Área: Ciencias Formales
Disciplina: TICS
Tipo de artículo: Artículo Original
ISSN: 2697-3316
DOI: https://doi.org/10.69825/cienec.v8i35.396

Análisis del impacto de los delitos informáticos en la protección de los sistemas de información en Milagro, Ecuador: identificando riesgos y fortaleciendo medidas tecnológicas, período 2023–2025

Analysis of the impact of computer crimes on the security of information systems in Milagro, Ecuador: identifying risks and strengthening technological measures, period 2023–2025

Rosa Elizabeth Molina Izurieta[a]
rosa.molinai@ug.edu.ec

Andrés Ubaldo Cedeño Carrasco[a]
ab.cede.2010@hotmail.com

Alba Alexandra Arreaga Ganchozo[a]
alba.arreagag@ug.edu.ec

Génesis Judith Guamán Naula[a]
genesis.guamann@ug.edu.ec

a. Facultad de Ciencias Matemáticas y Físicas, Universidad de Guayaquil (UG), Guayaquil, Ecuador.

Autor por correspondencia: Génesis Guamán Naula; genesis.guamann@ug.edu.ec

Citation: Molina Izurieta R.; Cedeño Carrasco A.; Arreaga Ganchozo A. & Guamán Naula A. Análisis del impacto de los delitos informáticos en la protección de los sistemas de información en Milagro, Ecuador: identificando riesgos y fortaleciendo medidas tecnológicas, periodo 2023-2025. Revista Ciencia Ecuador 2026, 8, 35.URL: https://cienciaecuador.com.ec/index.php/ojs/article/view/396

Received: 05/08/2026
Accepted: 05/09/2026
Published: 19/09/2026

Publisher's Note: Ciencia Ecuador stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Resumen

La presente investigación analiza el impacto de los delitos informáticos en la protección de los sistemas de información del cantón Milagro, Ecuador, durante el período 2023-2025. A partir de datos oficiales de la Fiscalía, se identificó un crecimiento sostenido de las denuncias, que pasaron de 54 casos en 2023 a 150 en 2025. El análisis reveló una alta concentración del fenómeno delictivo en dos modalidades de riesgo crítico suplantación de identidad y apropiación fraudulenta por medios electrónicos registrados en 2025. Mediante un enfoque cuantitativo y descriptivo, se procesaron y clasificaron los datos según tipo de delito y nivel de riesgo, lo que permitió construir una matriz de riesgo y un conjunto de indicadores de gestión. Los resultados sustentan la propuesta de un modelo de gestión orientado a la prevención y el monitoreo, que integra un dashboard en Power BI y un protocolo de actuación, contribuyendo al fortalecimiento de las medidas tecnológicas de seguridad institucional.

Palabras clave: Delitos informáticos; Seguridad de la información; Gestión de riesgos; Ciberseguridad; Indicadores de gestión (KPI)

Abstract

This research analyzes the impact of cybercrimes on the protection of information systems in the Milagro Canton, Ecuador, during the 2023–2025 period. Based on official data from the Prosecutor's Office, a sustained increase in reported cases was identified, rising from 54 in 2023 to 150 in 2025. The analysis revealed a high concentration of criminal activity within two critical-risk categories: identity theft and fraudulent misappropriation via electronic means. Using a quantitative and descriptive approach, the data were processed and classified by crime type and risk level, enabling the creation of a risk matrix and a set of management indicators. The results support a proposed management model focused on prevention and monitoring integrating a Power BI dashboard and an action protocol thereby contributing to the strengthening of institutional technological security measures.

Keywords: *Cybercrime; Information security; Risk management; Cybersecurity; Management indicators (KPIs).*

Introducción

La creciente incorporación de las tecnologías de la información en las actividades institucionales, comerciales y sociales ha generado importantes beneficios en la gestión y el acceso a la información; sin embargo, también ha incrementado la exposición a diferentes modalidades de delitos informáticos. Estas amenazas pueden comprometer la confidencialidad, integridad y disponibilidad de la información, convirtiéndose en un desafío para la protección de los sistemas de información.

En este contexto, la presente investigación analiza el impacto de los delitos informáticos en la protección de los sistemas de información en el cantón Milagro, Ecuador, durante el período 2023–2025. El estudio se centra en los registros oficiales de noticias del delito de la Fiscalía, con el propósito de identificar las principales modalidades delictivas, su frecuencia, comportamiento, riesgos y vulnerabilidades asociados.

El análisis de los registros de la Fiscalía, período 2023-2025 evidencia un incremento acumulado del 183% en el número de denuncias por delitos informáticos, al pasar de 54 casos en 2023 a 150 en 2025.

Este crecimiento no solo refleja una mayor exposición de la ciudadanía a estas amenazas, sino también una concentración significativa del fenómeno en dos modalidades específicas la suplantación de identidad y la apropiación fraudulenta por medios electrónicos, las cuales en conjunto representaron el 98% de los casos registrados durante el último año del período analizado.

Objetivo General

Analizar el impacto de los delitos informáticos registrados por la Fiscalía del cantón Milagro durante el período 2023–2025 sobre la seguridad de los sistemas de información, mediante el estudio de su comportamiento, modalidades y riesgos asociados, con el propósito de identificar vulnerabilidades y proponer medidas orientadas al fortalecimiento de la protección tecnológica.

Objetivos específicos

- Identificar los principales delitos informáticos registrados en la fiscalía del cantón Milagro durante el período 2023–2025, a partir de los reportes de noticias de los delitos
- Describir las características, modalidades y frecuencia de los delitos informáticos identificados en los registros analizados.
- Analizar los riesgos y vulnerabilidades que evidencian los delitos informáticos registrados, en relación con la protección de los sistemas de información.
- Proponer medidas de protección tecnológica orientadas al fortalecimiento de la seguridad de los sistemas de información, a partir de los hallazgos obtenidos en el estudio.

Metodología

La investigación se desarrolló bajo un enfoque cuantivo, con alcance descriptivo y diseño ex post facto, complementado con un componente cualitativo de carácter interpretativo. La fuente principal de información estuvo constituida por los registros oficiales contenidos en los reportes gerenciales de noticias del delito de la Fiscalía del cantón Milagro correspondientes al período 2023–2025.

La población documental estuvo conformada por los registros relacionados con delitos informáticos o conductas ilícitas cometidas mediante tecnologías de la información, medios informáticos o electrónicos.

Como fuente complementaria se consideraron informantes clave vinculados con la investigación de delitos informáticos. La muestra fue de tipo no probabilístico por criterio e incluyó a dos informantes seleccionados debido a su experiencia profesional y conocimiento relacionado con este tipo de delitos.

Para la recolección de información se utilizaron dos instrumentos: una matriz de análisis documental y una guía de entrevista semiestructurada. La matriz permitió registrar el tipo de delito, modalidad, tipificación legal, frecuencia, estado del delito y riesgos asociados a la protección de los sistemas de información. La guía de entrevista estuvo conformada por preguntas abiertas relacionadas con modalidades delictivas, vulnerabilidades, afectaciones a la confidencialidad, integridad y disponibilidad de la información, causas, capacitación y medidas de protección tecnológica.

El procesamiento de los registros documentales se realizó mediante organización y clasificación de la información en matrices y hojas de cálculo, obteniendo frecuencias y porcentajes por modalidad delictiva y año. Posteriormente se realizó un análisis comparativo del período 2023–2025 para identificar tendencias y variaciones. La información obtenida mediante las entrevistas fue categorizada e interpretada y posteriormente contrastada con los resultados documentales.

Las entrevistas fueron semiestructuradas, realizadas de manera presencial, con una duración aproximada de 30 a 45 minutos. La información fue registrada mediante notas de campo y grabación de audio, previa autorización de los participantes, y posteriormente fue transcrita, categorizada y analizada de manera interpretativa.

Nombre/Apellido	Código	Cargo	Formación	Experiencia
Israel Maldonado	-	Secretario	Abogado	14 años
Carlos Suarez	11.236.C.A.G	Secretario	Abogado	24 años

Resultados

La propuesta se fundamenta en el análisis de los registros de casos atendidos por la Fiscalía del cantón Milagro, período 2023–2025 y responde a un incremento sostenido y acelerado de este tipo de infracciones, que exige una respuesta institucional estructurada, basada en datos y orientada tanto a la persecución penal como a la prevención.

La transformación digital de la vida cotidiana banca electrónica, comercio en línea, redes sociales y trámites digitales ha ampliado la superficie de exposición de la ciudadanía frente a la delincuencia informática. En este escenario, la información que la propia Fiscalía genera a través de sus registros constituye un activo estratégico: analizada de forma sistemática, permite anticipar patrones, focalizar campañas de prevención y medir la efectividad de la respuesta institucional.

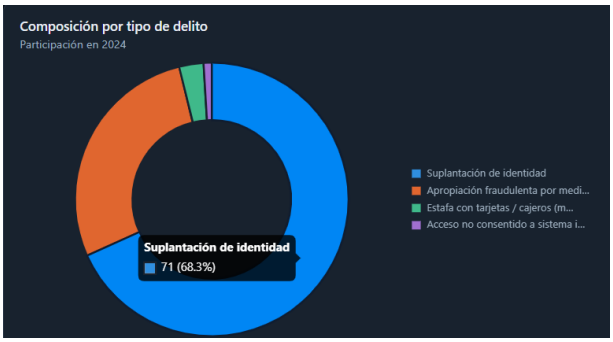
Análisis de los delitos Año 2023

Durante el año 2023 se registraron 54 noticias del delito relacionadas con delitos informáticos. La suplantación de identidad fue el delito con mayor incidenci, lo que evidencia que los ciberdelincuentes utilizaron principalmente técnicas orientadas a hacerse pasar por otra persona para obtener beneficios ilícitos o acceder a información confidencial.

El resto de los delitos presentó una frecuencia considerablemente menor, entre ellos las estafas mediante clonación de dispositivos electrónicos, la apropiación fraudulenta por medios electrónicos, los ataques contra la integridad de sistemas informáticos, la falsificación informática y el acceso no autorizado a sistemas. Aunque su incidencia fue reducida, estos delitos representan amenazas importantes para la confidencialidad, integridad y disponibilidad de la información.

En términos generales, el comportamiento observado en 2023 muestra un predominio de delitos orientados al engaño y la apropiación de identidades digitales, por encima de los ataques dirigidos directamente a la infraestructura tecnológica.

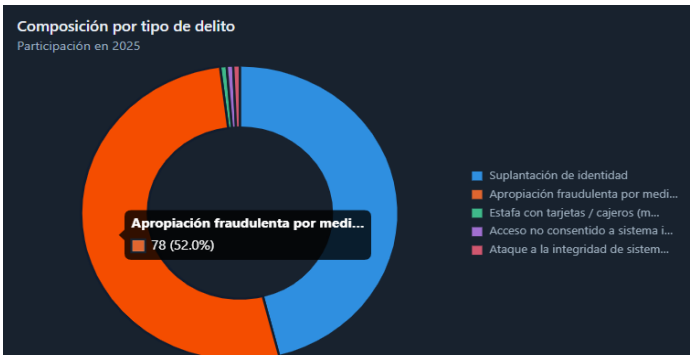
Análisis de los delitos año 2024



En 2024 se registraron 103 noticias del delito, representando un incremento significativo respecto al año anterior, lo que evidencia un aumento importante en la incidencia de delitos informáticos.

La suplantación de identidad continuó siendo el delito más frecuente, con 71 casos. Este comportamiento demuestra que la obtención ilícita de credenciales personales y el uso indebido de identidades digitales continuaron siendo el principal mecanismo empleado por los delincuentes informáticos. En segundo lugar, se ubicó la apropiación fraudulenta por medios electrónicos, con 28 casos, reflejando un incremento considerable de los delitos asociados al fraude económico mediante plataformas digitales y sistemas electrónicos. Los resultados muestran que durante 2024 los delitos informáticos evolucionaron hacia modalidades con un impacto económico más directo sobre las víctimas, especialmente mediante fraudes electrónicos.

Análisis de los delitos año 2025



En el año 2025 se registraron 150 noticias del delito, constituyendo el valor más alto del período analizado. En comparación con 2024, el número de casos aumentó, evidenciando que los delitos informáticos continuaron en crecimiento.

A diferencia de los años anteriores, la apropiación fraudulenta por medios electrónicos pasó a ocupar el primer lugar, con 78 casos. Este cambio sugiere un incremento en las actividades delictivas enfocadas en obtener beneficios económicos mediante medios electrónicos.

La suplantación de identidad permaneció como uno de los delitos predominantes, con 69 casos, manteniendo una incidencia muy elevada y confirmando que continúa siendo una de las principales amenazas para la seguridad de la información.

En conjunto, los resultados de 2025 muestran que los delitos con mayor crecimiento fueron aquellos relacionados con el fraude económico y el robo de identidad, mientras que los ataques dirigidos específicamente contra la infraestructura tecnológica mantuvieron una incidencia mucho menor.

Análisis comparativo del periodo 2023-2025

Los resultados obtenidos permiten concluir que los delitos informáticos registrados durante el período 2023–2025 presentan una tendencia creciente y una evolución hacia modalidades cada vez más orientadas al fraude económico.

Estos hallazgos demuestran que la seguridad de los sistemas de información no depende únicamente de la implementación de soluciones tecnológicas, sino también del fortalecimiento de las capacidades de los usuarios para reconocer y prevenir amenazas informáticas.

La implementación de una estrategia integral de capacitación, complementada con mecanismos de autenticación robusta, políticas de seguridad, monitoreo continuo y campañas de concienciación, constituye una alternativa viable para disminuir la incidencia de los delitos informáticos y fortalecer la protección de los sistemas de información en el cantón Milagro.

Propuesta

Con base en los resultados obtenidos durante el período 2023–2025, se propone implementar una Estrategia Integral de Capacitación para el Reconocimiento de los Delitos Informáticos, orientada a fortalecer la seguridad de los sistemas de información mediante acciones preventivas dirigidas tanto a usuarios como a organizaciones.

1. Capacitación permanente en ciberseguridad

Desarrollar programas de formación dirigidos a usuarios, empleados y responsables de sistemas de información sobre:

- Reconocimiento de delitos informáticos;
- Identificación de correos electrónicos fraudulentos (phishing);
- Protección de datos personales;

- Uso seguro de redes sociales y servicios digitales.

2. Fortalecimiento de los mecanismos de autenticación

Implementar controles que reduzcan el riesgo de suplantación de identidad, tales como:

- Políticas de contraseñas robustas;
- Renovación periódica de credenciales;
- Verificación de identidad para accesos críticos.

3. Protección de la información

Adoptar medidas que garanticen la confidencialidad e integridad de los datos mediante:

- Cifrado de información sensible;
- Copias de seguridad periódicas;
- Control de accesos basado en roles;
- Actualización continua de sistemas y aplicaciones.

4. Monitoreo y respuesta ante incidentes

Implementar herramientas que permitan:

- Detectar actividades sospechosas;
- Registrar eventos de seguridad;
- Responder oportunamente ante incidentes;
- Reducir el impacto de ataques informáticos.

5. Campañas de concienciación

Realizar campañas informativas dirigidas a la ciudadanía y organizaciones del cantón Milagro sobre:

- Principales delitos informáticos identificados.
- Buenas prácticas de seguridad digital.
- Mecanismos de denuncia.
- Recomendaciones para prevenir fraudes electrónicos.

Los resultados se presentan conforme a los objetivos específicos de la investigación, considerando los registros documentales de la Fiscalía del cantón Milagro correspondientes al período 2023–2025. El análisis se realizó a partir de las frecuencias de delitos vinculados con medios tecnológicos, electrónicos e informáticos, tales como estafa, suplantación de identidad, apropiación fraudulenta por medios electrónicos, acceso no consentido a sistemas informáticos, ataque a la integridad de sistemas informáticos, interceptación ilegal de datos, falsificación informática y transferencia electrónica de activo patrimonial.

Delitos informáticos registrados durante el período 2023–2025

Delito informático	2023	2024	2025	Total	%
Suplantación de identidad	35	71	69	175	56.81%
Apropiación fraudulenta por medios electrónicos	2	28	78	108	35,06%
Interceptación ilegal de datos	6	0	0	6	1,94%
Ataque a la integridad de sistemas informáticos	2	0	1	3	0.97%
Acceso no consentido a sistema informático	1	1	1	3	0,97%
Falsificación informática	2	0	0	2	0,64%
Estafa mediante usos de dispositivos electrónicos	3	0	0	3	0.97%

Difusión de información restringida	3	0	0	3	0.97%
Estafa mediante el uso de tarjeta de créditos.	0	3	1	4	1.30%
Total	**54**	**103**	**150**	**307**	**100%**

Discusión

Los resultados obtenidos en el cantón Milagro durante el período 2023–2025 evidencian una tendencia creciente de los delitos informáticos, con predominio de la suplantación de identidad y la apropiación fraudulenta por medios electrónicos. Este comportamiento coincide con lo señalado por Toala Indio (2021) en Ecuador, quien identificó entre las modalidades frecuentes el fraude informático, el acceso no autorizado y el phishing, destacando la necesidad de fortalecer los mecanismos de protección frente a las vulnerabilidades de los sistemas digitales.

En el ámbito internacional, los hallazgos también guardan relación con Riega Virú et al. (2021), quienes señalaron que la digitalización incrementa la exposición a fraudes, suplantación de identidad, accesos indebidos y afectación de datos. De manera similar, Solís Tejedor et al. (2023) determinaron que la seguridad de los sistemas informáticos requiere políticas, capacitación, análisis de vulnerabilidades y auditorías permanentes. La principal diferencia radica en que dichos estudios abordaron el fenómeno desde perspectivas documentales e institucionales, mientras que la presente investigación analiza específicamente los delitos registrados en el cantón Milagro.

Estos resultados tienen implicaciones para la seguridad de los sistemas de información, debido a que las modalidades identificadas pueden comprometer la confidencialidad, integridad y disponibilidad de la información. En consecuencia, se evidencia la importancia de fortalecer los controles de acceso, la protección de credenciales, la actualización de sistemas, el monitoreo de

eventos y la capacitación de los usuarios. En el contexto local, esta necesidad también coincide con Bermeo Almeida et al. (2017), quienes identificaron riesgos y brechas de seguridad en el GAD Municipal de Milagro y plantearon controles y procedimientos basados en ISO/IEC 27001 para su gestión.

Conclusión

Se identificó que los principales delitos informáticos registrados en el cantón Milagro durante el período 2023–2025 estuvieron relacionados principalmente con la suplantación de identidad y la apropiación fraudulenta por medios electrónicos, evidenciando la presencia de modalidades delictivas asociadas al uso de tecnologías digitales.

El análisis de los registros permitió determinar una tendencia creciente de los delitos informáticos durante el período estudiado, con un total de 54 casos en 2023, 103 en 2024 y 150 en 2025. Estos resultados permiten caracterizar el comportamiento y la frecuencia de las modalidades identificadas en el cantón Milagro.

En relación con la seguridad de los sistemas de información, los delitos analizados evidencian riesgos asociados principalmente a la protección de la información personal, las credenciales, la autenticación y las transacciones digitales, aspectos vinculados con la confidencialidad, integridad y disponibilidad de la información. Estos hallazgos sustentan la necesidad de fortalecer las medidas de protección frente a las modalidades delictivas identificadas.

Finalmente, a partir de los resultados obtenidos, se establecieron medidas de protección orientadas a la gestión de riesgos, control de accesos, monitoreo de incidentes y capacitación en ciberseguridad, tomando como referencia las buenas prácticas de ISO/IEC 27001 y el Marco de Ciberseguridad del NIST.

Identificación de la responsabilidad y contribución de los autores: Los autores declaran haber contribuido en el estudio de la siguiente manera: Conceptualización y diseño (GG), Metodología: (GG) Análisis estadístico: (AA), Escritura – Revisión: (RM) Supervisión: (AC.); Administrador del Proyecto: (GG; AA) Todos los autores han leído y aceptado la versión publicada del manuscrito.

Financiamiento:

Financiación propia.

Conflictos de intereses

No hubo ningún conflicto de interés entre los autores.

Revisión por pares:

El manuscrito fue revisado por pares ciegos y fue aprobado oportunamente por el Equipo Editorial de la revista CIENCIA ECUADOR.

Bibliografía

Acosta, M. G., Benavides, M. M., & García, N. P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89).

Agua Santa Gualinga, P. A. (2024). *Plan de seguridad informático basado en las normas ISO 27001 y 27002 para el comercial "El ferretero" de la ciudad de Tena.* Obtenido de Repositorio Digital Uniandes:

Áldaz, I., & Angulo Moncayo, N. (2025). Informática y sociedad. Datos, algoritmos y plataformas en la tecnificación de la vida social. *Revista digital UCE, 1*(30).

Angulo Chica, D. D. (2024). *Análisis de un sistema de gestión de seguridad de la información para la PUCE-E basado en la norma ISO 27001.* Obtenido de Biblioteca General PUCE:

Arzamendi, J. L. (2022). *Ciberdelincuencia y Derecho penal: aproximación a su clasificación y tratamiento jurídico*.

Asamblea Nacional. (s.f.). *Exposición de motivos - Seguridad integral.* Obtenido de Asobanca: https://asobanca.org.ec/wp-content/uploads/2021/10/Proyecto-de-Ley-Organica-de-Seguridad-Digital-Ciberseguridad-Ciberdefensa-y-Ciberinteligencia.pdf

Ávila-Coello, A. A. (30 de abril de 2024). *Seguridad de la información en instituciones públicas: desafíos y buenas prácticas en el contexto ecuatoriano.* Obtenido de Economic Social Research: https://economicsocialresearch.com/index.php/home/article/view/96

Banco Pichincha. (08 de diciembre de 2020). *¿Qué es el phishing? Cómo reconocerlo y evitarlo*. Obtenido de Banco Pichincha: https://www.pichincha.com/blog/que-es-phishing

Bermeo Almeida, O. X., Paguay Lema, C., & Zamora Arana, G. E. (septiembre de 2017). Auditoría de la Seguridad Informática basado en la ISO 27001 Sistema de Gestión de Seguridad de la Información para el GAD Municipal de Milagro. *UNEMI*.

Bravo Mora, B. S., & Daudo Nieto, A. A. (11 de diciembre de 2017). *Diseño De Gestión De Seguridad De La Información En Base A La Norma ISO 27002 Y Al Estudio De Situación Actual De La Empresa Proveedora De Internet "Posorja En Acción CIA. LTDA."*. Obtenido de Repositorio Institucional - Universidad de Guayaquil: https://repositorio.ug.edu.ec/items/137c772c-0c10-4fe2-8afa-5575e22019df

Briones Pincay, G. H., & Hernández Peñaherrera, E. (2018). *Auditoria de Seguridad del Servidor Web de la Empresa PUBLYNEXT S.A. Utilizando Mecanismos Basados en OWASP.* Obtenido de Repositorio Institucional - Universidad de Guayaquil: https://repositorio.ug.edu.ec/items/faa0578b-e796-48f9-aab2-b67e3ff23a30

Cando Estrella, C. A. (2020). *Análisis e implementación de plataforma de seguridad para la protección de la información a través de la administración de los dispositivos finales en la Unidad Educativa Fiscomisional San Juan Bosco.* Obtenido de Repositorio Institucional - Universidad de Guayaquil: https://repositorio.ug.edu.ec/items/344a94bd-6c30-4c84-823e-2b51a9cd3562