RESUMEN

Los últimos reportes Internacionales de incidencias de seguridad indicados en ICS-CERT (2013) han venido dando a conocer durante estos 3 últimos años un creciente número de ataques cibernéticos a Sistemas de Control Industrial (SCI) y sobre todo en países de Latino América. A estos informes se suma una escasa implementación de soluciones de Seguridad de Información por parte de los fabricantes, profesionales de automatización y de informática en lo referente al ámbito Industrial. Esto nos ha llevado a proponer un proyecto, cuyo fin es presentar a la empresa COMERCIALIZADORA SAN REMIGIO un conjunto de Estrategias de Mitigación para mejorar la Seguridad de Información de su SCI. Este trabajo se desarrolla en coordinación con todos los interesados del proyecto en el cual básicamente se realiza un diagnóstico situacional basado en la identificación de amenazas y vulnerabilidades tecnológicas, administrativas y operativas. A su vez esto conduce a visualizar y analizar los riegos críticos de la empresa, para los cuales se revisa la efectividad de los controles actualmente usados con el propósito de diseñar otros que complementen la correcta gestión gerencial-tecnológica del negocio.

PALABRAS CLAVE:
SISTEMA DE CONTROL INDUSTRIAL

NIST

ISO

RIESGO,

AMENAZA

VULNERABILIDAD

ISA 99

CONTROLES

SGSI

ABSTRACT

Last international cyber-security reports according to the ICS-CERT (2013) manifest that in the last three years, the attacks to Industrial Control Systems (ICS) have increased and the most of victims are companies from Latin American countries. In addition to this, another issue has been the lack of solutions of information security systems in charge of industrial providers, automation and system engineers. That is why we propose a Project, which will show a set of mitigation strategies to improve the information security of an ICS. The work is developed in collaboration with the stakeholders of this Project, for which we do a situational diagnostic based on the identification of threats and vulnerabilities in the contexts of technology, administration and operation. In the same time these analysis lead to find critical risks, effectiveness of the actual security controls and also to design another controls, which complement the proper technical management and directive for this business.