RESUMEN

El crecimiento y la evolución de las amenazas, las vulnerabilidades y los ciberataques aumentan los incidentes de seguridad y generan impactos negativos en las organizaciones. Este estudio presenta un sistema de procesamiento analítico en línea (OLAP) para alertas tempranas de actividades maliciosas. El objetivo de esta plataforma es sistematizar el apoyo a la ciberseguridad provisto por un Equipo de Respuesta a Incidentes de Seguridad Informática (CSIRT) y establecer un mecanismo de análisis con el fin de mejorar el nivel general de seguridad de redes y equipos mediante servicios de alerta temprana. Para cumplir este objetivo, se ha desarrollado una solución de inteligencia de negocios adaptando la metodología de desarrollo de Ralph Kimball para apoyar el análisis de incidentes de seguridad informática. Esta metodología genera un almacén de datos de información recopilada de alertas y eventos grabados de una transmisión continua de datos de varias fuentes de seguridad de Internet que recopilan, rastrean y reportan malware, botnet y fraude electrónico. Además, con Pentaho BI se desarrolla procesos de carga de dimensiones, medidas y hechos, cubos OLAP, informes y cuadros de mando. Los resultados obtenidos demuestran claramente la funcionalidad de la aplicación, donde es posible visualizar con certeza, tanto las advertencias tempranas como el nivel de seguridad de las Instituciones miembros sobre las amenazas y vulnerabilidades registradas.

PALABRAS CLAVES:

- **BUSINESS INTELLIGENCE**
- **ALERTAS TEMPRANAS DE ATAQUES COMPUTACIONALES**
- **CUBOS OLAP**
- **MODELO DE DATOS DIMENSIONAL**
- **METODOLOGÍA DE RALPH KIMBALL**

ABSTRACT

The growth and evolution of threats, vulnerabilities and cyber-attacks increase security incidents and generate negative impacts on organizations. We present an online analytical processing (OLAP) system for early alerts of upcoming malicious activities. This study aims to systematize the support of cybersecurity granted by a Computer Security Incident Response Team (CSIRT) and shall help to establish a mechanism to analyze and improve the overall level of security of networks and equipment by providing early warning services. In order to accomplish this task, a business intelligence solution has been developed adapting the methodology of Ralph Kimball to support the analysis of computer security incidents. This generates a data warehouse of information collected from alerts and events recorded from a continuous transmission of data from various Internet security sources that gather, trace and report malware, botnet, and electronic fraud. Furthermore, we constructed with Pentaho BI load data into the dimensions, measures and facts, OLAP cubes, reports and dashboards. The acquired results clearly demonstrate the functionality of the application where it is possible to visualize with certainty of both, the early warnings, as well as the level of security of the participant Institutions, about the registered threats and vulnerabilities.

KEYWORDS:

- **BUSINESS INTELLIGENCE**
- **EARLY WARNING TO COMPUTER ATTACKS**
- **OLAP CUBES**
- **DIMENSIONAL DATA MODEL**
- **RALPH KIMBALL METHODOLOGY**