ANEXO B

RECOMENDACIONES PARA LLEVAR A CABO UN PROGRAMA DE SEGURIDAD INFORMATICA DE ACUERDO CON LA NORMAL ISA 99 Y COMO EVITAR FALLAS EN CUANTO A CYBER-SEGURIDAD EN LA EMPRESA

En el presente documento se indicará un grupo de recomendaciones acerca de evitar y controlar las fallas al interior de la empresa tomando como referencia el caso de estudio desarrollado en la Sociedad Portuaria de Buenaventura, estas recomendaciones pueden ser tenidas en cuenta cuando se desean tomar medidas y procedimientos en cuanto a *cyber*-seguridad; de igual manera se describe un grupo de fallas que es posible se presenten en otras empresas dentro de los sistemas de control y manufactura.

Dentro de los sistemas Empresariales la información de producción de la planta, los reportes administrativos y financieros del sistema de negocios, manejan un considerable flujo de información de manera continua; por esta razón es adecuado implementar una serie de pautas mediante los cuales se realiza un análisis de riesgos que permiten determinar cómo es, cuánto vale y qué tan protegidos se encuentran los activos o elementos que son considerados importantes para una organización, en este caso dentro del Terminal de Contenedores Refrigerados de la Soc. Portuaria de Buenaventura a cargo de la empresa Soluciones Globales de Energía Ltda. (S.G.E. Ltda.). En conjunto con los objetivos, estrategias y políticas dentro de la empresa S.G.E. Ltda., se siguió una estrategia propuesta por la norma ISA 99 para la gestión de riesgos la cual permitió elaborar una adecuación de la Fase de PLAN dentro de un programa de seguridad informática.

Los Objetivos de Seguridad, constituyen un importante punto dentro de la norma ISA 99, ya que con la identificación y establecimiento de estos la empresa puede establecer, corregir o definir las políticas de seguridad, medidas y procedimientos de seguridad, a fin de obtener niveles aceptables de seguridad. Elementos esenciales en la implementación y establecimiento un Sistema de Administración de *Cyber*-Seguridad.

Para el caso de estudio que corresponde al patio de contenedores refrigerados se determino que se manejaría la prioridad de estos objetivos de seguridad, de acuerdo a lo expuesto por la norma ISA 99 para sistemas de control y automatización industrial. Aquí la principal prioridad la tiene la Disponibilidad entre los componentes de sistema; la

Integridad ocupa un segundo puesto en cuanto a la prioridad, en razón de que hay riesgos inherentes asociados con la maquinaria industrial, que es controlada; y, en último lugar, encontramos la Confidencialidad, en razón de que frecuentemente los datos son tomados en línea y tienen que ser analizados dentro de contexto para que tengan valor.

De acuerdo con la explicación expuesta anteriormente es pertinente establecer a continuación un conjunto de recomendaciones para llevar a cabo un Programa de Seguridad Informática de acuerdo con el estándar ISA 99 dentro del terminal de contenedores refrigerados.

- Para la óptima realización de la adecuación del sistema de administración de cyber seguridad en el terminal de contenedores refrigerados, fue de vital importancia contar con un equipo (compuesto por el Gerente General y el Ing. de Operaciones) que abordará el programa de seguridad informática a través de personas que tenían un gran conocimiento en los flujos informacionales de la empresa.

- Para la realización de una acertada evaluación de riesgos fue necesario que el equipo de trabajo en seguridad tuviera la claridad conceptual en las definiciones de vulnerabilidad y amenazas y cómo estas repercuten en los objetivos de seguridad dentro del sistema de Monitoreo y Supervisión.

- Dado que los problemas de seguridad son transversales a toda la empresa, es necesario que todos los miembros de las diferentes áreas (área técnica, área de operacional y área financiera) entender la importancia de la *cyber* seguridad en los procesos informacionales de la empresa.

- Para lograr la realización de un programa de administración de *cyber* seguridad es de gran relevancia un desarrollo en un nivel de detalle alto de la descripción de los modelos, dado que éstos permitieron entender los procesos informacionales de sistemas de manufactura y control.

- Durante el manejo de la norma ISA 99 por parte de los estudiantes encargados de este documento, fue importante hacer énfasis dentro del terminal de contenedores refrigerados, que al realizar acciones efectuadas hacia la reparación de equipos, sustitución de piezas o componentes, dicha labor debe ser realizada o asesorada por personal que conozca el proceso informacional del sistema, representando esto la disminución de inconvenientes durante el planteamiento de medidas y procedimientos de seguridad.

- Al aplicar un programa de seguridad informática dentro del terminal de contenedores refrigerados, fue posible innovar respecto a los procedimientos de

seguridad informacional, los cuales permitirán proteger los recursos que administran el flujo de información.

- Es conveniente tener en cuenta, a la hora de abordar proyectos basados en la norma ISA 99, recomendar a las directivas de la S.G.E. Ltda. capacitar a sus empleados o al equipo que se encargará del sistema de administración de *cyber*-seguridad en las operaciones de producción, con el fin de evitar fallas o incidentes en cuanto seguridad informacional.

- Cuando se pretenda trabajar sobre sistemas de monitoreo y supervisión (como el encontrado en el terminal de contenedores refrigerados) en los cuales se desee aplicar la norma ISA 99, es aconsejable tener conocimiento del software y de sus herramientas, a fin de evitar el colapso de la información en cuanto a capacidad y manejo, y de esta forma mantener un desarrollo adecuado de los procedimientos informacionales de cyber-seguridad.

- Se Aconsejo la utilización de sistemas de redundancia dentro de los sistemas de manufactura y control, que permita la utilización de un sistema de emergencia durante el tiempo en el cual se revisan o evalúan las medidas y procedimientos de seguridad que presentan fallas y no permiten el normal desarrollo del sistema original.

En cuanto a las fallas, dentro de la norma ISA 99 éstas son catalogadas como Vulnerabilidades; se refieren a qué tan susceptible es el recurso a ser afectado por la ocurrencia de una amenaza, mediante las cuales su ocurrencia puede o no ser controlada por el sistema. Esto implica que al asignarle la probabilidad de ocurrencia se debe pensar en qué posibilidades hay de que se presente la vulnerabilidad y ésta persista, pero no porque el sistema pueda no evitarla, sino porque un agente externo pueda o no activar esta vulnerabilidad.

Para identificar las fallas en cuanto a información es conveniente revisar el flujo de información entre los activos de cierto nivel para proceder a calificarlos de acuerdo con los objetivos de seguridad (Disponibilidad, Integridad, Confidencialidad). En seguida es conveniente revisar la comunicación entre niveles y de igual manera calificarlos a partir de los objetivos de seguridad. A continuación se detallan algunas de esas fallas presentas en el terminal de contenedores refrigerados y como evitar que sucedan nuevamente:

- Fallas de comunicación entre los niveles de Proceso (Medidores Multifuncionales donde alimentan los contenedores) y el Nivel de Controladores (PLCs). Para evitar

que se presente esta falla es importante realizar un revisión tanto física como de la configuración lógica de los equipos.

- Fallas en el Software (Supervisorio y de Monitoreo), por errores en ajustes de programación, los cuales con el tiempo generaron falta de capacidad y configuración y por tanto el colapso del Software. Para evitar esta falla es conveniente que desde el inicio del desarrollo el personal a cargo (labor realizada por la empresa Automatización Avanzada) realizara una labor óptima y detallada en cuanto a la selección de equipos y configuraciones en el software.

- Fallas en las redes de comunicaciones industriales (Modbus y Mobus +), por falta de mantenimiento. Aquí se debió efectuar una revisión física de estas redes, por parte del personal técnico de S.G.E. Ltda., efectuando pruebas de envío de datos y velocidad de comunicación.

- Fallas por parte de los operarios o personal de producción (dentro de S.G.E Ltda.), por mal manejo de los dispositivos y medios de comunicación. Ésta fue recurrente pudo evitar capacitando al personal que labora en la planta sobre las diferentes herramientas (físicas y lógicas) de trabajo que manipulará durante la producción.

- Falla por falta de calibración y mantenimiento en los equipos de campo. Esta falla pudo ser evitar realizando una labor de mantenimiento tanto preventivo como predictivo sobre los Medidores multifuncionales y los cables de conexión con el contenedor, por lo cual es adecuado realizar una programación en la cual se incluya la revisión periódica de los dispositivos de campo a fin de que éstos operen adecuadamente.

- Fallas en cuanto a la entrega de información por parte del operario al sistema de Administración de Operaciones. Es fundamental para evitar este tipo de fallas recalcar en los operarios y personal de producción que durante el proceso de introducir datos en los sistemas de operación de la planta, esta labor se realice con sumo cuidado de que los datos ingresados sean correctos.

- Fallas por parte de las directivas en cuanto al lanzamiento de órdenes de operación, las cuales no son entendidas por el personal de producción y realizan operaciones erróneas. Esta fue poco recurrente, pero se debe entrenar al personal de operación y además se debe tener disponible personal del equipo de seguridad informática para colaborar cuando se presenten este tipo de fallas.

- Falta de Protección en el sistema de Control y Monitoreo, lo cuales pueden ser manipulados directamente por personal no capacitado. Para evitar esta falla fue fundamental nombrar personas idóneas (dentro del personal de operaciones) en cuanto a capacidades laborales para manipular funciones delicadas del proceso.

- Fallas en la selección indebida de equipos que no soporten la capacidad de información que circula por el sistema. A fin de evitar esta falla, es obligación de los jefes y supervisores de personal o de áreas evitar estas fallas, involucrarse directamente en acciones que requieren conocimientos especiales y detallados.

- Fallas en cuanto a pruebas de control, monitoreo o instalación de equipos que tienen como objetivo prestar redundancia o ampliar el sistema. Esta falla se presenta si no se cuenta con el personal capacitado tanto de la empresa, como de miembros *outsourcing* o subcontratados, ya que las personas que realizan alguna aplicación debe realizar las pruebas pertinentes con base en que los sistemas elaborados funcionen de manera ideal.

Estas constituyen algunas de las principales fallas que se presentaron en la empresa caso de estudio en cuanto a *Cyber* Seguridad se refiere.