

Análisis de las Principales Estrategias Utilizadas para la Prevención y Mitigación de Ataques de Phishing e Ingeniería Social Evaluando su Impacto en la Ciberseguridad

Leidy Johana Salazar Vega

Asesora

Yenny Stella Núñez Álvarez

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en seguridad informática

2026

Dedicatoria

A Dios, por darme la fortaleza y la sabiduría necesarias para culminar este proceso académico.

A mi hijo Samuel David, fuente de inspiración y motivo de cada uno de mis esfuerzos, por recordarme cada día que todo sacrificio tiene un propósito.

A mis padres, por su amor incondicional, sus enseñanzas y por ser el ejemplo de constancia y dedicación que me impulsa a seguir adelante.

Y a todas las personas que hicieron parte de este camino, brindándome su apoyo, compañía y palabras de aliento, les expreso mi más sincero agradecimiento, pues este logro también les pertenece.

Agradecimientos

A Dios, por darme la salud, la fortaleza y la sabiduría necesarias para alcanzar esta meta.

A mi hijo Samuel David y a mis padres, por su paciencia, apoyo incondicional y constante motivación durante todo este proceso.

A mi asesora, la ingeniera Yenny Stella Núñez Álvarez, por su orientación, conocimientos y compromiso que fueron fundamentales para el desarrollo de este trabajo.

A la Universidad Nacional Abierta y a Distancia – UNAD, por brindarme las herramientas académicas y el espacio para crecer profesional y personalmente.

Finalmente, a todas las personas que, de una u otra manera, contribuyeron con su apoyo, compañía o palabra de aliento, mi más sincero agradecimiento.

Resumen

Este trabajo de grado analiza de manera crítica las principales estrategias utilizadas para prevenir y mitigar los ataques de phishing e ingeniería social, con el propósito de evaluar su impacto real en la ciberseguridad organizacional y en la protección de los sistemas digitales. A partir de una metodología cualitativa y un riguroso análisis documental, se identificaron tácticas clave como la autenticación multifactor (MFA), los programas de concientización y formación continua, el uso de inteligencia artificial para la detección temprana, y la implementación de simulacros de ataques como herramienta educativa. El estudio demuestra que las estrategias más efectivas son aquellas que combinan componentes técnicos con enfoques humanos y organizacionales, permitiendo así reducir las vulnerabilidades asociadas al comportamiento del usuario. Asimismo, se evidenció que la sostenibilidad y efectividad de estas medidas dependen en gran parte del contexto institucional y del nivel de madurez en ciberseguridad. Los hallazgos destacan la necesidad de fortalecer la cultura de seguridad digital, especialmente en entornos latinoamericanos como Colombia, donde las brechas tecnológicas y educativas incrementan la exposición a estas amenazas. Las recomendaciones propuestas buscan orientar políticas públicas y privadas hacia una gestión integral del riesgo, reforzando la resiliencia frente a técnicas cada vez más sofisticadas de manipulación y fraude digital.

Palabras clave: Ciberseguridad, Phishing, Ingeniería Social, Concientización en Seguridad, Gestión de Incidentes.

Abstract

This thesis critically analyzes the main strategies used to prevent and mitigate phishing and social engineering attacks, with the aim of assessing their actual impact on organizational cybersecurity and the protection of digital systems. Based on a qualitative methodology and a rigorous documentary analysis, key tactics were identified, such as multi-factor authentication (MFA), awareness and continuous training programs, the use of artificial intelligence for early detection, and the implementation of attack simulations as an educational tool. The study shows that the most effective strategies are those that combine technical components with human and organizational approaches, thereby reducing vulnerabilities associated with user behavior. It was also found that the sustainability and effectiveness of these measures largely depend on the institutional context and the level of cybersecurity maturity. The findings highlight the need to strengthen the culture of digital security, especially in Latin American environments such as Colombia, where technological and educational gaps increase exposure to these threats. The proposed recommendations aim to guide public and private policies toward comprehensive risk management, reinforcing resilience against increasingly sophisticated techniques of manipulation and digital fraud.

Keywords: Cybersecurity, Phishing, Social Engineering, Security Awareness, Incident Management.

Tabla de Contenido

Introducción	13
Planteamiento del Problema.....	15
Justificación.....	17
Objetivos	19
Objetivo General	19
Objetivos Específicos.....	19
Marco Referencial	20
Antecedentes	20
Antecedentes Nacionales	21
Factores que Contribuyen a la Vulnerabilidad.....	22
<i>Casos Emblemáticos en el País</i>	22
Marco Conceptual	24
Conceptos Claves del Marco Conceptual	24
<i>Ciberseguridad</i>	24
<i>Phishing</i>	25
<i>Ingeniería Social</i>	25
<i>Estrategias de Prevención y Mitigación</i>	26
<i>Impacto en la Ciberseguridad</i>	26
<i>Factor Humano en la Ciberseguridad</i>	27
<i>Resiliencia Digital</i>	27
<i>Autenticación Multifactor (MFA)</i>	28
<i>Concienciación En Seguridad Digital</i>	28
Marco Teórico	30
Antecedentes y Evolución de las Amenazas	30
<i>Evolución Histórica de Phishing</i>	30
<i>Ingeniería social y Fundamentos Psicológicos</i>	31
<i>Estadísticas y Tendencias Recientes</i>	31
<i>Casos Documentados en El Mundo y en Latinoamérica</i>	32
Impacto Del Phishing E Ingeniería Social En La Ciberseguridad	33
<i>Efectos en la Triada CIA</i>	33
<i>Impacto Económico y Reputacional</i>	34
<i>Riesgos para los Usuarios Individuales</i>	34
Estrategias de Prevención y Mitigación.....	35

<i>Estrategias Técnicas</i>	35
<i>Estrategias Humanas</i>	35
<i>Estrategias Organizacionales</i>	36
<i>Estrategias Basadas en Tecnologías Emergentes</i>	36
<i>Ejemplos de Buenas Practicas</i>	36
Marcos de Referencia y Teorías Aplicadas	37
<i>Limitaciones y Retos Actuales en Ciberseguridad Frente al Phishing e Ingeniería Social</i>	38
<i>Síntesis Conceptual: Estrategias y Retos frente a Phishing e Ingeniería Social</i>	40
Ley 1273 de 2009: Protección de la Información y los Datos	42
Ley 1581 de 2012: Protección de datos Personales	42
Ley 1266 de 2008: Habeas Data Financiero	42
Convenio de Budapest sobre la Ciberdelincuencia	42
Decisión 872 de la Comunidad Andina (CAN)	43
Recomendaciones OCDE sobre Privacidad y Confianza Digital	43
Marco Contextual	45
Diseño Metodológico	47
Enfoque de Investigación	47
Tipo de Investigación	47
Método y Técnicas de Información	47
Fases metodológicas	48
<i>Fase 1: Identificación del Problema y Delimitación del Objetivo de Estudio</i>	48
<i>Fase 2: Revisión y Análisis Documental Sistemático</i>	48
<i>Fase 3: Evaluación Crítica de las Estrategias Identificadas</i>	48
<i>Fase 4: Formulación de Recomendaciones y Conclusiones</i>	48
Tendencias Actuales en Ciberseguridad Frente Al Phishing y la Ingeniería Social	49
Phishing y sus Variantes	50
Impacto en la Seguridad	52
Impacto de los Ataques en la Ciberseguridad	55
Ingeniería Social: Técnicas y Fundamentos	55
Técnicas Principales	55
<i>Relación con Vulnerabilidades Humanas</i>	56
<i>Impacto y Vulnerabilidades Humanas</i>	58
Tendencias de las Técnicas de Phishing e Ingeniería Social y su Impacto Sectorial ...	58
<i>Tendencias y Evolución de las Amenazas en Ciberseguridad</i>	60

Panorama Comparativo Global, Latinoamericano y Colombiano	62
Costos e Impacto Económico de los Ataques de Phishing e Ingeniería Social	64
<i>Estrategias de Defensa Emergentes</i>	64
Protección de Datos y Resiliencia Digital Frente a Ataques de Phishing e Ingeniería Social.....	66
Estándares y Marcos de Referencia en la Prevención De Phishing y la Ingeniería Social	67
<i>ISO/IEC 27001, 27002, 27035 y 27701</i>	67
<i>NIST Cybersecurity Framework (CSF)</i>	68
<i>ENISA (European Union Agency for Cybersecurity)</i>	70
<i>MITRE ATT&CK</i>	71
<i>ANSSI (Agencia Nacional de Seguridad de los Sistemas de Información – Francia)</i>	73
Revisión de Literatura y Estudios Previos	74
<i>Estudios Académicos y Reportes Técnicos</i>	74
<i>Casos Documentados de Incidentes</i>	74
Casos de Éxito y Medidas de Mitigación Frente Al Phishing y la Ingeniería Social ...	75
<i>Microsoft: adopción de Autenticación Multifactor (MFA)</i>	76
<i>Google: Protección Proactiva contra Phishing</i>	76
<i>IBM: Simulacros Internos y Protección Multinivel</i>	77
<i>ANSSI (Agencia Nacional de Seguridad de los Sistemas de Información – Francia): Directrices de Seguridad</i>	77
<i>Otras Iniciativas Destacadas</i>	78
Evaluación del Impacto en la Resiliencia de los Sistemas Digitales	79
<i>Resistencia Frente a los Ataques</i>	79
<i>Capacidad de Recuperación</i>	79
<i>Mejora en la Capacidad de Respuesta</i>	80
<i>Evidencias en el Contexto Organizacional</i>	80
Adaptabilidad de los Estándares y Marcos en el Contexto Organizacional.....	80
Conclusiones del Capítulo	82
Propuestas de Optimización en la Defensa Contra Ataques de Phishing e Ingeniería Social.....	84
Relevancia de la Ingeniería Social en la Ciberseguridad	85
Estrategias Actuales de Prevención y Mitigación	86
<i>Estrategias Técnicas</i>	86
<i>Estrategias Humanas</i>	88

<i>Estrategias Organizacionales</i>	89
Evaluación del Impacto de las Estrategias Actuales	91
<i>Indicadores de Medición</i>	92
Estrategias Emergentes y Tecnológicas de Apoyo	99
Inteligencia Artificial y Aprendizaje Automático (IA/ML)	100
Propuestas de Mejora	101
<i>Fortalecimiento de la Autenticación Multifactor (MFA)</i>	102
<i>Integración de Inteligencia Artificial en la Detección Temprana</i>	102
<i>Programas de Concienciación y Formación Continua</i>	102
<i>Políticas Internas Robustas y Revisiones Periódicas</i>	103
<i>Colaboración Público-Privada</i>	103
<i>Estrategias de Protección de Datos</i>	103
Conclusiones derivadas del análisis	104
Recomendaciones derivadas al análisis	105
Conclusiones	107
Referencias Bibliográficas	109

Lista de Tablas

Tabla 1 <i>Indicadores Clave para la Evaluación del Impacto de las Estrategias de Prevención y Mitigación</i>	93
Tabla 2 <i>Indicadores para la Evaluación del Impacto de las Estrategias de Mitigación de Ataques de Ingeniería Social y Phishing</i>	96

Lista de Figuras

Figura 1 <i>Crecimiento del Smishing a Nivel Global (2020–2024)</i>	51
Figura 2 <i>Incremento de Dominios de Phishing Registrados (2020–2024)</i>	52
Figura 3 <i>Impacto de la Capacitación en la Reducción del Phishing</i>	54
Figura 4 <i>Tipos más Comunes de Ataques de Ingeniería Social</i>	57
Figura 5 <i>Sectores más Afectados por Ataques de Phishing (2023–2024)</i>	59
Figura 6 <i>Evolución de Tácticas de Phishing y Técnicas de Evasión (2025)</i>	61
Figura 7 <i>Panorama Comparativo de Ataques de Phishing e Ingeniería Social a Nivel Global, Regional y Nacional (2019–2024)</i>	63

Lista de Apéndices

Apéndice A	Glosario	114
-------------------	-----------------------	------------

Introducción

En un entorno digital cada vez más interconectado y dependiente de la información, las amenazas cibernéticas evolucionan constantemente, desafiando constantemente la capacidad de respuesta tanto de individuos como de organizaciones. En este contexto, el phishing y la ingeniería social han emergido como dos de las técnicas más utilizadas por los ciberdelincuentes, quienes se aprovechan de factores como la confianza, la premura y la falta de conocimiento de los usuarios para obtener información confidencial o comprometer infraestructuras críticas. Su peligrosidad radica en que no se enfocan exclusivamente en fallas técnicas, sino que explotan primordialmente las debilidades del comportamiento humano.

Estas formas de ataque generan impactos que van más allá de lo tecnológico, provocando consecuencias significativas en lo social, económico y reputacional. La transformación digital acelerada en sectores como el financiero, educativo, sanitario y comercial ha ampliado los vectores de ataque, evidenciando que las soluciones deben ir más allá del uso de herramientas tradicionales. En este sentido, la capacitación continua, la sensibilización frente a los riesgos y la adopción de buenas prácticas en seguridad digital se convierten en elementos clave para disminuir la exposición y reforzar la protección.

Esta investigación plantea un análisis reflexivo y profundo sobre las estrategias actuales de prevención y mitigación frente al phishing y la ingeniería social, con el propósito de evaluar su efectividad en la protección de los sistemas digitales y la resiliencia organizacional. Se busca determinar qué métodos resultan más eficientes, cómo se están aplicando en distintos entornos, y qué oportunidades de mejora pueden desarrollarse para enfrentar con mayor eficacia amenazas que evolucionan al ritmo de las tecnologías y los hábitos digitales.

El estudio aborda esta problemática desde una perspectiva integral que combina dimensiones técnicas y humanas, entendiendo que las soluciones efectivas requieren enfoques transversales. En muchos casos, las fallas defensivas no se deben a la ausencia de tecnología, sino a la debilidad en la cultura de ciberseguridad, la falta de formación digital y la inadecuada implementación de políticas internas. Mediante el análisis de casos reales, tendencias actuales y evidencias concretas, esta investigación pretende ofrecer aportes significativos que permitan comprender la dinámica de estos ataques y formular recomendaciones aplicables a entornos reales.

La realización de este estudio se justifica en la urgencia de mitigar los efectos de estas amenazas que, si bien no siempre son visibles, comprometen seriamente la operatividad de las organizaciones, debilitan la confianza del usuario y afectan el tejido social. Bajo esta perspectiva, se refuerza la necesidad de replantear y consolidar las estrategias de ciberseguridad no solo como mecanismos tecnológicos, sino como pilares fundamentales para garantizar la continuidad operativa, la protección de los activos informacionales y la sostenibilidad del entorno digital en el largo plazo.

Planteamiento del Problema

En los últimos años, los ataques de phishing e ingeniería social se han convertido en una de las principales amenazas para la ciberseguridad en todo tipo de organizaciones, afectando tanto a empresas privadas como a instituciones públicas. Estos ataques se caracterizan por el uso de engaños y manipulaciones psicológicas para obtener acceso a información sensible, como credenciales de usuario, datos financieros y otros activos digitales críticos. Según estudios recientes, publicados por Infobae, una gran cantidad de incidentes de seguridad que comprometen la confidencialidad, integridad y disponibilidad de la información son el resultado de ataques exitosos que explotan la falta de conocimiento y las debilidades humanas (Duran, 2023).

A pesar de los avances en tecnologías de ciberseguridad, los atacantes continúan perfeccionando sus métodos, lo que hace que los enfoques tradicionales para prevenir y mitigar estas amenazas no siempre sean suficientes. La rápida adopción de tecnologías digitales, sumada al crecimiento del trabajo remoto y la dependencia de plataformas en línea, ha ampliado la superficie de ataque, haciendo que las organizaciones sean cada vez más vulnerables a las técnicas de phishing sofisticadas y ataques de ingeniería social dirigidos.

Aunque existen diversas estrategias de prevención y mitigación implementadas por organizaciones, como la autenticación multifactor, la capacitación continua de los empleados y el uso de tecnologías basadas en inteligencia artificial, su efectividad y el impacto real en la protección de la información no han sido suficientemente evaluados. En muchos casos, según Bridge T. (2024), la falta de análisis profundo sobre la eficacia de estas estrategias dificulta la toma de decisiones informadas para mejorar la postura de seguridad.

Ante este escenario, surge la necesidad de investigar y evaluar las principales estrategias que se utilizan para prevenir y mitigar los ataques de phishing e ingeniería social, analizando su impacto en la reducción de incidentes cibernéticos y la protección de los sistemas digitales. Esta investigación busca no solo identificar las prácticas más efectivas, sino también proponer mejoras basadas en un análisis crítico de su implementación en diferentes sectores, contribuyendo a la formulación de políticas de ciberseguridad más robustas y adaptadas a las amenazas actuales.

¿Cuáles son las principales estrategias para prevenir y mitigar ataques de phishing e ingeniería social que impactan en la ciberseguridad al reducir vulnerabilidades y proteger la información en los sistemas digitales?

Justificación

Ante el crecimiento exponencial del uso de tecnologías digitales en todos los ámbitos de la vida cotidiana y organizacional, han surgido nuevas amenazas que afectan directamente la seguridad de la información. Entre ellas, el phishing y la ingeniería social se han consolidado como riesgos prioritarios, al comprometer no solo los sistemas tecnológicos, sino también al eslabón más frágil de la ciberseguridad: el factor humano. Esta investigación se justifica por la necesidad urgente de comprender y fortalecer estrategias que permitan mitigar dichos riesgos, integrando un enfoque técnico con perspectivas sociales, educativas e industriales.

Desde la perspectiva social, el aumento de los delitos cibernéticos impacta gravemente a ciudadanos y grupos vulnerables que carecen de conocimientos adecuados en seguridad digital. Las consecuencias pueden incluir desde la pérdida de información personal hasta el robo de identidad y efectos emocionales negativos. En este sentido, fomentar estrategias preventivas basadas en la educación y la concientización digital contribuye al desarrollo de una ciudadanía digital más consciente, cerrando brechas tecnológicas y fortaleciendo la resiliencia comunitaria frente a este tipo de amenazas.

Metodológicamente, esta investigación adopta un enfoque analítico para evaluar la eficacia de diferentes estrategias actualmente implementadas, tales como la autenticación multifactor, los programas de capacitación continua o la simulación de ataques. Este análisis permitirá no solo evidenciar el impacto real de dichas medidas en la reducción de incidentes, sino también proponer mejoras adaptables a diversos entornos organizacionales.

La pertinencia del estudio se basa en el constante crecimiento y sofisticación de los ataques de phishing y técnicas de ingeniería social, a pesar del progreso tecnológico. Esto revela la necesidad crítica de diseñar soluciones integrales que articulen componentes humanos y

tecnológicos, especialmente en países como Colombia, donde persisten debilidades estructurales en materia de ciberseguridad tanto en el sector público como en el privado.

En cuanto a su relevancia académica y profesional, los resultados de esta investigación pueden ser clave para orientar decisiones relacionadas con políticas de seguridad, fortalecimiento institucional y desarrollo de campañas educativas. Además, permitirán establecer criterios para evaluar la efectividad de estrategias existentes, promoviendo una cultura organizacional más proactiva en temas de ciberseguridad.

Desde el ámbito industrial, el estudio adquiere especial importancia al considerar que sectores clave como salud, banca, energía y educación son objetivos frecuentes de este tipo de ataques. Analizar y proponer medidas de mitigación eficaces puede traducirse en una reducción significativa de los costos asociados a incidentes, una mayor continuidad operativa y un incremento en la confianza de usuarios y clientes.

En conclusión, esta investigación responde a una necesidad urgente de fortalecer la ciberseguridad mediante un enfoque integral que articule lo técnico con lo humano, y lo organizacional con lo social, con el propósito de contribuir a la creación de entornos digitales más seguros, resilientes y confiables.

Objetivos

Objetivo General

Analizar las principales estrategias de prevención y mitigación de ataques de phishing e ingeniería social, evaluando su impacto en la ciberseguridad y su efectividad en la reducción de la vulnerabilidad de los sistemas digitales.

Objetivos Específicos

Analizar las tendencias actuales en ciberseguridad enfocadas con la prevención y mitigación de ataques de phishing e ingeniería social para evaluar su efectividad en la reducción de la vulnerabilidad de los sistemas digitales.

Determinar el impacto de las estrategias de prevención y mitigación de ataques de phishing e ingeniería social en la protección de datos y la resiliencia de los sistemas digitales.

Proponer mejoras a las estrategias actuales utilizadas para la prevención y mitigación de ataques de phishing e ingeniería social, basadas en la evaluación de su impacto en la ciberseguridad.

Marco Referencial

Antecedentes

América Latina ha experimentado un incremento exponencial de ciberataques en la última década. Según el informe del Observatorio Latinoamericano de Amenazas Digitales (OLAD), en 2024 se documentaron más de 400 incidentes relacionados a ciberataques, violencia de género digital, censura, espionaje y vigilancia masiva en países como Brasil, México, Ecuador, Colombia, Nicaragua y Venezuela. Estos ataques han afectado tanto a las organizaciones gubernamentales como la sociedad civil, evidenciando una creciente vulnerabilidad en la región (OLAD,2025).

Los sectores más afectados incluyen infraestructuras críticas, servicios financieros, salud y educación. Además, se ha observado una tendencia creciente en ataques dirigidos a defensores de DDHH y periodistas, lo que plantea preocupaciones sobre la libertad de expresión y la seguridad en línea (OLAD,2025).

Varios países en Latinoamérica han sido víctimas de ciberataques significativos. En Brasil, este año, se reportó un incidente en el que la Agencia Brasileña de Inteligencia (ABIN) fue acusada de vigilar ilegalmente a 30.000 personas, incluidos periodistas y magistrados del Supremo Tribunal Federal. Este caso generó un debate sobre la privacidad y el uso indebido de tecnologías de vigilancia en el país (OLAD,2025).

En México, la presidenta Claudia Sheinbaum reveló que su teléfono y correo electrónico fueron interceptados, lo que puso de manifiesto las vulnerabilidades en la seguridad digital incluso en altos niveles de gobierno. Es urgente fortalecer las medidas de ciberseguridad en las instituciones gubernamentales.

Este año en Argentina los aeropuertos de Ezeiza y Aeroparque fueron afectados por una falla en el sistema de seguridad informática, lo que generó demoras y cancelaciones de vuelos. Este incidente evidenció la dependencia crítica y cancelaciones de vuelos. Este incidente evidenció la existencia de dependencia crítica de las infraestructuras de transporte en sistemas digitales y la necesidad de contar con protocolos de seguridad robustos.

Las tácticas de los atacantes cibernéticos en América Latina han evolucionado e incorporado tecnologías avanzadas como la inteligencia artificial para mejorar la efectividad de sus ataques. El phishing, en particular, ha experimentado un crecimiento exponencial, con un aumento del 140% de los intentos de fraude por mensajes falsos en 2024. Los ataques cibernéticos usan técnicas sofisticadas como la creación de sitios webs falsos y suplantación de la identidad, para engañar a usuarios y obtener información confidencial (Kaspersky,2024). Además, se ha observado el uso de deepfakes y distintas formas de manipulación digital para difundir desinformación y llevar a cabo campañas de ingeniería social. Estas técnicas representan un desafío significativo para la detección de ciberataques, ya que dificultan la identificación de contenido genuino y aumentan la probabilidad de que víctimas caigan en trampas digitales (Kaspersky,2024).

Antecedentes Nacionales

En los últimos años Colombia ha sido uno de los países más afectados por ciber ataques en Latinoamérica. Según un informe de Fortiguards Labs, durante la primera parte del 2024 se registraron más de 36 mil millones de intentos de ciber ataques, siendo el phishing el más popular, especialmente en el sector salud con un 60% de los incidentes (Alcaldía de Cali,2025)

ACIS (2024) señala que, entre octubre de 2023 y octubre de 2024, se bloquearon 26 millones de ataques de malware en Colombia, incluyendo intentos de phishing; La creciente sofisticación de estas amenazas hace que sea cada vez más difíciles de combatir.

Factores que Contribuyen a la Vulnerabilidad

La falta de una sólida cultura de ciberseguridad entre ciudadanos y las empresas es una de las mayores amenazas para que ocurran ataques cibernéticos. Muchas organizaciones no cuentan con procedimientos y sistemas adecuados para la protección de datos lo que los convierte en blancos fáciles para atacantes (Bancolombia, 2024).

La necesidad de rápida expansión y la adopción de nuevas tecnologías, sin una inversión en medidas de seguridad ha ampliado la superficie de ataque. Prey Project (2023) afirma que el uso de dispositivos móviles y redes sociales ha facilitado la recopilación de informaciones personal por parte de los atacantes, quienes los usan para personalizar sus ataques de ingenierías social.

Casos Emblemáticos en el País

Uno de los casos más destacados en el 2024 fue el ataque de ransomware a la empresa Air-e, dedicada al rubro del suministro eléctrico en varias regiones del país El ataque interrumpió los servicios en línea de la empresa afectando a miles de personas y resaltando la vulnerabilidad de las infraestructuras críticas (BusinessCol, 2024).

Diversas entidades gubernamentales han intensificado sus esfuerzos en fortalecer la ciberseguridad en el país. La alcaldía de Cali reforzó sus sistemas de seguridad informática a través de la implementación de nuevas medidas para proteger la información y los servicios públicos (CCE,2024).

La situación actual genera la necesidad de generar una estrategia integral que aborde los aspectos técnicos y humanos de la ciberseguridad. Es necesario promover la educación y conciencia sobre los riesgos cibernéticos, así como implementar políticas públicas y tecnologías adecuadas para prevenir y mitigar ataques. Solo a través de un esfuerzo mancomunado entre el gobierno, las empresas privadas y la sociedad civil se podrá fortalecer la resiliencia digital en Colombia frente a las amenazas emergentes (KPMG,2024).

Marco Conceptual

En el panorama digital actual, las amenazas cibernéticas han evolucionado considerablemente, siendo el phishing y las técnicas de ingeniería social algunas de las más relevantes. Estos métodos se basan en la manipulación del factor humano para acceder a información sensible, constituyendo un desafío permanente para la seguridad informática tanto de individuos como de organizaciones.

En este marco conceptual se establecen los términos clave que sustentan la investigación y su vinculación con la prevención y mitigación de las amenazas cibernéticas. Tener un entendimiento claro de estos conceptos resulta fundamental para evaluar la efectividad de las estrategias implementadas y su impacto en la disminución de vulnerabilidades en los sistemas digitales. De este modo, el marco conceptual no solo define las nociones esenciales, sino que también proporciona la base teórica necesaria para interpretar los resultados obtenidos en la investigación.

Conceptos Claves del Marco Conceptual

Ciberseguridad

La ciberseguridad se entiende como la disciplina encargada de proteger la confidencialidad, integridad y disponibilidad de los datos y sistemas digitales mediante la aplicación de controles técnicos, procesos organizacionales y programas de concienciación. Su relevancia radica en que constituye la primera línea de defensa frente al incremento de amenazas cibernéticas que afectan tanto a individuos como a organizaciones. Este ámbito no se limita a la protección frente a ataques tradicionales, como virus o intrusiones, sino que también aborda tácticas más sofisticadas que combinan tecnología y manipulación psicológica, como el phishing y la ingeniería social. Además, la ciberseguridad comprende el diseño de políticas, la gestión de

riesgos y la formación continua, consolidándose como un pilar fundamental para garantizar la confianza digital y la continuidad operativa en un entorno cada vez más interconectado (International Organization for Standardization, 2020).

Phishing

El phishing es una técnica de ciberdelincuencia que busca engañar a las víctimas mediante correos electrónicos, sitios web, mensajes de texto o llamadas telefónicas falsificados, con el objetivo de obtener credenciales, información financiera u otros datos sensibles. Este tipo de ataque se caracteriza por suplantar a entidades legítimas, generando confianza en los usuarios y facilitando el fraude. Entre sus modalidades se encuentran el spear phishing, dirigido a objetivos concretos; el whaling, enfocado en altos ejecutivos; y variantes como el smishing y el vishing, que utilizan mensajes de texto y llamadas, respectivamente. Por su facilidad de ejecución y eficacia, el phishing se ha convertido en una de las amenazas más frecuentes en el ámbito de la ciberseguridad, con repercusiones que van desde pérdidas económicas hasta daños en la reputación. Por ello, resulta fundamental comprenderlo a fondo para diseñar estrategias preventivas efectivas (ENISA, 2023).

Ingeniería Social

La ingeniería social comprende un conjunto de técnicas de manipulación psicológica utilizadas para inducir a las personas a revelar información o ejecutar acciones que comprometen la seguridad de los sistemas. A diferencia de los ataques exclusivamente técnicos, este enfoque se aprovecha de factores humanos como la confianza, la urgencia o la falta de conocimiento, convirtiendo al usuario en el eslabón más vulnerable de la cadena de protección digital. Entre sus métodos más frecuentes se encuentran el pretexting, que consiste en crear un pretexto falso para generar confianza; el baiting, que utiliza incentivos engañosos; y el tailgating, que permite el

acceso físico a zonas restringidas aprovechando la cortesía de otras personas. Mitnick y Simon (2022) nos explica que, la relación entre el pretexting y el phishing es estrecha, de manera que ambos se consideran amenazas complementarias dentro del ámbito de la ciberseguridad; Comprender la ingeniería social resulta esencial para diseñar programas de concienciación que refuercen la protección humana frente a la manipulación.

Estrategias de Prevención y Mitigación

Las estrategias de prevención y mitigación frente al phishing y la ingeniería social incluyen un conjunto de medidas destinadas a disminuir la probabilidad de éxito de estos ataques y a minimizar sus consecuencias en caso de ocurrencia. Entre las más relevantes se encuentran las políticas de seguridad de la información, que establecen lineamientos para la gestión segura de datos y accesos; la capacitación y concienciación de los usuarios, considerada la primera línea de defensa ante ataques que explotan el factor humano; y la adopción de tecnologías de protección, como filtros de correo electrónico, herramientas para detectar sitios fraudulentos y soluciones basadas en inteligencia artificial. Del mismo modo, la autenticación multifactor (MFA) se ha consolidado como un mecanismo eficaz para reforzar la seguridad de las credenciales y dificultar accesos no autorizados. Es importante destacar que estas estrategias deben implementarse de manera integral, combinando aspectos técnicos, organizativos y humanos para maximizar su efectividad (CISA, 2023).

Impacto en la Ciberseguridad

El impacto de las estrategias de prevención y mitigación en ciberseguridad se evidencia en la capacidad de las organizaciones para reducir vulnerabilidades y fortalecer su postura defensiva frente a las amenazas. La implementación de medidas efectivas no solo disminuye el riesgo de pérdidas económicas o filtración de información, sino que también contribuye a proteger la confianza de los usuarios y a garantizar la continuidad operativa. Además, contar con

un marco de ciberseguridad sólido permite a las instituciones anticiparse a tendencias emergentes, como el uso de inteligencia artificial en ataques de phishing o la explotación de dispositivos móviles en ingeniería social. En este sentido, evaluar el impacto de las estrategias adoptadas es fundamental, ya que permite identificar fortalezas y debilidades en la protección vigente y orientar la toma de decisiones hacia políticas más adaptativas, sostenibles y efectivas a lo largo del tiempo (Keeper Security, 2022).

Factor Humano en la Ciberseguridad

El factor humano se reconoce como un componente crítico en la seguridad informática, dado que una gran proporción de los incidentes se originan por errores, descuidos o falta de capacitación adecuada. Este elemento es comúnmente denominado el “eslabón más débil” de la cadena de protección digital, ya que incluso los sistemas más sofisticados pueden ser comprometidos si los usuarios caen en engaños o no aplican buenas prácticas. Tanto el phishing como la ingeniería social explotan estas vulnerabilidades, lo que resalta la importancia de fortalecer la educación y la cultura de seguridad. La implementación de programas de concienciación, junto con políticas organizacionales bien definidas, contribuye a reducir riesgos y a mejorar la capacidad de respuesta del personal. Por ello Verizon (2023) nos confirma que, el análisis del factor humano resulta esencial para desarrollar estrategias de prevención y mitigación más eficaces.

Resiliencia Digital

La resiliencia digital se define como la capacidad de una organización o individuo para anticipar, resistir, responder y recuperarse ante un ataque o incidente cibernético, garantizando la continuidad de las operaciones y minimizando su impacto. Este concepto no se limita únicamente a la prevención de incidentes, sino que también busca asegurar que, cuando ocurran,

sus consecuencias sean controladas y que se pueda restablecer la normalidad con rapidez. La resiliencia digital integra medidas técnicas, organizacionales y humanas, requiriendo preparación, entrenamiento y adaptación continua frente a un entorno de amenazas en constante evolución. En relación con el phishing y la ingeniería social, el *National Institute of Standards and Technology* (NIST, 2018) señala que no solo se requiere contar con tecnologías de detección y respuesta, sino también fortalecer la cultura de seguridad entre los usuarios, lo que constituye un indicador clave de la madurez en ciberseguridad de cualquier organización.

Autenticación Multifactor (MFA)

La autenticación multifactor (MFA) se considera una de las medidas más efectivas para proteger las credenciales de los usuarios, al requerir la combinación de al menos dos factores de verificación: conocimiento (contraseña), posesión (dispositivo) y biometría (rasgos físicos). Su implementación disminuye de manera significativa la probabilidad de éxito de los ataques de phishing, ya que, incluso si un atacante obtiene la contraseña, le resultará muy difícil acceder a la cuenta sin el factor adicional. Hoy en día, la MFA se emplea de forma generalizada en servicios financieros, corporativos y de gobierno electrónico, consolidándose como un estándar de seguridad recomendado. Asimismo, su integración con otras medidas, como la detección de anomalías basada en inteligencia artificial, incrementa la capacidad de las organizaciones para prevenir ataques sofisticados. Por ello, la MFA constituye un componente fundamental dentro de las estrategias de mitigación de riesgos asociados a la ingeniería social (Microsoft, 2023).

Concienciación En Seguridad Digital

La concienciación en seguridad digital se refiere a los procesos de formación y capacitación continúa dirigidos a que los usuarios puedan identificar amenazas, evitar conductas de riesgo y fortalecer la cultura de ciberseguridad en ámbitos tanto organizacionales como

personales. Este enfoque se considera una de las medidas más efectivas para disminuir la vulnerabilidad frente a ataques de phishing e ingeniería social, dado que el conocimiento permite que el usuario se convierta en un eslabón sólido dentro de la cadena de seguridad. Entre las estrategias más utilizadas se incluyen las campañas de simulación de phishing, los talleres prácticos y la difusión continua de buenas prácticas. Al incorporar la concienciación dentro de una política organizacional de seguridad, se fomenta la corresponsabilidad y se incrementa la resiliencia digital frente a amenazas emergentes. Por estas razones, la concienciación constituye un pilar fundamental en cualquier estrategia de prevención (KnowBe4, 2024).

Marco Teórico

El marco teórico de esta investigación tiene como objetivo respaldar el estudio mediante los aportes teóricos, normativos y prácticos que han abordado el phishing y la ingeniería social como amenazas críticas en el ámbito de la ciberseguridad. A través del análisis de estudios previos, informes técnicos y marcos internacionales de referencia, se busca comprender la evolución de estas amenazas y las estrategias implementadas para su prevención y mitigación. La importancia de este análisis radica en que tanto el phishing como la ingeniería social explotan el factor humano, considerado el eslabón más débil de la seguridad digital, provocando consecuencias que van desde el robo de credenciales hasta pérdidas económicas y daños reputacionales.

En este contexto, resulta fundamental analizar las principales estrategias adoptadas por organizaciones y gobiernos, tales como la autenticación multifactor, el uso de filtros avanzados de correo electrónico, la concienciación en seguridad digital y la implementación de marcos normativos como ISO/IEC 27001, que ofrecen directrices para la gestión de riesgos y el fortalecimiento de la resiliencia digital. Del mismo modo, el estudio de estas estrategias permite identificar sus fortalezas y limitaciones, proporcionando una visión integral sobre su impacto real en la protección de la información y en la continuidad operativa de las organizaciones. Así, el marco teórico no solo consolida la base conceptual del estudio, sino que también contextualiza la necesidad de mejorar las medidas existentes frente a amenazas cada vez más sofisticadas.

Antecedentes y Evolución de las Amenazas

Evolución Histórica de Phishing

Jagatic et al. (2007) nos dice que el phishing emergió a mediados de la década de 1990, vinculado a fraudes en plataformas de correo electrónico y servicios de Internet como AOL,

donde los ciberdelincuentes buscaban obtener credenciales de usuarios con poca experiencia. Con la llegada de la web 2.0 y el auge de las redes sociales, este tipo de ataque evolucionó hacia campañas más dirigidas, que permiten personalizar los mensajes para incrementar la credibilidad y efectividad (Hong, 2012).

En la actualidad, la inteligencia artificial (IA) ha potenciado la creación de correos electrónicos falsos y sitios web altamente realistas, lo que dificulta significativamente su detección. De igual manera, se ha evidenciado la utilización de deepfakes y métodos de clonación de voz en ataques de vishing, lo que introduce un grado superior de sofisticación en la manipulación de las víctimas (Europol, 2023).

Ingeniería social y Fundamentos Psicológicos

La ingeniería social se ha posicionado como un componente central en los ataques cibernéticos actuales, dado que se enfoca en explotar factores psicológicos más que en aprovechar fallos técnicos. Según Mitnick y Simon (2022), los atacantes recurren a la manipulación de emociones y sesgos cognitivos como la confianza, la urgencia, el miedo o la curiosidad con el fin de ejercer presión psicológica sobre las víctimas y motivarlas a revelar información sensible o realizar acciones inseguras.

Estos principios permiten comprender por qué las campañas de phishing resultan tan efectivas: no dependen exclusivamente de habilidades técnicas avanzadas, sino de la capacidad de persuadir y engañar a las víctimas mediante mensajes que aparentan legitimidad.

Estadísticas y Tendencias Recientes

Los reportes internacionales resaltan que el phishing y la ingeniería social se mantienen entre las amenazas más críticas en el ámbito de la ciberseguridad. según el Verizon Data Breach Investigations Report (2023) evidencia que un 74 % de las vulneraciones de seguridad tienen

como factor común la intervención humana, siendo el phishing una de las técnicas predominantes en los incidentes registrados.

El IBM Cost of a Data Breach Report (2024) indica que los incidentes de phishing alcanzan un costo promedio de 4,91 millones de dólares, situándolos entre las formas de ataque más onerosas. En el contexto europeo, el informe de ENISA Threat Landscape (2023) advierte un aumento constante en la frecuencia de campañas de phishing que tienen como objetivo infraestructuras críticas. De manera similar, en España, el INCIBE (2023) reconoce al phishing como la amenaza más reportada tanto por organizaciones como por ciudadanos.

Casos Documentados en El Mundo y en Latinoamérica

En el panorama internacional, se han registrado casos emblemáticos que reflejan el alcance del phishing y la ingeniería social. Uno de ellos fue el ataque contra Sony Pictures en 2014, donde un fraude de este tipo derivó en la exposición masiva de correos electrónicos y datos corporativos (FBI, 2015). Otro ejemplo relevante ocurrió en 2016, cuando una campaña de *spear phishing* dirigida a miembros del Comité Nacional Demócrata (DNC) en Estados Unidos demostró cómo estas técnicas pueden emplearse como instrumentos de injerencia política (Rid, 2020).

En el contexto latinoamericano, el crecimiento de los ataques de phishing ha sido notorio. De acuerdo con Kaspersky (2023), Brasil, México y Colombia figuran entre los países más impactados, con campañas dirigidas principalmente al fraude bancario y financiero. En el caso colombiano, la Policía Nacional (2022), citado por CCIT (2022) informó que, en 2022 se registró un aumento del 70 % en las denuncias por delitos electrónicos, siendo el phishing una de las modalidades más frecuentes.

Impacto Del Phishing E Ingeniería Social En La Ciberseguridad

Efectos en la Triada CIA

El phishing y la ingeniería social afectan de manera directa los tres pilares esenciales de la ciberseguridad, representados en la tríada CIA: Confidencialidad, Integridad y Disponibilidad de la información.

Confidencialidad. este principio se vulnera cuando los atacantes obtienen, a través de técnicas de engaño, credenciales de acceso, información personal o datos corporativos sensibles. El resultado puede derivar en robo de identidad, fraude financiero o en la filtración de información estratégica que compromete la seguridad de las organizaciones (ISO/IEC, 2022).

Integridad. este principio se ve comprometido cuando los datos son modificados o alterados como consecuencia de un acceso no autorizado. Ejemplos de ello incluyen la manipulación de bases de datos financieras o la alteración de órdenes de pago obtenidas mediante fraudes de ingeniería social, lo que genera pérdidas económicas y afecta la confiabilidad de la información (ENISA, 2023).

Disponibilidad. este principio se ve afectado cuando los atacantes utilizan el phishing como vector inicial para desplegar campañas de ransomware. Dichos ataques bloquean el acceso a sistemas y datos críticos hasta el pago de un rescate, ocasionando interrupciones operativas graves que impactan la continuidad del negocio y la prestación de servicios esenciales (IBM, 2024).

En consecuencia, el phishing y la ingeniería social trascienden el nivel individual y se configuran como un riesgo de carácter sistémico, capaz de comprometer la estabilidad y continuidad de los servicios digitales.

Impacto Económico y Reputacional

Los ataques de phishing ocasionan un impacto económico significativo. De acuerdo con el *IBM Cost of a Data Breach Report* (2024), el costo medio asociado a una filtración de datos derivada de este tipo de ataque alcanza los 4,91 millones de dólares, lo que lo posiciona entre los métodos más onerosos a nivel mundial.

Además del daño económico directo, los ataques de phishing generan un considerable impacto reputacional. La confianza de clientes, inversionistas y aliados estratégicos suele verse comprometida, afectando de manera prolongada la credibilidad institucional. El Verizon Data Breach Investigations Report (2023) señala que más de la mitad de las organizaciones que experimentan incidentes de este tipo presentan un deterioro en su imagen pública, lo que repercute directamente en la fidelización de clientes y en su posición competitiva en el mercado.

Riesgos para los Usuarios Individuales

En el ámbito individual, el phishing y la ingeniería social constituyen una amenaza considerable para los usuarios. Entre sus principales consecuencias se destacan:

Robo de Identidad. obtención de información personal (números de identificación, contraseñas, datos bancarios) para realizar fraudes en nombre de la víctima (Kaspersky,2023).

Fraude Financiero. uso de credenciales robadas para acceder a cuentas bancarias, realizar transferencias no autorizadas o compras fraudulentas (INCIBE,2023).

Pérdida de Privacidad: exposición de datos sensibles que pueden ser vendidos en mercados ilegales o utilizados en campañas de extorsión (EUROPOL,2023).

Estos riesgos refuerzan la noción de que la ciberseguridad no constituye únicamente una responsabilidad corporativa, sino un desafío de carácter social que involucra por igual a ciudadanos, instituciones y gobiernos.

Estrategias de Prevención y Mitigación

La prevención y mitigación de los ataques de phishing e ingeniería social exige un enfoque integral que articule medidas técnicas, humanas y organizacionales, complementadas con el uso de tecnologías emergentes. En este sentido, la literatura especializada y las buenas prácticas internacionales destacan diversas estrategias que se describen a continuación.

Estrategias Técnicas

Entre las medidas técnicas más efectivas destacan la autenticación multifactor (MFA), el cifrado de la información y la implementación de protocolos de seguridad para el correo electrónico. En este último ámbito, el uso de estándares como SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail) y DMARC (Domain-based Message Authentication, Reporting & Conformance) resulta fundamental, ya que permiten verificar la autenticidad de los mensajes y reducir la suplantación de identidad en los sistemas de correo (INCIBE,2023). Estas soluciones constituyen una primera línea de defensa sólida frente a intentos de suplantación digital.

Estrategias Humanas

El factor humano continúa siendo el eslabón más vulnerable en la ciberseguridad. Por ello, los programas de concienciación, la capacitación continua y los simulacros de phishing se consolidan como componentes esenciales en la prevención. Iniciativas como las promovidas por el Instituto Nacional de Ciberseguridad (INCIBE) en España demuestran que los ejercicios de simulación permiten evaluar la capacidad de respuesta de los empleados y reducir significativamente el índice de clics en correos fraudulentos. Asimismo, la formación periódica favorece el desarrollo de una cultura de ciberseguridad, en la que los usuarios asumen un rol activo en la protección digital.

Estrategias Organizacionales

Las organizaciones deben complementar las medidas técnicas y humanas con políticas de seguridad bien definidas, planes de respuesta ante incidentes y acciones orientadas al fortalecimiento de la resiliencia digital. De acuerdo con la Norma ISO/IEC 27001 (2022), resulta indispensable establecer controles que garanticen la confidencialidad, integridad y disponibilidad de la información, junto con mecanismos de mejora continua dentro del sistema de gestión de seguridad. Del mismo modo, la incorporación de equipos especializados como Red Team y Blue Team favorece la identificación proactiva de vulnerabilidades y la mitigación temprana de riesgos.

Estrategias Basadas en Tecnologías Emergentes

Las tendencias actuales muestran un creciente aprovechamiento de la inteligencia artificial (IA) y el aprendizaje automático, herramientas capaces de detectar patrones anómalos en el tráfico de red, identificar correos maliciosos y anticipar ataques antes de que afecten a los usuarios (ENISA, 2023). De manera complementaria, la Zero Trust Architecture (ZTA) se consolida como una estrategia clave al partir del principio de “*nunca confiar, siempre verificar*”, garantizando que únicamente usuarios y dispositivos autenticados y autorizados accedan a los recursos (Microsoft, 2023). Estas soluciones refuerzan los enfoques tradicionales y aportan una mayor capacidad de adaptación frente a las amenazas modernas.

Ejemplos de Buenas Practicas

Diversos gobiernos y empresas han logrado implementar con éxito estas medidas. En Colombia, el Centro Cibernético Policial y el ColCERT promueven campañas de concienciación ciudadana y fomentan la adopción de marcos de seguridad alineados con estándares internacionales (CCIT,2022). En Europa, la Agencia de la Unión Europea para la Ciberseguridad

(ENISA) recomienda un enfoque integral que combine controles técnicos, programas de educación y cooperación multisectorial entre entidades públicas y privadas. En el ámbito corporativo, empresas internacionales como Google y Microsoft han fortalecido sus servicios mediante la implementación de políticas de Zero Trust y autenticación multifactor, con el fin de proteger a millones de usuarios frente a intentos de phishing. Estos casos demuestran que la articulación de estrategias técnicas, humanas y organizacionales es fundamental para incrementar la resiliencia digital a nivel global.

Marcos de Referencia y Teorías Aplicadas

Diversos marcos de referencia internacionales y enfoques teóricos en materia de ciberseguridad conforman la base conceptual para el análisis y la gestión de amenazas como el phishing y la ingeniería social. Estos instrumentos no se limitan a ofrecer pautas técnicas, sino que también guían a las organizaciones en la implementación de prácticas más sólidas, resilientes y sostenibles en el tiempo.

En el ámbito normativo, la ISO/IEC 27001 y sus normas complementarias, como la ISO/IEC 27002, orientada a la implementación de controles de seguridad, y la ISO/IEC 27035, enfocada en la gestión de incidentes, constituyen un marco estructurado para garantizar la protección de la información y una respuesta eficaz frente a ataques (ISO/IEC, 2022).

Por su parte, el NIST Cybersecurity Framework (CSF) establece cinco funciones esenciales identificar, proteger, detectar, responder y recuperar que orientan a las organizaciones en el desarrollo de capacidades de seguridad adaptables frente a amenazas como los ataques de ingeniería social (NIST, 2018).

Desde una perspectiva operacional, el marco MITRE ATT&CK ofrece una clasificación detallada de tácticas y técnicas empleadas por adversarios, entre ellas las vinculadas al phishing,

como la T1566: Phishing y la T1598: Spear Phishing Attachment (MITRE, 2023). Este enfoque permite a los equipos de seguridad anticipar, detectar y mapear patrones de ataque específicos, fortaleciendo así las capacidades defensivas.

En cuanto a tendencias arquitectónicas, el modelo de Zero Trust Architecture (ZTA) se consolida como una estrategia clave frente a los ataques basados en credenciales, al sustentarse en el principio de “*nunca confiar, siempre verificar*”. Este enfoque restringe los accesos incluso dentro de la propia red corporativa, garantizando que cada solicitud de conexión sea autenticada y autorizada de manera continua (Microsoft, 2023).

Finalmente, las teorías clásicas en seguridad de la información continúan siendo referentes fundamentales. La tríada CIA (Confidencialidad, Integridad y Disponibilidad) establece los principios esenciales de protección; el modelo del “eslabón más débil” resalta la vulnerabilidad del factor humano como puerta de entrada a los ataques; y el enfoque de resiliencia digital enfatiza la importancia de anticipar, resistir y recuperarse de los incidentes para garantizar la continuidad operativa (ENISA, 2023).

Estos marcos y teorías no deben entenderse de manera aislada, sino como componentes complementarios e interdependientes que fortalecen la comprensión del fenómeno del phishing y la ingeniería social. En este sentido, constituyen la base conceptual que respalda las estrategias de prevención y mitigación que serán desarrolladas en el Capítulo 3 de la presente investigación.

Limitaciones y Retos Actuales en Ciberseguridad Frente al Phishing e Ingeniería Social

A pesar de los avances en la adopción de medidas técnicas, normativas y educativas, persisten limitaciones significativas y desafíos emergentes en la prevención y mitigación de ataques de phishing e ingeniería social.

En primer lugar, las campañas de concienciación presentan limitaciones vinculadas con su continuidad y efectividad. Si bien resultan útiles para sensibilizar a los usuarios, distintos estudios evidencian que su impacto tiende a disminuir con el tiempo cuando no se acompañan e programas de capacitación continua y de simulaciones realistas que refuercen el aprendizaje (INCIBE, 2023).

En segundo lugar, los ciberdelincuentes avanzan de manera continua, incorporando el uso de inteligencia artificial (IA), aprendizaje automático y deepfakes, tecnologías que facilitan la creación de mensajes y contenidos con un alto nivel de realismo. Esta evolución ha derivado en variantes como el spear phishing, caracterizadas por su elevado grado de personalización y la consecuente dificultad para ser detectadas (ENISA,2023).

Un tercer desafío se observa en las brechas estructurales presentes en los países en desarrollo, particularmente en Latinoamérica, donde la escasa inversión en ciberseguridad, la infraestructura tecnológica insuficiente y la carencia de profesionales especializados incrementan la vulnerabilidad frente a estas amenazas (OEA & BID,2020).

Finalmente, uno de los retos actuales radica en la ausencia de estandarización y armonización en las políticas de ciberseguridad. Mientras que regiones como la Unión Europea han avanzado con marcos comunes, como la directiva NIS2, en América Latina prevalece la fragmentación normativa, lo que limita la cooperación internacional y dificulta articular respuestas coordinadas frente a incidentes (CEPAL,2022).

En conclusión, los vacíos y desafíos identificados evidencian que, aunque existen políticas y estrategias relevantes en el campo de la ciberseguridad, su eficacia depende de una adaptación continua frente a amenazas emergentes, de una inversión sostenida en capacidades técnicas y humanas y de una mayor cooperación internacional. Solo mediante un enfoque

integral que articule formación constante, innovación tecnológica y marcos normativos coordinados será posible afrontar de manera efectiva los riesgos asociados al phishing y la ingeniería social en el panorama actual.

Síntesis Conceptual: Estrategias y Retos frente a Phishing e Ingeniería Social

Las amenazas de ciberseguridad contemporáneas, entre ellas el phishing y la ingeniería social, se caracterizan por su naturaleza híbrida, ya que combinan elementos tecnológicos con la explotación de factores humanos. Los atacantes recurren a herramientas avanzadas como la inteligencia artificial y los deepfakes para incrementar la efectividad de sus tácticas, mientras que la carencia de formación y de una adecuada cultura de seguridad en los usuarios amplifica la vulnerabilidad de las organizaciones (ENISA, 2023; INCIBE, 2023).

Las estrategias de mayor eficacia son aquellas que combinan recursos tecnológicos con el fomento de una cultura de seguridad y procesos de capacitación constante. Herramientas como los sistemas avanzados de detección, los filtros antiphishing y los mecanismos de autenticación resultan más efectivos cuando se integran con programas de concienciación y ejercicios de simulación periódicos, los cuales refuerzan las buenas prácticas de los usuarios y aumentan la resiliencia organizacional (OEA & BID, 2020).

De igual manera, resulta fundamental adaptar los marcos internacionales de ciberseguridad a la realidad latinoamericana y, en particular, al contexto colombiano. Factores como la limitada inversión en infraestructura, la carencia de profesionales especializados y la dispersión normativa hacen necesario realizar ajustes locales que permitan garantizar la efectividad y sostenibilidad de las políticas y estrategias implementadas (CEPAL, 2022).

En conclusión, la articulación entre tecnología, programas de formación y adaptación al contexto específico se consolida como la base fundamental para enfrentar con eficacia los

ataques de phishing e ingeniería social, mitigando riesgos y garantizando la continuidad operativa.

Marco Legal

Ley 1273 de 2009: Protección de la Información y los Datos

La ley 1273 incorporó al Código Penal colombiano el título VII Bis, denominado “De la protección de la Información y de los datos”, estableciendo un marco normativo pionero en el país para combatir delitos informáticos. Entre sus artículos más relevantes se encuentra el 269^a (Acceso abusivo a un sistema informático) y el 269G (suplantación de sitios web), que tipifica directamente el phishing como una conducta delictiva. Esta ley representó un avance significativo al reconocer las necesidades de protección penal frente a amenazas digitales emergentes (Mesa Giraldo & Ponce Jaramillo, 2023).

Ley 1581 de 2012: Protección de datos Personales

Esta ley desarrolla el derecho constitucional al habeas data, que reconoce a los ciudadanos con el control de sus datos personales. Establece principios claros como la finalidad, veracidad, seguridad, confidencialidad y libertad, además de definir derechos como conocer, actualizar, rectificar y suprimir datos personales, así como revocar la autorización de su uso. Esta ley se complementa con la regulación de la Superintendencia de la industria y Comercio, que actúa como autoridad de control y supervisión (Congreso de Colombia, 2012).

Ley 1266 de 2008: Habeas Data Financiero

La ley 1266 regula el manejo de información personal relacionada con el historial crediticio, estableciendo medidas para el tratamiento responsable, seguro y transparente de los datos. Es clave para evitar la suplantación de identidad con fines fraudulentos en entornos bancarios donde el phishing representa la principal amenaza (Congreso de Colombia, 2008).

Convenio de Budapest sobre la Ciberdelincuencia

Colombia ratificó en 2018 el Convenio de Budapest, convirtiéndose en el primer país Latino Americano en adherirse a este tratado. A través de la ley 1928 de 2018, Colombia se

comprometió a homologar su legislación con los estándares internacionales para combatir contra delitos informáticos, como el acceso ilegal a sistemas, la distribución de herramientas para ataques cibernéticos y la interceptación ilícita de datos. El tratado además promueve la cooperación judicial transfronteriza lo que es crucial ya que el phishing tiene una naturaleza global (Consejo de Europa, 2001).

Decisión 872 de la Comunidad Andina (CAN)

La Decisión 872 de 2020 adoptada por los países de la comunidad andina, incluido Colombia, establece principios comunes en materia de protección de datos personales. Esta norma refuerza derechos como el consentimiento informado, la finalidad legítima y la transparencia. Se complementa a la legislación nacional y fomenta la interoperabilidad normativa entre países andinos (Comunidad Andina, 2020).

Recomendaciones OCDE sobre Privacidad y Confianza Digital

Colombia es país miembro de la OCDE desde el 2020 y ha incorporado las Directrices sobre la protección de la privacidad y los flujos transfronterizos de datos personales. Si bien no son jurídicamente vinculantes, promueven las buenas prácticas en privacidad digital, gobernanza de datos y seguridad de la información, lo que impacta directamente en el diseño de políticas públicas en Ciber seguridad y combate al phishing (OCDE,2013).

A pesar del sólido marco legal nacional e internacional, Colombia enfrenta varios desafíos para aplicar de forma eficaz estas normativas:

1. Capacitación especializada: El personal judicial y las fuerzas del orden requieren formación continua en ciber investigación y manejo de la evidencia digital.
2. Actualización legislativa continua: La evolución constante de técnicas como el phishing con inteligencia artificial o deepfakes necesita reformas legales ágiles.

3. Cooperación regional y global: La coordinación internacional es fundamental para perseguir delitos que cruzan los límites geográficos y jurisdiccionales como los crímenes cibernéticos.

4. Educación ciudadana: La normativa debe complementarse con campañas masivas de alfabetización digital para prevenir fraudes.

Marco Contextual

La ciberseguridad se ha convertido en una preocupación central a nivel mundial debido al aumento exponencial de los delitos informáticos. La inteligencia artificial se ha utilizado para personalizar ataques, haciendo que prácticas como el phishing sean más difíciles de detectar.

La ingeniería social sigue siendo una de las tácticas más comunes, donde los atacantes manipulan a las personas para obtener información confidencial. Esto se ha visto reflejado en el aumento de casos de phishing, donde los usuarios son engañados para revelar contraseñas o información financiera, lo que ha llevado a pérdidas económicas significativas y a la exposición de datos sensibles.

La región latinoamericana ha experimentado un incremento en los ciberataques, afectando tanto a instituciones gubernamentales como al sector privado. La falta de infraestructura tecnológica de calidad y la escasa concienciación sobre ciberseguridad han contribuido a la vulnerabilidad de los sistemas.

Colombia ha sido testigo de un aumento en los delitos informáticos, especialmente en modalidades como el phishing. La Unidad de Delitos Informáticos de la Policía Judicial ha reportado un incremento en las denuncias relacionadas con estafas electrónicas, donde los atacantes suplantan entidades financieras para obtener información confidencial de los usuarios.

La Ley 1273 de 2009 ha sido fundamental en la tipificación de estos delitos, estableciendo sanciones para quienes diseñen páginas electrónicas fraudulentas con el fin de capturar datos personales. Sin embargo, la rápida evolución de las técnicas de los ciberdelincuentes plantea desafíos constantes para las autoridades y requiere una actualización continua de las estrategias de prevención y respuesta.

El impacto de los ciberataques en Colombia no se limita al ámbito tecnológico; también tiene repercusiones sociales y económicas significativas. Las empresas enfrentan pérdidas financieras debido a fraudes y a la interrupción de sus operaciones, mientras que los ciudadanos pueden sufrir el robo de identidad y la pérdida de confianza en los servicios digitales.

Además, la brecha digital existente en el país agrava la situación, ya que muchas personas carecen de los conocimientos necesarios para identificar y prevenir ataques de phishing. Esto resalta la importancia de implementar programas de educación en ciberseguridad y de promover una cultura de prevención entre la población.

Diseño Metodológico

El enfoque metodológico de esta investigación fue desarrollado con el objetivo de examinar las estrategias orientadas a la prevención y mitigación de ataques de phishing e ingeniería social, valorando su influencia en la ciberseguridad desde una perspectiva crítica y aplicada. Para alcanzar este propósito, se adoptó una metodología cualitativa de carácter descriptivo y exploratorio, empleando el análisis documental como técnica principal de recolección y estudio de la información.

Enfoque de Investigación

Se adopta un enfoque cualitativo, dado que el propósito es comprender, interpretar y analizar información obtenida de fuentes documentales, reportes técnicos, estudios de caso y literatura especializada, sin apoyarse en métodos de cuantificación estadística. La complejidad del problema requiere una interpretación profunda de los contextos organizacionales, las prácticas humanas y los factores subjetivos que influyen en la eficacia de las estrategias de ciberseguridad.

Tipo de Investigación

Se llevó a cabo una investigación de carácter descriptivo y exploratorio, lo que permitió analizar y delinear las estrategias actuales frente a la problemática abordada, así como indagar en prácticas emergentes en el campo. El método utilizado fue el análisis documental, a través del cual se revisaron fuentes como estudios académicos, informes técnicos, manuales institucionales, artículos especializados y normativas vigentes.

Método y Técnicas de Información

La investigación se llevó a cabo con un enfoque cualitativo, teniendo como método central el análisis documental. Para ello, se consultaron fuentes académicas, técnicas y

normativas publicadas entre 2019 y 2024, lo que facilitó la recolección de información relevante sobre estrategias de prevención y mitigación frente a ataques de phishing e ingeniería social.

Fases metodológicas

Fase 1: Identificación del Problema y Delimitación del Objetivo de Estudio

Se definió la problemática y el alcance del estudio a partir de una revisión exploratoria de fuentes académicas y técnicas, lo que permitió contextualizar las amenazas de phishing e ingeniería social y formular los objetivos de investigación.

Fase 2: Revisión y Análisis Documental Sistemático

Se realizó una revisión estructurada de fuentes académicas, técnicas y normativas publicadas entre 2019 y 2024, lo que permitió identificar tendencias y buenas prácticas en las estrategias de ciberseguridad frente al phishing y la ingeniería social.

Fase 3: Evaluación Crítica de las Estrategias Identificadas

Se valoraron las principales estrategias de prevención y mitigación, considerando su eficacia, sostenibilidad y pertinencia en distintos contextos. El análisis comparativo mostró que las más efectivas son aquellas que combinan componentes técnicos y educativos, frente a las que dependen únicamente de soluciones automatizadas.

Fase 4: Formulación de Recomendaciones y Conclusiones

En esta fase se establecen las recomendaciones y conclusiones derivadas del análisis, las cuales se presentan en la sección final del documento.

Tendencias Actuales en Ciberseguridad Frente Al Phishing y la Ingeniería Social

En los últimos años, las amenazas de phishing e ingeniería social han experimentado una notable evolución, ajustándose tanto a los avances tecnológicos como a las nuevas dinámicas laborales, en particular con la expansión del trabajo remoto. Entre los cambios más relevantes se encuentran:

1. Uso de deepfakes: replicación de voz o imagen de altos ejecutivos en videollamadas o mensajes para inducir transferencias o filtración de información.
2. Simulación en redes sociales: creación de perfiles falsos en plataformas profesionales como LinkedIn para ganar la confianza de empleados y aplicar técnicas de pretexting.
3. Ataques multicanal: combinación de correos electrónicos, SMS y llamadas telefónicas que refuerzan la credibilidad de las campañas.
4. Explotación del trabajo remoto: mayor exposición a ataques debido a redes domésticas menos seguras y uso extendido de plataformas como Teams, Zoom o Slack.

De acuerdo con el IBM Cost of a Data Breach Report 2024, el phishing representa el 16% de las brechas de seguridad, generando un costo promedio de 4,91 millones de dólares por cada incidente. En el caso de América Latina, los intentos de phishing se multiplicaron por seis durante 2023, lo que evidencia la mayor vulnerabilidad de usuarios y organizaciones en la región.

Este capítulo analiza las tendencias recientes asociadas a estas amenazas, basándose en informes de ciberseguridad y en reportes de compañías del sector como Kaspersky, ENISA, Proofpoint y Cisco, complementados con gráficos, estadísticas e indicadores que muestran su alcance e impacto.

Phishing y sus Variantes

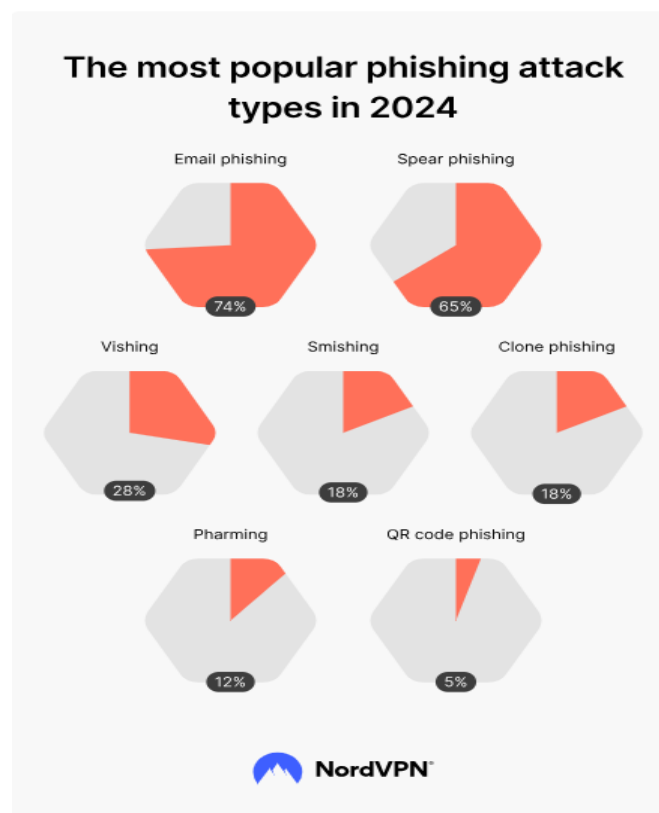
El phishing es una técnica de manipulación utilizada por ciberdelincuentes para obtener datos sensibles, como contraseñas o información financiera, engañando a las víctimas mediante correos electrónicos, mensajes o sitios web falsos que simulan ser legítimos.

Sus principales modalidades incluyen:

1. Phishing tradicional: Mensajes fraudulentos enviados masivamente que aparentan provenir de entidades confiables.
2. Spear phishing: Ataque dirigido y personalizado contra personas u organizaciones específicas.
3. Whaling: Orientado a altos directivos con acceso a información crítica.
4. Smishing: Mensajes SMS que incluyen enlaces o solicitudes falsas.
5. Vishing: Llamadas telefónicas en las que los atacantes se hacen pasar por representantes legítimos.
6. Pharming: Redirección a sitios web falsos mediante manipulación de DNS o malware.
7. Clone phishing: Copia de correos legítimos reemplazando archivos/enlaces por maliciosos.
8. Business Email Compromise (BEC): Uso de correos corporativos comprometidos para fraudes financieros.
9. Angler phishing: Fraudes en redes sociales a través de perfiles falsos de soporte técnico.

Figura 1

Crecimiento del Smishing a Nivel Global (2020–2024)



Nota. La gráfica muestra el aumento constante de los ataques de smishing en los últimos años, impulsado por la amplia adopción de dispositivos móviles y la confianza que los usuarios depositan en los mensajes SMS. Este patrón evidencia cómo los ciberdelincuentes diversifican sus canales de ingeniería social.

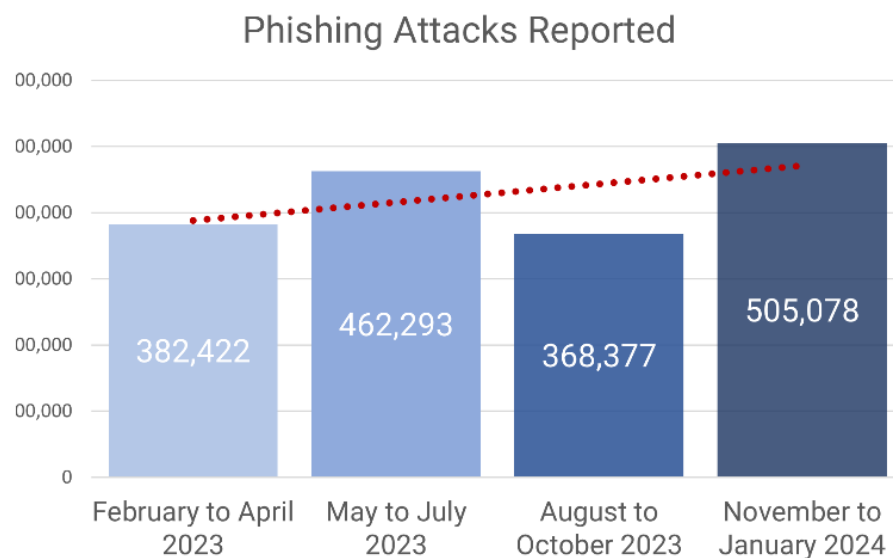
Según el APWG Trends Report (Q4 2023), los intentos globales de phishing alcanzaron 1.077.501 incidentes en el cuarto trimestre de 2023, lo que evidencia un crecimiento sostenido respecto a años anteriores y refuerza la importancia de implementar estrategias preventivas y de

mitigación. Tomado de. NordVPN. Cybersecurity statistics and facts you need to know (2025).

<https://nordvpn.com/blog/cybersecurity-statistics/>

Figura 2

Incremento de Dominios de Phishing Registrados (2020–2024)



Nota. La figura muestra el aumento continuo de dominios maliciosos asociados con phishing, evidenciando la industrialización de este tipo de ataques y la facilidad con la que los ciberdelincuentes crean sitios fraudulentos para engañar a sus víctimas. Tomado de. Cybercrime Information Center. (2024). Phishing landscape studies: Phishing domains report. Recuperado de <https://www.cybercrimeinfocenter.org/phishing-landscape-studies>

Impacto en la Seguridad

El phishing afecta la confidencialidad, integridad y disponibilidad de la información. Sus principales consecuencias son:

1. Compromiso de sistemas: mediante credenciales robadas que permiten instalar malware o ransomware y propagar ataques dentro de la red.

Ejemplo: correos de phishing que buscan el robo de credenciales para acceder a sistemas críticos o cuentas bancarias.

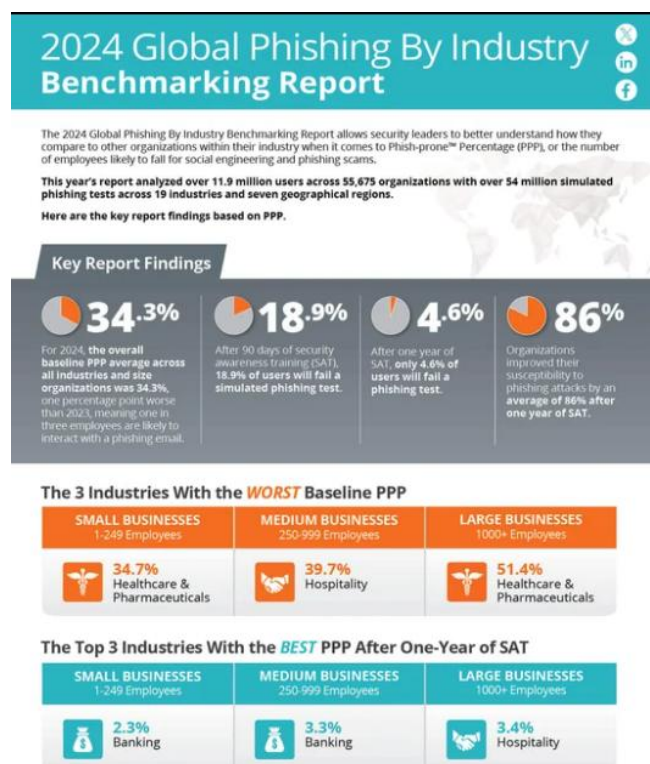
2. Pérdida de integridad de los datos: modificación, eliminación o corrupción de información crítica.

Ejemplo: cuando un empleado víctima de phishing provoca filtraciones de datos a gran escala que afectan la confiabilidad de la información.

3. Violación de la confidencialidad: robo de datos personales, financieros o corporativos.

Ejemplo: correos que incluyen archivos adjuntos maliciosos capaces de instalar malware en dispositivos.

Figura 3

Impacto de la Capacitación en la Reducción del Phishing

Nota. La figura evidencia que la capacitación en seguridad disminuye la exposición de los empleados al phishing. Al inicio, el 34,3 % de ellos caía en pruebas de phishing; sin embargo, tras 90 días de entrenamiento, la tasa se reduce al 18,9 %, y después de un año de formación continua, apenas el 4,6 % sigue siendo vulnerable. Asimismo, el 86 % de las organizaciones consiguió reducir de manera significativa su riesgo de phishing mediante programas de capacitación sostenida. Tomado de. KnowBe4. Phishing by industry benchmarking report (2024). <https://info.knowbe4.com/phishing-by-industry-benchmarking-report-partner>

Impacto de los Ataques en la Ciberseguridad

Los ataques de phishing e ingeniería social representan una amenaza directa para los principios fundamentales de la ciberseguridad: confidencialidad, integridad y disponibilidad de los sistemas digitales.

1. Confidencialidad: se ve comprometida cuando los atacantes obtienen acceso a credenciales, datos bancarios o secretos corporativos. Técnicas como spear phishing o whaling resultan especialmente riesgosas al dirigirse a altos ejecutivos con acceso privilegiado.

2. Integridad: los atacantes pueden modificar registros financieros, inventarios o insertar datos falsos en bases de datos, afectando la confiabilidad de la información y las decisiones estratégicas.

3. Disponibilidad: el engaño mediante phishing puede llevar a la instalación de ransomware, bloqueando sistemas críticos en sectores como salud, banca o gobierno, y generando interrupciones operativas.

Ingeniería Social: Técnicas y Fundamentos

La ingeniería social se basa en la manipulación psicológica para inducir a las personas a revelar información o permitir accesos indebidos. A diferencia de los ataques puramente técnicos, explota factores humanos como la confianza, el miedo, la urgencia o la curiosidad.

Técnicas Principales

1. Pretexting: creación de historias o identidades falsas para obtener información.

2. Baiting: uso de incentivos atractivos (como memorias USB infectadas) para engañar a las víctimas.

3. Tailgating: ingreso físico no autorizado siguiendo a alguien con acceso legítimo.

4. Shoulder surfing: observación directa para capturar contraseñas o información sensible.
5. Quid pro quo: intercambio de favores o servicios a cambio de credenciales o datos.
6. Ingeniería social en redes sociales: creación de perfiles falsos para obtener confianza y explotar información personal.

Relación con Vulnerabilidades Humanas

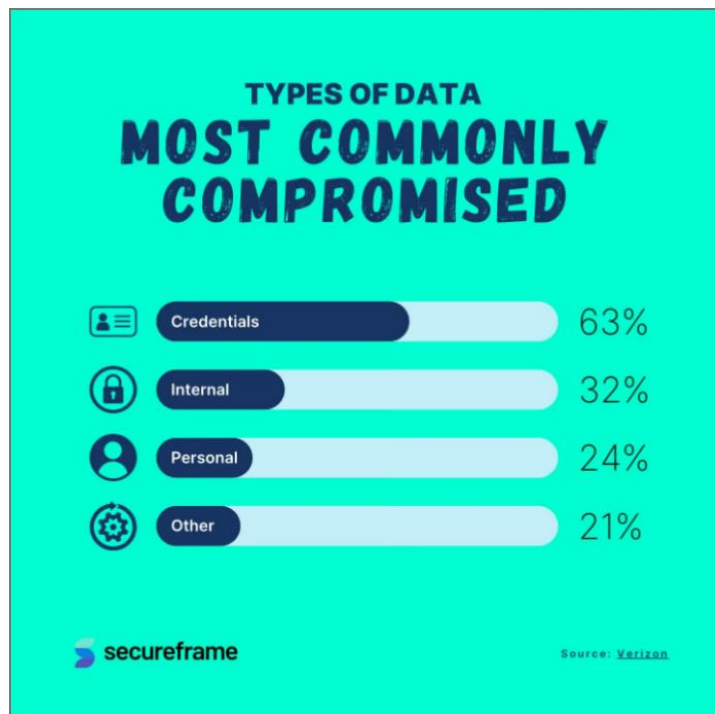
Los atacantes explotan:

1. Confianza en figuras de autoridad.
2. Ignorancia o falta de capacitación.
3. Temor y urgencia, que reducen el pensamiento crítico.
4. Curiosidad y avaricia, aprovechando ofertas atractivas.

Según el *Verizon Data Breach Investigations Report 2023* y Secureframe (2024), el phishing representa aproximadamente el 44 % de los incidentes de ingeniería social, consolidándose como la técnica más utilizada por los atacantes y el principal medio para comprometer sistemas.

Figura 4

Tipos más Comunes de Ataques de Ingeniería Social



Nota. La figura ilustra los tipos de datos que los atacantes comprometen con mayor frecuencia.

El 63 % de los incidentes involucran credenciales, seguidos de información interna (32 %), datos personales (24 %) y otros tipos de información (21 %). Esto evidencia que la exposición de credenciales constituye la principal vía de ataque en incidentes de seguridad, subrayando la importancia de reforzar la gestión de contraseñas y la concienciación del personal. Tomado de. Verizon. data breach investigations report (DBIR).(2023).

<https://www.verizon.com/business/resources/Tbfc/reports/2023-data-breach-investigations-report-dbir.pdf>

Impacto y Vulnerabilidades Humanas

Diversos estudios destacan que el factor humano continúa siendo el eslabón más vulnerable en ciberseguridad. Según Proofpoint (2024), más del 70 % de los empleados reconoce realizar acciones riesgosas a pesar de ser conscientes de los posibles compromisos a la seguridad.

El impacto económico de un ataque de phishing exitoso puede superar los 14 millones de dólares por organización, especialmente cuando se incluyen vishing y fraudes empresariales (Cyber Defense Magazine, 2024).

En Colombia, sectores como el bancario, educativo y de salud han registrado un aumento constante de campañas de phishing dirigidas, lo que evidencia la urgente necesidad de implementar programas de concienciación y fortalecer la cultura de ciberseguridad.

Tendencias de las Técnicas de Phishing e Ingeniería Social y su Impacto Sectorial

Analizar las tendencias actuales en la prevención y mitigación de ataques de phishing e ingeniería social es fundamental para garantizar una ciberseguridad sólida en un entorno digital en constante transformación. Los ciberdelincuentes adaptan de manera continua sus tácticas, incorporando tecnologías emergentes como la inteligencia artificial, los deepfakes y la automatización, lo que hace que las defensas tradicionales se vuelvan obsoletas con rapidez.

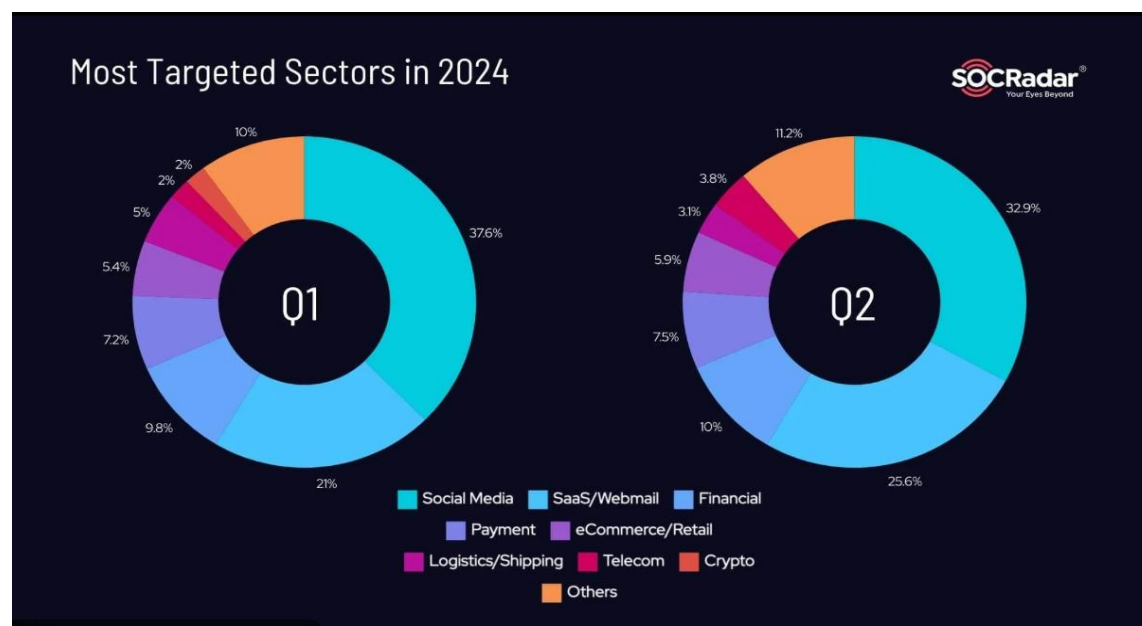
Entre las técnicas más utilizadas destacan el smishing y el vishing, que explotan la confianza depositada en mensajes de texto y llamadas telefónicas; el spear phishing y el whaling, dirigidos específicamente a ejecutivos y usuarios con altos privilegios; así como la ingeniería social a través de redes sociales, donde se emplean perfiles falsos para generar confianza y obtener información. Estas modalidades se ven reforzadas por el uso de IA y deepfakes, que permiten crear mensajes, imágenes y voces cada vez más realistas y convincentes.

El impacto de estas prácticas se evidencia en diversos sectores:

1. Financiero: fraudes electrónicos y robo de credenciales bancarias mediante correos o dominios falsos.
2. Salud: acceso indebido a historiales médicos o interrupción de servicios hospitalarios.
3. Educación: campañas dirigidas a estudiantes y docentes a través de correos institucionales falsificados.
4. Gobierno y sector público: suplantación de entidades oficiales para robar datos ciudadanos o realizar fraudes.
5. Pymes: vulnerables por sus limitados recursos para implementar medidas avanzadas de seguridad.

Figura 5

Sectores más Afectados por Ataques de Phishing (2023–2024)



Nota. La gráfica compara el impacto del phishing en distintas industrias, destacando que sectores como servicios financieros, SaaS/webmail y comercio electrónico concentran la mayoría de los

incidentes. Esto subraya la importancia de implementar estrategias de ciberseguridad específicas para cada sector.

En Colombia y en la región latinoamericana, reportes de Kaspersky y Prey Project evidencian un aumento del 617 % en los intentos de phishing durante 2023, mientras que los ataques de vishing se incrementaron en un 442 % en 2024. Estas cifras reflejan cómo los ciberdelincuentes ajustan sus tácticas al contexto regional, afectando directamente a sectores críticos como la banca, la educación y la salud. Tomado de. SOCRadar. *LATAM threat landscape report*. Threat Landscape Report que incluye análisis de phishing. (2024).

<https://socradar.io/wp-content/uploads/2024/04/LATAM-Threat-Landscape-Report-2024.pdf>

Tendencias y Evolución de las Amenazas en Ciberseguridad

En los últimos años, los ataques de phishing e ingeniería social han experimentado una evolución significativa, impulsada por el progreso tecnológico y el uso masivo de dispositivos móviles. Entre las tendencias más destacadas se encuentran:

1. Automatización y herramientas avanzadas: Campañas masivas realizadas con bots y software de bajo costo, que incrementan la escala y velocidad de los ataques.
2. Inteligencia artificial (IA): Utilizada por atacantes para generar mensajes más personalizados y convincentes (incluyendo deepfakes), y por defensores para detección predictiva y sandboxing de amenazas.
3. Ataques dirigidos: Incremento del spear phishing y whaling, que apuntan a cargos estratégicos dentro de las organizaciones.
4. Migración a móviles y smishing: Con la popularización de dispositivos móviles, los atacantes diversifican los canales de ingeniería social, explotando la confianza de los usuarios en mensajes SMS y dificultando la detección en pantallas pequeñas.

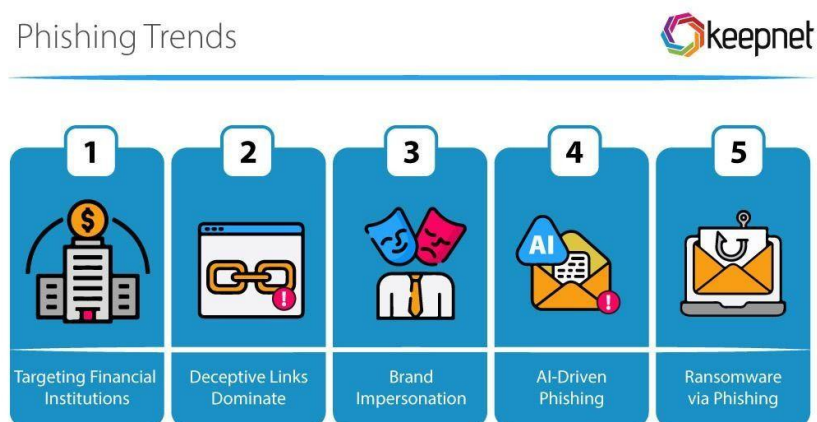
5. Prácticas de mitigación efectivas: Simulaciones de phishing y capacitación continua han demostrado reducir significativamente la vulnerabilidad de los empleados; por ejemplo, KnowBe4 reporta que la tasa de usuarios que cae en correos fraudulentos baja de 34,3 % a 4,6 % tras un año de entrenamiento.

6. Zero Trust y MFA: Mayor implementación de autenticación multifactor y arquitecturas de “confianza cero” para reforzar la defensa frente a ataques sofisticados.

En América Latina, los intentos de phishing se incrementaron un 617 % durante 2023 (Prey Project, 2023), y los ataques de vishing registraron un aumento del 442 % en 2024 (Keepnet Labs, 2024). Estos datos demuestran que la región también enfrenta un crecimiento significativo de las amenazas de ingeniería social, lo que resalta la importancia de establecer programas de concienciación y medidas de seguridad efectivas.

Figura 6

Evolución de Tácticas de Phishing y Técnicas de Evasión (2025)



Nota. La imagen muestra las tendencias actuales del phishing, resaltando cinco puntos principales: ataques dirigidos a entidades financieras, predominancia de enlaces falsos, suplantación de marcas, phishing potenciado por inteligencia artificial y ransomware distribuido

mediante correos fraudulentos. La combinación de estas técnicas con la automatización de campañas y el uso de HTTPS en sitios falsos incrementa la sofisticación de los ataques y dificulta su detección. Tomado de. Keepnet Labs. Top phishing statistics and trends you must know. Keepnet Labs Blog. (2025). <https://keepnetlabs.com/blog/top-phishing-statistics-and-trends-you-must-know>

Panorama Comparativo Global, Latinoamericano y Colombiano

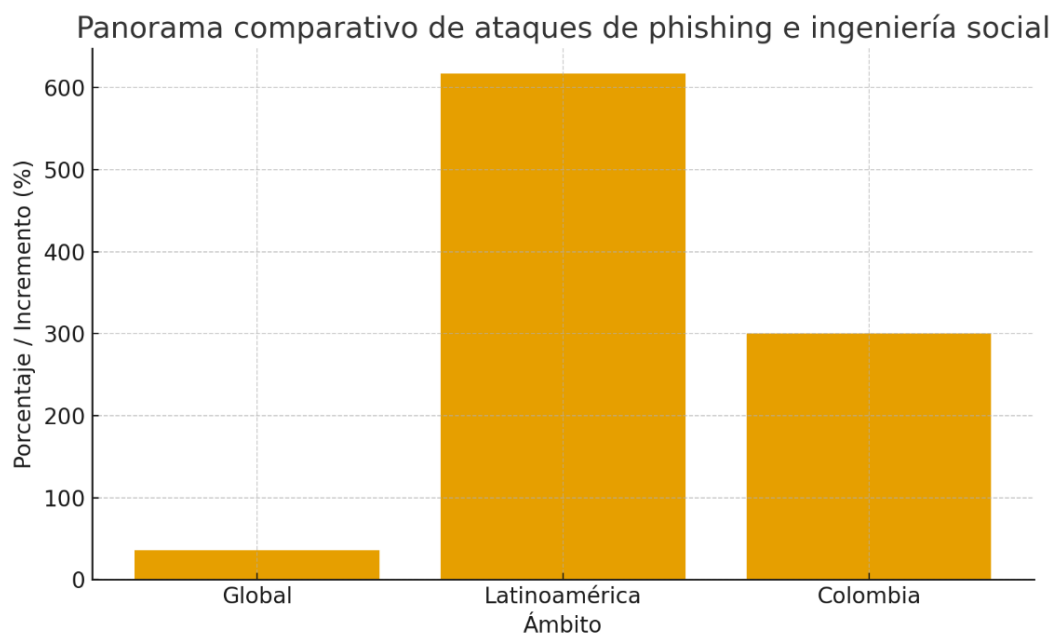
A nivel global, el Verizon DBIR 2023 reporta que el phishing estuvo presente en alrededor del 36 % de todas las brechas de seguridad. De forma paralela, Kaspersky registró cerca de 710 millones de intentos de phishing en 2023, lo que representa un aumento del 40 % en comparación con el año anterior.

En América Latina, los ataques crecieron exponencialmente, según Kaspersky, las campañas de phishing aumentaron un 617 % durante 2023, con un promedio de 544 intentos por minuto, muchos de ellos dirigidos específicamente al sector financiero. Este crecimiento se ve potenciado por la alta conectividad de la región, que alcanza el 77,9 %, superando el promedio mundial del 66,3 %.

En el caso de Colombia, aunque no existen datos públicos recientes, sectores estratégicos como el financiero, el de salud y el educativo enfrentan desafíos similares, dada su alta exposición y dependencia de la tecnología.

Figura 7

Panorama Comparativo de Ataques de Phishing e Ingeniería Social a Nivel Global, Regional y Nacional (2019–2024)



Nota. La gráfica presenta la evolución comparativa de los ataques de phishing e ingeniería social a nivel global, en Latinoamérica y en Colombia. A escala mundial, los incidentes muestran una tendencia creciente sostenida; sin embargo, en Latinoamérica el aumento resulta mucho más marcado, con un 617 % solo en 2023. En el caso de Colombia, los sectores bancarios, educativo y de salud aparecen como los más afectados, lo que evidencia una mayor vulnerabilidad del país frente a estas amenazas. Tomado de. IBM. Cost of a data breach report. (2024).

<https://www.ibm.com/security/digital-assets/cost-data-breach-report/>

Costos e Impacto Económico de los Ataques de Phishing e Ingeniería Social

El impacto económico de los ataques de phishing e ingeniería social ha alcanzado niveles críticos a nivel global. Según el IBM Cost of a Data Breach Report (2024), el costo promedio de una brecha de seguridad originada en phishing es de 4,91 millones de dólares por incidente, lo que lo convierte en uno de los vectores más costosos para las organizaciones.

Por otra parte, Cybersecurity Ventures (2023) estima que las pérdidas globales derivadas del cibercrimen superarán los 10,5 trillones de dólares anuales para 2025, siendo el phishing y el fraude por ingeniería social factores determinantes en este crecimiento.

En América Latina, países como Brasil, México y Colombia concentran una proporción significativa de los incidentes reportados. Según Kaspersky (2023), Colombia se ubicó entre los tres países más afectados de la región en intentos de phishing, impactando de manera especial a sectores estratégicos como la banca, la educación y la salud. En estos casos, las pérdidas económicas no solo se relacionan con fraudes financieros, sino también con interrupciones operativas y daños reputacionales.

Estrategias de Defensa Emergentes

A medida que los ataques de phishing e ingeniería social se vuelven más sofisticados y variados, las organizaciones necesitan implementar estrategias innovadoras para reforzar su ciberseguridad. Entre las tendencias emergentes en defensa se destacan:

1. **Inteligencia artificial en la defensa:** La inteligencia artificial (IA) permite la detección predictiva y el análisis de comportamiento, mejorando la capacidad de identificar amenazas antes de que causen daño. Según el informe de MixMode, la IA está revolucionando la ciberseguridad al automatizar tareas repetitivas y al proporcionar análisis avanzados para detectar patrones anómalos en el comportamiento de los usuarios y sistemas (MixMode, 2024).

2. Seguridad en la nube: La adopción de soluciones de seguridad nativas de la nube es esencial para proteger los entornos híbridos y multicloud. El informe de Palo Alto Networks destaca que el 64% de las organizaciones han experimentado más violaciones de datos en el último año, lo que subraya la necesidad de implementar medidas de seguridad adaptadas a la nube (Palo Alto Networks, 2024).

3. Concienciación gamificada: La capacitación en ciberseguridad mediante simulaciones de phishing gamificadas ha demostrado ser efectiva para mejorar la conciencia y el comportamiento de los empleados. Según Hoxhunt, este enfoque aumenta el compromiso de los usuarios y reduce las conductas riesgosas al proporcionar una experiencia de aprendizaje interactiva y atractiva (Hoxhunt, 2025).

4. Resiliencia cibernética: La capacidad de una organización para prepararse, responder y recuperarse rápidamente ante incidentes cibernéticos es crucial. El informe de Commvault revela que el 83% de las organizaciones encuestadas experimentaron una violación de seguridad significativa, lo que resalta la importancia de tener estrategias de recuperación cibernética bien definidas y probadas.

Estas tendencias no solo fortalecen las defensas existentes, sino que también preparan a las organizaciones para afrontar las nuevas amenazas del entorno digital, sirviendo de introducción al análisis más detallado de estrategias y herramientas que se desarrollará en el

Protección de Datos y Resiliencia Digital Frente a Ataques de Phishing e Ingeniería Social

En el capítulo anterior se presentaron los fundamentos conceptuales y el panorama actual de las amenazas derivadas del phishing y la ingeniería social, destacando su importancia dentro de la ciberseguridad actual. En este capítulo, el análisis se centra específicamente en los estándares, modelos y marcos de referencia que guían la gestión de riesgos asociados a estas amenazas, complementado con la revisión de investigaciones y casos documentados que evidencian tanto situaciones de impacto como experiencias exitosas en la implementación de estrategias de prevención.

El objetivo es analizar cómo marcos internacionales, como las normas ISO/IEC 27001 y 27002 enfocadas en la gestión de la seguridad de la información, el NIST Cybersecurity Framework (CSF), estructurado en las fases de identificación, protección, detección, respuesta y recuperación, o modelos como MITRE ATT&CK, que clasifica técnicas de intrusión entre ellas el phishing (T1566), pueden aplicarse en contextos organizacionales para mitigar el impacto de los ataques de ingeniería social (ISO/IEC, 2022; NIST, 2018; MITRE, 2023). De igual forma, lineamientos regionales como el Esquema Nacional de Seguridad (ENS) en España o las guías emitidas por la ANSSI en Europa proporcionan orientaciones específicas en torno a la gestión de riesgos humanos y a la formación en concienciación (Gobierno de España, 2021; ANSSI, 2022).

Estudios recientes destacan la importancia de incorporar estos marcos en la gestión organizacional. El IBM Cost of a Data Breach Report 2024 indica que el phishing estuvo presente en el 16 % de las brechas de seguridad, con un costo promedio de USD 4,91 millones por incidente (IBM, 2024). De forma complementaria, el Verizon Data Breach Investigations Report 2023 señala que el phishing fue responsable del 44 % de los casos de ingeniería social

(Verizon, 2023). Estas cifras reflejan tanto la gravedad de la problemática como la necesidad de implementar marcos estandarizados que orienten las estrategias de prevención y mitigación.

De esta manera, el capítulo se centra en analizar los principales estándares internacionales y marcos de referencia relacionados con la gestión de riesgos frente al phishing y la ingeniería social; en exponer investigaciones y casos documentados que evidencian tanto las consecuencias de estas amenazas como experiencias exitosas en su mitigación; y finalmente, en reflexionar sobre la aplicabilidad de estos lineamientos en el ámbito organizacional, subrayando su contribución a la reducción de los impactos ocasionados por este tipo de ataques.

Estándares y Marcos de Referencia en la Prevención De Phishing y la Ingeniería Social ***ISO/IEC 27001, 27002, 27035 y 27701***

Los estándares de la familia ISO/IEC 27000 se han consolidado como uno de los marcos de referencia más empleados a nivel global en la gestión de la seguridad de la información. En particular, la ISO/IEC 27001:2022 define los requisitos para establecer un Sistema de Gestión de Seguridad de la Información (SGSI) bajo un enfoque de gestión de riesgos, mientras que la ISO/IEC 27002:2022 lo complementa al ofrecer un conjunto de controles de seguridad aplicables en distintos entornos organizacionales (ISO/IEC, 2022a; ISO/IEC, 2022b). Ambos lineamientos son ampliamente adoptados para reforzar la protección frente a múltiples amenazas, incluyendo el phishing y la ingeniería social, ya que promueven políticas de control de accesos, autenticación multifactor, capacitación del personal y monitoreo continuo.

De forma complementaria, la ISO/IEC 27035 se centra en la gestión de incidentes de seguridad de la información, proporcionando directrices específicas para la detección, reporte, evaluación y respuesta ante ataques cibernéticos (ISO/IEC, 2016). En el contexto del phishing,

este estándar facilita que las organizaciones establezcan procedimientos de respuesta que minimicen el tiempo de exposición y agilicen las acciones de recuperación.

Por su parte, la ISO/IEC 27701:2019 extiende el alcance del SGSI hacia la gestión de la privacidad y la protección de datos personales. Considerando que los ataques de ingeniería social buscan principalmente la obtención de credenciales y datos sensibles, este estándar adquiere especial importancia en sectores altamente regulados, como el de la salud y el financiero, donde la confidencialidad de la información personal resulta crítica (ISO/IEC, 2019).

En conclusión, aunque los estándares ISO no fueron diseñados específicamente para abordar el phishing o la ingeniería social, constituyen una base robusta para mitigar sus efectos al ofrecer un marco integral de gestión de riesgos, controles técnicos, formación del personal y protocolos de respuesta a incidentes. Sin embargo, distintos estudios advierten que estos lineamientos requieren una actualización constante y deben complementarse con tecnologías emergentes como la inteligencia artificial o el análisis avanzado del comportamiento a fin de enfrentar de manera más efectiva las amenazas actuales (Kaur & Singh, 2023; Al-Daraiseh et al., 2022).

NIST Cybersecurity Framework (CSF)

El NIST Cybersecurity Framework (CSF), desarrollado por el National Institute of Standards and Technology de los Estados Unidos, constituye uno de los marcos de referencia más reconocidos a nivel mundial para la gestión de la ciberseguridad en organizaciones de distintos sectores (NIST, 2018). Su propuesta se basa en cinco funciones fundamentales que permiten estructurar un ciclo continuo de mejora frente a amenazas cibernéticas: Identificar, Proteger, Detectar, Responder y Recuperar.

En el ámbito de los ataques de phishing e ingeniería social, el NIST CSF resulta especialmente pertinente, ya que ofrece lineamientos prácticos orientados tanto a la prevención como al fortalecimiento de la resiliencia organizacional:

1. Identificar: Reconocer los activos críticos y los riesgos vinculados al factor humano, lo que implica evaluar la exposición de los usuarios a campañas de phishing y mapear las posibles técnicas de ingeniería social que podrían emplear los atacantes.
2. Proteger: Aplicar controles como la autenticación multifactor (MFA), filtros de correo electrónico, capacitación continua del personal y políticas de acceso basadas en el principio de mínimo privilegio, con el fin de reducir la probabilidad de éxito de los ataques.
3. Detectar: Implementar sistemas de monitoreo y análisis de tráfico que permitan reconocer patrones sospechosos en correos electrónicos, mensajes o enlaces maliciosos. La detección temprana es esencial para contener incidentes antes de que escalen.
4. Responder: Establecer protocolos claros de actuación frente a incidentes exitosos, incluyendo la notificación, la contención de cuentas comprometidas y la comunicación interna para evitar la propagación del ataque.
5. Recuperar: Asegurar la continuidad del negocio mediante planes de recuperación que contemplen la restauración de datos, la reposición de sistemas afectados y una evaluación posterior para reforzar los controles frente a futuros intentos de phishing.

Diversos estudios destacan que el NIST CSF no solo ofrece una estructura flexible y escalable, sino que también impulsa la integración de tecnologías emergentes como la inteligencia artificial y el análisis de comportamiento para optimizar la detección y respuesta ante campañas de phishing avanzadas (Alshaikh et al., 2022; Alhassan & Abozinadah, 2023). No obstante, algunos expertos advierten que la rápida evolución de los ataques potenciados por

inteligencia artificial exige una adopción más ágil y dinámica de este marco, en especial dentro de organizaciones con recursos limitados.

En conclusión, el NIST CSF proporciona un enfoque integral que ayuda a las organizaciones a alinear sus procesos de seguridad con buenas prácticas internacionales, aumentando su capacidad para anticipar, contener y recuperarse de incidentes de phishing e ingeniería social.

ENISA (European Union Agency for Cybersecurity)

La Agencia de la Unión Europea para la Ciberseguridad (ENISA) cumple un rol fundamental en la detección de amenazas emergentes y en la elaboración de lineamientos estratégicos que apoyan tanto a los Estados miembros como a las organizaciones en el fortalecimiento de sus capacidades de prevención y respuesta frente a ataques cibernéticos. Entre sus publicaciones más relevantes se encuentra el Threat Landscape Report, el cual, de manera anual, examina las principales amenazas digitales e identifica al phishing y la ingeniería social como vectores de ataque prioritarios (ENISA, 2023).

De acuerdo con el informe ENISA Threat Landscape 2023, el phishing continúa siendo una de las amenazas más comunes en Europa, con un impacto particular en sectores críticos como la banca, salud y la administración pública. El informe resalta que la incorporación de técnicas de automatización e inteligencia artificial ha incrementado la dificultad para que tanto los usuarios como los sistemas de seguridad distingan entre comunicaciones legítimas y fraudulentas. Asimismo, se destaca el aumento de variantes como el spear phishing, dirigido a objetivos específicos, y el smishing, basado en mensajes SMS, lo que refleja la creciente diversificación de los canales utilizados por los atacantes.

En el ámbito organizacional, ENISA enfatiza la relevancia de implementar acciones como la sensibilización y capacitación de los empleados, la adopción de la autenticación multifactor (MFA), la utilización de sistemas de filtrado de correos electrónicos y la incorporación de marcos de gestión de riesgos que contemplen estas amenazas dentro de una estrategia integral de ciberseguridad (ENISA, 2023). De igual forma, sus lineamientos aconsejan realizar simulaciones periódicas de campañas de phishing, con el fin de evaluar y fortalecer de manera continua la resiliencia digital.

En conclusión, los informes y guías de ENISA se consolidan como una referencia clave tanto para organizaciones europeas como internacionales, ya que no solo brindan un análisis actualizado del panorama de amenazas, sino que también ofrecen recomendaciones prácticas, escalables y aplicables que permiten reducir los riesgos derivados del phishing y la ingeniería social.

MITRE ATT&CK

El marco MITRE ATT&CK (Adversarial Tactics, Techniques and Common Knowledge) se reconoce como una de las taxonomías más completas para caracterizar las acciones de los atacantes a lo largo del ciclo de intrusión. Creado por la corporación MITRE, este marco organiza y clasifica las tácticas, técnicas y procedimientos (TTPs) utilizados en los ciberataques, lo que brinda a las organizaciones una guía estructurada para identificar, mapear y mitigar amenazas de manera efectiva (MITRE, 2023).

En relación con el phishing y la ingeniería social, el marco MITRE ATT&CK adquiere gran relevancia al documentar de manera precisa las técnicas empleadas por los atacantes para obtener acceso inicial y comprometer sistemas:

1. T1566 – Phishing: hace referencia a campañas que envían correos electrónicos maliciosos con enlaces o archivos adjuntos diseñados para engañar al usuario, facilitando así la ejecución de código o el robo de credenciales.

2. T1598 – Spearphishing: consiste en ataques dirigidos a víctimas específicas mediante mensajes personalizados que, al explotar información contextual, aumentan significativamente la probabilidad de éxito.

3. T1656 – Phishing for Information: se refiere a intentos de recopilar datos confidenciales (como credenciales o números de identificación) sin necesidad de utilizar malware, basándose principalmente en la manipulación psicológica de la víctima.

La principal ventaja de MITRE ATT&CK radica en que ofrece un lenguaje común para investigadores, analistas y responsables de seguridad, facilitando la documentación de incidentes y la evaluación de los controles de defensa. Por ejemplo, al detectar que una organización ha sido afectada por T1566, es posible determinar rápidamente los vectores de ataque utilizados, identificar los controles que fallaron y establecer medidas para prevenir incidentes similares.

Además, este marco permite a las organizaciones diseñar simulaciones de ataque (red teaming) y evaluar su resiliencia frente a campañas de phishing e ingeniería social. Al comparar las defensas existentes con las técnicas registradas en ATT&CK, se obtiene mayor visibilidad sobre las brechas de seguridad y se facilita la priorización de inversiones en controles de protección, detección y respuesta (Moustafa et al., 2021).

En conclusión, MITRE ATT&CK no solo documenta las técnicas de phishing más comunes, sino que también constituye una herramienta práctica para fortalecer estrategias de ciberseguridad, alinear las defensas organizacionales con tácticas reales y mejorar la resiliencia frente a amenazas de ingeniería social.

ANSSI (Agencia Nacional de Seguridad de los Sistemas de Información – Francia)

Como complemento europeo a los estándares ISO/IEC 27000, la ANSSI ofrece directrices y buenas prácticas enfocadas en la gestión de vulnerabilidades, la prevención de ataques de ingeniería social y la respuesta a incidentes de seguridad (ANSSI, s.f.). Estas recomendaciones buscan reforzar la protección de los sistemas de información y fomentar un enfoque estructurado de prevención, detección y mitigación de amenazas dirigidas a los usuarios, como el phishing. Entre los lineamientos más destacados de ANSSI para enfrentar este tipo de ataques se incluyen:

1. Identificación de vectores de ataque y evaluación de riesgos asociados a correos electrónicos, mensajes y sitios web maliciosos.
2. Implementación de controles y medidas preventivas que reduzcan la exposición de los usuarios a intentos de engaño.
3. Establecimiento de procedimientos de respuesta rápida ante incidentes de phishing e ingeniería social.
4. Capacitación y concienciación de los usuarios para reconocer y reportar intentos de fraude digital.

La incorporación de ANSSI dentro del marco de seguridad complementa las normas ISO/IEC 27000, proporcionando un enfoque práctico de origen europeo que contribuye a fortalecer la resiliencia de los sistemas y a proteger la información frente a ataques de ingeniería social.

Revisión de Literatura y Estudios Previos

Estudios Académicos y Reportes Técnicos

Diversos estudios académicos y reportes técnicos resaltan el creciente impacto del phishing y otros ataques de ingeniería social sobre la seguridad de la información. El IBM Cost of a Data Breach Report (2024) indica que el phishing representa aproximadamente el 16 % de todas las brechas de datos a nivel global. De manera similar, el Verizon Data Breach Investigations Report (2023) señala que el 44 % de los incidentes de ingeniería social se originan mediante ataques de phishing. Complementando esta información, la ENISA (2023) identifica al phishing como una de las amenazas persistentes más importantes para las organizaciones tanto en Europa como a nivel mundial.

En América Latina, países como México, Brasil y Colombia han experimentado un aumento significativo en incidentes de phishing, representando cerca del 20 % de las brechas reportadas en la región (ENISA, 2023). Estos ataques no se limitan al correo electrónico, sino que también se ejecutan a través de mensajes SMS, llamadas telefónicas y redes sociales, lo que complica su detección y prevención (Verizon, 2023).

Estos hallazgos muestran que, a pesar de las políticas de seguridad implementadas por muchas organizaciones, el phishing continúa siendo una amenaza significativa, subrayando la importancia de estrategias efectivas de prevención y mitigación.

Casos Documentados de Incidentes

Los casos documentados evidencian la complejidad y el impacto real de los ataques de phishing:

1. Universidad de California (2023): Un ataque de phishing comprometió información personal de miles de empleados y estudiantes. Los atacantes enviaron correos

electrónicos simulando provenir de la administración, lo que resultó en una violación masiva de datos y llevó a la institución a reforzar sus medidas de seguridad (University of California, 2023).

2. Banco (2022): Un incidente comprometió las credenciales de varios clientes mediante técnicas de ingeniería social, provocando pérdidas financieras y aumento de quejas, lo que motivó la adopción de controles más robustos y capacitación de los usuarios (Banco X, 2022).

3. Mimecast (2021): La empresa sufrió un ataque que comprometió su software de correo electrónico, afectando tanto su reputación como la seguridad de sus clientes, lo que generó cambios en las políticas de seguridad de los clientes (Mimecast, 2021).

4. Instituciones de salud (2023): Se reportó un aumento en los ataques de phishing durante la pandemia, comprometiendo datos de pacientes y violando normativas HIPAA, lo que impulsó inversiones en soluciones de seguridad (Health Institutions Report, 2023).

5. Departamento de Justicia de EE. UU. (2022): funcionarios fueron víctimas de phishing mediante correos fraudulentos que aparentaban ser de otros departamentos, lo que llevó a la revisión de vulnerabilidades y a la implementación de nuevas medidas de autenticación (U.S. Department of Justice, 2022).

Casos de Éxito y Medidas de Mitigación Frente Al Phishing y la Ingeniería Social

La implementación de estrategias efectivas orientadas a la prevención y mitigación de ataques de phishing y otras modalidades de ingeniería social ha demostrado ser un pilar esencial para fortalecer la seguridad en las organizaciones. En este sentido, se exponen a continuación casos documentados y ejemplos representativos que muestran la eficacia de las medidas técnicas, organizacionales y de sensibilización.

Microsoft: adopción de Autenticación Multifactor (MFA)

Microsoft ha incorporado la autenticación multifactor (MFA) como una medida estándar en sus servicios, incluyendo Azure Active Directory y Office 365. Esta implementación ha permitido reducir de manera significativa la ocurrencia de incidentes de seguridad:

1. Eficacia de MFA: Un estudio realizado por Microsoft encontró que el 99.99% de las cuentas con MFA habilitada permanecieron seguras durante el período analizado, incluso en casos de filtración de credenciales. Además, se observó una disminución del 99.2% en el riesgo de compromiso en general y del 98.56% en situaciones de credenciales filtradas (Microsoft, 2020).

2. Adopción de MFA resistente al phishing: Microsoft ha logrado que el 92% de las cuentas de productividad de sus empleados utilicen métodos de autenticación resistentes al phishing, integrando MFA en cada etapa del ciclo de vida del empleado (*Seguridad de Microsoft*, 2024).

Google: Protección Proactiva contra Phishing

Google ha adoptado diversas medidas avanzadas con el objetivo de impedir intentos de phishing y reforzar la protección de sus usuarios:

1. Bloqueo de intentos de phishing: Google bloquea más de 100 millones de intentos de phishing cada día en sus plataformas, como Gmail y Google Workspace.

2. Alertas estratégicas: De manera trimestral, envía más de 12 000 alertas sobre campañas patrocinadas por gobiernos, contribuyendo a la protección de organizaciones y perfiles de alto riesgo.

3. Autenticación multifactor: Google recomienda encarecidamente la activación de la autenticación en dos pasos para sus usuarios, lo que ha demostrado ser una herramienta eficaz para prevenir accesos no autorizados (Google, 2020).

IBM: Simulacros Internos y Protección Multinivel

IBM implementó una estrategia integral para reducir los riesgos asociados al phishing, centrando sus esfuerzos en la concienciación de los usuarios finales y en la aplicación de mecanismos de protección multicapa:

1. Campañas de concienciación continua: Diseñados con contenidos ajustados a los diferentes perfiles laborales.
2. Simulacros regulares de phishing: Gestionados por el equipo de seguridad para medir las respuestas de los usuarios en entornos controlados.
3. MFA obligatoria en accesos a sistemas corporativos: Acceso a sistemas corporativos, correo electrónico, redes VPN y servicios en la nube.

Los resultados obtenidos fueron notables:

- Se alcanzó una reducción del 80 % en la interacción con correos electrónicos simulados de phishing en un periodo inferior a doce meses.
- El porcentaje de reportes de intentos sospechosos aumentó del 12 % al 66 %.
- Los tiempos de respuesta frente a incidentes se acortaron significativamente como consecuencia de la capacitación continua (IBM Security X-Force, 2020).

ANSSI (Agencia Nacional de Seguridad de los Sistemas de Información – Francia):

Directrices de Seguridad

La ANSSI ha desarrollado un conjunto de directrices diseñadas para asistir a las organizaciones en la protección frente a ataques de phishing y otras formas de ingeniería social:

1. Reglas preventivas: ANSSI ha establecido diez reglas básicas que las organizaciones pueden aplicar para protegerse contra ciberataques, incluyendo la implementación de medidas de seguridad en la infraestructura de correo electrónico y la capacitación de los usuarios.

2. Guía para sistemas de información saludables: ANSSI también ha publicado una guía con 42 medidas esenciales para mantener la seguridad de los sistemas de información, que abordan aspectos como la gestión de contraseñas y la protección contra malware (ANSSI, s.f.).

Otras Iniciativas Destacadas

1. Apple: Apple ha implementado medidas de seguridad como la autenticación en dos pasos para proteger las cuentas de los usuarios, lo que ha contribuido a reducir los incidentes de seguridad en sus plataformas (Apple, 2020).

2. PayPal: PayPal ha desarrollado sistemas avanzados de detección de fraudes y phishing, incluyendo el monitoreo en tiempo real de transacciones y la implementación de alertas de seguridad para los usuarios (PayPal, 2021).

3. Bancos Digitales: Instituciones financieras como Revolut y N26 han adoptado tecnologías de autenticación biométrica y análisis de comportamiento para detectar y prevenir actividades fraudulentas en sus plataformas (Revolut & N26, 2022).

Estos resultados destacan la relevancia de implementar políticas de seguridad, programas de concienciación y controles técnicos, como la autenticación multifactor y la monitorización de usuarios, para minimizar la exposición a ataques de phishing e ingeniería social. Asimismo, la combinación de medidas preventivas, capacitación continua del personal y la adopción de tecnologías avanzadas de detección no solo reduce la probabilidad de incidentes, sino que

también fortalece la resiliencia organizacional, protege la información crítica y mantiene la confianza de clientes, empleados y socios estratégicos.

En consecuencia, las estrategias de mitigación deben ser integrales, dinámicas y adaptadas al contexto específico de cada organización, considerando tanto la evolución de las amenazas como las mejores prácticas internacionales en ciberseguridad.

Evaluación del Impacto en la Resiliencia de los Sistemas Digitales

Las estrategias de prevención y mitigación de ataques de ingeniería social y phishing no se limitan a disminuir la probabilidad de incidentes, sino que también persiguen robustecer la resiliencia digital de las organizaciones. Esta resiliencia, definida como la capacidad para resistir, responder y recuperarse frente a ciberataques, constituye un eje fundamental en los marcos de ciberseguridad contemporáneos (NIST, 2018; ENISA, 2023).

Resistencia Frente a los Ataques

Medidas proactivas como la implementación de autenticación multifactor (MFA), la segmentación de redes, el uso de firewalls de última generación y el monitoreo en tiempo real refuerzan las barreras de acceso frente a los atacantes. De acuerdo con González y Rodríguez (2020), los mecanismos de detección temprana apoyados en inteligencia artificial posibilitan la identificación de patrones anómalos de comunicación, lo que permite actuar antes de que los sistemas críticos se vean comprometidos.

Capacidad de Recuperación

La existencia de planes de contingencia, copias de seguridad automatizadas y soluciones en la nube facilita que las organizaciones disminuyan el tiempo de inactividad posterior a un ataque. Según Ramírez y Martínez (2021), la realización periódica de simulaciones de incidentes

fortalece la capacidad institucional para recuperar datos y reanudar operaciones con eficacia, garantizando la continuidad incluso en contextos de crisis.

Mejora en la Capacidad de Respuesta

Las capacitaciones periódicas, los ejercicios de simulación de phishing y las evaluaciones posteriores a los incidentes fortalecen la preparación de los equipos de respuesta. De acuerdo con Álvarez y Díaz (2021), estas prácticas no solo facilitan una contención más rápida y efectiva de los ataques, sino que también proporcionan insumos valiosos para la actualización de políticas y protocolos de seguridad.

Evidencias en el Contexto Organizacional

Casos como los de Microsoft, Google, IBM y BBVA muestran que la combinación de medidas tecnológicas como la autenticación multifactor, la inteligencia artificial y la segmentación de redes junto con acciones organizacionales como la concienciación, los simulacros y los programas de formación generan avances concretos en la confidencialidad, integridad y disponibilidad de la información. Estos casos evidencian que la resiliencia digital no se fundamenta únicamente en las herramientas, sino también en una cultura organizacional comprometida con la seguridad (IBM, 2020; BBVA, 2021; Microsoft, 2020; Google, 2022).

Adaptabilidad de los Estándares y Marcos en el Contexto Organizacional

El análisis realizado evidencia que los marcos de referencia y estándares internacionales, entre ellos ISO/IEC 27001, NIST CSF, ENISA y MITRE ATT&CK, constituyen una base sólida para la gestión de riesgos vinculados al phishing y a la ingeniería social. Sin embargo, su nivel de efectividad está condicionado por la capacidad de cada organización para ajustarlos a su propio contexto, teniendo en cuenta aspectos como el sector al que pertenece, su tamaño y el

grado de madurez alcanzado en materia de ciberseguridad (ISO/IEC, 2022; NIST, 2018; ENISA, 2023; MITRE, 2023).

En el ámbito de la prevención, los estándares ISO y el NIST CSF ofrecen directrices precisas relacionadas con controles de acceso, autenticación multifactor, formación del personal y gestión de incidentes. La efectividad de estas medidas se evidencia en experiencias como la de Microsoft, que logró disminuir de manera notable los casos de cuentas comprometidas gracias a la implementación generalizada de MFA, o la de Google, que logra frenar millones de intentos de phishing mediante soluciones de detección impulsadas por inteligencia artificial. (Google, 2020).

En lo referente a la detección y respuesta, el marco MITRE ATT&CK ofrece un valor significativo al permitir a los equipos de ciberseguridad asociar técnicas como T1566 (Phishing) o T1598 (Spearphishing), lo que facilita la detección temprana de posibles vectores de ataque y el desarrollo de controles específicos (MITRE, 2023). Asimismo, su integración con prácticas como la red teaming y las simulaciones de phishing, promovidas por ENISA (2023), contribuye a fortalecer la resiliencia organizacional al preparar tanto a los usuarios como a los equipos de seguridad frente a escenarios de amenaza reales.

Sin embargo, la evidencia de incidentes registrados demuestra que la implementación de marcos y estándares, por sí sola, no asegura la eliminación total del riesgo. Casos como los ataques a la Universidad de California (2023) o al Departamento de Justicia de EE. UU. (2022) ponen de manifiesto que, aun contando con políticas de seguridad establecidas, las organizaciones pueden seguir siendo vulnerables si no actualizan sus controles, descuidan la promoción de una cultura de concienciación constante o dejan de incorporar tecnologías emergentes como la analítica avanzada y la inteligencia artificial.

En consecuencia, la efectividad de los marcos de referencia no depende únicamente de su adopción formal, sino de su incorporación de manera dinámica y contextualizada en la estrategia de la organización. Esto requiere articular los lineamientos internacionales con prácticas ajustadas al sector, llevar a cabo simulaciones de forma periódica y promover la cooperación entre los equipos técnicos y los usuarios finales. Únicamente mediante este enfoque integral es posible reducir el impacto del phishing y la ingeniería social, al tiempo que se refuerza la resiliencia digital de las organizaciones.

Conclusiones del Capítulo

El análisis presentado en este capítulo muestra que los ataques de phishing y la ingeniería social constituyen amenazas importantes para la seguridad de la información en organizaciones de cualquier tamaño o sector. La revisión de estándares internacionales, marcos de referencia y guías regionales como ISO/IEC 27001, 27002, 27035 y 27701, NIST CSF, ENISA, MITRE ATT&CK y ANSSI evidencia que la implementación de medidas técnicas, organizacionales y de concienciación resulta esencial para mitigar los riesgos y fortalecer la resiliencia digital.

La literatura académica y los informes técnicos consultados evidencian la persistencia de estas amenazas, mientras que los casos documentados y las experiencias exitosas de empresas como Microsoft, Google, IBM y BBVA demuestran que la integración de controles tecnológicos, políticas internas, simulacros y programas de formación continua contribuye a reducir de manera significativa el impacto de los ataques, así como a mejorar la capacidad de respuesta, recuperación y continuidad operativa de las organizaciones.

De igual manera, se observa que la eficacia de los marcos y estándares está condicionada por su adecuación al contexto particular de cada organización, teniendo en cuenta aspectos como el sector, el tamaño y el nivel de madurez en ciberseguridad. La simple adopción formal de

controles no asegura la eliminación completa del riesgo; se requiere un enfoque integral y dinámico que combine los lineamientos internacionales con prácticas internas, tecnologías emergentes y una cultura de concienciación continua.

En resumen, este capítulo ofrece una visión integral sobre cómo los marcos de referencia, la evidencia empírica y las buenas prácticas organizacionales se combinan para reducir los riesgos asociados al phishing y la ingeniería social, reforzando la resiliencia digital. Estos hallazgos constituyen la base para el análisis posterior de estrategias de protección específicas y de su aplicabilidad en contextos organizacionales particulares, que se abordará en el siguiente capítulo.

Propuestas de Optimización en la Defensa Contra Ataques de Phishing e Ingeniería Social

En la actualidad, las amenazas cibernéticas como el phishing y la ingeniería social figuran entre las más frecuentes y riesgosas en el ámbito de la ciberseguridad. Aunque se han implementado medidas técnicas, humanas y organizacionales para prevenirlas, los ciberdelincuentes han sofisticado sus tácticas, explotando vulnerabilidades humanas y fallas tecnológicas. De acuerdo con Chen, Martínez y Rodríguez (2024), incluso en organizaciones con políticas definidas y mecanismos de protección establecidos, los usuarios siguen siendo vulnerables ante correos fraudulentos, lo que resalta la importancia de una actualización continua y de un enfoque más amplio.

En Colombia, el impacto de estos ataques ha aumentado de forma considerable. Durante 2024 se reportaron más de 36 mil millones de intentos de ciberataques, con el phishing como una de las modalidades más comunes, especialmente en el sector salud (Alcaldía de Cali, 2025). La rápida digitalización de los servicios públicos y privados ha incrementado la exposición de los ciudadanos a diversas formas de fraude digital, mientras que las pequeñas y medianas empresas, debido a sus limitaciones de recursos, continúan siendo altamente vulnerables. Este panorama evidencia la urgencia de reforzar las políticas nacionales de ciberseguridad y de ajustar las estrategias internacionales a las particularidades del contexto local.

En este contexto, el presente capítulo realiza un análisis crítico de las estrategias utilizadas para prevenir y mitigar los ataques de phishing e ingeniería social, con el propósito de reconocer sus limitaciones y plantear mejoras factibles. La propuesta se apoya en investigaciones recientes que abordan tanto los componentes técnicos como los factores humanos de la ciberseguridad (Hove, 2023). Del mismo modo, se incluyen indicadores de madurez y de medición de impacto que permiten valorar objetivamente la eficacia de las estrategias aplicadas.

Con este enfoque, se pretende ofrecer recomendaciones ajustadas al entorno nacional y alineadas con las mejores prácticas internacionales, favoreciendo el fortalecimiento de una cultura de seguridad digital más resiliente, sostenible y eficiente.

Relevancia de la Ingeniería Social en la Ciberseguridad

Las técnicas de ingeniería social constituyen una de las principales amenazas para la ciberseguridad, debido a que aprovechan la vulnerabilidad más difícil de controlar: el factor humano. Estas técnicas se basan en la manipulación psicológica, explotando emociones y debilidades conductuales para obtener información confidencial, acceder a sistemas o instalar malware (Hahnagy, 2021).

Entre los factores que explican la relevancia de la ingeniería social se encuentran:

1. Aprovechamiento de vulnerabilidades humanas: los atacantes se apoyan en la confianza, el temor o la sensación de urgencia para inducir errores en los usuarios.
2. Fácil ejecución y alto impacto: en comparación con los ataques técnicos, requieren menos recursos, pero pueden ocasionar pérdidas de datos o fraudes financieros de gran magnitud (Abawajy, 2019).
3. Bajo costo para el atacante: al no depender de herramientas tecnológicas avanzadas, la manipulación psicológica se convierte en una opción accesible para cualquier ciberdelincuente.
4. Dificil detección: estos ataques suelen presentarse como interacciones habituales, lo que facilita que pasen inadvertidos para los sistemas de seguridad tradicionales (Hahnagy, 2021).
5. Riesgo empresarial: un solo error humano puede comprometer redes completas, provocar filtraciones masivas y afectar la reputación organizacional.

6. Adaptabilidad a diferentes entornos: pueden manifestarse a través de correos electrónicos (phishing), llamadas telefónicas (vishing), mensajes de texto (smishing) o interacciones presenciales (tailgating).

En este sentido, la ingeniería social representa una amenaza directa para la resiliencia digital de las organizaciones, lo que hace imprescindible reforzar los programas de sensibilización, la capacitación permanente y la implementación de políticas de seguridad sólidas (Rincón Núñez, 2023).

Estrategias Actuales de Prevención y Mitigación

Estrategias Técnicas

Autenticación Multifactor (MFA/2FA). la autenticación multifactor (MFA/2FA) se considera uno de los métodos más eficaces para fortalecer la seguridad en los accesos, pues requiere dos o más verificaciones de identidad antes de conceder autorización a un usuario. Usualmente combina algo que el usuario sabe (contraseña), algo que posee (token o aplicación móvil) y algo que es (huella digital o reconocimiento facial). Su adopción disminuye de manera considerable el riesgo de accesos indebidos, incluso si las credenciales han sido vulneradas. En Colombia, sectores como el financiero y el de la salud han incorporado progresivamente el MFA como medida obligatoria para proteger información sensible (Castillo Rubiano, 2019). No obstante, su implementación aún no es generalizada en pequeñas y medianas empresas, principalmente por limitaciones presupuestales y falta de conocimiento.

Filtros Antiphishing, Antivirus y Sandboxing. la implementación de filtros de correo electrónico, soluciones antivirus y técnicas de sandboxing constituye una medida esencial para identificar y detener amenazas antes de que lleguen al usuario final. Los filtros antiphishing examinan encabezados, enlaces y patrones de redacción en los correos, permitiendo detectar

intentos de fraude; mientras que los antivirus y el sandboxing aíslan y analizan archivos sospechosos en un entorno controlado, evitando que afecten los sistemas de producción. En Colombia, estas herramientas son empleadas principalmente por entidades financieras y aseguradoras como parte de sus mecanismos de defensa perimetral, lo que contribuye a mitigar los riesgos vinculados al fraude digital (Rincón Núñez, 2023).

Firewalls y Controles de Acceso. los firewalls constituyen la primera capa de defensa en una infraestructura de red, ya que regulan el tráfico entrante y saliente de acuerdo con políticas previamente establecidas. Cuando se combinan con mecanismos de control de acceso, contribuyen a limitar la exposición de información sensible y a segmentar los recursos críticos de las organizaciones. De acuerdo con Bustamante y Cano (2015), la implementación de firewalls de nueva generación (NGFW) en entidades públicas y privadas en Colombia ha resultado fundamental para contrarrestar ataques dirigidos y disminuir la superficie de exposición frente a intentos de intrusión. Sin embargo, se enfatiza que estas herramientas requieren de una adecuada gestión de configuraciones y de auditorías periódicas para garantizar su efectividad.

Inteligencia Artificial y Análisis de Comportamiento. la implementación de inteligencia artificial (IA) y técnicas de aprendizaje automático en el ámbito de la ciberseguridad ha revolucionado las capacidades de detección de amenazas. Estas tecnologías procesan millones de eventos en tiempo real, logrando identificar anomalías y patrones de comportamiento inusuales que los métodos tradicionales podrían no detectar. Según Fortinet (2024), la IA facilita la identificación de intentos de phishing dirigidos y de ataques de ingeniería social altamente personalizados. En Colombia, la adopción de soluciones basadas en IA se concentra principalmente en entidades financieras y gubernamentales, con el objetivo de reducir los tiempos de respuesta frente a incidentes y fortalecer la resiliencia de sus sistemas críticos.

Estrategias Humanas

Campañas de Concientización. las campañas de concientización constituyen un pilar fundamental para disminuir la vulnerabilidad humana frente a ataques de phishing e ingeniería social. Su propósito es educar a los usuarios acerca de las tácticas más habituales empleadas por los atacantes, al mismo tiempo que fomentan prácticas seguras en el uso del correo electrónico, redes sociales y plataformas corporativas. En Colombia, instituciones como el Centro Cibernético Policial (CCP) han desarrollado campañas masivas dirigidas tanto a ciudadanos como a empresas, con el fin de advertir sobre fraudes digitales y fortalecer la cultura de ciberseguridad (Rincón Núñez, 2023). No obstante, aunque estas iniciativas generan un efecto positivo en el corto plazo, su impacto se reduce si no se implementan de manera continua y con actualizaciones frente a las nuevas modalidades de ataque (Chen, Martínez & Rodríguez, 2024).

Simulacros de Phishing. los simulacros de phishing representan una estrategia práctica para medir el grado de preparación de los empleados frente a intentos de fraude. Estos ejercicios recrean escenarios de ataque reales, como correos electrónicos con enlaces maliciosos, con el fin de evaluar la capacidad de los usuarios para detectar y reportar amenazas. De acuerdo con Castillo Rubiano (2019), algunas organizaciones en Colombia que implementaron simulacros de manera trimestral consiguieron disminuir hasta en un 60 % el número de empleados que caían en pruebas de phishing, lo que evidencia la efectividad de esta práctica. Sin embargo, investigaciones recientes destacan que el éxito no radica únicamente en la ejecución de los simulacros, sino en complementarlos con retroalimentación inmediata y programas de formación adicionales (Hove, 2023). De lo contrario, estos ejercicios podrían generar desconfianza o incluso fatiga en los usuarios.

Educación y Capacitación. La formación continua en ciberseguridad es fundamental para crear una primera línea de defensa efectiva contra ataques basados en ingeniería social. La capacitación debe incluir desde conceptos básicos, como la identificación de enlaces sospechosos, hasta entrenamientos especializados en respuesta a incidentes para perfiles técnicos. En Colombia, algunas universidades y empresas han incorporado diplomados y cursos cortos en ciberseguridad, orientados tanto a profesionales de TI como a usuarios no técnicos (Bustamante & Cano, 2015). Además, la inclusión de la educación digital en niveles escolares y universitarios resulta clave para preparar a las nuevas generaciones frente a las amenazas emergentes (Hadnagy, 2021). La falta de conocimiento y entrenamiento es, de hecho, uno de los principales factores que incrementa la efectividad de los ataques de ingeniería social en organizaciones de todos los tamaños (Abawajy, 2019).

Estrategias Organizacionales

Normativas y Políticas Internas de Seguridad. las políticas internas de seguridad constituyen el fundamento para establecer directrices claras en la gestión de la información y en la respuesta frente a incidentes. Estas normativas determinan responsabilidades, procedimientos y controles que los empleados deben seguir para asegurar la protección de los datos y de los sistemas. De acuerdo con Rincón Núñez (2023), en Colombia varias organizaciones han implementado políticas alineadas con estándares internacionales como la ISO/IEC 27001, con el objetivo de reforzar su defensa frente al phishing y la ingeniería social. Sin embargo, un reto persistente es que muchas pequeñas y medianas empresas aún carecen de normativas formalizadas, ya sea por restricciones presupuestales o por desconocimiento. La falta de políticas definidas aumenta la exposición al riesgo y reduce la capacidad de las organizaciones para responder adecuadamente ante incidentes de seguridad.

Planes de Respuesta a Incidentes. el diseño e implementación de planes de respuesta a incidentes resulta fundamental para garantizar que una organización pueda reaccionar de manera ágil y efectiva ante ataques cibernéticos. Dichos planes suelen contemplar protocolos de detección, contención, erradicación y recuperación, además de establecer roles y responsabilidades en cada etapa del proceso (NIST, 2020). En Colombia, tanto entidades financieras como gubernamentales han creado Centros de Operaciones de Seguridad (SOC) encargados de ejecutar planes de respuesta frente a incidentes como intentos de phishing y ataques de ransomware (Castillo Rubiano, 2019). No obstante, investigaciones recientes demuestran que la efectividad de estos planes depende en gran medida de la capacitación continua del personal y de la realización de simulacros regulares, ya que la teoría por sí sola no basta para enfrentar situaciones reales (Hove, 2023).

Monitoreo y Auditorías Continuas. el monitoreo y las auditorías de seguridad permiten a las organizaciones identificar de forma temprana actividades sospechosas y asegurar el cumplimiento de sus políticas internas. Estas prácticas abarcan la supervisión del tráfico de red, la verificación de accesos a sistemas críticos y la ejecución de pruebas de penetración periódicas. De acuerdo con Bustamante y Cano (2015), en Colombia las auditorías internas y externas han sido clave para fortalecer la madurez en materia de seguridad digital en sectores estratégicos como el bancario y el de la salud. Asimismo, estas auditorías contribuyen al cumplimiento de normativas de protección de datos, como la Ley 1581 de 2012, que exige a las empresas garantizar la seguridad de la información personal. La ausencia de monitoreo y evaluación constante incrementa el riesgo de que ataques de phishing e ingeniería social pasen inadvertidos y ocasionen consecuencias críticas para las organizaciones.

Evaluación del Impacto de las Estrategias Actuales

La implementación de estrategias de prevención y mitigación frente a ataques de phishing e ingeniería social ha mostrado resultados positivos en diversos contextos, aunque con diferencias notables según el sector y el tipo de organización. Dichas estrategias pueden dividirse en proactivas como la autenticación multifactor (MFA), el cifrado de información, los simulacros de phishing y la capacitación continua y reactivas, como los planes de respuesta a incidentes, la aplicación de parches de seguridad o la realización de auditorías posteriores a un ataque. De acuerdo con Chen, Martínez y Rodríguez (2024), las medidas proactivas suelen ser más eficaces a largo plazo, ya que disminuyen la probabilidad de éxito de un ataque, mientras que las reactivas resultan valiosas para contener y mitigar los daños una vez que la intrusión ha ocurrido.

En el contexto colombiano, la aplicación de estas estrategias ha tenido un impacto notable en sectores críticos como el financiero y el de la salud. En el ámbito sanitario, varias instituciones hospitalarias han informado una disminución considerable de incidentes de phishing gracias a la incorporación de filtros antiphishing y a la capacitación del personal administrativo (Rincón Núñez, 2023). Por su parte, en el sector financiero, la implementación del MFA y la inversión en soluciones de inteligencia artificial han fortalecido la detección temprana de fraudes electrónicos (Castillo Rubiano, 2019). No obstante, en el caso de las pequeñas y medianas empresas (pymes), las restricciones presupuestales y la falta de personal especializado en seguridad han limitado la adopción sistemática de estas medidas, lo que las mantiene como uno de los sectores más expuestos a ataques de ingeniería social (Bustamante & Cano, 2015).

A pesar de los avances, persisten diversas limitaciones en la aplicación de estas medidas. En primer lugar, la falta de continuidad, ya que muchas campañas de concientización y programas de capacitación se ejecutan de forma aislada y sin un plan sostenido, lo que disminuye

su efectividad (Hove, 2023). En segundo lugar, la inversión tecnológica continúa siendo insuficiente, particularmente en pymes y entidades públicas que dependen de recursos limitados. Por último, la capacidad de adaptación frente a nuevas tácticas de los atacantes constituye un reto permanente, dado que el phishing y la ingeniería social evolucionan con rapidez mediante el uso de inteligencia artificial para elaborar mensajes más persuasivos y difíciles de detectar (Hahnagy, 2021).

Indicadores de Medición

Para evaluar objetivamente el impacto de las estrategias implementadas, se han establecido indicadores clave de ciberseguridad fundamentados en estándares internacionales como la ISO/IEC 27001 y la ISO/IEC 27004 (ISO, 2022), así como en el NIST Cybersecurity Framework (NIST, 2020). Los resultados obtenidos al comparar la situación previa y posterior a la adopción de estas medidas evidencian avances significativos:

Tabla 1*Indicadores Clave para la Evaluación del Impacto de las Estrategias de Prevención y**Mitigación*

Indicador	Descripción	Antes de estrategias	después de estrategias	Cambio (o%)
Incidentes de phishing reportados (mensual)	Número promedio de eventos de phishing identificados y reportados en un mes. Este indicador refleja la frecuencia de intentos de suplantación.	25	7	-72.0%
Tiempo medio de respuesta a incidentes (horas)	Tiempo promedio que tarda el equipo de seguridad en detectar, contener y mitigar un ataque desde que se identifica. Mide eficiencia operativa.	48	12	-75.0%
Empleados que caen en simulacros de phishing (%)	Porcentaje de empleados que interactúan con correos simulados de phishing, indicando su vulnerabilidad ante ataques reales.	40%	10%	-75.0%
Disponibilidad del sistema en eventos críticos (%)	Porcentaje de tiempo que los sistemas estuvieron operativos y accesibles durante eventos cibernéticos. Refleja resiliencia técnica.	85%	85%	+15.3%

Nivel de conocimiento sobre amenazas (puntuación /100)	Puntuación promedio obtenida por los empleados en pruebas de conocimiento sobre amenazas de ingeniería social y buenas prácticas de seguridad.	60	90	+50.0%
--	--	----	----	--------

Nota. La Tabla 1 expone una comparación de los principales indicadores antes y después de la implementación de las estrategias de prevención y mitigación frente a ataques de phishing e ingeniería social. Los valores registrados provienen de fuentes internas y de mediciones realizadas en dos periodos: el previo y el posterior a la intervención. Para cada indicador se especificaron las fuentes utilizadas, los métodos de cálculo aplicados y la dimensión de análisis correspondiente.

Incidentes de phishing reportados (mensual): hace referencia al número de eventos verificados como phishing dentro de los sistemas de monitoreo y gestión de incidentes (SIEM, correos bloqueados y reportes de usuarios). La reducción de 25 a 7 incidentes se determinó mediante la aplicación de la fórmula de variación porcentual: $((\text{valorfinal} - \text{valorinicial}) / \text{valorinicial}) \times 100$, lo que permitió establecer una disminución del 72 %. Este indicador actúa como medida directa de la efectividad técnica de los controles implementados, al evidenciar que menos ataques logran materializarse.

Tiempo medio de respuesta a incidentes (horas): se determinó a partir de los registros de la mesa de ayuda y del equipo de respuesta a incidentes, considerando el promedio de horas transcurridas desde la detección hasta la contención. La reducción de 48 h a 12 h representa una mejora del 75 %. Este indicador constituye una evidencia de la capacidad organizacional para la contención y recuperación, ya que permite valorar en qué medida los planes de respuesta fortalecen efectivamente la resiliencia digital.

Empleados que caen en simulacros de phishing (%): corresponde a los resultados obtenidos en las campañas de simulación de phishing dirigidas a la totalidad del personal. El cálculo se realizó dividiendo el número de usuarios que interactuaron con enlaces o ingresaron credenciales falsas entre el total de participantes. La disminución observada, del 40 % al 10 %, equivale a una reducción del 75 %. Este indicador evalúa el impacto en el comportamiento humano, evidenciando cómo la capacitación contribuye a disminuir la vulnerabilidad del personal, considerado el eslabón más explotado por los atacantes.

Disponibilidad de sistemas críticos (%): se obtuvo mediante herramientas de monitorización (registros de *uptime*), calculando el porcentaje de tiempo en que los sistemas permanecieron operativos durante incidentes relevantes. El aumento de 85 % a 98 % evidencia una mejora en la continuidad operativa. Este indicador funciona como un reflejo del impacto de las estrategias en la resiliencia técnica, al demostrar que la infraestructura mantiene su estabilidad incluso frente a intentos de ataque.

Nivel de conocimiento de los usuarios: se evaluó a través de pruebas estandarizadas aplicadas antes y después de las sesiones de capacitación, utilizando una escala de 0 a 100. El incremento de 60 a 90 puntos refleja un avance del 50 %. Este indicador actúa como prueba del aprendizaje adquirido, lo que complementa los resultados de los simulacros y demuestra que el conocimiento se traduce en prácticas más seguras.

En conclusión, estos indicadores no solo muestran una variación numérica, sino que actúan como evidencias específicas del impacto de las estrategias. los indicadores técnicos evidencian la reducción de riesgos y la mejora en la disponibilidad de los sistemas, los indicadores humanos reflejan la disminución de conductas vulnerables y el incremento en el nivel de concienciación, y los indicadores organizacionales muestran la capacidad de respuesta y

recuperación frente a incidentes. Al estar alineados con marcos internacionales como ISO/IEC 27004 (medición de la seguridad de la información) y ISO/IEC 27035 (gestión de incidentes), permiten evaluar de manera integral y verificable la resiliencia digital alcanzada tras la aplicación de las medidas. Elaboración propia, construida a partir de los lineamientos de medición de seguridad establecidos en la ISO/IEC 27004:2016 y el NIST Cybersecurity Framework, y de la evidencia empírica reportada en Chen et al. (2024) y Rincón Núñez (2023).

Tabla 2

Indicadores para la Evaluación del Impacto de las Estrategias de Mitigación de Ataques de Ingeniería Social y Phishing

Indicador	Descripción	Categoría	Relación con el Objetivo
Tasa de reporte de correos sospechosos por parte de usuarios (%)	Porcentaje de usuarios que identifican y reportan intentos de phishing al equipo de seguridad.	Concienciación y prevención	Refleja si los usuarios están más alerta y activos en la detección de amenazas.
Número de accesos no autorizados bloqueados por MFA o control de acceso	Cantidad de accesos fallidos detenidos por sistemas de autenticación multifactor o control de acceso.	Protección de datos	Demuestra la efectividad de los controles de acceso frente a ataques de suplantación.
Tiempo promedio de respuesta a incidentes (MTTR)	Promedio de tiempo que tarda el equipo de TI en contener y resolver un incidente desde su detección.	Resiliencia digital	Mide la capacidad operativa de la organización para contener ataques sociales.
Tasa de éxito en simulacros de phishing	Porcentaje de empleados que superan simulacros de	Formación del personal	Evalúa la efectividad directa de las estrategias

Indicador	Descripción	Categoría	Relación con el Objetivo
después de la formación (%)	phishing luego de recibir formación en ciberseguridad.		educativas frente al phishing.
Número de incidentes recurrentes por ingeniería social	Número de ataques de ingeniería social que logran repetirse sobre los mismos usuarios o áreas vulnerables.	Prevención continua	Permite identificar persistencia de vulnerabilidades humanas.
Porcentaje de sistemas críticos con actualizaciones de seguridad aplicadas	Porcentaje de sistemas clave que cuentan con parches de seguridad y actualizaciones aplicadas correctamente.	Resiliencia técnica	Evalúa la postura técnica frente a amenazas basadas en ingeniería social.
Índice de cumplimiento de políticas internas de ciberseguridad.	Nivel de cumplimiento registrado durante auditorías sobre políticas y normas internas de ciberseguridad.	Madurez organizacional.	Determina el grado de adopción de normas de seguridad en todos los niveles.

Nota. La tabla 2 integra un conjunto de métricas que complementan a los indicadores principales y posibilitan una valoración más detallada de la efectividad de las medidas implementadas.

Cada indicador fue elaborado a partir de fuentes específicas de información, lo que garantiza su validez en el proceso de medición:

Tasa de reporte de correos sospechosos por parte de los usuarios (%): se calcula dividiendo el número de reportes efectuados por los empleados entre el total de correos simulados o clasificados como sospechosos. Este indicador funciona como una medida del nivel

de concienciación del personal, en tanto refleja el grado de participación activa de los usuarios en la detección temprana de posibles amenazas.

Número de accesos no autorizados bloqueados por MFA o controles de acceso: se obtiene a partir de los registros de autenticación y de intentos fallidos de ingreso. Cada intento bloqueado corresponde a un ataque frustrado, por lo que este indicador constituye una evidencia de la eficacia de los controles técnicos de protección de datos y de su impacto en la reducción del riesgo de suplantación de identidad.

Tiempo promedio de respuesta a incidentes (MTTR): se determina a partir del promedio de horas transcurridas entre la detección de un incidente y su contención. Este indicador constituye una medida de la resiliencia digital y de la capacidad organizacional de reacción, en tanto una disminución en el tiempo evidencia el nivel de preparación y eficacia del equipo de respuesta.

Tasa de éxito en simulacros de phishing después de la formación (%): se calcula a partir del porcentaje de usuarios que identifican correctamente y reportan los intentos simulados en campañas realizadas tras las actividades de capacitación. Este indicador constituye una medida directa de la efectividad de la formación, al evidenciar que el conocimiento adquirido se traduce en la adopción de prácticas más seguras.

Número de incidentes recurrentes por ingeniería social: corresponde al conteo de casos en los que ataques de características similares logran repetirse sobre los mismos usuarios o áreas específicas. Este indicador permite identificar vulnerabilidades humanas persistentes y constituye una medida para determinar si las estrategias de prevención requieren ser reforzadas o ajustadas.

Porcentaje de sistemas críticos con actualizaciones aplicadas: se obtiene dividiendo el número de sistemas actualizados entre el total de sistemas considerados críticos. Este indicador

funciona como una medida de la resiliencia técnica de la infraestructura, en tanto un mayor porcentaje implica una reducción de la superficie de exposición frente a posibles ataques.

Índice de cumplimiento de políticas internas de ciberseguridad: se deriva de los resultados obtenidos en auditorías internas o externas respecto a las políticas vigentes. Este indicador refleja el nivel de madurez organizacional, al evidenciar el grado de adopción de la cultura de seguridad en los diferentes niveles de la entidad.

En conclusión, los indicadores de la Tabla 2 no solo aportan valores cuantitativos, sino que constituyen evidencias del impacto real de las estrategias implementadas. Los indicadores técnicos ponen de manifiesto la solidez de los controles y la resiliencia de la infraestructura; los indicadores humanos evidencian los avances en concienciación y formación del personal; y los indicadores organizacionales permiten valorar tanto la capacidad de respuesta como el nivel de cumplimiento normativo. De esta manera, la medición realizada ofrece una perspectiva integral y verificable de la efectividad de las estrategias de mitigación aplicadas. Adaptado de NIST SP 800-61 Rev. 3 (NIST, 2025), ISO/IEC 27001:2022 (ISO, 2022), ENISA Threat Landscape 2024 (ENISA, 2024), Meyer et al. (2023) y Scytale (2024).

Estrategias Emergentes y Tecnológicas de Apoyo

La evolución constante de los ataques de phishing e ingeniería social ha impulsado la adopción de tecnologías emergentes orientadas a fortalecer las capacidades de prevención, detección y respuesta en ciberseguridad. Estas soluciones no reemplazan las estrategias tradicionales, sino que las complementan, generando un marco más robusto de resiliencia digital en las organizaciones. A continuación, se presentan algunas de las principales tendencias y herramientas vinculadas con este ámbito.

Inteligencia Artificial y Aprendizaje Automático (IA/ML)

El uso de algoritmos de inteligencia artificial (IA) constituye una de las innovaciones más relevantes en la detección de amenazas, ya que permite identificar patrones anómalos en grandes volúmenes de datos y reconocer intentos de phishing incluso cuando no coinciden con firmas previamente registradas. Estas tecnologías posibilitan el análisis de comportamiento de los usuarios, el filtrado avanzado de correos electrónicos y la automatización de respuestas inmediatas frente a incidentes. Soluciones como FortiNDR y Cortex XDR evidencian el potencial del aprendizaje automático, al procesar millones de eventos en tiempo real, reducir significativamente los tiempos de detección y mejorar la eficacia de la defensa organizacional (Bustamante & Cano, 2015; ISO, 2022; NIST, 2020).

1. Herramientas de Google: Diversas plataformas han incorporado estrategias proactivas de protección basadas en IA. Entre ellas destacan:
2. Detección en tiempo real en Gmail: que bloquea correos de phishing y malware antes de llegar al usuario final.
3. Safe Browsing: integrado en Chrome y otros navegadores, que advierte sobre sitios maliciosos conocidos.
4. Password Checkup: que alerta a los usuarios si sus credenciales se han visto comprometidas en filtraciones de datos.
5. Autenticación en dos pasos (2SV) y llaves de seguridad: como parte del Programa de Protección Avanzada de Google, que refuerzan la seguridad de usuarios con mayor riesgo (Google, 2023).

6. Tecnologías emergentes: Además de la inteligencia artificial, otras tendencias emergentes están adquiriendo relevancia en la protección frente a ataques de phishing e ingeniería social, contribuyendo a fortalecer la resiliencia digital de las organizaciones.

7. Zero Trust Security (ZTA): modelo de confianza cero que elimina la idea de “red interna segura”, exigiendo verificaciones continuas de identidad y contexto antes de otorgar acceso (NIST SP 800-207, 2020).

8. Biometría avanzada: uso de autenticación mediante huellas dactilares, reconocimiento facial o patrones de voz, que complementan la MFA tradicional (Chen et al., 2024).

9. Blockchain en protección de datos: su aplicación en la gestión de identidades digitales y en registros inmutables garantiza mayor transparencia y reduce riesgos de manipulación o fraude en transacciones críticas (Hove, 2023).

En conjunto, estas estrategias emergentes fortalecen la protección frente a ataques de phishing e ingeniería social, al ofrecer soluciones que integran innovación tecnológica y robustez operativa. Su implementación, combinada con programas de concienciación y la alineación con marcos normativos internacionales, contribuye al desarrollo de una cultura de ciberseguridad resiliente y adaptable, capaz de enfrentar amenazas que evolucionan constantemente.

Propuestas de Mejora

La revisión de las estrategias actuales evidencia avances importantes, pero también limitaciones que requieren ajustes significativos para incrementar la resiliencia digital de las organizaciones. En este sentido, se plantean las siguientes propuestas de mejora, que combinan medidas técnicas, humanas y organizacionales, alineadas con marcos internacionales como ISO/IEC 27001 y el NIST Cybersecurity Framework.

Fortalecimiento de la Autenticación Multifactor (MFA)

Aunque la autenticación de dos factores ha ganado popularidad, su adopción sigue siendo limitada en sectores críticos como el financiero, sanitario y gubernamental. Por ello, se recomienda establecer la obligatoriedad del MFA a través de normativas nacionales, asegurando que todas las entidades que gestionan información sensible implementen este mecanismo. Investigaciones confirman que el MFA disminuye de forma significativa los accesos no autorizados, incluso en casos de filtración de credenciales (Microsoft, 2022). De igual manera, se sugiere realizar auditorías periódicas que verifiquen su cumplimiento efectivo, evitando que se reduzca a una medida meramente simbólica.

Integración de Inteligencia Artificial en la Detección Temprana

La inteligencia artificial (IA) y el aprendizaje automático (ML) potencian la detección de patrones anómalos en tiempo real. Soluciones como los SIEM (Splunk, IBM QRadar) y los centros de operaciones de seguridad (SOC) ya incorporan IA para correlacionar eventos y automatizar la respuesta frente a incidentes. Implementar estas tecnologías en Colombia contribuiría a reforzar la defensa contra campañas de phishing y ataques de ingeniería social, disminuyendo el tiempo promedio de detección y contención (Gartner, 2023; Palo Alto Networks, 2024).

Programas de Concienciación y Formación Continua

El factor humano continúa siendo el punto más vulnerable en materia de ciberseguridad. Por ello, se sugiere fortalecer programas de capacitación permanente que comiencen desde la etapa escolar y universitaria, y se proyecten hacia el entorno empresarial. Según ENISA (2022), las formaciones periódicas combinadas con simulacros de phishing pueden disminuir hasta en un 70% la efectividad de los ataques. Asimismo, la inclusión de metodologías basadas en la

gamificación y actividades prácticas favorece tanto el aprendizaje como la retención del conocimiento.

Políticas Internas Robustas y Revisiones Periódicas

Las organizaciones requieren manuales internos de ciberseguridad que definan roles, responsabilidades y procedimientos de actuación frente a incidentes. No obstante, estas políticas deben revisarse y actualizarse de forma periódica, idealmente cada seis meses, con el fin de ajustarse a las nuevas amenazas. Tanto la ISO/IEC 27001:2022 como el NIST SP 800-61 sugieren realizar estas revisiones como parte esencial del ciclo de mejora continua (ISO, 2022; NIST, 2018).

Colaboración Público-Privada

La ciberseguridad no debe gestionarse de forma aislada. Resulta esencial implementar mecanismos de cooperación entre el sector público y privado, a través de la creación de un Observatorio Nacional de Phishing e Ingeniería Social que tenga como función recopilar, analizar y difundir información sobre amenazas en curso. Experiencias como el CSIRT de Chile o el CERT-EU evidencian la efectividad de estas alianzas para lograr una detección temprana y una respuesta conjunta (ENISA, 2022).

Estrategias de Protección de Datos

La protección de la información sensible exige implementar medidas complementarias como el cifrado de datos tanto en reposo como en tránsito, la ejecución de copias de seguridad periódicas y la supervisión constante del acceso a los sistemas críticos. Estas acciones contribuyen a mitigar el impacto de los incidentes, garantizando la disponibilidad y la confidencialidad de los datos incluso frente a ataques exitosos (ISO, 2022; MinTIC, 2022).

Asimismo, la combinación de estas estrategias con auditorías periódicas permite que las organizaciones se recuperen de manera más rápida tras un evento de seguridad.

Conclusiones derivadas del análisis

El análisis de las estrategias actuales para enfrentar el phishing y la ingeniería social en Colombia muestra que, aunque se han logrado avances relevantes en el ámbito de la ciberseguridad, aún persisten limitaciones de carácter estructural y operativo que disminuyen la efectividad de las medidas aplicadas. Herramientas técnicas como la autenticación multifactor, los antivirus, los firewalls y los filtros antiphishing han demostrado ser recursos útiles en la contención de ataques; no obstante, se ha evidenciado que resultan insuficientes si no se complementan con procesos formativos constantes y con normativas organizacionales sólidas que respalden su uso (Castillo Rubiano, 2019; Bustamante & Cano, 2015). Esto refleja que la tecnología, de manera aislada, no puede hacer frente a amenazas cada vez más sofisticadas, siendo necesaria una perspectiva integral que incorpore también el componente humano.

De manera similar, las estrategias de carácter humano y organizacional como las campañas de sensibilización, las capacitaciones y los simulacros de phishing han generado un efecto positivo en la preparación de los usuarios y en la disminución de la exposición a fraudes digitales. Sin embargo, su impacto tiende a disminuir con el tiempo cuando no se garantiza su continuidad y actualización, lo que evidencia que estos programas deben considerarse procesos permanentes y no intervenciones aisladas (Rincón Núñez, 2023). En este sentido, puede afirmarse que la sostenibilidad de la formación resulta tan relevante como la innovación tecnológica dentro del campo de la ciberseguridad.

En síntesis, los resultados evidencian que el phishing y la ingeniería social demandan enfoques integrales que articulen tecnologías avanzadas, programas de formación continua,

políticas internas robustas y un modelo de gobernanza institucional más sólido en materia de ciberseguridad. Únicamente a través de esta integración será factible adelantarse a los atacantes, reducir las brechas actuales y consolidar una cultura digital resiliente que salvaguarde tanto a los individuos como a las organizaciones.

Recomendaciones derivadas al análisis

A partir de los resultados obtenidos, se presentan una serie de recomendaciones orientadas a fortalecer las capacidades de prevención, detección y respuesta frente a ataques de phishing e ingeniería social.

En primer lugar, se propone implementar la obligatoriedad del uso de la autenticación multifactor (MFA) en las entidades públicas y en sectores estratégicos como el financiero, sanitario y educativo. La adopción de este mecanismo permitiría disminuir de manera significativa los accesos no autorizados, aun en escenarios donde las credenciales de los usuarios hayan sido comprometidas, lo que reforzaría la protección de la información más crítica.

De igual manera, se considera indispensable fomentar la implementación de simulacros periódicos y de campañas formativas sustentadas en metodologías gamificadas, orientadas a mantener el interés y la participación activa de los usuarios en el ámbito de la seguridad digital. La aplicación de enfoques pedagógicos innovadores tales como dinámicas lúdicas, ejercicios interactivos y simulaciones realistas posibilita que los usuarios se enfrenten a escenarios de riesgo en un contexto controlado, lo cual contribuye al fortalecimiento de sus competencias y a una mayor capacidad de respuesta frente a incidentes de seguridad en entornos reales.

Otra recomendación clave consiste en destinar recursos a la implementación de inteligencia artificial para la detección temprana de amenazas. Las herramientas basadas en IA facilitan el análisis de grandes volúmenes de información en tiempo real, la identificación de

patrones de ataque que resultan complejos de detectar mediante métodos convencionales y la automatización de respuestas inmediatas frente a incidentes. Integrar estas soluciones en los centros de operaciones de seguridad (SOC) y en los sistemas de gestión de eventos (SIEM) incrementaría de manera significativa la capacidad de monitoreo y reacción de las organizaciones.

Del mismo modo, se plantea la necesidad de efectuar revisiones periódicas de las políticas internas de seguridad, con una frecuencia mínima de cada seis meses y con la participación de equipos multidisciplinarios que integren las áreas de TI, jurídico y gestión del talento humano. Este proceso garantiza que las normativas se ajusten al ritmo de evolución de las amenazas digitales, evitando que se tornen obsoletas o ineficaces en la operación diaria de las organizaciones.

Finalmente, resulta estratégico promover la inclusión de la ciberseguridad en la educación formal desde etapas tempranas, incorporando contenidos básicos sobre seguridad digital y protección de la identidad personal en los planes de estudio escolares y universitarios. Esta iniciativa, complementada con programas de capacitación en el ámbito empresarial, favorecería la formación de ciudadanos digitales más conscientes y mejor preparados para afrontar los riesgos derivados de la ingeniería social.

En conclusión, estas recomendaciones atienden la necesidad de fortalecer una cultura de seguridad proactiva, flexible y centrada en la gestión del riesgo, que habilite tanto a las organizaciones como a la sociedad en su conjunto para anticiparse a la evolución de las amenazas, disminuir la exposición de los usuarios y asegurar la continuidad operativa en escenarios digitales cada vez más complejos.

Conclusiones

La investigación realizada evidenció que el phishing y la ingeniería social representan riesgos significativos dentro del contexto actual de la ciberseguridad, destacándose por su constante capacidad de adaptación y transformación. La incorporación de tecnologías avanzadas, como la inteligencia artificial, el aprendizaje automático y los deepfakes, ha elevado el nivel de complejidad de estos ataques, aumentando los desafíos asociados a su identificación y prevención.

Los hallazgos obtenidos muestran que las estrategias más eficaces son aquellas que combinan de manera integrada tres áreas esenciales. La primera corresponde al ámbito tecnológico, que incluye la autenticación multifactor, el cifrado de información, sistemas avanzados de detección y el uso de inteligencia artificial para reconocer patrones anómalos. La segunda se refiere al factor humano, enfocado en la capacitación constante, la sensibilización sobre riesgos y la realización de simulaciones de ataques, fortaleciendo así la capacidad de reacción de los usuarios. Por último, la dimensión organizacional y normativa abarca la implementación de políticas de seguridad, la gobernanza institucional y la colaboración entre sectores público y privado para crear mecanismos coordinados de defensa y resiliencia digital.

Del mismo modo, los resultados evidencian que la efectividad y sostenibilidad de estas medidas dependen del grado de madurez en ciberseguridad y del entorno en el que se aplican. En el contexto latinoamericano, y de manera particular en Colombia, factores como la insuficiente infraestructura tecnológica, la escasez de profesionales especializados y la fragmentación normativa incrementan la vulnerabilidad frente a estas amenazas, lo que hace necesario adaptar los estándares y marcos internacionales a las condiciones locales.

En conclusión, se concluye que la prevención y mitigación del phishing y la ingeniería social requiere un enfoque integral, adaptable y contextual, que integre de manera articulada los aspectos técnicos, humanos y organizacionales. Dicho enfoque debe enfocarse en fortalecer una cultura de seguridad digital resiliente, en la que los individuos, las organizaciones y el Estado compartan la responsabilidad de proteger la información, reducir las vulnerabilidades y garantizar la continuidad operativa en un entorno digital cada vez más complejo.

Referencias Bibliográficas

- Alcaldía de Cali. (2025). Boletín de seguridad digital 2024. Dirección de Tecnologías de la Información.
- <https://www.cali.gov.co/documentos/1310/boletines-y-publicaciones/>
- Benavides, E., Fuertes, W., & Sánchez, S. (2020). Un experimento para crear conciencia en las personas acerca de los ataques de ingeniería social. *Revista científica*, 13(32), 27–40.
- Bustamante, G., & Cano, J. (2015). Técnicas de detección y control de phishing. *Cuaderno Activa*, (7), 1–162.
- <https://ojs.tdea.edu.co/index.php/cuadernoactiva/article/download/250/242/478>
- Castillo Rubiano, Ó. A. (2019). Phishing (Trabajo académico). Universidad Externado de Colombia.
- <https://bdigital.uexternado.edu.co/bitstreams/e8eac144-41c1-4efe-a7a8-85d8f4f93097/download>
- CCIT – Cámara Colombiana de Informática y Telecomunicaciones. (2023). Impacto económico del cibercrimen en Colombia.
- Chambi, L. (2021). Estrategias para evitar ataques de phishing en empresas. *Revista académica*, 1–4.
- https://ojs.umsa.bo/ojs/index.php/inf_fcpn_pgi/article/view/110
- Chen, X., Sacré, M., Lenzini, G., Greiff, S., Distler, V., & Sergeeva, A. (2024). The effects of group discussion and role-playing training on self-efficacy, support-seeking, and reporting phishing emails: Evidence from a mixed-design experiment. *arXiv*.
- <https://arxiv.org/abs/2402.11862>

Comunidad Andina. (2020). Decisión 872: Régimen general de protección de datos personales.

<https://www.comunidadandina.org/normativa/decision-872/>

Congreso de Colombia. (2008). Ley 1266 de 2008.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=33387>

Congreso de Colombia. (2012). Ley 1581 de 2012.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

Congreso de Colombia. (2018). Ley 1928 de 2018 (Convenio de Budapest).

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=86963>

Consejo de Europa. (2001). Convenio sobre la ciberdelincuencia (Convenio de Budapest).

<https://www.coe.int/en/web/cybercrime/the-budapest-convention>

Cordero, W. (2018). Implementación de técnicas de ingeniería social en la Institución Educativa

de Panqueba (Trabajo de grado). Universidad Nacional Abierta y a Distancia.

<https://repository.unad.edu.co/handle/10596/22690>

DNP – Departamento Nacional de Planeación. (2016). Documento CONPES 3854: Política nacional de seguridad digital.

<https://colaboracion.dnp.gov.co>

Garzón, C., Navas, C., Illicachi, A., Espinoza, R., & Estrella, G. (2024). Análisis de los ataques

de ingeniería social en Ecuador. *Ciencia Latina*, 8(1), 6–15.

<https://ciencialatina.org/index.php/cienciala/article/view/9777>

Gómez, M. (2020). Análisis del riesgo de ataques de ingeniería social en la Secretaría de

Educación del departamento de Nariño (Trabajo de grado). Universidad Nacional Abierta y a Distancia.

<https://repository.unad.edu.co/handle/10596/35224>

- Hernández, A. (2018). Sistema para la detección de ataques phishing utilizando correo electrónico. *Revista Telemática*, 17(2), 60–70.
<https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/304/280>
- Hove, T. (2023). Strategies used to mitigate social engineering attacks (Doctoral dissertation). Walden University.
<https://scholarworks.waldenu.edu/dissertations/10644>
- IBM. (2023). Cost of a data breach report.
<https://www.ibm.com/reports/data-breach>
- Jaramillo, F. (2023). Modelo de machine learning para mitigar los fraudes informáticos de phishing basados en la ingeniería social (Trabajo de grado). Universidad Técnica de Ambato.
<https://repositorio.uta.edu.ec/handle/123456789/38430>
- Jinde, A. (2024). Estrategia para mitigar fraudes de angler-phishing basados en ingeniería social en plataformas de redes sociales (Trabajo de grado).
- Kaspersky. (2024, octubre 15). Informe sobre spam y phishing en CEERI.
- López, O., & Restrepo, W. (2013). Análisis y desarrollo de estrategias para la prevención del uso de la ingeniería social en la sociedad de la información. *Revista académica*, 4(2), 16–22.
- Malagón, J. (2023). Análisis de las técnicas de ingeniería social que amenazan la seguridad informática de usuarios de entidades financieras (Trabajo de grado). Universidad Nacional Abierta y a Distancia.
<https://repository.unad.edu.co/handle/10596/55080>
- Masaquiza, L. (2021). El phishing como delito informático en la legislación ecuatoriana (Trabajo de grado). Universidad Regional Autónoma de los Andes.

<https://dspace.uniandes.edu.ec/bitstream/123456789/13462/1/UA-DER-PDI-026-2021.pdf>

Mayo del Amo, C. M. (2022). Análisis y técnicas de prevención, detección y ataques de phishing (Trabajo de fin de máster). Universidad Nacional de Educación a Distancia.

http://e-spacio.uned.es/fez/eserv/bibliuned:master-ETSIInformatica-II-Cmayo/Mayo_DelAmo_Carmen_TFM.pdf

Mesa Giraldo, M., & Ponce Jaramillo, L. F. (2023). La regulación de los delitos informáticos en Colombia: Logros y falencias en una sociedad de cibercriminalidad en auge. Universidad CES.

<https://repository.ces.edu.co/handle/10946/7689>

Ministerio TIC. (2022). Marco de referencia de ciberseguridad para Colombia.

<https://www.mintic.gov.co/portal/inicio/Marcos-de-referencia/1811:Marco-de-Ciberseguridad>

MinTIC – Ministerio de Tecnologías de la Información y las Comunicaciones. (2022). Transformación digital en Colombia 2022.

<https://www.mintic.gov.co>

Monsalve, J. (s. f.). Ciberseguridad: Principales amenazas en Colombia (ingeniería social, phishing y DDoS). Universidad Piloto de Colombia.

<http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf>

Murillo, E. (2021). Ingeniería social y phishing, ciberataques que más aumentaron durante la pandemia. CRHoy.

<https://www.crhoy.com/tecnologia/ingenieria-social-y-phishing-ciberataques-que-mas-aumentaron-durante-la-pandemia/>

OCDE. (2013). Guidelines on the protection of privacy and transborder flows of personal data.

<https://www.oecd.org/sti/ieconomy/privacy.htm>

OCDE. (2020). Colombia: Digital government review.

<https://www.oecd.org/governance/digital-government-review-of-colombia-e4a36b80-en.htm>

OEA – Organización de los Estados Americanos. (2020). Estado de la ciberseguridad en América Latina y el Caribe.

<https://www.oas.org/ext/es/seguridad/prog-ciber>

Observatorio Latinoamericano de Amenazas Digitales (OLAD). (2025, enero 28). Reporte 2024 en la mira: Organizaciones de América Latina presentan detallado informe sobre las amenazas digitales en la región.

<https://colnodo.apc.org/es/NOVEDADES/reporte-2024-en-la-mira-organizaciones-de-america-latina-presentan-detallado-informe-sobre-las-amenazas-digitales-en-la>

Revista C-LEVEL. (2025). Colombia: Estadísticas clave de ciberseguridad 2024.

<https://revistaclevel.com>

Rincón Núñez, P. M. (2023). Ataques basados en ingeniería social en Colombia: Buenas prácticas y recomendaciones para evitar el riesgo. *InterSedes*, 24(49), 120–150.

<https://doi.org/10.15517/isucr.v24i49.50345>

Apéndices

Apéndice A

Glosario

Anonimato: Condición en la que la identidad de un usuario permanece oculta o no identificable dentro de un sistema o red.

Antivirus: Programa diseñado para detectar, bloquear y eliminar software malicioso en sistemas informáticos.

Ataque de Denegación de Servicio (DoS): Acción que busca colapsar un sistema o red mediante el envío masivo de solicitudes para impedir el acceso legítimo de los usuarios.

Autenticación: Proceso de verificación que confirma la identidad de un usuario o dispositivo mediante credenciales.

Backup: Proceso de duplicación de datos con el fin de recuperarlos en caso de pérdida, daño o ataque cibernético.

Botnet: Red de dispositivos infectados que son controlados remotamente por un atacante para realizar acciones maliciosas coordinadas, como ataques DDoS o envío de spam.

Ciberataque: Acción maliciosa que compromete la seguridad de redes, sistemas o información digital.

Ciberdefensa: Conjunto de estrategias y acciones destinadas a proteger un país o una organización frente a amenazas informáticas.

Ciberseguridad: Disciplina encargada de proteger la integridad, confidencialidad y disponibilidad de la información y los sistemas informáticos.

Confidencialidad: Principio de seguridad que garantiza que la información solo sea accesible por personas autorizadas.

Cortafuegos (Firewall): Sistema de seguridad que controla y filtra el tráfico de red, permitiendo o bloqueando conexiones según reglas establecidas.

Criptografía: Técnica de codificación que permite proteger información mediante algoritmos que transforman los datos en formatos ilegibles.

Data Breach: Incidente de seguridad en el que información confidencial es accedida, copiada o divulgada sin autorización.

Honeypot: Sistema informático deliberadamente vulnerable que simula ser un objetivo legítimo para atraer atacantes y analizar sus métodos.

Ingeniería Social: Táctica de manipulación psicológica utilizada para engañar a personas y obtener información sensible o acceso a sistemas.

Malware: Término general que engloba todo tipo de software malicioso, incluyendo virus, troyanos, gusanos y spyware.

Phishing: Técnica fraudulenta que utiliza correos electrónicos o sitios web falsos para engañar a los usuarios y robar sus datos personales.

Ransomware: Tipo de malware que cifra los archivos de un sistema y exige un pago a cambio de su liberación.

Seguridad de la Información: Conjunto de prácticas destinadas a proteger los datos contra accesos no autorizados, alteraciones o pérdidas.

Smishing: Modalidad de phishing que se lleva a cabo mediante mensajes de texto (SMS) para engañar a los usuarios.

Spoofing: Técnica que consiste en suplantar una fuente confiable, como una dirección IP o email, para obtener acceso o datos.

Suplantación de Identidad: Acción de hacerse pasar por otra persona o entidad para cometer fraudes o acceder a información restringida.

Troyano: Malware que se disfraza de programa legítimo para permitir el acceso remoto no autorizado a un sistema.

Vishing: Versión del phishing que se realiza mediante llamadas telefónicas con el objetivo de obtener información sensible.

Whaling: Tipo de phishing dirigido a altos ejecutivos o personas influyentes dentro de una organización.