Resumen

La ciberseguridad intenta proteger datos, dispositivos, identidad y sistemas contra amenazas cibernéticas para el bienestar personal, académico, estatal o militar; hay que recordar que en la actualidad toda institución maneja datos, y en la mayoría hacen un uso continuo del internet y vincular sus sistemas con ellos. Existen instituciones médicas, financieras, educativas o del gobierno, que optan por el uso del internet para funcionar de una manera más óptima y eficaz.

De acuerdo con la problemática actual de la ESPE, no posee un Centro de Operaciones de Seguridad de la Información propio, formalmente establecido que permita actuar, monitorear y dar seguimientos a las alertas o amenazas informáticas presentadas.

El siguiente trabajo de titulación busca como objetivo poner en marcha inicial un Centro de Operaciones de Seguridad (SOC) dentro de la Universidad de las Fuerzas Armadas ESPE en la unidad de Tecnologías de la Información (UTIC) ,a través de un análisis preliminar de la situación actual de la universidad que nos permitirá escoger las herramientas más optimas de seguridad de la información para así levantar un nuevo servicio cuyo objetivo principal sea detectar amenazas y mitigar riesgos para garantizar la seguridad de las conexiones y sus dispositivos en el desarrollo de las actividades diarias de la comunidad universitaria de la ESPE.

Palabras clave:

- **EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA**
- **SOC**
- **ITIL V4**
- **HERRAMIENTAS DE CIBERSEGURIDAD**

Abstract

Cybersecurity attempts to protect data, devices, identity, and systems against cyber threats to personal, academic, state, or military well-being; It must be remembered that at present every institution handles data, and most of them make continuous use of the Internet and link their systems with it. There are medical, financial, educational or government institutions that choose to use the Internet to function in a more optimal and efficient way.

In accordance with the current problems of the ESPE, it does not have its own Information Security Operations Center, formally established that allows it to act, monitor and follow up on the alerts or computer threats presented.

The following degree work seeks as an objective to start up a Security Operations Center (SOC) within the University of the Armed Forces ESPE in the Information Technology unit (UTIC), through a preliminary analysis of the current situation of the university that will allow us to choose the most optimal information security tools in order to build a new service whose main objective is to detect threats and mitigate risks to guarantee the security of connections and their devices in the development of daily activities of the ESPE university community.

Key words:

- **COMPUTER SECURITY INCIDENT RESPONSE TEAM**
- **CSIRT**
- **ITIL V4**
- **CYBERSECURITY TOOLS**