Resumen

Este estudio busca establecer estrategias que fortalezcan la seguridad de la información de las Instituciones de Educación Superior (IES) del Ecuador. Su enfoque se centra en desarrollar soluciones relacionadas con la detección de intrusos, detección de anomalías, detección de vulnerabilidades y detección de incidentes de seguridad. Estas actividades forman parte de los principales servicios de un Equipo de Respuesta ante Incidentes de Seguridad Informático (CSIRT). Sin embargo, actualmente la gestión de alertas tempranas se realiza de forma manual, lo que puede derivar en incidentes de seguridad. A esto se suma que en las IES dado el incremento del teletrabajo y la teleeducación, se ha aumentado el número de amenazas, vulnerabilidades, ataques cibernéticos, fallos en los bugs de aplicaciones y sistemas operativos, lo que conlleva a buscar soluciones para proteger a los activos (física y lógicamente) en estas organizaciones.

Este estudio tiene como objetivo incrementar los niveles de seguridad de la información de las IES, para reducir el número de incidentes, que se registran diariamente. Como metodología general, se inició con la revisión del estado del arte, el análisis de la información para definir las fuentes de datos a ser utilizados, y la evaluación y selección de técnicas y herramientas de aprendizaje automático que mejor se adapten a la gestión de alertas de seguridad de la información. Posteriormente se diseñó el modelo de minería de datos y la base de conocimientos de la que se derivó la implementación de un sistema de soporte a la toma de decisiones (DSS) para la gestión de alertas de seguridad. Para esto, se aplicó la metodología de Investigación – Acción, bibliográfica, descriptiva y causal.

Dentro de los resultados esperados, se obtuvo un prototipado DSS, para mostrar, mediante una interfaz de usuario, información que sirva de apoyo a las IES en la toma de decisiones ante eventos de seguridad de la información.

Palabras Clave:

- **APRENDIZAJE AUTOMÁTICO**
- **MINERÍA DE DATOS**
- **ALERTAS DE SEGURIDAD DE LA INFORMACIÓN**
- **GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN**

Abstract

This study seeks to establish strategies that strengthen the information security of Higher Education Institutions (IES) of Ecuador. Its focus is on developing solutions related to intrusion detection, anomaly detection, vulnerability detection, and security incident detection. These activities are part of the primary services of a Computer Security Incident Response Team (CSIRT). However, early warning management is currently done manually, which can lead to security incidents. Added to this is the fact that in IES, given the increase in teleworking and Tele-education, the number of threats, vulnerabilities, cyber-attacks, bugs in applications and operating systems has increased, which leads to the search for solutions to protect users assets (physically and logically) in these organizations.

The main of this study is to increase the information security levels of IES to reduce the number of incidents, which are recorded daily. As a general methodology, it began with the review of state of the art, the analysis of the information to define the data sources to be used, and the evaluation and selection of techniques and machine learning tools that are best adapted to the management of alerts information security. Subsequently, the data mining model and the knowledge base from which the implementation of a decision support system (DSS) for the management of security alerts derived was designed.

To do this, the Action Research methodology combined with a bibliographic and descriptive research were applied. Among the expected results, a DSS prototyping was obtained to show, through a user interface, information that serves as support to IES in making decisions in the face of information security events.

Key words:

- **MACHINE LEARNING**
- **DATA MINING**
- **INFORMATION SECURITY ALERTS**
- **INFORMATION SECURITY MANAGEMENT**