RESUMEN

Actualmente, las amenazas y vulnerabilidades han tenido un rápido crecimiento en el mundo tecnológico; teniendo en cuenta que el desarrollo de las estrategias a nivel de seguridad de información comprende tres campos fundamentales: personas, procesos y tecnología, por lo cual las empresas se ven en la necesidad de identificar mediante el concepto de Pareto el nivel prioritario de seguridad, es decir identificar el veinte por ciento (20%) de la información que genera beneficios en la Organización y que facilita la operaciones en un ochenta por ciento (80%). Para llegar a comprender qué información se debe proteger de posibles amenazas y vulnerabilidades se debe realizar un análisis de riesgos que permita gestionar los incidentes de forma proactiva y dar un adecuado tratamiento en el proceso ya que el principal objetivo es degradar los activos de información que generan valor para la Organización, y adicional a los sistemas de información. El presente proyecto se utilizó la Metodología de Análisis y Gestión de Riesgos MAGERIT V3., la cual contempla una herramienta para automatizar el trabajo denominada PILAR. Adicional se contempló la Norma Internacional ISO 27000 y los resultados obtenidos fue la identificación de dos activos de información críticos/sensibles: ERP Infor LN y las Bases de Datos; adicional se determinó que los dominios de la Norma que más carecen de controles son: Política de Seguridad de la Información, Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información y Gestión de los Aspectos de la Seguridad de la Información para la Continuidad del Negocio.

PALABRAS CLAVE:

- **SEGURIDAD DE INFORMACIÓN**
- **ANÁLISIS DE RIESGOS**
- **ACTIVOS DE INFORMACIÓN**

ABSTRACT

Nowadays, threats and vulnerabilities have been rapidly growing in the technological world; considering that the development of strategies at the level of information security comprises three fundamental fields: people, processes and technology, so that companies need identifying through

the concept of Pareto the priority level of security, that is, to identify twenty percent (20%) of the information that generates benefits in the Organization and that facilitates the operations in eighty percent (80%). To understand what information should be protected against possible threats and vulnerabilities, a risk analysis must be carried out that allows to manage the incidents proactively and give an adequate treatment in the process since the main objective is to degrade the information that generate value for the Organization, and in addition to information systems. The present project used Risk Analysis and Management Methodology MAGERIT V3, which includes a tool to automate the work called PILAR. Additionally, the International Standard ISO 27000 was considered and the results obtained were the identification of two critical / sensitive information assets: ERP Infor LN and Databases; Additional it was determined that the domains of the Standard that lack the most controls are: Information Security Policy, Acquisition, Development and Maintenance of Information Systems and Management of Aspects of Information Security for Business Continuity.

KEYWORDS:

- **INFORMATION SECURITY**
- **RISK ANALYSIS**
- **INFORMATION ASSETS**