

INFORMÁTICA FORENSE Y LOS RETOS DE LA CIBERSEGURIDAD EN MÉXICO**FORENSIC INFORMATICS AND THE CHALLENGES OF CYBERSECURITY IN MEXICO**García Álvarez N.^(†)

Peña J. A.

Centro Universitario del Sur.

Universidad de Guadalajara.

México.

Correspondencia: forensejoseantoniop@gmail.com

Resumen: En este artículo tratamos de incentivar a los actores del sistema de justicia a reconocer que existen nuevas formas de delitos, la delincuencia no es estática sino que va al día y las tecnologías cibernéticas es un medio utilizado para producir daño a la sociedad en general, por lo que hacemos un breve enfoque sobre lo que en México se debería de hacer o por lo menos saber de que existe e ir pensando como trabajar en esta área criminal.

Palabras clave: Informática forense, ciberseguridad, retos, avances.

Abstract: In this article, we aim to encourage actors in the justice system to recognize that there are new forms of crime; delinquency is not static but evolves daily, and cyber technologies are used as a means to cause harm to society in general. Therefore, we provide a brief overview of what should be done in Mexico or at least be aware of its existence and start thinking about how to work in this criminal area.

Key words: Forensic informatics, cybersecurity, challenges, advances.

INTRODUCCIÓN

Las relaciones personales en el mundo son cada vez más digitales, modificando la forma de educar, socializar, consumir, producir y trabajar. En la era digital, la informática forense y la ciberseguridad se han convertido en dos pilares fundamentales para la protección de la información, los datos personales, la investigación y la persecución de los delitos.

La creciente dependencia de las tecnologías de la información y la comunicación (TIC) ha elevado la necesidad de contar con profesionales especializados en estas áreas.

La informática forense juega un papel crucial en la lucha contra la ciberdelincuencia a nivel Global. A través de la investigación científica de los delitos informáticos, se pueden obtener pruebas digitales que permitan identificar a los responsables y llevarlos ante la justicia.

En un mundo cada vez más digitalizado, la seguridad de la información se ha convertido en un tema de vital importancia. México, como muchos otros países, no está exento de los riesgos que acechan en el ciberespacio. En este contexto, la informática forense juega un papel fundamental en la lucha contra el ciberdelito y la protección de la infraestructura crítica.

DEFINICIÓN Y APLICACIONES

La informática forense, como disciplina científica, se encarga de la identificación, preservación, análisis y presentación de pruebas digitales en un contexto legal. En otras palabras, los informáticos forenses son los encargados de investigar los delitos informáticos y recuperar información de dispositivos electrónicos que pueda ser utilizada como prueba en un juicio. Por otro lado, la ciberseguridad se enfoca en la protección de sistemas informáticos y redes contra ataques y vulnerabilidades.

La informática forense, también conocida como **computo forense** o **ciberforense**, se define como la ciencia que se encarga de la identificación, preservación, análisis y presentación de evidencia digital en un contexto legal. Esta disciplina juega un papel crucial en la investigación de delitos informáticos, como el robo de identidad, la piratería informática, el fraude electrónico y el acceso ilegal a sistemas informáticos.

La ciberseguridad se define como el conjunto de medidas técnicas y organizativas que se implementan para proteger los sistemas informáticos, redes y datos frente a amenazas, vulnerabilidades y ataques cibernéticos. Es fundamental para garantizar la confidencialidad, integridad y disponibilidad de la información.

IMPLICACIONES DE LA INFORMÁTICA FORENSE EN LA CIBERSEGURIDAD

A continuación, se describen algunas de las implicaciones de la informática forense en la ciberseguridad:

- **Investigación de delitos cibernéticos:** La informática forense permite la identificación y análisis de pruebas digitales en casos de delitos como robo de identidad, acceso ilegal a sistemas informáticos, fraude electrónico, y pornografía infantil.
- **Peritaje digital:** Los profesionales de la informática forense pueden actuar como peritos en juicios, proporcionando análisis y opiniones técnicas sobre las pruebas digitales. La evidencia digital recopilada por los peritos informáticos es fundamental para identificar a los responsables de los ataques cibernéticos y llevarlos ante la justicia.
- **Prevención de ataques cibernéticos:** Los análisis forenses pueden revelar las técnicas y herramientas utilizadas por los ciberdelincuentes, lo que permite a las empresas e instituciones implementar medidas de seguridad más efectivas. Los análisis forenses pueden ayudar a identificar las vulnerabilidades en los sistemas informáticos y tomar medidas para prevenir futuros ataques.
- **Disuadir a los ciberdelincuentes:** La presencia de profesionales de la informática forense puede disuadir a los ciberdelincuentes de cometer delitos, ya que saben que existe una mayor probabilidad de ser detectados y procesados.
- **Recuperación de datos:** En caso de un ataque cibernético, la informática forense puede ayudar a recuperar datos perdidos o dañados.
- **Contribuir a la mejora de la seguridad informática:** Los análisis realizados por los peritos informáticos pueden ayudar a identificar las vulnerabilidades de los sistemas informáticos y recomendar medidas para mejorar su seguridad.

Los profesionales de la informática forense son responsables de:

- **Identificar y preservar la evidencia digital:** Esto incluye la búsqueda y recuperación de datos de dispositivos informáticos, como discos duros, memorias USB, teléfonos móviles y servidores.
- **Analizar la evidencia digital:** Se utilizan diversas herramientas y técnicas para extraer información relevante de la evidencia, como archivos borrados, correos electrónicos, registros de actividad y contenido multimedia.
- **Presentar la evidencia digital en un contexto legal:** Los informes y análisis realizados por los peritos informáticos deben ser claros, concisos y comprensibles para los jueces, abogados y demás actores del sistema judicial.

La ciberseguridad es un tema de creciente importancia debido a:

- **El aumento del número de ciberataques:** El país ha sido blanco de diversos ataques en los últimos años, incluyendo ataques de ransomware, malware y phishing.
- **La falta de inversión en seguridad informática:** Muchas empresas e instituciones mexicanas aún no destinan los recursos necesarios para protegerse adecuadamente de las amenazas cibernéticas.
- **La falta de cultura de seguridad informática:** Es necesario sensibilizar a la población sobre los riesgos de la ciberdelincuencia y la importancia de adoptar medidas de seguridad básicas.

PANORAMA ACTUAL DE LA CIBERSEGURIDAD EN MÉXICO

México se encuentra en un contexto complejo en materia de ciberseguridad. De acuerdo con el Índice Global de Ciberseguridad 2023 (<https://www.itu.int/pub/D-STR-SECU/es>), el país ocupa el lugar 67 de 194 en términos de seguridad cibernética. Entre los principales desafíos que enfrenta México se encuentran:

- **Falta de inversión en ciberseguridad:** Las empresas e instituciones mexicanas aún no destinan suficientes recursos a la implementación de medidas de seguridad informática.
- **Escasez de profesionales especializados:** Existe una brecha significativa en el número de profesionales especializados en informática forense y ciberseguridad. Las Universidades en el país nos cuentan todavía con investigadores específicos y suficientes, para atender las necesidades cada día más creciente de especialistas.
- **Marco legal incompleto:** La legislación mexicana en materia de ciberseguridad aún se encuentra en desarrollo, lo que dificulta la investigación y persecución de delitos cibernéticos.

Retos de la informática forense y la ciberseguridad en México

Las perspectivas para la informática forense en México son positivas, a pesar de múltiples desafíos. Se espera que la demanda por profesionales en esta área siga aumentando en los próximos años, lo que impulsará el desarrollo de la disciplina y la fortalecerá como herramienta fundamental para la ciberseguridad del país.

A pesar de su importancia, la informática forense y la ciberseguridad aún enfrentan diversos retos en México, como:

- **La falta de recursos humanos y financieros:** La inversión en tecnología y capacitación para la investigación forense digital sigue siendo insuficiente. El país no cuenta con suficientes profesionales especializados en estas áreas, y las instituciones públicas no siempre tienen los recursos necesarios para invertir en tecnología y capacitación.
- **La fragmentación del marco legal:** La legislación mexicana en materia de delitos informáticos aún es dispersa y no siempre está actualizada. Además, que algunas normatividades existentes, nos se encuentran adaptadas completamente a las necesidades de la investigación forense digital.
- **La falta de coordinación entre las diferentes instituciones:** Es necesario mejorar la coordinación entre las fuerzas del orden, las instituciones judiciales y los expertos en informática forense para combatir eficazmente la ciberdelincuencia.
- **Actualización permanente:** La formación de profesionales en informática forense es esencial para fortalecer la capacidad de México para combatir el ciberdelito. La constante evolución de las técnicas, metodologías y herramientas utilizadas por los ciberdelincuentes exige una actualización permanente de los profesionales de la informática forense.

Avances y perspectivas

En los últimos años, se han logrado avances importantes en materia de informática forense en México:

- **Creación del Centro Nacional de Respuesta a Incidentes Cibernéticos (CERT-MX):** El Centro de Respuesta a Incidentes Cibernéticos depende de la Dirección General Científica de la Guardia Nacional y tiene como objetivo prevenir, detectar y responder a incidentes de ciberseguridad.
- **Creación de la Policía Cibernética:** La Policía Federal creó en 2011 la Policía Cibernética, una unidad especializada en la investigación de delitos informáticos.

- **Aprobación de la Ley Federal de Telecomunicaciones y Radiodifusión:** Esta ley, aprobada en 2014, incluye disposiciones relacionadas con la ciberseguridad y la investigación forense digital.
- **Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos:** Tiene como objetivo fortalecer la Ciberseguridad en las Dependencias Federales, Entidades Federativas, Organismos Constitucionales Autónomos, Academia e Instancias del Sector Privado del país. Y fue aprobado en octubre de 2021.
- **Estrategia Digital Nacional:** se emite en el DOF el 06 de sep. Del 2021, y es la hoja de ruta para que las instituciones de la Administración Pública Federal utilicen para orientar los esfuerzos e iniciativas tecnológicas y de seguridad de la información, en una misma dirección y sentido tecnológico.

CONCLUSIONES

La informática forense y la ciberseguridad son dos áreas de vital importancia para la protección de la información y la seguridad nacional en la era digital. Además de ser herramientas fundamentales en la protección de la información y la lucha contra el ciberdelito. En México, es necesario fortalecer estas áreas mediante la inversión en recursos humanos y financieros, la actualización del marco legal y la mejora de la coordinación entre las diferentes instituciones. El desarrollo y fortalecimiento de estas disciplinas son esenciales para enfrentar los desafíos que presenta la era digital. Es ineludible la aprobación de presupuestos, que permitan la inversión en tecnología, capacitación y coordinación interinstitucional para fortalecer la capacidad de México, para enfrentar los desafíos de la seguridad informática en el siglo XXI.

REFERENCIAS BIBLIOGRÁFICAS

1. Alestra: Los retos del cómputo forense en México. <https://www.alestra.mx/blog/etiqueta/24390826159/computo-forense>
2. CLEU: Licenciatura en Computo Forense y Ciberseguridad. <https://www.cleu.edu.mx/Campus/CampusMerida/LicenciaturaComputoForense>
3. IBM: ¿Qué es la informática forense? <https://www.ibm.com/es-es/topics/computer-forensics>
4. Mextudia: CLEU Licenciatura en Computo Forense y Ciberseguridad. <https://mextudia.com/universidades/cleu/cleu-licenciatura-en-computo-forense-y-ciberseguridad/>
5. Tecnología Educativa Revista CONAIC: La Importancia del Cómputo Forense en la Actualidad. <https://terc.mx/index.php/terc/article/view/298>
6. UNIR México: Informática forense: en qué consiste y ámbitos de aplicación. <https://www.unir.net/revista/ingenieria/informatica-forense/>
7. <https://www.itu.int/pub/D-STR-SECU/es>
8. <http://oferta.unam.mx/ciencia-forense.html>
9. https://es.wikipedia.org/wiki/C%C3%B3mputo_forense
10. <https://www.gob.mx/gncertmx/documentos/94081>