pero desconozco si hay ramos que sigan esta linea en Ing. Civil Informática.'