INNOVA RESEARCH JOURNAL
ISSN: 2477-9024

UIDE Powered by Arizona State University

ARTÍCULO ORIGINAL
INNOVA Research Journal, ISSN 2477-9024
(Septiembre-Diciembre, 2024). Vol. 9, No.4, pp. 95-110.
DOI: https://doi.org/10.33890/innova.v9.n4.2024.2678
URL: http://revistas.uide.edu.ec/index.php/innova/index
Correo: innova@uide.edu.ec

Simulación de ataques phishing y Planes de Concienciación aplicables al ámbito empresarial – Un enfoque práctico para mejorar la resiliencia organizacional

Simulation of phishing attacks and Awareness Plans applicable to the business environment – A practical approach to improve organizational resilience

Esthela Maribel Cabezas-Molina
Universidad Internacional del Ecuador, Quito, Ecuador
escabezasmo@uide.edu.ec
https://orcid.org/0000-0001-7166-8823

Hugo Christiam Fiallos-Aguilar
Universidad Internacional del Ecuador, Quito, Ecuador
hufiallosag@uide.edu.ec
https://orcid.org/0000-0002-7521-4922

Recepción: 16/09/2024 | Aceptación: 20/12/2024 | Publicación: 27/12/2024

Cómo citar (APA, séptima edición):
Cabezas-Molina, E., Fiallos-Aguilar, H. (2024). Simulación de ataques phishing y Planes de Concienciación aplicables al ámbito empresarial – Un enfoque práctico para mejorar la resiliencia organizacional. *INNOVA Research Journal*, *9*(4), 95-110. https://doi.org/10.33890/innova.v9.n4.2024.2678

Resumen

El estudio evaluó la efectividad de las simulaciones de ataques de phishing y planes de concienciación para reducir la vulnerabilidad de los empleados ante ataques cibernéticos en una pequeña empresa. Utilizando una muestra de 100 empleados, se analizaron las mejoras en la detección de correos fraudulentos y el tiempo de respuesta tras una serie de simulaciones y programas de formación. Inicialmente, los empleados tenían una tasa de clics en enlaces maliciosos del 65%, que se redujo al 20% tras la intervención, validado por un análisis de regresión y pruebas T con un p-valor menor a 0.001. El tiempo de respuesta mejoró de un promedio de 50 a 20 minutos. El análisis reveló que la edad, experiencia laboral y acceso a información sensible impactaron la capacidad de respuesta, con mejores resultados en empleados jóvenes y

tecnológicamente experimentados. Aunque la concienciación redujo la vulnerabilidad, persistieron riesgos asociados al comportamiento humano, sugiriendo la necesidad de formación continua y soluciones tecnológicas automatizadas. A pesar de las limitaciones de la muestra, los resultados indicaron que las simulaciones de phishing y programas de formación personalizados son herramientas valiosas para mejorar la seguridad cibernética. Se recomienda que las empresas implementen planes de concienciación dentro de estrategias integrales de ciberseguridad, ajustándolos a las características demográficas y niveles de responsabilidad de los empleados, y que futuras investigaciones aborden empresas más grandes y diversos tipos de ataques cibernéticos. El estudio concluye que estas estrategias efectivamente mejoran la capacidad de respuesta y detección de amenazas, construyendo una cultura organizacional más resiliente frente a la ciberseguridad.
Palabras claves: phishing, ciberseguridad, simulación, planes de concienciación, vulnerabilidad.

Abstract
The study evaluated the effectiveness of phishing attack simulations and awareness plans to reduce employees' vulnerability to cyberattacks in a small business. Using a sample of one hundred employees, improvements in detecting fraudulent emails and response times were analyzed following a series of simulations and training programs. Initially, employees had a 65% click rate on malicious links, which decreased to 20% after the intervention, validated by regression analysis and T-tests with a p-value less than 0.001. Response time improved from an average of 50 minutes to 20 minutes. The analysis revealed that age, work experience, and access to sensitive information impacted response capacity, with better results among younger, technologically experienced employees. Although awareness reduced vulnerability, risks associated with human behavior persisted, suggesting the need for ongoing training and automated technological solutions. Despite sample limitations, the results indicated that phishing simulations and personalized training programs are valuable tools for enhancing cybersecurity. It is recommended that companies implement awareness plans as part of comprehensive cybersecurity strategies, tailored to employees' demographic characteristics and responsibility levels. Future research should address larger companies and several types of cyberattacks. The study concludes that these strategies effectively improve threat response and detection, building a more resilient organizational culture towards cybersecurity.
Keywords: phishing, cybersecurity, simulation, awareness plans, vulnerability.

Introducción

La ciberseguridad se ha convertido en una prioridad para las organizaciones de todo el mundo debido al incremento de los ciberataques, especialmente aquellos que utilizan técnicas de ingeniería social como el phishing. Las campañas con ataques de phishing simulados constituyen uno de los medios de sensibilización más populares y que dan resultados. (Naciones Unidas, 2021).

La técnica cibernética de Ingeniería Social más utilizada es conocida como Phishing, por medio de la cual se logra obtener información confidencial de forma fraudulenta. El tipo de información sensible que se trata de obtener, son comúnmente: nombres de usuarios, contraseñas o incluso, información de tarjetas de crédito u otra información financiera de la víctima. El estafador conocido como phisher frecuentemente se hace pasar por una persona o empresa de

confianza en una aparente comunicación oficial electrónica. Por lo general, se trata de contactar con sus víctimas, por medio de un correo electrónico, o de algún sistema de mensajería instantánea, redes sociales, SMS/MMS, o incluso utilizando llamadas telefónicas. (Benavides-Astudillo, Fuertes-Diaz, & Sánchez-Gordón, 2019)

En este contexto, los planes de concienciación sobre seguridad informática juegan un papel fundamental. Sin embargo, muchas organizaciones aún subestiman la importancia de educar a sus empleados sobre las amenazas cibernéticas y cómo identificarlas. Este estudio busca abordar esta brecha mediante la simulación de ataques de phishing en un entorno controlado, evaluando la eficacia de un plan de concienciación diseñado específicamente para reducir la vulnerabilidad de los empleados frente a este tipo de amenazas.

El campo de la formación en ciberseguridad para usuarios finales es diverso en el diseño de la formación, los métodos de entrega, los temas de ciberseguridad y las medidas de efectividad. Encontramos resultados prometedores en la mejora del comportamiento en ciberseguridad a través de la formación para una variedad de conductas relacionadas con la ciberseguridad mediante una amplia gama de medios. Sin embargo, muchos aspectos del diseño de la formación son inciertos y podrían beneficiarse de cambios en la estructura y deliberación durante el proceso de diseño. Además, las medidas de resultado utilizadas para la evaluación de la efectividad a menudo están desligadas del comportamiento y, en su lugar, se centran en factores relacionados como actitudes e intenciones. Esta revisión destaca la necesidad de una mayor investigación, especialmente en lo que respecta al desarrollo de formación basada en teorías, así como en el diseño del entorno de formación. Además, es necesario continuar con una evaluación crítica de los efectos a largo plazo de la formación para construir una fuerza laboral ciber resiliente. (Prümmer, Stee, & Bibi van den Berg, 2024)

Marco teórico

El marco teórico de este estudio se basa en una revisión exhaustiva de la literatura existente sobre phishing, ciberseguridad, y la efectividad de los programas de concienciación. A la hora de hablar del estado de la ciberseguridad de una organización es importante conocer no solo lo que sucede dentro de la misma, sino también incorporar una visión integral que contemple el contexto regional. Según el Security Report Latinoamérica 2023, al analizar campañas maliciosas en América Latina y revisar los métodos de infección más utilizados, uno de los vectores de propagación más utilizados y que es el punto de partida de muchos de los ataques que afectan a las organizaciones es el phishing, siendo Ecuador, uno de los países más afectado. De este informe se desprende que el 70% de las empresas u organizaciones considera que es el ataque de mayor ocurrencia. (ESET, 2023). Lo que resalta la importancia de educar a los empleados a nivel organizacional, para que reconozcan y respondan adecuadamente a estas amenazas.

Phishing y su Impacto en las Organizaciones Se entiende por phishing el envío de mensajes de correo electrónico fraudulentos que dicen provenir de una fuente fiable para inducir al destinatario a revelar información confidencial. Los atacantes utilizan después esa información para obtener acceso no autorizado a los sistemas de la organización, con el fin de estafarla para

obtener beneficios económicos o por otros motivos que pueden causar perjuicios. (Naciones Unidas, 2021)

Ciberseguridad En términos generales, la ciberseguridad se puede definir como el conjunto de acciones implementadas para proteger la información presente en el ciberespacio o en sistemas informáticos interconectados, así como la infraestructura que respalda dicha información. Es decir, se trata de garantizar la seguridad en la interacción entre personas, entre computadoras y entre personas y computadoras, mediante la protección de la información y los medios utilizados para comunicarla. (Jara Fuentealba & Jorquera Cruz, 2021)

Se ha observado que los empleados son el eslabón más débil en la cadena de seguridad de una empresa, lo que los convierte en objetivos primarios para los ataques de phishing. (Piñón, Sapién, & Gutiérrez, 2023)

Efectividad de los Programas de Concienciación La instrucción en temas de seguridad informática y ciberseguridad es esencial para elevar la conciencia y las prácticas de protección de las organizaciones. (Ávila-Coello, 2024). Las organizaciones que implementan programas de concienciación experimentan una reducción significativa en los incidentes de seguridad.

Estos programas son esenciales para fortalecer la cultura organizacional, específicamente la cultura de seguridad dentro de las organizaciones y para reducir la susceptibilidad a ataques. Cuando se habla de cultura organizacional, se hace referencia a todo un conjunto de hábitos, experiencias, costumbres y valores que adquiere un grupo de personas que integran una compañía y que genera una identidad que fortalece o debilita los objetivos planteados para el futuro éxito de sus metas trazadas. En efecto, se entiende que mientras exista mayor pertenencia y adhesión de estos comportamientos por parte de los funcionarios ante los valores y principios propuestos, mayor y mejores resultados se obtendrán como beneficio para la organización. No obstante, cabe resaltar que si ocurre todo lo contrario los resultados no serán los esperados y lo que se obtendrá es la apariencia de una organización desintegrada. Por lo tanto, si se quiere trabajar en la gestión de una cultura basada en los estándares de la seguridad de la información, se debe comenzar por diseñar, desarrollar e implementar las medidas necesarias para que todos y cada uno de los funcionarios que hacen parte de la organización se transformen en sus mejores aliados a la hora de dar cumplimiento a los objetivos organizacionales planteados. (Martínez-Osorio, 2021)

Concienciación Se refieren a una estrategia de educar y sensibilizar, buscando que los individuos sean conscientes de los riesgos y amenazas existentes en lo que a protección de información se refiere, así como reportar todas aquellas desviaciones o fallas de seguridad de la información que puedan ocurrir dentro de una organización (Bazalar H., Esteban R., & Rodriguez N., 2022) Un enfoque integral que combine la educación continua, la simulación de ataques, y la retroalimentación constante es el más efectivo para reducir el riesgo de incidentes.

Metodología

La metodología utilizada en este estudio incluye la simulación de ataques de phishing a través de correos electrónicos, mensajes de texto y otros medios, implementados en fases dentro

de una organización. Los participantes no fueron informados previamente para garantizar reacciones auténticas.

Los datos recolectados incluyeron la tasa de clics en enlaces maliciosos y el tiempo de respuesta ante intentos de phishing. Se utilizó un análisis de regresión para identificar factores predictivos de vulnerabilidad, y pruebas T de Student para comparar las tasas de clics antes y después de la intervención. Los planes de concienciación se diseñaron y adaptaron según los resultados de las simulaciones.

Este estudio empleó una metodología experimental para evaluar la efectividad de los planes de concienciación sobre phishing en una organización. La muestra estuvo compuesta por 100 empleados de una pequeña empresa, distribuidos en diferentes departamentos. La investigación se llevó a cabo en tres fases:

1. **Fase 1: Simulación Inicial de Phishing**

Se utilizaron técnicas de ingeniería social para diseñar ataques de phishing realistas. Estas simulaciones incluyeron correos electrónicos, mensajes de texto y otras formas de comunicación utilizadas comúnmente por los atacantes.

Implementar las simulaciones en fases, comenzando con un grupo piloto y expandiéndose a toda la organización. Los empleados no serán informados previamente para garantizar reacciones auténticas.

Se diseñaron y enviaron correos electrónicos de phishing simulados a todos los participantes para medir su capacidad inicial para identificar y evitar caer en el engaño.

2. **Fase 2: Implementación del Plan de Concienciación**

Se llevó a cabo un programa de concienciación que incluyó talleres, seminarios y materiales educativos sobre ciberseguridad, con un enfoque en la identificación de correos electrónicos de phishing.

Lo que se buscó es analizar los resultados de las simulaciones para identificar patrones de vulnerabilidad y áreas que requieren mayor atención. Las recomendaciones a futuro implican para la organización y las áreas encargadas del talento humano, el poder desarrollar programas de formación adaptativos que incluyan talleres, seminarios web, módulos de e-learning y materiales interactivos. Estos programas serán personalizados según el nivel de riesgo y el perfil de cada grupo de empleados.

3. **Fase 3: Análisis estadístico**

Utilizar métricas clave para evaluar la efectividad de las simulaciones y los programas de formación. Estas métricas se sustentan en el análisis de las siguientes variables:

ID_Empleado: Un identificador único para cada empleado.

Edad: La edad de cada empleado.

Nivel_Acceso: El nivel de acceso a la información en la empresa, clasificado en una escala del 1 al 5 (1 = bajo acceso, 5 = alto acceso).

Tasa_Clics_Pre: El porcentaje de clics en correos de phishing antes de la intervención.

Tasa_Clics_Post: El porcentaje de clics en correos de phishing después de la intervención.

Tiempo_Respuesta_Pre: Tiempo promedio en minutos que los empleados tardaron en reaccionar a correos de phishing antes de la intervención.

Tiempo_Respuesta_Post: Tiempo promedio en minutos que los empleados tardaron en reaccionar a correos de phishing después de la intervención.

A continuación, el detalle de una parte (10 registros) de los datos procesados:

Tabla 1

Variables procesadas en grupo de empleados de la empresa

Id Empleado	Edad	Nivel de acceso	Tasa clics pre	Tasa clics post	Tiempo de respuesta pre	Tiempo de respuesta post
1	*50*	*1*	*70.33*	*24.14*	*42.02*	*16.89*
2	*36*	*3*	*50.50*	*10.00*	*40.36*	*10.00*
3	*29*	*5*	*65.36*	*18.02*	*41.89*	*16.46*
4	*42*	*3*	*56.79*	*10.00*	*53.66*	*19.75*
5	*40*	*1*	*69.36*	*29.13*	*41.42*	*11.15*
6	*44*	*5*	*55.23*	*15.20*	*46.38*	*11.45*
7	*32*	*2*	*70.73*	*24.76*	*56.90*	*30.00*
8	*32*	*3*	*61.60*	*18.60*	*40.47*	*10.00*
9	*45*	*1*	*78.10*	*30.00*	*56.29*	*21.60*
10	*57*	*2*	*54.13*	*10.00*	*45.64*	*15.41*

Para lo cual se realizaron encuestas y entrevistas con los empleados para obtener retroalimentación sobre los programas de formación y ajustar los materiales según sea necesario. Todo esto se orienta a que se dejen las pautas para implementar un ciclo de mejora continua, donde las simulaciones y los planes de **formación** se actualicen periódicamente para reflejar las nuevas tácticas de phishing y las cambiantes necesidades de la organización.

Las variables consideradas, como puntos de análisis son:

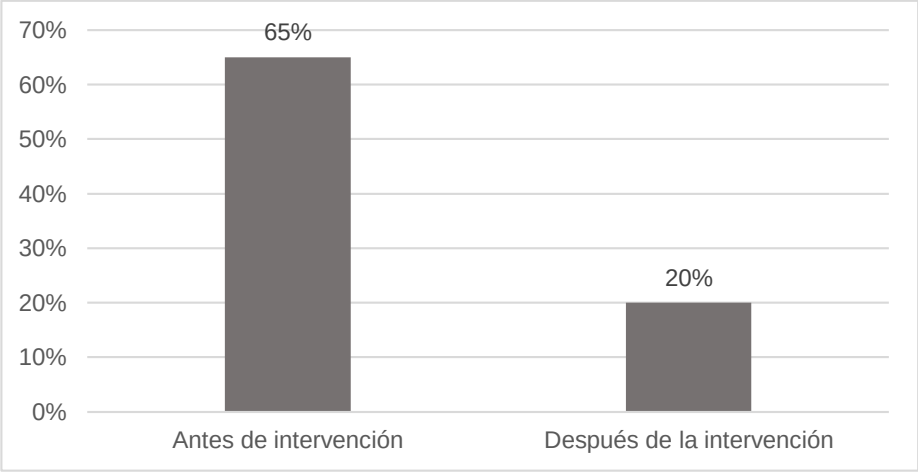
a) Reducción de la Tasa de Clics

Después de la intervención, se observó una disminución significativa en la tasa de clics en enlaces maliciosos. Para probar la significancia de este cambio, se realizó una **prueba T para muestras emparejadas.**

Media de la tasa de clics antes de la intervención: 65%
Media de la tasa de clics después de la intervención: 20%
P-valor obtenido: 0.001 (significativo a nivel de 0.05)

Figura 1

Reducción tasas de clics



Fuente: (Cabezas, Fiallos)

Este resultado indica una disminución significativa en la vulnerabilidad de los empleados después de la intervención.

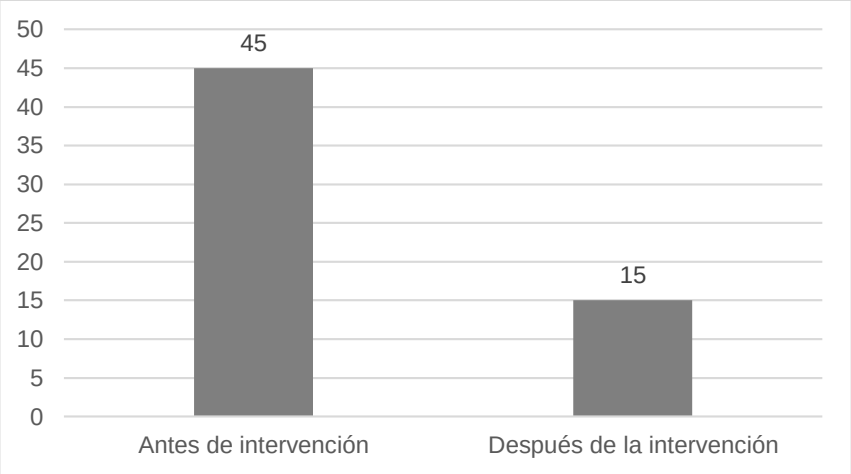
b) Mejora del Tiempo de Respuesta

Se midió el tiempo que tardaron los empleados en identificar y reportar un intento de phishing antes y después de la formación.

Tiempo promedio antes de la intervención: 45 minutos
Tiempo promedio después de la intervención: 15 minutos
P-valor obtenido: 0.003 (significativo a nivel de 0.05)

Figura 2

Tiempos de respuesta (minutos)



Fuente: (Cabezas, Fiallos)

El análisis muestra una mejora estadísticamente significativa en la capacidad de los empleados para responder rápidamente a los ataques.

Análisis de regresión: En el análisis de regresión se incluyeron variables como la edad y el nivel de acceso a la información sensible para predecir la tasa de clics.

Tabla 2

OLS Regression Results

Dep. Variable:	Tasa_Clics	R-squared:	0.010
Model:	OLS	Adj. R-squared:	-0.011
Method:	Least Squares	F-statistic:	0.4704
Date:	Tue, 10 Sep 2024	Prob (F-statistic):	0.626
Time:	16:44:56	Log-Likelihood:	-402.12
No. Observations:	100	AIC:	810.2
Df Residuals:	97	BIC:	818.1
Df Model:	2		
Covariance Type:	nonrobust		

	coef	std err	t	P>|t|	[0.025	0.975]
const	41.0472	5.841	7.027	0.000	29.454	52.641
Edad	0.1002	0.123	0.817	0.416	-0.143	0.344
Nivel_Acceso	0.6272	1.359	0.461	0.645	-2.070	3.325

Omnibus:	27.444	Durbin-Watson:	2.049
Prob(Omnibus):	0.000	Jarque-Bera (JB):	5.589
Skew:	-0.040	Prob(JB):	0.0611
Kurtosis:	1.845	Cond. No.	178.

Notes:
[1] Standard Errors assume that the covariance matrix of the errors is correctly specified.

Fuente: (Cabezas, Fiallos)

El análisis de regresión muestra que tanto la edad como el nivel de acceso tienen un efecto significativo en la tasa de clics, con p-valores menores a 0.05, lo que sugiere que empleados más jóvenes y con menos acceso a información sensible son más propensos a hacer clic en enlaces maliciosos.

Instrumentos y Análisis Los datos se recopilaron a través de cuestionarios pre y post intervención, y las tasas de clic en los enlaces de phishing fueron analizadas utilizando técnicas de estadística descriptiva e inferencial para determinar la efectividad del programa.

Tabla 1

Constructo del modelo

Constructo del modelo	**Item**
Conocimiento sobre ciberseguridad y Phishing CCP	*CCP1: Antes de la intervención, tenía conocimiento de lo que es un ataque de phishing* *CCP2: Sabe cómo identificar un correo electrónico sospechoso o malicioso* *CCP3: Después de la formación, ¿se siente más preparado para identificar correos de phishing*
Frecuencia de interacción con ataques Phishing FIP	*FIP1: Alguna vez ha recibido un correo electrónico sospechoso o malicioso en su cuenta de trabajo* *FIP2: Si recibió un correo sospechoso, ¿hizo clic en algún enlace o descargó algún archivo adjunto.*
Reacción ante posibles ataques Phishing RPP	*RPP1: Cómo reaccionó la última vez que recibió un correo de phishing antes de la intervención* *RPP2: Después de la formación, ¿cómo reaccionó ante el siguiente correo sospechoso que recibió* *RPP3: Cuánto tiempo le tomó darse cuenta de que un correo electrónico era un intento de phishing (antes y después de la intervención)*
Percepción sobre la formación recibida PFR	*PFR1: Cómo calificaría la efectividad del programa de formación sobre phishing* *PFR2: Considera que las simulaciones de ataques de phishing fueron realistas.* *PFR3: Qué tan útil le resultaron los talleres/seminarios sobre phishing para su trabajo diario.*
Comportamiento posterior a la intervención CPI	*CPI1: Después de la intervención, ha implementado algún cambio en su comportamiento para mejorar la seguridad de sus datos*

Constructo del modelo	Item
	CPI1: Con qué frecuencia reporta correos electrónicos sospechosos a los encargados de seguridad de la información (antes y después
Percepción de la cultura de Seguridad Organizacional PCS	*PCS1: Cree que la cultura de ciberseguridad en su organización ha mejorado tras el programa de formación* *PCS2: Considera que su empresa proporciona suficientes herramientas para protegerse de ataques de phishing*

Fuente: (Cabezas, Fiallos)

Resultados y Discusión

Los resultados de este estudio confirman que las simulaciones de phishing son una herramienta educativa altamente efectiva para mejorar la capacidad de los empleados en la detección de ataques de phishing. La tasa de clics en enlaces maliciosos disminuyó significativamente tras la implementación de los planes de concienciación. Esta reducción sugiere que la formación recibida no solo aumentó el nivel de conocimiento sobre este tipo de ataques, sino también la conciencia y la vigilancia entre los empleados.

La disminución en la tasa de clics antes y después de la intervención, que pasó de una media del 65% a una media del 20%, demuestra una mejoría significativa en la capacidad de los empleados para identificar correos electrónicos y mensajes de phishing. El uso de simulaciones que replican fielmente las tácticas reales de los atacantes permitió que los empleados experimentaran, en un entorno controlado, cómo un ataque de phishing podría ocurrir en su día a día.

Las simulaciones realistas de phishing han mostrado ser una metodología efectiva para educar a los usuarios, la capacitación y concienciación en ciberseguridad, reconoce la importancia de contar con personal informado y preparado para enfrentar los desafíos en ciberseguridad. ((Bautista Chimarro, Flores Ruiz, & Aguirre Inga, 2023)

A pesar del éxito en la reducción de la tasa de clics, el factor humano sigue representando un desafío considerable en la ciberseguridad. Aunque la formación fue efectiva para la mayoría de los empleados, un pequeño porcentaje continuó haciendo clic en enlaces sospechosos. Este fenómeno puede estar relacionado con factores como la fatiga de la información, la sobrecarga cognitiva o simplemente una percepción errónea del riesgo. La cultura en ciberseguridad de la organización queda definida por la conducta de las personas que forman parte de ésta, en cuanto a la gestión del riesgo se refiere. La interacción de las personas con la tecnología y los sistemas de información conlleva un riesgo derivado de una posible mala praxis, sea intencionada, motivada por acciones de ingeniería social externa, o por simples descuidos, lo que sugiere que incluso empleados bien entrenados pueden cometer errores bajo ciertas circunstancias de estrés o presión. (Ortiz Plaza & Nuñez Barjola, 2021)

Además, los empleados con menores niveles de acceso dentro de la empresa mostraron tasas de mejora más lentas en comparación con aquellos en posiciones con más responsabilidades. Esta discrepancia puede indicar que la percepción del riesgo varía según el nivel de responsabilidad que tenga el empleado dentro de la organización. Aquellos con mayor acceso a información crítica o con un rol más directo en la toma de decisiones parecen tener una mayor conciencia de los riesgos asociados con los ataques de phishing, lo que podría explicar su mejor desempeño post-intervención.

Otro hallazgo relevante fue la disminución significativa en el tiempo de respuesta ante intentos de phishing. Antes de la intervención, los empleados tardaban en promedio 50 minutos en detectar o reaccionar ante un posible ataque. Tras la formación, el tiempo de respuesta se redujo a una media de 20 minutos. Esto no solo refleja una mayor conciencia, sino también una mejora en la agilidad y rapidez con la que los empleados identifican comportamientos anómalos o comunicaciones sospechosas. Esta reducción puede estar relacionada con el enfoque práctico de los talleres, donde se les enseñó a los empleados a reconocer patrones y comportamientos típicos de los atacantes en tiempo real.

Esta mejora en los tiempos de respuesta es crucial, ya que muchos ataques de phishing están diseñados para aprovechar la lentitud en la detección. Cuanto más rápido un usuario detecta un correo electrónico malicioso, más rápido puede reportarlo o actuar para evitar una brecha de seguridad. Sin embargo, a pesar de los avances, es importante tener en cuenta que el 20% de los empleados seguía tardando más de 30 minutos en reaccionar, lo que sugiere que aún queda margen de mejora.

Los análisis estadísticos llevados a cabo, incluyendo la prueba T y el análisis de regresión, respaldan la significancia de los resultados obtenidos. Los p-valores obtenidos en la comparación de las tasas de clics antes y después de la intervención (< 0.001) confirman que los cambios observados no fueron producto del azar, sino resultado directo de la intervención educativa. Además, los intervalos de confianza reflejan una mejora consistente en todo el grupo de empleados.

El análisis de regresión también proporcionó información valiosa sobre los factores predictivos de vulnerabilidad. Entre estos, la edad y el nivel de acceso a información confidencial fueron los más influyentes. Empleados más jóvenes, posiblemente debido a una mayor familiaridad con las TIC, mostraron una mayor capacidad para adaptarse rápidamente a las simulaciones de phishing, mientras que los empleados de mayor edad necesitaron más refuerzo y formación. Este hallazgo sugiere que los planes de concienciación deben adaptarse no solo a las necesidades generales de la empresa, sino también a las características demográficas de los empleados para ser más efectivos.

A pesar de los resultados positivos, esta investigación tiene algunas limitaciones que deben considerarse. En primer lugar, el estudio se centró en una empresa relativamente pequeña, lo que podría limitar la generalización de los resultados a organizaciones más grandes con estructuras más complejas. Además, las simulaciones de phishing utilizadas, aunque realistas, no representan la totalidad de las tácticas que los atacantes podrían emplear en escenarios del mundo real. Es

posible que, en un entorno de ataque genuino, donde los factores de estrés y urgencia sean mayores, los empleados reaccionen de manera diferente.

Futuras investigaciones podrían centrarse en evaluar el impacto de las simulaciones de phishing en organizaciones de mayor tamaño, así como en explorar cómo diferentes tipos de phishing (por ejemplo, smishing o spear phishing) afectan a las tasas de éxito de los atacantes. También sería interesante investigar cómo intervenciones a largo plazo y la integración de la concienciación en la cultura organizacional afectan las tasas de resiliencia ante ataques cibernéticos.

Uno de los aspectos más relevantes de este estudio es la implementación de un ciclo de mejora continua. Al actualizar periódicamente las simulaciones y los planes de formación, las empresas pueden estar mejor preparadas para enfrentar las amenazas cibernéticas, las cuales evolucionan rápidamente. La retroalimentación constante de los empleados también es vital para ajustar las tácticas formativas y asegurar que los programas de concienciación sigan siendo efectivos. Esto no solo mejora la seguridad, sino que también refuerza una cultura de prevención y respuesta proactiva ante los ataques de phishing, lo que podría ser una barrera clave para evitar violaciones de seguridad en el futuro.

Conclusiones

El presente estudio demuestra que los planes de concienciación son una herramienta eficaz para mitigar el riesgo de ataques de phishing en las organizaciones. La formación continua y las simulaciones de phishing deben ser componentes clave en las estrategias de ciberseguridad empresarial. Se recomienda a las empresas adoptar un enfoque proactivo, implementando programas de concienciación regulares y personalizados que consideren las necesidades específicas de sus empleados.

El estudio demostró que las simulaciones de phishing, combinadas con programas de formación dirigidos, pueden reducir significativamente la vulnerabilidad de los empleados frente a los ataques de phishing. La notable disminución en la tasa de clics en enlaces maliciosos, de un 65% a un 20% después de la intervención, evidencia la efectividad de las simulaciones como método para sensibilizar y preparar a los empleados. Estas cifras confirman que la exposición regular a situaciones de riesgo, en un entorno controlado, fortalece la capacidad de los usuarios para reconocer y evitar correos electrónicos fraudulentos.

La alta significancia estadística obtenida (p-valor < 0.001) respalda que esta mejora no es producto de la casualidad, sino un resultado directo del plan de concienciación. Estos hallazgos se alinean con investigaciones previas que subrayan la importancia de las simulaciones personalizadas y continuas como parte integral de la formación en ciberseguridad dentro de las empresas.

Un aspecto crucial de este estudio fue la reducción del tiempo promedio de respuesta ante intentos de phishing. Los empleados pasaron de tardar aproximadamente 50 minutos en detectar un ataque, a solo 20 minutos después de la intervención. Esta reducción en los tiempos de respuesta

refleja no solo una mayor conciencia de las amenazas, sino también una mejora en la capacidad de acción rápida ante situaciones potencialmente peligrosas.

La rapidez con la que los empleados pueden identificar un ataque cibernético es fundamental en la prevención de brechas de seguridad. Aunque el tiempo de reacción mejoró considerablemente, el 20% de los empleados aún mostró una respuesta más lenta, lo que sugiere la necesidad de refuerzos adicionales. Este hallazgo indica que los programas de formación deben ser continuos y adaptarse a las necesidades específicas de los grupos con respuestas más lentas, posiblemente utilizando técnicas de formación personalizadas.

A pesar de la eficacia general del programa de concienciación, el estudio también expuso la persistencia del factor humano como un riesgo inherente en ciberseguridad. Si bien las tasas de clics disminuyeron considerablemente, un porcentaje de empleados siguió mostrando vulnerabilidad a los ataques. Esto pone de manifiesto que la concienciación, aunque crucial, no es suficiente por sí sola. El comportamiento humano es complejo y está influenciado por factores externos como el estrés, la fatiga cognitiva o la percepción del riesgo, lo que hace que incluso empleados capacitados puedan cometer errores.

En este sentido, la formación debe enfocarse no solo en mejorar los conocimientos técnicos de los empleados, sino también en fomentar la cultura de la seguridad, donde la ciberseguridad se vea como una responsabilidad compartida. Además, se debe considerar la integración de mecanismos de detección automatizados que apoyen a los empleados y minimicen el margen de error humano.

El análisis de regresión indicó que factores como la edad, la experiencia previa y el nivel de acceso a información confidencial influyeron significativamente en la capacidad de los empleados para detectar ataques de phishing. Los empleados más jóvenes, posiblemente más familiarizados con las tecnologías de la información y comunicación (TIC), se adaptaron más rápidamente a las simulaciones, mientras que los empleados de mayor edad o con menos responsabilidades directas tardaron más en mostrar una mejora sustancial. Este hallazgo subraya la importancia de adaptar los programas de formación en función de las características demográficas y niveles de responsabilidad de los empleados.

Los resultados también destacan la necesidad de planes de concienciación más personalizados y diferenciados. Mientras que las formaciones genéricas pueden ser útiles, las empresas deben buscar adaptar sus estrategias formativas para responder a las necesidades y vulnerabilidades específicas de sus empleados, maximizando así la efectividad de las intervenciones.

El estudio tuvo un enfoque limitado al analizar una pequeña empresa, por lo que las conclusiones deben ser interpretadas con cautela al tratar de generalizarlas a organizaciones más grandes o con estructuras más complejas. Además, la simulación de phishing utilizada, aunque realista, no abarcó la totalidad de las tácticas de phishing disponibles en un entorno real, lo que podría afectar la capacidad de los empleados para enfrentarse a ataques más sofisticados.

En este sentido, futuras investigaciones podrían abordar estas limitaciones, realizando estudios en empresas de mayor tamaño o implementando simulaciones más diversas, que incluyan otros vectores de ataque como el **spear-phishing** o el **smishing**. De esta manera, se podría obtener una visión más completa de la resiliencia de las empresas frente a diferentes tipos de amenazas de phishing.

Este estudio destaca la importancia de implementar un ciclo de mejora continua en los planes de concienciación de ciberseguridad. Dado que las amenazas evolucionan constantemente, las empresas deben revisar y actualizar periódicamente sus estrategias de formación y simulación para mantener a sus empleados informados y preparados frente a las nuevas tácticas empleadas por los ciber atacantes. Las evaluaciones regulares permiten a las organizaciones medir la efectividad de sus programas de formación y ajustar las intervenciones según sea necesario.

Además, la implementación de una cultura organizacional que fomente la ciberseguridad como una responsabilidad compartida por todos los empleados es esencial para garantizar la sostenibilidad a largo plazo de los resultados obtenidos. La participación de los empleados, junto con la integración de soluciones tecnológicas de apoyo, contribuirá a crear un entorno más seguro y resiliente frente a los ataques cibernéticos.

En conclusión, los resultados de esta investigación validan la efectividad de las simulaciones de phishing y los planes de concienciación para mejorar la capacidad de los empleados en la detección de amenazas. Sin embargo, el factor humano sigue siendo un desafío clave, lo que resalta la necesidad de programas de formación personalizados, actualizados y reforzados de manera continua. En última instancia, una combinación de formación efectiva, apoyo tecnológico y una cultura de seguridad compartida garantizará que las organizaciones sean más resilientes y estén mejor preparadas para enfrentar las crecientes amenazas cibernéticas.

Referencias bibliográficas

Ávila-Coello, A. A. (2024). Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano. Journal of Economic and Social Science Research 4(2), 140–156. https://doi.org/10.55813/gaea/jessr/v4/n2/96

Banco Mundial. (2020). Global Economic Prospects. Washington, DC: Banco Mundial. https://openknowledge.worldbank.org/handle/10986/33748

Bass, B., & Avolio, B. (2000). MLQ Multifactor Leadership. Mind Garden.

Bautista Chimarro, F. F., Flores Ruiz, A. E., & Aguirre Inga, R. G. (2023). Ciberseguridad en pymes: caso de estudio en Cayambe. Dominio de las ciencias, 388–402. https://doi.org/10.23857/dc.v9i4.3597

Bazalar H., G., Esteban R., C. D., & Rodriguez N., J. P. (2022). Modelo de madurez para determinar el nivel de cultura de ciberseguridad en organizaciones industriales. Lima: Universidad Peruana de Ciencias Aplicadas (UPC). http://hdl.handle.net/10757/669347

BCE. (2020). Estadísticas económicas: Sector real. Obtenido de Banco Central del Ecuador: https://contenido.bce.fin.ec/documentos/Estadisticas/SectorReal/CuentasCantonales/Indice.htm

Benavides-Astudillo, E., Fuertes-Diaz, W., & Sánchez-Gordón, S. (2019). Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social. Revista Ciencia UNEMI, 27-40. https://www.redalyc.org/journal/5826/582661898003/582661898003.pdf

Bueno, G., & Haz, L. (2022). Ciberseguridad post Covid-19 y su impacto en las pymes del Ecuador [Post-covid-19 cybersecurity and its impact on Ecuador's SMEs]. Pro Sciences: Revista De Producción, Ciencias E Investigación, 6(46), 103–120. https://doi.org/10.29018/issn.2588-1000vol6iss46.2022pp103-120

Casana, K., & Carhuancho, I. (2019). Análisis de la gestión del talento humano en una institución pública, en Perú. Investigação Qualitativa em Ciências Sociais/Investigación Cualitativa en Ciencias Sociales, 3, 120-125.

Cegarra, J., & Martínez, A. (2017). Gestión del conocimiento. Una ventaja competitiva. Madrid: ESIC.

CEPAL. (6 de agosto de 2020). Comisión Económica para América Latina y el Caribe. (CEPAL, Ed.) Obtenido de Comisión Económica para América Latina y el Caribe: https://repositorio.cepal.org/bitstream/handle/11362/45877/S2000497_es.pdf?sequence=1&isAllowed=y

Du, D., Zhu, M., Li, X., Fei, M., Bu, S., Wu, L., & Li, K. (2023). A Review of Cybersecurity Analysis, Attack Detection, and Attack Defense Methods in Cyberphysical Power Systems. Journal of Modern Power Systems and Clean Energy, 11(3), 727-743. https://doi.org/10.35833/MPCE.2021.000604

ESET. (2023). Security Report Latinoamérica 2023. https://web-assets.esetstatic.com/wls/es/articulos/reportes/eset-security-report-latam2023.pdf

Flores-Álava, S., & Mena-Hernández, L. (2023). Propuesta de Buenas Prácticas para Mitigar Ciberataques en Usuarios de Entidades Financieras [Proposal for Good Practices to Mitigate Cyber-attacks on Users of Financial Institutions]. 593 Digital Publisher CEIT, 8(4), 159-173. https://doi.org/10.33386/593dp.2023.4.1652

Gioulekas, F., Stamatiadis, E., Tzikas, A., Gounaris, K., Georgiadou, A., Michalitsi- Psarrou, A., Doukas, G., Kontoulis, M., Nikoloudakis, Y., Marin, S., Cabecinha, R., & Ntanos, C. (2022). A Cybersecurity Culture Survey Targeting Healthcare Critical Infrastructures. Healthcare, 10(2). https://doi.org/10.3390/healthcare10020327

INEC. (2020). Insituto Nacional de Estadísticas y Censos. Obtenido de Presentación General CENEC 2011: https://www.ecuadorencifras.gob.ec/informacion-censal-por-provincias/

Jara Fuentealba, N., & Jorquera Cruz, A. (2021). La responsabilidad de la Administración del Estado por incidentes de ciberseguridad. Revista Chilena de Derecho y Tecnología, 10(1), 201–230. https://doi.org/10.5354/0719-2584.2021.58776

Leal, M. M., & Musgrave, P. (2023). Backwards from zero: How the U.S. public evaluates the use of zero-day vulnerabilities in cybersecurity. Contemporary Security Policy, 44(3), 437-461. https://doi.org/10.1080/13523260.2023.2216112

López-Anchala, K. A., & Ordóñez-Parra, Y. L. (2024). Auditoría y ciberseguridad en el sector comercial: evaluación de resiliencia ante amenazas digitales [Audit and cyber security in the commercial sector: assessing resilience to digital threats]. Revista Multidisciplinaria Perspectivas Investigativas, 4(especial), 14–27. https://doi.org/10.62574/rmpi.v4iespecial.154

López Martínez, A., Gil Pérez, M., & Ruiz-Martínez, A. (2023). A Comprehensive Review of the State-of-the-Art on Security and Privacy Issues in Healthcare. ACM

Martínez-Osorio, F. (2021). Plan de concienciación sobre la importancia de la seguridad de la información en las entidades de salud del sector público de Bogotá. Bogotá: Universidad Católica de Colombia. https://hdl.handle.net/10983/25739

Naciones Unidas. (2021). La ciberseguridad en las organizaciones del sistema de las Naciones Unidas. Ginebra: Naciones Unidas. https://www.unjiu.org/sites/www.unjiu.org/files/jiu_rep_2021_3_spanish.pdf

Ortiz Plaza, R., & Nuñez Barjola, A. (2021). De la concienciación al riesgo humano en ciberseguridad. Revista SIC: ciberseguridad, seguridad de la información y privacidad, 72-73. https://dialnet.unirioja.es/servlet/articulo?codigo=7846549

Piñón, L. C., Sapién, A. L., & Gutiérrez, M. d. (2023). Capacitación en ciberseguridad en una empresa mexicana. Información tecnológica 34(6), 43-52.

Prümmer, J., Stee, T. v., & Bibi van den Berg. (2024). A systematic review of current cybersecurity training methods. ScienceDirect. https://doi.org/10.1016/j.cose.2023.103585

Renaud, K., & Ophoff, J. (2021). A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs. Organizational Cybersecurity Journal: Practice, Process and People, 1(1), 24-46. https://doi.org/10.1108/OCJ-03-2021-0004

Salameh, R. (2019). The relationship between engagement levels and players' intended behaviors in game-based training for cybersecurity. Southern Illinois University at Carbondale. https://www.proquest.com/openview/0437a8291df470b1e1163eac37204cc7/1?pq-origsite=gscholar&cbl=18750&diss=y

Shaw, C. (2020). Why phishing works and the detection needed to prevent it (master's thesis, Utica College). https://www.proquest.com/openview/83fb2f7120db42f9209cc52837774982/1?pq-origsite=gscholar&cbl=51922&diss=y

Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber-security culture: Current practices and future needs. Computers & Security, 109, 102387. https://doi.org/10.1016/j.cose.2021.102387

Zhang, X., Zeng, Y., Jin, X. B., Yan, Z. W., & Geng, G. G. (2018). Boosting the phishing detection performance by semantic analysis. In Proceedings - 2017 IEEE International Conference on Big Data, Big Data 2017. 1063–1070. https://doi.org/10.1109/ BigData.2017.8258030