Resumen

En la actualidad existen muchos ataques en la red que se deben al desconocimiento de técnicas en seguridad informática, el mayor riesgo para la información se encuentra en las redes sociales y en el acceso a la red en diferentes dispositivos, en los últimos años la información tiene mayor índice de vulnerabilidades por diferentes intereses, a pesar de la existencia de métodos para evitar amenazas y el robo de datos personales, estos métodos son desconocidos por los usuarios, lo que limita el uso correcto de la información y herramientas de protección, el análisis permite determinar el proceso de segregación y elección de la víctima.

Una de sus causas es desconocimiento de las técnicas utilizadas por OSINT, para ello al desarrollar una propuesta metodológica, basada en el análisis de riesgos de seguridad informática en OSINT, para minimizar el impacto de los ciberataques mediante métodos y técnicas de ciberseguridad y ciberdefensa donde se usara OCTAVE permite un plan de mitigación. Al diseñar la metodológica para el empleo ético de los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa, de esta manera aportar a las necesidades administrativas de las empresas, en la investigación se recomienda el proceso metodológico para el empleo ético de los métodos y técnicas de OSINT, tanto en ciberseguridad como en ciberdefensa, para conseguir habilidad en el empleo de las técnicas presentadas, para que se pueda establecer procesos seguros y evitar riesgos informáticos.

-Palabras clave:

- **OSINT**
- **OCTAVE**
- **MEHARI**

Abstract

Currently there are many attacks on the network that are due to ignorance of computer security techniques, the greatest risk for information is in social networks and in access to the network on different devices, in recent years information has higher index of vulnerabilities due to different interests, despite the existence of methods to avoid threats and the theft of personal data, these methods are unknown by users, which limits the correct use of information and protection tools, among other private information, the analysis makes it possible to determine the process of segregation and choice of the victim.

One of its causes is ignorance of the techniques used by OSINT, for this by developing a methodological proposal, based on the analysis of computer security risks in OSINT, to minimize the impact of cyberattacks using cybersecurity and cyber defense methods and techniques where using OCTAVE allows a mitigation plan. When designing the methodological for the ethical use of OSINT methods and techniques, both in cybersecurity and cyber defense, in this way to contribute to the administrative needs of companies, the research recommends the methodological process for the ethical use of methods and OSINT techniques, both in cybersecurity and cyberdefense, to achieve skill in the use of the techniques presented, so that safe processes can be established and computer risks avoided.

-Key words:

- **OSINT**
- **OCTAVE**
- **MEHARI**