



Maestría en

CIBERSEGURIDAD

Tesis previa a la obtención del título de Magíster en Ciberseguridad

AUTORES: Ing. Ramiro Ernesto Andrade Tandazo
Ing. Geovanny Patricio Cumbal Rodríguez
Ing. Ariana Maricel Flores Muñoz
Ing. José Alexander Serrano Dávila
TUTOR: Ing. Jaime Bladimir Ibarra Jiménez

Implementación e Integración de un Sistema de Monitoreo de Eventos
(SIEM) basado en OpenSource para la DINARP

RESUMEN

En el presente proyecto de tesis se aborda como temática todos los trabajos relacionados que conllevan la implementación e implantación de un sistema de monitoreo y correlación de eventos para la Dirección Nacional de Registros Públicos (DINARP), basado en código libre (OpenSource), adaptándolo a la infraestructura de la DINARP; el mismo que ayudará a dar un completo entendimiento tanto al personal técnico como personal de tipo administrativo de la Institución, sobre la información que muchas veces no es tangible por la dificultad que conlleva la interpretación de millones de logs que se generan en el día a día; mejorando de esta forma la capacidad de detección y respuesta ante amenazas cibernéticas.

ABSTRACT

This thesis project addresses all the work that involves the implementation of a monitoring and correlation system of events for the Dirección Nacional de Registros Públicos (DINARP), based on Open Source, adapting it to the infrastructure of the Institution; this project will help give a complete understanding to the technical staff and administrative staff of the Institution, about the information that is often not tangible due to the difficulty involved in interpreting millions of logs that are generated on a daily basis; thus improving the ability to detect and respond to cyber threats.