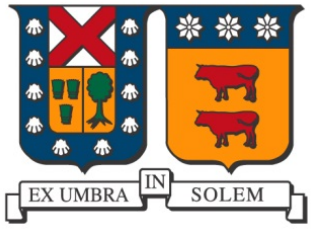
UNIVERSIDAD TÉCNICA FEDERICO SANTA MARÍA
DEPARTAMENTO DE INFORMÁTICA
VALPARAÍSO - CHILE



“DISEÑO, DESARROLLO E IMPLEMENTACIÓN DE SISTEMA DE INDUCCIÓN SOBRE TÓPICOS DE CIBERSEGURIDAD PARA ALUMNOS DE PRIMER AÑO”

JOAQUÍN GALLEGOS ITURRIAGA

MEMORIA PARA OPTAR AL TÍTULO DE
INGENIERO CIVIL EN INFORMÁTICA

Profesor Guía: Gabriel Torres Yarza
Profesor Correferente: Cecilia Reyes Covarrubias

Noviembre - 2024

DEDICATORIA

Esta memoria esta dedicada a todas las personas que fueron parte de mi paso por la UTFSM, sobre todo a mi familia y novia por estar siempre en los momentos en que necesitaba un abrazo para poder seguir adelante.

AGRADECIMIENTOS

Quiero partir agradeciendo a mis padres y hermana, Andrea Iturriaga, Roberto Gallegos y Daniela Gallegos, quienes me apoyaron desde el minuto en que me decidí en estudiar en la UTFSM con tan solo 14 años de edad, gracias por todo, por sus consejos, sus abrazos, sus retos, por cuidarme y protegerme incluso estando a más de 100[Km] de distancia.

Agradecer a mis abuelos, tíos, primos por la preocupación y apoyo dado durante toda mi vida universitaria, el preguntar como iba con la carrera, si necesitaba ayuda en algo. Por todo ello, muchas gracias.

A mi abuelo Oscar Iturriaga que no pudo ser parte de este proceso, debido a que falleció cuando yo tenía 11 años. Él me introdujo en el mundo de la tecnología, en los videojuegos, en las radios de transmisión libre (radioaficionado), de muy chiquito. No sé cuál hubiese sido mi carrera sin todo lo que él me enseñó cuando joven.

A mis amigos de la universidad, Renata Guzmán, Gabriel Díaz, Bruno Liberona, Ignacio Méndez, José Gutierrez, Pablo Voigt y Valeria Gaete. Gracias por todo los momentos vividos, gracias por las salidas, por estar ahí cuando yo estaba mal, cuando pensaba que no podría con el semestre.

A mi profesor guía Gabriel Torres, por haber confiado en mí para el desarrollo de esta memoria y por todos los conocimientos entregados durante este proceso. Además de permitirme ser su ayudante de Seguridad de Sistemas.

A la profesora Cecilia Reyes, cariñosamente llamada tía Ceci. Muchas gracias por los consejos cuando éramos mechones, por las sesiones que realizaba cada 2 meses para preguntar cómo íbamos con la carrera, si nos sentíamos bien, si necesitábamos ayuda en algo.

Agradecer especialmente a mi novia Estefany Silva, muchas gracias amor por tu apañe, por los momentos vividos, por estar ahí cuando más mal estaba, por ayudarme a calmar el estrés de FESW el año 2023, eres mi pilar fundamental y motivación diaria para seguir adelante, para seguir floreciendo juntos.

Muchas gracias a todos, sin su apoyo yo no podría haber llegado a este momento.

RESUMEN

Resumen— Se diseña, desarrolla e implementa un sistema de inducción en ciberseguridad, que contempla diagnóstico y evaluación, mediante 2 *ethicals phishings* y una sesión de clases presencial donde se enseñan los tópicos como las medidas que deben tomar los alumnos, frente a diversos riesgos asociados a los activos de información que usan. Para llevar a cabo este sistema se utiliza Gophish para la gestión de la campaña, *Mailcow* para la gestión de correos y *Kahoot* para una evaluación luego de la inducción. Debido a una configuración del servidor de correos institucional, no fue posible obtener la tasa de éxito de una campaña sin inducción. Por lo que se determina utilizar el promedio de América del Sur obtenido por la empresa KnowBe4 para realizar la comparación con las métricas del segundo experimento, obteniendo en este una tasa de éxito de 8.1 %.

Palabras Clave— Ciberseguridad; Cartelería Social; Phishing; Concienciación; Riesgos;

ABSTRACT

Abstract— A cybersecurity induction system is designed, developed and implemented, which includes diagnosis and evaluation, by means of 2 phishings and a face-to-face induction session where the established topics are taught as measures to be taken by the students, in the face of different risks associated with the information assets they use. To carry out this system, Gophish is used for campaign management, mailcow for mail management and kahoot for an evaluation after the induction. Due to an insitutional mail server configuration, the success rate of a campaign without induction is not obtained. Therefore, it was decided to use the South American average obtained by the company KnowBe4 to compare with the metrics of the second experiment, obtaining a success rate of 8.1 %.

Keywords— Cybersecurity; Social Signage; Phishing; Awareness; Risks;

GLOSARIO

ANCI: Agencia Nacional de Ciberseguridad
AWS: *Amazon Web Services*
CI: Consentimiento Informado
CIA: *Confidenciality, Integrity, Availability*
CISO: *Chief Information Security Officer*
CMEIS:Comisión Asesora de Ética de la Investigación en Salud
CTF: *Capture The Flag*
DGC: Dirección General de Comunicaciones
DGD: Dirección General de Docencia
DHHS: *Department of Health and Human Services*
DI: Departamento de Informática
DTI: Departamento de Tecnologías de la Información
GCE: *Google Compute Engine*
IRB: *Institutional Review Board*
MFA: *Multi Factor Authentication*
NIST: *National Institute of Standards and Technology*
PPP: *Phish-prone Percentage*
SIGA: Sistema de Información de Gestión Académica
UTFSM: Universidad Técnica Federico Santa María

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

El uso de las Tecnologías de la Información se ha vuelto un pilar fundamental en el funcionamiento del mundo, si bien es importante el saber cómo utilizarla, qué se puede lograr con ella, actualmente es igual de importante saber cómo protegerse al usarla. La ciberseguridad es un área que principalmente se centra en como poder proteger los sistemas, pero también en como el usuario se debe proteger.

La concienciación en ciberseguridad, se preocupa de enseñar al usuario técnicas para protegerse de los diversos ciberdelitos, como lo es el robo de credenciales mediante la técnica del *phishing*. Estos tópicos no son exclusivos de un Ingeniero Civil Informático, sino que son transversales a todas las carreras (incluso en la vida diaria), por lo que contar con este tipo de instancias en la formación de ingenieros es completamente necesaria para desarrollar una buena ciberhigiene.

En esta memoria se presenta el diseño, desarrollo e implementación del Sistema de Inducción de Ciberseguridad USM, este sistema satisface la falta de instancias en que se concienciе sobre ciberseguridad en la formación del estudiantado. Para este sistema se realiza un análisis de riesgo para establecer qué tópicos se deben enseñar, se plantean 2 experimentos de *phishing* y una inducción en ciberseguridad. El primer experimento busca generar un escenario inicial con el cual compararse después de realizada la inducción y campaña de socialización, y la ejecución de un 2 experimento.

Sin embargo, se presenta un inconveniente en el primer experimento que no permite obtener datos válidos, por o que para realizar la comparación y evidenciar si hubo o no cambio de comportamiento en e estudiantado, se utiliza como valor de tasa de éxito, el promedio de América del Sur obtenido por la empresa Knowbe4.

Este trabajo se conforma de 5 capítulos. En el *Capítulo 1: Definición del problema*, se presenta el contexto del problema a nivel nacional y de la Universidad, se explica lo que es la ingeniería social y concienciación en ciberseguridad. En este capítulo también se presentan los objetivos, la metodología con la que se aborda la problemática y cuál es el alcance de este.

El *Capítulo 2: Marco Conceptual*, busca realizar una contextualización de la SP 800-50, como está se aplica en una organización con normativas centralizadas y en las etapas de diseño, desarrollo e implementación. Además, se aborda la gestión de riesgo de en la seguridad de la información y las consideraciones éticas y legales que se debe tener al realizar experimentos de *phishing*.

En el *Capítulo 3: Propuesta de Solución*, se realiza la gestión de riesgo, junto con establecer las medidas que deben ejecutar los estudiantes para mitigar cada riesgo. Además, se presenta el diseño, desarrollo y la implementación de este sistema, presentando el proceso de diseño de campañas, correos, páginas, afiches y el material usado en las sesiones presenciales.

En el *Capítulo 4: Validación*, se realiza la comparativa de los resultados de las campañas de *phishing*, debriefing y un impacto económico referente a la ejecución de este sistema a comparación de contratar un servicio de este tipo.

Finalmente, el *Capítulo 5: Conclusiones*, contiene el análisis de los resultados obtenidos en la fase de validación, el análisis del diseño y uso de tecnologías, junto con presentar recomendaciones, trabajo futuro y palabras de cierre del escrito.

CAPÍTULO 1
DEFINICIÓN DEL PROBLEMA

1.1. CONTEXTO

1.1.1. CIBERSEGURIDAD

La ciberseguridad es la disciplina de la informática que vela por la seguridad tanto de las aplicaciones como de la información que se manejan en los servidores de las distintas empresas, servicios bancarios, hospitales, entre otros. Sin embargo, también vela por la seguridad de los usuarios y su información personal, esto se hace mediante capacitaciones, concienciaciones e incluso ciberataques a las personas, esto último con el objetivo de poder obtener un diagnóstico de como es la capacidad de respuesta frente a un ciberataque (comúnmente a un ataque de *phishing*) [Finn y Jakobsson, 2007].

Actualmente, el ser humano es dependiente del uso de dispositivos móviles, computadores de escritorio/portátiles, para trabajar, estudiar, comprar la mercadería del mes, entretenerse, incluso para buscar pareja. Para ser más exactos según un reportaje de *baenegocios.com*, a nivel mundial un 67 % de la población posee un dispositivo móvil (no contempla computadores ni otro símil), donde el principal uso de ellos es la navegación por internet [Negocios, 2021], número que no es para nada despreciable, dado que todos ellos son posibles víctimas de algún tipo de ciberataque.

En septiembre del año 2023 [Welle, 2023] *IFX NETWORKS* fue víctima de un *ransomware*, donde se encriptaron las máquinas virtualizadoras de cuya empresa, donde se encontraban las páginas del Gobierno de Chile, mercadopublico.cl y chilecompra.cl, las cuales son utilizadas principalmente por los entes públicos para realizar las compras de productos y servicios, y los proveedores del estado ofertan a las distintas licitaciones publicadas. Lamentablemente, este hecho afectó al mercado chileno con US$ 2 millones de perdidas según palabras del senador Pugh [Rivas, 2023].

Este ataque a IFX se produce porque se explota alguna vulnerabilidad de sus máquinas virtualizadoras, sin embargo, un 91 % de los ciberataques han comenzado mediante un ataque por ingeniería social, ataque donde la víctima inicial es el usuario, generalmente mediante un correo electrónico falso[Sjouwerman, 2020] o una página web falsa que aparenta ser una verdadera.

1.1.2. INGENIERÍA SOCIAL COMO TÉCNICA

Una de las tantas definiciones que tiene la ingeniería social es la que indica *kaspersky*, "*Es una técnica de manipulación que aprovecha el error humano para obtener información privada, acceso a sistemas u objetos de valor*" [karspersky.com, 2024]. Los ataques por ingeniería social tienen por objetivo el manipular a las personas para que compartan información sensible, descarguen archivos contaminados, entreguen datos bancarios o cometan errores que comprometan tanto la seguridad personal como de la organización en que trabajan.

El *Phishing* es un ejemplo de ciberataque por ingeniería social cuyo objetivo, es incitar a que la víctima ingrese o comparta su información sensible, estos pueden ser datos bancarios, credenciales de los correos electrónicos que la víctima posea, credenciales de servicios que use la víctima, entre otros, a través de un correo electrónico y/o página web aparentemente confiable. Otro método que también se utiliza es que mediante un archivo u orden ejecutada por el usuario en un sitio web, se active un *Ransomware* que encripte y filtre los datos que la víctima posea en su computador.

El mecanismo psicológico principal que utiliza el *phishing* y sus variantes (*vishing y smishing*) es generar sentimientos que alteren el raciocinio de la víctima al momento de recibir un correo, mensaje de voz, o al entrar a una página web "aparentemente confiable", este último tiene como fin el detectar las diferencias respecto a la página web verídica. Generalmente, los atacantes redactan correos donde se le indica a la víctima que perderá el acceso a las cuentas, que sus cuentas bancarias serán bloqueadas o que ganó un jugoso premio, entre otros tipos de mensajes. Los casos anteriormente descritos, suelen generar en las víctimas sentimientos de ansiedad, miedo y estrés (también sentimientos completamente opuestos en caso de que sea algo "bueno") provocando que tomen decisiones apresuradas respecto a qué hacer con sus datos.

La preocupación por los ataques de ingeniería social recae en la reducción que están teniendo los tiempos en que los atacantes obtener acceso a la infraestructura de una organización o sistema de uso personal de la víctima, debido a las credenciales entregadas por esta misma, ya que el atacante podrá atacar desde dentro de la empresa u organización. De esta forma se reduce el tiempo que el atacante debe invertir para acceder a los sistemas, sorteando antivirus y *firewalls*.

1.2. CONCIENCIACIÓN/CONCIENTIZACIÓN EN CIBERSEGURIDAD

La concientización en ciberseguridad según *NIST* en la SP 800-50 [Wilson y Hash, 2003] es un programa que explica como debe ser un buen comportamiento para el uso de la información y los sistemas de la organización. Aquel programa debe contemplar cómo reconocer un problema de seguridad en la empresa y como responder al ataque, protegiendo la información dentro de la empresa, los dispositivos extraibles, y todo lo que sus normas de la seguridad

de la información establezcan.

Un ejemplo clásico es informar qué es el *phishing*, que canal de comunicación se utiliza, las indicaciones de cómo identificarlo, que hacer cuando se detecte y que hacer en caso de ser víctima de él. En la actualidad es completamente necesario el tener una buena cibercultura, o en otras palabras es necesario conocer cómo hacer una buena contraseña, cómo proteger nuestra información personal, nuestros dispositivos y sobre todo cómo identificar cuando estamos frente a un correo, mensaje de texto, *Whatsapp* o sitio web malicioso, por lo que contar con una campaña o curso de inducción sobre este tipo de tópicos no solamente es necesario para un ambiente laboral y/o estudiantil, sino que también en el diario vivir de las personas.

1.2.1. CAMPAÑA DE CONCIENCIACIÓN/CONCIENTIZACIÓN DEL GOBIERNO DE CHILE

En el año 2018 el Gobierno de Chile lanza una campaña de ciberseguridad [MinInterior, 2018] con el objetivo de generar y mejorar la cibercultura del país. La metodología de esta campaña constaba de vídeos cortos de no más de 90 segundos, junto con infografías donde se explican los conceptos de *phishing*, *malware*, ciberseguridad, ciberdelito, cómo crear contraseñas y consejos al momento de realizar descargas en internet, la cual información se encuentra recopilada en el sitio web de conciencia digital.

Esta campaña presentaba cuatro enfoques distintos, para personas mayores en la era digital, para trabajadores en sus puestos laborales, para estudiantes y la ciudadanía en general. Las infografías con enfoque para personas mayores presenta consejos sobre la transformación digital y qué precauciones deben tener al momento de utilizar internet, por ejemplo qué sitios de e-commerce existen, qué trámites pueden hacer en línea, qué es una *fake news*, cómo deben hacer una contraseña segura y que ellos puedan recordar, entre otros consejos.

La campaña enfocada a los trabajadores, se basa principalmente en denominados “ciberconsejos” para el manejo de información en la zona de trabajo, como por ejemplo: no mantener las contraseñas anotadas en papeles en el escritorio, siempre bloquear la sesión cuando no se esté usando el computador de la empresa, el eliminar “definitivamente” los archivos confidenciales una vez ya no tengan utilidad, no hacer mal uso del correo institucional, realizar respaldos frecuentes de la información del computador, entre otros.

Lamentablemente, esta campaña de concientización pasa completamente desapercibida debido a la nula masificación, no apareció en *spots* publicitarios en televisión, tampoco afiches pegados en las calles y ningún otro tipo de difusión, salvo una página web en la cual se recopila todo el material producido sobre ciberseguridad, página que se encuentra en un mal estado, junto con problemas de certificados que validan la veracidad de este sitio (lo cual es contradictorio).

1.3. IDENTIFICACIÓN DEL PROBLEMA

Actualmente, en la UTFSM, se cuenta con una mínima capacitación en ciberseguridad para funcionarios y profesores. Esta se realiza mediante una campaña de *ethical phishing* para seleccionar a qué funcionarios y/o profesores hay que realizar una capacitación, la cual es una charla sobre la robustez, seguridad de las contraseñas, pero no basándose en las normativas de seguridad de información de la universidad. Por otra parte, hacia el estudiante, no existe ninguna instancia en las que se les explique o "capacite"sobre ciberseguridad, ya sea de manera formal en alguna asignatura o coloquial, por ejemplo, un afiche.

Desde el retorno a la presencialidad ha habido un aumento de campañas de *phishing* dentro de la universidad, siendo realizadas por correos de alumnos que fueron víctimas previamente de estos ataques. Si se contara con un sistema de capacitación de ciberseguridad real, estos alumnos no tendrían comprometidas sus credenciales de la universidad. Este problema pone en jaque a toda la infraestructura de la institución, ya que las credenciales de los estudiantes sirven para conectarse a ciertos servicios de la universidad, permitiendo al atacante un ingreso directo a la red interna de esta.

Cabe además destacar el impacto que una capacitación a futuros profesionales puede tener, por su aporte directo al mundo laboral al cual se integrará, a su entorno familiar y social y a su propia persona. Es por ello que es crucial que los alumnos de la universidad tengan un curso, instancia y/o capacitación sobre ciberseguridad en algún momento de su formación y profesional.

En Figura 1 se esquematiza en un árbol, el problema en sí que busca solucionar en esta memoria.

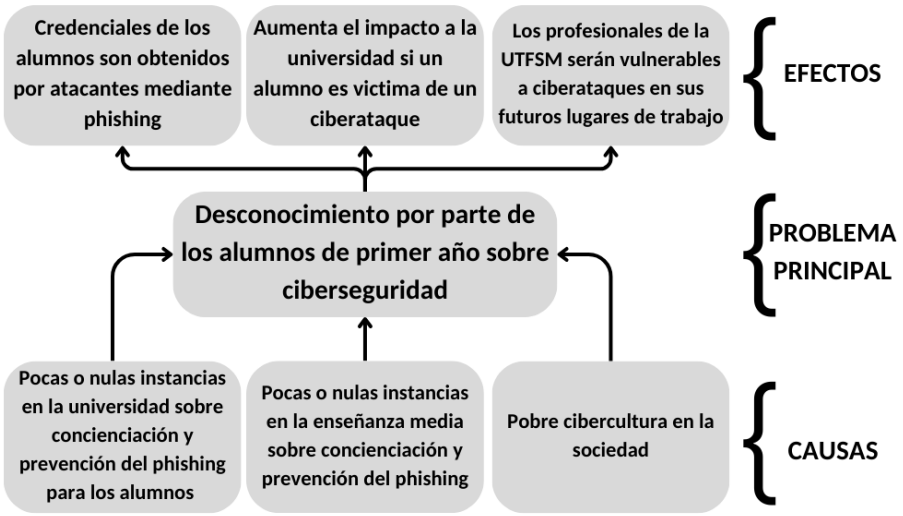


Figura 1: Árbol del Problema.
Fuente: Elaboración Propia.

1.3.1. ACTORES RELEVANTES

En la realización de un programa de concienciación de ciberseguridad se consideran los siguientes actores relevantes:

- ***Managers***: Son los responsables de cumplir los requisitos de concienciación y formación en seguridad informática.
- ***Usuarios***: Grupo de personas que puede ayudar a reducir los errores involuntarios y las vulnerabilidades informáticas. En nuestro contexto acá se encuentran los estudiantes de nuestra universidad.

Según los indicadores institucionales, al año 2024, la UTFSM cuenta con 20.353 estudiantes (19.321 de pregrado y 1.032 de postgrado), todos potenciales víctimas de un ciberataque por ingeniería social.

1.4. METODOLOGÍA

Se contempla comenzar con la realización de un *ethical phishing* a los estudiantes de primer año de Ingeniería Civil Informática, esto con el fin de obtener un diagnóstico de la capacidad de respuesta sin tener una formación previa sobre este tipo de ciberataques. Luego todos los estudiantes de la generación 2024 deberán realizar la inducción de ciberseguridad, esto con el objetivo de que los estudiantes logren tener un piso común sobre las normativas de seguridad de la información de la universidad y sobre como protegerse de los ciberataques por ingeniería social.

Para que la capacitación sea atractiva para el estudiante, esta se realizará contemplando una actividad de carácter competitivo para el cierre de esta. Además, se realizará cartelería social dentro de la universidad donde se mostrarán diversos consejos, recomendaciones y situaciones en los que se transmitirán también los contenidos del curso. Finalmente, se realizará un segundo *ethical phishing* para obtener las métricas de los estudiantes luego de haber realizado la capacitación/concienciación de ciberseguridad.

1.5. OBJETIVOS

Objetivo general: Implementar un sistema de inducción sobre temáticas de ciberseguridad, enfocado principalmente en *phishing* a estudiantes de primer año, que permita disminuir la probabilidad de éxito de este tipo de ataques.

Objetivos Específicos

- Crear una matriz de riesgo para incidentes de seguridad que involucren a estudiantes de primer año.
- Elaborar un plan de acción sobre los tópicos que se enseñarán para mejorar la capacidad de respuesta a este tipo de ataque, junto con mostrarle las consecuencias que podrían tener al momento de ser víctimas de un ciberataque.
- Obtener tasa de éxito de una campaña de *phishing* dirigida a los estudiantes de primer año de Ingeniería civil Informática.
- Obtener tasa de éxito de una segunda campaña de *ethical phishing* post “capacitación” para ver la efectividad del sistema de inducción.

1.6. ALCANCE

Se realiza la evaluación de riesgos de forma teórica, es decir, se analiza que podría pasar si los estudiantes no son capacitados en las temáticas que se abordarán en la inducción,

para ello se utiliza como base la información recopilada del primer *ethical phishing* junto con información recopilada con *stakeholders* e información disponible en internet para llevar a cabo la matriz de riesgo.

Es importante destacar que lo que se busca con esta memoria es sentar las bases para generar un sistema de inducción de ciberseguridad que contemple diagnóstico, educación y comparación, para la formación de los ingenieros de la UTFSM.

Respecto a los alumnos de primer año, se prioriza inicialmente a los estudiantes de Ingeniería Civil Informática, dado que una de las competencias con las que egresan es la ciberseguridad. Se trabaja con los servicios propios de la UTFSM, es decir con los correos electrónicos usm.cl y con el apartado de campañas de *ethical phishing* de Microsoft 356, además del servicio GCE y la infraestructura del DI.

La razón de usar los correos usm.cl como medio de entrega del *phishing*, es debido al poco uso que los estudiantes de nuevo ingreso de informática tienen con los servicios que provee el mismo departamento, además de que la gran mayoría de la información de los ramos, correos y otros servicios lo hacen con el correo institucional.

Debido a un inconveniente ocurrido durante el primer experimento de *phishing*, no se obtiene la tasa de éxito previo a la inducción, por consiguiente se utiliza las métricas de KnowBe4 de América del Sur para hacer la comparación.

CAPÍTULO 2
MARCO CONCEPTUAL

2.1. CONCIENCIACIÓN EN CIBERSEGURIDAD

El uso de la tecnología y la informática se ha vuelto un pilar fundamental en los diversos ámbitos de la vida cotidiana. Las organizaciones públicas y privadas, incluidas las instituciones educativas (como las universidades), cuentan con procesos apoyados la gran mayoría de ellos por algún tipo de servicio informático, los cuales son manejados por distintos tipos de usuarios que requieren variados permisos de accesos para interactuar con dichos sistemas.

Esto implica distintos niveles de conocimiento en lo que a protección de datos y ciberseguridad se refiere, aumentando las probabilidades de que un ataque por vector usuario tenga éxito. Dado lo anterior, por más inversión que se realice para la protección física y lógica de los servidores y dispositivos a fines, no servirá de nada si no se invierte en seguridad para el eslabón más débil, ya que ese eslabón es quien define la seguridad de la organización, generalmente los usuarios [Dash y Ansari, 2022].

2.1.1. DISEÑO DE UN PROGRAMA DE CONCIENCIACIÓN

La publicación especial 800-50 del ***NIST*** establece los siguientes tres conceptos (*Awareness*), entrenamiento (*Training*) y educación (*Education*) [Wilson y Hash, 2003]. La concienciación según esta publicación es “presentar un enfoque principalmente en la seguridad, es decir están enfocadas en presentar a los individuos”(que a partir de ahora se llamará alumno dado el contexto de esta memoria) cuáles son los ciberataques, cómo ocurren, cómo identificarlos y lo más importante en como se debe reaccionar ante estos, un ejemplo de esto es el *phishing*.

El entrenamiento tiene como fin el generar las habilidades relevantes y necesarias para los trabajadores del área TI que permiten al trabajador realizar una función específica, mientras que la educación incorpora las distantes áreas y habilidades de la seguridad de la información.

Al alumno se le debe indicar qué es, cómo ocurre, por cuál medio y qué pistas o indicios hay que detectar para responder de forma acorde a este ataque. En la concienciación, otro aspecto a considerar es la motivación del alumno, es decir que la concienciación no sea de forma aburrida ni monótona, en otras palabras que el contenido de la concienciación sea motivante para que no la abandone a medio camino.

Esta publicación plantea tres etapas para desarrollo de un sistema de concienciación. El diseño del programa incluyendo el desarrollo del programa de concienciación y formación de

seguridad informática[1], el desarrollo del material de concienciación y formación, y la implementación del programa. Al momento de diseñar el programa hay que tener siempre en cuenta la misión de la organización donde se implementará, que apoye a las necesidades de negocio y sea relevante para la cultura y la arquitectura TI que posea. Se debe preguntar: ¿cómo el plan de acción del programa se apega a las normativas actuales de la organización? Para ello existen tres métodos que pueden ayudar en el diseño, desarrollo e implementación:

- Modelo de gestión del programa centralizado.
- Modelo de gestión del programa parcialmente descentralizado.
- Modelo de gestión del programa totalmente descentralizado.

Modelo de gestión del programa centralizado En este modelo, la responsabilidad y el presupuesto de todo el programa de concienciación en seguridad informática se asigna a una autoridad central, como se muestra en la figura 2

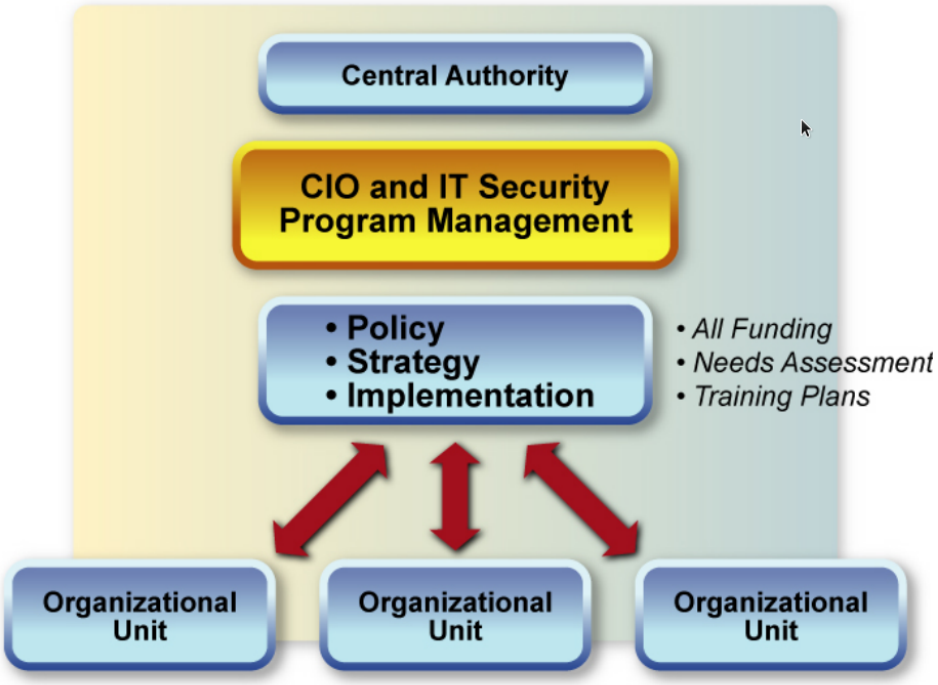


Figura 2: Gestión Centralizada del Sistema
Fuente: NIST SP 800-50

Esta autoridad central está encargada de desarrollar todo lo relacionado con el sistema, debe establecer la estrategia de sensibilización y formación junto con la evaluación de las necesi-

[1]Esto quiere decir el que como se planificarán según el enfoque de la organización.

dades de la organización[2]. Además, debe establecer cuáles y de qué forma se transmitirán los contenidos a los alumnos. Generalmente, el CISO como el director del programa de seguridad están dentro de esta autoridad central, además la institución debe contar con una normativa general de gobernanza de datos las cuales rige toda la orgánica institucional. Como se mencionaba en el capítulo anterior, esta memoria tiene como profesor guía al CISO de la UTFSM, Señor Gabriel Torres Yarza.

2.1.2. EVALUACIÓN DE NECESIDADES

La publicación SP 800-50 define la **evaluación de necesidades** como "proceso que puede utilizarse para determinar las necesidades de concienciación y formación de una organización". Al momento de realizar esta evaluación, es importante que los roles claves participen en ella, por ejemplo:

- **Dirección Ejecutiva**: deben comprender plenamente las directivas y leyes que constituye la base del programa de concienciación.
- **Personal de Seguridad**: deben estar bien informados sobre la política de seguridad y las mejores prácticas aceptadas.
- **Propietarios de Sistemas**: deben tener un amplio conocimiento de las normas y cómo estás aplican a los sistemas que gestionan.
- **Administradores de Sistemas y soporte TI**: deben tener un alto conocimiento técnico en prácticas de seguridad efectivas, además de poseer un alto grado de autoridad en el soporte de operaciones críticas.
- **Operaciones y usuarios de sistemas**: estos individuos deben poseer un alto grado de concienciación y formación en materia de seguridad informática, además de conocer bien las normas que los rigen al momento de hacer uso de los activos informáticos de la empresa.

Para poder obtener estas necesidades se recomienda realizar actividades como, entrevistas con todos los grupos claves y las organizaciones identificadas, realizar encuestas dentro de la organización, revisar material disponible de concienciaciones y formaciones, junto con su programación y su lista de asistentes, analizar las métricas obtenidas en los programas pasados, revisar el inventariado y los ID de los usuarios para saber quién tiene acceso a los servicios, entre otros métodos.

Para realizar de buena manera la evaluación de necesidades se deben establecer un conjunto de métricas para próximamente evaluar el cumplimiento de las metas y objetivos del

[2]Recuerde que en este caso la organización es la Universidad.

programa de concienciación y formación, cuantificando el nivel de implementación, la eficacia y eficiencia del programa de concienciación, para en un futuro realizar mejora continua y seguir aumentando el nivel de seguridad de los individuos y a su vez el de la organización.

Otro aspecto a tener en consideración son los requisitos técnicos que debe cumplir para que se realice de forma expedita, por ejemplo en caso de realizar pruebas de *phishing*, revisar si la red aguanta el tráfico, la capacidad de los servidores puede soportar el envío masivo a las casillas de los alumnos, si hay espacio suficiente en los diarios murales o paredes de la universidad para poder colocar los carteles complementarios de la concienciación (recordar que también se utilizará cartelería social).

2.1.3. DESARROLLO DEL MATERIAL DEL PROGRAMA

Cuando ya se ha diseñado el plan de concienciación se debe tener en cuenta la siguiente pregunta *¿Qué comportamiento se espera reforzar?*. Acá el foco debe estar en que el material diseñado debe incorporarse a las funciones que realizan en este caso los alumnos, es decir, hay que lograr que el material con que el programa se realizará, sea lo más familiar a las tareas que los alumnos desarrollan, como lo podría ser revisar correos electrónicos, crear cuentas en plataformas para el desarrollo de las diversas actividades, tareas y proyectos que realizarán durante la carrera.

La SP 800-50, recomienda en general los siguientes tópicos al momento de desarrollar el material: Creación y gestión segura de las contraseñas, protección de *malware*, *phishing*, uso de la web, uso de los sistemas de la organización (correos, por ejemplo), respuestas a incidentes, utilización de software recomendado por la institución, entre otras recomendaciones. Para la realización de la presente memoria, el énfasis principal estará en *¿Qué tipo de hábitos esperamos que los estudiantes de la universidad posean respecto a la ciberseguridad?* Para ello se usará lo presentado en la publicación del *NIST*, junto con recomendaciones y/o preocupaciones que tengan las autoridades pertinentes a la seguridad de la información de la universidad.

2.1.4. IMPLEMENTACIÓN DEL PROGRAMA DE CONCIENCIACIÓN

Para proceder con esta etapa se deben tener listas las etapas anteriores, es decir, tener vistas las necesidades a cubrir, cómo será la estrategia y el programa de concienciación y, finalmente, el contenido, cómo lo indica la figura 3.

Al momento de implementar el programa se tiene que explicar a las autoridades pertinentes sobre cómo será su implementación y qué recursos se necesitarán, ya sean monetarios, de infraestructura, espacios físicos, entre otros requisitos. Es importante tener en conocimiento las expectativas de las autoridades respecto al programa de concienciación, junto con los

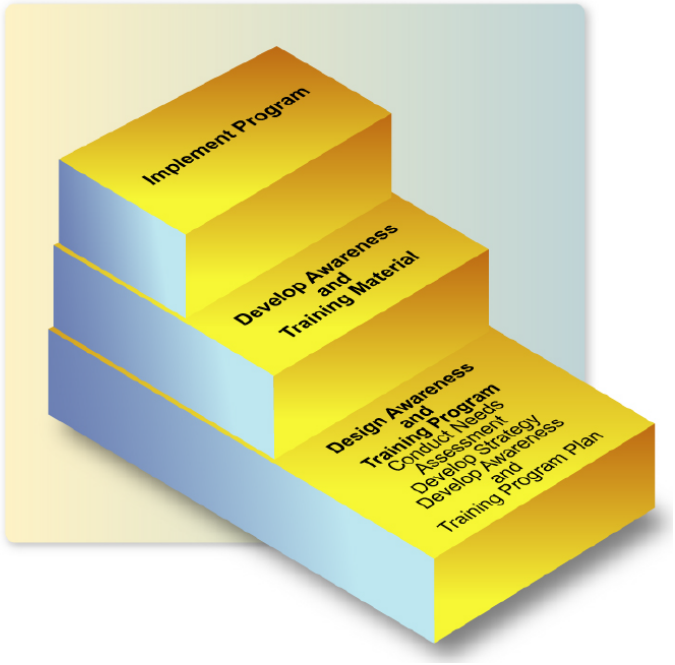


Figura 3: Pasos para la Implementación del programa
Fuente: NIST SP 800-50

resultados esperados y los beneficios de este para la organización, además de establecer una carta gantt de los hitos que se deben cumplir.

Por otra parte, de nada sirve el tener el material del programa si este no es publicado por algún medio, esto puede ser mediante mensajes en útiles de trabajo, en posters, fondos de pantallas, sesiones en persona. La publicación recomienda otros tipos de medio de difusión, pero para el alcance de la memoria se nombran principalmente los que se pretenden utilizar en ella.

2.2. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La norma ISO 27001 [ISO, 2020] establece que la seguridad de la información se debe establecer como eje central de la evaluación de riesgo, esto permite tener una visión para definir el alcance y ámbito de aplicación de la norma. Lo primero es una evaluación del riesgo apropiada para las necesidades de la organización. Esta Norma presenta la siguiente metodología para la gestión del riesgo (Figura 4).

1. Identificar los **activos de información** junto con sus responsables [3].

[3]Activo: aquello que tiene valor para la organización, en este caso la información.

2. Identificar las **vulnerabilidades** de los activos, es decir las debilidades que tienen aumentando su probabilidad de ser afectados negativamente.

3. Identificar las **amenazas** [4].

4. Identificar los **requisitos legales** y contractuales que tiene la organización.

5. **Identificar los riesgos**, se debe identificar la probabilidad de que las amenazas o vulnerabilidades del activo puedan causar daño total o parcial al activo, siempre teniendo en cuenta la tríada CIA .[5]

6. **Cálculo del riesgo**: este cálculo se realiza multiplicando el impacto de la perdida del activo, por la probabilidad de que ocurra la perdida.

7. **Plan de tratamiento del riesgo**, en este punto se establece cómo se tratará el riesgo, acá se selecciona si asume, reduce, elimina y/o se transfiere el riesgo.

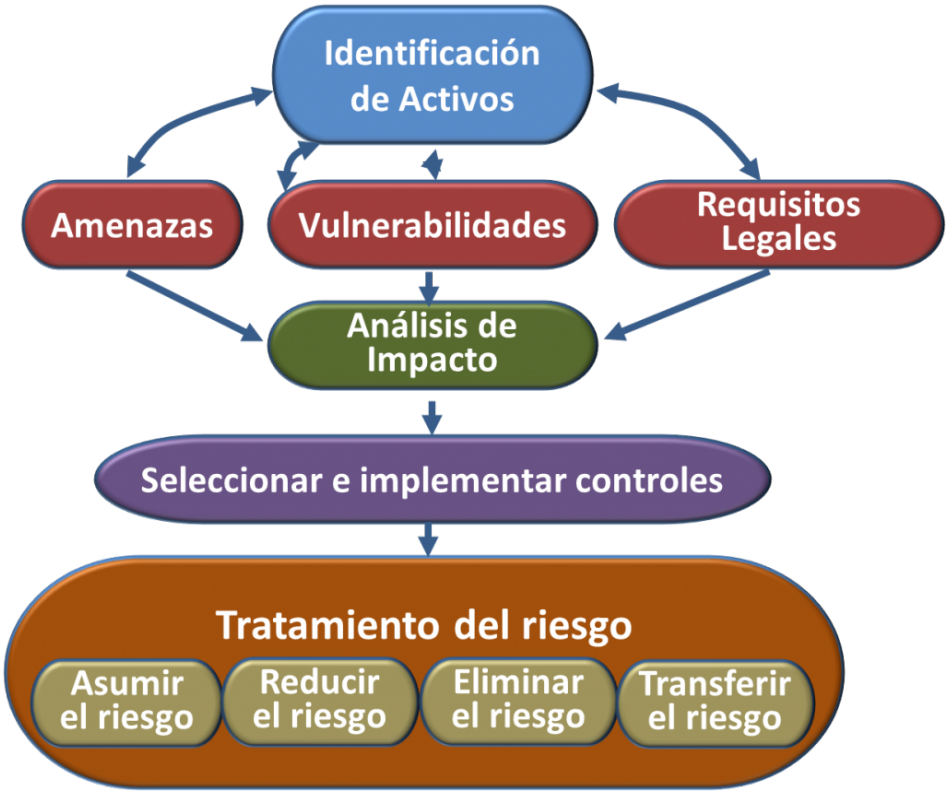


Figura 4: Método de Evaluación y tratamiento del riesgo
Fuente: [ISO, 2020]

[4]Todo lo que tiene la potencialidad de dañar el activo.
[5]C: Confidencialidad, I: Integridad, A: Disponibilidad (Availability).

2.2.1. MATRIZ DE RIESGO

Esta matriz permite representar el riesgo e impacto de que poseen los activos de información de una empresa. La matriz de riesgo contempla cinco niveles de impacto y probabilidad, los niveles de impacto son los siguientes:

1. **Insignificante**: pocas consecuencias.
2. **Menor**: consecuencias manejables con facilidad.
3. **Moderada**: consecuencias tardarán en mitigarse.
4. **Importante**: consecuencias significativas con probables daños a largo plazo.
5. **Catastrófica**: consecuencias muy perjudiciales y puede ser difícil recuperarse.

Respecto a los niveles de probabilidad estos son:

1. Muy improbable
2. No es probable
3. Posible
4. Probable
5. Muy probable

Para obtener el riesgo como se mencionó anteriormente se calcula como $\texttt{Riesgo} = \texttt{Probabilidad} * \texttt{Impacto}$, sin embargo, se debe discretizar en tres niveles de riesgo. Si la multiplicación queda en el intervalo de [1-6] es un riesgo bajo, que no tendrán consecuencias relevantes para la organización, estas se pueden etiquetar como de baja prioridad. En caso de quedar entre [7-12] riesgo medio, generalmente este tipo de riesgos son una molestia para la organización, sin embargo, una vez tomado el plan de acción para la mitigación, el impacto se ve altamente reducido, pero no son una prioridad. Si resulta la multiplicación entre [13-25] estamos en un riesgo alto, este tipo de riesgo posee un gran impacto y una alta probabilidad de que ocurra, por lo que debe ser una prioridad para la organización el mitigar el riesgo, ya que pone en peligro el futuro y funcionamiento de esta.

2.3. EXPERIMENTOS DE PHISHING

El *phishing* es un método en el cual un mensaje ya sea por correo, llamada (*vishing*) o mensaje de texto(*smishing*) fraudulento, es disfrazado para que parezca un mensaje legítimo. Esto con el objetivo de persuadir, presionar y/o manipular para que las víctimas compartan su información personal, credenciales y/o datos sensibles[George A. Thomopoulos y Fidas, 2023].

El *phishing* hace relación a la técnica de la pesca con redes, suponga la siguiente situación: Usted de se encuentra pescando en el mar y lanza una red y con el pasar del tiempo la red se va llenando de pescados. El *phishing* como tal realiza las mismas acciones, lanza la red al mar (envía el mensaje a un universo de correos) y a medida que pasa el tiempo obtiene pescados, que en este caso son las personas que han abierto el correo y comprometido sus datos personales.

El realizar estudios de *phishing* de forma periódica a una institución y/u organización es una buena forma de conocer la capacidad de respuesta de sus integrantes ante este tipo de ataques. Sin embargo, hay que tener consideraciones éticas, legales y psicológicas al momento de planificar, solicitar autorización y realizar el estudio. En los artículos de [George A. Thomopoulos y Fidas, 2023] y [Finn y Jakobsson, 2007] se hace mención de tres enfoques para llevar a cabo los estudios de *phishing*: encuestas, laboratoristas y naturalistas (o estudios de campo).

Uno de los objetivos de los estudios de *phishing*, es obtener la tasa de respuesta o capacidad de identificar los ataques de *phishing*. En el experimento realizado por[Rizzoni, 2022], se realizan tres campañas de *phishing*, en la primera se envían 5223 correos, donde 2657 son correos personalizados *(spear phishing)*. En la segunda campaña se envían 2700 correos personalizados y en la tercera campaña reciben un correo masivo personalizado a 5198 cuentas.

En las tres campañas se miden los siguientes indicadores:

1. Total de correos enviados.
2. Recibido y no abierto.
3. Recibido y abierto.
4. Recibido, abierto, y enlace clickeado.

2.3.1. ENFOQUES DE ESTUDIOS DE PHISHING

ENFOQUE DE ENCUESTAS

Este enfoque utiliza las encuestas y/o entrevistas para recopilar información de los individuos sobre su experiencia ante ataques de *phishing*, brechas de seguridad y/o compromisos

de sistemas y credenciales de acceso personal. Sin embargo, este enfoque presenta 2 debilidades, la primera es que puede sub o sobrestimar el riesgo de los ataques de *phishing* debido a la percepción y el conocimiento por parte de los usuarios sobre este tipo de ataques. La segunda debilidad es que no permite estudiar las características de ataques que no hayan sucedido, ya que se trabaja solamente sobre la experiencia de los usuarios.

ENFOQUE DE LABORATORIO

Este enfoque tiene como objetivo medir la capacidad de detectar *phishing* en las personas participantes del estudio, como una "*prueba sobre phishing*", este enfoque permite poder probar nuevos ataques, ver cómo se comportan los usuarios y qué contra medidas usar para hacer frente a estos nuevos métodos de ataques.

Sin embargo, este método presenta una debilidad. Para poder llevar a cabo este estudio de laboratorio los individuos deben ser informados y avisados sobre las actividades, provocando que su comportamiento sea completamente distinto debido a que están siendo vigilados, provocando que este estudio no sea *ecológicamente válido*[George A. Thomopoulos y Fidas, 2023]. El término ecológicamente válido hace referencia a que los resultados obtenidos puedan probarse en la vida cotidiana, como lo pueden ser situaciones o entornos del día a día de las personas, y la credibilidad de los resultados obtenidos basados en el contexto y lugar que ha sido realizado.

ENFOQUE NATURALISTA (O DE CAMPO)

Este enfoque trata de recrear un ataque de *phishing*, con el objetivo de medir cuál es la tasa de éxito real de uno de estos ataques. Sin embargo, se debe tener un especial manejo ético en este enfoque, dado que se busca replicar un ataque de *phishing* real este debe tener claros indicios de que es un ataque falso, ya que en caso de ser exactamente idéntico a un ataque real, el estudio de *phishing* se convierte en un ataque hecho y derecho. Sin embargo, si la recreación del ataque es demasiado irreal, no se obtendrán los resultados esperados.

Este enfoque a diferencia del enfoque laboratorista si es ecológicamente válida, esto es debido a que el medio por el cual se realiza y la forma es exactamente la misma a como ocurre en la vida real. Por lo que el comportamiento de los individuos será lo más similar a como son en su día a día.

2.3.2. CONSIDERACIONES ÉTICAS

CONSENTIMIENTO, ENGAÑO y *DEBRIEFING*

Al momento de realizar un experimento (sea del tipo que sea) se debe de pedir al sujeto en estudio su consentimiento de participar o no, junto con indicarle qué es lo que se realizará y cómo esto les afectará. Según el informe *Belmont* (informe que indica consideraciones éticas al momento de realizar una investigación que involucre seres humanos) existe una

problemática con el consentimiento informado, cuando la realización de este pone en riesgo de que los resultados obtenidos en la investigación queden invalidados. Sin embargo, con solo indicar a los participantes que algunos aspectos de la investigación se revelarán una vez concluido el estudio basta.

En estos casos solamente se puede realizar si *"(1) si la declaración incompleta en completamente necesaria para lograr los objetivos de la investigación, (2) dentro de la información retenida no existen riesgos que no sean mínimos para los sujetos y (3) existe un plan adecuado para informar a los sujetos, cuando sea apropiado."*[U.S.DHHS, 1979]. Aun así, nunca se debe retener información a cerca de la investigación, en caso de que un participante pregunte de forma directa sobre la investigación, se le debe responder con la verdad.

Los estudios de *phishing* con enfoque naturalista o de campo son el enfoque que más controversia genera, debido a que violan el consentimiento informado por parte de los usuarios y la decisión de ser o no parte de este tipo de estudio. Para que el enfoque sea naturalista, se debe realizar un ataque de *phishing* lo más símil a la realidad posible, por lo que se les debe ocultar cómo serán los métodos de la investigación (comúnmente conocido como engaño).

La ley chilena no contempla el desarrollo de investigaciones sin el CI, sin embargo, se puede generar una autorización, basándose en las pautas de bioéticas internacionales y consideraciones del CMEIS. Para un protocolo de investigación que omita el CI este debe cumplir las siguientes consideraciones [Zúñiga y Zúñiga-Hernández, 2019]:

- La investigación no puede llevarse a cabo sin la extensión de este consentimiento.
- La investigación tuviera un valor social importante.
- La investigación expondrá a riesgos mínimos [6] a los individuos.

Para desarrollar estudios de *phishing* con este enfoque, se debe realizar un proceso llamado *debriefing*. Este proceso consiste en explicar a los individuos que fueron estudiados, que el estudio se realizo, cuál fue su objetivo, la metodología y los resultados obtenidos, además de disminuir los posibles sentimientos negativos generados por la realización del experimento [George A. Thomopoulos y Fidas, 2023, Finn y Jakobsson, 2007]. El proceso de *debriefing* debe ser realizado de manera presencial para obtener una mejor recepción de los participantes. Si además se habla sobre cómo prevenir, detectar y reportar los intentos de *phishing* y se entregan consejos sobre la protección de datos y credenciales, el *debriefing* tendrá resultados positivos duraderos.

[6] El DHHS define el riesgo mínimo como "la probabilidad y magnitud del daño o malestar previsto en la investigación, no son mayores que los que se encuentran normalmente en la vida cotidiana o durante la realización de exámenes o pruebas físicas o psicológicas rutinarias".

CAPÍTULO 3
PROPUESTA DE SOLUCIÓN

3.1. ANÁLISIS DE RIESGO

Cabe recordar que el sujeto principal de estudio en esta memoria es el alumno de primer año de Ingeniería Civil Informática. Como el análisis de riesgo considera elementos externos a los que puede controlar un estudiante de primer año, se realiza a continuación un análisis de los principales activos de uso cotidiano que este actor utiliza en su vida universitaria y a qué vulnerabilidades se puede enfrentar, de tal manera de establecer que acciones proactivas deben tomar los estudiantes para reducir la probabilidad de que un riesgo ocurra.

El análisis de riesgo si bien considera elementos externos a los que puede controlar un estudiante de primer año, cabe recalcar que el sujeto principal en estudio es el alumno de primer año de informática, es decir se analizaron los principales activos de uso cotidiano y que vulnerabilidades pueden tener estos activos cuando lo usa dicho actor.

3.1.1. IDENTIFICACIÓN DE ACTIVOS y VULNERABILIDADES

A todo estudiante de primer año de la UTFSM, se le entrega un nombre de usuario y una contraseña temporal, la cual debe ser cambiada en el primer ingreso al servicio de correo electrónico. Dicho par de credenciales le permite el acceso a todos los servicios que la universidad provee correo institucional, SIGA y AULA (entre otros).

Los activos considerados para el análisis de riesgo son los siguientes:

- Credenciales
- Correo Electrónico
- SIGA
- AULA

La razón de la selección de estos activos es por la importancia que tienen para la vida universitaria, las credenciales permiten el acceso de los estudiantes a todos los servicios web de la universidad. SIGA es el servicio por el cual los estudiantes pueden acceder a leer y modificar su información personal, además de realizar solicitudes de excepción reglamentaria referentes a la continuidad, retiro o cambio de carrera y asignaturas que el estudiante puede cursar. AULA es el servicio web por el cual los alumnos pueden acceder a los contenidos de

las asignaturas que tiene inscrita en SIGA, en este servicio los estudiantes pueden realizar las entregas y algunas evaluaciones rápidas.

En Tablas 1, 2, 3 y 4 se presentan las vulnerabilidades y/o amenazas y riesgos de los activos analizados:

- **Código**: Código de identificación único del riesgo.
- **Amenaza o Vulnerabilidad**: Condición de debilidad o factor externo que afecta al activo.
- **Descripción**: Descripción de la consecuencia que puede tener en el proceso.

Tabla 1: Riesgos de Credenciales
Fuente: Elaboración Propia.

Código	Amenaza o Vulnerabilidad	Descripción
CRED-1	***CONTRASEÑAS DÉBILES***, el estudiante hace uso de contraseñas, fáciles o que no cumplen con los requisitos mínimos de seguridad [7] o son de diccionario [8]	Las credenciales del estudiante están expuestas y los servicios que se usan para acceder también
CRED-2	***ENTREGA DE CREDENCIALES***, el estudiante entrega las credenciales a sus compañeros o terceros (de forma consentida o no)	Las credenciales del estudiante están expuestas y los servicios que se usan para acceder también
CRED-3	***CONTRASEÑAS REUTILIZADAS***, el estudiante utiliza solamente una contraseña para todas las cuentas de él (tanto personales como universitarias)	Las credenciales del estudiante están comprometidas de forma colateral[9]
CRED-4	***CONTRASEÑAS POR DEFECTO***, el estudiante no realiza el cambio de las credenciales predeterminadas	Las credenciales pueden ser encontradas mediante fuerza bruta
CRED-5	***ALMACENAMIENTO INSEGURO***, el estudiante no almacena las contraseñas en un lugar seguro (un gestor de contraseñas por ejemplo)	Las contraseñas son encontradas y usadas por un tercero
CRED-6	***FALTA DE MFA***, el estudiante no utiliza un 2 factores de autenticación	Reduce el trabajo que debe realizar el atacante para tomar el control de la cuenta comprometida

Tabla 2: Riesgos de Correo Electrónico
Fuente: Elaboración Propia.

Código	**Amenaza o Vulnerabilidad**	**Descripción**
EMAIL-1	***PHISHING***, el estudiante interactúa con un correo malicioso	Las credenciales del estudiante son comprometidas
EMAIL-2	***MALWARE EMBEBIDO***, el estudiante descarga un archivo de un correo electrónico desconocido	Información y dispositivo comprometidos
EMAIL-3	***SPOOFING***, el estudiante no identifica el dominio de un correo electrónico entrante e interactúa con él	El estudiante expone sus credenciales
EMAIL-4	***ENLACES MALICIOSOS***, el estudiante no lee o pasa por alto el enlace adjunto en el correo electrónico	El estudiante expone sus credenciales
EMAIL-5	***REALIZACIÓN DE DELITOS***, el correo del estudiante es utilizado para la realización de actividades ilícitas	El estudiante es acusado de ciberdelito
EMAIL-6	***SUPLANTACIÓN DE IDENTIDAD***, el correo del estudiante es usado para actividades que suplanta la identidad	El estudiante es acusado de ciberdelitos
EMAIL-7	***CUENTAS FALSAS EN REDES SOCIALES***, el correo del estudiante es usado para la creación de cuentas de *Instagram* u otras redes sociales	El estudiante es acusado de de ciberdelitos

Tabla 3: Riesgos de AULA Virtual
Fuente: Elaboración Propia.

Código	Amenaza o Vulnerabilidad	Descripción
AULA-1	***ACCESO NO AUTORIZADO***, un tercero ingresa a la cuenta del estudiante sin su consentimiento	Información del estudiante es expuesta
AULA-2	***SUBIDA DE ARCHIVOS NO AUTORIZADAS***, un tercero sabotea un entrega del estudiante afectado	Estudiante obtiene una mala calificación
AULA-3	***RESOLUCIÓN DE EVALUACIONES NO AUTORIZADAS***, un tercero resuelve una evaluación de forma no autorizada por el dueño, afectando negativamente en la evaluación	Estudiante obtiene una mala calificación
AULA-4	***NO CERRAR SESIÓN***, el estudiante no cierra sesión al hacer uso de un computador de uso público	Un tercero accede a la sesión del estudiante

Tabla 4: Riesgos del SIGA
Fuente: Elaboración Propia.

Código	Amenaza o Vulnerabilidad	Descripción
SIGA-1	***ACCESO NO AUTORIZADO***, un tercero ingresa a la cuenta del estudiante sin su consentimiento	Información del estudiante es expuesta
SIGA-2	***MANIPULACIÓN DE DATOS PERSONALES***, un tercero altera los datos del estudiante afectado	Información errónea en el sistema
SIGA-3	***OBTENCIÓN DATOS SENSIBLES DEL ALUMNO***, un tercero obtiene información sensible del estudiante disponible en el sistema	La información sensible del estudiante es expuesta en internet
SIGA-4	***SOLICITUDES ACADÉMICAS POR TERCERO***, un tercero realiza una solicitud de cambio de carrera.	El alumno es cambiado de carrera
SIGA-5	***SOLICITUDES ACADÉMICAS POR TERCERO***, un tercero realiza una solicitud de retiro definitivo.	El alumno queda eliminado de la carrera
SIGA-6	***NO CERRAR SESIÓN***, el estudiante no cierra sesión al hacer uso de un computador de uso público.	Un tercero accede a la sesión del estudiante

3.1.2. CÁLCULO DE RIESGOS Y MEDIDAS

Para el cálculo de la severidad de los riesgos se utilizó una matriz de riesgo con valores de probabilidad de ocurrencia de 1 a 5 e impactos desde 1 a 5 igualmente, estableciendo niveles de criticidad de bajo riesgo a riesgo extremo.

Luego del análisis de los activos y sus respectivos riesgos, se obtuvo los valores de Tabla 5 para cada una de las vulnerabilidades.

Tabla 5: Evaluación de Riesgos de los activos analizados
Fuente: Elaboración Propia.

Nivel de Probabilidad	Nivel de Impacto	Nivel del Riesgo	Riesgos Analizados
Muy Alta	Catastrófico	Riesgo Extremo	CRED-1
Muy Alta	Catastrófico	Riesgo Extremo	CRED-6
Muy Alta	Catastrófico	Riesgo Extremo	EMAIL-1
Muy Alta	Mayor	Riesgo Extremo	CRED-3
Alta	Catastrófico	Riesgo Extremo	AULA-1
Alta	Catastrófico	Riesgo Extremo	SIGA-3
Alta	Catastrófico	Riesgo Extremo	SIGA-5
Alta	Mayor	Riesgo Alto	EMAIL-4
Alta	Mayor	Riesgo Alto	AULA-2
Media	Catastrófico	Riesgo Alto	CRED-2
Media	Catastrófico	Riesgo Alto	EMAIL-6
Media	Catastrófico	Riesgo Alto	AULA-3
Media	Catastrófico	Riesgo Alto	AULA-4
Media	Catastrófico	Riesgo Alto	SIGA-1
Media	Catastrófico	Riesgo Alto	SIGA-2
Media	Mayor	Riesgo Tolerable	EMAIL-3
Media	Mayor	Riesgo Tolerable	SIGA-4
Alta	Moderado	Riesgo Tolerable	CRED-5
Baja	Catastrófico	Riesgo Tolerable	CRED-4
Baja	Catastrófico	Riesgo Tolerable	EMAIL-2
Baja	Catastrófico	Riesgo Tolerable	EMAIL-5
Baja	Catastrófico	Riesgo Tolerable	EMAIL-7

En esta ocasión dado que el actor que interactúa con los activos mencionados no los puede administrar [10], no se establecen controles para la seguridad de los activos en sí, pero si se establecen medidas (Tabla 6) que permitan al estudiante a llevar una mejor gestión y cuidados de los activos de información a su cargo y su información personal fuera de la universidad. Dichos controles son traducidos a consejos y/u obligaciones que el estudiante debe realizar

[10] Esto quiere decir que no puede establecer configuraciones de seguridad, permisos especiales, entre otros.

para aumentar la seguridad de sus activos de información, además de ser la base para los contenidos de las sesiones de inducción de ciberseguridad.

Tabla 6: Medidas para la reducción de probabilidad de que ocurra un riesgo
Fuente: Elaboración Propia.

Número de medida	**Descripción**	**Riesgo Afectado**
MED-1	Cumplir con requisitos mínimos de contraseña	CRED-1
MED-2	No entregar credenciales bajo ninguna circunstancia	CRED-2 EMAIL-5 EMAIL-6 EMAIL-7 AULA-1 AULA-2 AULA-3 SIGA-1 SIGA-2 SIGA-3 SIGA-4
MED-3	No utilizar contraseñas repetidas	CRED-3
MED-4	Cambiar contraseñas por defecto	CRED-4
MED-5	Utilizar un gestor de contraseñas	CRED-1
MED-6	Utilizar un MFA	CRED-1
MED-7	Protocolo de lectura de un correo electrónico entrante	EMAIL-1 EMAIL-2 EMAIL-3 EMAIL-4
MED-8	Utilizar sesión de incógnito en un computador de un tercero	AULA-4 SIGA-5

MED-1: Cumplir con requisitos mínimos de contraseña

Los requisitos mínimos de seguridad para que una contraseña sea robusta, consideran una longitud de al menos 12 caracteres, utilizando alfanuméricos, minúsculas, mayúsculas y símbolos.

MED-2: No entregar credenciales bajo ninguna circunstancia

El entregar credenciales siempre es malo incluso cuando se hace de forma premeditada, esto debido a que quedan más propensas a ser filtradas, en caso de que la persona (o las personas) que entregan las credenciales sean víctimas de *phishing* o robo de datos. En caso de necesitar compartir una contraseña debe ser almacenada en un gestor de contraseñas por el receptor.

MED-3: No utilizar contraseñas repetidas

El utilizar contraseñas repetidas, aumenta el impacto que tendrá el receptor en caso de que filtre o le roben una contraseña. Esto debido a que si tiene la misma contraseña en dos o más servicios, estos servicios también son expuestos y tendrán un impacto diferente según el tipo de servicio que sea.

MED-4: Cambiar contraseñas por defecto

Se deben cambiar las contraseñas por defecto si o si, ya que generalmente siguen un patrón establecido o es de conocimiento público.

MED-5: Utilizar un gestor de contraseñas

Las contraseñas si no se almacenan de buena forma pueden ser expuestas (ya sea por un *phishing* o por tenerla anotada en un papel), además de estar la latente posibilidad de que se olviden, lo que puede provocar la perdida del acceso y/o acceso no autorizado a los servicios que se tengan. El utilizar un gestor de contraseñas, no solamente abstrae el memorizar las contraseñas o anotarlas y guardarlas bajo llave, sino que también ayuda a generar nuevas contraseñas robustas.

MED-6: Utilizar un MFA

La Autenticación Multifactor (MFA por sus siglas en inglés) se refiere a utilizar más de un método para autenticarse en un servicio como lo puede ser realizar una elección de un número en el *smartphone* o utilizar la huella dactilar. Tener este tipo de autenticación activada ayuda a controlar los accesos a los servicios, en caso de que detecte un intento de ingreso no autorizado está el control de denegar el acceso (control que es imposible si no se tiene MFA).

MED-7: Protocolo de lectura de un correo electrónico entrante

Esta medida toma en cuenta una serie de pasos que se deben realizar antes de interactuar con el contenido de un correo electrónico. Estos pasos son:

1. Identificar si el remitente es conocido o no.
2. Identificar si el dominio del correo electrónico no presente anomalías (letras de otros alfabetos, apostrofes, comillas u otros símbolos).
3. Identificar si el asunto indica alguna situación que involucre una reacción rápida.
4. Identificar si el cuerpo del correo indica alguna reacción rápida (cambiar contraseña, iniciar sesión, enviar datos, descargar algún archivo).

5. Identificar si existe algún enlace, en caso de existir verificar si el enlace corresponde con el sitio al que debería dirigir.

6. Identificar si existe algún documento adjunto, en caso de existir solamente debe descargarse si se cumplen los pasos 1, 2, 3 y 4.

MED-8: Utilizar una sesión de incógnito en un computador de un tercero

En caso de que se utilice un computador público o uno de un amigo, conocido o colega, se debe usar una sesión en incógnito, ya que en esta sesión no se guardan las credenciales ni en el navegador ni en el dispositivo.

3.2. DISEÑO SISTEMA DE INDUCCIÓN DE CIBERSEGURIDAD (SIC USM)

3.2.1. ESTRUCTURA DE GESTIÓN DEL SIC USM

La UTFSM posee Políticas Generales de Datos[UTFSM, 2024], dichas políticas rigen para cada uno de los organismos de la casa de estudio, identificando los roles y atribuciones que tiene cada responsable. El SIC sigue una estructura centralizada, donde existe la autoridad central compuesta por el CISO de la UTFSM (profesor guía de esta memoria) y el ejecutor del programa (memorista), quienes deben establecer las políticas, estrategias de desarrollo y la implementación del SIC USM.

Las unidades organizacionales en este sistema corresponden a los departamentos académicos responsables de las carreras (dado el alcance de esta memoria será el Departamento de Informática, representado por sus jefes de carrera, Pedro Godoy Barrera y José Luis Martí), a quienes se les entrega la planificación del proceso de inducción, el material y los métodos que se usarán en la sesión presencial.

Cabe mencionar que existe un hito que debe ser realizado por la autoridad central, dada la delicadeza y experiencia con la que se debe ejecutar. Se trata de la inducción, la cual contempla dos experimentos de *phishing* a modo de diagnóstico y evaluación (previo y post a la sesión de presencial), por lo que los departamentos deben proveer al CISO y ejecutor del plan, la lista de correos electrónicos de los estudiantes que se utilizarán en los distintos experimentos de *phishing*. Y a su vez la autoridad central debe proveer a los departamentos los resultados de las campañas.

3.2.2. EVALUACIÓN DE NECESIDADES

Actualmente, en la UTFSM no se realizan actividades sobre concienciación de ciberseguridad (aunque se realizan los Campos de Marte[11]) enfocada hacia los estudiantes.

Se realiza una encuesta con el fin de obtener cuantos estudiantes fueron parte de alguna sesión de inducción de ciberseguridad cuando entraron a la Universidad. El 81 % de los encuestados nunca ha participado en instancias de este tipo, además el 90 % de los encuestados encuentra necesaria este tipo de instancias de forma obligatoria en su formación.

Además, este Sistema de Inducción de Ciberseguridad viene a cubrir una necesidad que detectó el autor de la memoria siendo estudiante de primer año, cuando enfrentó una campaña de *phishing* vía un correo que informaba sobre la caducidad de las credenciales. Sin saber lo que significaba *phishing*, el autor pensó que perdería acceso a los servicios que él frecuentemente usaba, por lo que ante el miedo generado, hace entrega de las credenciales mediante un formulario que aparecía en la página del *phishing*. Gracias a un compañero que tenía conocimiento sobre dicho ciberataque, le dice al autor que debe cambiar las credenciales a la brevedad.

Con lo anterior se evidencia la necesidad de una inducción de ciberseguridad para los alumnos de primer año enfocado en la detección de *phishing*, si bien no es algo exclusivo para estudiantes novatos, este sistema se limita a trabajar con ellos dado que existe una asignatura que posee la flexibilidad para la realización de este tipo de actividades, Introducción a la Ingeniería.

3.2.3. ESTRATEGIA Y PLAN DE SENSIBILIZACIÓN

En el año 2024 el gobierno de Chile promulga la Ley Marco de Ciberseguridad (N.° 21.663) que crea la ANCI y establece responsabilidades, procedimientos y deberes que deben tener las instituciones privadas y públicas ante incidentes de ciberseguridad. En el artículo 8°, apartado h), la Ley Marco de Ciberseguridad establece que los *operadores de importancia vital deben contar con programas de capacitación, formación y educación continua de sus trabajadores y colaboradores, que incluyan campañas de ciberhigiene.*

Esta ley contempla en este aspecto solamente a los operadores de importancia vital (OIV), lo que no contempla a las universidades, sin embargo, es necesario que todas las personas, ya sean parte de los OIV o no, tengan en conocimiento el cómo detectar un correo malicioso, identificar páginas fraudulentas, cómo crear y almacenar las contraseñas, entre otros conceptos y principios. Ya que todos tenemos la misma probabilidad de ser víctima de un cibercrimen.

[11]Los Campos de Marte son eventos de ciberseguridad, orientados a la ofensiva, de tipo CTF, que en ciberseguridad se refiere a capturar la bandera dentro de un servidor utilizando diversas técnicas de *ethical hacking*.

El plan del sistema de inducción propuesto cumple solamente con el nivel de *awareness* del NIST SP 800-50, el cual tiene como objetivo el aumentar la capacidad de respuesta, detección y reporte de correos de *phishing* de los estudiantes de la universidad. El plan contempla las siguientes fases:

1. **Experimento de *Phishing* n.° 1**: Este experimento de *phishing* tiene como objetivo obtener un diagnóstico de la capacidad de respuesta de los estudiantes ante este tipo de ataques, enfocándose en las métricas de: correos enviados, correos abiertos, links clickeados, datos subidos y correos reportados.
2. **Inducción de Ciberseguridad**: Esta fase es el núcleo del sistema, en este hito se realiza un *debriefing* a los estudiantes sobre de qué se trata la actividad, y poder recopilar información sobre el impacto psicológico que les generó el primer ataque de *phishing*, además de preguntar qué notaron de raro en el correo electrónico o si el enlace les pareció raro.
3. **Experimento de *Phishing* n° 2**: Este experimento de *phishing* tiene como objetivo obtener la nueva tasa de respuesta ante este tipo de ataques, al igual que el primero se utilizan las mismas 5 métricas para la medición.

ROLES Y RESPONSABILIDADES

En el SIC USM se encuentran los siguientes roles y responsabilidades:

- **Autoridad**: Debe velar que se cumplan las normas y reglamentos de la universidad al momento de realizar las distintas fases del SIC USM. Es la conexión entre el sistema de inducción y la administración de la Universidad.
- **Coordinador**: Debe crear el contenido y eventos del sistema de inducción, esto quiere decir que es quien establece las fechas en que se realizan los experimentos de *ethical phishing* de diagnóstico y evaluación, la sesión de *debriefing* e inducción de ciberseguridad y el despliegue del material dentro de las dependencias de la Universidad.
- **Auditor**: Debe realizar los experimentos de *phishing*, el auditor debe elegir las páginas que serán clonadas y conseguir los permisos para la utilización de estas.
- **Relator**: Debe realizar el ***debriefing*** y la sesión de inducción de ciberseguridad a los estudiantes.
- **Estudiante**: Es sujeto de estudio del sistema SIC, debe participar de forma obligatoria en la inducción de ciberseguridad.

Para el material de la sesión de inducción de ciberseguridad se deben utilizar como base los tópicos propuestos por la NIST SP 800-50 y las Políticas Generales de Datos de la USM, esto

último con el fin de dar a conocer a los estudiantes cuáles son las políticas de seguridad que los rigen al momento de hacer uso de los servicios que la universidad provee.

El hito principal del SIC USM es la inducción de ciberseguridad, esta es la primera fecha que debe ser conversada y fijada, esto para poder establecer las fechas límites del primer experimento de *phishing*, obtener las métricas del experimento que serán expuestas en la inducción. Luego de hacer la inducción, se inicia con la cartelería social en la universidad y en redes sociales.

Idealmente, el sistema debe ser ejecutado como mínimo una vez en el semestre, esto para generar una formación continua en los estudiantes y fortalecer los conocimientos que se entregan en la inducción. Lo ideal es que se ejecute el sistema 2 veces en el semestre, dando a 4 instancias durante el año.

En la Figura 30 se presenta un diagrama de como es el funcionamiento del Sistema de Inducción de Ciberseguridad USM.

3.3. PRIMER EXPERIMENTO DE ETHICAL PHISHING

Para llevar una mejor gestión y ejecución de los experimentos de *phishing*, se utilizó Gophish. Gophish es una plataforma de código abierto desarrollada en Go que facilitó la simulación de ataques de *phishing*. Esta plataforma permitió automatizar el proceso de diseño de las páginas y correos electrónicos que se utilizaron para las simulaciones, permitiendo una mayor personalización de los correos que se enviaron a la organización (en este caso, a la universidad).

3.3.1. ARQUITECTURA USADA PARA EL DESPLIEGUE

Para el despliegue de Gophish, se utilizó Google Cloud Platform. Esta decisión se basó principalmente en la abstracción de crear la infraestructura on-premise para un correcto despliegue de los servicios. Se utilizaron dos servicios principalmente para el despliegue: *Compute Engine* y *VPC* (Virtual Private Cloud) con una dirección IPv4 estática.

Las características de la instancia de *Compute Engine* que se utilizó para el despliegue correspondieron a una instancia e2-micro con 2 CPU virtuales de un procesador AMD Rome (no se especificaron las características de este), 1 GB de RAM (no se especificaron frecuencia ni generación) y 15 GB de almacenamiento (no se especificó tipo de disco duro). Todo esto bajo una imagen de Ubuntu 20.04 LTS.

GCE asignó automáticamente una IP pública para acceder a los servicios que alojaba la instancia (como un sitio web). Sin embargo, para poder tener asignado un registro A y un CNAME al servicio de Gophish tanto para administración como para el acceso a las páginas de

phishing, se estableció una IP estática pública con VPC y Dreamhost para DNS. A modo de aumentar un poco la complejidad de la identificación del *phishing*, en *dreamhost* se usó el dominio usrn.noexiste.cl con registro A usrn.noexiste.cl para poder acceder a la página.

3.3.2. INSTALACIÓN DE GOPHISH

La instalación de Gophish se realizó usando la versión v0.12.1-linux-64bit disponible en su repositorio en GitHub. Lo bueno de esta versión fue su facilidad de instalación. Para poder iniciar los servicios, se descomprimió, se accedió a la carpeta, se habilitó la ejecución (`chmod +x gophish`) y se ejecutó el archivo llamado `gophish`, levantando así los servicios.

Sin embargo, al acceder a los servicios de Gophish mediante navegador, se alertó sobre la caducidad de los certificados de la página, por lo que se debieron instalar los certificados en la instancia para evitar que apareciera este mensaje a los estudiantes cuando secomenzaran las campañas.

La instalación de certificados fue trivial, pero se necesitó contar con el servicio ya público y que estuviera asociado a un dominio. Esta instalación de certificados se realizó con *certbot*, una herramienta de código abierto para utilizar automáticamente certificados Let's Encrypt en sitios web administrados manualmente para habilitar HTTPS. Para crear los certificados se utilizó el siguiente comando:

```
1  sudo certbot certonly --standalone --cert-name usrn.noexiste.cl -d usrn.
     noexiste.cl -m joaquingallegost@gmail.com --agree-tos --noninteractive
```

La configuración de los certificados se realizó agregando la ruta del certificado y la llave privada al archivo `config.json` de Gophish. En este archivo se configuró el puerto 443 para acceder a las páginas de las campañas y el puerto 3333 para acceder a la administración del sistema. Con esto último la plataforma ya se encuentra lista para realizar las campañas de *phishing*.

3.3.3. CONFIGURACIÓN SERVIDOR DE CORREO ELECTRÓNICO

Para la distribución de los correos electrónicos se debe contar un servidor de correos electrónicos propietario, esto quiere decir que no se debe usar un correo de terceros (como *Gmail*, *Outlook*, entre otros) principalmente por las políticas *anti-spam* que tienen estos servicios.

Para levantar el servicio de correo electrónico se utilizó *mailcow-dockerized*, un servidor de correos listo para configurar y desplegar usando las tecnologías de Docker. En esta ocasión se utiliza el dominio safesym.cl para la configuración del servidor de correos, junto con una máquina virtual entregada por el DI con una IP pública.

Se debe seguir el siguiente procedimiento para poder instalar e:

1. Instalar Docker[12]
2. Clonar repositorio https://github.com/mailcow/mailcow-dockerized
3. Ingresar a la carpeta descargada y ejecutar el archivo `generate_config.sh` y seguir los pasos
4. Ejecutar el comando `docker-compose pull`
5. Ejecutar el comando `docker-compose up`

Con los pasos anteriores el servidor de correos está listo para que sean configurados los dominios y los buzones de correos electrónicos.

Una vez concluida la instalación y todos los contenedores se están ejecutando se debe ingresar a la consola de administración de *mailcow*. Una vez dentro se pide cambiar la contraseña por defecto del administrador por razones de seguridad, para luego configurar el dominio de los buzones de correo.

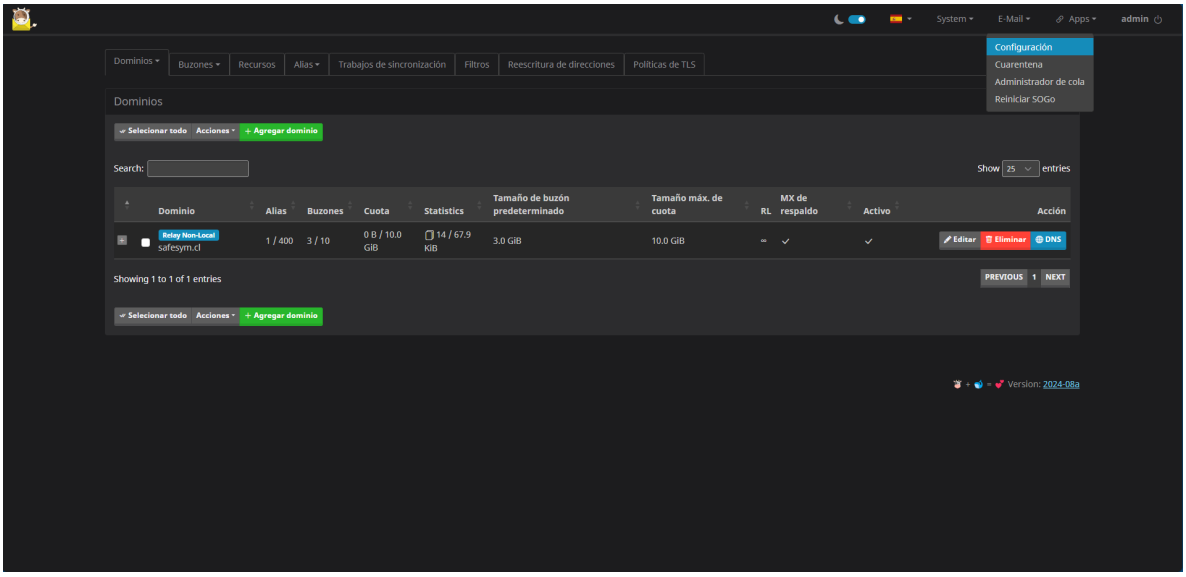


Figura 5: Vista de administración de dominios
Fuente: *Screenshot mailcow*

La configuración de los dominios en *mailcow* debe hacerse en la ventana configuración que muestra la figura 5. En *Agregar dominio* se realizan lan configuraciones del dominio, una vez estén listas se deben agregar en el servidor de nombre que esté administrando dicho

[12]En esta ocasión, Docker fue instalado previamente por los administradores del DI.

dominio, cada uno de los registros que se indican en el apartado DNS de mailbox (Figura 6, registros que deben ser agregados en este caso a *cloudflare*.

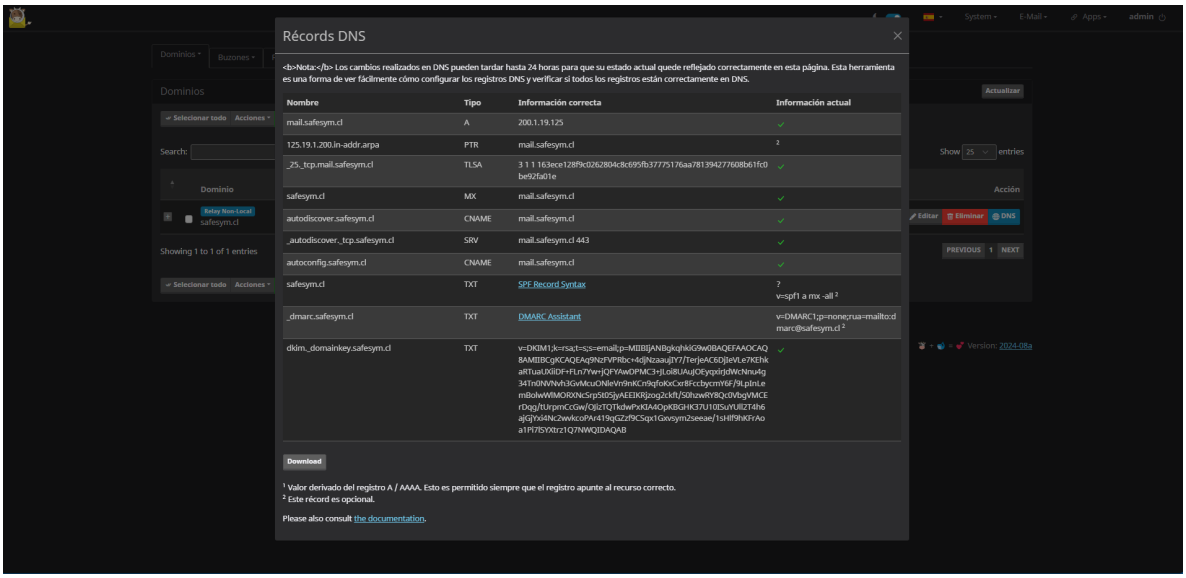


Figura 6: Registros DNS del dominio safesym.cl
Fuente: *Screenshot mailcow*

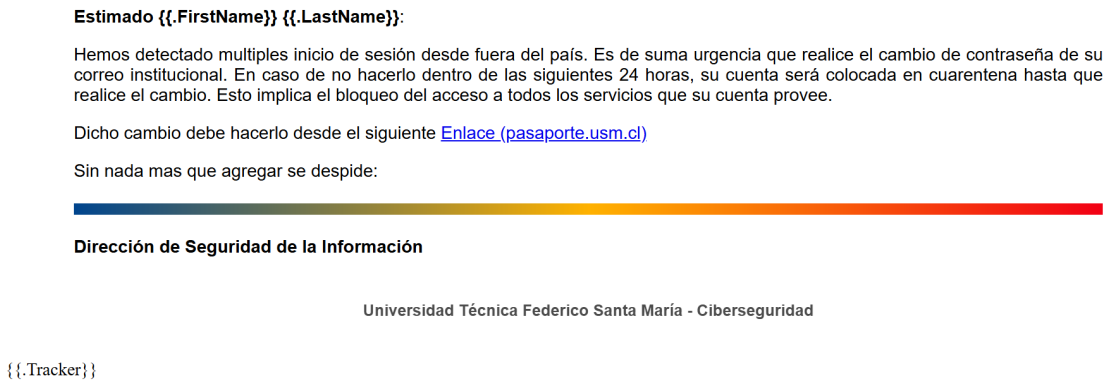
3.3.4. PREPARACIÓN DEL CORREO

En el primer experimento de *phishing* se simula la siguiente situación: Al alumno le llega un correo personalizado con su nombre y apellido, indicándole que su cuenta ha presentado múltiples inicios de sesión fuera del país, por lo que es de suma urgencia que realice el cambio de contraseña de su correo institucional y, en caso de no hacerlo dentro de las siguientes 24 horas, su cuenta será bloqueada. Si bien es una situación de un correo típico de *phishing*, en este experimento se busca que el estudiante se percate a través de múltiples pistas en el correo, sitio y enlace, de que es un *phishing*.

Para generar el template del correo electrónico (Figura 7) que se envía al alumno se utilizó la funcionalidad de *Email Templates* presente en Gophish, esta función automatiza y aumenta la capa de personalización de los correos, incrementando la apariencia de ser un correo genuino enviado por la organización. Esto último se logró utilizando las siguientes flags:

- **{{.FirstName}}**: Este flag coloca el nombre del receptor.
- **{{.LastName}}**: Este flag coloca el apellido del receptor.
- **{{.URL}}**: Este flag coloca la dirección con la que se accede a la página.

- **{{.Tracker}}**: Este flag coloca el rastreador de estado del correo para obtener las métricas.



Estimado {{.FirstName}} {{.LastName}}:

Hemos detectado multiples inicio de sesión desde fuera del país. Es de suma urgencia que realice el cambio de contraseña de su correo institucional. En caso de no hacerlo dentro de las siguientes 24 horas, su cuenta será colocada en cuarentena hasta que realice el cambio. Esto implica el bloqueo del acceso a todos los servicios que su cuenta provee.

Dicho cambio debe hacerlo desde el siguiente Enlace (pasaporte.usm.cl)

Sin nada mas que agregar se despide:

Dirección de Seguridad de la Información

Universidad Técnica Federico Santa María - Ciberseguridad

{{.Tracker}}

Figura 7: *Template* correo electrónico del primer experimento de phishing
Fuente: Elaboración Propia

3.3.5. PREPARACIÓN PÁGINA PHISHING

Dado que se espera que el alumno cambie las credenciales de su cuenta, este debe hacerlo en el sitio Pasaporte USM - Modificar Contraseña USM, iniciar sesión con sus credenciales actuales y luego se le redirige donde la debe cambiar.

Es por ello que se clonó dicha página en Gophish con su funcionalidad *Import Site* para ser usada como *landing page* para el experimento de *phishing* (Figura 8). No obstante la página verídica (Figura 9) utiliza un servicio embebido de inicio de sesión, aquella parte del sitio Gophish no la clona, es por ello que se diseñó un formulario de inicio de sesión lo suficientemente similar y a la vez distinto para que el estudiante pueda percatarse que se trata de un intento de *phishing*.

Figura 8: Landing page que simula ser pasaporte.usm.cl
Fuente: Elaboración Propia

Figura 9: Sitio web pasaporte.usm.cl original
Fuente: https://pasaporte.usm.cl

Existe en Gophish una opción de capturar las credenciales, esta opción se debe habilitar para hacer uso del redireccionamiento una vez subido los datos. Sin embargo, se debe desactivar la opción capturar contraseñas, para no comprometer las credenciales de los estudiantes (Figura 10).

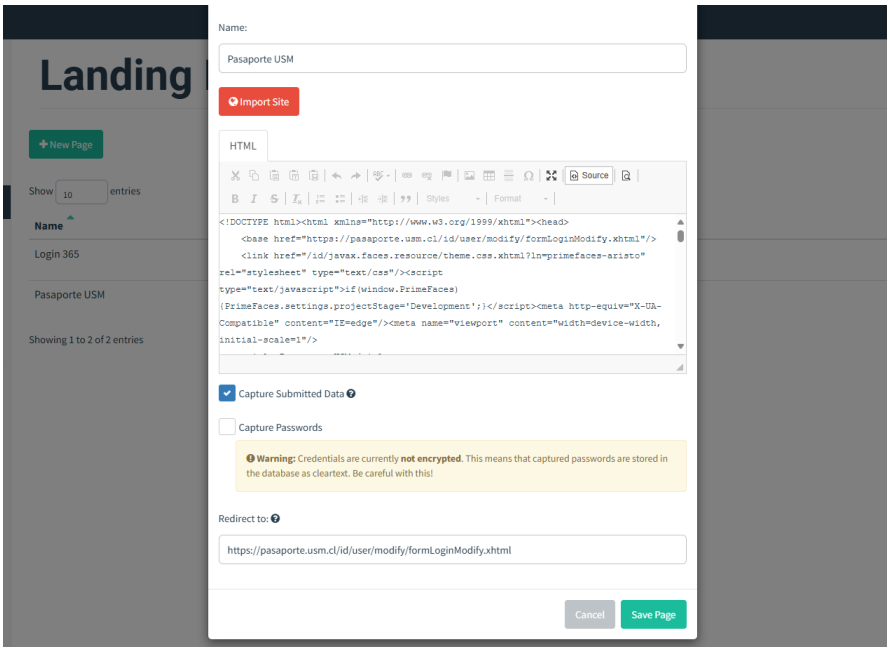


Figura 10: Configuración captura de datos
Fuente: Gophish

3.4. INDUCCIÓN DE CIBERSEGURIDAD Y CARTELERÍA SOCIAL

3.4.1. OBJETIVOS Y ESTRUCTURA DE LA INDUCCIÓN

La inducción de ciberseguridad tiene como objetivos, el mejorar la tasa de respuesta de los estudiantes de primer año ante las campañas de *phishing* y establecer las bases de una ciber-cultura y ciberhigiene dentro del estudiantado de primer año de Ingeniería Civil Informática. La inducción de ciberseguridad contempla 3 etapas principales en la charla, primero se realiza el *debriefing*, en esta parte se realizan preguntas sobre la experiencia de los estudiantes al momento de enfrentarse al primer experimento de *phishing*. Luego del *debriefing* se realiza la sesión de inducción, en esta parte se le explica a los estudiantes los tópicos seleccionados del NIST SP 800-50 junto con el apoyo de Gabriel Torres.

La profundidad de los tópicos como se trata de un *awareness* deben ser superficiales, que generen conciencia sobre cómo protegerse en internet y sobre cómo identificar los correos electrónicos maliciosos. Una vez terminada la inducción se inicia con un *Kahoot* donde se realizan preguntas acerca de los contenidos expuestos.

Esto para medir los conocimientos adquiridos por los estudiantes luego de la inducción de una forma no tan aburrida como lo puede ser una prueba escrita. Para los tres estudiantes que queden en el podio, se le entrega un diploma (Figura 11) a modo de reconocimiento por

su participación y quedar dentro de los tres primeros.

Figura 11: Ejemplo de formato de diploma de participación
Fuente: Elaboración Propia

3.4.2. PREGUNTAS Y ESTRUCTURA DEL *DEBRIEFING*

Una sesión de *debriefing* posee una estructura de tres partes, intercambio de impresiones, análisis conjunto y las conclusiones [Díaz, 2021], sin embargo, en este sistema el análisis conjunto corresponde a la inducción y las conclusiones a la actividad de *Kahoot*. En la parte de intercambio de impresiones se realizan las siguientes preguntas:

- ¿Leíste el correo electrónico?
- ¿Revisaste el dominio y nombre del remitente?
- ¿Revisaste el enlace adjunto?
- ¿Cómo te sientes ahora que sabes que fue un experimento de *phishing*?
- ¿Anteriormente tuviste una inducción de ciberseguridad?
- ¿Sabes lo que es el *phishing* (o correos maliciosos)?
- ¿Encuentras necesarias estas instancias de forma continua en los estudiantes?

3.4.3. CONTENIDOS DE LA INDUCCIÓN

Para la exposición de la sesión de inducción se consideraron los siguientes tópicos en conjunto con el CISO y el coordinador: Ingeniería social, uso y protección de contraseñas, protección contra *malware*, buen uso del correo electrónico, buen empleo de la web, SPAM, respaldos y respuestas a incidentes.

Ingeniería Social

- Manipulación de las personas con el objetivo de la divulgación de información personal, confidencial o las credenciales de la víctima
- Tiene como objetivo obtener las credenciales de las víctimas y acceder a los servicios de la organización o propio de la persona
- El *phishing* es la técnica más común, la cual hace pasar un correo malicioso por uno real

Contraseñas

- Primera línea de defensa contra los accesos no autorizados.
- Estas deben ser de al menos 16 caracteres, utiliza combinaciones de letras mayúsculas y minúsculas, números y símbolos. Si bien es difícil memorizar una contraseña para cada cuenta o servicio, existen los gestores de contraseñas, las cuales son aplicaciones que crean y gestionan contraseñas seguras, que cumplen con los criterios anteriores, sin embargo, debemos proteger la contraseña del gestor de contraseña.
- Existe una tendencia en que la contraseña deja de ser el único factor de autenticación, se debe contar ya con un 2FA.

Protección Contra Malware

- El malware (popularmente conocido como virus) puede comprometer la seguridad de los datos y los sistemas.
- Generalmente se presentan como activadores o cracks para instalar versiones de pago de las aplicaciones o videojuegos.
- Mantener el antivirus activado, actualizado y, constantemente, debe ser escaneado el computador y/o teléfono para determinar la salud del dispositivo.

- Evitar hacer click en enlaces de una ventana web emergente y descargar archivos adjuntos de correos.
- Mantener actualizado el sistema operativo a la última versión con los parches de seguridad al igual que las aplicaciones y servicios que uno utilice.
- Usar solamente aplicaciones que están compradas o descargadas de sitios oficiales. Para los servicios de pago, existen convenios con la Universidad para que se haga uso de forma gratuita siendo estudiante, asociado al correo institucional.

Uso del Correo Electrónico

- El correo electrónico es la primera línea de fuego contra el *phishing*.
- El *phishing* hace alusión a la pesca con redes, donde se despliega el correo electrónico esperando que una víctima caiga para robar las credenciales.
- Cuando recibas un correo electrónico debes leer detalladamente el correo del remitente, es decir que puedas corroborar que la dirección de correo no presente anomalías como lo pueden ser apóstrofes, comillas, tildes o letras de otros alfabetos (punny code).
- No descargues los archivos adjuntos si no has verificado que el remitente es quien dice ser. Puede ser un *malware*.
- Revisa que el enlace adjunto sea el que debe ser. Por ejemplo, todos los sitios de una universidad poseen `usm.cl` en el URL, en el caso de pasaporte usm, el link es `pasaporte.usm.cl`, por lo que si el sitio no corresponde, no tiene relación URL/sitio o simplemente no confías, no ingreses al sitio.
- Además, debes evitar ingresar datos en las páginas que se vean poco confiables o que no tengan relación con el enlace, ya que acá es donde se origina el robo de las credenciales.

Uso de la Web

- Cuando estés navegando, evita hacer clicks en los pop-ups de “activar notificaciones”, puesto que estas activan un script que sirve de adware (virus especializado en mostrar publicidad).
- En caso de que estés utilizando un wifi público, como lo puede ser una cafetería, hotel o aeropuerto, procura hacer uso de una VPN, esto te protegerá a ti y a tus datos.

- Verifica siempre que la URL del sitio tenga correlación con el contenido de la página, esto es un indicio de que si la página es o no confiable. Además, verifica siempre que el candado esté cerrado, si no lo está hay que preocuparse y no navegar por dicha página.
- Mantén siempre actualizado tu navegador a la última versión.

SPAM

- El SPAM son los mensajes, llamadas y/o publicaciones que no son esperadas por los receptores, ya sean por motivos empresariales o maliciosos.
- Debes evitar abrir los mensajes que parezcan SPAM y sobre todo NO debes descargar y/o abrir enlaces que contengan estos correos. Muchas veces contienen *malware* que roban tu información personal y/o credenciales de tus cuentas.

Respaldos

- Siempre ten una copia de tus archivos más importantes en la nube, esto te puede ayudar en caso de que seas víctima de un *ransomware* y se comprometan tus archivos del computador, así podrás recuperarlos y el impacto no será tan grande, tanto en la universidad como en tu vida personal.

Respuestas a incidentes

En caso de que seas víctima de *phishing* o te llegue un intento de *phishing*, no te quedes callado debes reportar este hecho, lo recomendado es que lo hagas de esta forma:

1. Encuentra el correo en cuestión
2. Luego mediante el cliente de Outlook, ingrese a los tres puntos de la esquina superior derecha
3. Luego en denunciar debe hacer click en informar sobre *phishing*

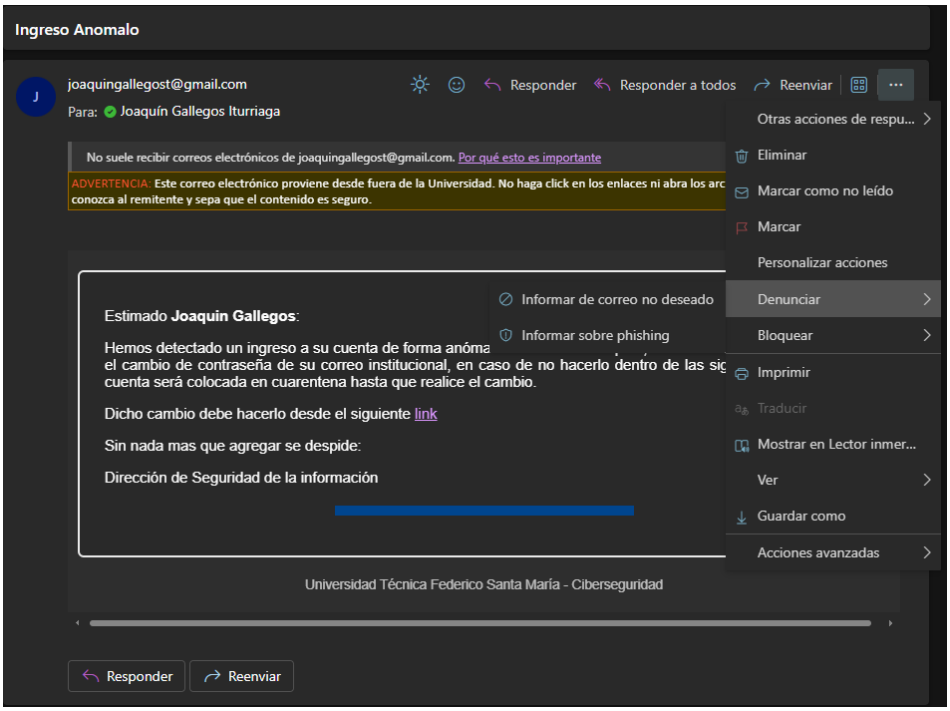


Figura 12: Imagen Referencial del Protocolo de Reporte
Fuente: Elaboración Propia

Además de reportar el correo mediante el protocolo anterior, se debe dar aviso a la Mesa 360 (requerimientos.usm.cl) o al *chatbot* de Teams “Aranda Virtual Agent”para que se tomen las medidas y se bloquee la llegada de mensajes con ataques o con contenido no deseado.

Una vez concluida la presentación se da inicio a una sesión de Kahoot donde los estudiantes deben responder una serie de preguntas enfocadas a los comportamientos adquiridos luego de la sesión de inducción, esto a modo de realizar una medición de cómo los contenidos llegaron a los estudiantes y gamificar la experiencia de la inducción de ciberseguridad. Sin embargo, dado que Kahoot presenta un límite de 20 alumnos por sesión, por lo que se debe realizar la actividad en equipo de 2 a 3 estudiantes[13].

3.4.4. CARTELES INFORMATIVOS SOBRE CIBERSEGURIDAD

Según la NIST SP 800-50 [Wilson y Hash, 2003] se debe establecer técnicas de despliegue del material de la inducción, dentro del marco de la asignatura Introducción a la Ingeniería se cuenta con la posibilidad de publicar el material de la inducción dentro del sistema de aula virtual para la completa disponibilidad de las diapositivas usadas en la sesión de inducción.

Para generar una mayor concienciación no solo en los estudiantes objetivos de este sistema

[13]Esto considerando un máximo de 60 estudiantes, en caso de haber más de 3 a 4 estudiantes por equipo.

de inducción, sino que en toda la comunidad universitaria, se debe hacer uso de cartelería social dentro de la Universidad. Para esto se utilizan los diarios murales que están dentro de la Universidad. Los tópicos que cubren los carteles son los mismos que en la sesión de inducción presencial. En la Figura 13 se muestra un ejemplo de afiche.

Los puntos de despliegue en Casa Central son: Laboratorio de Proyectos Informáticos (Lab-Pro) y diarios murales del edificio F. En Campus San Joaquín son: áreas del DI en edificio K, Pañol edificio B y el Laboratorio de Desarrollo de Software. Además, se debe hablar con los Centros Estudiantiles de ambos campus para que se publique por redes sociales los afiches, esto con el fin de alcanzar a más estudiantes y generar una concienciación continua en la comunidad.

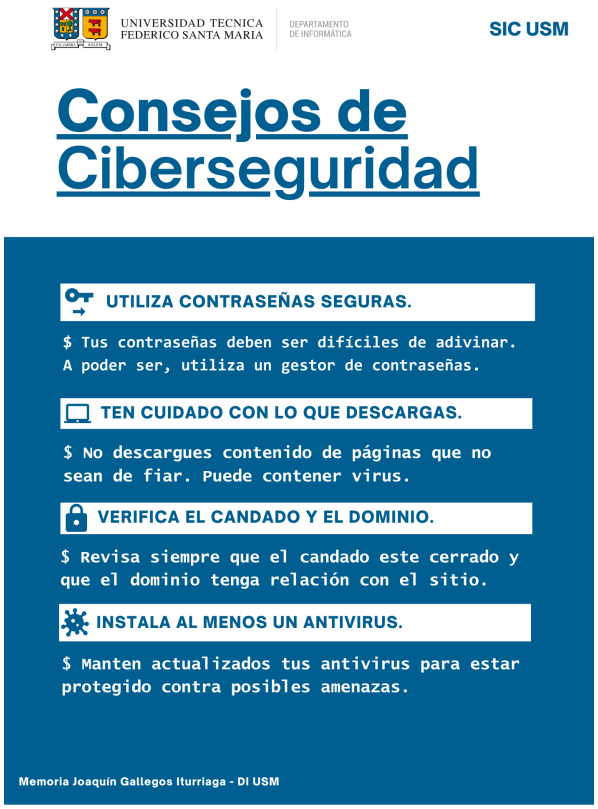


Figura 13: Ejemplo de formato de afiche para la formación continua
Fuente: Elaboración propia

3.5. SEGUNDO EXPERIMENTO DE ETHICAL PHISHING

Cronológicamente, el segundo *ethical phishing* se realiza dos semanas después de la inducción de ciberseguridad, por lo que se debe evaluar con un mayor nivel de dificultad el *ethical phishing*, es decir no dejar tantas pistas claras que el correo se trata de un *phishing*, como lo

pueden ser las faltas ortográficas o poca formalidad en el cuerpo del correo electrónico. Para este experimento las únicas pistas que se muestran es el dominio del correo electrónico y la URL del sitio que se redirigirá cuando hagan click.

La situación a simular en este segundo experimento cambia el enfoque del *ethical phishing*, esta ocasión se simula una actualización de las fechas de la atención de los casinos de la universidad, donde deberán iniciar sesión para poder ingresar a revisar las supuestas actualizaciones del casino.

3.5.1. PREPARACIÓN DEL CORREO

Para llevar a cabo este *ethical phishing* se debe crear una nueva dirección de correo, esta vez la cuenta de correo electrónico es casino.usm.cl@safesym.cl[14]. El nombre de usuario tiene como objetivo de que los estudiantes piensen a primera vista que la cuenta de correo electrónico es de la Universidad, sin embargo, el dominio no corresponde a una cuenta de la universidad (dado que pertenece a safesym.cl y no a usm.cl), por lo que es una clara pista de que el correo no es de fiar (Figura 14).

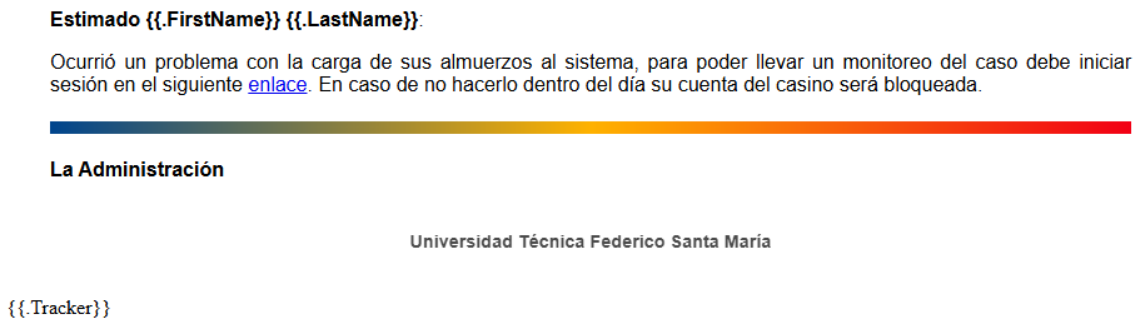


Figura 14: *Template* correo electrónico del segundo experimento de *phishing*
Fuente: Elaboración Propia

3.5.2. PREPARACIÓN PÁGINA PHISHING

En este experimento se pretende que el estudiante inicie sesión para poder revisar el estado de la carga de los almuerzos, por lo que la página clonada corresponde al login de *Microsoft 365* (Figura 16). Dada la complejidad que posee dicha página para hacer uso de la funcionalidad de importar sitio que posee Gophish, se hizo una *clonación a mano*, es decir, se replicó

[14]En las sesiones de inducción se le recalca a los estudiantes que las cuentas de correos oficiales de la universidad son las cuentas usm.cl.

el login usando HTML y CSS puro (Figura 15).

Para poder generar un *template* mucho más similar al original, se utiliza la *flag* `{{.Position}}`, dicha *flag* tiene como fin indicar la posición de la víctima en el cuerpo del correo o la página, pero en esta ocasión se utiliza para indicar el correo del estudiante en la página.

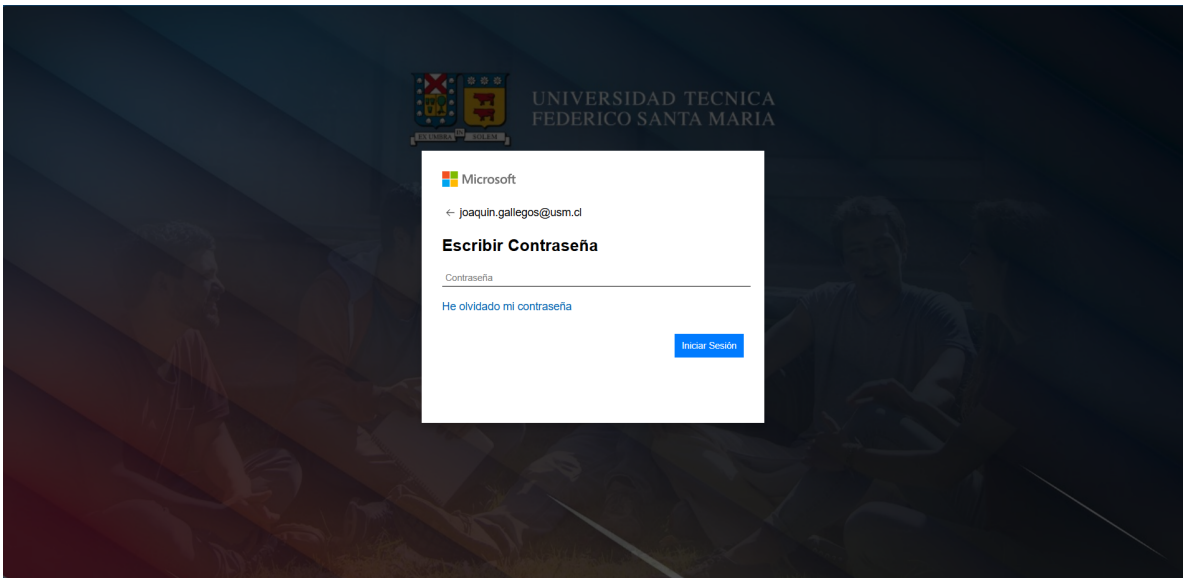


Figura 15: Landing Page que simula ser el login de Microsoft 365
Fuente: Elaboración Propia

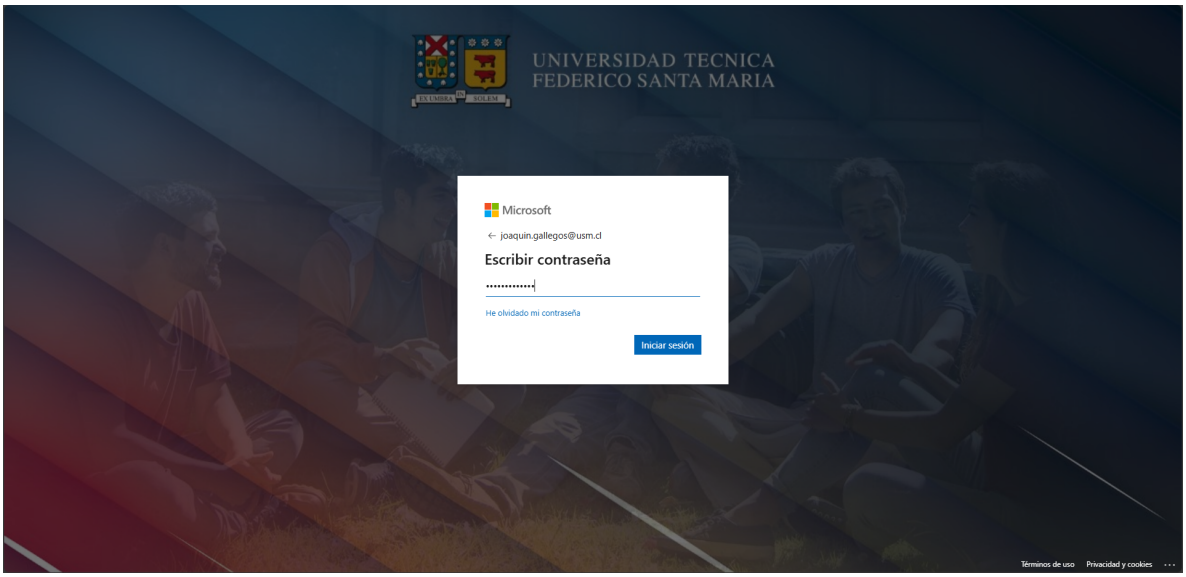


Figura 16: Login Microsoft 365
Fuente: login.microsoftonline.com

Al igual que en el primer experimento se tiene activado el capturar datos, pero no se guardan las contraseñas y en este experimento solamente se tiene un campo en la página, el cual es la contraseña, por lo que no se capturan datos.

3.6. IMPLEMENTACIÓN DEL SISTEMA SIC USM

3.6.1. REUNIONES CON PROFESORES DE INTRODUCCIÓN A LA INGENIERÍA Y JEFES DE CARRERA

El SIC USM es pensado como una programa que debe ser realizado como mínimo una vez a todos los estudiantes de primero año de la Universidad de forma obligatoria dentro de la asignatura de Introducción a la Ingeniería, esto con el objetivo de reducir la brecha de conocimiento que pueden traer los estudiantes y fomentar la cibercultura.

Para establecer las fechas de la inducción de ciberseguridad (fecha crucial para establecer la duración de las campañas), se fijó una reunión con el profesor coordinador de la asignatura Víctor Gutiérrez Fierro 17. En dicha reunión se establecieron las fechas 30 de septiembre y 4 de octubre en Casa Central y, 1 y 2 de octubre en San Joaquín; para la realización de las inducciones de ciberseguridad a los estudiantes, cuya duración de las sesiones es de 70 minutos, abarcando toda la clase.

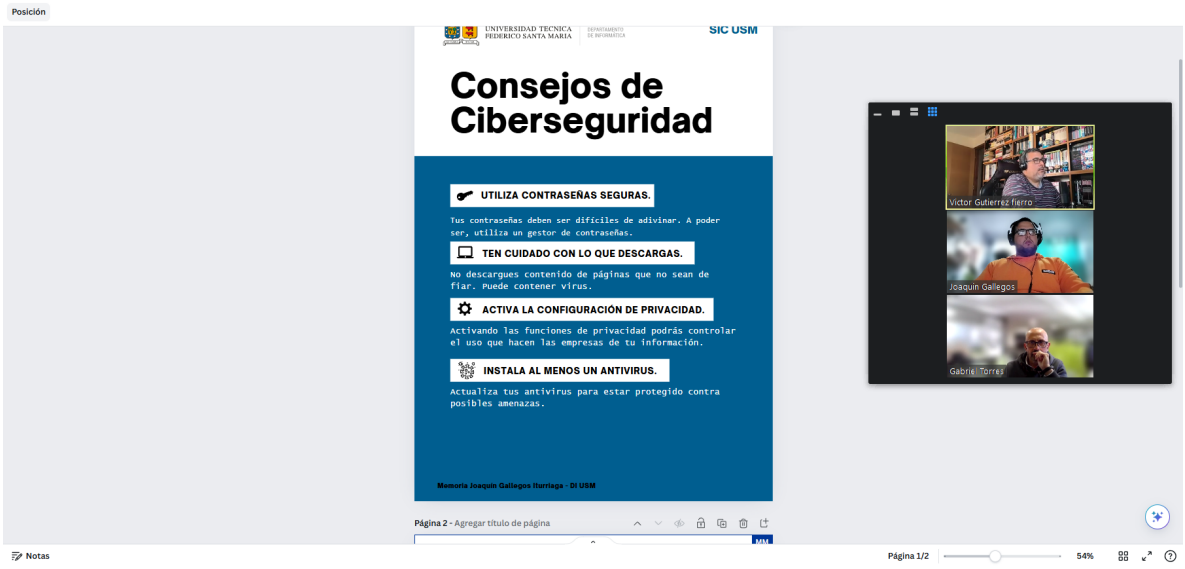


Figura 17: Reunión de Programación de fechas para las inducciones
Fuente: Elaboración Propia

Para solicitar de manera formal los correos de los estudiantes de la asignatura y dar aviso sobre la actividad que se quiere llevar a cabo se solicitó una reunión con los jefes de carrera

de ambos campus, Pedro Godoy y José Luis Martí, los cuales manifestaron estar muy de acuerdo en que esta actividad se realice.

3.6.2. COORDINACIÓN CON DTI Y FECHAS DE CAMPAÑAS DE PHISHING

Para llevar a cabo ambos experimentos de *phishing* se debe solicitar a DTI el añadir a un filtro específico para la realización de experimentos de *phishing* que posee Microsoft 365. Para ello se debe solicitar activar el filtro, enviando la cabecera del correo electrónico[15] a DTI para que lo habilite.

Además, se debe indicar las fechas en las que se realizarán los experimentos para deshabilitar los filtros una vez concluido el despacho de los correos electrónicos. Las fechas tentativas de realización de *ethical phishing* son:

- Primer *Ethical Phishing*: 16 de septiembre - 29 de septiembre
  - Envíos de Correos: 16 de septiembre - 29 de septiembre
  - Captura de Datos[16]: 16 de septiembre - 29 de septiembre
- Segundo *Ethical Phishing*: 14 de octubre - 20 de octubre
  - Envíos de correos: 14 de octubre - 15 de octubre
  - Captura de Datos: 14 de octubre - 20 de octubre

[15] La cabecera contiene todos los datos necesarios para poder activar los filtros.
[16] Esto se refiere a la toma de métricas.

CAPÍTULO 4
VALIDACIÓN DE LA SOLUCIÓN

4.1. RESULTADOS PRIMER ETHICAL PHISHING

4.1.1. MÉTRICAS OBTENIDAS

Los resultados obtenidos durante el primer experimento de *phishing* se detallan en la Figura 18, donde queda reflejado que de los 295 correos que fueron despachados. Los 295 correos solamente 12 fueron abiertos, 0 fueron clickeados[17] y 0 datos fueron enviados. En la Tabla 7 se presenta el porcentaje de las métricas mostradas en la Figura 18.

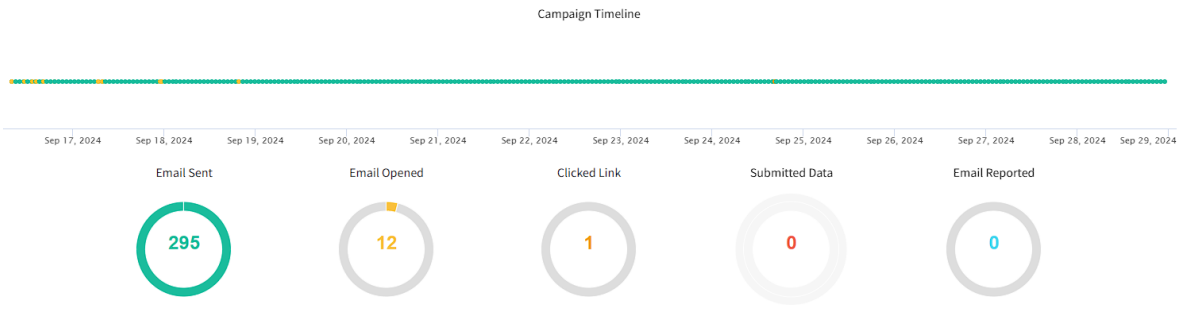


Figura 18: Resultados primer experimento de *phishing*
Fuente: Elaboración Propia, Gophish

Tabla 7: Resultados primer experimento de phishing.
Fuente: Elaboración Propia.

Métrica	**Porcentaje**
Correos Enviados	100 %
Correos Abiertos	1,7 %
Enlaces Clickeados	0 %
Datos Subidos	0 %

Dados los resultados del experimento se sospecha que los estudiantes, no revisan los correos electrónicos de forma constante por lo que es urgente que se le inculque a los estudiantes que deben revisar su correo por lo menos 3 veces al día (mañana, mediodía y tarde-noche).

[17] En la imagen 18 aparece un click, esto fue a modo de prueba.

4.1.2. EXPERIENCIA CON LA ADMINISTRACIÓN DE CORREOS ELECTRÓNICOS

Durante el desarrollo de la campaña se detectó que los estudiantes no estaban abriendo los correos. En primera instancia se asume que los estudiantes no verificaban los correos electrónicos, por lo que se incluye una mención en la charla de inducción de la importancia de considerar como una buena práctica de su vida universitaria, la revisión de su correo institucional por lo menos 3 veces al día

En la sesión de inducción se preguntó a los estudiantes si recibieron un correo electrónico con el asunto *Problemas de Seguridad*, donde la gran mayoría respondió que no. Con esta información se hace un análisis de la configuración, donde se evidencia que no era la apropiada para este caso. Como consecuencia, no fue posible obtener la métrica exacta del experimento. Sin embargo, de los correos que fueron abiertos ninguno ingreso credenciales por lo que es buena señal.

Dada esta situación se estableció que se agregaran dos cuentas de correos extras a la de los estudiantes, que corresponden a los correos de los realizadores de este proyecto, para poder monitorear el correcto despacho de los correos electrónicos.

Si bien no se pudo obtener las tasas de éxito de una campaña de *phishing* con una mayor muestra, se pudo evidenciar que con los recursos utilizados se puede realizar de forma constante este tipo de experimentos.

4.2. RESULTADOS SESIONES DE INDUCCIÓN DE CIBERSEGURIDAD

Como se define en la sección 3.4 en las sesiones de inducción de ciberseguridad, se debe realizar un *debriefing* en este tipo de experimentos de *phishing*, en esta oportunidad se realiza una encuesta sobre los hábitos al leer los correos electrónicos cuando son recibidos. En las 4 sesiones de inducción de ciberseguridad asistieron 179 alumnos de 295 (un 60 % aprox.) un poco más de la mitad de los estudiantes de Introducción a la Ingeniería, aunque esto también implica que el resto de los estudiantes no fueron educados en los tópicos en esta instancia.

4.2.1. ¿Qué tan seguido revisas tu casilla de correos?

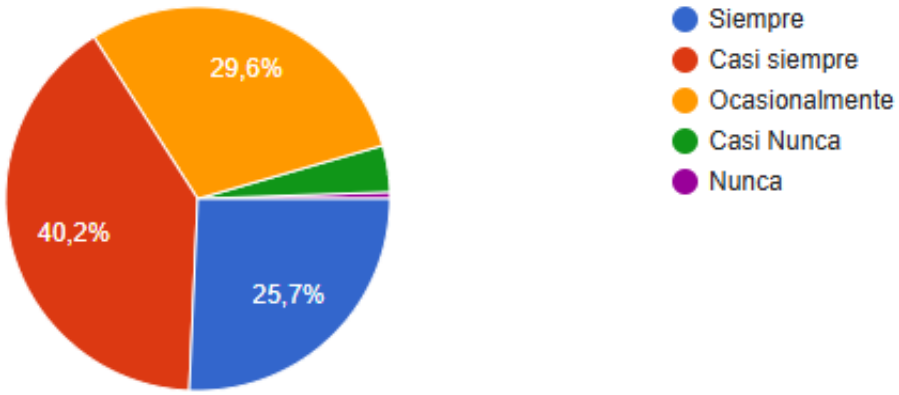


Figura 19: Gráfico pregunta 1, encuesta debriefing
Fuente: Elaboración Propia

Esta pregunta apunta a tener en conocimiento cuál es la frecuencia con la que los estudiantes revisan sus casillas de correos, dado que se sospechaba que la causa de la baja interacción con los correos enviados, era debido a un mal habito de los estudiantes al no verificar el correo. Sin embargo, se obtuvo que aproximadamente un 96 % de los estudiantes verifican por lo menos una vez al día su casilla de correos electrónicos, descartando esta hipótesis.

4.2.2. ¿Leíste el correo electrónico?

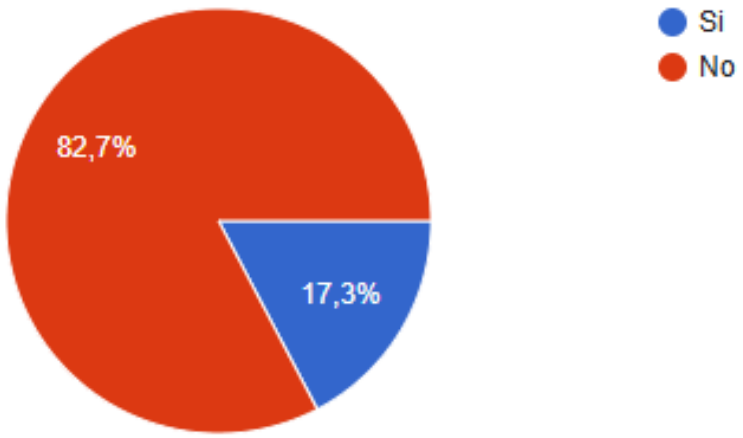


Figura 20: Gráfico pregunta 2, encuesta debriefing
Fuente: Elaboración Propia

Este resultado permitió descubrir el problema con los despachos de correos por la configuración de la administración de correos electrónicos, dado que se preguntó a los estudiantes "*¿Ustedes recibieron un cierto correo indicándoles un problema de seguridad con su cuenta?*", donde la gran mayoría indico que no recibió el correo electrónico. 31 personas leyeron el correo, mientras que el resto no. Si bien solo 12 correos fueron abiertos, según las métricas de Gophish, el resto de las personas afirman haber leído el correo, se puede explicar a una difusión de los correos recibidos entre compañeros.

Se considera que existe una mínima incerteza sobre la apertura de los correos, esto debido a un problema de sincronización sobre el registro de la lectura del correo, ya que es posible leer un correo electrónico en un dispositivo, pero que no se registre como correo leído.

4.2.3. ¿Revisaste el dominio y nombre del remitente?

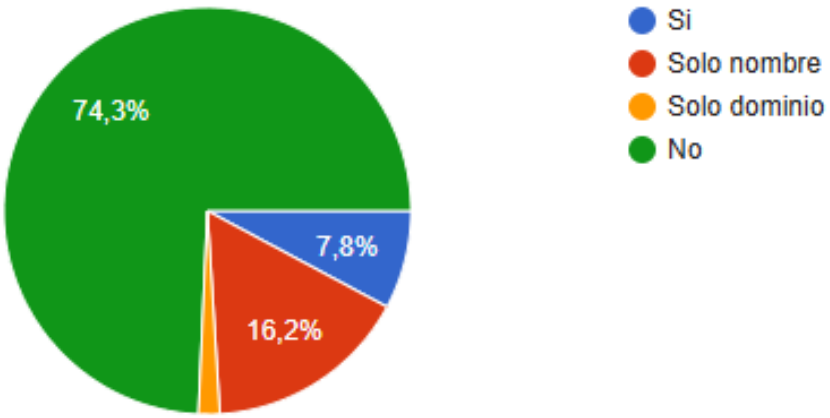


Figura 21: Gráfico pregunta 3, encuesta debriefing
Fuente: Elaboración Propia

La gran mayoría de los estudiantes participantes de la sesión de *debriefing*, tienen un comportamiento que aumenta la probabilidad de ser víctimas de *phishing*, por lo que es un acierto incluir este tópico en la sesión de inducción.

4.2.4. ¿Revisaste el enlace adjunto?

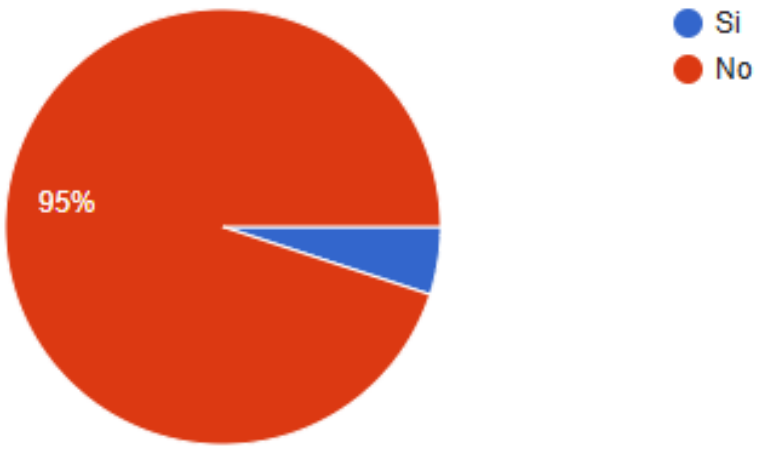


Figura 22: Gráfico pregunta 4, encuesta *debriefing*
Fuente: Elaboración Propia

El 95 % de los estudiantes no posee el hábito de revisar los enlaces adjuntos en los correos electrónicos ni tampoco en las páginas web que son adjuntadas en dichos correos. El identificar si una página web es verídica o no, es uno de los puntos de inflexión de caer o no en un *phishing*, al igual que verificar el remitente de un correo electrónico.

4.2.5. ¿Cómo te sientes ahora que sabes que fue un experimento de *phishing*?

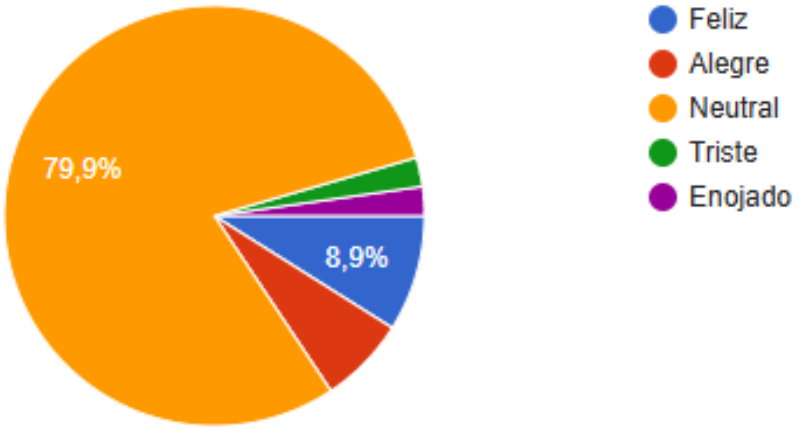


Figura 23: Gráfico pregunta 5, encuesta *debriefing*
Fuente: Elaboración Propia

Esta pregunta apunta a obtener como fue la sensación de los estudiantes al saber que fueron parte de un estudio de *phishing*, donde la gran mayoría de ellos no presentó alguna queja u mala opinión sobre la actividad realizada.

4.2.6. ¿Anteriormente tuviste una inducción de ciberseguridad?

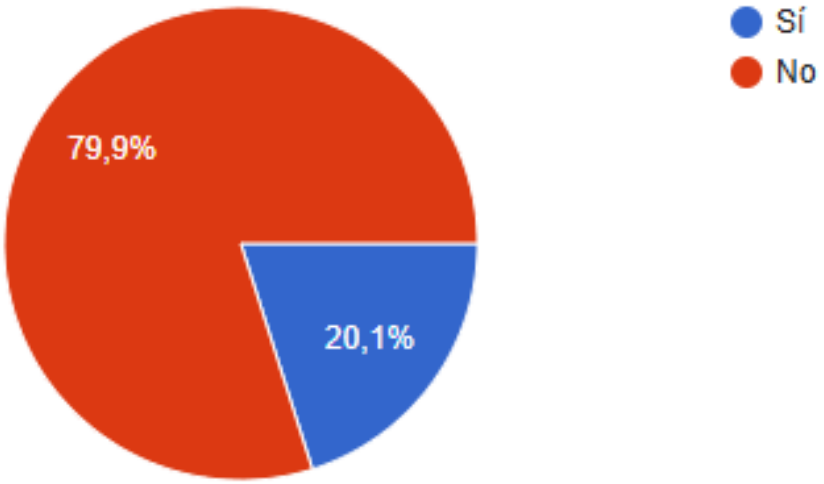


Figura 24: Gráfico pregunta 6, encuesta *debriefing*
Fuente: Elaboración Propia

Aproximadamente 143 personas nunca han sido parte de una inducción de ciberseguridad como esta, por lo que esta instancia aumenta el número a 179 personas que han tenido este tipo de experiencia y, por lo tanto, cómo defenderse de un *phishing*.

4.2.7. ¿Sabes lo que es el *phishing* (o correos maliciosos)?

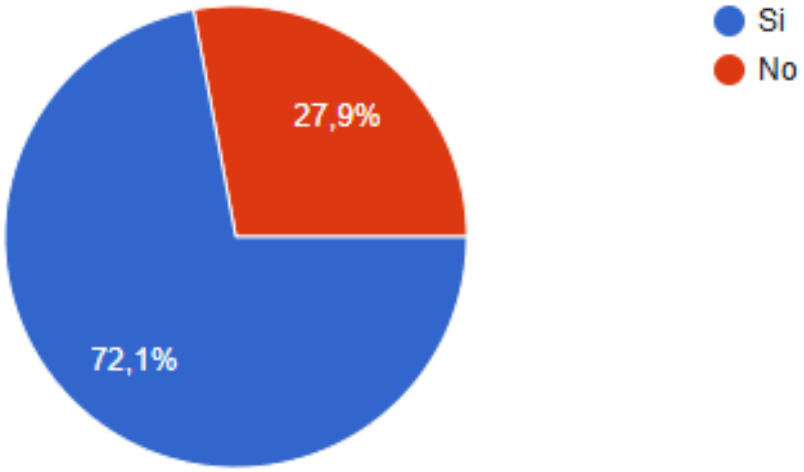


Figura 25: Gráfico pregunta 7, encuesta *debriefing*
Fuente: Elaboración Propia

Si bien gran parte de los estudiantes son conscientes sobre lo que es el *phishing*, existe una porción considerable que no tiene conocimientos sobre estos temas, por lo que se evidencia la necesidad de contar con este tipo de instancias.

4.2.8. ¿Encuentras necesarias estas instancias de forma continua en los estudiantes?

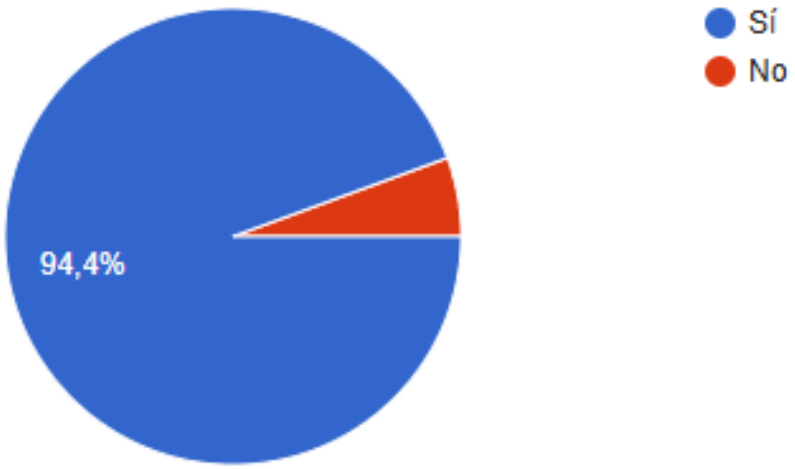


Figura 26: Gráfico pregunta 8, encuesta *debriefing*
Fuente: Elaboración Propia

Esta pregunta apunta a como percibir los estudiantes este tipo de instancias, donde más del 90 % percibe de forma necesaria este tipo de instancias de formación, por lo que es necesario que estas instancias se mantengan en el tiempo de forma obligatorio y sea parte de la formación integral de un *sansano*.

4.2.9. SESIONES DE INDUCCIÓN

Las sesiones de inducción (Figura 27) fueron desarrolladas de forma exitosa, logrando una participación del 60 % de la generación 2024 de primer año en ambos campus. Los estudiantes presentaron una muy buena disposición, siempre atentos y participativos con las sesiones, además de recibir un constante apoyo de los profesores de la asignatura en los momentos previos, durante y post sesión de inducción.

Un imprevisto que surgió durante la primera sesión de inducción es que no se tenía en conocimiento que *kahoot.it* está limitado solamente a un máximo de 20 participantes por sesión, por lo que se tuvo que tomar la decisión de que los alumnos formen equipos de 2 a 3 estudiantes.

Figura 27: Sesión de Inducción de Ciberseguridad
Fuente: Víctor Gutiérrez

A pesar de ello se obtuvieron muy buenos resultados de la sesión de *Kahoot*, logrando un 74 % de respuestas correctas en promedio en todas las generaciones o en otras palabras, se obtuvo un 74 como nota promedio de la sesión de inducción como generación 2024.

Esta nota indica que gran parte de los contenidos fueron comprendidos por los estudiantes, sin embargo, aún existe un 26 % de mejora en ellos, mejora que se logra al realizar de forma continua este tipo de sesiones.

4.2.10. RESULTADOS KAHOOT

En la parte final de la sesión se obtuvieron los resultados mostrados en la Tabla 8:

Pregunta	**Porcentaje**
¿Qué debes hacer con los mensajes que parecen spam?	94 %
¿Por qué es importante tener respaldos de tus archivos?	94 %
¿Qué debes hacer para mantener tu dispositivo seguro contra malware?	94 %
¿Qué es el *phishing*?	94 %
¿Qué beneficios tiene el usar un gestor de contraseñas?	94 %
¿Qué debes evitar al navegar por la web?	94 %
¿Qué debes hacer si identificas un correo de *phishing*?	85 %
¿Es el mismo enlace?	81 %
¿Es el mismo sitio que la imagen anterior?	81 %
¿Cada cuánto debes revisar el correo electrónico?	64 %
¿Qué debes verificar en un correo electrónico para evitar el *phishing*?	46 %

Tabla 8: Promedio de respuestas correctas por pregunta
Fuente: Elaboración Propia

Los estudiantes en general tuvieron un muy buen entendimiento en la mayoría de los temas, alcanzando un 94 % en 6 de las 11 preguntas que se realizaron. Por otro lado, existen tópicos que necesitan una mayor profundización, como lo es "¿Qué debes verificar en un correo electrónico para evitar el *phishing*?". Esta pregunta apuntaba a que los estudiantes se fijarán en el tono de la redacción del cuerpo y asunto del correo.

Los estudiantes entendieron qué para verificar que un correo no era *phishing*, deben revisar el remitente del correo. Esto es parcialmente correcto, debido a que se valida que proviene de una fuente conocida y confiable, más esto no es suficiente, ya que puede ser el caso de que la cuenta remitente sea comprometida, por lo que se les explica, que deben revisar que el correo no incite a realizar alguna acción de forma inmediata o en el corto plazo.

4.3. RESULTADOS SEGUNDO ETHICAL PHISHING

Este experimento tuvo un mejor rendimiento que el primero, esto debido principalmente a que las configuraciones de Microsoft 365 por parte de la administración de correos fueron realizadas de forma correcta. Para esta instancia se incluyen 4 correos para revisar la configuración y entrega de correos de la campaña. Los resultados de la segunda campaña de *ethical phishing* se detallan en la Figura 28.

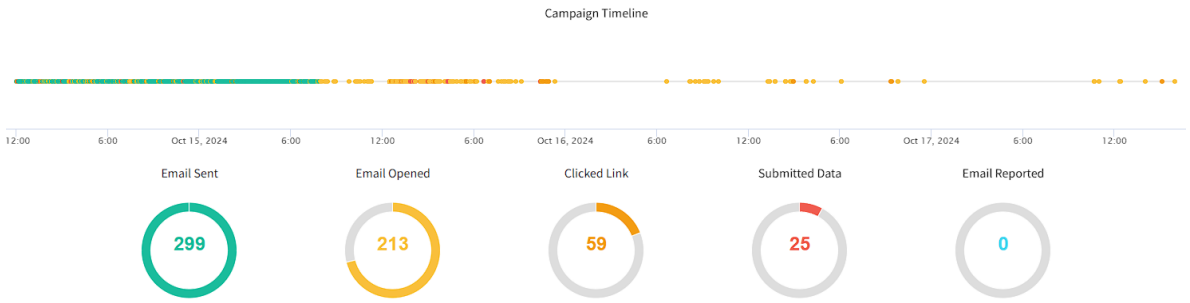


Figura 28: Resultados segundo experimento de *phishing*
Fuente: Elaboración propia

Se debe considerar que 4 correos son de prueba, por lo que no se contabilizan en el cálculo. De los 295 correos de estudiantes, 211 fueron abiertos, 57 fueron abiertos y 24 estudiantes ingresaron datos al sistema. Obteniendo las siguientes tasas mostradas en la Tabla 9.

Tabla 9: Resultados primer experimento de *phishing*.
Fuente: Elaboración Propia.

Métrica	**Porcentaje**
Correos Enviados	100 %
Correos Abiertos	71.5 %
Enlaces Clickeados	19.3 %
Datos Subidos	8.1 %

En comparación al primer experimento de *phishing*, se observa un alza en los correos electrónicos que fueron abiertos, enlaces clickeados y, esto se debe a que las configuraciones realizadas no permiten la entrada de los correos a las casillas. Debido a este problema, no se cuenta con dichas métricas por lo que se determina utilizar las métricas de la empresa KnowBe4 [Collard, 2023] que obtuvo en América del Sur para la comparativa de campañas.

KnowBe4 utiliza una métrica llamada *Phish-prone percetage*(PPP), la cual consiste en la división de los sujetos que cayeron en la prueba de *phishing* entre la cantidad total de sujetos que fueron parte del experimento, misma métrica usada en esta memoria. Según KnowBe4, en una organización entre 250 a 999 empleados (en este caso estudiantes) que nunca hayan recibido una inducción de ciberseguridad, poseen un PPP de 27.7 %.

A 90 días de ser realizada la inducción, KnowBe4 reporta que el PPP es de 25.8 % y al año es de 10.2 %. En el caso del SIC USM, la segunda campaña de ethical *phishing* se realiza 2 semanas después de la sesión de inducción, obteniéndose un PPP de 8.1 %, lo que lo colocaría en lo esperado luego de un año de formación continua en estos temas.

4.4. IMPACTO ECONÓMICO

Al implementar el SIC USM se incurrieron en los siguientes gastos, detallados en la Tabla 10:

Tabla 10: Costos 1 instancia SIC USM
Fuente: Elaboración Propia.

Item	**Costo**
Dominio	$10,000
8 Afiches	$12,000
12 Diplomas	$16,800
2,160 Horas GCP	$34,000
8 HH AdminSys	$75,000
16 HH *Ethical Phishing*	$150,000
TOTAL	$297,800

Una empresa que ofrece servicios de concienciaciones en ciberseguridad similares a los del SIC USM, que contempla 4 ethical phishings, cartelería social y sesión de inducción presencial [18], mas no diploma de podio, tiene un valor de $ USD 12.40 por persona a capacitar. Si se considera que el SIC USM contempla a todos los estudiantes de primer año (4,000 aproximadamente este 2024), la universidad debería incurrir en un gasto de $USD 49,600 anuales. En caso de que realizase 2 veces al semestre, tiene un costo de $USD 99,200 al año.

Si la universidad hubiera contratado el servicio anterior para los 295 estudiantes, tendría un costo de $USD 3,660 aproximadamente, sin embargo, la ejecución del SIC USM para la misma cantidad de estudiantes tiene un costo de aproximadamente $USD 298.

Con el SIC USM la universidad se abstrae de incurrir en gastos relacionados con los relatores, esto principalmente a que considera que los relatores de las sesiones de inducción de ciberseguridad las realicen los profesores de la universidad en sus asignaturas. No obstante, la universidad debe incurrir en gastos de *hosts*, ya que, actualmente la DTI no contempla en sus funciones brinda este tipo de servicios.

Los costos de ejecutar el SIC USM 2 y 4 veces al año con los estudiantes de primer año se detallan en las tablas 11 y 12:

[18] Equivalente a dos instancias SIC USM.

Tabla 11: Costos 2 instancia SIC USM
Fuente: Elaboración Propia.

Item	**Costo**
2 Dominios	$20,000
40 Afiches	$60,000
600 Diplomas	$720,000
4,320 Horas GCP	$68,000
16 HH AdminSys	$150,000
32 HH *Ethical Phishing*	$300,000
TOTAL	$1,318,000

Tabla 12: Costos 4 instancias SIC USM
Fuente: Elaboración Propia.

Item	**Costo**
2 Dominio	$20,000
80 Afiches	$120,000
1200 Diplomas	$16,800
8,640 Horas GCP	$136,000
32 HH AdminSys	$300,000
64 HH *Ethical Phishing*	$600,000
TOTAL	$2,616,000

CAPÍTULO 5
CONCLUSIONES

5.1. ANÁLISIS DE DISEÑO

El Sistema de Inducción de Ciberseguridad USM, fue diseñado para ser implementado principalmente para estudiantes de primer año, aunque por el alcance de esta memoria solo para Ingeniería Civil Informática. Esto no limita a ser aplicable para todas las carreras que imparte la Universidad, incluyendo las carreras técnicas e ingenierías no civiles.

La elección de realizar las sesiones de inducción de ciberseguridad en las cátedras de Introducción a la Ingeniería, fue un acierto, se alcanzó un 60 % de alumnos participantes en las sesiones, lo que genera una buena base de estudiantes con conocimientos de ciberseguridad. Sin embargo, el 40 % restante no recibe estos contenidos, esto no es malo, de hecho deja un buen margen de mejora continua para una segunda iteración del sistema.

Respecto al despliegue de servicios, utilizar GCE presentó varias ventajas, como lo es la capacidad del sistema. Esta no presentó latencias ni problemas de disponibilidad por sobrecarga de servicios. Esto se debe a que los correos electrónicos no fueron entregados de forma inmediata, dado que se configuró la entrega de los correos dentro de un margen de tiempo de 48 horas (para el segundo experimento de *phishing*).

Si se hubiese configurado Gophish para que el despacho de correos fuera de dos semanas (como fue en el primer experimento), los resultados del segundo experimento se hubiesen visto afectado por la difusión de la campaña entre pares.

Utilizar un servidor de correos electrónicos propios presenta ventajas frente a utilizar el servicio de un tercero, debido a lo siguiente: Los proveedores de correos electrónicos poseen una política que limita la cantidad de correos que una cuenta puede enviar y recibir. Además, al momento de crear una cuenta, se acepta el "*no utilizarla para hacer envío de spam, distribuir virus ni abusar del servicio de ninguna otra forma*"[Google, 2024]. Sin embargo, la configuración del servidor de correo propio fue un desafío, principalmente por la configuración de certificados en el servidor DNS y la reputación de la IP del servidor.

Inicialmente, se utilizó AWS para la configuración de *mailcow*, sin embargo, los correos enviados desde este no llegaban a las cuentas Gmail ni Outlook. Esto se debe a la reputación de la IP, ya que los servicios de hosts muchas veces son utilizados para *phishing* de forma maliciosa. Debido a esto, los *blacklisters*[19] reportan estas IP's a los proveedores de correos para que bloqueen cualquier correo entrante de algunas de esas IP's.

Es por lo anterior, que se toma la decisión de solicitar al DI un servidor con una IP pública

[19]Servicios que llevan un registro de la reputación de la IP para el envío de correos.

estática para desplegar el servidor de correo. Se revisa la IP en *dnsbl.info*, arrojando que no está en una *blacklist* y esto permite finalmente el despacho de correos electrónicos.

5.2. ANÁLISIS DE RESULTADOS

La configuración inicial efectuada por los administradores del sistema de correo no permitió concretar de manera apropiada la entrega de los correos de la primera campaña, por lo que no es posible obtener el PPP de los estudiantes previo a la inducción y la campaña promocional. Por consiguiente, se toma la decisión de utilizar las métricas promedio de América del Sur obtenidas por KnowBe4. La reducción en el PPP resulta especialmente notable, ya que la base de estadísticas utilizadas sugiere que la reducción obtenida es esperable para un trabajo de campañas y educación de un año, es decir, un PPP esperado de 10.2 % y se obtiene un 8.1 %.

La administración del sistema de correos, en consecuencia de lo sucedido, desarrolla un proceso de preparación de los servidores de correo electrónico para *ethical phishing*. Esto demuestra que la institución no contaba con la madurez para poder llevar a cabo un proceso de *ethical phishing*, y que con el desarrollo de esta memoria ahora poseen un proceso de preparación para este tipo de ejercicios.

Se puede establecer una aproximación de la capacidad de respuesta de los estudiantes, a partir del *debriefing* inicial de las inducciones, lo que permite respaldar la referencia estadística de KnowBe4. El 73 % de los estudiantes participantes de la inducción no revisaban quién envía el correo, el simple acto de revisar quién envía el correo, evita ser víctima de uno de estos ataques. Además, el 95 % de los estudiantes no realizaban la acción de verificar que el dominio real del enlace tenga relación con el contenido mostrado por la página.

Esta instancia disminuyó una gran brecha de conocimientos que traen consigo los estudiantes. Un 80 % de los estudiantes nunca había recibido una inducción de ciberseguridad, por lo que no sabían cómo defenderse de este tipo de ataques. El apoyo de que se realicen este tipo de instancias alcanza un 94.4 % dentro de los estudiantes de primer año.

Este sistema de inducción permite un ahorro financiero para la Universidad en este tipo de instancias. El servicio ofrecido por la empresa de ciberseguridad, si es solicitado para que se realice durante 4 veces al año, considerando a todos los estudiantes de primer año, este tendría un coste de $USD 99,200 al año. Mientras que llevar a cabo las 4 instancias del SIC USM significa un costo de $USD 2,616 al año, siendo significativamente menor en comparación. Cabe recalcar que la difusión de estas campañas se ve impulsada por el cumplimiento normativo nacional como institucional.

5.3. RECOMENDACIONES

Este sistema de inducción de ciberseguridad está diseñado para poder ser aplicado en todo tipo de ambiente laboral y/o académico, por lo que puede ser perfectamente aplicado también para los funcionarios de la Universidad o para el ambiente en que el lector de esta memoria necesite.

En caso de ser necesario realizar una segunda inducción de ciberseguridad, esta debe ser enfocada en los estudiantes y/o trabajadores que sean reincidentes en el segundo *ethical phishing*, esto para optimizar tiempo, esfuerzo y dinero en mejorar los conocimientos y prácticas de ellos.

Una recomendación personal del autor es que, si detectan una falla, mejora o la necesidad de un proceso, tomen acción lo antes posible, ya que contar con un proceso necesario (como lo es SIC USM) con anterioridad, es mucho mejor que esperar a necesitarlo como contra medida (como lo puede ser un seguro de vida).

5.4. TRABAJO FUTURO

Para poder ver en su máximo funcionamiento el SIC USM, primero que todo, debe ser implementado como un proceso más en el funcionamiento cotidiano de la Universidad y que este sea aplicado a todos los estudiantes de primer año. Sin embargo, se ha quedado en el tintero realizar un estudio completo, es decir llevar a cabo 4 instancias del sistema y analizar los resultados y evolución de los estudiantes en cada una de ellas.

Respecto a las funcionalidades de Gophish, en esta oportunidad no se pudo implementar un servicio de monitoreo IMAP para contabilizar la cantidad de estudiantes que reportan un phishing. El poder contar con cantidad de estudiantes/funcionarios que reportan este tipo de correos implicaría tener un mejor conocimiento de como es la capacidad de respuesta de los sujetos estudiados.

Para quien tome este proyecto en el futuro, se recomienda establecer las comunicaciones con la DGD para establecer las instancias de inducción de ciberseguridad durante el mes de enero, para que sean realizados los experimentos antes de que los estudiantes ingresen a clases.

Otra recomendación es implementar este sistema dentro de la asignatura de Programación, esto debido a que no todas las carreras cuentan con Introducción a la Ingeniería durante el primer semestre (como lo es el caso de Ingeniería Civil Informática) y viceversa para los estudiantes que no tengan Introducción a la Ingeniería el segundo semestre.

5.5. COMENTARIOS FINALES

Todo nuevo proceso siempre es un desafío, en este caso el proceso de ciberseguridad diseñado, desarrollado e implementado, es el primero que es desarrollado en toda la historia de la universidad. Los resultados mostrados evidencian que es posible ejecutar este tipo de procesos para la formación de estudiantes con los recursos mínimos, pero necesarios para el buen funcionamiento de este.

El desafío más grande presentado en la memoria fue sin duda el despliegue y configuración del servidor de correos, esto principalmente porque es la primera vez que el autor incursionaba en este tipo de sistemas, desconociendo los requerimientos tan finos de seguridad que se necesita para tener un servidor de correos en óptimas condiciones.

Si bien en esta memoria solo se llevó a cabo una implementación, es necesario que este sistema sea implementado de forma permanente en la universidad, sobre todo para el cumplimiento de la nueva ley de seguridad informática. Es por ello que el autor espera de cierta forma seguir siendo parte de este sistema, para ver cómo evoluciona y cómo se puede mejorar.

ANEXOS

		MATRIZ DE RIESGO				
		IMPACTO				
		Mínimo	Menor	Moderado	Mayor	Catastrofico
PROBABILIDAD		1	2	3	4	5
Muy Alta	5	5	10	15	20	25
Alta	4	4	8	12	16	20
Media	3	3	6	9	12	15
Baja	2	2	4	6	8	10
Muy Baja	1	1	2	3	4	5

Bajo Riesgo	
Riesgo Moderado	
Riesgo Alto	
Riesgo Extremo	

Figura 29: Matriz de Riesgo.
Fuente: Elaboración Propia.

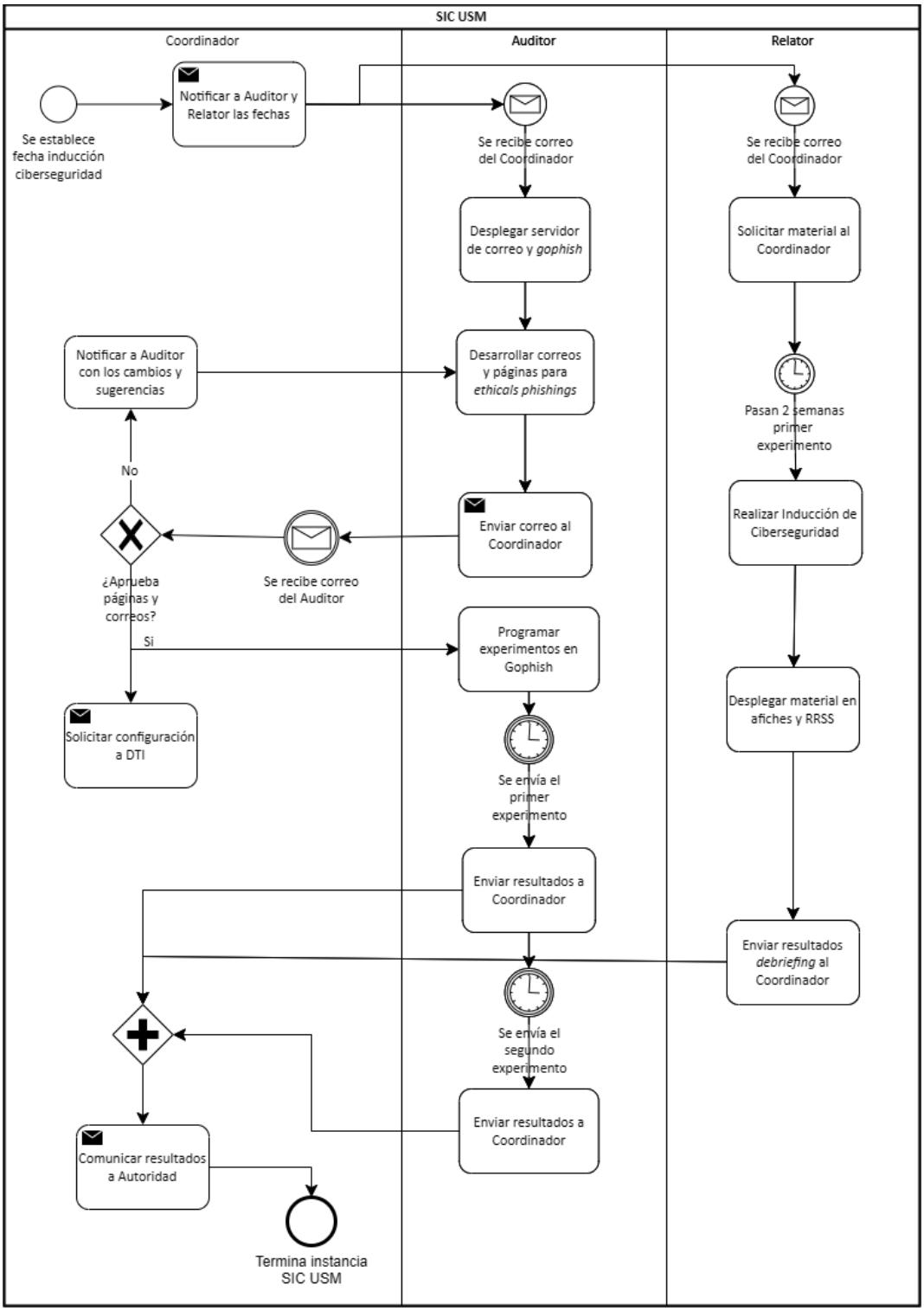


Figura 30: Diagrama SIC USM
Fuente: Elaboración propia

Figura 31: Material SIC USM
Fuente: Elaboración propia

Figura 32: Material SIC USM
Fuente: Elaboración propia

Figura 33: Material SIC USM
Fuente: Elaboración propia

Figura 34: Material SIC USM
Fuente: Elaboración propia

Figura 35: Material SIC USM
Fuente: Elaboración propia

Figura 36: Material SIC USM
Fuente: Elaboración propia

Figura 37: Material SIC USM
Fuente: Elaboración propia

Figura 38: Material SIC USM
Fuente: Elaboración propia

Figura 39: Material SIC USM
Fuente: Elaboración propia

Figura 40: Material SIC USM
Fuente: Elaboración propia

Figura 41: Material SIC USM
Fuente: Elaboración propia

Figura 42: Material SIC USM
Fuente: Elaboración propia

Figura 43: Material SIC USM
Fuente: Elaboración propia

Figura 44: Material SIC USM
Fuente: Elaboración propia

Figura 45: Material SIC USM
Fuente: Elaboración propia

Figura 46: Material SIC USM
Fuente: Elaboración propia

Figura 47: Material SIC USM
Fuente: Elaboración propia

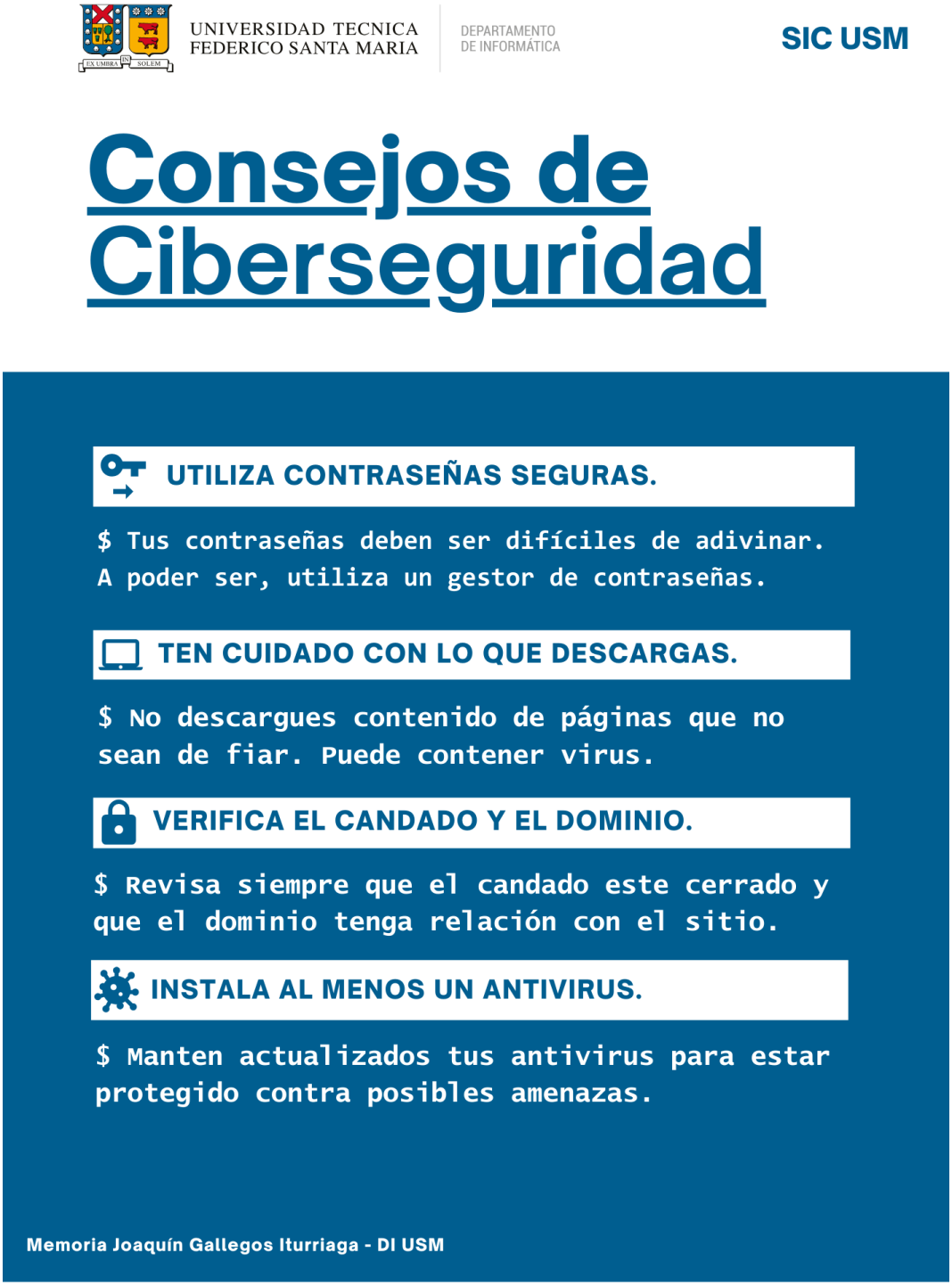


Figura 48: Afiche SIC USM
Fuente: Elaboración propia

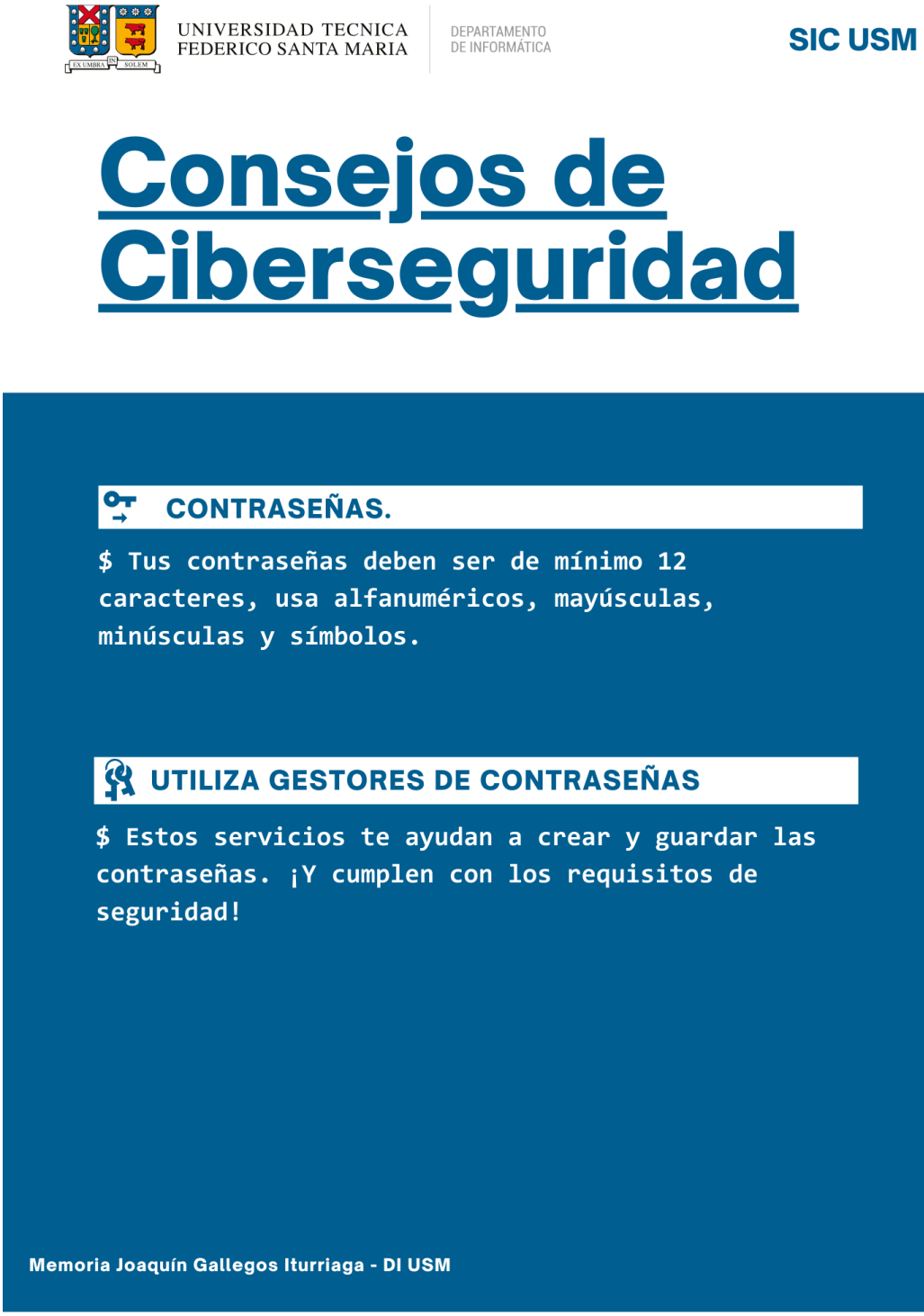


Figura 49: Afiche SIC USM
Fuente: Elaboración propia

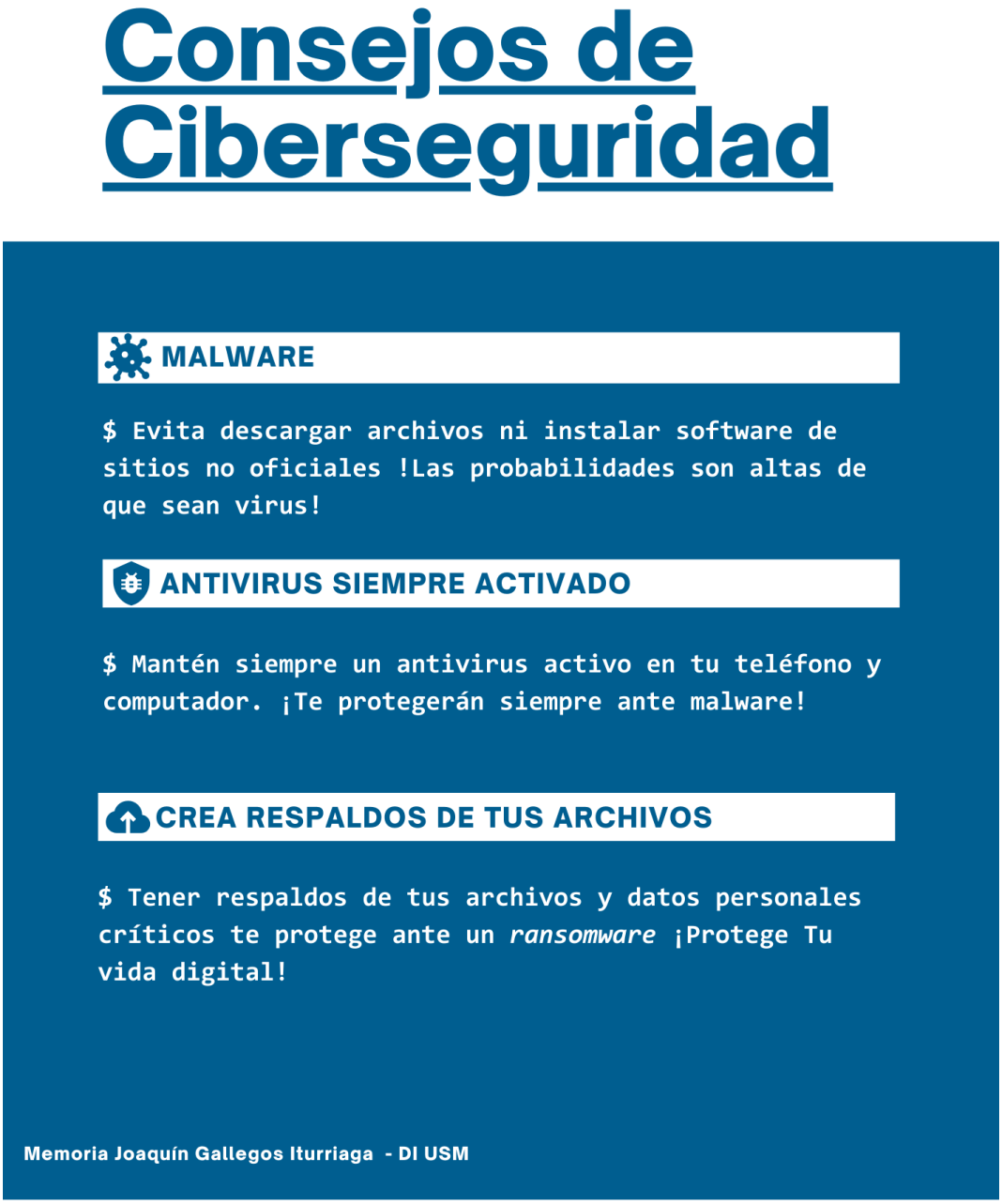


Figura 50: Afiche SIC USM
Fuente: Elaboración propia

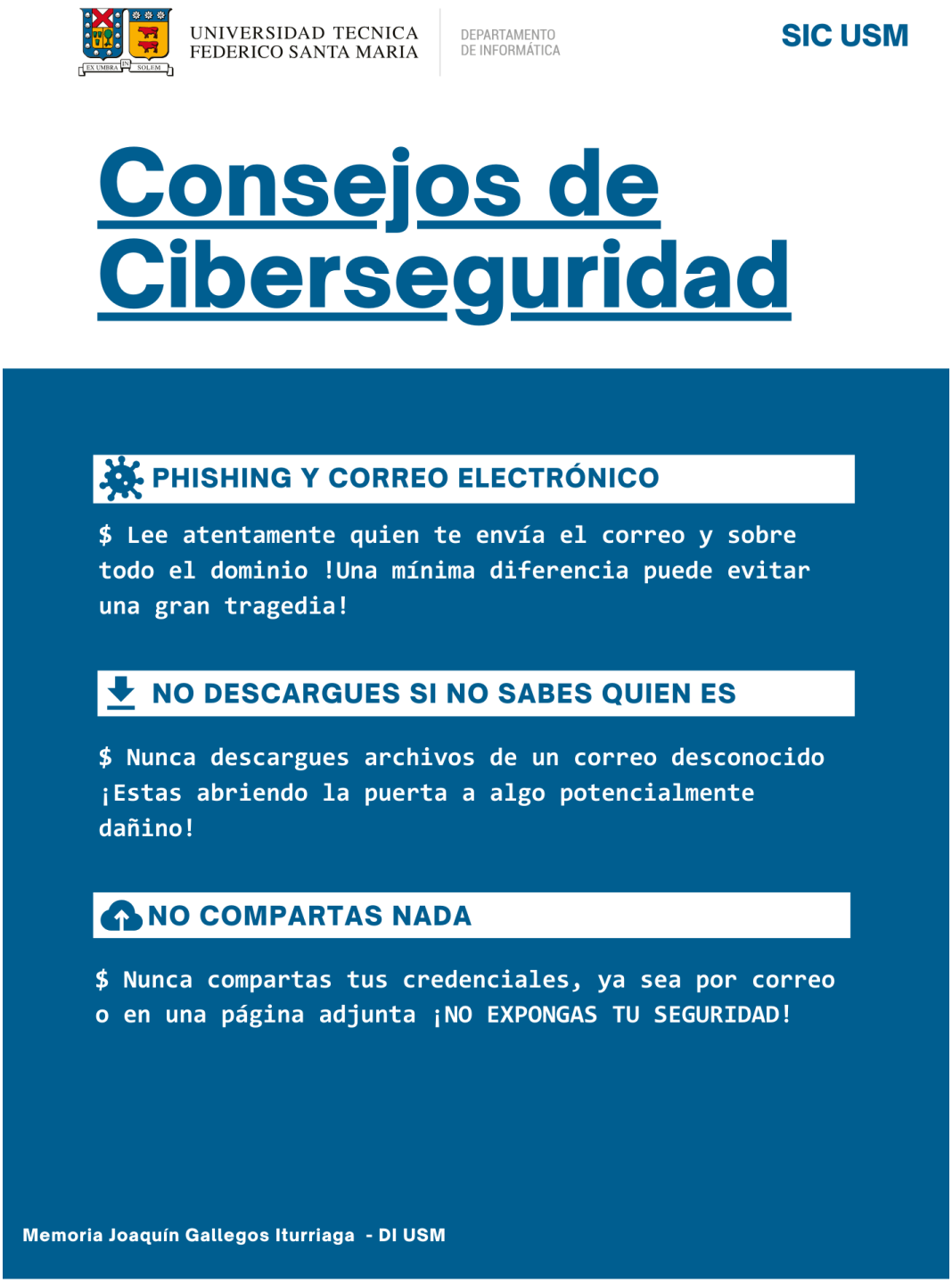


Figura 51: Afiche SIC USM
Fuente: Elaboración propia

REFERENCIAS BIBLIOGRÁFICAS

[Collard, 2023] Collard, A. (2023). Phishing by industry benchmarking report 2023. *KnowBe4*.

[Dash y Ansari, 2022] Dash, B. y Ansari, M. F. (2022). An effective cybersecurity awareness training model: First defense of an organizational security strategy. *International Research Journal of Engineering and Technology, vol. 9, n° 4*.

[Díaz, 2021] Díaz, M. (2021). Debriefing en simulación clínica: ¿qué es y cómo realizarlo? https://codimg.com/healthcare/blog/es/debriefing.

[Finn y Jakobsson, 2007] Finn, P. y Jakobsson, M. (2007). Designing ethical phishing experiments. *IEEE Technology And Society Megazine*.

[George A. Thomopoulos y Fidas, 2023] George A. Thomopoulos, D. L. y Fidas, C. A. (2023). Methodologies and ethical considerations in phishing research: A comprehensive review. *CHIGREECE*.

[Google, 2024] Google (2024). Política de spam y de abuso de gmail. https://support.google.com/a/answer/178266?sjid=7717059662475637538-SA.

[ISO, 2020] ISO (2020). Iso27001. https://www.normas-iso.com/iso-27001/.

[karspersky.com, 2024] karspersky.com (2024). ¿qué es la ingeniería social? https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering.

[MinInterior, 2018] MinInterior (2018). Conciencia digital. https://www.concienciadigital.gob.cl/#tenconciencia.

[Negocios, 2021] Negocios, B. (2021). El uso de teléfonos móviles a nivel mundial se duplicó en la última década. https://www.baenegocios.com/negocios/El-uso-de-telefonos-moviles-a-nivel-mundial-se-duplico-en-la-ultima-decada-20210506-0139.html.

[Rivas, 2023] Rivas, C. (2023). Senador pugh pidió oficiar a hacienda e interior por alerta de ciberseguridad que paralizó al sistema de compras públicas. https://www.df.cl/economia-y-politica/congreso/senador-pugh-pidio-oficiar-a-hacienda-e-interior-por-alerta-de.

[Rizzoni, 2022] Rizzoni, F. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health*.

[Sjouwerman, 2020] Sjouwerman, S. (2020). 91 % of cyberattacks begin with spear phishing email. https://blog.knowbe4.com/bid/252429/91-of-cyberattacks-begin-with-spear-phishing-email.

[U.S.DHHS, 1979] U.S.DHHS (1979). The belmont report. *Department of Health, Education, and Welfare*.

[UTFSM, 2024] UTFSM (2024). Políticas de datos. https://gobiernodedatos.usm.cl/politicas/.

[Welle, 2023] Welle, D. (2023). Masivo ciberataque secuestra los datos de cientos de portales en chile, colombia y panamá. https://www.biobiochile.cl/noticias/internacional/america-latina/2023/09/15/masivo-ciberataque-secuestra-los-datos-de-cientos-de-portales-en-chile-colombia-y-panama.shtml.

[Wilson y Hash, 2003] Wilson, M. y Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication 800-50*.

[Zúñiga y Zúñiga-Hernández, 2019] Zúñiga, C. y Zúñiga-Hernández, J. (2019). Excepciones al uso del consentimiento informado en investigación: ¿cuándo es esto posible en chile? *Rev Med Chile*.