Information Security Awareness in Organizations: Simulation of Web-Based Phishing Attack

JEAN-PIERRE VILLACURA, Universidad Técnica Federico Santa María, Chile

CCS Concepts: • **Security and privacy** → **Phishing**; • **Information systems** → *Intranets*; • **Human-centered computing** → Social engineering (social sciences).

Additional Key Words and Phrases: Information Security Awareness, Phishing, organizations

ACM Reference Format:
Jean-Pierre Villacura. 2023. Information Security Awareness in Organizations: Simulation of Web-Based Phishing Attack. 1, 1 (January 2023), 13 pages. https://doi.org/XXXXXXX.XXXXXXX

1 ABSTRACT

Un adecuado índice de ISA mantiene un comportamiento seguro y positivo en los trabajadores respecto a la seguridad de información. Esta investigación aplica el cuestionario HAIS-Q para la medición del ISA sobre académicos de distintos departamentos académicos de una organización educativa latinoamericana con los siguientes objetivos: 1) Ser la primera organización que aplica este instrumento en Latinoamérica, con la intención que en un futuro sirva como métrica de comparación con otras regiones y organizaciones, 2) Aplica un experimento de simulación de Phishing utilizando el framework Gophish para establecer una correlación entre el índice de ISA obtenido con el cuestionario HAIS-Q y comportamientos 'riesgosos' que puedan derivarse del personal humano medidos en el experimento, 3) Establecer fortalezas y debilidades del personal de la organización con el objetivo de plantear posteriormente mejoras.

2 INTRODUCCIÓN

Las organizaciones continuamente dedican esfuerzos en la implementación de contramedidas frente los ciberataques, causantes de pérdidas monetarias significativas año a año con una gran cantidad de incidentes de esta índole debido a explotaciones de elementos humanos [3]. Resulta relevante el estudio del comportamiento humano en temáticas de Phishing con el personal de la organización frente a amenazas mediante la ISA con el objetivo de establecer fortalezas y debilidades en el factor humano de las organizaciones para protegerse frente a ataques digitales.

3 TRABAJO RELACIONADO

Information Security Awareness(ISA) se ocupa del uso de programas de Seguridad de la Información para crear y mantener un comportamiento-seguro positivo **en los trabajadores** como un elemento crítico en un entorno efectivo de seguridad de la información [6]. El ISA es definido como el grado en el cual cada miembro de la organización entiende la importancia de la seguridad de la información, los niveles de seguridad de información apropiados a la organización y sus responsabilidades

Author's address: Jean-Pierre Villacura, jean-pierre.rojas@sansano.usm.cl, Universidad Técnica Federico Santa María, Av España 1680, Valparaíso, Chile,

XXXX-XXXX/2023/1-ART $15.00
https://doi.org/XXXXXXX.XXXXXXX

individuales respecto a la seguridad [5]. Su implementación es vital para las organizaciones al ocuparse del aspecto humano en los ataques y amenazas en Ciberseguridad. El Phishing forma parte de estas amenazas y es una técnica para intentar conseguir información confidencial a través de una solicitud fraudulenta en email ó sitio web [4], la medición de ISA considera este apartado con el instrumento HAIS-Q.

Este trabajo ocupa el cuestionario HAIS-Q para la planificación de ISA debido a que este instrumento en forma de encuesta resulta práctico y concreto para medir este factor en empleados en una variedad de contextos relacionados, sin embargo tambien existe otros Frameworks conceptuales que ofrecen una oportunidad para ser usados como approach para la planificación de ISA: Bounded Reality, Mental Models y Extended Parallel Processing Models [8] junto con teorías como Theory of Reasoned Action (TRA), Protection Motivation Theory (PMT) y Behaviourism Theory (BT), todos utilizados en el desarrollo de contenido relacionado con ISA para lograr una influencia positiva en la intención conductual de los empleados [3].

El uso del instrumento HAIS-Q posee ventajas frente a otras encuestas académicas relacionadas con el ISA ya que estas examinan una sola componente [6] siendo el cuestionario HAIS-Q el cuestionario más adecuado para medir la ISA en trabajadores al ser más completo debido a que considera una extensiva cantidad de áreas tales como: 'uso de correo electrónico', 'uso de internet', 'respuesta de incidentes', 'gestión de claves', 'uso de redes sociales', 'uso de Dispositivos móviles' y 'manejo de la información', todas abarcando desde la perspectiva del comportamiento humano, lo que es deseable para los propósitos de esta investigación.

A nivel organizacional, el tipo de organización y la modalidad de trabajo son factores que influyen en la Information Security Awareness. Solic et al. [7] descubrieron que empleados en Croacia dentro del sector privado tienden a tener un mayor comportamiento riesgoso en el uso de sistemas de información y menores niveles de Information Security Awareness que trabajadores de empresas públicas. Por otra parte, Hadlington [2] menciona que trabajadores que suelen trabajar remoto tienden a tener un menor nivel de ISA que quienes trabajan presencial en Reino Unido.

Existe una cantidad considerable de organizaciones que han aplicado el instrumento HAIS-Q para medir el Information Security Awareness de sus trabajadores[1]. Sin embargo, no existe investigación de esta temática en organizaciones Latinoamericanas ni tampoco en personal académico de universidades. Resulta interesante entonces la aplicación de este instrumento para medir la ISA en una organización educativa Chilena ya que nos permite, en primera instancia, tener una medida de la conciencia de la seguridad de la información en una institución chilena, lo cual podría en trabajos posteriores ser un base para que puedan realizarse comparaciones entre estos índices arrojados por la encuestade este índice entre paises y/o organizaciones. Por otra parte resulta interesante la idea de enfocar el estudio en una organización latinoamericana ya que a pesar que no han habido aplicaciones masivas de este cuestionario para la medición de ISA en distintas organizaciones y paises que sirvan de comparación, se puede esperar que Latinoamerica en promedio tenga peores puntuaciones que otros paises con normativas más estrictas relacionadas con el manejo de información, sin embargo, la hipótesis anterior no forma parte del estudio de esta investigación y actualmente en la literatura académica no existe una cantidad considerable de casos de aplicación de este instrumento para poder verificar esta idea, por lo que plantea abiertamente como trabajo posterior.

Nuestra pregunta de investigación es cómo varían los niveles de ISA dentro de académicos de distintos departamentos en una institución educativa como la UTFSM, visto desde una temática de comportamiento del personal humano sometidos a un escenario simulado de Phishing, lo que resulta completamente relevante para la mejora continua de la organización en temáticas de capacitación a sus académicos que la conforman.

4 APORTES DE ESTA INVESTIGACIÓN

En la literatura científica, hasta el momento no existe la aplicación de un instrumento para la medición del ISA en alguna organización situada en Latinoamérica. Por lo que esta investigación pretende formar una base en la medición de este concepto sobre la literatura académica con la idea que en trabajos posteriores pueda servir como parámetro para la realización de comparaciones de este concepto en distintas organizaciones diferenciada por países.

La aplicación de esta encuesta en una organización educativa Chilena tambien traería como aporte la determinación de fortalezas y debilidades en el personal de la organización, además de brindar la posiblidad de encontrar alguna relación entre bajos indices de ISA y comportamientos efectivamente 'riesgosos' ante un escenario simulado de Phishing. Esta idea de establecer relaciones entre un bajo índice de ISA y comportamientos riesgosos podría ser tambien objeto de estudio en investigaciones posteriores, que reforzaría aún más los alcances e implicaciones del estudio de ISA.

5 AIMS OF THE RESEARCH

Al conducir el experimento de Pishing, se espera que efectivamente los departamentos académicos ligados al uso de TI y Ciencias de la Computación tengan mejores niveles de ISA que los otros, y a su vez tengan una menor cantidad de comportamientos considerados 'riegosos' en el experimento, por lo que nuestra investigación busca abordar las siguientes preguntas:

- ¿Cómo son los índices de Information Security Awareness entre los distintos departamentos académicos?
- ¿Cómo es el comportamiento de los académicos de distintas disciplinas cuando son enfrentados a situaciones de Phishing Simulado?
- ¿Existe una correlación entre los niveles percibidos de ISA y un comportamiento que pueda ser considerado 'riesgoso' en escenarios de Phishing?

La primera variable dependiente **V.D.1** corresponde al nivel de ISA arrojado por el cuestionar Hais-Q[5]. El cual es distinto para cada persona que realiza el cuestionario.

La segunda variable dependiente **V.D.2** corresponde al comportamiento del usuario en la simulación de una situación de Phishing, en concreto si acierta o falla en reconocer una acción riesgosa en el escenario de Phishing.

En cuanto a la variable independiente **V.I.1** se tiene el departamento académico al que pertenecen los participantes, los cuales para esta investigación corresponden a los académicos de la organización educativa UTFSM de ciertos departamentos informados en la sección de metodología.

Con respecto a la tercera pregunta, notar que la variable dependiente**V.D.1** se transforma en una variable independiente y en este caso el comportamiento 'riesgoso' para a ser la variable dependiente, asignada como una variable discreta con valores de 0 ó 1. Las hipótesis de investigación son las siguientes:

- 1) Los departamentos académicos ligados al uso de tecnologías de Información y Ciencias de la computación tendrán mejores niveles de ISA (En la sección de Participantes se detalla la lista de departamentos).
- 2) Aquellos departamentos con mejores niveles de ISA, ejecutarán una menos comportamientos riesgosos.

El fundamento teórico de ambas hipótesis radica en que Khando et al.[3] propone que las características demográficas de la población de estudio y niveles de educación tienen efectos considerables en la medición del ISA.

6 METODOLOGÍA

6.1 Resumen

La metodología de esta investigación se basa en la aplicación del cuestionario HAIS-Q[5] para la medición del ISA, asignando como población de estudio a académicos de la organización educativa Chilena UTFSM, Casa Central y posteriormente la realización de un experimento que consiste en un escenario simulado de situación de Phishing enviada a los correos electrónicos con un Link suplantador de identidad que al pincharlo en el navegador dirige a un sitio web suplantador de identidad con aspecto idéntico al portal original, el cual pide el ingreso de credenciales al participante para interceptar sus credenciales. La idea es verificar las hipótesis H1. tabulando los datos obtenidos mediante la aplicación de esta encuesta, validada para este propósito en los papers de Parsons et al. [6] [5] y revisar si existe una relación con H2 en cuanto al comportamiento de los participantes según los niveles de ISA tabulados anteriormente.

Los etapas propuestas en la Figura 1 corresponden a 1) Informar a la población de estudio la aplicación de determinados tests sin mencionar intencionadamente este test específico, 2) el envío de este cuestionario en un formato Web-Based, 3) Lanzamiento de la campaña de Phishing enviando un correo de simulación de Phishing que recopila si el usuario accede al enlace secuestrador y envía sus credenciales y por último 4) donde se da término a la campaña con un periodo de duración de 1 mes procediendo a la tabulación de resultados y se informa a la población de estudio el motivo del experimento, fortalezas y debilidades encontradas en el personal mencionando aspectos de mejora como retroalimentación y se concluyen resultados de la investigación.

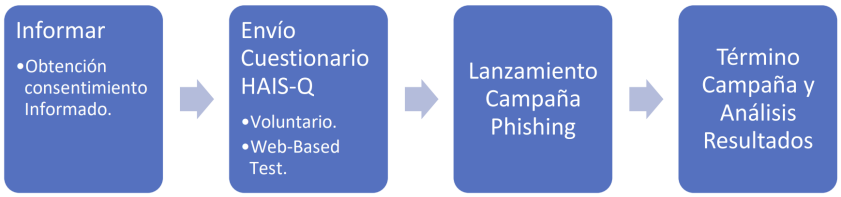

Fig. 1. Metodología Propuesta

El motivo principal de escoger como población a académicos jornada completa de la organización educativa UTFSM Casa Central corresponde a ajustar el problema investigativo a una primera versión partiendo de un conjunto pequeño, se espera que en trabajos posteriores se consideren a todos los funcionarios de la organización y pueda ampliarse la población de estudio.

6.2 Participantes

La investigación está dirigida hacia académicos de la Universidad Técnica Federico Santa María en el Campus Casa Central. Se realiza una distinción por el departamento de enseñanza al que pertenecen los participantes, lo cual forma parte de la Variable Independiente en las preguntas RQ1 y RQ2. En cuanto a características demográficas, según Khando La edad, la industria de trabajo y los niveles de educación tienen efectos significativos en el ISA[3] lo que sustenta teóricamente las hipótesis planteadas en esta investigación, en este caso intuitivamente se podría esperar que académicos más jovenes y pertenecientes a áreas afines a TI y CS tengan mejor desempeño en la encuestra al estar más expuestos a la reciente tecnología.

Notar que en esta organización existen los departamentos académicos y los departamentos docentes, se consideran sólo los departamentos académicos al estar todos dentro del campus

Casa Central con una razón de acotar la población de estudio. Con respecto a las características demográficas: La edad de los participantes está dentro del rango de edad en las personas pueden legalmente trabajar, por lo que se estima que sea entre los 18 y 80 años según legislaciones Chilenas y esperanza de vida. La industria de trabajo pertenece al sector privado y los trabajadores suelen tener capacitaciones y envío de información constante sobre el uso de tecnologías de información, por lo que los niveles de educación podrían considerarse estándar.

La lista de los departamentos que se consideran ligados fuertemente al uso de tecnologías de Información y Ciencias de la Computación se resume en la siguiente tabla:

Departamentos Ligados suavemente al uso de TI y CS	Departamentos Ligados fuertemente al uso de TI y CS
Departamento de Aeronáutica	
Departamento de Arquitectura	
Departamento de Diseño y Manufactura	
Departamento de Ed. Física, Deportes y Recreación	
Departamento de Electricidad	
	Departamento de Electrónica
	Departamento de Informática
Departamento de Estudios Humanísticos	
Departamento de Industrías	
Departamento de Ingeniería Comercial	
Departamento de Ingeniería Metalúrgica y Materiales	
Departamento de Ingeniería Química y Ambiental	
Departamento de Matemática	
Departamento de Mecánica	
Departamento de Obras Civiles	

Table 1. Clasificación de Departamentos académicos según vínculo con Tecnologías de Información y Ciencias de la computación

Las razones detrás de esta categorización se basan según el programa académico impartido por los departamentos a las carreras de Ingeniería e Ingeniería Civil en el campus Casa Central, donde se determina que se encuentras más ligadas al área de Ciencias de Computación y Tecnologías de Información según las asignaturas impartidas en la malla curricular. Además, se espera que el orden de funcionarios sea cerca de 400 en Casa Central. De momento capacitaciones en materias de Ciberseguridad han sido mínimas por parte de la organización, por lo que de arrojar debilidades esta investigación en este aspecto podría promover la aplicación de campañas más fuertes relacionadas con la seguridad de la información a los funcionarios.

6.3 Ventajas y Desventajas

El uso del cuestionario HAIS-Q es adecuado en esta investigación debido al ser de uso modular, permitiendo escoger las dimensiones y áreas más adecuadas para la medición, en este caso relacionadas directamente con el Phishing: 'Email Use', 'Internet Use' y 'Incident Reporting'. Otros instrumentos que miden este constructo miden sólo una perspectiva por lo que no resultan adecuados para 'reflejar' un panorama general a nivel individual y organizacional respecto al ISA [5],

siendo la opción más viable el uso de HAIS-Q para medir este apartado al considerar 7 dimensiones: Password Management, Internet Use, Social Media Use, Mobile Devices, Information Handling, Incident Reporting y Email Use[5]. Una de las desventajas del diseño de este experimento es que no se analiza a todos los actores que conforman la organización, sólo a los académicos que responden la encuesta, por lo que los resultados podrían no ser tan representativos a la realidad, esto debido a que al ser una primera versión de este experimento es buena idea acotarlo.

6.4 Etapas de la investigación

De acuerdo a los fines de la investigación, las personas participantes del experimento se les pide completar el cuestionario HAIS-Q de manera voluntaria enviándoles el set de preguntas en formato Web-Based Form mediante el correo corporativo. Durante esta primera etapa 'Informar', es requerido que las directivas de la organización firmen el consentimiento informado para que los empleados puedan ser sometidos a este experimento. Se utiliza como instrumento de medición el Cuestionario HAIS-Q para la medición de Information Security Awareness, que contiene 63 preguntas y se enfoca en 7 áreas particulares: Password Management, Internet Use, Social Media Use, Mobile Devices, Information Handling, Incident Reporting y Email Use [5]. El cuestionario permite el uso de sub-áreas y sub-items para la medición del ISA en áreas específicas, por lo que el set de preguntas se enfoca principalmente en las áreas de comportamiento correspondientes a 'Email-Use', 'Internet-Use' y 'Incident-Response', todas directamente relacionadas con comportamiento humano ante ataques de Phishing las que son enviadas en formato Web-Based a su correo.

La etapa 1 consiste en conseguir el consentimiento informado desde la directiva de la organización para continuar con el experimento, de las que se sugiere la participación del comité de ética de la Organización para que exista un respaldo legal y ético para la realización de este experimento. Cuando se consigue esta aprobación, continua la etapa 2 donde se procede al envío del cuestionario HAIS-Q mediante correo electrónico desde la directiva explicando que durante el presente periodo(1 mes) serán realizados ciertas encuestas pidiendo colaboración a los académicos y al mismo tiempo mencionando que la participación es voluntaria para concretar posteriormente el envío del cuestionario HAIS-Q en formato Web-Based a la población de estudio, este formato contiene los siguientes ítems de pregunta y se evalua con formato Likert entre 1-5: Strongly Desagree – Strongly Agree, como muestra en la Tabla 2.

En la etapa 3 corresponde el lanzamiento de la campaña Phishing utilizando el Framework GoPhish[9], el cual permite realizar con facilidad campañas de Phishing pudiendo establecer la estructura de la página secuestradora, enviar los correos de simulación de Phishing y recopilar los datos de los participantes que incurran en acciones riesgosas en el experimento.
De esta manera, utilizando un formato de cuerpo de correo similar al que utiliza la organización con la diferencia de un dominio diferente, se envía un correo a la misma población objetivo que en la encuesta mencionando la necesidad de entrar al portal para poder actualizar sus datos personales, como muestra la siguiente figura:

Fig. 2. Estructura Correo en el Experimento de Phishing

Dado que es una simulación de situación de Phishing, la dirección a la que apunta el correo al cliquear el enlace es el sitio 'suplantador de identidad'.
Hasta el momento existen 2 comportamientos riesgosos, el primero es no notar que el dominio emisor de este correo no pertenece a la Institución y el segundo es no notar que la dirección que apunta el correo al pinchar el enlace no corresponde al sitio web del portal de la institución. Estos comportamientos son medidos en el cuestionario enviado y además es posible tabular resultado de las personas que pinchen el enlace y envien sus credenciales en la página secuestradora.
En el caso de pinchar el enlace que apunta el correo, se abrirá un sitio que simula ser el portal de la Organización, con una estructura de página web idéntica al sitio real, con la diferencia que la dirección web no es auténtica al no pertenecer al dominio de la Universidad, como muestra la siguiente Figura 3:

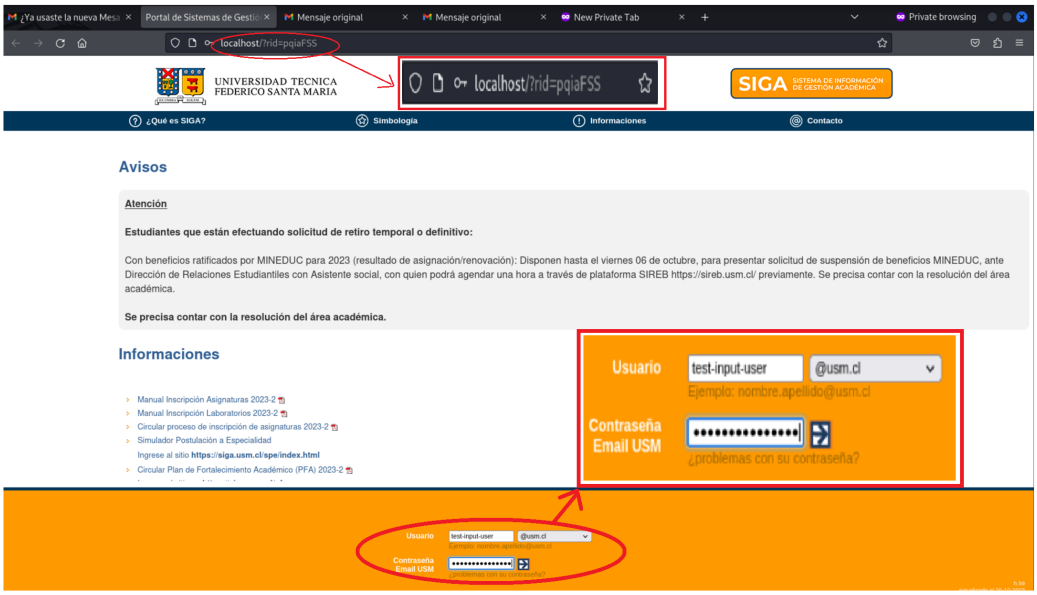

Fig. 3. Experimento: Portal Escenario de Phishing

Si el participante del experimento no se da cuenta de las consideraciones anteriores, ingresa sus credenciales y presiona el botón de envío en el portal, se ejecuta efectivamente un comportamiento riesgoso el cual será estadísticamente registrado para responder la tercera pregunta de investigación. Una vez finalice el periodo asignado para la campaña(1 mes), se procede con la etapa 4: Término Campaña y Análisis de resultado' donde se analizan los datos obtenidos utilizando estadísticas que el framework utilizado GoPhish arroja, tales como cantidad de personas que clickean el link y envían sus datos al sitio secuestrador de información en el experimento de Phishing. A continuación se muestra una imagen de la interfaz de este framework cuando arroja los resultdos de la campaña:

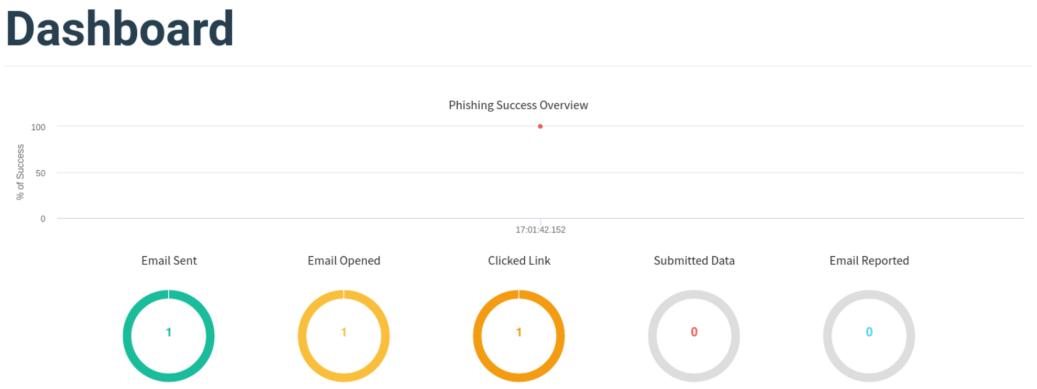

Fig. 4. Imagen de Dashboard de Framework para campañas de Phishing

Corresponde luego analizar las estadísticas arrojada por el cuestionario enviado por Web-Based Form. De esta información es posible dar respuesta a nuestra primera pregunta de investigación.

Analizando los participantes que enviaron sus datos en el sitio simulado de Phishing, diferenciándolos por el link de la campaña en que se encuentran asociados según departamento académico, se puede establecer la estadística de cuantos participantes actuaron riesgosamente, y con esta información es posible responder la segunda pregunta de investigación.
Para responder a la tercera pregunta de investigación, nuestra variable Dependiente 'Nivel de ISA' tabulado según departamento académico para a ser independiente y la cantidad de comportamientos riesgosos realizados pasa a ser la variable dependiente. A continuación se resumen los siguientes comportamientos que podrían ser considerados riesgosos ante ataques de Phishing por parte de los académicos y que efectivamente son evaluados en el instrumento HAIS-Q:

Focus Area – Behaviour (HAIS-Q Items)	Pregunta de HAIS-Q	Comportamiento
Email Use	"If an Email from an unknown sender looks interesting, I click on a link within it. "	Usuario debería fijarse en la dirección de correo del remitente en el correo enviado como simulación de Phishing.
Internet Use	"I assess the safety of websites before entering Information."	Antes de pinchar el link, usuario debería fijarse que el dominio del enlace pertenece al dominio de la organización.
Password Management	"I use a different password for my Social media and work accounts."	Potencialmente riesgoso.
Incident Reporting	"If I noticed a security incident, I would report it."	Usuario al darse cuenta de un fenómeno extraño (Correo remitente e hipervínculos no perteneciente a dominio organizacional) debería reportarlo.

Table 2. Área de Medición, Preguntas y Comportamiento en Experimento

De estas cuatro preguntas, las dos primeras, correspondientes a la dimensión "Email Use" y "Internet Use" son las relevantes al experimento y el comportamiento .

Luego de la aplicación de este experimento, se propone que la directiva envíe un correo agradeciendo la colaboración y mencionando la aplicación de esta encuesta, señalando las principales fortalezas y debilidades que arroja el test, además de enviar una serie de recomendaciones para mejorar el comportamiento humano respecto al Phishing.

7 PILOTO

Se propone como trabajo posterior la aplicación de un plan piloto siguiendo la metodología de este experimento. A continuación se muestra un formato de los resultados esperables, estas cifras han sido inventadas y la intención es que sirvan de guía para tener una idea del formato de los resultados. Suposiciones:

- La muestra que responde la encuesta tambien realiza el experimento.
- La directiva aprueba el experimento, entrega las direcciones de correo electrónico de la población cuya data se encuentra categorizada por departamento académico al que pertenecen.

- Se realiza una campaña distinta en el framework Gophish para cada departamento académico consiguiendo tener identificación del departamento académico al que pertenece el participante que clickea el enlace en el experimento.

En cuanto a la primera pregunta de investigación: "**¿Cómo son los índices de Information Security Awareness entre los distintos departamentos académicos?**", se espera una gráfica promedio del ISA v/s departamentos académicos como muestra la Figura 5 que pueda dar respuesta a esta pregunta:

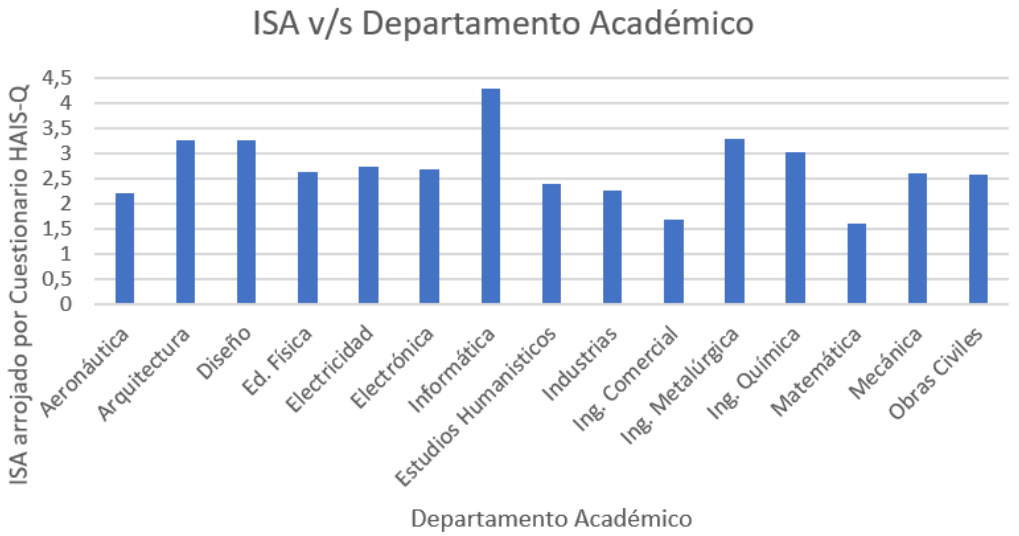

Fig. 5. Ejemplo de Piloto: ISA v/s Departamento académico

En la Hipótesis 1 se espera que los departamentos de Informática y Electrónica, declarados como afines a TI y Ciencias de la Computación reflejen un mayor nivel de ISA que los otros departamentos. La gráfica propuesta permite poder verificar esta hipótesis además de responder a la RQ1.

Para responder RQ2: "¿Cómo es el comportamiento de los académicos de distintas disciplinas cuando son enfrenta- dos a situaciones de Phishing Simulado?" nos podemos apoyar en la siguiente figura 6 la cual muestra el gráfico Número de participantes según comportamiento v/s Departamento académico.

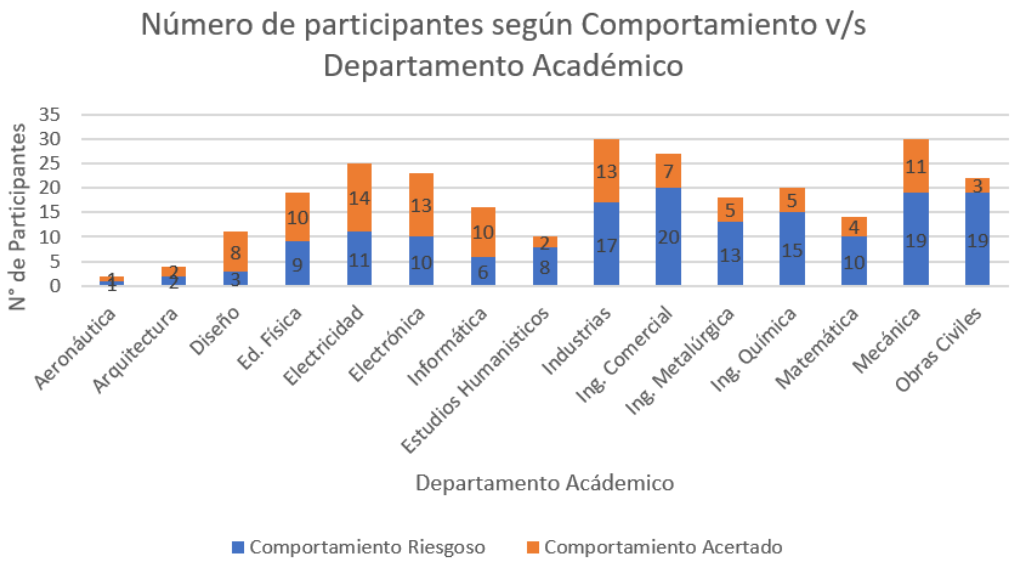

Fig. 6. Ejemplo de Piloto: N° de participantes según comportamiento en el experimento v/s Departamento Académico

Para este caso se considera como comportamiento riesgoso cuando el participante decide abrir el link del correo electrónico de Phishing del experimento aún cuando existen señales evidentes de Phishing: 1) la dirección no corresponde con el dominio de la organización y 2) la dirección del sitio web a la que apunta el enlace tampoco corresponde con el dominio de la organización. En este caso se asume que todos los participantes del experimento leen el correo enviado y deciden no apretar el enlace debido al riesgo de Phishing, lo que se considera como comportamiento acertado.

Respecto a la RQ3: '¿Existe una correlación entre los niveles percibidos de ISA y un comportamiento que pueda ser considerado 'riesgoso' en escenarios de Phishing?' se propone la siguiente gráfica Factor Comportamiento Riesgoso v/s ISA en la Figura 7:

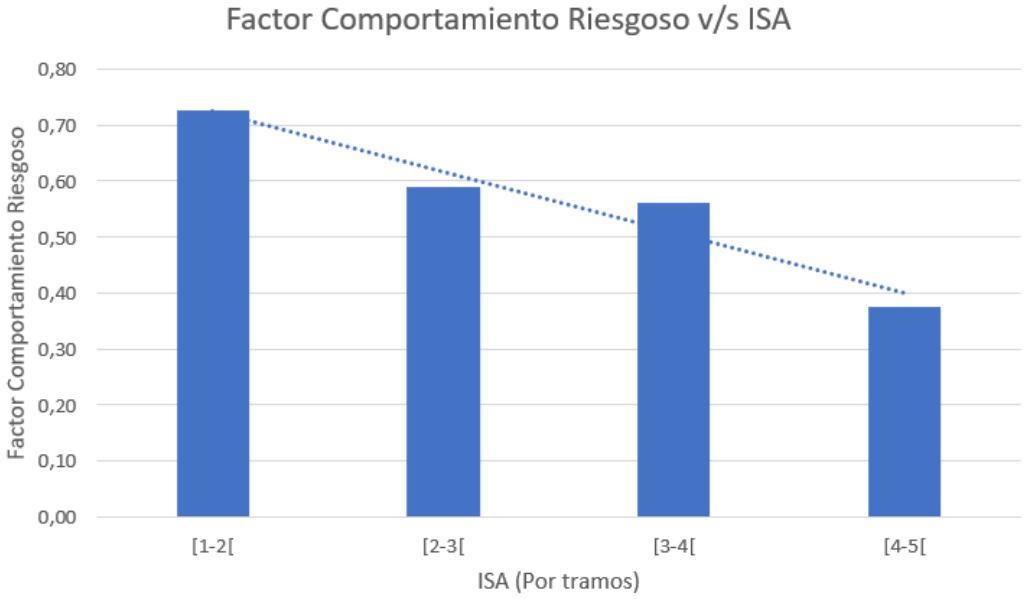

Fig. 7. Factor Comportamiento Riesgoso v/s ISA

Se establecen cuatro tramos de índices obtenidos de ISA según la encuesta aplicada: 1-2, 2-3, 3-4 y 4-5. Para cada tramo se calcula el promedio de Factor Comportamiento Riesgoso definido como el cociente entre la cantidad de comportamientos riesgosos detectados por tramo entre el la cantidad total de acciones por tramo(Considera los acertados y riesgosos), se espera encontrar una correlación entre los niveles de ISA y la ejecución de comportamientos riesgosos que apoyaría la Hipótesis 2.

Para el caso de departamentos académicos donde se encuentran debilidades según el puntaje obtenido en la encuesta se sugiere indicar consejos que expliquen como actuar adecuadamente ante estos casos con el objetivo fortalecer estos aspectos.

8 CONCLUSIÓN

El estudio del Information Security Awareness(ISA) en organizaciones resulta sumamente importante para identificar fortalezas y debilidades en el personal humano de la organización respecto a su comportamiento en temáticas de seguridad. Esta investigación pretende ser la primera en aplicar la encuesta de medición de ISA llamada HAIS-Q[6] en organizaciones educativas y Latinoamérica con la intención que en trabajos posteriores esta encuesta sea aplicada a multiples organizaciones en distintos paises para establecer comparaciones de ISA por región y tipo de organización lo que seguramente trará conclusiones interesantes.

Por otra parte, esta investigación además de aplicar la encuesta propone la realización de un experimento de situación de Phishing utilizando el framework GoPhish[9] a los académicos de distintos departamentos educativos de una organización educativa,previa aprobación por directivas y comité de ética de la Universidad, con la intención que pueda encontrarse alguna relación entre el nivel de ISA obtenido por académicos según el área de enseñanza al que pertenecen y la ejecución de comportamientos riesgosos en este experimento de situación de Phishing.

Se proponen las etapas de metodología para llevar a cabo un piloto de esta investigación junto

con gráficas esperables que se esperan obtener en la aplicación de este experimento. Fortalezas y debilidades del personal reveladas con la aplicación de la encuesta se sugiere que sean abordadas mediante técnicas para la mejora de ISA propuesto por Khando [3].

REFERENCES

[1] Alvin Cindana and Yova Ruldeviyani. 2018. Measuring Information Security Awareness on Employee Using HAIS-Q: Case Study at XYZ Firm. 289–294. https://doi.org/10.1109/ICACSIS.2018.8618219

[2] Lee Hadlington, Maša Popovac, Helge Janicke, Iryna Yevseyeva, and Kevin Jones. 2019. Exploring the role of work identity and work locus of control in information security awareness. *Computers & Security* 81 (2019), 41–48. https://doi.org/10.1016/j.cose.2018.10.006

[3] Khando Khando, Shang Gao, Sirajul M. Islam, and Ali Salman. 2021. Enhancing employees information security awareness in private and public organisations: A systematic literature review. *Computers & Security* 106 (2021), 102267. https://doi.org/10.1016/j.cose.2021.102267

[4] Michael Nieles, Kelley Depmsey, and Victoria Yan Pillitteri. 2017. An Introduction to Information Security. 81.

[5] Kathryn Parsons, Dragana Calic, Malcolm Pattinson, Marcus Butavicius, Agata McCormac, and Tara Zwaans. 2017. The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers and Security* 66 (2017), 40–51. https://doi.org/10.1016/j.cose.2017.01.004

[6] Kathryn Parsons, Agata McCormac, Marcus Butavicius, Malcolm Pattinson, and Cate Jerram. 2014. Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security* 42 (2014), 165–176. https://doi.org/10.1016/j.cose.2013.12.003

[7] K. Solic, T. Velki, and T. Galba. 2015. Empirical study on ICT system's users' risky behavior and security awareness. In *2015 38th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*. 1356–1359. https://doi.org/10.1109/MIPRO.2015.7160485

[8] G Stewart and Laceym D. 2012. Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security* 20 (2012). https://doi.org/10.1108/096852212112191827

[9] John Wright. 2017. An Introduction to Information Security. GoPhish: Open Source Phishing Framework. https://getgophish.com

Received 20 February 2007; revised 12 March 2009; accepted 5 June 2009