RESUMEN

En la actualidad las universidades están siendo amenazadas por ataques informáticos, lo que puede deteriorar su imagen, reducir estudiantes y hasta terminar en robo de información o alteración. Esta investigación tiene como objetivo diseñar una solución mediante Inteligencia de Negocios que actúe como un factor estratégico en el análisis de vulnerabilidades de un equipo de emergencias ante incidentes informáticos CSIRT, de una corporación del desarrollo de Internet avanzado que agrupa a varias universidades miembros del Ecuador. Para llevarlo a cabo se aplicó la metodología de Investigación-acción con un enfoque cualitativo, dividido en tres fases: Primera, se realizó una evaluación cualitativa de dos herramientas de análisis de intrusos como son, "Passive Vulnerability Scanner" y "Snort" que estaban siendo utilizadas, para verificar si eran excluyentes o complementarias. Paralelamente, se iban registrando los logs en tiempo real de los incidentes registrados por dichas herramientas en una base de datos relacional MySQL. Segunda, se aplicó la metodología de Ralph Kimball, para el desarrollo de varias rutinas que permitan aplicar el proceso "Extraer, Transformar y Cargar" de los logs no normalizados que luego serán procesados por una interfaz gráfica. Tercera, se construyó una aplicación de software mediante SCRUM, que permita vincular los logs obtenidos a la herramienta Pentaho BI, con el propósito de generar alertas tempranas como un factor estratégico. Los resultados muestran la funcionalidad de esta solución que ha generado alertas tempranas y que en consecuencia ha incrementado el nivel de seguridad de los miembros de este CSIRT.

PALABRAS CLAVES:

- **INTELIGENCIA DE NEGOCIOS**
- **CIBERSEGURIDAD**
- **DATAMART**
- **CSIRT**
- **VULNERABILIDADES**