PROPUESTA DE CONCIENCIACIÓN ESTRATÉGICA ANTE RIESGOS DE SEGURIDAD INFORMÁTICA EN LA EFICIENCIA OPERATIVA ADMINISTRATIVA AUTOMATIZADA

Strategic Awareness Proposal Regarding Information Security Risks in Automated Administrative Operational Efficiency

Stiven Yiovanny Moreira Villafuerte [1] · **Gabriela Stephania Delgado Saavedra** [2]

[1,2]Instituto Superior Universitario Bolivariano de Tecnología (ITB)
[1]symoreira@itb.edu.ec , [2]gsdelgado2@itb.edu.ec

RESUMEN

La ingeniería social representa una de las principales amenazas a la seguridad de la información en el entorno empresarial, debido a que explota las vulnerabilidades humanas en lugar de fallas técnicas. Entre sus manifestaciones más comunes se encuentra el phishing, que utiliza el correo electrónico como medio principal para engañar a usuarios y obtener información confidencial. Diversos estudios evidencian que los ataques de ingeniería social generan impactos significativos en las organizaciones, tanto a nivel económico como operativo. A pesar de los avances tecnológicos en detección temprana, inteligencia artificial y automatización, el factor humano continúa siendo el eslabón más vulnerable dentro de la cadena de seguridad. En el contexto regional, y particularmente en Ecuador, el crecimiento sostenido de los ciberataques refleja la necesidad urgente de fortalecer las estrategias de prevención. En este sentido, la capacitación continua del personal, junto con la implementación de políticas de seguridad y marcos tecnológicos adecuados, se posiciona como un elemento clave para mitigar los riesgos asociados a los ataques de ingeniería social y fortalecer la resiliencia de las empresas frente a estas amenazas. Para el desarrollo del estudio se aplicó una encuesta dirigida a personas laboralmente activas con el objetivo de identificar el nivel de conocimiento y concienciación sobre ataques de phishing y seguridad del correo electrónico. Los resultados evidenciaron debilidades en capacitación y protocolos institucionales, así como un alto interés en recibir formación especializada, permitiendo establecer una propuesta de capacitación orientada al fortalecimiento de la cultura de ciberseguridad organizacional.

Palabras clave:

Correos electrónicos, vulnerabilidad, seguridad de la información, ingeniería social

FECHA DE RECEPCIÓN:
17 de junio de 2026

FECHA DE ACEPTACIÓN:
21 de julio de 2026

FECHA DE PUBLICACIÓN:
03 de agosto de 2026

ABSTRACT

Social engineering represents one of the main threats to information security in the business environment because it exploits human vulnerabilities rather than technical flaws. Among its most common manifestations is phishing, which uses email as the primary means to deceive users and obtain confidential information. Several studies show that social engineering attacks generate significant impacts on organizations, both economically and operationally. Despite technological advances in early detection, artificial intelligence, and automation, the human factor remains the most vulnerable link in the security chain. In the regional context, and particularly in Ecuador, the sustained growth of cyberattacks reflects the urgent need to strengthen prevention strategies. In this regard, continuous staff training, along with the implementation of appropriate security policies and technological frameworks, is a key element for mitigating the risks associated with social engineering attacks and strengthening companies' resilience to these threats. For this study, a survey was administered to employed individuals to identify their level of knowledge and awareness regarding phishing attacks and email security. The results revealed weaknesses in training and institutional protocols, as well as a high level of interest in receiving specialized training, leading to the development of a training proposal aimed at strengthening the organization's cybersecurity culture.

Keywords:

emails, vulnerability, information security, social engineering

INTRODUCCIÓN

La ingeniería social se fundamenta en la premisa de que el usuario es el eslabón más débil de la cadena de seguridad, ya que, a diferencia de los sistemas de software, las personas son susceptibles a la manipulación psicológica. El phishing representa la ejecución más clara de este principio, al utilizar el engaño y la suplantación de identidad para que la víctima, bajo una falsa apariencia de confianza, entregue voluntariamente sus credenciales. De este modo, el atacante no necesita vulnerar la seguridad técnica del sistema, sino simplemente aprovechar la disposición del usuario a colaborar ante una solicitud que parece legítima pero que, en realidad, es la puerta de entrada para un daño mayor.

El correo se ha consolidado como herramienta clave en la comunicación empresarial. En la actualidad hay tecnologías más sofisticadas, sin embargo, el email resulta una tecnología esencial para el funcionamiento de las empresas, especialmente en las numerosas pymes donde es el único medio disponible de comunicación electrónica. Su facilidad y versatilidad explican su uso tan extendido, pero a la vez lo convierte en una herramienta que precisa de una política de uso para potenciar sus beneficios. Dicha política comprendería regular sus usos profesionales, el cumplimiento de la legislación y su empleo como herramienta de gestión del conocimiento.

Los ataques de ingeniería social generan un impacto significativo en las empresas, especialmente en términos económicos y operativos. Según el informe Cost of a Data Breach 2025 de IBM (2025), el costo promedio mundial de una vulneración de datos en 2025 se ubicó en 4,44 millones de dólares, lo que representa una disminución del 9 % en comparación con el año anterior de 4,88 millones de dólares. Esta reducción se atribuye, en gran medida, a la rápida identificación de incidentes por parte de los equipos de seguridad de las organizaciones, apoyados en el uso de inteligencia artificial y procesos de automatización. Asimismo, el costo medio de un incidente relacionado con extorsión se estima en aproximadamente 5,08 millones de dólares, lo que evidencia la gravedad de este tipo de ataques y su impacto directo en la estabilidad financiera de las empresas.

Latinoamérica se ha convertido en una de las regiones con mayor crecimiento de ciberataques, con un aumento anual cercano al 25–30%, impulsado por el uso de ransomware, robo de credenciales y amenazas potenciadas con inteligencia artificial. En este contexto, Ecuador destaca como uno de los países más vulnerables, con más de 12 millones de ataques registrados en 2023 y un bajo nivel de preparación: solo aprox. 6% de las empresas consideran poder resistir un ataque. Entre las principales causas están la digitalización acelerada sin inversión en seguridad, la escasez de talento especializado y la baja cultura de ciberseguridad. Entre las soluciones más recomendadas se encuentran fortalecer políticas y marcos legales, implementar tecnologías como MFA, cifrado y monitoreo continuo, mejorar la capacitación del personal y promover la colaboración público-privada para elevar la resiliencia regional.

En este contexto, el presente estudio tiene como finalidad analizar el nivel de conocimiento y concienciación sobre ataques de phishing y seguridad del correo electrónico en personas laboralmente activas, con el propósito de identificar debilidades formativas y establecer una propuesta de capacitación orientada al fortalecimiento de la cultura de ciberseguridad organizacional

Volumen 01 No. 1. Agosto 2026, pp. 71-80

DESARROLLO

El phishing es una herramienta que en los últimos años ha incrementado su uso en los cuales ha provocado grandes pérdidas en instituciones financieras y en diferentes sectores en los cuales se utiliza el acceso a internet para almacenar sus datos (Mohd & Mohammad, 2025). Por los cual las empresas deben aportar a sus empleados la capacitación adecuada al momento de manejar toda la información de sus bases de datos y tener todas las llaves de seguridad adecuadas y guardadas en sitios seguros tanto. El estudio busca contribuir al desarrollo y mejora de estrategias de mitigación para ataques de phishing. Al investigar investigaciones recientes en diferentes enfoques, como la conciencia del usuario, la basada en listas, la búsqueda y el aprendizaje automático, la investigación busca identificar técnicas efectivas que puedan prevenir o minimizar el impacto de los ataques de phishing. Una parte significativa de la investigación en este campo se centra en la detección efectiva de ataques de phishing. Basándose en el cuerpo de trabajo existente, este artículo presenta un enfoque novedoso en forma de un marco de detección y mitigación de phishing. El marco propuesto ofrece una solución para mitigar los riesgos asociados a los incidentes de phishing.

La ingeniería social es el arte de influir en las personas con el fin de obtener información confidencial, como contraseñas, direcciones, datos bancarios, etc., aprovechando las vulnerabilidades humanas (Chetioui, Bah, Alami, & Bahnasse, 2022). En lugar de utilizar vulnerabilidades tecnológicas, estos ataques se aprovechan de las debilidades humanas, como los sentimientos, la confianza y los hábitos, para obtener información o datos confidenciales de las personas. Aunque es menos avanzada que otras estrategias de ciberataque, la ingeniería social puede causar graves daños a la víctima . Muchos delincuentes utilizan tácticas de ingeniería social porque suele ser más fácil explotar en la inclinación natural a confiar que descubrir que hay formas de piratear el software. Por ejemplo, es mucho más fácil engañar a alguien para que te dé su contraseña que intentar piratearla. Las estafas de ingeniería social se centran en cómo piensan, reaccionan y se comportan las personas. Una vez que el atacante sabe qué es lo que desencadena las acciones de un usuario, puede manipularlo fácilmente. La mayoría de las estafas de ingeniería social se basan en la comunicación directa entre el atacante y la víctima. En lugar de utilizar métodos de fuerza bruta para romper los datos, el atacante intentará convencer al usuario de que se comprometa.

La susceptibilidad de los usuarios ante los peligros de la ingeniería social ha sido objeto de estudio para varios autores. Por ejemplo, (Bakhshi, M., & Furnell, 2008) realiza un experimento social utilizando técnicas de escenarios realistas a empleados de una empresa mediante el canal del correo electrónico, donde se les pide una instalación de actualización de software por medio de un enlace atado al mensaje. Los resultados de los autores revelaron un nivel significativo de vulnerabilidad a los ataques de ingeniería social, donde alrededor del 23% de la población dieron clic al enlace. Esto indicaría que estas personas llegaron a acceder a una solicitud que ponía el riesgo del sistema con el que trabajaba la organización y es un problema evidente donde se infiere a las posibilidades de haberlo manejado en una situación real. Existen demasiados métodos de ingeniería social, sin embargo, el punto de atención no va directamente al perpetrador, más bien a las personas vulnerables que forman parte de la organización víctima del ataque. Por lo tanto, una recomendación factible que mencionan los

autores es la persuasión y tipo de capacitación de los empleados al proporcionar información sensible, concienciar y formar adecuadamente a los trabajadores para preservar la seguridad.

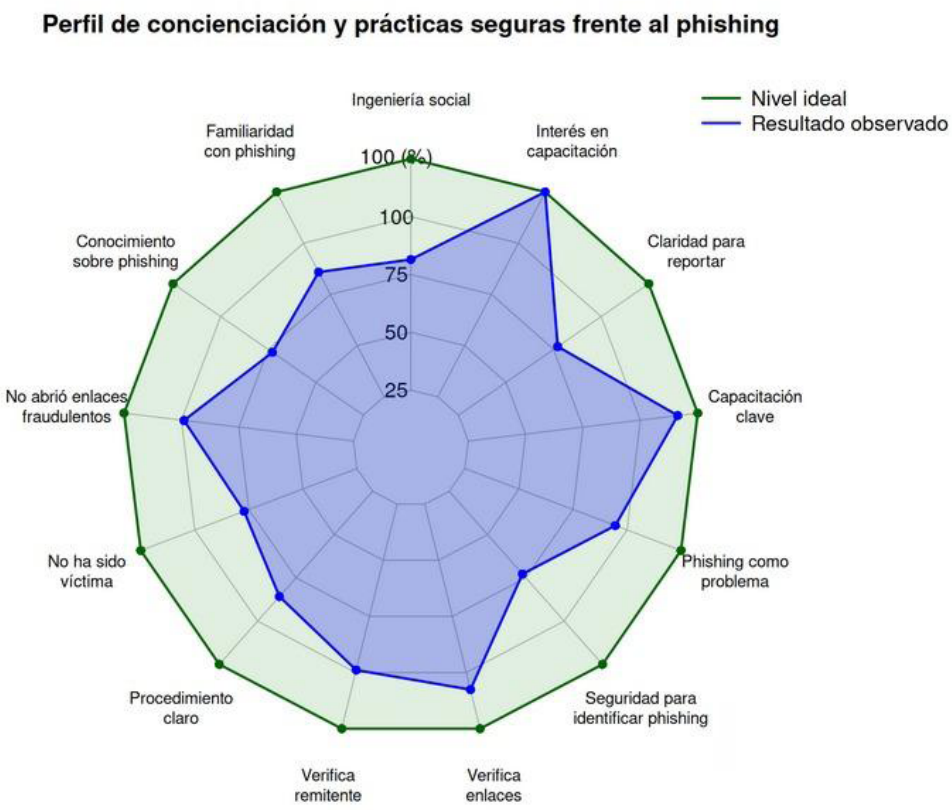
Según Steinmetz, Pimentel, & Goe, 2021 en su estudio cualitativo sobre los engaños de la materia de seguridad de la información realizado todo el conocimiento se ha ampliado a una escala mundial lo que hace que podamos detectar a tiempo algún ataque cibernético aunque todavía hay hacker que lo logran esto ya no es tan común como en otros tiempos. Lo que nos hace poder confiar un poco más en la tecnología y el avance que ha tenido con los años nos ha hecho poder detectar también creaciones falsas ya que hay estudios que nos enseñan a examinar y analizar los ataques antes de ser realizados. Por esto siempre debemos de estar atentos a cualquier ataque a la seguridad de nuestra información que tenemos guardado o registrada en nuestro operador.

Marco, Vallazza, Falcomatà, Aruväli, & Rauch, 2025 desarrollan e implementan un taller educativo eficaz que mejore las competencias en materia de ciberseguridad de las personas que participan en cualquier nivel de la gestión y el funcionamiento de los sistemas de producción ciberfísicos. Más allá del potencial que ofrece la adopción de los CPS en el contexto de la fabricación, cabe destacar una serie de vulnerabilidades. Las prácticas de codificación inseguras pueden introducir problemas graves, como desbordamientos de búfer y ataques de inyección, mientras que la dependencia de componentes de terceros añade riesgos adicionales. Una mitigación eficaz requiere actualizaciones periódicas, pruebas exhaustivas y el cumplimiento de normas de codificación seguras para garantizar la solidez y la seguridad del software CPPS. En consecuencia, las vulnerabilidades del hardware suponen amenazas importantes debido a su impacto directo en los procesos y operaciones físicos. El acceso físico inseguro es una preocupación fundamental, ya que personas no autorizadas pueden dañar dispositivos críticos o alterar su comportamiento de forma incontrolada. Las debilidades de los sistemas integrados y los controladores lógicos programables (PLC) pueden ser explotadas, lo que da lugar a interrupciones o a un control no autorizado.

Para comprender la percepción y el nivel de conocimiento sobre la ingeniería social, el phishing y los ataques de ciberseguridad en el ámbito laboral, se realizó una encuesta mediante Google Forms dirigida a personas que actualmente se encuentran trabajando. El objetivo principal fue medir el grado de conocimiento, las experiencias previas y las prácticas de seguridad digital de los participantes frente a posibles amenazas cibernéticas. En total, se encuestó a 23 personas, obteniéndose resultados relevantes sobre el nivel de preparación y concientización en temas de ciberseguridad.

Los resultados muestran que el correo electrónico constituye una herramienta de uso frecuente dentro del entorno laboral, ya que el 65.2% de los encuestados afirmó utilizarlo muy frecuentemente en sus actividades diarias. Asimismo, el 56.5% manifestó conocer el término “ingeniería social”, lo que evidencia que más de la mitad de los participantes posee cierta familiaridad con conceptos relacionados con la manipulación digital y los riesgos informáticos. En relación con el phishing, los resultados reflejan distintos niveles de familiaridad entre los encuestados. El 34.8% indicó estar bastante familiarizado con este tipo de ataque, mientras que el 26.1% señaló encontrarse algo familiarizado y el 21.7% poco familiarizado. De igual manera, el 47.8% afirmó poseer conocimientos altos o muy altos sobre ataques de phishing, mientras que el 34.7% reconoció tener conocimientos bajos o muy bajos.

Volumen 01 No. 1. Agosto 2026, pp. 71-80



Respecto a la exposición a amenazas digitales, el 87% de los encuestados indicó haber recibido alguna vez correos electrónicos sospechosos solicitando información personal, contraseñas o enlaces desconocidos. Aunque el 73.9% señaló no haber abierto enlaces que resultaron fraudulentos, un 26.1% admitió haberlo hecho, lo que evidencia la persistencia del riesgo asociado al phishing en el entorno laboral. En cuanto a las experiencias relacionadas con ciberataques, el 52.2% manifestó no haber sido víctima de algún ataque cibernético, mientras que el 47.8% indicó sí haber experimentado este tipo de incidentes.

Sobre las prácticas de seguridad digital, el 73.9% de los participantes afirmó verificar frecuentemente o muy frecuentemente el remitente de un correo electrónico antes de descargar archivos o abrir enlaces. De igual manera, el 82.6% indicó revisar los enlaces antes de acceder a ellos. Sin embargo, pese a estas prácticas preventivas, el 39.1% manifestó sentirse poco seguro al momento de identificar correos fraudulentos o intentos de phishing, mientras que solo el 21.7% afirmó sentirse bastante seguro. Además, el 39.1% considera que los correos de phishing son difíciles de identificar, lo que evidencia la complejidad de este tipo de amenazas.

Los encuestados también reconocen el impacto potencial de estos ataques sobre la seguridad de la información. En este sentido, el 69.6% se mostró totalmente de acuerdo con que los correos de phishing representan un problema importante para la seguridad informática dentro de las organizaciones.

En relación con la capacitación en ciberseguridad, el 78.3% indicó no haber recibido charlas o capacitaciones sobre este tema en su lugar de trabajo. Entre quienes sí recibieron capacitación, algunos calificaron su calidad como alta, mientras que otros la consideraron baja. A pesar de las limitaciones en capacitación, existe una percepción clara sobre su importancia. El 91.3% de los encuestados estuvo de acuerdo o totalmente de acuerdo en que la formación del personal es fundamental para prevenir ciberataques y fortalecer la seguridad de la información dentro de las empresas.

Finalmente, los resultados evidencian debilidades en los protocolos institucionales de reporte frente a incidentes de phishing. El 47.8% desconoce si en su lugar de trabajo existen protocolos para reportar ataques de phishing, el 34.8% indicó que no existen y únicamente el 17.4% afirmó que sí cuentan con ellos. Además, el 47.8% manifestó no tener claro a quién reportar un correo sospechoso, mientras que el 43.5% señaló tenerlo algo claro. Estos resultados demuestran la necesidad de implementar mecanismos de comunicación y respuesta más efectivos dentro de las organizaciones. Como resultado final, el 100% de los encuestados expresó interés en recibir capacitaciones o talleres sobre ciberseguridad y uso seguro del correo electrónico, evidenciando una alta disposición para fortalecer sus conocimientos en esta área.

Propuesta de capacitación en concienciación sobre phishing

Tabla 1
Propuesta de Capacitación en Concienciación sobre Phishing y Seguridad del Correo Electrónico

Componente Estratégico	Descripción	Metodología Aplicada	Valor Diferenciador
Diagnóstico Inicial de Vulnerabilidades Humanas	Evaluación del nivel de conocimiento y comportamiento de los colaboradores frente a correos sospechosos y ataques de ingeniería social.	Encuestas diagnósticas y escenarios simulados.	Permite identificar áreas críticas y perfiles de mayor vulnerabilidad.
Talleres de Identificación de Phishing	Capacitación práctica sobre detección de enlaces maliciosos, remitentes falsos, archivos sospechosos y suplantación de identidad.	Talleres interactivos y análisis de casos reales.	Desarrollo de pensamiento crítico frente a amenazas digitales.
Simulación Controlada de Ataques	Ejecución de campañas simuladas de phishing enviadas de manera inesperada a los colaboradores para evaluar sus reacciones.	Simulaciones reales de ataques controlados.	Permite medir el comportamiento real y no solamente el conocimiento teórico.

Componente Estratégico	Descripción	Metodología Aplicada	Valor Diferenciador
Metodología "Sombrero Gris" de Concienciación	Aplicación de ejercicios internos donde determinados participantes actúan como atacantes simulados para identificar vulnerabilidades humanas dentro de la organización.	Aprendizaje basado en roles y simulación ofensiva controlada.	Introduce un enfoque inmersivo y experiencial poco utilizado en capacitaciones tradicionales.
Laboratorios de Análisis de Correos Fraudulentos	Evaluación práctica de correos reales y falsos para identificar patrones de ingeniería social.	Laboratorios colaborativos y análisis guiado.	Fortalece habilidades de análisis y toma de decisiones rápidas.
Simulación de Incidentes Empresariales	Recreación de escenarios organizacionales donde un ataque de phishing compromete información sensible.	Aprendizaje basado en problemas (ABP).	Permite comprender el impacto operativo y económico de los ataques.
Protocolos de Respuesta y Reporte	Capacitación sobre procedimientos institucionales para reportar incidentes y actuar frente a amenazas digitales.	Charlas prácticas y ejercicios de respuesta inmediata.	Reduce tiempos de reacción ante incidentes reales.
Cultura Organizacional de Ciberseguridad	Fortalecimiento de hábitos seguros en el manejo del correo electrónico y protección de la información.	Estrategias de concienciación continua y microcapacitaciones.	Genera sostenibilidad preventiva dentro de la organización.
Gamificación en Ciberseguridad	Desarrollo de retos y dinámicas competitivas relacionadas con detección de ataques y buenas prácticas digitales.	Retos interactivos y dinámicas grupales.	Incrementa participación y retención del aprendizaje.
Evaluación y Retroalimentación Continua	Medición periódica del progreso de los colaboradores y retroalimentación sobre errores detectados.	Evaluaciones prácticas y seguimiento continuo.	Permite mejorar progresivamente el nivel de preparación organizacional.

Volumen 01 No. 1. Agosto 2026, pp. 71-80

CONCLUSIONES

- La ingeniería social constituye una amenaza crítica para las empresas, ya que no depende de vulnerar sistemas tecnológicos complejos, sino de manipular el comportamiento humano. Esto convierte al personal en un punto clave de riesgo, independientemente del nivel de sofisticación de las herramientas de seguridad implementadas.
- Si bien el uso de tecnologías como la inteligencia artificial, la automatización y los sistemas de detección temprana ha contribuido a reducir el impacto de algunos ataques, estos mecanismos no son suficientes por sí solos. La evidencia demuestra que la falta de concienciación y preparación de los usuarios sigue siendo una de las principales causas de éxito de los ataques de ingeniería social en el entorno empresarial.
- En consecuencia, la capacitación continua del personal debe considerarse una estrategia fundamental dentro de la gestión de la seguridad de la información. Programas de formación, simulaciones de ataques, políticas claras de uso del correo electrónico y una cultura organizacional orientada a la ciberseguridad permiten reducir significativamente la vulnerabilidad humana, fortaleciendo la protección de los activos de información y la continuidad operativa de las empresas.
- Los resultados obtenidos evidencian que, aunque existe cierto nivel de conocimiento sobre phishing, persisten debilidades importantes relacionadas con la identificación de correos fraudulentos, protocolos de reporte y capacitación institucional. La alta disposición de los participantes para recibir formación especializada demuestra la necesidad de implementar programas permanentes de concienciación en ciberseguridad dentro de las organizaciones

Volumen 01 No. 1. Agosto 2026, pp. 71-80

REFERENCIAS

Bakhshi, T., M., P., & Furnell, S. (2008). A Practical Assessment of Social Engineering Vulnerabilities. Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance, 12-23. Obtenido de https://www.researchgate.net/publication/265491384_A_Practical_Assessment_of_Social_Engineering_Vulnerablities

Chetioui, K., Bah, B., Alami, A. O., & Bahnasse, A. (2022). Overview of Social Engineering Attacks on Social Networks. Procedia Computer Science. doi:10.1016/j.procs.2021.12.302.

Marco, M. D., Vallazza, R., Falcomatà, I., Aruväli, T., & Rauch, E. (2025). Enhancing IT/OT Cybersecurity Knowledge Transfer Through Demonstrative Workshops in Cyber-Physical Production Systems. Procedia Computer Science. doi:10.1016/j.procs.2025.01.290.

Mohd, S., & Mohammad, S. U. (2025). Managing Security Issues in Phishing using Machine Learning Techniques. Procedia Computer Science. doi:10.1016/j.procs.2025.04.007.

Steinmetz, K., Pimentel, A., & Goe, W. R. (2021). Performing Social Engineering: A Qualitative Study of Information Security Deceptions. Computers in Human Behavior. doi:10.1016/j.chb.2021.106930.

Volumen 01 No. 1. Agosto 2026, pp. 71-80