Guía de adecuación de Modelos, Actividades y Elementos Claves dentro de la fase de PLAN de un Programa de *Cyber*-Seguridad según la Norma ISA 99

Cristian Alexis Gonzalíaz Sánchez

Wilfrido Quiñones Sinisterra

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE ELECTRÓNICA, INSTRUMENTACIÓN Y CONTROL

INGENIERÍA EN AUTOMÁTICA INDUSTRIAL

POPAYÁN

MAYO, 2009

Guía de adecuación de Modelos, Actividades y Elementos Claves dentro de la fase de PLAN de un Programa de *Cyber*-Seguridad según la Norma ISA 99

Cristian Alexis Gonzalíaz Sánchez

Wilfrido Quiñones Sinisterra

Director: Ing. Juan Martin Velasco Mosquera

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE ELECTRÓNICA, INSTRUMENTACIÓN Y CONTROL

INGENIERÍA EN AUTOMÁTICA INDUSTRIAL

POPAYÁN

MAYO, 2009

AGRADECIMIENTOS

Los autores del presente trabajo, manifiestan sus agradecimientos a su director, Ing. Juan Martin Velasco Mosquera, al Ing. Syler Amador del Dpto. de Sistemas y demás ingenieros del Departamento de Instrumentación y Control, a la Universidad del Cauca, amigos y compañeros, quienes contribuyeron con el desarrollo de este trabajo.

Cristian Alexis Gonzalíaz Sánchez y Wilfrido Quiñones Sinisterra

Gracias a Dios por su Infinito Amor...

A mi padre por su apoyo y sabiduría,

A mi madre por su amor y apoyo incondicional,

A mi hermana por su entereza y colaboración,

A mi familia por su fe incansable,

A mis amigos y compañeros por creer...

A todos ustedes dedico este logro...

CRISTIAN GONZALIAZ

Gracias a Dios por su Infinito Amor...

A mi padre por su paciencia y sabiduría,

A mi madre por su gran amor infinito,

A mis Hermanos por su afecto y colaboración,

A mi familia y amigos por creer...

A todos ustedes dedico este logro...

WILFRIDO QUIÑONES

Resumen

Actualmente la Sociedad Regional Portuaria de Buenaventura cuenta con un Patio para almacenamiento de Contenedores Refrigerados, el cual hasta el año 2002 contaba con un aceptable nivel de tecnología para realizar operaciones de monitoreo y supervisión, dentro de las cuales se llevaban a cabo acciones de automatización necesarias para la detección y corrección de errores en el registro y almacenamiento de contenedores, que necesitan ser refrigerados de manera eficaz y en el menor tiempo posible garantizar que los productos se mantengan en buen estado y que la comunicación entre los contenedores y la sala de control arroje datos con una alta fiabilidad.

Debido a las fallas en el sistema de automatización y con el objetivo de continuar mejorando la competitividad y calidad del sistema prestado por la Sociedad Regional Portuaria de Buenaventura en su Patio de Contenedores Refrigerados, se realizó este proyecto guiado hacia un estándar internacional en donde se adecuaron algunos Parámetros dentro un Programa de *cyber* seguridad industrial, para el cual fue importante el uso de algunas de las herramientas Hardware y Software que se encuentran en las instalaciones del patio, con el fin de optimizar de la mejor manera las herramientas que ya poseen en esta área.

Durante este proyecto se adecuaron modelos, arquitecturas, elementos claves y actividades propias de la fase de PLAN dentro de un Programa de *Cyber* Seguridad propuesto por la Norma ISA-S99.

De igual manera se logró establecer una serie de factores que pudieron incurrir para producir la falla en el Sistema de Monitoreo y Supervisión implementado hasta el año 2002 y proponer cómo es posible evitar futuras fallas de seguridad según la Norma ISA-S99.

Con esta Adecuación de Estándares Internacionales de Automatización, en este caso propuestos por ISA (Sociedad Internacional para Automatización), se aporta al desarrollo de procesos industriales, con un enfoque de estandarización, para mejorar el tiempo de respuesta a mantenimientos correctivos que aportan a la seguridad industrial, logrando incrementar la eficacia de producción.

INTRODUCCIÓN

En esta introducción se presenta un panorama de los procesos de seguridad, dando a conocer los antecedentes y retos de la seguridad en la Automatización Industrial y Sistemas de Control, así como los avances que se han dado en la posible solución de los inconvenientes presentados. Por otro lado, se definen los requerimientos de seguridad en el caso de estudio y la manera como se abordan haciendo uso del estándar ISA S99.

PANORAMA GENERAL DE LOS PROCESOS DE SEGURIDAD EN M&CS (SISTEMAS DE MANUFACTURA Y CONTROL)

En la actualidad con los grandes tratados que se firman a nivel mundial, que tienen como objetivo alcanzar la globalización del mercado, las industrias están obligadas a buscar nuevas formas de producción que las fortalezcan y las hagan más competitivas. Por lo tanto, es imperioso para la industria nacional adoptar medidas de seguridad para proteger y facilitar la utilización de información de manufactura en procedimientos tanto de producción como administrativos en la empresa.

Se ha buscado por medio de la automatización en las empresas una integración de la información desde los niveles bajos del proceso, pasando por el nivel de control, hasta el nivel de gestión, pero en la mayoría de empresas los sistemas de control de manufactura (nivel de manufactura) se encuentran separados, no por falta de tecnología, sino por falta del manejo adecuado de la información [1] y es ahí donde entran las temáticas de seguridad, para permitir un intercambio adecuado de información entre los niveles inferiores (nivel de campo, nivel de control, nivel de supervisión) e intermedio (nivel de manufactura) a fin de obtener una comunicación adecuada con el nivel de gestión. Sin embargo, los recientes avances de las TICs (Tecnologías de la Comunicación y la Información) incluyen la implementación de sistemas de seguridad para que aquellos inconvenientes de comunicación que conducen la información generalmente sean superados de manera satisfactoria.

Esta notable separación se debe en su gran mayoría a la formación profesional y a las diversas experiencias que poseen las personas involucradas en el desarrollo de sistemas [1]. Unos están familiarizados con los procesos administrativos, como finanzas, contabilidad, recursos humanos, entre otros, mientras que los otros están involucrados en la administración de datos en tiempo real que provienen directamente del proceso.

Teniendo en cuenta esta problemática, hace algunos años, la ISA (Instrumentation Systems and Automation Society), de acuerdo con su misión de contribuir con el desarrollo de tecnologías para el control de procesos y automatización, decidió crear el comité ISA 99 con el objetivo de encontrar una solución, en la cual participaron firmas industriales muy prestigiosas, como ABB, Invensys Systems, Inc. / Wonderware, Rockwell Automation, Emerson, Honeywell, Yokogawa, Chevron Information Technology Co., Siemens, entre muchas otras [1].

Dicho comité llegó a la conclusión de que la mejor manera de abordar el problema era mediante la elaboración de un estándar que simplificara el trabajo de seguridad en la información entre los sistemas de gestión empresarial y los de manufactura. Por fortuna, no fue necesario comenzar el trabajo desde cero, ya que con anterioridad se habían formado otros comités enfocados a resolver los problemas de normalización de la planta a nivel de Ejecución de Manufactura y Célula de manufactura [1]. Este trabajo previo se materializó en la norma ANSI/ISA-95.00.01, la cual fue adoptada como el estándar internacional IEC-62264, y la norma ANSI/ISA-88.01, equivalente al estándar internacional IEC-61512-01.

El estándar S88 es utilizado para estandarizar los procesos en los sistemas de manufactura por tandas, mejor conocidos como *batch*, mientras que el estándar S95 se enfoca hacia la frontera entre los dominios de los sistemas empresariales (nivel de Ejecución de Manufactura nivel 3 y el nivel de Gestión nivel 4) y los de control y automatización característicos de la planta [1], independiente del tipo de procesos que se lleven a cabo en ella (batch, discreto o continuo).

Al igual que la norma ISA S88 e ISA S95, ISA S99 está comenzando a tener gran acogida a nivel mundial como una importante referencia para la seguridad de sistemas de manufactura, ya que éstas tres se complementan. A pesar de ello, en Colombia las empresas no se han visto interesadas aún, tal vez debido a la falta de personal capacitado en esta área o a la falta de soluciones que sirvan como punto de referencia para tomar la decisión de adecuarla a una tecnología que brinde estos beneficios.

REQUERIMIENTOS DE SEGURIDAD EN EL CASO DE ESTUDIO.

Dentro de industrias en las cuales sus procesos y empleados se involucran en una variedad de riesgos para la seguridad se genera gran cantidad de información, relevante tanto para el negocio como para los procesos de producción; toda esta información en conjunto puede facilitar a las empresas una garantía en cuanto al cumplimiento de los estándares de calidad

establecidos por la legislación, aumentar los niveles de productividad y mejorar el desempeño en los procesos, lo cual se traduce en grandes beneficios para el negocio.

Para esto se necesita un Programa de Seguridad eficiente entre los diferentes sistemas de información que generan y administran datos en los diferentes niveles de la empresa, facilitando al nivel de Ejecución de Manufactura comunicar los requerimientos de producción y a su vez conocer el desempeño de las operaciones de manejo de materia prima con el fin de orientar las acciones dentro de la empresa.

En el caso de estudio se tiene la necesidad de establecer acciones para determinar los Elementos Claves y Actividades dentro de la fase de PLAN para un Programa de Seguridad Industrial, donde la información del registro físico de los Contenedores que ingresan al Patio facilitan la comunicación de los requerimientos al cuarto de control, los cuales son establecidos por el nivel de negocios después de realizar un análisis de demanda de producto; estos requerimientos le indican al área de producción o patio de contenedores refrigerados, de acuerdo con la cantidad y tiempo de estadía del Contenedor, el Valor a Cobrar por el servicio de Conexión dentro de sus instalaciones.

De la misma manera es importante que el nivel de negocios conozca cuál fue el tiempo de conexión y la ejecución del cuarto de control del patio de contenedores refrigerados, donde es conveniente detallar la cantidad de contenedores y tipos de producto que éstos poseen, así como los diferentes recursos utilizados, con el fin de realizar un análisis, determinar costos y establecer acciones para mejorar los posibles inconvenientes presentados.

1 DESCRIPCIÓN DE LA NORMA ISA 99

1.1 NORMA ISA 99: SEGURIDAD PARA AUTOMATIZACIÓN INDUSTRIAL Y SISTEMAS DE CONTROL.

La norma ISA 99 direcciona la aplicación de conceptos y modelos en áreas tales como la definición de un programa de seguridad y los requerimientos mínimos de seguridad. El estándar ISA 99 está dividido en cuatro (4) partes, de las cuales las dos (2) primeras serán utilizadas dentro de este proyecto; las dos (2) partes finales aún no son liberadas por ISA y no están disponibles al público.

1.2 ISA99.00.01 – Parte 1: Terminología, Conceptos y Modelos

La parte 1 describe los conceptos básicos y modelos relacionados con la seguridad electrónica; de igual manera establece el contexto para todas las normas restantes en esta serie de estándares; así mismo, describe la terminología usada para la seguridad electrónica en el ambiente de los sistemas de control y la automatización industrial.

1.2.1 Seguridad

El término seguridad es considerado en el estándar ISA 99 como la prevención de la penetración ilegal o no deseada, la interferencia intencional o no intencional o el inapropiado acceso a información confidencial en la automatización industrial y sistemas de control. La seguridad electrónica, particular foco de este estándar, incluye computadores, redes, sistemas operativos, aplicaciones y otros componentes programables configurables del sistema [5].

1.2.2 Objetivos de Seguridad

El enfoque tradicional de la seguridad informática está basado en ejecutar 3 objetivos: Confidencialidad, Integridad y Disponibilidad (CIA) [5]. En la Figura 1 se muestra el enfoque de seguridad informática bajo la ejecución de 3 objetivos (CIA).

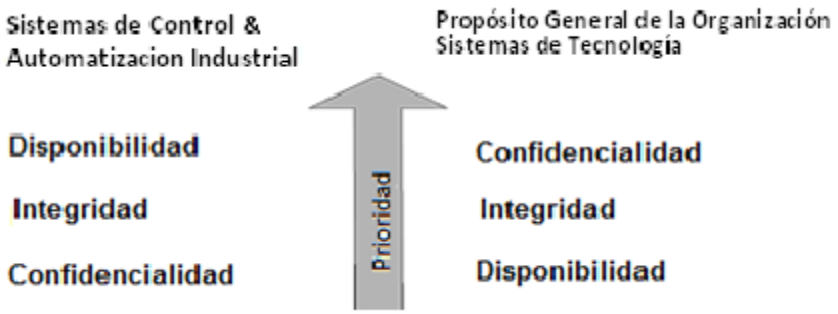


Figura 1 Comparación de Objetivos, Norma ISA 99 Parte 1. ISA 99.00.01 Fig. 1, pág. 36

En el ambiente de la automatización industrial y sistemas de control, la prioridad general de estos objetivos es a menudo diferente; en estos sistemas de seguridad es prioridad la concerniente al mantenimiento de la disponibilidad de todos los componentes del sistema. Hay riesgos inherentes asociados con la maquinaria industrial, que es controlada, monitoreada o de otra manera afectada por la automatización industrial y los sistemas de control. Por lo tanto, la integridad es frecuentemente segunda en importancia. Usualmente la confidencialidad es de menor importancia, porque frecuentemente los datos son tomados en línea y tienen que ser analizados dentro de contexto para que tengan valor [5].

1.2.3 Políticas de Seguridad:

Las políticas de seguridad son las reglas que especifican o regulan cómo una organización protege los sensibles y críticos recursos del sistema [5]. Las políticas de seguridad se complementan con procedimientos; estos procedimientos de seguridad definen en detalle la secuencia de pasos necesarios para proveer una cierta medida de seguridad. Por su nivel de detalle, los procedimientos se aplican a un problema específico, e inclusive pueden pertenecer a una tecnología específica [5].

1.2.4 Zona de Seguridad:

Una Zona de Seguridad es una agrupación lógica de activos físicos, informacionales o de aplicación que comparten requerimientos comunes de seguridad [5]. También pueden existir zonas dentro de zonas o sub-zonas que proporcionan capas de seguridad, dando protección en profundidad y direccionando múltiples niveles de requerimientos de seguridad [5].

Este concepto define la comunicación y accesos requeridos para permitir mover información y personas dentro y entre las zonas de seguridad [5]. Las Zonas de seguridad pueden ser definidas en algún censo físico (zona física) o de una manera lógica (zona virtual) [5].

1.2.5 Conducto:

Un conducto es un tipo particular de zona de seguridad que agrupa comunicaciones que pueden ser lógicamente organizadas en una agrupación de flujos de información dentro y también al exterior de una zona [5]. Puede ser un servicio único, es decir, una sola red de internet, o puede estar constituida por múltiples portadores de datos (múltiples cables de redes y accesos físicos directos); igual que las zonas, los conductos pueden realizarse de ambas maneras, física y lógica. Los conductos pueden conectar entidades dentro de una zona o diferentes zonas [5].

1.2.6 Modelos

El estándar ISA 99 describe una serie de modelos que pueden ser usados en el diseño de un apropiado programa de seguridad. Los objetivos están en identificar la necesidad de seguridad y características importantes del ambiente en un nivel de detalle necesario para dirigir los temas de seguridad. Toda esta información es usada para desarrollar un programa detallado que dirija la seguridad de la automatización industrial y los sistemas de control [5].

1.2.6.1 Modelo de Referencia

Provee el concepto general y las bases para detallar mejor los modelos siguientes presentes en este Estándar, como el Modelo de Activos, Modelo de Zona, Modelo de Conducto [5].

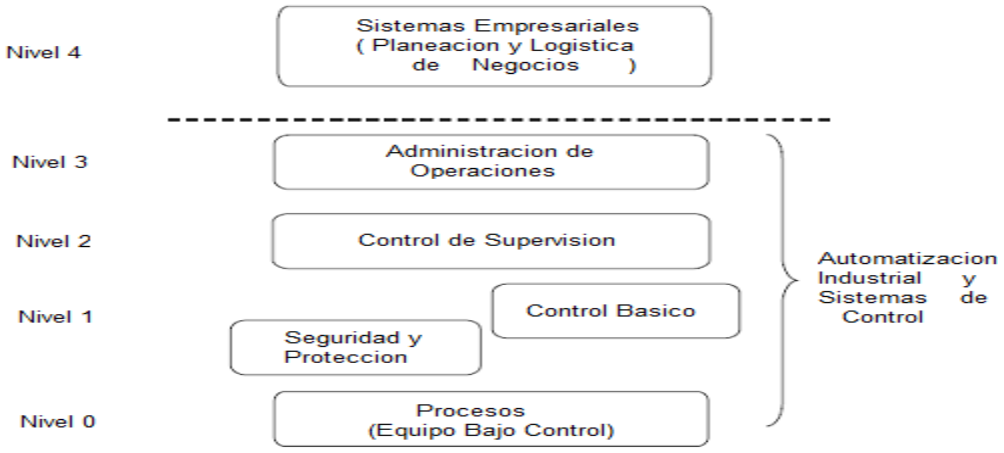


Figura 2 Modelo de Referencia Norma ISA 99, Norma ISA 99 Parte 1. ISA 99.00.01 Fig. 12, pág. 70

1.2.6.1.1 Nivel 4 - Sistemas Empresariales

Consiste en las funciones relacionadas con la planeación y programación de la empresa. Este nivel es el encargado de la administración operativa de la empresa, garantizando rentabilidad del negocio, productividad, altos índices de calidad y satisfacción de las necesidades del cliente [5].

Las actividades del nivel 4 incluyen:

- **a.** Recolección y mantenimiento de inventario de uso y disponibilidad de materia prima y partes de repuesto. Provisión de datos para la compra de materias primas y partes de repuesto
- **b.** Colección y mantenimiento de inventario de uso y disponibilidad de la energía total y provisión de datos para la compra de fuente de energía
- **c.** Colección y mantenimiento de archivos de inventario de todos los bienes en proceso y producidos.
- **d.** Colección y mantenimiento de archivos de control de calidad en lo relacionado con los requisitos del cliente.
- **e.** Colección y mantenimiento de los archivos de uso e historia de vida de maquinaria y equipo, necesarios para planificación de mantenimiento preventivo y predictivo.

f. Colección y mantenimiento de datos de uso de mano de obra para transmitir a personal y contabilidad.

g. Establecimiento del programa básico de producción de planta.

h. Modificación del programa básico de fabricación de la planta para órdenes recibidas, basada en cambios de la disponibilidad de recursos, disponibilidad de fuentes de energía, niveles de demanda de personal y requerimientos de mantenimiento.

i. Desarrollo de mantenimiento óptimo preventivo y programas de renovación de equipo en coordinación con el programa básico de producción.

j. Determinación de niveles óptimos de inventario de materia prima, fuentes de energía, partes de repuesto y productos en proceso en cada punto de almacenamiento. Estas funciones también incluyen planificación de los requerimientos de materiales (MRP) y suministro de partes de repuesto.

k. Modificación del programa básico de fabricación en cuanto sea necesario cuando ocurran interrupciones mayores de producción.

l. Planificación de la capacidad, basada en todas las actividades arriba mencionadas.

1.2.6.1.2 Nivel 3- Administración de Operaciones

Este nivel incluye las funciones involucradas en el manejo de los flujos de trabajo, producción y las expectativas del producto terminado. Ejemplo: los despachos de producción, programas detallados de producción, aseguramiento de la confiabilidad y control óptimo a lo ancho de la empresa [5].

Las actividades del nivel 3 incluyen:

a. Informar sobre la producción del área incluyendo los costos variables de manufactura.

b. Acumular y mantener datos de área sobre producción, inventario, mano de obra, materia prima, partes de repuesto y uso de energía.

c. Realizar recolección de datos y análisis fuera de línea en cuanto lo requieran las funciones de ingeniería. Esto puede incluir análisis estadístico de calidad y funciones de control relacionadas.

d. Llevar a cabo funciones de personal requeridas tales como: estadística de periodos de trabajo (tiempo, tareas, etc.), programación de vacaciones, programaciones de mano de obra, línea de promoción, entrenamiento dentro de la empresa y calificación de personal.

e. Establecer el plan de fabricación detallado inmediato para su propia área incluyendo mantenimiento, transporte y otras necesidades relacionadas con la producción.

f. Optimizar localmente los costos para su área individual de producción, mientras se lleva a cabo el plan de fabricación establecido por las funciones del nivel 4.

g. Modificar los planes de producción para compensar las interrupciones de producción de la planta que puedan ocurrir en su área de responsabilidad.

1.2.6.1.3 Nivel 2 – Control de Supervisión:

Este nivel incluye las funciones que involucran el monitoreo y control de los procesos físicos, usualmente estas funciones se realizan en múltiples áreas de producción en una planta; tales como destilación, conversión, procesos de mezcla [5].

Actividades del Nivel 2:

a. Interfaz Hombre-máquina para el Operador.
b. Alertas de alarmas para el operador.
c. Funciones del Control de Supervisión.
d. Históricos del proceso.

1.2.6.1.4 Nivel 1- Control Básico o Local

Este nivel incluye las funciones involucradas en el sensado y manipulación física de procesos. Aquí se monitorean los equipos, se leen los datos de sensores, se ejecutan algoritmos si es necesario y se mantienen los datos históricos; algunos ejemplos son calibración de un sistema de tanques, sistemas indicadores de temperatura y los sistemas de seguridad y protección de equipos. En el nivel 1 los controladores están directamente conectados a los sensores y actuadores del proceso. Algunos de los equipos que se incluyen en el nivel 1 son: controladores DCS, PLCs, RTUs [5].

1.2.6.1.5 Nivel 0 - Proceso

Este nivel describe el proceso físico que está siendo controlado, que puede incluir diferentes tipos de instalaciones de producción incluyendo los sensores y actuadores directamente conectados al proceso.

1.2.6.2 Modelo de activos

El modelo de Activos representa sistemas de información secundarios los cuales pueden estar presentes en los varios niveles jerárquicos. En este sistema se interactúa con el equipo de control, recolectando datos desde éste y enviándole recetas e instrucciones de proceso. Sistemas de información de Línea, Área y Sitios actúan también como repositorios para servir información de producción a los usuarios a lo largo de la empresa y pueden interactuar con aplicaciones de planificación de recursos de la empresa que corran en el centro de datos corporativos [5]. A continuación se muestra un ejemplo de modelo de activos de acuerdo con la Norma ISA 99.

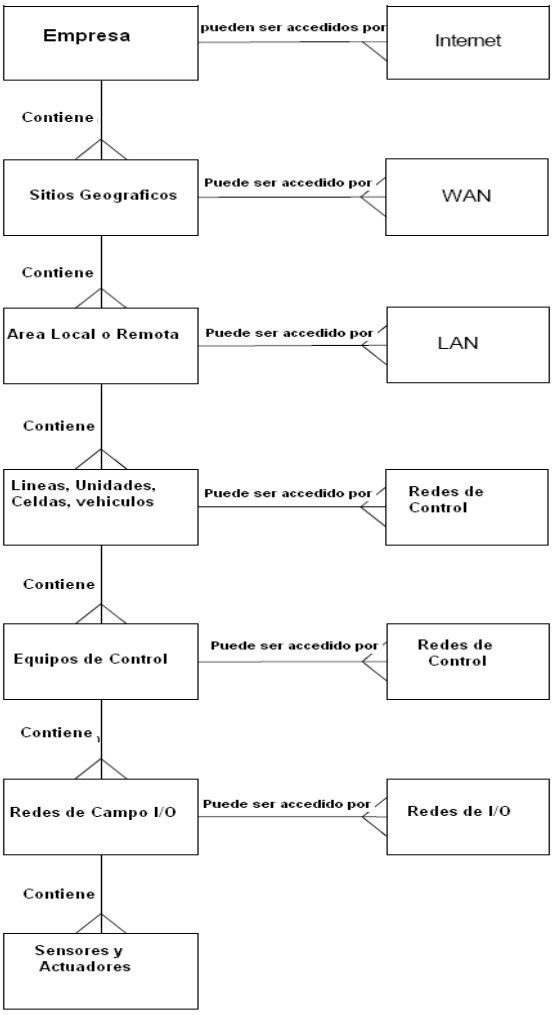


Figura 3 Ejemplo del Modelo de Activos, Norma ISA 99 Parte 1. ISA 99.00.01 Fig. 14, pág. 74

1.2.6.3 Arquitectura de referencia

La arquitectura de referencia es construida a partir de las entidades definidas en el modelo de activos. Una arquitectura de referencia es específica para cada situación bajo revisión y será específica para ese análisis. Cada organización crea una o más arquitecturas de referencia dependiendo de las funciones de negocio realizadas, así como de las funciones bajo revisión. Podría ser común para una organización tener una arquitectura única de referencia para la corporación, generalizada para cubrir todas las instalaciones de operación. Cada instalación o tipo de instalación puede también tener un diagrama de arquitectura de referencia de redes más

detallado que se expanden sobre el modelo de empresa [5]. A continuación se muestra un ejemplo de arquitectura de referencia de acuerdo con la Norma ISA 99.

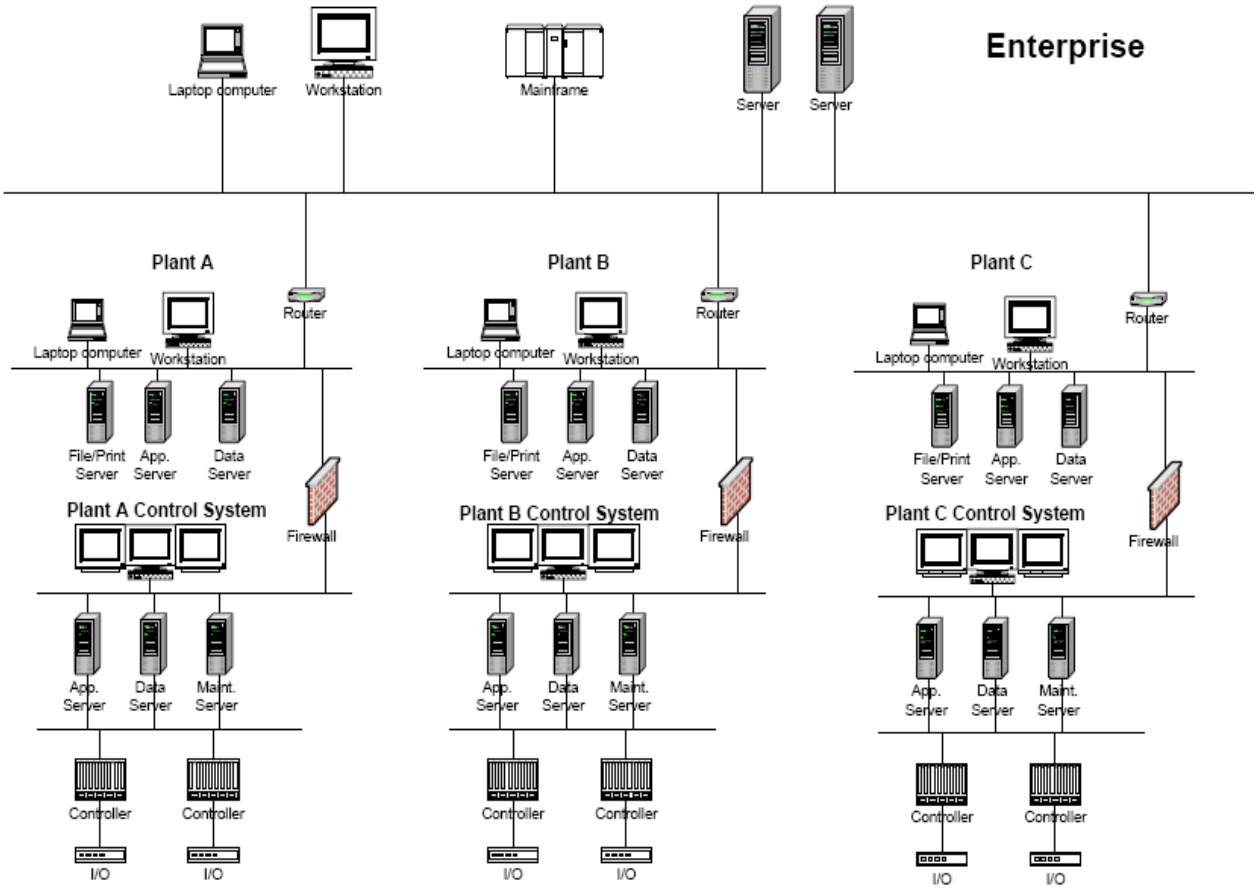


Figura 4 Ejemplo de Arquitectura de Referencia, Norma ISA 99 Parte 1. ISA 99.00.01 Fig. 16, pág. 78

1.2.6.4 Modelo de zona y conducto.

Un modelo de zona y conducto es desarrollado con base en la arquitectura de referencia. Este modelo permite describir la agrupación lógica de activos dentro de una empresa o subconjunto de la empresa [5]. Los activos son agrupados dentro de entidades (ejemplo: negocios, instalación, sitio o automatización industrial y Sistemas de Control), que pueden analizarse para políticas y, como consecuencia, requerimientos de seguridad. El modelo ayuda en la valoración de amenazas comunes, vulnerabilidades y las correspondientes contramedidas necesarias para

lograr la seguridad (apuntar al nivel de seguridad) requerida para la protección de los recursos agrupados. A continuación se muestra un ejemplo de modelo de zona y conducto de acuerdo con la Norma ISA 99.

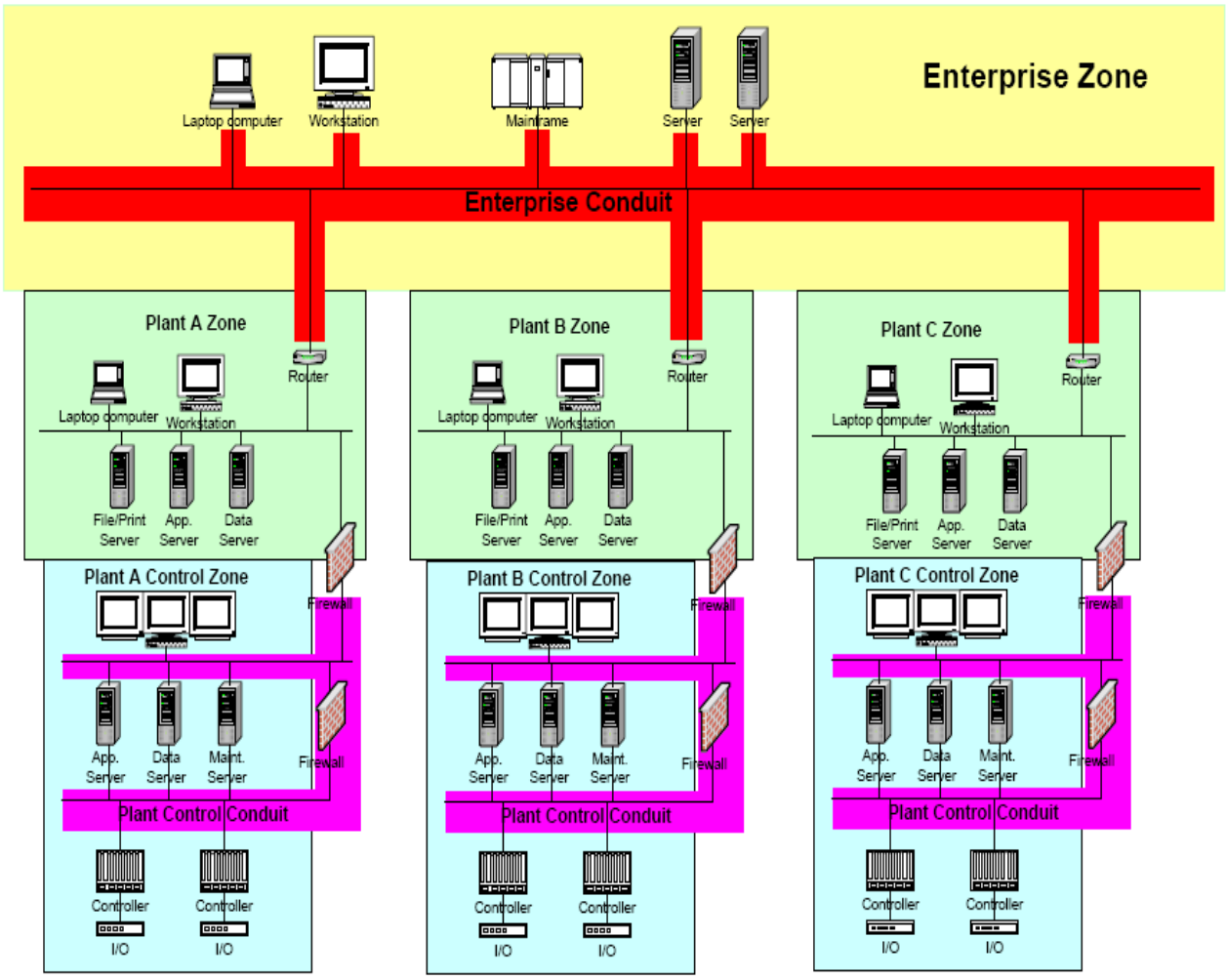


Figura 5 Ejemplo modelo de zona y conducto, Norma ISA 99 Parte 1. ISA 99.00.01 Fig. 7, pág. 59

1.3 PARTE 2 ESTABLECIMIENTO DE UN PROGRAMA DE SEGURIDAD PARA MANUFACTURA Y SISTEMAS DE CONTROL

1.3.1 Apreciación global de la administración de un programa de seguridad

La administración de un sistema de *cyber* seguridad es el conjunto de políticas de seguridad y procedimientos que colectivamente son usados para manejar la *cyber* seguridad en toda la compañía. El sistema de administración está direccionado a la creación de políticas y procedimientos, las actividades de mitigación para reducir las vulnerabilidades, las periódicas reevaluaciones del cambiante panorama de vulnerabilidades y la efectividad para la institucionalización de procedimientos, y finalmente, la efectividad del programa.

Un completo sistema de administración de *cyber* seguridad consiste en (18) claves elementales que toman lugar en las siguientes 4 fases principales:

- **Planear** (Plan) – establece el alcance y políticas del sistema de administración de *cyber* seguridad, identifica, clasifica y evalúa riesgos, y desarrolla un plan continuidad de negocios.
- **Realizar** (Do) – implementa y opera el sistema de administración de seguridad y todos sus procesos.
- **Verificar** (Check) -- supervisa, evalúa, mide el desempeño y reporta resultados a la administración para la revisión.
- **Actuar** (Act) — toma acciones correctivas y preventivas, y continuamente perfecciona el desempeño.

Como se observa a continuación el proceso es continuo:

Figura 6 Continuidad de Actividades en un Sistema de Administración de *Cyber* Seguridad, Norma ISA 99 Parte 2. ISA 99.00.02 Fig. 4, pág. 3

1.3.2 Los 18 elementos claves para un sistema de administración de *cyber* seguridad

A continuación se muestra la cartografía de los (18) elementos claves importantes en las cuatro fases Planear-Hacer-Revisar-Actuar.

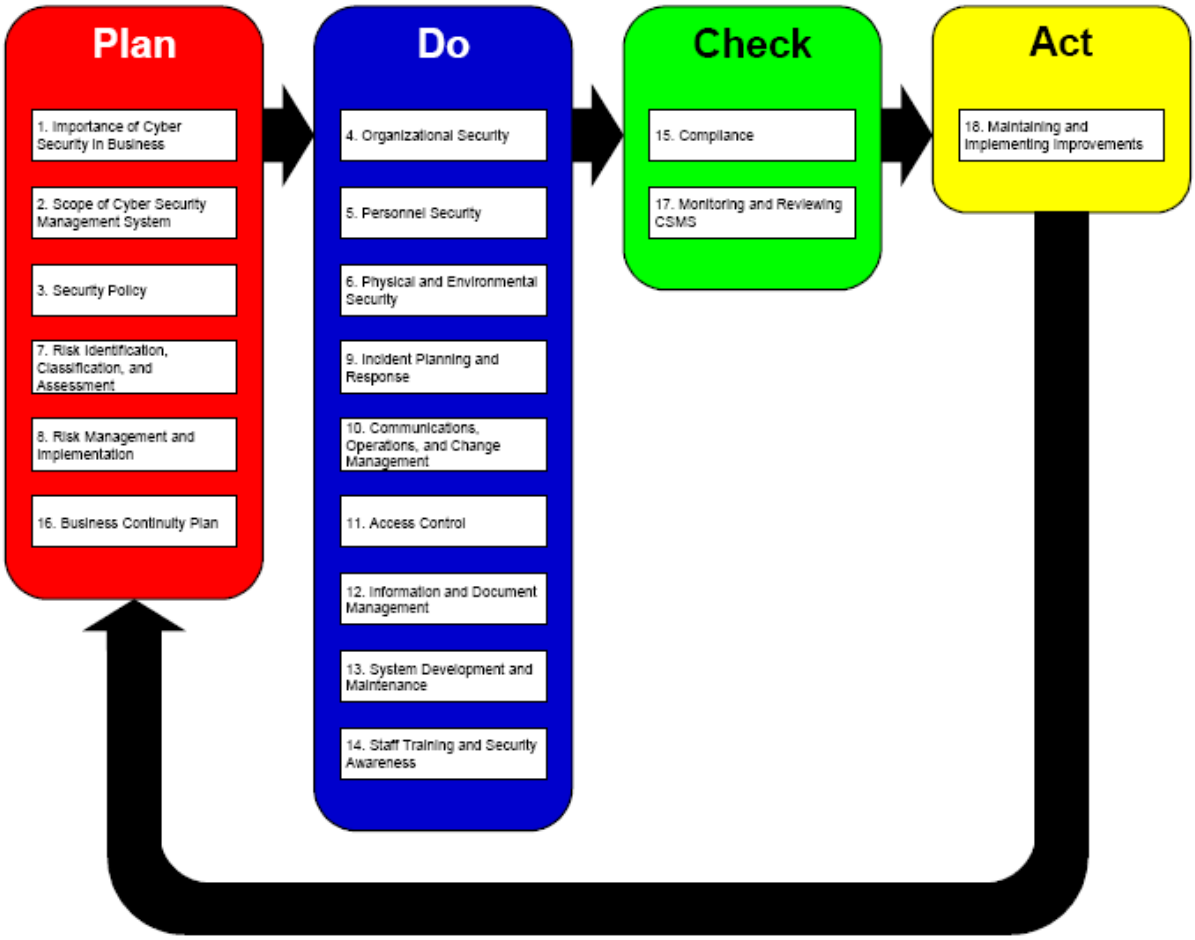


Figura 7. Los 18 Elementos Claves de un CSMS mapeado dentro de las Fases Plan-Hacer-Chequear-Actuar, Norma ISA 99 Parte 2. ISA 99.00.02 Fig. 5, pág. 31

El presente trabajo de grado se limitará a la fase de **PLAN,** la cual es la más viable para llevar a cabo de acuerdo con el caso de estudio que será detallado en el siguiente capítulo.

Dentro de la empresa caso de estudio se trabajaron los siguientes Elementos Claves para la fase de **PLAN,** los cuales serán detallados a continuación:

- Importancia de la *cyber* seguridad en las empresas.
- Ámbito de aplicación de un sistema de administración de cyber seguridad.
- Políticas de seguridad.
- Identificación Clasificación y Evaluación de Riesgo.
- Gestión de Riesgo e Implementación.

En la fase de PLAN no es conveniente desarrollar el elemento clave denominado Plan de Continuidad de Negocios, dado que para su realización es necesario haber cumplido con elementos claves pertenecientes a otras dos Fases siguientes a la fase de PLAN como son (Hacer y Revisar), por lo tanto no se cuenta con la información necesaria para su elaboración.

1.3.2.1 Importancia de la *Cyber* Seguridad en las Empresas.

La importancia de la *cyber* seguridad en los negocios establece que la empresa es consciente y entiende la importancia de su(s) actividad(es) en relación con la Tecnología de la Información (IT) y los riesgos de IT. Estos riesgos se extienden a la manufactura y los sistemas de control, las empresas mixtas, los terceros y socios de *outsourcing*, así como las empresas relacionadas con las actividades de tecnologías de información [2].

- **Aplicabilidad a la *cyber* seguridad en M&CS (Manufactura y Sistemas de Control)**

Los riesgos para los recursos tradicionales de IT se centran en la confidencialidad, integridad y disponibilidad de la información. Los riesgos en la manufactura y los sistemas de control son diferentes; los indicadores se centran en la seguridad y fiabilidad operativa, además de la tradicional protección de la confidencialidad, integridad y disponibilidad de la información. Los riesgos de usar *outsourcing*, terceros contratistas u otros socios en la cadena de valor de manufactura incluyen una sensible información transmitida, almacenada o procesada. La integración de estos socios comerciales en las operaciones de la compañía potencialmente permite el acceso involuntario a los sistemas de la empresa [2].

1.3.2.2 Ámbito de aplicación de un sistema de administración de *Cyber* seguridad

En esta sección se describe un procedimiento práctico para definir el alcance de un sistema de administración de *cyber* seguridad (CSMS). El alcance puede incluir todos los aspectos de los sistemas de manufactura y de control, puntos de integración con socios comerciales, clientes y proveedores [2].

- **Aplicabilidad de la *cyber* seguridad en M&CS**

Una organización responsable de determinar y comunicar las políticas corporativas en lo que se refiere a la *cyber* seguridad es esencial para proteger los recursos de la empresa desde una perspectiva de la *cyber* seguridad. Las empresas tienen que reconocer que en el mundo actual de los negocios regido por internet, la conectividad de la información electrónica es una parte integral para hacer negocios y, por tanto, la *cyber* seguridad es esencial. Las transacciones comerciales no sólo son contenidas dentro del *firewall* de internet de la empresa (sistema diseñado para prevenir el acceso ilegal a una red privada conectada a Internet), sino se extienden a los clientes, proveedores, terceros contratistas, socios y socios en *outsourcing* [2].

1.3.2.3 Política de Seguridad

Al definir una política de seguridad, el personal directivo ha puesto de manifiesto el compromiso de mejora continua a través de las políticas publicadas. Las políticas deben ser proporcionadas a los empleados y se revisarán periódicamente para asegurarse que siguen siendo apropiadas [2].

- **Aplicabilidad de la *cyber* seguridad en M&CS**

El compromiso de liderazgo es relativo a las actividades de política de seguridad que implican el reconocimiento de las directivas de la empresa de las políticas de seguridad, como una responsabilidad de negocio compartida por todos los miembros del equipo administrador y como una política que incluye componentes físicos y componentes lógicos [2].

1.3.2.4 Identificación Clasificación y Evaluación de Riesgos

La identificación, clasificación y evaluación de riesgos son los pasos claves para reconocer dónde existen vulnerabilidades de seguridad en la empresa y los potenciales impactos / consecuencias que podrían producirse como resultante de un incidente de seguridad [2].

- **Aplicabilidad de la *cyber* seguridad en M & CS**

La evaluación del riesgo se ocupa del análisis de las amenazas, vulnerabilidades y las consecuencias. La evaluación y análisis del riesgo identifican la forma de mejorar aún más la seguridad de toda la cadena de suministro (es decir, la manufactura, distribución, venta de productos, etc.). La evaluación del riesgo examina cómo la confidencialidad, integridad y disponibilidad pueden verse comprometidas y el impacto resultante de tal compromiso [2].

1.3.2.5 Gestión de Riesgos e Implementación

Gestión de Riesgos e implementación se ocupa del desarrollo y la aplicación de las medidas de seguridad que sean proporcionales a los riesgos. Las medidas de seguridad pueden tener en cuenta los enfoques inherentemente más seguros para el diseño de procesos, ingeniería y control administrativo, manual y de procedimiento, y las medidas de prevención y mitigación. La importancia de la mitigación del riesgo es convertir todos los planes de gestión del riesgo en acciones [2].

- **Aplicabilidad de la *cyber* seguridad en M & CS**

Las empresas toman medidas después de que identifican y evalúan los posibles riesgos de seguridad. Las acciones pueden incluir colocar adicionales o diferentes medidas de seguridad para proporcionar una mayor protección a la industria, los sistemas de control y los sistemas de información involucrados [2].

1.3.3 Actividades requeridas para desarrollar un sistema de administración de *cyber* seguridad

Los elementos claves y las actividades fundamentan el programa de *cyber* seguridad; estas actividades también se encuentran ubicadas o mapeadas con sus correspondientes fases de Planear-Hacer-Revisar-Actuar. A continuación se muestra las actividades requeridas para un programa de seguridad especificadas en un marco de tiempo.

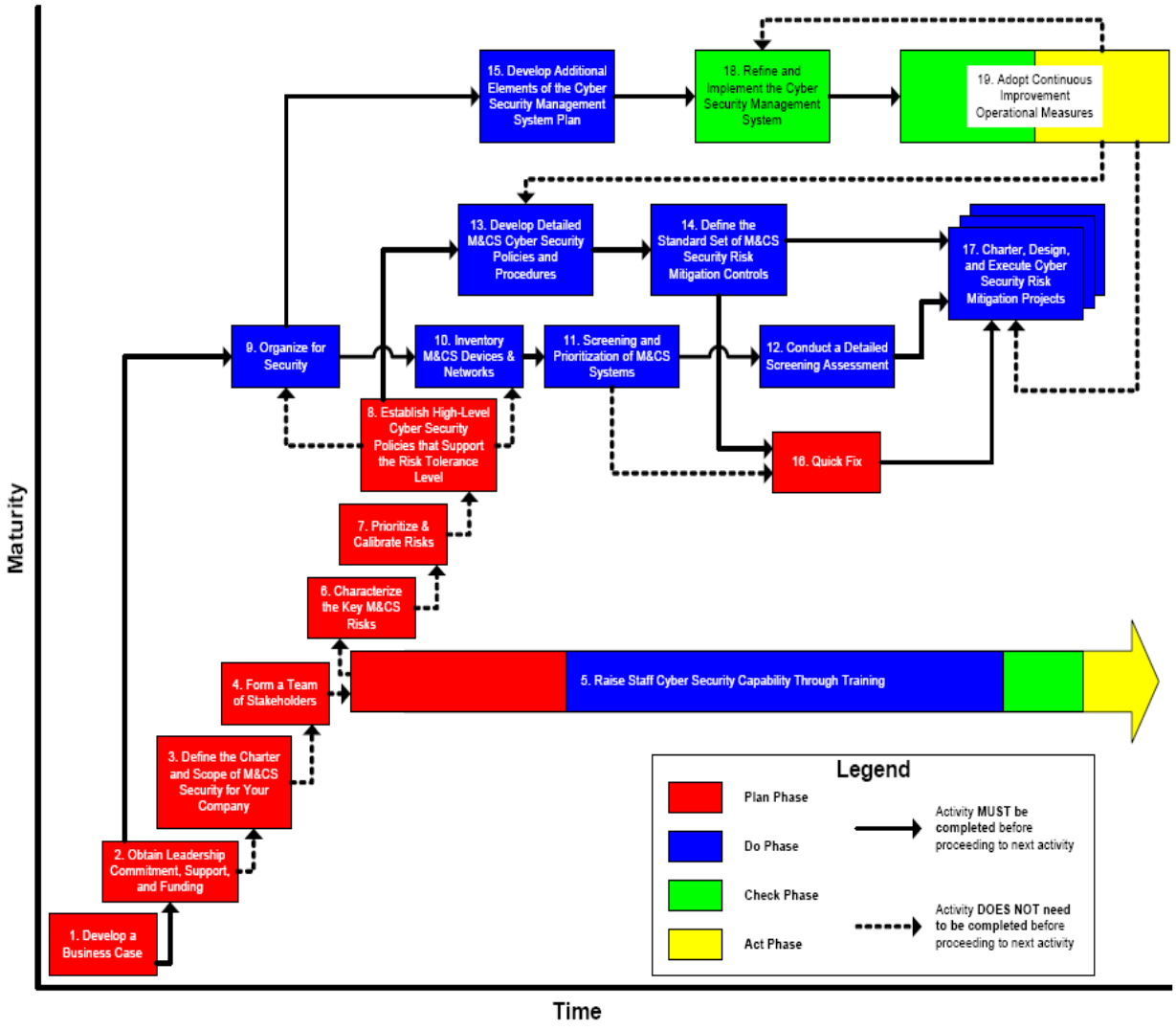


Figura 8. Actividades requeridas para un programa de seguridad expuestas dentro de la Norma ISA 99 Parte 2. ISA 99.00.02 Fig. 8, pág. 33

El presente trabajo de grado se limitará a la fase de **PLAN,** la cual es la más viable para llevar a cabo de acuerdo con el caso de estudio que será detallado en el siguiente capítulo.

Dentro de la empresa caso de estudio se trabajaron las siguientes Actividades para la fase de **PLAN,** los cuales serán detallados a continuación:

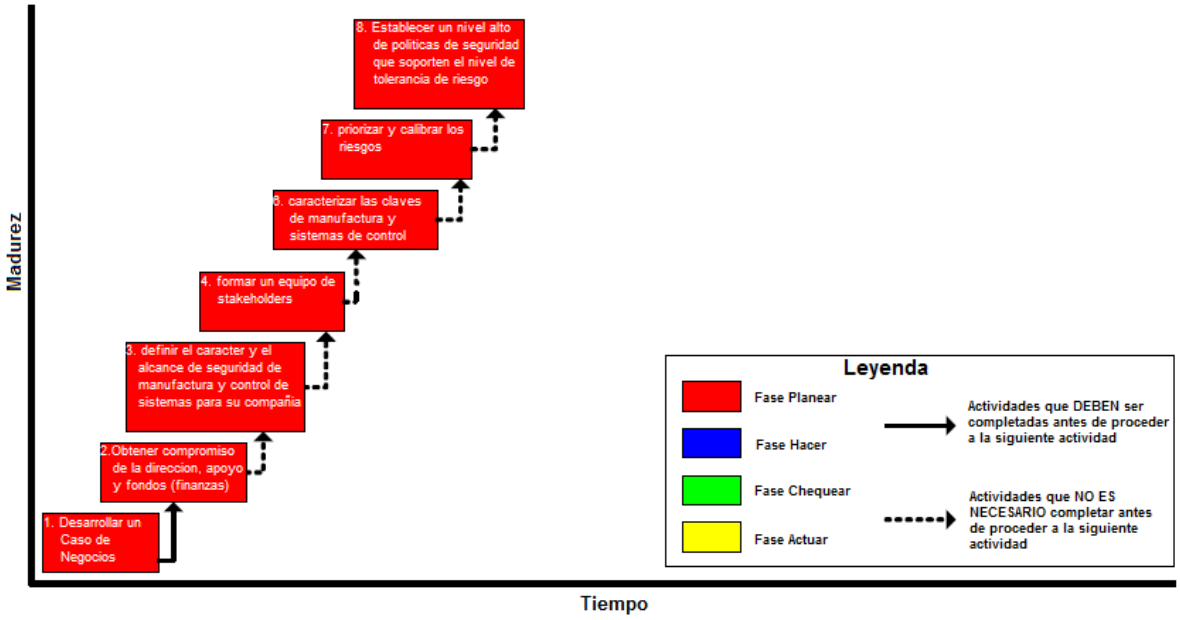


Figura 9. Actividades requeridas para adecuar el programa de Seguridad presente dentro de la Norma ISA 99 en la empresa Caso de Estudio.

1.3.3.1 Actividad 1 - Desarrollar un Caso de Negocios

Los casos de negocios proporcionan la justificación (impacto financiero y de negocio) para crear un programa de *cyber* seguridad integrada. Debe incluir la información detallada sobre:

- Los beneficios de crear un programa de seguridad integrado.
- Los riesgos potenciales si el sistema no se crea.
- Costos y recursos requeridos para desarrollar el programa de seguridad.
- Escenarios de potenciales costos y daños si un sistema no se pone en marcha.

- Una apreciación global de alto nivel de los procesos requeridos para la implementación, operación, supervisión, revisión, mantenimiento y mejoramiento del programa de *cyber* seguridad.

1.3.3.2 Actividad 2 - Obtener Compromiso, Apoyo y Financiación de la Dirección (gerencia)

Presentar el caso de negocio para ser liderado por tecnología de información, sistemas de manufactura y control, cadenas de valor y terceras partes involucradas. Obtener apoyo financiero y soporte de todas las partes involucradas y determinar cómo serán divididos los requerimientos de fondos (financieros) [2].
La dirección de negocios será responsable de aprobar e impulsar las políticas de *cyber* seguridad, asignando roles de seguridad e implementando el programa de seguridad en la compañía.

1.3.3.3 Actividad 3 - Definir el Carácter y Ámbito de Aplicación de la Seguridad de Manufactura y Sistemas de Control (M&CS) para la compañía

Establecer las políticas corporativas que definen los estatutos guías y roles de la organización de seguridad y responsabilidades de los propietarios y los usuarios del sistema. Decidir y documentar los objetivos del sistema de *cyber* seguridad, las organizaciones de negocios afectadas, todos los sistemas de computación y redes involucradas, el presupuesto, recursos requeridos y división de responsabilidades. El alcance también puede dirigirse a los requerimientos de negocio, de ley y regulatorios, calendarios y responsabilidades [2].

1.3.3.4 Actividad 4 - Formar un Equipo de abanderados

El objetivo de un sistema de administración de *cyber* seguridad es un acercamiento integral que involucre los tradicionales sistemas desktop y sistemas computarizados de negocios, sistemas de manufactura y control, y sistemas de cadena de valor que interactúan con los clientes, proveedores y proveedores de transporte. Aun cuando los representantes de estas organizaciones son los abanderados automáticos en el programa de *cyber* seguridad, la lista

de sujetos impactados por incidentes de *cyber* seguridad podría extenderse a un rango amplio de disciplinas y funciones, incluyendo recursos humanos, seguridad y jurídicas [2].

1.3.3.5 Actividad 5 – Elevar la capacidad de *cyber* seguridad del staff mediante capacitación

Instalar un programa de *cyber* seguridad puede traer cambios en la forma en que el personal accesa los programas de computador, las aplicaciones y hasta el propio computador de escritorio. Diseñar efectivos programas de entrenamiento y vehículos de comunicación para ayudar a los empleados a entender por qué se requieren nuevos métodos de acceso y control, ideas que pueden utilizar para reducir los riesgos y el impacto sobre la compañía si los métodos de control no se incorporan. Los programas de entrenamiento demuestran también el compromiso y la valoración de la administración hacia el programa de seguridad [2].

1.3.3.6 Actividad 6 - Caracterizar los riesgos claves de los Sistemas de Manufactura y Control (M&CS)

Cada compañía debe clarificar los riesgos de los sistemas de manufactura y control que ellos están experimentando. Esos riesgos pueden impactar en la compañía de las siguientes maneras:

- Seguridad de personal.
- Pérdida financiera o impacto financiero.
- Consecuencias medioambientales y regulatorias.
- Daños a la imagen de la compañía.
- Impacto a los inversionistas.
- Pérdida de confianza del cliente.
- Impacto a la infraestructura.

1.3.3.7 Actividad 7 - Priorizar y Calibrar los Riesgos

Una vez se clarifican las amenazas, vulnerabilidades y consecuencias, cada escenario necesita ser priorizado y calibrado frente al nivel de tolerancia de riesgo que se ha desarrollado con otros

sistemas de administración de riesgo. Por ejemplo, la organización de administración de riesgo medioambiental de una compañía podría tener ya una escala de severidad que describa qué debe ser considerado como un incidente medioambiental de alta severidad [2].

1.3.3.8 Actividad 8 - Establecer políticas de *cyber* seguridad de alto nivel que soporten el nivel de tolerancia de riesgos

Desarrollar políticas de *cyber* seguridad y obtener la aprobación de las directivas. Comunicar las políticas para que todos entiendan el objetivo de las políticas, cómo obedecerlas y cómo reforzarlas [2].

La mayoría de compañías ya tienen un programa de seguridad y políticas que direccionan activos y prácticas de tecnología de información tradicional. Una política de *cyber* seguridad integrada define y direcciona varios riesgos asociados con los recursos de tecnología de información tradicionales, de igual manera que los sistemas de manufactura y control y otros socios involucrados en la cadena de valor [2].

2. DESCRIPCIÓN DEL CASO DE ESTUDIO (TERMINAL DE CONTENEDORES REFRIGERADOS DE LA SOCIEDAD PORTUARIA DE BUENAVENTURA)

2.1 SOCIEDAD PORTUARIA DE BUENAVENTURA- TERMINAL DE CONTENEDORES REFRIGERADOS

La Sociedad Portuaria de Buenaventura está dentro de los principales puertos marítimos que poseen las mejores rutas marítimas que atraviesan el planeta de norte a sur y de oriente a occidente. Las condiciones geográficas le permiten ser un puerto concentrador y de transbordo, optimizado para uso de barcos de gran porte [8]. En el interior de esta instalación marítima se encuentra ubicado un patio definido únicamente para el uso de aquellos contenedores que transportan alimentos o productos que necesitan refrigeración, conocido como el Patio de Contenedores Refrigerados. A través del patio se encuentra un Sistema de Monitoreo y Supervisión de dicho terminal (Terminal de Contenedores Refrigerados), propiedad de la Sociedad Portuaria Regional de Buenaventura; éste comprende la supervisión de las medidas eléctricas de los tableros de tomas que alimentan a los Contenedores Refrigerados, así como la entrega de Información para la facturación de la energía consumida por éstos. Adicionalmente, este sistema tiene diferentes herramientas que son de gran ayuda para la supervisión y análisis del comportamiento de cada uno de los 384 tomas del patio, que permiten la conexión para la posterior refrigeración de los contenedores.

2.2 SISTEMA DE SUPERVISIÓN Y MONITOREO DEL TERMINAL DE CONTENEDORES REFRIGERADOS DE LA SOCIEDAD PORTUARIA REGIONAL DE BUENAVENTURA S.A.

El Sistema de Supervisión y Monitoreo del Terminal de Contenedores Refrigerados, propiedad de la Sociedad Portuaria Regional de Buenaventura, comprende la supervisión de las medidas eléctricas de los tableros de tomas TT que alimentan a los contenedores refrigerados, así como la entrega de información para la facturación de la energía consumida por éstos.

Adicionalmente este sistema tiene diferentes herramientas que son de gran ayuda para la supervisión y análisis del comportamiento de cada una de las tomas a la cual se le ha asignado

un contenedor refrigerado. A continuación se muestra el diagrama que representa la Arquitectura del sistema de monitoreo.

2.1.1 Arquitectura del sistema de monitoreo

Figura 10. Arquitectura del sistema de monitoreo Terminal de Contenedores Refrigerados

La automatización de este proceso tiene dos redes *Modbus* por cada PLC y cada una de ellas captura las medidas eléctricas correspondientes a 24 medidores multifuncionales tipo *Power Meter*, que se encuentran alojados en los tableros de tomas.

El terminal de contenedores refrigerados tiene 384 tomas distribuidas de la siguiente manera:

- 8 Tableros de distribución, cada uno contiene 48 tomas:

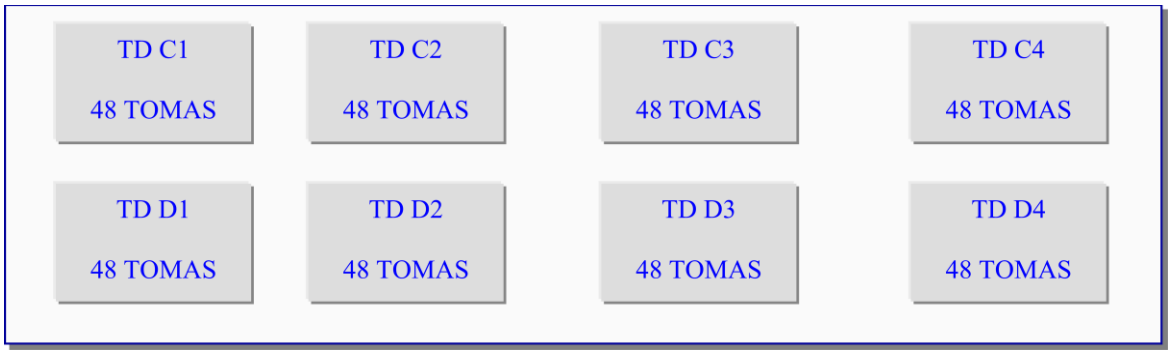


Figura 11. Distribución Tomas Terminal de Contenedores Refrigerados

Los tableros de distribución están dispuestos en dos filas: fila C y fila D, y cuatro columnas: columna 1, columna 2, columna 3, columna 4; con base en esta disposición están identificados de la siguiente manera:

1. TD C1, tablero de distribución ubicado en la fila C columna 1.
2. TD C2, tablero de distribución ubicado en la fila C columna 2.
3. TD C3, tablero de distribución ubicado en la fila C columna 3.
4. TD C4, tablero de distribución ubicado en la fila C columna 4.
5. TD D1, tablero de distribución ubicado en la fila D columna 1.
6. TD D2, tablero de distribución ubicado en la fila D columna 2.
7. TD D3, tablero de distribución ubicado en la fila D columna 3.
8. TD D4, tablero de distribución ubicado en la fila D columna 4.

2.2.2 Tablero de Distribución TD XX

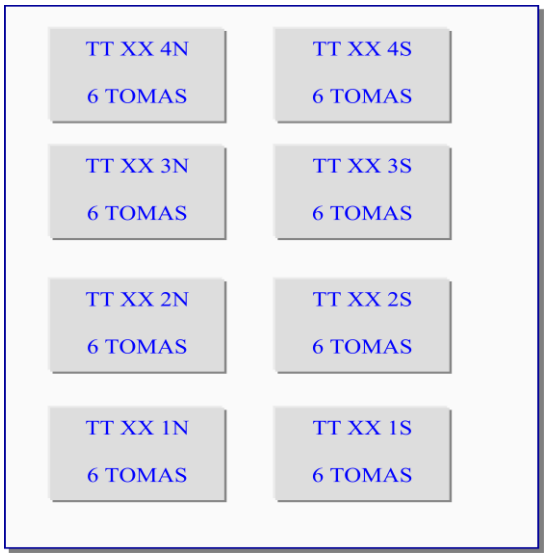


Figura 12. Pantalla tablero de Tomas TD XX

Para el sistema de supervisión y monitoreo del Puerto de Buenaventura se disponen de ocho TC o Tableros Concentradores y cada uno de ellos recoge las señales de un Tablero de Distribución.

En cada tablero concentrador se encuentra alojado un Controlador (PLC) el cual posee un puerto Modbus Plus a través del cual se gestiona la comunicación con la Interfaz Hombre-Máquina y dos puertos Modbus: el primero de ellos se comunica con todos los Medidores Multifuncionales ubicados en los tableros de tomas zona norte. Ejemplo: Si el tablero de concentrador corresponde al tablero de distribución TD C1 entonces este puerto de comunicación Modbus recoge las señales de las tomas ubicadas en los siguientes tableros de tomas: TT C1 1N, TT C1 2N, TT C1 3N, TT C1 4N.

Los tableros de tomas están dispuestos en los tableros de distribución; dentro de cada tablero de distribución los tableros de tomas están distribuidos en 4 niveles y dentro de cada nivel están organizados en dos zonas: norte y sur.

1. TT XX 1N, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 1, zona Norte.

2. TT XX 1S, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 1, zona Sur.

3. TT XX 2N, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 2, zona Norte.

4. TT XX 2S, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 2, zona Sur.

5. TT XX 3N, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 3, zona Norte.

6. TT XX 3S, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 3, zona Sur.

7. TT XX 4N, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 4, zona Norte.

8. TT XX 4S, tablero de tomas ubicado en el tablero de distribución que se encuentra en la fila F, columna C, nivel 4, zona Sur.

Finalmente cada tablero de tomas contiene 6 tomas y cada una de ellas tiene asociado un Medidor Multifuncional.

TT XX 1N

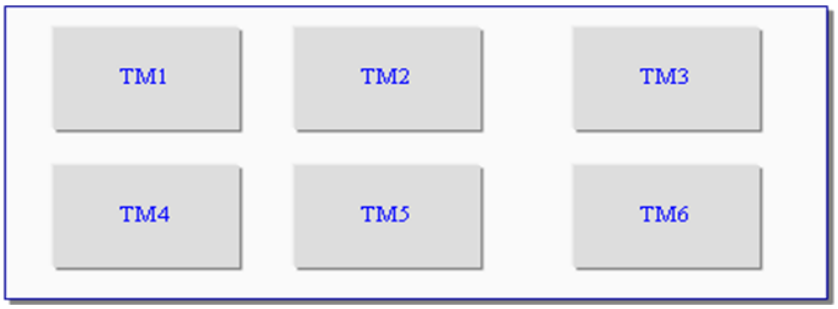


Figura 13. tablero de tomas TT XX 1N

A continuación se ilustra un ejemplo de la distribución de los tomas del Terminal de Contenedores Refrigerados para un mayor entendimiento de este ítem:

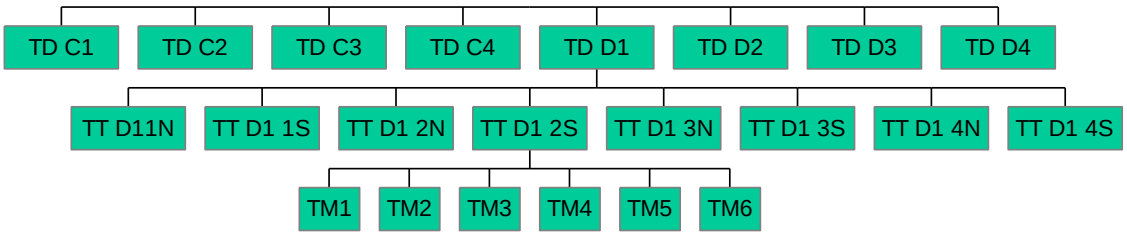


Figura 14. Distribución de Tomas

2.2.3 Comunicaciones

2.2.3.1 Protocolo MODBUS

Es un protocolo que fue creado por Modicon y es un protocolo estándar. Este protocolo define un mensaje con una estructura que los equipos reconocen y utilizan, acorde con el tipo de red en la cual están estableciendo comunicación. Esta estructura proporciona las herramientas necesarias para que un controlador haga peticiones de lectura o escritura a los medidores multifuncionales y para que éstos, a su vez, respondan a esas peticiones, reportando a su vez errores que se hayan detectado en el proceso de comunicación.

Durante las comunicaciones en una red Modbus, el protocolo determina cómo cada medidor multifuncional reconoce en su propia dirección en la red un mensaje que haya sido direccionado hacia él.

Características:

- Capa de Aplicación MBAP (Modbus Aplication Protocol)
- Sólo permite 2 tipos de Objetos: bits y registros.
- Cada objeto puede ser de entrada o salida.
- Los objetos de salida pueden ser salidas físicas o posiciones de memoria.
- Protocolo de 3 capas (Física, enlace y aplicación).
- Capa física RS232/RS422/RS485.
- Half dúplex.
- Velocidad de Transmisión de 1200 a 19200 Bps.
- Hasta 32 dispositivos.

2.2.3.2 Protocolo MODBUS PLUS

En este tipo de protocolo se habla de la técnica “peer to peer”, que puede interpretarse como Maestro flotante. Esto implica que el dispositivo dentro de la red que lleve el token en un momento dado podrá comportarse como maestro o esclavo, en la medida que puede o no iniciar transacciones con otros dispositivos de la red. Adicionalmente es importante saber que en Modbus Plus la velocidad de transmisión de los datos es única y corresponde a 1Mbs.

Características:

- Protocolo de 3 capas (Física, enlace y aplicación).
- Capa física RS485 o Fibra óptica.
- *Peer to Peer*.
- Velocidad de Transmisión de 1 Mbps.
- *Token Pass*.
- No existe maestro, ni esclavos.
- Hasta 64 Estaciones.

2.2.4 Software de programación de los controladores (PL7-PRO)

El software utilizado para la programación de los TSX Premium es el PL7-Pro; a continuación se describe el tratamiento general de las funciones por el programa PL7.

2.2.4.1 Inicio de un programa

Pantalla de Inicio para la configuración de los PLC's mediante el Software PL7 de Schnneider Electronics; aquí en la pantalla aparecen las configuraciones para seleccionar cuál será el *Procesador y la tarjeta de memoria* que utilizar.

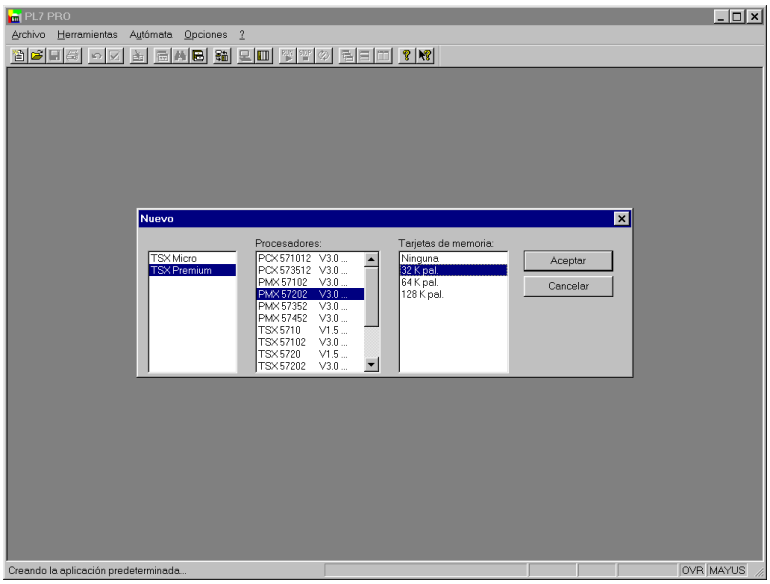


Figura 15. Pantalla de configuración PLC

2.2.4.2 **Configuración de los módulos**

Para configurar los módulos que van integrados en el Controlador, se selecciona la siguiente pantalla y se accede a las pestañas de Configuración y luego se ingresa a Configuración Hardware.

Aparece entonces en la pantalla una ventana con los racks de dos tarjetas, la fuente PSY 2600, el procesador y las expansiones para las que serán las tarjetas de los módulos.

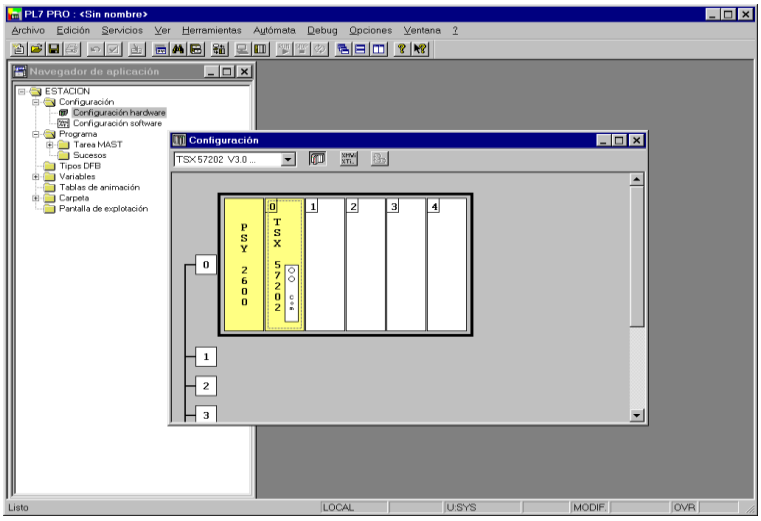
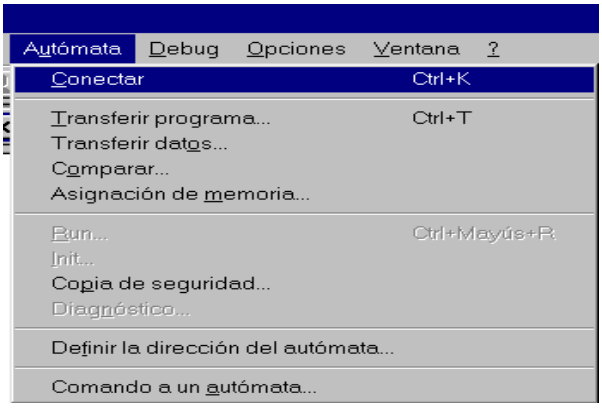


Figura 16. Pantalla de configuración de los módulos

Figura 16.1 Pantalla de configuración de los módulos, Selección Slots

2.2.4.3 Conexión con el controlador

Para realizar la comunicación entre la consola de programación y el Controlador para efectos de ver el programa que se encuentra en el PLC o para introducir el programa de la consola de programación al Controlador se debe tener un cable referencia TSXPCU1030 y conectarse al puerto TER del Controlador ubicado en el procesador del mismo y al puerto COM 1 de la consola de programación.



Conectar:

Con esta opción se conecta el Controlador en línea con la consola de programación y se puede observar el estado de las diferentes variables implementadas en el Controlador.

Figura 17. Pantalla de opción para conectar el controlador

Transferir Programa:

Con esta opción se puede transferir el programa desde:

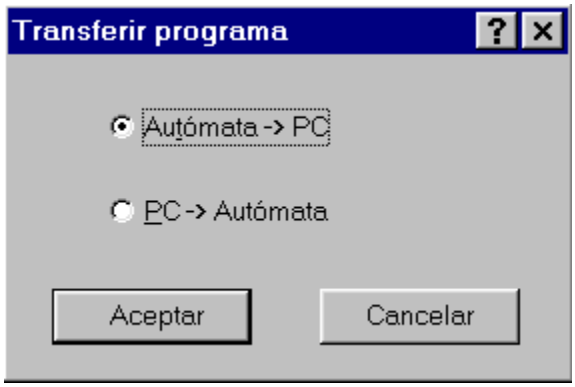


Figura 17.1. Pantalla de opción para conectar el controlador, Selección Autómata

2.2.4.4 Creación de tablas de animación

La creación de tablas es un procedimiento importante para visualizar el estado de las diferentes variables cuando se encuentra conectado ON LINE con el controlador. A continuación se muestra la pantalla que permite la creación de tablas de animación

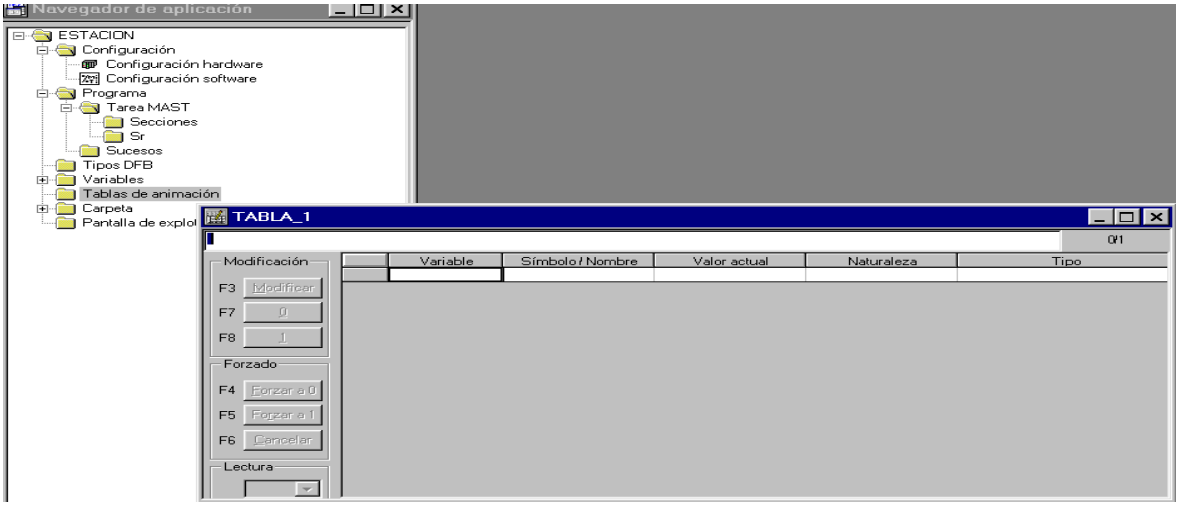


Figura 18. Pantalla de creación de tablas de animación

2.2.5 VENTANAS SISTEMA DE SUPERVISIÓN

2.2.5.1 Despliegue de presentación

Figura 19. Pantalla de ventana de despliegue de presentación

2.2.5.2 Tablero de tomas xx

Figura 20. Pantalla de tablero de tomas XX

Este despliegue muestra los componentes de un tablero de distribución del cual se alimentan 8 tableros de tomas y 2 reservas instaladas.

A continuación se realiza una descripción más detallada de los elementos que conforman este despliegue:

***** El botón con una flecha hacia abajo se acciona al hacer clic sobre él o al pulsar la tecla PgDown. Este botón permite visualizar el unifilar del tablero de distribución anterior (de acuerdo con la ubicación de este tablero).

Ejemplo: Si se encuentra ubicado en el despliegue del tablero de distribución TD D3 y pulsa este botón, entonces aparece en la pantalla el tablero de distribución TD D2.

***** El botón con una flecha hacia arriba se acciona al hacer clic sobre él o al pulsar la tecla PgUp. Este botón permite visualizar el unifilar del tablero de distribución siguiente (de acuerdo con la ubicación de este tablero).

Ejemplo: Si se encuentra ubicado en el despliegue del tablero de distribución TD C4 y pulsa este botón, entonces aparece en la pantalla el tablero de distribución TD D1.

***** El botón EQUIPOS se acciona al dar clic sobre éste o al pulsar las teclas SHIFT-ENTER. Este botón permite ingresar al despliegue ASIGNACIÓN DE TOMAS.

2.2.5.3 MEDIDAS TOMA XX

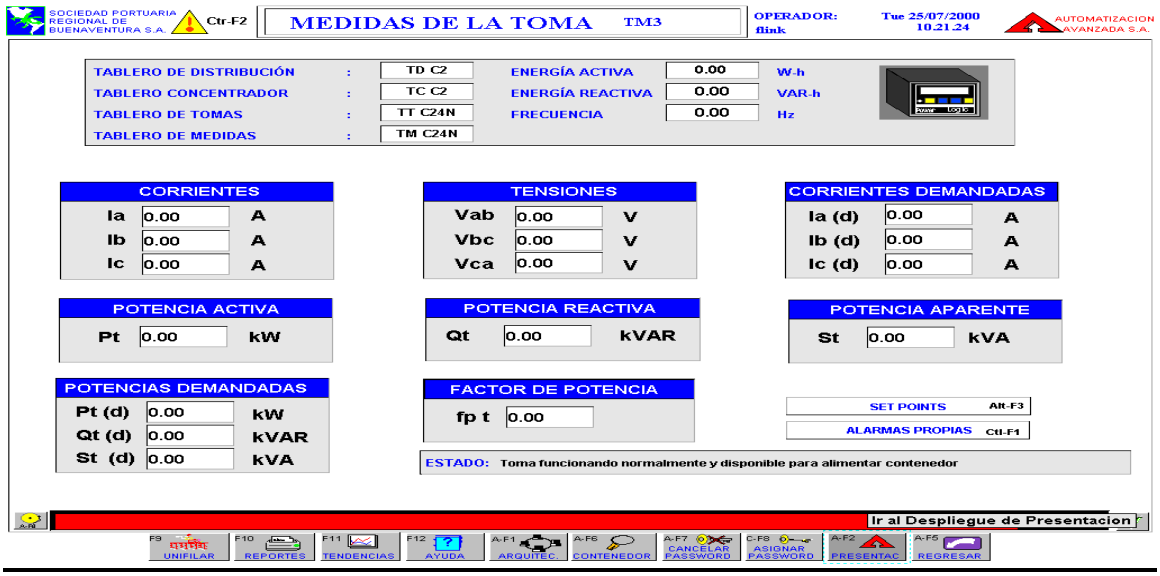


Figura 21 Pantalla de Medida de tomas

En este despliegue se observa un diagrama unifilar de un tablero de tomas escogido previamente.

CONVENCIONES:

- Medidor Multifuncional fondo Gris, si la toma está funcionando en condiciones normales y está disponible para alimentar un contenedor refrigerado.

- Medidor Multifuncional fondo Verde, si la toma está funcionando en condiciones normales y ya está alimentando un contenedor refrigerado.

- Medidor Multifuncional fondo Naranja, si se ha asignado la entrada de un contenedor a la toma y aún no se encuentra entregando energía.

- Medidor Multifuncional fondo Naranja Intermitente, si no se ha asignado la entrada de un contenedor a la toma o se ha registrado la salida de un contenedor asociado a la toma y ésta se encuentra entregando energía.

Medidor Multifuncional fondo Rojo Intermitente, si en la toma existe cualquier condición anómala con sus parámetros eléctricos corrientes, tensiones y frecuencia.

- Medidor Multifuncional tachado por una Equis Roja Intermitente, si se presenta pérdida de comunicaciones con el Power Meter asociado a la toma.

En los demás recuadros se encuentra la siguiente información:

***** Corrientes: Allí se visualiza el valor de las corrientes de la fases A-B-C

***** Tensiones: Allí se visualiza el valor de los voltajes: Vab-Vbc-Vca.

***** Corrientes Demandadas: Allí se visualiza el valor de las corrientes demandadas de las fases A-B-C.

***** Potencia Activa: Allí se visualiza el valor de la potencia activa de esta toma.

***** Potencia Reactiva: Allí se visualiza el valor de la potencia reactiva de esta toma.

***** Potencia Aparente: Allí se visualiza el valor de la potencia aparente de esta toma.

***** Potencia Demandada: Allí se visualiza el valor de las potencias activa, reactiva y aparente demandadas por esta toma.

***** Factor de Potencia: Allí se visualiza el valor del factor de potencia de esta toma.

SET-POINT: A continuación aparece en la pantalla una ventana, en la cual se puede parametrizar los siguientes límites:

-Límite Inferior de Tensión

-Límite Superior de Tensión

-Límite Inferior de Corriente

-Límite Superior de Corriente

-Límite Inferior de Frecuencia

-Límite Superior de Frecuencia

Figura 22. Pantalla de límites de corriente tensión frecuencia

2.2.5.4 Alarmas

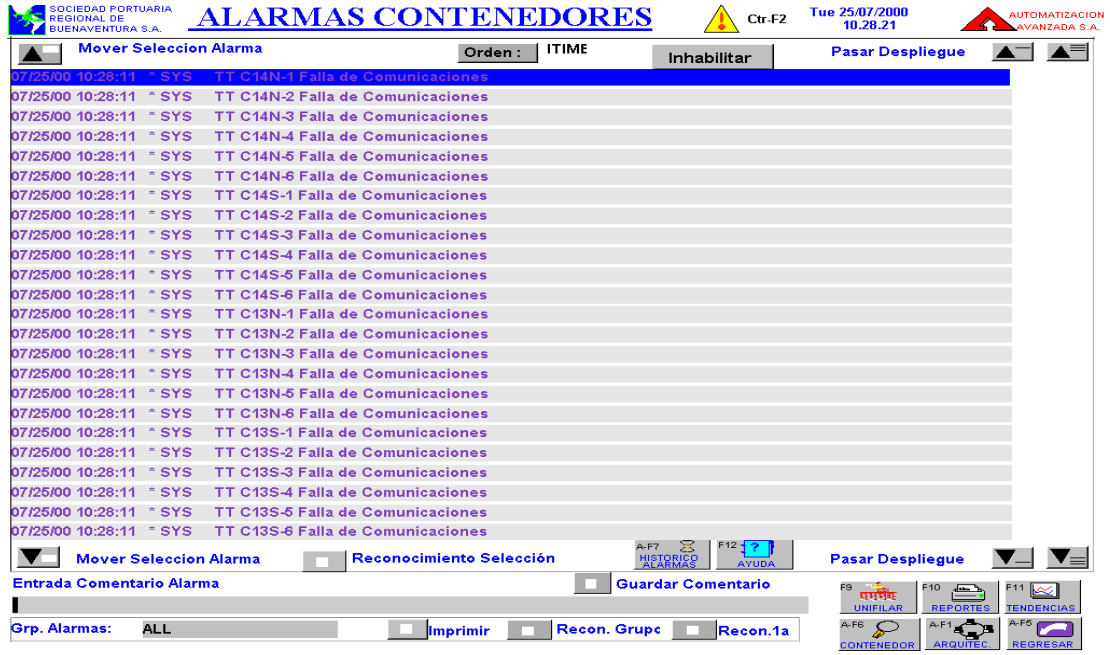


Figura 23. Pantalla de alarmas del patio de contenedores

La tarea de alarmas identifica las condiciones de funcionamiento anormales del sistema e informa de ello al operador mediante mensajes y alarmas sonoras.

El sistema supervisor de alarmas tiene las siguientes funciones:

- Asignación de un orden de prioridad a las alarmas.
- Inhibición selectiva de las alarmas por el supervisor.
- Selección según hora de aparición o prioridad.
- Registro de alarmas en un archivo histórico.
- Asignación de la prioridad de alarmas.
- Ordenamiento de alarmas por tiempo en forma cronológica.
- Muestra de condición de las alarmas y mensajes.
- Muestra del sumario de todas las alarmas activas y mensajes.

- Reconocimiento y limpieza de las alarmas.

- Impresión de las alarmas y mensajes.

2.2.5.5 Tendencias

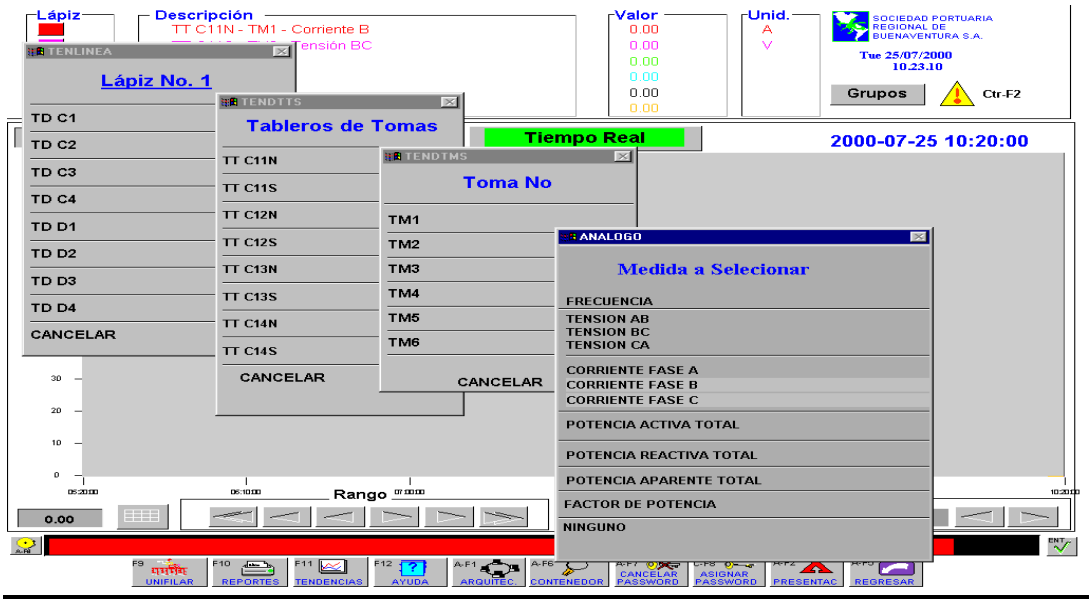


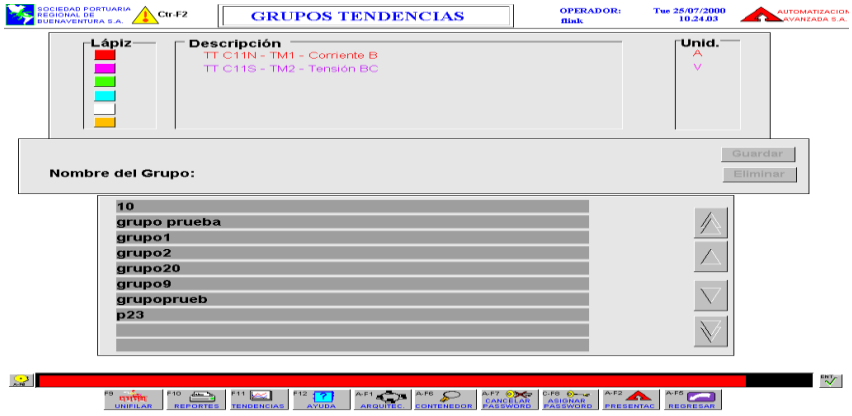
Figura 24**.** Pantalla de tendencias del Patio de Contenedores Refrigerados

Este despliegue permite observar los valores de medición que son desplegados en gráficos que representan el comportamiento de la medida con respecto al tiempo.

Esta representación puede ser histórica o en tiempo real, y permite un análisis visual de la evolución de las medidas durante un período de tiempo deseado.

- *GRUPOS TENDENCIAS*

La funcionalidad de este despliegue es poder organizar diferentes grupos de medidas evitando la necesidad de estar siempre configurando la carta de colores en el despliegue de Tendencias



. Figura 25. Pantalla de grupos de tendencias

2.2.5.6 Reportes

Figura 26. pantalla de reporte sobre laactualidad de los contenedores

Los reportes son guardados en archivos de texto, lo cual permite su posterior edición desde cualquier editor de texto, con el fin de adicionar comentarios o ser insertados en formatos internos de informes de operación.

El reporte está comprendido por los siguientes ítems:

-FECHA DEL REPORTE

-NÚMERO DE AUTORIZACIÓN: Éste es un código de entrada del contenedor asignado por el ASPA.

-HORA Y FECHA DE ENTRADA DEL CONTENEDOR.

-HORA Y FECHA DE SALIDA DEL CONTENEDOR.

-ENERGÍA CONSUMIDA POR EL CONTENEDOR.

-NÚMERO DE PLACA DEL CONTENEDOR.

-NOMBRE DE LA TOMA A LA CUAL FUE ASIGNADA EL CONTENEDOR.

2.2.5.7 CONTENEDORES

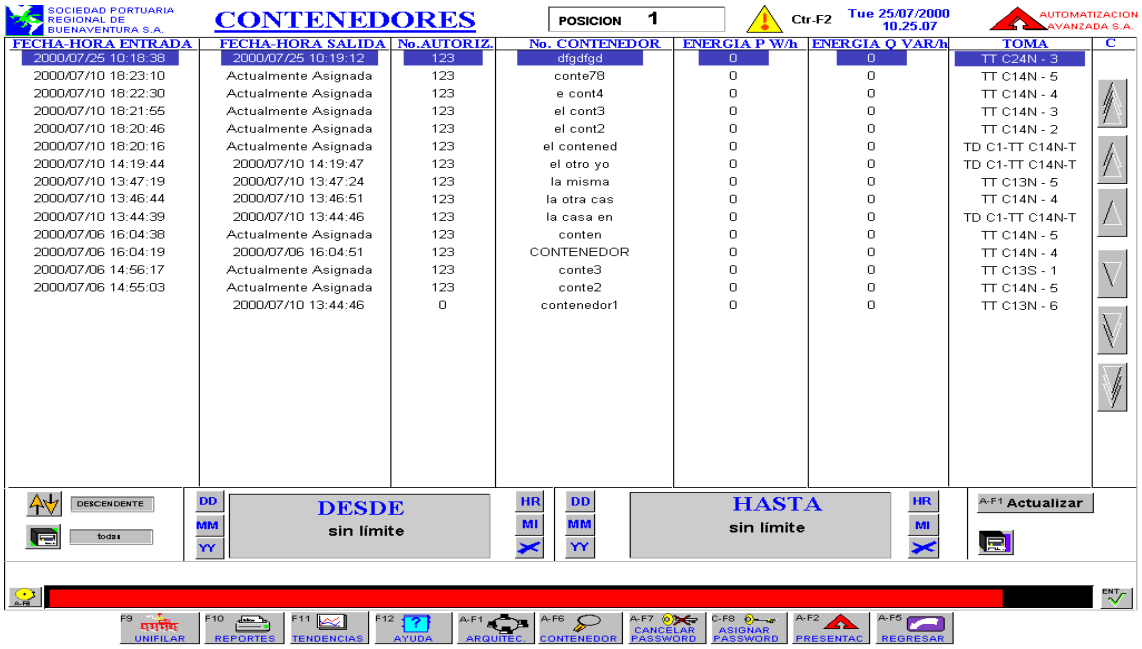


Figura 27. Pantalla de reportes patio de contenedores

En este despliegue se puede observar cuáles tomas están asignadas en el momento, cuáles fueron asignadas y ya fueron desasignadas en cierto periodo de tiempo, el cual puede ser parametrizado de igual manera que el histórico de alarmas.

Este despliegue consta de seis columnas:

-HORA Y FECHA DE ENTRADA DEL CONTENEDOR.

-HORA Y FECHA DE SALIDA DEL CONTENEDOR.

-NÚMERO DE AUTORIZACIÓN: Éste es un código de entrada del contenedor asignado por el ASPA.

-NÚMERO DE PLACA DEL CONTENEDOR.

-ENERGÍA CONSUMIDA POR EL CONTENEDOR.

-NOMBRE DE LA TOMA A LA CUAL FUE ASIGNADA EL CONTENEDOR.

2.3 Software portuario “Cosmos”: Es un software portuario diseñado para suplir las necesidades de planeación y administración del espacio de los patios de contenedores, generando un mayor rendimiento en las áreas de almacenamiento y control de movimientos de las grúas RTGs, guarda y registra las operaciones que se le realiza a cada contenedor, actualiza y valida en línea los datos en tiempo real de toda la información de contenedores, carga a granel y general tanto en ubicación como en saldos de averías, pesos y sellos. Además agiliza los procesos de recepción y documentación vía EDI, Internet o fax. Brindando así una mayor seguridad y confiabilidad a la comunidad portuaria y a los agentes que intervienen en su fusión tales como: Autoridades, SIAS, Agencia Navieras, Operadores Portuarios, Compañía transportadoras, Importadores y Exportadores etc. [8].

3. GUÍA DE IMPLEMETACIÓN DE LA FASE DE PLAN DE UN PROGRAMA DE CYBER-SEGURIDAD SEGÚN LA NORMA ISA 99

La presente Guía abarca empresas tanto de Automatización Industrial y Sistemas de Control como de gases y combustibles, empresas textiles, empresas de alimentos, empresas de desarrollo de Ingeniería y Aplicaciones Industriales, entre otras; se da por entendido que dentro de estos tipos de ámbitos empresariales (Automatización Industrial y Sistemas de Control) se incluyen tanto las empresas de Servicios (por ejemplo empresas de desarrollo de Software), como las empresas de Bienes (por ejemplo empresas dedicadas a la producción de un producto determinado).

RECOMENDACIONES

Se recomienda a la persona o personal de la compañía que deseen seguir esta guía, leer y tener en cuenta las siguientes recomendaciones:

- Preparación: Para preparar el personal que integra la compañía, así como la parte física en cuanto al tema de seguridad informática, es conveniente:
    - Antes de aplicar esta guía leerla detalladamente y observar cómo se encuentran las condiciones en cuanto a *cyber* seguridad en la empresa.
    - Analice cada uno de los pasos en esta guía para observar cuales son convenientes de implementar, si no todos son necesarios.
    - Desarrolle esta guía de manera consiente a fin de obtener los resultados que Ud. desea y su compañía requiere.
- Acompañamiento: Durante el desarrollo de la presente guía se detallan procedimientos y ejemplos para poder entender y llevar a cabo los pasos descritos hacia la adecuación de modelos, actividades y elementos claves dentro de la fase de PLAN de un programa de *cyber*-seguridad según la norma ISA 99.

- Seguimiento: Al considerar la utilización de esta guía de adecuación se recomienda al personal que estará a cargo de implementarla y alcanzar las medidas de seguridad informática óptimas para el nivel actual de la empresa, tenga en cuenta:

  - Cuando se cumpla paulatinamente con los pasos aquí descritos incluir en una bitácora el cumplimiento de determinado paso y cuáles fueron sus resultados.

  - Durante el desarrollo de la guía llevar un seguimiento de los riesgos presentes que hayan sido reducidos y eliminados, para así considerar dentro de futuros casos cuáles medidas ya han sido implementadas con éxito.

  - El seguimiento de las actividades que se haga al equipo de trabajo a cargo de la seguridad informática por parte del personal o persona que se propuso adecuar esta guía, constituirá un aporte muy importante para alcanzar la meta establecida.

  - Desarrollar cada paso como se plantea en la guía no es obligatorio, pero sí es importante que realice las etapas que considere faltan en la empresa y con las cuales se determinen y fortalezcan las medidas de seguridad.

GUÍA DE IMPLEMENTACIÓN

3.1 Conocimiento de la Empresa:

Este paso es primordial y fundamental para el desarrollo de la presente guía, debido a que la persona o personas que deseen plantear medidas y procedimientos de seguridad deben tener claro el funcionamiento tanto operacional como informacional de la empresa o compañía, donde desee PLANEAR un Programa de *Cyber*-Seguridad según la Norma ISA 99. Conocer la empresa implica tener claro el funcionamiento de cada uno de los procesos tanto operacionales como de flujo de información, que se efectúan entre cada nivel (si los niveles están identificados) y que permiten llevar a cabo el objetivo de la empresa.

3.2 Sustentación de la importancia de la *Cyber* seguridad en la empresa:

Aquí se busca explicar a los directivos de la empresa acerca de la importancia de la cyber seguridad; con esto se busca alcanzar un convencimiento por parte de la directiva, de que si no se adoptan medidas y procedimientos para proteger la información es posible que ocurran graves inconvenientes. Es conveniente que los canales de comunicación con las directivas les permitan entender el objetivo de Planear y Adecuar un programa de Cyber Seguridad para mantener el flujo informacional entre la producción de planta, los reportes administrativos y financieros del sistema de negocios. Este paso se puede realizar mediante las siguientes pautas:

- Reunión con los Directivos de la Empresa.
- Reunión con los Jefes de Departamento.
- Reunión con los Jefes de Zona.
- Reunión con los Supervisores de Área.

3.3 Creación del Equipo de Trabajo:

Como resultado del convencimiento de los Directivos en la etapa realizada en el paso anterior, se debe deducir la necesidad de contar con un grupo humano que desee y pueda suministrar los conocimientos necesarios concernientes a *cyber* seguridad dentro del área de la empresa en la cual se pretende instaurar un programa de seguridad informática. Este grupo de trabajo puede estar compuesto por:

- Personal de sistemas de control.
- Personal de atención al cliente.
- Personal de telecomunicaciones.
- Personal de sistemas de información.
- Personal de recursos humanos.
- Personal del campo jurídico.

3.4 Capacitación del Grupo de Trabajo:

Luego de la creación del grupo de trabajo y de tener certeza del compromiso del personal que desempeñará esta labor, es fundamental capacitar al personal acerca de los conocimientos entregados por la norma ISA 99, proceso mediante el cual se explicarán los Conceptos, Modelos, Terminología, Elementos Claves y Actividades que constituyen la fase de PLAN. En esta etapa es conveniente evaluar el grado de conocimiento previo que posee el grupo acerca de Seguridad a fin de determinar el nivel de entrenamiento. A continuación se presentan algunas pautas para el entrenamiento:

- Definir el nivel de entrenamiento del grupo de trabajo.

  Establecer las virtudes y debilidades que en cuanto al conocimiento de *cyber* seguridad posee el grupo de trabajo.

- Definir niveles de entrenamiento personalizado.

  Aquí se propone qué profundidad en cuanto a conocimientos dentro de la fase de PLAN tendrá el entrenamiento según el personal; por ejemplo, el personal de Telecomunicaciones y sistemas de control requerirán un nivel más bajo en cuanto a información, entre tanto que el personal de recursos humanos y/o jurídico requiere de mayor información.

3.5 Identificación de Recursos protegibles:

En este paso se pretende tener una idea de todos los recursos de la empresa que deberían ser protegidos para garantizar el funcionamiento de un sistema de manufactura o un sistema de control, dado que no se puede pretender desarrollar un sistema de administración de *cyber* seguridad si no se sabe con claridad qué es lo que se desea proteger, es decir, los recursos que desean protegerse. Esta etapa debe ser efectuada por el Equipo de Trabajo en Seguridad Informacional. La manera de realizar esta identificación es por medio de una lista de recursos que debe ser regularmente actualizada y puede considerar los siguientes aspectos:

- Hardware: servidores, sensores, PLCs, enrutadores, puentes módems, PC'S, estaciones de trabajo, etc.

- Software: aplicaciones de red, programas de comunicación, supervisorios, software de programación, etc.
- Datos: durante la ejecución, almacenamientos en línea, de auditoría, bases de datos, en tránsito, sobre medios de comunicación, etc.
- Comunicaciones: medios de comunicación de información.
- Personas: usuarios, personal para operación y mantenimiento, administradores del sistema de manufactura o sistemas de control.
- Documentación: sobre programas, hardware, sistemas, procedimientos, recetas de producción, Políticas de Seguridad Informacional.

3.6 Selección de Recursos objeto de protección:

Una vez identificados los recursos protegibles al interior de la empresa, es adecuado seleccionar aquellos recursos físicos y lógicos a los que sea conveniente aplicar seguridad. Con esto se busca proteger los recursos sensibles y críticos del sistema, y de igual manera aquéllos que puedan ser víctimas de ataques a medio y largo plazo, estos recursos deben ser aquellos donde se necesitan implementar primariamente las medidas de seguridad y los cuales estarán catalogados como de mayor importancia. A continuación se lista una serie de recursos de vital importancia que puede servir de apoyo para esta selección:

- Comunicaciones: medios de comunicación de información.
- Hardware: Servidores, sensores, computadoras, PLCs, estaciones de trabajo, etc.
- Software: Aplicaciones de Red, supervisorios, software de programación, etc.
- Datos: Durante ejecución, bases de datos, almacenamiento en línea, etc.

3.7 Definición de la estructura Global de la Empresa:

A través de los diagramas de Modelos presentados por la norma ISA 99 se describe el concepto general de la organización, la relación entre los recursos de la empresa, la agrupación lógica de los recursos al interior de la empresa y los medios de comunicación que permiten el flujo de información entre los recursos. Para obtener las definiciones de los modelos referirse al capítulo 1 de este documento. A continuación se recomienda seguir el siguiente orden de adecuación para estos modelos:

1. Modelo de Referencia: es necesario que este modelo sea el primero en desarrollar dado que permite tener una concepto general de la empresa

2. Modelo de Activos: luego de entender el funcionamiento general de la empresa es necesario desarrollar el modelo de activos, dado que el fin de este modelo es mostrar cómo se relacionan los recursos importantes de la empresa y la forma que se puede acceder informacionalmente a cada uno de ellos.

3. Arquitectura de Referencia: después de haber identificado los recursos importantes de la empresa y la forma de acceder a cada uno de ellos es pertinente desarrollar una arquitecta de referencia que permita mostrar un diagrama de distribución jerárquica de la empresa en función de sus procesos informacionales.

4. Modelo de Zona y Conducto. Luego de realizar la distribución jerárquica de la empresa es necesario realizar una agrupación de recursos con características comunes concernientes a los objetivos de seguridad (Disponibilidad, Integridad y Confidencialidad) y detallar los medios de comunicación que permiten el flujo informacional de los recursos dentro y fuera de las zonas.

3.8 Identificación de Recursos al interior de la Estructura Global de la Empresa:

Después de tener los diagramas que representan la funcionalidad de la empresa se debe identificar dentro de estos diagramas (modelos) los recursos que deben ser protegidos, a fin determinar a qué nivel de la empresa pertenece cada recurso y qué actividades dentro de la empresa realiza este recurso. A continuación se describe cómo realizar esta etapa:

- Observar qué actividad realiza el recurso.

- Detallar con qué otros recursos comparte información.

- Identificar si comparte datos de información o datos de proceso.
- Definir a qué nivel de la empresa pertenece el recurso de acuerdo con el tipo de información que comparta y su actividad.

3.9 Agrupación de Recursos de acuerdo con su Funcionalidad:

Una vez se realice la adecuación del modelo de zona de seguridad es conveniente distinguir los recursos con base a las zonas de acuerdo con su funcionalidad en el sistema de control y manufactura. Se mencionan algunos ejemplos:

- Recursos para Control de Nivel (sensores, válvulas, etc.).
- Recursos para Control de Movimiento (variadores de velocidad, servomotores).
- Recursos de Control Programable (PLC, DCS, RTU).
- Recursos de Supervisión (HMI, Pantallas, PC Industriales, etc.).

3.10 Identificación de los Riesgos en los recursos de procesos de manufactura y control:

Aquí se procede a identificar los riesgos presentados en los recursos mediante el conocimiento de las vulnerabilidades, amenazas y consecuencias. Para efectuar este paso de la guía se necesita cumplir con los siguientes pasos (3.11, 3.12 y 3.13) a fin de determinar los riesgos.

3.11 Determinar las Vulnerabilidades en los recursos de procesos de manufactura y control:

Este paso consiste en conocer las diferentes fallas que se hayan presentado por pérdida de los Objetivos de Seguridad (Disponibilidad, Integridad y Confidencialidad) para las zonas de seguridad y sus recursos definidos en el paso anterior. Esto es posible a través de las siguientes pautas:

- Si se posee una herramienta software para la Administración de Operaciones de los Equipos es posible determinar dichas vulnerabilidades de acuerdo con su rendimiento.

- Mediante la comunicación con el personal encargado del proceso poder conocer el historial de fallas y obtener reportes acerca de las causas de estas fallas.

Luego de identificada la(s) vulnerabilidad(s) se debe proceder a determinar qué vulnerabilidades afectaron directamente el sistema.

3.12 Establecer las Amenazas en los recursos de procesos de manufactura y control:

Con la realización de este paso se conocen las acciones que pueden atentar negativamente contra las Vulnerabilidades en los procesos informacionales de la empresa. Tales amenazas pueden estar incluidas en los siguientes tipos:

1. Amenazas Naturales: no están dirigidas a los elementos de la aplicación ni sistemas de información, incluyen principalmente desastres naturales que pueden afectar de una manera u otra el normal desempeño de los procesos informacionales [15].

2. Amenazas Accidentales: Estas son las más comunes en los procesos informacionales de hoy, estas pueden ser causadas por un acceso no autorizado tales como errores de usuario, errores de los operarios, errores administrativos (instalación y configuración), datos mal preparados, errores en direccionamiento, errores del sistema, entre otros [15].

3. Amenazas Deliberadas: son de tipo activas y pasivas: las activas son las que incluyen accesos no autorizados, modificaciones no autorizadas, sabotaje, etc., en tanto que las pasivas son de naturaleza mucho mas técnica; dentro de éstas se encuentran: emanaciones electromagnéticas que pueden dañar la información sobre una red, microondas de interferencia, ruptura de cableado e información mal protegida [15].

Luego de identificado el tipo de amenaza se debe proceder a determinar qué amenaza se presentó al interior del sistema.

3.13 Estipular las Posibles Consecuencias en los recursos de procesos de manufactura y control:

Este paso se refiere a los posibles impactos que pueden suceder si las amenazas del sistema atacan las vulnerabilidades. Estos impactos pueden afectar los siguientes aspectos:

- Planificación continúa de negocios: ésta se refiere a la posible interrupción en el funcionamiento de un sitio de la empresa y sus repercusiones en el funcionamiento de la empresa.
- Seguridad de la información: aquí se hace referencia a las consecuencias relacionadas con las pérdidas económicas, conflictos legales y pérdida de imagen por parte de la compañía ante el incumplimiento de las necesidades de los socios.
- Seguridad de procesos: ésta hace referencia a consecuencias relacionadas con personal interno y externo de la compañía.
- Seguridad ambiental: es referida a conflictos con instituciones regionales o internacionales de carácter ambiental, ante daños ocasionados al medio ambiente.

Luego de identificado el aspecto de consecuencia se debe proceder a determinar qué consecuencia se presentó al interior del sistema.

3.14 Determinar el Riesgo en los recursos de los procesos de manufactura y control:

Luego de haber realizado los pasos 3.11, 3.12 y 3.13, se procede a evaluar estos riesgos de acuerdo con la apreciación de que el Riesgo es la Probabilidad de que una amenaza ataque una vulnerabilidad y sus posibles impactos al sistema de manufactura y control. En este paso se debe tener una(s) serie(s) de Riesgos por los cuales se establecerán las medidas de seguridad.

3.15 Determinar las Medidas de Seguridad que permitan Mitigar los Riesgos:

Este es un paso importante dentro de la guía de implementación. Por medio de éste se definen las medidas que se consideran necesarias y obligatorias para mitigar los riesgos encontrados con anterioridad; es así como dichas medidas se pueden evaluar de acuerdo con el lugar de la

empresa donde se presente el riesgo. A continuación se nombra algunas tipos de medidas que servirían de ejemplo de acuerdo con el lugar:

- En el Nivel de Administración de Operaciones: dichas medidas van tendientes a evitar, disminuir errores y pérdidas en la producción, referentes a la confidencialidad de la información, como son: uso de contraseñas para almacenar información, encriptación de la información, etc.

- En el Nivel de Supervisión: estas medidas deben procurar minimizar errores en cuanto a la información que será monitoreada y controlada por el sistema.

- En el Nivel de Control: Las medidas efectuadas buscan concientizar a las personas encargadas de realizar estos procesos sobre no olvidar las pautas de seguridad a fin de no permitir violación a la seguridad informacional de los sistemas que realizan.

- En el nivel de Proceso o Campo: la adecuación de medidas pueden tender a la protección de los dispositivos y adecuar medidas de seguridad para que la información no se pierda.

3.16 Discusión entre el equipo de trabajo, las directivas de la empresa y jefes de las dependencias afectadas por las medidas de seguridad

Este paso es de gran relevancia para determinar la verdadera viabilidad de la realización de las medidas de seguridad. Se deben hacer las discusiones necesarias a fin de obtener la aprobación de las medidas que realmente beneficien la seguridad de los procesos informacionales de la empresa. A continuación se mostrarán algunas pautas para cumplir este objetivo:

- Socialización y explicación detallada de cada una de las medidas.
- Debate de cada una de las medidas, donde el resultado puede ser aprobado, reprobado o en espera.
- Resolución de realización de las medidas de seguridad aprobadas.

3.17 Mantener y mejorar las Medidas de seguridad mediante Políticas de Seguridad

El establecimiento de políticas de seguridad es un paso fundamental en el desarrollo de la fase de PLAN para un programa de *cyber* seguridad. Las políticas representan las reglas que establecen el comportamiento de los empleados para proteger los recursos al interior de la empresa una vez se han determinado las medidas de seguridad. En esta etapa es necesario el compromiso del equipo de seguridad (equipo de trabajo) para realizar estas políticas, a fin de desarrollar mejoras que representen mayor rendimiento y productividad para el negocio. A continuación se presenta una serie de pasos que seguir, con el propósito de determinar estas políticas dentro de la empresa.

- Creación de políticas de seguridad que permitan que los riesgos controlados durante la etapa de determinación de medidas no se repitan.

- Desarrollar políticas de seguridad que permitan mejorar el nivel de seguridad de los recursos que han sido afectados por un riesgo determinado.

- Implementar políticas de seguridad para proteger recursos dentro del sistema que no han sido afectados por riesgos o en los cuales no se han detectado riesgos.

- Desarrollar un conjunto de políticas que permitan proteger la globalidad de los recursos.

- Determinar dentro del grupo de trabajo empleados que tendrían privilegios para la administración del sistema, a fin de proteger el acceso a los recursos informacionales.

- Determinar al interior del grupo de trabajo el personal encargado de tomar medidas de contención en el caso que se violen determinadas políticas y así evitar mayores efectos contraproducentes para la compañía.

- Determinar empleados dentro del grupo de trabajo que analicen y generen medidas en contra de las violaciones de seguridad y con esto montar estrategias para fortalecer el nivel de seguridad de la empresa.

3.18 Discusión entre el Equipo de Trabajo y los Jefes de las Dependencias afectadas por las Políticas de Seguridad.

Después de que el grupo de trabajo ha creado las políticas de seguridad es necesario realizar las discusiones necesarias, con el propósito que estas políticas no afecten el buen funcionamiento de los procesos productivos. A continuación se presentan una serie de pautas para cumplir este objetivo.

- Análisis comparativo entre las políticas de seguridad propuestas y las normas o procedimientos de calidad que permiten el buen funcionamiento de los procesos productivos en las empresa, como la Norma ISO 9001.

- Identificación y eliminación de las políticas de seguridad propuestas que interfieren con el buen funcionamiento de los procesos productivos estipulados en las normas o procedimientos de calidad, como puede ser la Norma ISO 9001.

- Relacionar correctamente las políticas de seguridad propuestas y las normas o procedimientos de calidad, a fin, de tener procesos integrales que permitan el buen funcionamiento de los procesos productivos asociados con la protección de los recursos que permiten el flujo informacional de la empresa.

3.19 Capacitación al Personal de la Empresa.

Luego de definir qué políticas de seguridad harán parte de los comportamientos que debe adoptar el personal, es necesario realizar una capacitación concerniente a estas nuevas políticas con el propósito de concientizar al personal de la importancia de proteger los recursos que permiten el flujo informacional en la empresa. A continuación se mencionarán algunas pautas para cumplir este objetivo:

- Entregar la documentación sobre las políticas de seguridad al personal de la empresa.

- Realizar jornadas de explicación de las políticas de seguridad en grupos pequeños de tal manera que puedan interactuar con el tutor.

- Hacer claridad sobre las obligaciones y posibles consecuencias si no acatan las políticas de seguridad.

3.20 Seguimiento de las Políticas de Seguridad por el Grupo de Trabajo

Es necesario que el equipo de trabajo realice periódicas revisiones para examinar el cumplimiento de las políticas de seguridad. A continuación se muestran algunas pautas:

- Es necesario que el grupo de trabajo defina el periodo de tiempo en que se realizarán las revisiones del cumplimiento de las políticas de seguridad.

- Estas revisiones deben ser de tal manera que el personal no advierta la realización de esta tarea.

- Si existe incumplimiento de políticas de seguridad puede ser necesario tomar medidas concernientes a las obligaciones contractuales del empleado(s) que no cumplen las políticas de seguridad.

- Es necesario evaluar si las políticas de seguridad establecidas realmente cumplen con el objetivo propuesto, de lo contrario habrá la necesidad de replantear aquella(s) política(s).

3.21 Glosario

Activo: Recurso: objeto lógico o físico que pertenece a una organización, el cual tiene un valor actual para la organización.

Amenaza: Cualquier evento que, pueda provocar daños en los Sistemas de Información, produciendo a la empresa pérdidas materiales o financieras.

Arquitectura de Referencia: es construida con base en la definición de entidades del modelo de activos, en la cual cada organización crea una o más arquitecturas de referencia dependiendo de las plantas que posea.

Conducto: es la agrupación de comunicaciones que pueden ser lógicamente organizadas en una agrupación de flujos de información dentro y también al exterior de una zona.

Confidencialidad: Protege los Activos de Información contra accesos o divulgación No autorizados.

***Cyber* seguridad:** involucra la protección de los procesos informacionales previniendo, detectando y respondiendo a los ataques**.**

Disponibilidad: Asegura que los Recursos Informáticos y los Activos de Información pueden ser utilizados en la forma y tiempo requeridos.

Fase de Plan: establece el alcance y políticas del sistema de administración de *cyber* seguridad, identifica, clasifica y evalúa riesgos, y desarrolla un plan continuidad de negocios.

Integridad: Garantiza la exactitud de los Activos de Información contra alteración, pérdida o destrucción, ya sea de forma accidental o fraudulenta.

Modelo: Los objetivos están en identificar la necesidad de seguridad y características importantes del ambiente en un nivel de detalle necesario para dirigir los temas de seguridad.

Modelo de Activos: Describe las relaciones entre los activos en la automatización industrial y sistemas de control.

Modelo de Referencia: provee el concepto general de la empresa y las bases para detallar mejor los modelos siguientes; modelo de activos, arquitectura de referencia, modelo de zona y conducto.

Modelo de Zona y Conducto: Este modelo permite describir la agrupación lógica de activos dentro de una empresa o subconjunto de la empresa.

Norma ISA 99: Esta norma está dividida en una serie de partes, direccionadas a la aplicación de conceptos y modelos en áreas tales como definición de programas de seguridad y requerimientos mínimos de seguridad**.**

Outsourcing*:* Empresas que realizan funciones por contratación (Subcontratación).

Política de seguridad: Las políticas de seguridad informacional establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la organización.

Recurso: **Activo** objeto lógico o físico que pertenece a una organización, el cual tiene un valor actual para la organización.

Riesgo: Es la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del Sistema de Información, causando un impacto en la empresa.

Sistema de Información: Son los Recursos Informáticos y Activos de Información que dispone la empresa para su correcto funcionamiento y la consecución de los objetivos propuestos por la Dirección.

Vulnerabilidad: Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas para causarles daño y producir pérdidas a la empresa.

Zona: es una agrupación lógica de activos físicos, informacionales o de aplicación que comparten requerimientos comunes de seguridad.

ANEXO

Recomendaciones y Fallas

A continuación se enunciaran una serie de Recomendaciones a tener en cuenta para poder llevar a cabo un programa de cyber seguridad de acuerdo a estándar ISA 99.

- Para la óptima realización de un programa de administración de *cyber* seguridad es de vital importancia contar dentro del equipo que abordará el programa de seguridad informática con personas que tengan un gran conocimiento en los flujos informacionales de los sistemas de manufactura y de control.

- Para realizar una acertada evaluación de riesgos es necesario que el equipo de trabajo en seguridad tenga claridad conceptual en las definiciones de vulnerabilidad y amenazas y cómo estas repercuten en los objetivos de seguridad de un sistema de manufactura y control.

- Dado que los problemas de seguridad son transversales a toda la empresa, es necesario que todos los miembros de las diferentes áreas entiendan la importancia de la *cyber* seguridad en los procesos informacionales de la empresa.

- Para lograr realizar 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 permiten entender los procesos informacionales de sistemas de manufactura y control.

- Durante el manejo de la norma ISA 99 es importante hacer énfasis dentro del sistema de manufactura y control 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 de la empresa, es 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 empresa 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 en los cuales se aplique 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.

- Aconsejar 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.

Dentro del desarrollo y aplicación de la guía para el programa de seguridad informática es posible que se presenten fallas que pueden alterar el normal desarrollo del sistema. A continuación se detallan algunas de esas posibles fallas y como evitar que sucedan:

- Fallas de comunicación entre los niveles de Proceso y el Nivel de Controladores. 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 o Dispositivos de Control), por errores en ajustes de programación, los cuales con el tiempo generan 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 realice una labor limpia y detallada en cuanto a la selección de equipos y configuraciones en el software.

- Fallas en las redes de comunicaciones industriales, por falta de mantenimiento. Aquí se debe efectuar una revisión física de estas redes, efectuado pruebas de envío de datos y velocidad de comunicación.

- Fallas por parte de los operarios o personal de producción, por mal manejo de los dispositivos y medios de comunicación. Ésta es recurrente dentro de las industrias de manufactura y se debe 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 es muy recurrente en la industria, 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 es 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 a los sistemas de Control y Monitoreo, lo cuales pueden ser manipulados directamente por personal no capacitado. Para evitar esta falla en fundamental nombrar personas idóneas 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.

4. DESCRIPCIÓN DETALLADA PARA LA IMPLEMENTACIÓN DE LA FASE DE PLAN DE UN PROGRAMA DE *CYBER*-SEGURIDAD DE ACUERDO CON LA NORMA ISA 99 PARA EL CASO DE ESTUDIO

En este capítulo se presentará la descripción correspondiente a la implementación de la fase de plan de un programa de cyber seguridad según la norma ISA 99 tomando como caso de estudio **Terminal de Contenedores Refrigerados (TECR) de la Sociedad Portuaria Regional Buenaventura.**

4.1 DESCRIPCIÓN DE LA IMPLEMENTACIÓN AL CASO DE ESTUDIO

4.1.1 Conocimiento del Terminal de Contenedores Refrigerados

El Terminal de Contenedores Refrigerados se encuentra administrado por Soluciones Globales de Energía (S.G.E), en donde el objetivo fundamental es ofrecer servicios de control de ingresos y retiros para conexión y desconexión de contenedores refrigerados y revisión del sistema eléctrico de la Terminal de Contenedores Refrigerados, propiedad de la SPRBUN (Sociedad Portuaria Regional Buenaventura), que satisfagan las necesidades del cliente y usuarios. Para lograr este objetivo el Terminal cuenta con un Sistema de Supervisión y Monitoreo, el cual tiene como función la supervisión de las medidas eléctricas de los tableros de tomas que alimentan a los Contenedores Refrigerados, así como la entrega de Información para la facturación de la energía consumida por éstos. Adicionalmente este sistema tiene diferentes herramientas que son de gran ayuda para la supervisión y análisis del comportamiento de cada uno de los 384 tomas del patio de Contenedores Refrigerados.

El Terminal de Contenedores Refrigerados también cuenta con el software Cosmos, el cual tiene como función suplir las necesidades de planeación y administración del patio de contenedores, generando un mayor rendimiento en las áreas de almacenamiento y control de movimientos de las grúas RTG; guarda y registra las operaciones que se le realizan a cada contenedor, actualiza y valida en línea los datos en tiempo real de toda la información de contenedores. Además, agiliza los procesos de recepción y documentación, brindando así una mayor seguridad y confiabilidad a la comunidad portuaria y a los agentes portuarios que interactúan con el software tales como: Autoridades, SIAS, Agencia Navieras, Operadores Portuarios, Compañía transportadoras, Importadores y Exportadores, etc.

El Terminal también tiene procesos bien establecidos para el óptimo funcionamiento de las operaciones realizadas en el Terminal. Estos procedimientos están avalados por la certificación de calidad ISO 9001, los cuales permiten establecer con claridad las funciones del personal asociado a S.G.E.

Es necesario mencionar que la empresa S.G.E, que es la encargada de administrar el Terminal, es una empresa contratista de la Sociedad Portuaria de Buenaventura, por tanto, S.G.E debe entregarle a la sociedad portuaria la información que manifieste la actualidad del Terminal.

4.1.2 Sustentación de la Importancia de la *Cyber* Seguridad en el Terminal de Contenedores Refrigerados:

Dado que el Terminal de Contenedores Refrigerados pertenece a la Sociedad Portuaria de Buenaventura, todas las decisiones que se tomen en el Terminal deben estar avaladas por los estamentos administrativos de la Sociedad Portuaria. Por tal razón, éstas son las primeras personas que se les debe explicar la importancia de un programa de *cyber* seguridad en el Terminal. El primer paso de un programa de *cyber* seguridad es la fase de PLAN, la cual tiene como objetivo establecer el alcance y políticas del sistema de administración de *cyber* seguridad, identificar, clasificar y evaluar riesgos, y desarrollar un plan de continuidad de negocios. Para sustentar la importancia de la *cyber* seguridad en el Terminal de contenedores es necesario argumentar lo siguiente:

La Sociedad Portuaria de Buenaventura se encuentra obligada a una mejora continua que conlleva un uso más intensivo de las tecnologías de la información para poder actuar de manera más ágil y eficaz. Mediante la integración de los sistemas, los procesos y la información portuaria se va construyendo una red de información y conocimiento que permite crear cierta inteligencia del negocio que facilita el análisis y la toma de decisiones en el menor tiempo posible. Considerando que el Terminal de Contenedores Refrigerados administrado por Soluciones Globales de Energía es uno de los principales procesos de importación y exportación de productos, el cual cuenta con un sistema de supervisión y monitoreo del Terminal, el software administrativo Cosmos y la disposición física y técnica para mantenerse en la vanguardia mundial, éste debe fundamentarse en tratar de presentar un óptimo flujo de información que supone una importante oportunidad de mejora en las actividades concernientes

a la refrigeración de productos perecederos, pero también entraña riesgos ante la vulnerabilidad a ataques contra los procesos de información, intencionados o no. A continuación se muestran algunos eventos que pueden repercutir negativamente en los procesos de información que inevitablemente afectarán el óptimo funcionamiento del Terminal.

- Empleados bien o mal intencionados que advertidamente o inadvertidamente realicen cambios erróneos al proceso de conexión, desconexión y supervisión del Terminal de Contenedores Refrigerados.

- Empleados que no cumplen con los requisitos de calidad y los procedimientos establecidos para el óptimo funcionamiento del Terminal de Contenedores Refrigerados.

- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del software de supervisión del Terminal y el software administrativo Cosmos, instalados (por inatención o maldad) en el ordenador o los ordenadores abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

- Fallas inadvertidas en el sistema de supervisión y monitoreo.

Un programa de *cyber* seguridad hace referencia a tomar algunas medidas contra estos eventos, dado que si éstos logran alterar el buen funcionamiento de los procesos concernientes al flujo de información del Terminal pueden repercutir en consecuencias tales como:

- Daños en los productos contenidos en los contenedores por insuficiencia en el suministro de energía, que equivaldrían a 100, 200 o 300 millones de pesos por contenedor dependiendo del producto contenido en estos.
- Pérdida de imagen con clientes y usuarios.

Éstos son los argumentos que son necesarios utilizar inicialmente para el convencimiento de las personas que administran la Sociedad Portuaria, y luego se deben utilizar estos argumentos con las personas que administran el TECR, es decir, los miembros administrativos de S.G.E.

4.1.3 Creación del Equipo de Trabajo:

Luego de conseguir el convencimiento de los administrativos de la Sociedad Portuaria y de S.G.E de un programa de *cyber* seguridad, es necesario crear un grupo de trabajo que pueda suministrar los conocimientos necesarios sobre *cyber* seguridad en el Terminal de Contenedores Refrigerados y en otras áreas de la empresa que se considere necesario tener procesos de *cyber* seguridad; en este equipo de trabajo es importante vincular personas de las siguientes dependencias de acuerdo con las características de la Sociedad Portuaria de Buenaventura. Este equipo puede estar formado por las siguientes personas:

- Persona(s) de control de procesos del Terminal que pueden implementar y mantener los dispositivos de sistemas de control.

  Debido a las necesidades habituales del Terminal de Contenedores Refrigerados en asuntos relacionados con dispositivos de sistemas de control, el personal idóneo es el jefe de mantenimiento, jefe de operaciones, junto con los auxiliares de operaciones y de monitoreo de Soluciones Globales de Energía. En algunas situaciones será necesario tener comunicación con el personal técnico de la empresa encargada de conferir soluciones de acuerdo con los productos instalados en el Terminal y también con miembros de la Gerencia de Ingeniería y Mantenimiento.

- Persona(s) responsables de operaciones relacionadas con el cumplimiento de las solicitudes de los clientes de la Sociedad Portuaria de Buenaventura.

  Dado que el objetivo final es satisfacer las necesidades de los clientes que usualmente están estipuladas por el estado de los productos dispuestos en los contenedores y la facturación del servicio prestado, es necesario que en este equipo de trabajo exista personal de la gerencia administrativa y de servicio al cliente de la Sociedad Portuaria.

- Persona(s) de tecnologías de información que puedan ser responsables del funcionamiento de la red, soporten las funcionen comerciales y servidores de la Sociedad Portuaria.

Para las funciones relacionadas con tecnologías de información es necesario vincular al grupo miembro(s) de la Gerencia de Informática y Telecomunicaciones, de tal manera que promuevan buenas prácticas de conectividad y el manejo del software ejecutado en el Terminal de Contenedores Refrigerados.

- Persona(s) de seguridad asociados con seguridad física de la Sociedad Portuaria de Buenaventura.

  Es necesario vincular al equipo personas de la Gerencia de Operaciones vinculados al sistema de seguridad física SISE, de tal manera que colaboren en los aspectos de la seguridad física del Terminal de Contenedores.

- Personas del campo jurídico y de recursos humanos de la Sociedad Portuaria de Buenaventura.

  Es importante la vinculación de estas dependencias dado que es necesario conocer los derechos y deberes del personal que realiza las operaciones en el Terminal y también es importante conocer de qué manera se pueden realizar modificaciones contractuales, si así se requieren para la óptima realización de un programa de *cyber* seguridad.

3.1.4 Capacitación del Equipo de Trabajo:

Es necesario capacitar al equipo de trabajo en todos los conceptos relacionados a *cyber* seguridad, es decir, todos los conceptos expresados en el capítulo 1 de este documento, en donde es importante realizar capacitaciones conceptuales más profundas en las personas asociadas al campo jurídico, recursos humanos y auxiliares de operación y monitoreo del Terminal y es necesario realizar capacitaciones conceptuales de menor intensidad al resto de personas vinculas al equipo de trabajo.

4.1.5 Identificación de Recursos protegibles en el TECR:

Dado que para el buen desempeño informacional del Terminal es necesario un buen funcionamiento y estado de los recursos que permiten los procesos, es necesario identificar los recursos de acuerdo con sus características:

- **Hardware:** 384 medidores multifuncionales *power meter*, 8 PLC concentradores, 1 enrutador entre el TECR y la SPRBUN, 2 PC (1 software Cosmos, 1 supervisorío), Contenedores Refrigerados, *firewall* de la SPRBUN, módems.

- **Software:** software supervisorio del sistema de monitoreo, software Cosmos, software de programación de PLC, software de programación del supervisorío, aplicaciones de la Red de Área Local, programas de configuración del sistema de monitoreo, software de programación, ODBC (Conexión Abierta a Base de Datos).

- **Datos:** datos tomados de los contenedores por los Medidores Multifuncionales y enviados a los PLC, información enviada de los PLC al supervisorio, información enviada del supervisorio al software Cosmos, información enviada del software Cosmos a la Sociedad Portuaria, información procesada manualmente.

- **Comunicaciones:** red Modbus, red Modbus Plus, Red de Área Local.

- **Personas:** jefe de mantenimiento, jefe de operaciones, auxiliares de mantenimiento, auxiliares de monitoreo. Gerente.

- **Documentación:** documentación certificación ISO 9001, Documentos sobre PBIP (Protección de Buques e Instalaciones Portuarias), Instructivos de conexión y desconexión de contenedores, documentación sobre los dispositivos que componen el sistema de monitoreo.

4.1.6 Selección de Recursos objeto de protección en el TECR:

Debido a la fuerte interacción que existe entre todos los recursos mencionados en el TECR se puede referenciar a todos estos recursos como importantes en el procesamiento informacional del Terminal. Pero considerando que el objetivo fundamental del terminal es realizar servicios de control para la conexión y desconexión de Contenedores y revisión del sistema eléctrico del

Terminal Refrigerados a satisfacción de clientes y usuarios es primordial la protección del hardware y software que permiten el monitoreo de los contenedores dispuestos en el Terminal, los datos que permiten el flujo informacional del sistema de monitoreo y es necesario considerar el cumplimiento de la documentación sobre procedimientos de calidad operacional en el Terminal, como la correspondiente a la certificación ISO 9001 que permite el funcionamiento óptimo de los procesos en el Terminal.

4.1.7 Definición de la estructura Global del Terminal de Contenedores Refrigerados:

Para el desarrollo de un programa de *cyber* seguridad es necesario realizar determinados diagramas y descripciones que permitan mostrar el funcionamiento del Terminal de manera práctica. Tales diagramas y descripciones deben manifestar por medio del **Modelo de Referencia** el concepto general del TECR, por medio del **Modelo de Activos** la relación entre los recursos del Terminal y la forma de acceder informacionalmente a ellos; con la **Arquitectura de Referencia** se debe mostrar un orden jerárquico de los dispuestos en el Terminal y con el **Modelo de Zona y Conducto** se muestra la agrupación de activos de acuerdo con sus características comunes concerniente a los objetivos de seguridad(confidencialidad, integridad y disponibilidad), asociado con los conductos que permiten el flujo informacional entre los recursos. En el **ANEXO A** se encuentra la descripción detallada de cada uno de estos modelos.

4.1.8 Identificación de Recursos al interior de la Estructura Global del TECR:

A continuación se muestran los recursos más importantes que permiten cumplir el objetivo de TECR; en este punto se realizan breves descripciones de acuerdo con sus funciones en el Terminal:

- **Medidores Multifuncionales *Power Meter***: toma las medidas eléctricas de consumo de los contenedores refrigerados (frecuencia, corriente, tensión) y envía esta información por medio de una **red modbus.** Este recurso pertenece al nivel 0.
- **PLC Concentradores**: concentran la información proveniente de los **Medidores Multifuncionales** por medio de una **red modbus**, y a su vez envían información al **supervisorio** por una red **modbus plus.** Este recurso pertenece al nivel 1.
- **Supervisorio:** recibe información de la **red modbus** plus proveniente de los **PLC** y a su vez entrega alguna información al **software Cosmos.** Este recurso pertenece al nivel 2.
- **Modbus:** permite la comunicación entre los **Medidores Multifuncionales** y los **PLC** concentradores. Comunica el nivel 0 con el nivel 1.

- **Modbus plus:** Permite la comunicación entre los **PLC** y el **supervisorio.** Comunica el nivel 1 con el nivel 2.
- **Procedimientos de calidad operacional (ISO 9001)**: hace referencia a las funciones que deben seguir los operarios para el buen funcionamiento del Terminal. Estos procedimientos son paralelos a todos los niveles.
- **Software Cosmos:** este software toma parte de la información del **supervisorio** y envía reportes a la Sociedad Portuaria sobre la planeación del **Terminal.** Este recurso pertenece al nivel 3.

4.1.9 Agrupación de Recursos de acuerdo con su Funcionalidad:

Para el cumplimiento del objetivo de la fase de PLAN de acuerdo con la Norma ISA 99 es necesario agrupar ciertos recursos importantes en el flujo informacional, de acuerdo con su funcionalidad en el Terminal de Contenedores Refrigerados para poder denominarlos como procesos informacionales y de esta manera buscar formas para la protección de cada uno de los recursos que lo componen.

- Sistema de supervisión y monitoreo (384 Medidores Multifuncionales *Power Meter,* (8 PLC concentradores, red modbus, red modbus plus, supervisorio)
- Procesamiento administrativo (software Cosmos, Red de Área Local, *Firewall*)
- Procedimientos de calidad operacional (procedimientos de Norma ISO 9001, PBIP, instructivos de conexión y desconexión de contenedores).

Que los recursos que no hayan sido tenidos en cuenta no significa que no sean importantes en los procesos informacionales, sino que los mencionados son los más importantes en las funciones del Terminal.

4.1.10 Identificación de los Riesgos en los procesos informacionales del Terminal de Contenedores Refrigerados:

En este punto se pretende identificar qué riesgos existen sobre los procesos informacionales, es decir, qué amenazas pueden atentar negativamente sobre las vulnerabilidades de los procesos informacionales y sus posibles consecuencias. Es necesario mencionar que las siguientes

descripciones de riesgos se han realizado de acuerdo con la experiencia manifiesta de los miembros de S.G.E y de la Gerencia de Informática y Telecomunicaciones. Es importante mencionar que para la identificación de los riesgos es necesario seguir los pasos establecidos en la guía como (3.11, 3.12 y 3.13)

Riesgo 1 (asociado al sistema de monitoreo)

Una de las funciones principales de S.G.E es supervisar y garantizar el suministro óptimo de energía a los contenedores; por este motivo se implementó en el Terminal el sistema de monitoreo, llevado a cabo por la empresa Automatización Avanzada; en esta implementación no se ejecutaron las adecuadas pruebas de campo, debido a que se realizó un desarrollo con los datos e información original que se encontraba dentro del patio en dicha época (Año 2000) y no consideraron que el flujo de información y de datos podría cambiar o aumentar con el pasar del tiempo; es así como la Base de Datos BD que controlaba este sistema SCADA, al igual que el software de Supervisión, en este caso Control PC de Schneider Electronics, presenta bloqueos significativos para el funcionamiento óptimo del sistema, por motivo de que no puede soportar y menos controlar la cantidad de variables que ingresan al Sistema, evidenciando una fuerte vulnerabilidad asociada a la disponibilidad de la información. También existen en el sistema de monitoreo las siguientes fallas que repercuten en la disponibilidad de la información, la cual es un objetivo primordial para la *cyber* seguridad en un sistema de control:

- En el sistema de monitoreo se detectó fallas de comunicación con la red modbus plus de los PLCs concentradores ubicados en TDC1 y TDD4; para este caso, se realizaron varias pruebas de funcionamiento, tales como ajuste de conexión de la red, revisión de los PLCs concentradores, intercambio de las tarjetas TSX MBP 100, y el problema persistió. De lo cual se concluye que las tarjetas TSX MPB 100 se encuentran dañadas.
- Se encontraron fallas en los medidores multifuncionales ubicados en la posición TD4-3N-T2. Este medidor en su medida de voltaje indica que la fase C no tuviera tensión. Indica tensión **Vab = 470 V, Vbc = 277 V** y **Vca = 277 V;** se midió la tensión de entrada al medidor y las tres fases están correctas; se procedió a colocar los cables de tensión en otro medidor e indicó la medida correctamente. Posteriormente se revisaron los parámetros de configuración del medidor y estaban correctos; por lo que se concluyó

que este medidor está defectuoso. El medidor TC3-1N-T5 presenta una falla similar al anterior.

- La medida de frecuencia de algunas tomas no se estaba visualizando en el computador de supervisión. Se revisó el programa y se encontró que estas tomas estaban mal direccionadas; se colocó la dirección correcta y quedaron funcionando correctamente.

Por tanto, estas vulnerabilidades pueden ser atacadas o aprovechadas por las siguientes amenazas que pueden potencialmente impactar en forma negativa en el Terminal:

- Empleados bien o mal intencionados que advertidamente o inadvertidamente alteren el suministro de energía a los contenedores.
- Fallas técnicas en los equipos encargados de suministrar energía por factores intrínsecos de los equipos, falta de mantenimiento y factores ambientales.
- Empleados que no cumplen con los requisitos de calidad y los procedimientos establecidos para el suministro y funcionamiento óptimo de los contenedores.

Si estas amenazas logran afectar las vulnerabilidades mencionadas se pueden presentar las siguientes consecuencias: daños en los productos contenidos en los contenedores por insuficiencia en el suministro de energía, que equivaldrían a 100, 200 o 300 millones de pesos por contenedor, dependiendo del producto contenido en éstos, pérdida de imagen con clientes y usuarios, factible pérdida del contrato de S.G.E con la Sociedad Portuaria para administrar el Terminal de Contenedores Refrigerados.

Riesgo 2 (asociado a la seguridad física del Terminal)

La sala de control del Terminal de Contenedores Refrigerados administrada por S.G.E no presenta una seguridad física bien definida, dado que para ingresar a este sitio no existen requerimientos de seguridad de acceso físico, permitiendo que muchas personas entren a la sala de control y más aún cuando las contraseñas para ingresar al software administrativo y el software de monitoreo se encuentran dispuestas en una bitácora. Al mismo tiempo hay que

asociar esta característica con que uno de los medios más utilizados entre los operadores portuarios y las diferentes áreas de la empresa es mediante tablas de informe (personal) que pueden permitir manipulación incorrecta de la información y reportes vía radiofrecuencia. Otra vulnerabilidad está dada por el hecho de que en la sala de control se puede manipular el suministro de energía hacia los contenedores debido que la planta de distribución de energía se encuentra en la sala de control.

Por tanto, estas vulnerabilidades pueden ser atacadas o aprovechadas por las siguientes amenazas que pueden potencialmente impactar en forma negativa en el Terminal:

- Empleados disgustados o contratistas que dañan sistemas, roban o alteran información por venganza o beneficio.
- Empleados bien intencionados que inadvertidamente hacen cambios erróneos al proceso de conexión, desconexión y supervisión del Terminal de Contenedores Refrigerados.
- Empleados que rompen la calidad y políticas de seguridad del Terminal de Contenedores Refrigerados.

Si estas amenazas logran afectar las vulnerabilidades mencionadas se pueden presentar las siguientes consecuencias: pérdida de información confidencial, alteración de la información para la ejecución de la facturación, manipulación inadecuada de los software de supervisión y administrativos del Terminal, proporcionando fallas en el monitoreo y registro de la actualidad del Terminal, mal operatividad en las funciones concernientes al Terminal por información errónea.

Riesgo 3 (asociado al *firewall* de la sociedad portuaria)

Dado que los equipos que administran y supervisan el Terminal de Contenedores Refrigerados tienen privilegios de conectividad con internet, el cual dispone de un *firewall* que permite ejercer políticas de control de acceso entre dos redes, tales como su red LAN privada de la Sociedad Portuaria e Internet. Aun cuando se tenga las habilidades y experiencia necesaria para configurar el *firewall* correctamente, será difícil determinar la cantidad de inconvenientes

que podrá resistir el *firewall*. Por tanto, el firewall no garantiza que se pueda desarrollar una vulnerabilidad debido que la operativa de estos sistemas se fundamenta en ser capaces de realizar filtrado de todo el tráfico de red, y autorizar o denegar conexiones conforme a una política compuesta por reglas basadas en criterios tales como la dirección de red, el servicio, sentido de comunicación o zona de los equipos.

La protección que ofrece el sistema de *firewall* depende, por tanto, de la correcta definición de su política de filtrado. Justamente aquí es donde se pueden evidenciar las siguientes vulnerabilidades:

- Cuando la arquitectura de red y los servicios que ofrece el *firewall* son complejos, se generan en la política más reglas, que, además, son más complejas. Según crece el número de reglas, disminuye el rendimiento, aumentan los errores y es más difícil de diagnosticar los problemas y localizarlos.

- Las arquitecturas de redes y servicios en evolución suponen cambios frecuentes en las reglas e incluso el establecimiento de reglas temporales. Estas reglas “de prueba” pueden suponer un grave riesgo para la seguridad y es complicado gestionar su eliminación cuando dejan de ser necesarias. También es difícil tener una visión clara del nivel de riesgo mientras la regla temporal se encuentra desplegada.

- Cuanto mayor sea el número de reglas existentes, más difícil es prever el impacto de modificar la política. Es una situación en la que surgen cuestiones como: ¿En qué posición se debe añadir una regla?, ¿cómo afecta la modificación de una regla?

Por tanto, estas vulnerabilidades pueden ser atacadas o aprovechadas por las siguientes amenazas que pueden potencialmente impactar en forma negativa en el Terminal:

- Programas maliciosos: programas destinados a perjudicar o a hacer un uso ilícito de los recursos del sistema. Es instalado (por inatención o maldad) en el ordenador abriendo una puerta a intrusos o bien modificando los datos. Estos programas pueden ser un

virus informático, un gusano informático, un troyano, una bomba lógica o un programa espía o Spyware.

- Hacking: ataques directos para robar, destruir información o romper las actividades de Terminal de Contenedores Refrigerados o cualquier área de la Sociedad portuaria.
- Empleados bien o mal intencionados que advertidamente o inadvertidamente hacen cambios erróneos a la configuración de los computadores dispuestos en el Terminal.

Si estas amenazas logran afectar las vulnerabilidades mencionadas se pueden presentar las siguientes consecuencias: alteración o daño permanente en el software y/o hardware de los computadores encargados de la administración y supervisión del terminal, dificultando y/o alterando las operaciones de facturación, comunicación con otros operadores portuarios y la parte administrativa de la Sociedad Portuaria e inconstancia en la supervisión de los contenedores refrigerados. Tales hechos significarían pérdida de confianza de los clientes y usuarios, facturaciones alteradas, posibles daños en los productos contenidos en los contenedores que equivaldrían a 100, 200 o 300 millones por contenedor, dependiendo del producto contenido en éstos.

Riesgo 4 (asociado al software Cosmos)

El software utilizado en el Terminal de Contenedores Refrigerados para realizar las operaciones administrativas es el software Cosmos, el cual realiza las funciones de almacenamiento de información por medio de Microsoft Office Excel. De acuerdo con el flujo informacional que se presenta y que se puede presentar por entrada masiva de contenedores refrigerados, crecimiento del Terminal y/o sofisticación del proceso de automatización existe la posibilidad de que esta manera de almacenamiento no permita un óptimo funcionamiento por motivos de capacidad y flexibilidad, considerando que lo recomendable para este tipo de organizaciones es utilizar software industriales o que estén configurados para flujos de información masiva que cumplan las exigencias del TECR.

El software Cosmos es un software portuario diseñado para suplir las necesidades de planeación y administración del espacio de los patios de contenedores, el cual tiene

componentes especializados para cada uno de los patios de contenedores y cada uno de estos componentes permite comunicación con la Sociedad Portuaria; es necesario mencionar que la comunicación entre el componente del Cosmos asociado al Terminal de Contenedores Refrigerados y la Sociedad Portuaria se han presentado reiteradas fallas en el momento de enviar la información para la facturación.

Por tanto, estas vulnerabilidades pueden ser atacadas o aprovechadas por las siguientes amenazas que pueden potencialmente impactar en forma negativa en el Terminal:

- Sofisticación del proceso de automatización, entrada masiva de contenedores refrigerados, crecimiento del Terminal.
- Empleados bien o mal intencionados que advertidamente o inadvertidamente envían o reciban información errónea y/o programas maliciosos, por métodos alternos (correos electrónicos, dispositivos de almacenamiento masivo) en el momento en que la forma de comunicación establecida en el software Cosmos presente fallas.

Si estas amenazas logran afectar las vulnerabilidades mencionadas se pueden presentar las siguientes consecuencias: colapso en procesamiento y almacenamiento de información concerniente esencialmente a conexión desconexión y supervisión del Terminal, facturación errónea, pérdida de imagen ante clientes y usuarios.

4.1.11 Determinar el Riesgo en los procesos informacionales del Terminal de Contenedores Refrigerados

En este paso se debe interactuar con personas que conozcan a profundidad los procesos informacionales del Terminal; estas personas deben realizar estimaciones de posible ocurrencia que las amenazas encontradas en la identificación de los riesgos que puedan atentar negativamente contra las vulnerabilidades del sistema. En donde el fin de este paso es realizar una valoración de importancia de cada uno de los riesgos encontrados.

Para lograr valorar los riesgos es necesario considerar la siguiente ecuación:

Riesgo = Probabilidad x Consecuencia.

Donde,

Probabilidad = Probabilidad de la Amenaza x Probabilidad de la Vulnerabilidad.

En la siguiente descripción cualitativa se estimará la probabilidad de que una amenaza pueda atacar o afectar las vulnerabilidades del Terminal de Contenedores Refrigerados. El criterio de medición está determinado por la siguiente escala de valores.

Probabilidad	
Categoría	**Descripción**
Alta	Una amenaza/vulnerabilidad cuya ocurrencia es probable en el siguiente año.
Media	Una amenaza/vulnerabilidad cuya ocurrencia es probable en los siguientes 10 años.
Baja	Una amenaza/vulnerabilidad cuya ocurrencia es probable en los siguientes 50 años.
No Aplicable	Una amenaza/vulnerabilidad para la cual no hay historia de ocurrencia y para la cual la probabilidad de ocurrencias es extremadamente improbable.

Tabla 1 Escala de probabilidad para riesgos del Terminal de contenedores Refrigerados [2]

De acuerdo con la descripción realizada en la identificación de riesgos se muestra el listado de riesgos los cuales mencionan claramente las vulnerabilidades del sistema y sus amenazas; por tanto, para el riesgo 1 se tiene la siguiente calificación de acuerdo con la escala anteriormente mencionada.

Riesgo 1

Probabilidad del riesgo numero 1	
Categoría	**Descripción**
Media	Una amenaza/vulnerabilidad cuya ocurrencia es probable en los siguientes 10 años

Riesgo numero 2

Probabilidad del riesgo numero 2	
Categoría	**Descripción**
Alta	Una amenaza/vulnerabilidad cuya ocurrencia es probable en el siguiente año

Riesgo numero 3

Probabilidad del riesgo numero 3	
Categoría	**Descripción**
Media	Una amenaza/vulnerabilidad cuya ocurrencia es probable en los siguientes 10 años

Riesgo numero 4

Probabilidad del riesgo numero 4	
Categoría	**Descripción**
Media	Una amenaza/vulnerabilidad cuya ocurrencia es probable en los siguientes 10 años

A continuación se muestra una escala de consecuencias estipulada de acuerdo con la experiencia manifiesta de algunos miembros de S.G.E tomando como referencia las consecuencias que pueden entrañar los riesgos en el Terminal.

Escala de Consecuencias

Área de riesgo	Planificación continua de negocios	Planificación continua de negocios	Seguridad de Información	Seguridad de Información	Seguridad de Información	Seguridad de procesos	Seguridad de procesos	Seguridad ambiental
categoría	Interrupción suministro de energía a 1 contenedor Daños en la sala de control(software hadware e instalaciones físicas)	Interrupción suministro de energía a varios contenedores Daños en la sala de control(softwar e hadware e instalaciones físicas)	Costo	legal	Confianza	Personal interno	Personal externo	Ambiente
Alto	Mayor 2 días	Mayor 1 día	Mayor $500 millones	Delito Criminal-Crimen	Pérdida de imagen de la sociedad portuaria	Perdida de contratación con la sociedad portuaria	Fatalidad o Incidentes mayores en la Comunidad	Citación por Agencia Regional/Nacional por daños a un gran área
Medio	Mayor 1 día	Mayor 10 horas	Mayor $100 millones	Delito menor	Pérdida de clientes confidenciales de la sociedad portuaria	Contravenciones en la contratación con la sociedad portuaria	Denuncia (enfermedad) o impacto a la comunidad local	Citación para agencias locales
Bajo	Menor 1 día	menor 10 horas	Menor $50 millones	Ninguno	Ninguno	Pago de multas	No enfermedades	Pequeños daños locales

Tabla 2 Escala de consecuencias para el Terminal de Contenedores

De acuerdo a las consecuencias del riesgo 1 descritas en la identificación de riesgos se tiene la calificación (**ALTO)** de acuerdo con la escala de consecuencias anteriormente mencionada.

De acuerdo a las consecuencias del riesgo 2 descritas en la identificación de riesgos se tiene la calificación (**MEDIO)** de acuerdo con la escala de consecuencias anteriormente mencionada.

De acuerdo a las consecuencias del riesgo 3 descritas en la identificación de riesgos se tiene la calificación (**MEDIO)** de acuerdo con la escala de consecuencias anteriormente mencionada.

De acuerdo con las consecuencias del riesgo 4 descritas en la identificación de riesgos se tiene la calificación (**MEDIO)** de acuerdo con la escala de consecuencias anteriormente mencionada.

De acuerdo con lo estipulado se procede a determinar el Nivel de Tolerancia al Riesgo, el cual consiste en realizar un cruce de los valores obtenidos.

		CONSECUENCIAS		
		Alto	Medio	Bajo
PROBABILIDAD	Alto	A	B	C
	Medio	B	C	D
	Bajo	C	D	D

Tabla 3 Nivel de Tolerancia al Riesgo

Las letras en cada segmento (A, B,C,D) corresponden a una combinación particular de probabilidad y consecuencias estipuladas de acuerdo con las características propias del Terminal de Contenedores Refrigerados. Esta matriz de Nivel de Tolerancia al Riesgo se estipula de acuerdo con la experiencia manifiesta de los encargados de administrar el Terminal de Contenedores Refrigerados, los cuales han convenido que el riesgo que amerite la calificación A debe resolverse en 5 meses, los riesgos que ameritan D no tendrán ningún esfuerzo dedicado a ellos, y los que ameriten B y C merecerán un esfuerzo intermedio, es decir, 2 o 3 meses.

De acuerdo con lo anteriormente manifestado y a las calificaciones de probabilidad y consecuencia y entendiendo que el Riesgo = probabilidad X consecuencia se tienen los siguientes resultados.

Para el riesgo 1 se obtuvo probabilidad= **MEDIA;** consecuencia =**ALTO**

Nivel de tolerancia al riesgo = B

Para el riesgo 2 se obtuvo probabilidad= **ALTA;** consecuencia =**MEDIA**

Nivel de tolerancia al riesgo = B

Para el riesgo 3 se obtuvo probabilidad= **MEDIA;** consecuencia =**MEDIA**

Nivel de tolerancia al riesgo = C

Para el riesgo 4 se obtuvo probabilidad= **MEDIA;** consecuencia =**MEDIA**

Nivel de tolerancia al riesgo = C

4.1.12 Determinar las Medidas de Seguridad que permitan Mitigar los Riesgos

Este paso se ocupa de las medidas de seguridad que sean proporcionales a los riesgos. Tras identificar la prioridad de cada uno de los riesgos, es necesario seleccionar un conjunto estándar de medidas de seguridad y controles de mitigación que pueden aplicarse para reducir el riesgo específico a un nivel aceptable.

Las medidas de seguridad propuestas en este punto están asociadas a mejorar el funcionamiento de los procesos informacionales del Terminal de Contenedores Refrigerados; esencialmente para mejorar la accesibilidad y confiabilidad concerniente a la realidad de los contenedores refrigerados.

Medidas de seguridad (Riesgo 1)

Uno de los principales problemas es el bloqueo reiterado en la consola de supervisión por el alto flujo de información. Como primera y primordial medida es necesario examinar las características del computador que contiene el software de supervisión, dado que la información que es enviada a este computador efectivamente es entregada a éste por el servidor *factorylink*

opc. Partiendo de este hecho, es necesario mencionar que el computador debe procesar mensajes de alarmas, tendencias históricas, informaciones de reportes, transferencia de información, entre otros, sabiendo que el flujo informacional proveniente del Terminal es de 850MB mensuales, estando el Terminal en un 15% de su capacidad total; por tanto, al observar las características del computador es evidente su baja capacidad de procesamiento para soportar un proceso de esta magnitud; tales propiedades se pueden observar en las características técnicas de la estación de trabajo ANEXO A; por tanto, la primera medida es realizar un proceso de sofisticación del procesamiento de información, avalado por las pruebas necesarias de flujo de información; para tal evento es preciso adquirir otro computador con características actuales, es decir, con procesador *dual core*, disco duro superior a 160 GB, memoria RAM de 2 a 4 MB y demás condiciones vigentes; con base en estas características se comienza a resolver las dificultades de disponibilidad de la información.

El sistema de monitoreo presenta otras fallas asociadas con los PLC's , los medidores *power meter* y problemas en el direccionamiento de algunos tomas en el supervisorio, las cuales han sido mencionadas en la Importancia de la *Cyber* Seguridad en el Terminal de Contenedores Refrigerados; tales inconvenientes afectan la disponibilidad de la información. De acuerdo con las referencias técnicas de los equipos las siguientes son las medidas para reparar las fallas mencionadas:

• Reparación o compra de los tres medidores power meter que se encuentran en falla.
• Cambio de los conectores de la red Modbus Plus por sulfatación.
• Reemplazo de las dos tarjetas TSX MBP 100 que se encuentran en falla.
• Colocación de Protectores contra transientes para la red Modbus Plus.

Medidas de seguridad (Riesgo 2)

La principal medida consiste en que no haya acceso a las personas vinculadas a otros operadores portuarios sin estar presente en la sala de control un operador o miembro de la empresa que administra el Terminal de Contenedores Refrigerados que en este momento está a cargo de S.G.E. La primera medida puede ser un acceso físico por accionamiento mecánico, es decir, con llaves o instrumentos similares; la otra alternativa es acceso físico por accionamiento lógico, que puede ser digitando una contraseña, por medio de las huella digital o

lectores biométricos; el algoritmo que permita el acceso físico a la sala de control debe tener la siguiente lógica: cuando se encuentre un miembro de S.G.E dentro de la sala de control los otros miembros no tendrán necesidad de realizar las operaciones de acceso físico; éstas sólo se realizarán cuando los miembros de S.G.E no puedan permanecer dentro de la sala de control, en donde el último miembro de S.G.E que abandone la sala de control debe garantizar el no acceso físico de personas no autorizadas.

Las medidas mencionadas sobre acceso físico garantizan en parte qué personas no autorizadas manipulen de manera inadecuada la información administrativa, supervisión, y la información que es manipulada por medio de reportes manuales. De acuerdo con lo estipulado por los miembros de S.G.E, consideran que para la efectividad y dinámica de las funciones que se realizan en el Terminal son necesarios los reportes escritos; por tanto, se debe garantizar por medio de políticas de seguridad el cumplimiento de los objetivos de seguridad, es decir, confidencialidad, integridad y disponibilidad de la información por medio de este tipo de reportes.

Medidas de seguridad (Riesgo 3)

La labor de crear y mantener una política de *firewall* puede ser muy complicada. Por ello, resulta lógico pensar en utilizar una herramienta especializada para ayudar al análisis y gestión de dichas políticas. Esta herramienta software debe auditar y chequear las reglas de la política del *firewall* para detectar fuentes de riesgo y mostrar los resultados mediante un informe en el que se describen los problemas detectados. De esta forma, se consigue realizar una auditoría completa de la política en minutos. El resultado del análisis que debe entregar esta herramienta es un informe completo y detallado, en el cual se listan todos los riesgos encontrados y se accede a su descripción, motivo o posible solución, identificando incluso la regla concreta de la política que produce el riesgo; usualmente estas herramientas entregan un listado de riesgos estándar con una valoración de su importancia y, además, permiten la definición de nuevos riesgos por parte del usuario con base en parámetros como zona de la red y servicio. A diferencia de estas herramientas un auditor, incluso con experiencia previa, le llevaría varios días de trabajo, y siempre cabe la posibilidad de que esa persona no detecte todos los errores.

Medida de seguridad (Riesgo 4)

Dado que en el flujo de información se están presentando fallas en la comunicación del software de supervisión al Cosmos por medio de una Conexión Abierta a Bases de Datos (ODBC) y también existen fallas esporádicas entre el componente del Cosmos asociado al Terminal de Contenedores Refrigerados y el componente del Cosmos de la Sociedad Portuaria, por tanto como primera medida es necesario restablecer la conexión abierta de base de datos y considerar la instalación de una base de datos asociada al software Cosmos que proporcione características necesarias de capacidad y flexibilidad, para lograr aprovechar de mejor manera las mensajes de alarmas, tendencias históricas, informaciones de reportes, provenientes del software de supervisión; como segundo paso es necesario reparar las fallas existentes entre la comunicación del componente del software Cosmos del Terminal y el componente de la Sociedad Portuaria.

4.1.13 Mantener y mejorar las Medidas de seguridad mediante Políticas de Seguridad

Las políticas de seguridad surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la compañía desarrollarse y mantenerse en su sector de negocios; además, establecen el canal formal de actuación del personal, en relación con los recursos y servicios informáticos importantes de la empresa para mantener un nivel alto de seguridad de la información; para la realización de las políticas de seguridad se debe tomar como fundamento los riesgos mostrados previamente, asociados con la experiencia manifiesta de integrantes del equipo de trabajo. Las políticas de seguridad que se mencionan a continuación establecen pautas complementarias a los procedimientos establecidas en la certificación ISO 9001 como se muestra en la Tabla 1 del ANEXO A: dado que estos procedimientos expresan la operaciones que se deben realizar para el funcionamiento regular del Terminal y las políticas de seguridad expresan reglas para proteger los recursos importantes de la empresa, por tanto esta interacción permite tener formas de operación integrales en el Terminal.

- **Políticas de seguridad para el personal de S.G.E**

Todo operario al ingresar como personal de Soluciones Globales de Energía (S.G.E) acepta las condiciones de confidencialidad, de uso adecuado de los recursos informáticos y de información del Terminal de Contenedores Refrigerados de la Sociedad Portuaria de Buenaventura.

- **Obligaciones del personal:**

Es responsabilidad del personal de Soluciones Globales de Energía cumplir las Políticas de Seguridad.

- **Entrenamiento en seguridad informática:**

Todo empleado (S.G.E) de nuevo ingreso deberá contar con la inducción sobre el "las Políticas de Seguridad" donde se den a conocer las obligaciones para los usuarios y las sanciones que pueden existir en caso de incumplimiento.

- **Medidas disciplinarias:**

Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático.

- **Uso de medios de almacenamiento:**

Los operarios de Soluciones Globales de Energía deben conservar los registros o información que se encuentra activa en los computadores y aquélla que ha sido clasificada como reservada o confidencial.

- **Instalación de software:**

Se considera una falta grave que los operarios instalen cualquier tipo de programa (software) en la consola de supervisión o cualquier equipo conectado a la red de la Sociedad Portuaria de Buenaventura , que no esté autorizado por el administrador de la red y el gerente de S.G.E.

- **Identificación del incidente:**

El operario que sospeche o tenga conocimiento de la ocurrencia de un incidente de seguridad informática deberá reportarlo al gerente de S.G.E o al administrador de la red lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las unidades administrativas competentes, el operario deberá notificar al gerente de S.G.E.

- **Seguridad para la red:**

Será considerado como un ataque a la seguridad informática y una falta grave cualquier actividad no autorizada por la Gerencia de Telecomunicaciones, en la cual los usuarios realicen la exploración de los recursos informáticos en la red de la Sociedad Portuaria de Buenaventura, así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

- **Uso del correo electrónico:**

Los operarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad de la Sociedad Portuaria. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

Queda prohibido falsear, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

- **Controles contra código malicioso:**

Los operarios de S.G.E encargados del Terminal de Contenedores Refrigerados deben verificar que la información y los medios de almacenamiento estén libres de cualquier tipo de código malicioso, para lo cual deben ejecutar el software antivirus autorizado por el administrador de la red.

Todos los archivos de computadora que sean proporcionados por personal externo o interno considerando al menos programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos, el operario debe verificar que estén libres de virus utilizando el software antivirus autorizado antes de ejecutarse.

Cualquier usuario que sospeche de alguna infección por virus de computadora, deberá dejar de usar inmediatamente el equipo y llamar al gerente de S.G.E o al administrador de la red para la detección y erradicación del virus.

El acceso a Internet provisto a los operarios de S.G.E es exclusivamente para las actividades relacionadas con las necesidades del puesto y función que desempeña.

- **Controles de acceso lógico:**

Todos los operarios de servicios de información son responsables por la contraseña que recibe para el uso y acceso de los recursos.

Los operarios no deben proporcionar información a personal externo de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de la sala de control, a menos que se tenga el visto bueno del gerente de S.G.E o el administrador de la red.

- **Administración y uso de contraseña:**

Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar. Hacer esto responsabiliza al operario que prestó la contraseña de todas las acciones que se realicen con el mismo.

Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

- **Seguridad para el software de supervisión:**

Los operarios de S.G.E deben verificar que el envío de información proveniente del patio de contenedores sea periódico; si se presentan retardos deben ser notificados al gerente de S.G.E.

Si el computador que contiene el software de supervisión presenta bloqueos o ineficiencia en su operación, los operarios de S.G.E deben dar aviso al gerente de S.G.E.

Los operarios de S.G.E deberán verificar el buen suministro de energía a los tomas de acuerdo con las convenciones dadas para ello en el manual de manejo de software de supervisión.

Los operarios de S.G.E deberán tomar las medidas pertinentes de acuerdo con los manuales de conexión y desconexión de contenedores en el momento que se haga manifiesto alguna alarma; en caso de no poder controlar la anomalía, se deberá dar aviso inmediatamente al gerente o al jefe de mantenimiento de S.G.E

Los operarios de S.G.E deberán vigilar si algún direccionamiento de los contenedores no corresponde con la referencia existente en el software de supervisión.

- **Seguridad para el software "Cosmos"**

Los operarios deben verificar que las notaciones hechas sobre conexión y desconexión de contenedores en el software Cosmos sean verídicas.

Los operarios de S.G.E serán responsables de anomalías en la notación de conexión y desconexión en el software Cosmos de contenedores durante la vigencia de su turno.

Los operarios de S.G.E deberán verificar que la información proveniente del sistema de supervisión sea periódica, para constatar un óptimo flujo de información.

En el momento que el equipo de cómputo que contiene el software Cosmos presente bloqueos los operarios deberán informar al gerente de S.G.E

Los operarios de S.G.E deben garantizar que los reportes escritos que se hagan deben ser fidedignos respecto a la realidad del patio de contenedores; en caso contrario, se tomará como una falla grave en el cumplimiento de sus funciones laborales; la finalidad de esta política es avalar que la información que alimenta al software Cosmos es verídica.

- **Violaciones de seguridad Informática:**

Está prohibido el uso de herramientas hardware o software para violar los controles de seguridad informática. A menos que se autorice por el gerente de S.G.E o el administrador de la red.

Ningún operario de S.G.E debe probar o intentar probar fallas de la Seguridad Informática o conocidas, a menos que estas pruebas sean controladas y aprobadas por el gerente de S.G.E o el administrador de la red.

No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, propagar, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos ó caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información de la sociedad portuaria.

- **Resguardo y protección de la información:**

El operario de S.G.E deberá reportar de forma inmediata a la Sociedad Portuaria cuando detecte que existan riesgos reales o potenciales para equipos de cómputo o comunicaciones, como pueden ser fugas de agua, conatos de incendio, fallas eléctricas u otros.

El operario de S.G.E tiene la obligación de proteger los equipos de procesamiento de información que se encuentren bajo su administración, aún cuando no se utilicen y contengan información reservada o confidencial.

Es responsabilidad de los operarios de S.G.E evitar en todo momento la fuga de la información del Terminal de Contenedores Refrigerados que se encuentre almacenada en los equipos de cómputo.

- **Controles de acceso físico:**

Los operarios de S.G.E deben garantizar que siempre haya un operario en la sala de control; en su defecto debe cerrarse la entrada por medio del accionamiento existente, constatando que no existan personas de otros operadores portuarios dentro de la sala.

Se considerara como una falta para los operarios que abandonen la sala de control sin cerrar la entrada a la sala o dejar personas externas dentro de ella.

- **Protección y ubicación de los equipos:**

Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del gerente de S.G.E o el administrador de la red; en caso de requerir este servicio deberá solicitarlo.

Será responsabilidad del operario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en los equipos, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

Mientras se operan los equipos de cómputo, no se deberán consumir alimentos o ingerir líquidos.

Se debe evitar colocar objetos encima del equipo o cubrir los orificios de ventilación del monitor o del CPU.

Se debe mantener el equipo informático en un entorno limpio y sin humedad.

El operario debe asegurarse de que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos; en caso de que no se cumpla solicitar un reacomodo de cables con el administrador de la red.

Queda prohibido que el operario abra o desarme los equipos de cómputo.

- **Mantenimiento de equipo:**

Únicamente el personal autorizado por el administrador de la red de la Sociedad Portuaria podrá llevar a cabo los servicios y reparaciones al equipo informático.

- **Pérdida de equipo:**

El operario que tenga bajo su resguardo algún equipo asociado al Terminal de Contenedores Refrigerados será responsable de su uso y custodia; en consecuencia, responderá por dicho bien.

El operario deberá dar aviso inmediato al gerente de S.G.E de la desaparición, robo o extravío del equipo de cómputo o accesorios bajo su resguardo.

- **Uso de dispositivos especiales:**

El uso de los grabadores de discos compactos es exclusivo para copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.

El usuario que tenga bajo su resguardo este tipo de dispositivos será responsable del buen uso que se le dé.

- **Daño del equipo:**

En el caso de que el equipo de cómputo o cualquier recurso de tecnología de información sufran alguna descompostura por maltrato, descuido o negligencia por parte del operario quien resguarda el equipo, se levantará un reporte de incumplimiento de políticas de seguridad

5 CONCLUSIONES

- En el trabajo se ha mostrado el proceso de aplicación de una guía para seguridad informática de acuerdo al estándar ISA 99, ofreciendo una visión clara y concisa sobre cómo abordar un proyecto para la implementación de medidas de seguridad entre los niveles de manufactura.

- En este proceso es relevante establecer una correcta separación del flujo de información entre el nivel de negocios y el nivel de manufactura dado que el estándar ISA 99 no aplica para el nivel de negocios y las medidas implementadas en cuanto a seguridad no afectan las operaciones de este sistema.

- En la implementación de la guía para seguridad informática es relevante concebir que en los sistemas de control y manufactura el intercambio de información es totalmente flexible, por esta razón las medidas y políticas de seguridad que se adopten deben ser totalmente transversales a todos los niveles de la empresa en donde se desarrolla la norma ISA 99.

- La ISA 99 sugiere una metodología para abordar un programa de *cyber* seguridad a través de los modelos, elementos claves y actividades que plantea para cada fase dentro del sistema de administración de *cyber* seguridad, es así como se desarrollo una guía para implementar estas etapas al interior de una empresa.

  Para abordar el modelado se inicia con la recolección de información, identificándose los componentes que permiten determinar los niveles al interior de la empresa y los medios que participan en el intercambio de información a través de estos. Para involucrase en los elementos claves se debe haber conformado el equipo de trabajo que identificara y determinara los riesgos, de acuerdo a las vulnerabilidades, amenazas y consecuencias en el interior de la empresa. Para implementar las actividades dicho equipo de trabajo debe establecer las políticas de seguridad y trabajar en conjunto con los directivos y el personal de la empresa para mantener el programa de *cyber* seguridad operando.

- En el futuro, será importante la unificación de conceptos del estándar ISA S99 con otros estándares de seguridad informática como el estándar 27001, a fin de trabajar con las otras

partes de la norma que no han sido liberadas y proponer un trabajo que permita la funcionalidad y seguimiento del Programa de *cyber* seguridad en la empresa.

- Actualmente se centran esfuerzos para el desarrollo de la parte 3 del estándar el cual permite el manejo del programa de *cyber* seguridad y que permite el desarrollo del mismo. La importancia de trabajar en estos proyectos se basa en la relevancia que tendría esa parte de la norma para integrarse dentro de la guía a fin de permitir un adecuado desarrollo y mejorar la calidad de las políticas de seguridad.

- Las figuras que se diseñaron al interior del caso de estudio para la recolección de la información de cada modelo pueden ser tomadas como base para el desarrollo de futuros proyectos, ya que cada una brinda una ilustración acerca de una adecuada estructuración de los elementos al interior de la empresa.

- Con este proyecto queda abierta la posibilidad de seguir desarrollando temáticas en base al estándar ISA 99, es así como sería posible trabajar en las fases siguientes (hacer, verificar, actuar) para un sistema de administración de *cyber* seguridad.

- Para la implementación del sistema administrativo de *cyber* seguridad con base en la guía es fundamental tener claridad conceptual de los objetivos de seguridad informacional, esto permite determinar las necesidades de seguridad para información en las que necesita trabajar la empresa.

- La guía de implementación permite asesorar para llegar a la creación de las medidas de seguridad a fin de mitigar los riesgos y llevar los procesos informacionales de la empresa a un nivel aceptable de seguridad y de igual manera como instaurar las políticas de seguridad para lograr mantener y mejorar el nivel de seguridad.

BIBLIOGRAFÍA

ISA S99.00.01. Review 1- Security for Industrial Automation and Control Systems Part1: "Terminology, Concepts, and Models", International Society for Automation. 2007.

ISA S99.00.02. Manufacturing and Control Systems Security Part 2: "Establishing a Manufacturing and Control System Security Program", International Society for Automation. 2007.

ISA Sección España: Vulnerabilidad de los Sistemas de Control a Ataques Informáticos, *ISA Sección España.* 2008

Norma ISO 9001. Soluciones Globales de Energía Terminal Marítimo Patio Contenedores Refrigerados, Sociedad Portuaria de Buenaventura. 2006

REFERENCIAS

[1] ISA Sección España, "Vulnerabilidad de los sistemas de Control a Ataques Informáticos," *ISA Sección España*, Enero 2008. [En Internet]. Disponible: http://www.isa-spain-org/Images%5proximas_act%5cvulnerabilidad_sistem.pdf. [Accedido. Jun. 5, 2008].

[2] ISA International, "ISA S99.00.02 Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program," *ISA International*, Sept. 20, 2005. [En Internet]. Disponible: http://www.isa.org. [Accedido. Abril 12, 2008].

[3] EL PAIS, "Más recursos dirigidos a seguridad informática," el país.com, parra. 3, Enero 25, 2008. [En Internet]. Disponible: http://www.elpais.com/articulo/empresas/recursos/dirigidos/seguridad/informatica. [Accedido. Mayo 25, 2008].

[4] ISA International, "About ISA," isa.org, parra. 1, Mayo, 1996. [En Internet]. Disponible: http://www.isa.org/Content/Navigationmenu/General_Information/About_ISA1/About_ISa.htm. [Accedido.. Junio 6, 2008].

[5] ISA International, "ISA S99.00.01 Security for Industrial Automation and Control Systems Part1: Terminology, Concepts, and Model," ISA International, Oct. 29, 2007. [En Internet]. Disponible: http://www.isa.org. [Accedido. Abril 8, 2008].

[6] ISA International, "ISA S99.00.02 Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program," *ISA International*, pág. 30, Sept. 20, 2005. [En Internet]. Disponible: http://www.isa.org. [Accedido. Abril 12, 2008].

[7] ISO 27000, “Familia de normas 27000 Seguridad de la información,” ISO 27000 en Español, 2005. [En Internet] Disponible: http://iso27000.es/iso27000.html. [Accedido. Agosto 26, 2008].

[8] Sociedad Portuaria Regional de Buenaventura, “Información de navieras y ubicación geográfica,” *Sociedad portuaria Regional de Buenaventura,* 1993, [En Internet] Disponible: http://www.sprbun.com/navieras/ubi_geografica.php. [Accedido. Marzo 16, 2008].

[9] Naedele, M.: Standardizing IndustrialIT Security – “A First Look at the IEC approach, 10th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA 05)”, Catania, September 2005.

[10] NERC “CIP-002 through CIP-009,” CIP Standars feb 5, 2006 [En internet] Disponible http://www.nerc.com/ [Accedido Diciembre 20, 2008]

[11] NIST “System Protection Profile - Industrial Control Systems” PCSRF Abril 14, 2004 [En Internet] Disponible http://www.isd.mel.nist.gov/projects/processcontrol/SPP-ICSv1.0.pdf [Accedido Diciembre 21, 2008]

[12] Foro de Requerimientos de Seguridad para el Control de Procesos PCSRF 2007 “Annual Meeting and Industry Questionnaire “Fairview Park Drive, Atlanta,GA marzo 6 al 8, 2007,[en internet] http://www.isd.mel.nist.gov/projects/processcontrol/index.html

[13] Dzung, D., Naedele, M., von Hoff, T., Crevatin, M.” Security for industrial communication systems, Proceedings of the IEEE, Vol. 93 (6)”, June 2005, pp 1152–1177.

[14] Jornada Nacional de Seguridad Informática ACIS 2008, “La Gestión de la Inseguridad Informática,” Biblioteca Luis Ángel Arango, Bogotá. Junio 18 al 20, 2008, [En Internet] http://www.acis.org.co

[15] Amador, D., Syler, Agredo, Guefry, Carrascal, Carolina.”Criterios para el desarrollo de una política de seguridad, Mayo 2002, 35 pag.