Resumen

La presente investigación propone el desarrollo de un Plan de Recuperación de Desastres (DRP) para los Laboratorios del Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE, con el objetivo de fortalecer la capacidad de adaptación ante posibles fallos o ataques cibernéticos. Se realizará una revisión de literatura de marcos de referencia, metodologías, normas y estándares relacionados con la gestión de la seguridad de la información. Se seleccionarán aquellos que se utilizarán como guías para la propuesta del DRP. Además, se llevará a cabo la detección de activos críticos y procesos fundamentales para la implementación de los tiempos de recuperación objetivo (RTO) y de trabajo (RWT).

El alcance del proyecto abarca la implementación de medidas para fortalecer la capacidad de recuperación frente a posibles fallos, minimizando el riesgo de interrupciones en las operaciones. En la actualidad, dada la creciente dependencia de las organizaciones en la tecnología de la información, un DRP se vuelve de vital importancia para garantizar la continuidad del negocio y proteger los datos críticos frente a amenazas.

La implementación exitosa del plan permitirá elaborar estrategias más sólidas para la protección y recuperación de datos, mejorando la capacidad de respuesta y facilitando una pronta recuperación de datos. Se busca optimizar continuamente el plan para garantizar una mayor preparación ante posibles desastres y asegurar la integridad y disponibilidad de los recursos críticos de los laboratorios.

Palabras claves: Plan de recuperación de desastres, Plan de continuidad del negocio, análisis de riesgos, departamento de informática, infraestructura IT.

Abstract

This research proposes the development of a Disaster Recovery Plan (DRP) for the Computer Laboratories of the ESPE Armed Forces University, with the objective of strengthening the capacity to adapt to possible failures or cyber attacks. An exhaustive literature review of reference frameworks, methodologies, norms and standards related to information security management will be carried out. Those will be selected to be used as guides for the DRP proposal. In addition, the detection of critical assets and fundamental processes will be carried out for the implementation of the objective recovery times (RTO) and work times (RWT).

The scope of the project covers the implementation of measures to strengthen recovery capacity against possible failures, minimizing the risk of interruptions in operations. Today, given the increasing dependence of organizations on information technology, a DRP becomes vitally important to ensure business continuity and protect critical data from threats.

The successful implementation of the plan will allow the development of more solid strategies for data protection and recovery, improving response capacity and facilitating prompt data recovery, improving response capacity and facilitating prompt recovery from adverse situations. It seeks to continually optimize the plan to ensure greater preparedness for possible disasters and ensure the integrity and availability of critical laboratory resources.

Keywords: Disaster recovery Plan, bussiness continuity plan, risk análisis, computer science departamento, IT infraestructura.