

## **Resumen**

Las amenazas informáticas han ido incrementando a los largos de los años, en donde Ecuador es el tercer país más atacado de América del sur y el cuarenta y cinco de todo el mundo. Estas amenazas son una parte fundamental que se debe considerar para el levantamiento de nuevos servicios tecnológicos ya que implican un riesgo para cualquier organización. El presente trabajo de titulación tiene como objetivo poner en marcha inicial a un Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT Académico) dentro de la Universidad de las Fuerzas Armadas ESPE mediante un análisis previo de la situación actual de la universidad y seleccionando herramientas de seguridad de la información que sean óptimas para levantar un nuevo servicio que tenga como objetivo detectar amenazas y mitigar riesgos para garantizar al personal de la ESPE seguridad en sus conexiones y dispositivos. La Espe pretende extender su desarrollo cognitivo sobre seguridad de la información dando continuidad al proyecto implementando más servicios en el futuro que servirán para la investigación continua y generar nuevas formas de protección de red en la universidad.

### **PALABRAS CLAVES**

- **CSIRT**
- **CERT**
- **ITIL V3**
- **CIBERSEGURIDAD**

## **Abstract**

Computer threats have been increasing over the years, where Ecuador is the third most attacked country in South America and the 45th in the world. These threats are a fundamental part that must be considered for the creation of new technological services since they imply a risk for any organization. The objective of the present degree work is to start up a Computer Security Incident Response Team (Academic CSIRT) within the Universidad de las Fuerzas Armadas ESPE by means of a previous analysis of the current situation of the university and selecting tools of Information security that are optimal for setting up a new service that aims to detect threats and mitigate risks to guarantee ESPE personnel security in their connections and devices. The Espe intends to extend its cognitive development on information security giving continuity to the project, implementing more services in the future that will serve for continuous research and generate new forms of network protection at the university.

## **KEYWORDS**

- **CSIRT**
- **CERT**
- **ITIL V3**
- **CYBERSECURITY**