RESUMEN

De acuerdo a estudios realizados, como el de Talib, Barchi, Khelifi y Ormandjieva (2012), se ha visto que la seguridad informática está mundialmente orientada a usarse en empresas del sector Público, Salud, Telecomunicaciones, Financiero, entre otras; siendo ISO/IEC 27001 el estándar favorito como marco referencial a seguir para la implementación de Sistemas de Gestión de Seguridad Informática (SGSI). En el ámbito industrial y manufactura si bien se han implementado SGSI estos han sido dirigidos para la gestión de informática del negocio, más no para el área industrial, en el cual actualmente también existe un componente importante de informática, conocido como los Sistemas de Control Industrial (SCI). La razón de no usar ISO 27000 y un SGSI tradicional en los SCI principalmente radica en que estos tienen algunas diferencias en la parte operativa con respecto a los sistemas de Tecnologías de Información y Comunicación (TICs) tradicionales, por lo que éste proyecto propone a la empresa COMERCIALIZADORA SAN REMIGIO utilizar estándares industriales internacionales como son los expedidos por el Instituto Nacional de Estándares y Tecnología de Estados Unidos (NIST). Concretamente este trabajo se enfoca en elaborar un manual de normas y políticas de seguridad informática basada en controles NIST 800-82.r1 y NIST 800-53 para la gestión de seguridad de la información, análogamente a lo que se hace en un SGSI basado en ISO. Con este manual la empresa podrá realizar un Gerenciamiento efectivo de la Seguridad de la Información en sus procesos de fabricación y manufactura en los contextos de confidencialidad, integridad y disponibilidad.

PALABRAS CLAVE:

SISTEMA DE CONTROL INDUSTRIAL

NIST

ISO

RIESGO

POLÍTICAS DE SEGURIDAD

CONTROLES

DISPONIBILIDAD

INTEGRIDAD