RESUMEN

Con el constante desarrollo de las Tecnologías de la Información y Comunicación, las organizaciones se han vuelto dependientes de una conectividad digital para la provisión de sus servicios; conjuntamente las actividades maliciosas relacionadas a la tecnología han crecido exponencialmente provocando enormes gastos y pérdidas económicas a causa de las actividades de contención y resolución efectuadas. Actualmente, cuando ocurre un incidente de seguridad informática, la rápida y eficaz respuesta es primordial. Por tal razón entra en contexto el Equipo de Respuesta ante Incidentes de Seguridad Informáticas (CSIRT), un equipo de especialistas de seguridad de TI que dan respuesta a incidentes o amenazas de seguridad de la información, que poseen la capacidad para detectar y mitigar incidentes, vulnerabilidades y riesgos que podrían presentarse. La presente tesis plantea una propuesta para la creación de un CSIRT Académico en la Universidad de las Fuerzas Armadas ESPE que al momento no cuenta con un grupo que se encargue de emitir alertas o de dar un tratamiento adecuado de los incidentes de seguridad informática, es decir, no se tiene un área formalmente establecida en donde se pueda reportar estos incidentes y darles un seguimiento apropiado. Además, la propuesta se encuentra basada en una guía práctica de creación de CSIRTs Académicos y estándares relacionados mundialmente aceptados.

PALABRAS CLAVES

- **EQUIPO DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD INFORMÁTICA - CSIRT**
- **CSIRT ACADÉMICO**
- **ESTÁNDAR ITIL V3**
- **PROYECTO DE CREACIÓN**

ABSTRACT

With the constant development of Information and Communication Technologies, organizations have become dependent on digital connectivity for the provision of their services; jointly the malicious activities related to technology have grown exponentially causing huge expenses and economic losses because of the containment and resolution activities carried out. Currently, when a computer security incident occurs, the quick and efficient response is essential. For this reason, the CSIRTs, a team of IT security specialists who respond to information security incidents or threats, who have the ability to detect and mitigate incidents, vulnerabilities and risks that may arise, come into context. These thesis proposes the creation of an Academic CSIRT at the Universidad de las Fuerzas Armadas ESPE that at the moment does not have a group that is in charge of issuing alerts or giving an adequate treatment to incidents of information security, that means, there is no formally established area where these incidents can be reported and given appropriate follow-up. In addition, the proposal is based on a practical guide for the creation of Academic CSIRTs and related standards worldwide accepted.

KEYWORD

- **COMPUTER SECURITY INCIDENT RESPONSE TEAM**
- **ACADEMIC CSIRT**
- **ITIL V3 FRAMEWORK**
- **CREATION PROJECT**