DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

MAESTRIA EN GERENCIA EN SISTEMAS

TESIS PREVIO A LA OBTENCION DEL TITULO DE MASTER EN GERENCIA EN SISTEMAS

ELABORACIÓN DE UN MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTÁNDARES INTERNACIONALES.

AUTORES: DIAZ PAÚL, BUSTAMANTE FABIAN

DIRECTOR: DR. FUERTES, WALTER

SANGOLQUI

2015

Certificación de autenticidad del Director de tesis

Certifico que el presente trabajo fue realizado en su totalidad por los Ingenieros Paúl Díaz y Fabián Bustamante como requerimiento a la obtención del título de Magister en Gerencia de Sistemas.

Sangolquí, 30 de abril del 2015

_____

Ing. Walter Fuertes

Director

Certificación de autenticidad del Oponente de tesis

Certifico que el presente trabajo fue realizado en su totalidad por los Ingenieros Paúl Díaz y Fabián Bustamante como requerimiento a la obtención del título de Magister en Gerencia de Sistemas.

Sangolquí, 30 de abril del 2015

_____

Ing. Walter Fuertes

Director

Certificado de la organización auspiciante

COMERCIALIZADORA SAN REMIGIO, Auspicia la Tesis de Grado para obtener el Título de Master en Gerencia en Sistemas en la Universidad de las fuerzas armadas, denominada **ELABORACIÓN DE UN MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTÁNDARES INTERNACIONALES**, que será realizado por los Ingenieros Fabián Bustamante y Paúl Díaz.

Sangolquí, 30 de abril del 2015.

_____

Ing. Rafael Simon

Gerente de COMERCIALIZADORA SAN REMIGIO

RUC: 0190311813001

Autorización y/o restricciones para la publicación de la tesis

Nosotros, Paúl Díaz y Fabián Bustamante, autorizamos a la Universidad de las fuerzas Armadas ESPE la publicación en la biblioteca virtual de la institución el trabajo **ELABORACIÓN DE UN MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTÁNDARES INTERNACIONALES**, cuyo contenido, ideas y criterios son de nuestra exclusiva responsabilidad y autoría.

Sangolquí, 30 de abril del 2015

_____ _____

Ing. Paúl Díaz Ing. Fabián Bustamante

DEDICATORIAS

Dedico este trabajo a mi esposa e hijos que me prestaron el tiempo que les correspondía a ellos para que pueda lograr la consecución de este logro profesional, sin su ayuda y esfuerzo no lo hubiera conseguido.

Fabián Bustamante

Dedico este trabajo a mi esposa Elsa Lucia e hija Leslier Gabriela que tuvieron la paciencia y la comprensión necesaria para otorgarme su tiempo, mismo que se vio reflejado en la consecución de este logro profesional, sin su apoyo y cariño entregado no lo hubiera podido alcanzar.

Paúl Díaz

AGRADECIMIENTO

Agradezco a Dios por permitir nutrirme de todos los conocimientos adquiridos en esta Maestría y por conocer a unos excelentes amigos y profesionales, como fueron el Dr. Walter Fuertes, Msc. Carlos Procel, Msc. Paúl Díaz, profesores y compañeros del paralelo B del programa de Maestría en Gerencia en Sistemas.

También quisiera agradecer al gerente de la empresa COMERCIALIZADORA SAN REMIGIO por su apoyo brindado en todo el programa de maestría y proyecto de Tesis.

Fabián Bustamante.

Agradezco a Dios por bendecirme con sabiduría, salud y todo lo necesario que sin su presencia en imposible continuar, además un especial agradecimiento a unos excelentes amigos y profesionales, como fueron el Dr. Walter Fuertes, Msc. Carlos Procel, Msc. Fabián Bustamante, director, coordinador, y compañeros del paralelo B del programa de Maestría en Gerencia en Sistemas.

También quisiera agradecer al gerente de la empresa COMERCIALIZADORA SAN REMIGIO por su apoyo brindado en todo el programa de maestría y proyecto de Tesis.

Paúl Díaz.

INDICE DE CONTENIDO

INDICE DE TABLAS

INDICE DE GRAFICOS

RESUMEN

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

PALABRAS CLAVE:

- **SISTEMA DE CONTROL INDUSTRIAL**
- **NIST**
- **ISO**
- **RIESGO**
- **POLÍTICAS DE SEGURIDAD**
- **CONTROLES**
- **DISPONIBILIDAD**
- **INTEGRIDAD**

- **CONFIDENCIALIDAD.**

ABSTRACT

According to some studies such as Talib, Barchi, Khelifi and Ormandjieva (2012), it has been seen that computer security is globally used in companies of Public Sector, Healthcare, Telecommunications, Finance, among others; being ISO / IEC 27001 the favorite standard to follow to implement the Information Security Management System (ISMS). In the industrial and manufacturing sectors have been implemented ISMS, these have been directed to the management of information technology for business, but not for the industrial area, where nowadays also there is an important component of computer science, known as the Industrial Control Systems (SCI). The reason for not using ISO 27000 and a traditional ISMS in the SCI is they primarily have some differences in the operative side compared to the traditional model of the Information and Communication Technologies (ICTs), so this project proposes to COMERCIALIZADORA SAN REMIGIO, to use international industry standards such as those issued by the National Institute of Standards and Technology, USA (NIST). Specifically this work focuses on developing a manual of rules and policies of information security based on: NIST 800-53 and NIST 800-82.r1 for managing information security, similar to what is done in ISMS based on ISO. With this manual the company will make an effective Management of Information Security in its manufacturing processes and production in the context of confidentiality, integrity and availability.

1. CAPÍTULO I – INTRODUCCION

1.1. Antecedentes

La empresa COMERCIALIZADORA SAN REMIGIO, una empresa de manufactura, actualmente cuenta con un Sistema de Control Industrial el cual ha ido implementándose y creciendo desordenadamente en el tiempo, lo cual ha provocado que sucedan incidentes de seguridad relacionados con la disponibilidad, confidencialidad e integridad de la información y activos de la empresa, llegándose a reportar hasta 5 incidentes mensualmente al soporte técnico de tecnologías de información. Por esta razón se requiere detectar los problemas y proponer una solución para reducir este nivel de incidentes.

1.2. Justificación e importancia

En las últimas décadas ha habido gran interés en la comunidad científica para crear manuales de seguridad industriales. Los más importantes se explicarán a continuación: En Estados Unidos el trabajo propuesto por Francia (2012) propone mejores prácticas y evaluación de riesgos de los SCI. En Canadá el trabajo realizado por Byres (2003) propone mitos y hechos tras la cyberseguridad en los SCI. En España Navarro (2013) expone una visión global de la cyberseguridad de los SCI. En Italia el trabajo elaborado por Tieghi (2007) presenta una introducción a la protección de información y sistemas de control y automatización. En Brasil Costa (2012) expone el trabajo de prospección de tecnologías para aumentar la seguridad en sistemas SCADA y en Colombia Villamizar (2013) propone el trabajo de implementación de seguridad de la información en SCI. En estos trabajos básicamente se hacen recomendaciones y análisis generales sobre los SCI, más no abordan un sistema de gestión de seguridad de la información como tal.

En cuanto al ámbito Nacional y Local se pudo observar escasos trabajos relacionados a planes de desastre y recuperación, análisis de riesgos, entre otros. Sin embargo tampoco hablan de sistema de gestión o controles para administrar la seguridad de la información en los SCI. Cabe resaltar que la mayoría de estos trabajos realizados a nivel nacional se basan en la ISO/IEC 27000.

1.3. Planteamiento del problema

La empresa COMERCIALIZADORA SAN REMIGIO dentro de su plan estratégico tiene como objetivo implementar un sistema de gestión de la seguridad de la información a todo nivel (área administrativa y área de producción), para lo cual ha iniciado varios proyectos que lleven al negocio a apuntar en este camino. Dentro de estos proyectos, el área de Tecnologías de Información de esta empresa, luego de un análisis previo conjuntamente con un experto en seguridad informática, determinaron que la implementación de un SGSI basado en ISO 27001 para el SCI no articulan lo suficiente, debido básicamente a las diferencias en los procesos de operación que la infraestructura informática brinda a este. Por esta razón el problema a resolver en este proyecto es: encontrar un marco referencial o estándar de la industria que por un lado articule bien con el SCI y que por otro sea compatible con el SGSI que se está implementando en la empresa COMERCIALIZADORA SAN REMIGIO.

1.4.Formulación del problema

De la revisión bibliográfica revisada, el presente proyecto se enfoca a preparar un manual de normas y políticas de seguridad informática que contemple controles gerenciales, operacionales, técnicos y al mismo tiempo sea fundamentado con el estándar NIST 800-82 y NIST 800-53. Las preguntas necesarias a realizar para presentar solución al problema planteado son las siguientes:

¿Cuáles son los controles de Gerenciamiento de la seguridad de la información del SCI?

El personal directivo de la empresa COMERCIALIZADORA SAN REMIGIO necesita conocer cuáles son los controles de Gerenciamiento, los que servirán para la adecuada gestión y dirección de la seguridad de información del Sistema de Control Industrial.

¿Cuáles son los controles Operacionales de la seguridad de la información del SCI?

El personal operativo de la empresa COMERCIALIZADORA SAN REMIGIO necesita conocer cuáles son los controles Operativos, los que servirán para la adecuada operación y utilización de la seguridad de información del Sistema de Control Industrial.

¿Cuáles son los controles Técnicos de la seguridad de la información del SCI?

El personal técnico de la empresa COMERCIALIZADORA SAN REMIGIO necesita conocer cuáles son los controles técnicos, los que servirán para la correcta instalación, configuración y mantenimiento de la seguridad informática del Sistema de Control Industrial.

¿Cómo se podrá Socializar, aplicar, verificar y aprobar el Manual?

El personal de Tecnologías de Información de la empresa COMERCIALIZADORA SAN REMIGIO necesita conocer cuáles son las formas de socializar, aplicar, verificar y probar los controles gerenciales, operacionales y técnicos del manual de seguridad informática del SCI.

1.5. Hipótesis

La empresa COMERCIALIZADORA SAN REMIGIO incrementará los niveles de seguridad de la información en su Sistema de Control Industrial, reduciendo en un 40% el número de incidentes anuales, al usar un manual de normas y políticas de seguridad informática basada en los estándares internacionales NIST 800-82 y NIST 800-53.

1.6. Objetivo General

Elaborar un Manual de Normas y Políticas de Seguridad Informática de un Sistema de Control Industrial para la empresa COMERCIALIZADORA SAN REMIGIO usando los estándares internacionales NIST 800-82 y NIST 800-53.

1.7. Objetivos Específicos

- Elaborar el manual de seguridad informática con los Controles de Gerenciamiento para el SCI de COMERCIALIZADORA SAN REMIGIO.

- Elaborar el manual de seguridad informática con los Controles Operacionales para el SCI de COMERCIALIZADORA SAN REMIGIO.

- Elaborar el manual de seguridad informática con los Controles Técnicos para el SCI de COMERCIALIZADORA SAN REMIGIO.

- Realizar una evaluación a la empresa COMERCIALIZADORA SAN REMIGIO con el manual ya elaborado, de manera que se pueda comprobar la efectividad de los controles propuestos.

- Socializar, aplicar, verificar y aprobar el Manual por un comité formado por Directivos, operativos y técnicos de la empresa COMERCIALIZADORA SAN REMIGIO.

2. CAPITULO II: FUNDAMENTACION TEORICA

Tanto en nuestro medio como en latino América, aún no se ha prestado atención a la gestión de la seguridad de la información en los Sistemas de Control Industrial, sobre todo en empresas Industriales y de manufactura con infraestructura informática crítica. A nivel mundial esta realidad es diferente, pues existen ya organizaciones, estándares y conceptos internacionalmente aceptados, que son parte de este fundamento teórico:

2.1. Sistemas de Gestión de Seguridad de Información (SGSI).

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este proceso podría considerarse por analogía una norma conocida como ISO 9001 (Ureña, 2008), al cual se lo conoce como Sistema de Calidad para la Seguridad de la Información. El propósito de un sistema de seguridad de información es por tanto garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de forma sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y la tecnología (Ureña, 2008). Según un SGSI la seguridad de la información se cimienta en la preservación de su confidencialidad, integridad y disponibilidad:

Confidencialidad: Que la información no sea disponible a individuos, entidades o procesos no autorizados.

Integridad: Que la información sea completa, exacta y la misma desde cualquier lugar que se la requiera.

Disponibilidad: Que la información esté disponible a individuos, entidades o procesos autorizados cuando se lo requiera.

La información, junto a los procesos y sistemas son activos importantes de una empresa, importantes para mantener los niveles de competitividad, rentabilidad, conformidad legal y la imagen empresarial. El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente, por esta razón es necesaria la efectiva gestión de la seguridad y ser parte neurálgica de toda organización. Según ISO la documentación de un SGSI se muestra como una pirámide, véase Figura 1.

Figura 1. Pirámide de Documentación ISO 27001
Fuente: López, 2005

Nivel 1 – Manual de Seguridad: Este documento dirige todo el sistema, determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales.

Nivel 2 – Procedimientos: Documentos de nivel operativo, aseguran que se cumpla la planificación, operación y control de procesos de la seguridad de la información

Nivel 3 – Instrucciones, checklists y formularios: Documentos que describen tareas y actividades específicas relacionadas con la seguridad de la información.

Nivel 4 – Registros: Documentos que demuestran evidencia objetiva del cumplimiento del SGSI, asociado a los niveles anteriores.

2.2. Guía para la seguridad de Sistema de Control Industrial NIST 800-82.

Este grupo de estándares provee una guía para establecer seguridad en Sistemas de Control Industrial (SCI). Estos SCI incluyen Sistema de Supervisión, Control y Adquisición de Datos (SCADA), Sistemas de Control distribuido (DCS) y Controladores lógicos programables (PLCs). La razón principal de usar una normativa para un SCI es que estos cada vez están adoptando componentes informáticos en su diseño y funcionamiento, esto ha provocado que los SCI sean

cada vez menos aislados e independientes como lo eran antes, creando una gran necesidad de asegurar estos sistemas.

Aunque algunas características son similares entre los SCI y los sistemas de tecnologías de información (TI) tradicionales, es importante entender que no se pueden tratar con la misma normativa a los SCI que a los TI, pues algunas de estas características incluyen significativos riesgos a la salud, protección a la vida humana, daños al ambiente, impactos financieros, pérdidas en producción, entre otros. NIST en analogía con otras normativas propone usar una estrategia de "Seguridad en Profundidad" la cual incluye lo siguiente:

- Desarrollo de políticas de seguridad, procedimientos, entrenamiento y material educativo.
- Implementación de topología de red para SCI que tengan múltiples capas
- Separación lógica entre la red corporativa y la red del SCI
- Emplear arquitectura de red considerando una zona desmilitarizada (DMZ)
- Considerar que componentes críticos sean redundantes
- Deshabilitar puertos no usados
- Restringir el acceso físico a la red del SCI y sus dispositivos
- Usar un mecanismo de autenticación separado al usado por la red corporativa.
- Usar tecnología para la identificación de personal
- Implementar controles de seguridad tal como IDS/IPS, Software de Antivirus, etc.
- Aplicar técnicas de seguridad para encriptación y criptografía para almacenamiento de datos del SCI donde sea necesario.
- Despliegue de parches de seguridad luego de haberlos probado previamente.
- Seguimiento y monitoreo de rastros de auditoría en las áreas críticas.

Por todo lo expuesto anteriormente el Instituto Nacional de estándares y tecnología del departamento de comercio de Estados Unidos (NIST) ha creado un proyecto denominado: "Industrial Control System Security Project" (Locke & Gallagher, 2011), el cual en colaboración con el sector público y privado ha desarrollado una guía específica para la aplicación controles de seguridad en el documento NIST SP 800-53 el cual tiene como título: "Controles de seguridad

recomendados para sistemas de información federal y Organizaciones para Sistemas de Control Industrial".

2.3. Política de seguridad informática NIST 800-12.

Una política es una directiva de gestión de la alta dirección para crear un programa de seguridad informática, en la que se establece sus objetivos y asigna responsabilidades. El término política es también usado para referirse a una regla de seguridad específica para un sistema en particular.

Las herramientas usadas para implementar políticas son: Procedimientos, estándares y directrices, las cuales describen como serán implementadas estas políticas dentro de una organización. Ya que la política es escrita en nivel amplio las organizaciones usan estas herramientas para ofrecer a los usuarios, directivos y demás miembros, un acercamiento más claro a la implementación de dichas políticas y así cumplir con los objetivos de la organización.

Según Guttmann (1995) el término política de seguridad es definido como la documentación de decisiones de seguridad informática, pudiendo estas clasificarse en 3 categorías:

Política de programa: Es usado para crear un programa de seguridad informática de una organización. Está formada por los siguientes componentes: Objetivo, alcance, responsabilidades y cumplimientos.

Políticas de asuntos específicos: Direcciona asuntos específicos de preocupación para la organización, por ejemplo: Acceso a internet, privacidad de e-mail, gestión de riesgos, planes de contingencia, protección de información confidencial, software no autorizado, adquisición de software, trabajo en casa, ingreso de dispositivos externos, encriptación de información, entre otros. A diferencia de las políticas de programa, estas políticas requieren más frecuentes revisiones cuando la tecnología cambia. Está formada por los siguientes componentes: Declaración del tema, declaración de la posición de la organización, roles y responsabilidades, aplicabilidad, cumplimiento y Puntos de contacto e información suplementaria.

Políticas de sistemas específicos: Se enfoca en decisiones tomadas por gerenciamiento para proteger un sistema en particular. A diferencia de las 2

categorías anteriores, esta provee más información y dirección. Esta categoría tiene dos componentes: Objetivos de seguridad (Ejemplo: "Solamente usuarios de automatización son autorizados a realizar modificaciones a las configuraciones de PLCs") y reglas de seguridad operacional (Ejemplo: "El Ingeniero de automatización podrá hacer cambios en las variables de entradas de PLCs siempre y cuando haya realizado un requerimiento de cambios RFC previamente").

2.4.Mapeo de controles de seguridad a ISO/IEC 27001.

Dentro de la documentación del estándar NIST, existen algunas publicaciones que direccionan a la convergencia y compatibilidad entre controles NIST e ISO/IEC 27001. En este contexto hay un apéndice de NIS 800-53 en el que se especifican lineamientos de convergencia de controles de seguridad, tecnologías de seguridad de información, Sistemas de manejo de seguridad de información y sus requerimientos.

ISO/IEC 27001, aplica a todos los tipos de organizaciones y especifica requerimientos para establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento de un sistema de gestión de seguridad documentado en el ámbito de todos los riesgos del negocio (Ureña, 2008). NIST se enfoca en el manejo del riesgo desde el punto de vista de los sistemas de información, tal como lo pide El Acta federal de la gestión de la seguridad de información de Estados Unidos (FISMA) y descritos también en NIST 800-39. En 800-39 se está trabajando para incorporar ISO/IEC 27001 con el fin de manejar riesgos de seguridad de información a través del establecimiento de un SGSI.

Por otro lado es importante mencionar que en la misión de NIST se incluye la adopción de estándares nacionales e internacionales en donde sea apropiado, de manera que se tienda a la convergencia y eliminación de carga de trabajo para las organizaciones que emiten dichos estándares. Esta iniciativa de convergencia será llevada en 3 fases (Locke & Gallagher, 2009):

Fase I: Mapeo de 2 vías entre controles de seguridad de NIST 800-53 y controles en ISO/IEC 27001

Fase II: Proveerá mapeo de 2 vías entre los conceptos de manejo de riesgos de nivel organizacional indicados en NIST 800-39 (versión en estudio) y los requerimientos generales de ISO/IEC 27001

Fase III: Usará los resultados de la fase I y de la fase II para integrar completamente ISO/IEC 27001 dentro de NIST.

Actualmente se está trabajando aún en la Fase II de este proyecto de convergencia y se espera a inicios del 2015 se tenga ya una versión de NIST 800-39 con las modificaciones respectivas. A continuación en la Tabla 1, se muestra un extracto del mapeo de controles de seguridad entre NIST e ISO/IEC 27001 que forman parte de este documento apéndice Fase I.

Tabla 1.

Extracto del mapeo NIST 800-53 a ISO/IEC 27001

NIST SP 800-53 CONTROLS		ISO/IEC 27001 (Annex A) CONTROLS
AU-12	Audit Generation	A.10.10.1, A.10.10.4, A.10.10.5
AU-13	Monitoring for Information Disclosure	None
AU-14	Session Audit	None
CA-1	Security Assessment and Authorization Policies and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3 A.6.1.4, A.8.1.1, A.10.1.1, A.15.1.1, A.15.2.1
CA-2	Security Assessments	A.6.1.8, A.10.3.2, A.15.2.1, A.15.2.2
CA-3	Information System Connections	A.6.2.1, A.6.2.3, A.10.6.1, A.10.8.1, A.10.8.2, A.10.8.5, A.11.4.2
CA-4	**Withdrawn**	---
CA-5	Plan of Action and Milestones	None
CA-6	Security Authorization	A.6.1.4, A.10.3.2
CA-7	Continuous Monitoring	A.6.1.8, A.15.2.1, A.15.2.2
CM-1	Configuration Management Policy and Procedures	A.5.1.1, A.5.1.2, A.6.1.1, A.6.1.3, A.8.1.1, A.10.1.1, A.10.1.2, A.12.4.1, A.12.5.1, A.15.1.1, A.15.2.1
CM-2	Baseline Configuration	A.12.4.1, A.10.1.4
CM-3	Configuration Change Control	A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.1, A.12.5.2, A.12.5.3
CM-4	Security Impact Analysis	A.10.1.2, A.10.3.2, A.12.4.1, A.12.5.2, A.12.5.3
CM-5	Access Restrictions for Change	A.10.1.2, A.11.1.1, A.11.6.1, A.12.4.1, A.12.4.3, A.12.5.3
CM-6	Configuration Settings	None
CM-7	Least Functionality	None
CM-8	Information System Component Inventory	A.7.1.1, A.7.1.2
CM-9	Configuration Management Plan	A.6.1.3. A.7.1.1, A.7.1.2, A.8.1.1, A.10.1.1, A.10.1.2, A.10.3.2, A.12.4.1, A.12.4.3, A.12.5.1, A.12.5.2, A.12.5.3

Fuente: Locke & Gallagher, 2009

3. CAPITULO III: ELABORACION DEL MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA.

Un sólo producto de seguridad o tecnología no puede proteger adecuadamente un SCI. La seguridad de un SCI según Stouffer, Falco & Scarfone (2013) está basada en una combinación de políticas de seguridad efectivas y un set de controles de seguridad debidamente configurados.

3.1.Reunión con los interesados

En este paso nos reunimos con todos los interesados del proyecto: Ingenieros de Automatización, Ingenieros de Tecnologías de información, Ingenieros de Producción, Ingenieros de mantenimiento y operadores de máquinas de las 2 líneas de producción. El objetivo de esta reunión era conocer los requisitos del proyecto y los controles de seguridad implementados. Para esto utilizamos plantillas de prediseñadas e indicadas en NIST 800-30, para el levantamiento de requerimientos. En estas plantillas se realizaron preguntas básicas de carácter investigativo: Quien, Que, Donde, Cuando, Por qué y Cómo.

Como en la primera reunión no estuvieron presentes todos los stakeholders, se pasaron por correo electrónico las encuestas y sus respuestas fueron tabuladas conjuntamente con las realizadas en la reunión presencial y se adjuntan en el anexo 1 y anexo 2. La encuesta sobre los controles actuales se los hizo al final de la reunión (Anexo 3), con el fin de no sesgar criterios y así provocar errores en la recolección de estos requerimientos.

3.2. Elaboración de acta de constitución del proyecto (ACP)

En base a Bustamante y Díaz (2015), las lecciones aprendidas de este proyecto y los requerimientos recopilados en el punto anterior se desarrollar el ACP. Este ACP se lo hizo firmar al gerente de la empresa COMERCIALIZADORA SAN REMIGIO con el fin de iniciar formalmente el proyecto.

Es importante mencionar que en el ACP se pueden visualizar algunas cosas importantes para el proyecto como son: El nivel de autoridad de los encargados de

este proyecto, Riesgos del proyecto, Oportunidades del proyecto para la organización, Interesados del proyecto, su influencia e interés en el mismo. Ver anexo 4.

3.3. Elaboración del manual con los controles de seguridad del tipo gerencial.

Estos controles son contramedidas de seguridad para un SCI que se enfocan en el manejo del riesgo y la gestión de la seguridad informática. NIST SP 800-53 (Blank & Gallagher, 2013) define 5 familias de controles:

3.3.1. Valoración de la seguridad y Autorización (CA):

Asegura que los controles son implementados correctamente, operando como se diseñaron y produciendo la eficacia deseada. La guía para los controles CA pueden ser encontrados en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-26, NIST SP 800-37

En este punto se ha realizado una política que se refiere a la valoración de controles de seguridad. Ver anexo 5.

3.3.2. Planeación (PL):

Desarrollo y mantenimiento de un plan realizando valoraciones, especificando e implementando controles de seguridad, asignando niveles de seguridad y respondiendo a incidentes. La guía para los controles PL pueden ser encontrados en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-18

En este control se ha realizado una política que se refiere al mantenimiento del plan de seguridad. Ver anexo 5

3.3.3. Valoración de Riesgos (RA):

Proceso de identificar riesgos de las operaciones, valoraciones, individuos mediante la determinación de ocurrencia, impacto resultante y

controles adicionales que mitigarían este impacto. La guía para los controles RA pueden ser encontrados en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-30, NIST SP 800-12, NIST SP 800-39, NIST SP 800-40, NIST SP 800-115, NIST SP 800-60

Basado en este control se ha realizado una política para mantener actualizado la valoración de riesgos de la empresa y las mitigaciones correspondientes. Anexo 5.

3.3.4. Sistema y Adquisición de servicios (SA):

Asignación de recursos del SCI para ser mantenido a través de acuerdo al ciclo de vida y al desarrollo de políticas de adquisición basado en los resultados de la valoración de riesgos, criterios de diseño, procedimientos de prueba y documentación asociada. La guía para los controles SA pueden ser encontrados en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-23, NIST SP 800-27, NIST SP 800-35, NIST SP 800-36, NIST SP 800-64, NIST SP 800-65, NIST SP 800-70

Con este control se ha creado una política para la adquisición de recursos para una adecuada protección del SCI. Anexo 5.

3.3.5. Gerenciamiento del programa (PM):

Provee controles de seguridad a nivel organizacional más que el nivel del sistema de información. La guía para los controles PM pueden ser encontrados en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53

Para este control no se ha visto necesario hacer una política, pues existen otras políticas en la organización que ya mencionan puntos relacionados.

3.4. Elaboración del manual con los controles de seguridad del tipo operacional

Estos controles son contramedidas de seguridad para un SCI que son primariamente implementados y ejecutados por la gente. NIST SP 800-53 (Blank & Gallagher, 2013) define 9 familias de controles:

3.4.1. Seguridad del Personal (PS):

Políticas y procedimientos para caracterización de posición del personal, tamizaje, transferencia, penalidades y terminación; también direcciona a personal de seguridad tercerizados. La guía para los controles PS puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-35, NIST SP 800-73, NIST SP 800-76

Con este control se crearon políticas para reducir el riesgo de errores humanos, robo, fraude u otro mal uso intencional o no intencional del SCI. Ver el Anexo 6.

3.4.2. Protección física y ambiental (PE):

Políticas y procedimientos direccionando controles de accesos físicos, de transmisión y de visualización al igual que también controles ambientales para acondicionamiento y disposiciones de emergencia. La guía para los controles PE puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-46.

En este punto se consiguió realizar políticas relacionadas a: Protección de lugares físicos, Controles de acceso, monitoreo de acceso, Seguimiento de valores y gente, factores ambientales, alimentación, cuartos de control, dispositivo portátil y cableado. Ver Anexo 6.

3.4.3. Plan de Contingencia (CP):

Políticas y procedimientos diseñados a mantener o restaurar operaciones del negocio, incluyendo operaciones informáticas, posiblemente en localidades alternas, en el evento de emergencias, fallas del SCI o desastres. La guía para los controles CP puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-34

Con este control se hicieron políticas referentes al plan de continuidad del negocio y plan de desastre-recuperación. Ver Anexo 6.

3.4.4. Gestión de la configuración (CM):

Políticas y procedimientos para controlar modificaciones a hardware, firmware, software y documentación para asegurar que el SCI sea protegido en contra de modificaciones impropias antes, durante y después de la implementación de sistemas. La guía para los controles CM puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-70.

En este control se elaboraron políticas para formalizar los cambios en la infraestructura del SCI y sus configuraciones. Ver Anexo 6.

3.4.5. Mantenimiento (MA):

Políticas y procedimientos para manejar todos los aspectos del mantenimiento del SCI. La guía para los controles MA puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-63

En este punto se elaboraron políticas referentes a las rutinas de mantenimiento preventivo y correctivo en los componentes del SCI. Ver Anexo 6.

3.4.6. Integridad del sistema e información (SI):

Políticas y procedimientos para proteger sistemas de información y sus datos de las fallas de diseño y modificaciones de datos usando verificación de funcionalidad, chequeo de integridad de datos, detección de intrusos, detección de código malicioso y alertas de seguridad y controles de consultoría. La guía para los controles SI puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-40, NIST SP 800-94

Para este control se vio necesario realizar políticas relacionadas al uso de antivirus, monitoreo de red y gestión de parches. Ver anexo 6.

3.4.7. Protección de medios (MP):

Políticas y procedimientos para asegurar el manejo de medios, cubiertas de control de acceso, etiquetado, almacenamiento, transporte, sanitación, destrucción y disposición. La guía para los controles MP puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-88

En este control se consideraron políticas referentes al uso de floppy disks, CDs, DVDs, usbs, memory sticks, reportes impresos y documentos. Ver Anexo 6.

3.4.8. Respuesta a incidentes (IR):

Políticas y procedimientos pertenecientes a capacitación de respuesta de incidentes, pruebas, manejo, monitoreo, reporte y servicios de soporte. La guía para los controles IR puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-61, NIST SP 800-83

En este punto se pudieron realizar políticas sobre clasificación de incidentes, acciones de respuesta y acciones de recuperación. Ver Anexo 6.

3.4.9. Entrenamiento y concienciación (AT):

Políticas y procedimientos para asegurar que todos los usuarios del sistema de información sean capacitados en seguridad apropiadamente en temas relativos al uso del sistema y que los registros de entrenamiento sean mantenidos. La guía para los controles AT puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-16, NIST SP 800-50

En este control se desarrollaron políticas relacionadas al programa de entrenamiento, responsables y evaluación del mismo. Ver Anexo 6.

3.5. Elaboración del manual con los controles de seguridad del tipo técnico.

Los controles técnicos son contramedidas de seguridad para los SCI que son primariamente implementados y ejecutados por el sistema a través de mecanismos que contienen componentes de hardware, software o firmware del sistema. NIST SP 800-53 (Blank & Gallagher, 2013) define 4 familias de controles dentro de la clase de controles técnicos:

3.5.1. Identificación y autenticación (IA):

El proceso de verificación, la identificación de un usuario, proceso o dispositivo, a través del uso de credenciales específicas (ej.: contraseñas, tokens, biométricos) como un prerrequisito para conceder accesos a recursos en el sistema. La guía para los controles IA puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-63, NIST SP 800-73, NIST SP 800-76

En este control se realizaron políticas referentes al manejo de contraseñas. Ver anexo 7.

3.5.2. Control de acceso (AC):

El proceso de conceder o denegar requisitos específicos para obtener y usar información y servicios de procesamiento de información relacionada al acceso físico o servicios relacionados al ambiente del SCI. La guía para los controles AC puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-63, NIST SP 800-48, NIST SP 800-97, FIPS 201, NIST SP 800-96, NIST SP 800-73, NIST SP 800-76, NIST SP 800-78

En este punto se realizaron políticas relacionadas a los controles de acceso a cuartos de control, servidores web, vlans y wireless. Ver el anexo 7.

3.5.3. Auditoría y rendición de cuentas (AU):

Revisión independiente, examinación de registros y actividades para valorar la adecuación de sistemas de control, para asegurar conformidad con las políticas establecidas, procedimientos operacionales y recomendar cambios necesarios en controles, políticas o procedimientos. La guía para los controles AU puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-12, NIST SP 800-61, NIST SP 800-92.

En este punto se desarrollaron políticas relacionadas a la auditoría de seguridad informática relacionada al SCI. Ver anexo 7.

3.5.4. Protección del sistema y las comunicaciones (SC):

Mecanismos para proteger los sistemas y componentes de transmisión de datos. La guía para los controles SC puede ser encontrada en los siguientes documentos:

- NIST SP 800-82, NIST SP 800-53, NIST SP 800-28, NIST SP 800-52, NIST SP 800-56, NIST SP 800-57, NIST SP 800-58, NIST SP 800-63, NIST SP 800-77.

En este control se desarrollaron políticas referentes a encriptación de información y Redes privadas virtuales (VPN). Ver anexo 7.

Guías adicionales para los controles técnicos pueden ser encontrados en ISA TR99.00.01 y en el EPRI report.

Al finalizar la elaboración de todos los documentos de controles gerenciales, operacionales y técnicos se los compilaron y se los puso en el formato sugerido por la empresa ver el anexo 8. Además se adjuntó el primer proyecto: “Diseño de Estrategias de Mitigación” con el fin de que en el manual se tenga toda la información necesaria para la gestión de seguridad informática del SCI de la empresa, ver anexo 9.

4. CAPITULO IV: EVALUACION, VERIFICACION Y VALIDACION DE RESULTADOS.

Con el fin de verificar y validar los resultados de disminuir en un 40% los incidentes de seguridad, se realizó una prueba, simulando los incidentes de los 5 últimos años, para lo cual se siguieron los siguientes pasos:

4.1.Evaluación.

Se entregó el manual a un comité de 10 personas formado por personal directivo, técnico y operacional para que lo revisen y hagan cualquier sugerencia o comentario que sirva para mejorar el contenido del manual de políticas, luego de esto en una reunión formal se recolectaron respuestas a una encuesta, comentarios y sugerencias utilizando formatos elaborados en Microsoft Excel con temas relativos a la estructura del manual, a los objetivos estratégicos de la empresa y de Tecnologías de Información. Las 11 preguntas realizadas, sus respuestas y el proceso estadístico se pueden observar en el anexo 10. De un total de 11 datos, el rango de porcentajes de aceptación fue de 30% a 100% con una mediana en 75%, el promedio de aceptación del manual fue de 79,09% (media), la mayoría de preguntas tuvieron una aceptación de 90% (moda), los valores menores a 55,24% (desviación estándar) pueden haberse dado por falta de criterio o conocimiento de los encuestados.

4.2.Simulación de solución

En base al punto anterior, en este paso se probó que las políticas implementadas a nivel gerencial, operativo y técnico reduzcan el impacto de los incidentes de seguridad.

En esta simulación se pidió ayuda a los Ingenieros de: Tecnologías de Información, Automatización, directivos de producción y operadores de máquinas de producción, en total 10 personas. Los resultados de las 10 preguntas se los documentaron en el anexo 11 conjuntamente con el respectivo proceso estadístico. De un total de 100 datos, el rango de porcentajes de percepción fue desde 15% hasta el 80% con una mediana en 45%, el promedio de percepción de cumplimiento de las políticas fue de 41,05% (media), La percepción más común de cumplimiento fue de 40% (moda), los valores de percepción de cumplimiento fuera del rango: 20,61% al 61,49% (desviación estándar) pueden haberse dado por falta de criterio o

desconocimiento por parte de los encuestados, ya que la seguridad informática en los SCI es un tema nuevo y especializado todavía en nuestro medio.

4.3.Documentación de resultados.

Se realizó un resumen ejecutivo para informar a la gerencia sobre los resultados de la evaluación y simulación (ver anexo 12) y así solicitar la aprobación definitiva del manual de normas y políticas de seguridad informática del SCI de COMERCIALIZADORA SAN REMIGIO.

5. CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

Observando los resultados obtenidos en la evaluación y simulación del manual se puede concluir que con el manual de normas y políticas de seguridad para la empresa COMERCIALIZADORA SAN REMIGIO se podrá reducir un 41,05% aproximadamente los incidentes de seguridad de informática de su sistema de control industrial, en sus contextos de disponibilidad, integridad y confidencialidad de información, demostrando así la hipótesis expuesta la cual habla de un valor algo inferior (40%). Valga mencionar que este valor de 40% coincide con la percepción de cumplimiento el manual de calidad que esta empresa posee, por lo que se puede inferir que está ligado a la cultura organizacional de la compañía. Por otro lado también se puede concluir que NIST 800-82 es una normativa internacional muy adecuada para el SCI, por lo que se adapta idóneamente a los ámbitos gerenciales, operativos y técnicos que una empresa industrial de manufactura requiere y mejor funcionalmente a su similar ISO/IEC 27000.

5.2. Recomendaciones.

Se recomienda aprobar, implementar y difundir el manual de normas y políticas de seguridad informática para el SCI de COMERCIALIZADORA SAN REMIGIO, con el fin de reducir los incidentes de seguridad y así evitar pérdidas de información, productividad y dinero. Se hace también hincapié en mantener el manual de seguridad de tal forma que sea una gestión dinámica y acorde a las necesidades cambiantes de las empresas y el mercado de las industrias de manufactura.

6. BLIBLIOGRAFIA

Blank, R., & Gallagher, P. (2013). Security and Privacy Controls for Federal Information Systems and Organizations NIST SP 800-53 (Rev. April). National Institute of Standards and Technology United States.

Bustamante, F., & Díaz, P. (2015). Elaboración de un manual de normas y políticas de seguridad informática de un sistema de control industrial para la empresa Comercializadora San Remigio usando estándares internacionales. Universidad de las fuerzas armadas, Pichincha, Ecuador.

Byres, E., & Lowe, J. (2003). The Myths and Facts behind Cyber Security Risks for Industrial Control Systems. British Columbia Institute of Technology, Burnaby, UK.

Costa, L. (2012). Prospección de tecnologías para aumentar la seguridad en sistemas SCADA. Universidad Federal Tecnológica de Paraná, PR, Brasil.

Cosman, E., Gilsinn, J., & ISA99. (2013). NIST Cybersecurity Framework ISA 99 Response to Request for Information (Rv. April 5). International Society of Automation (ISA), NC, USA.

Francia, A., Thornton, D., & Dawson, J. (2012). Security Best Practices and Risk Assessment of SCADA and Industrial Control Systems. Jacksonville State University, AL, USA.

Guttman, B., & Roback, E. (1995). An Introduction to Computer Security: The NIST HandBook. National Institute of Standards and Technology United States, WA, USA.

ICS-CERT. (2013). Responses to sector specific cybersecurity threat across the critical infrastructure sectors. Industrial Control Systems Cyber Emergency Response Team. U.S Department of Homeland Security.

ISA99. (2012). Security for industrial automation and control systems (Draft 6, Edit 7). International Society of Automation, NC, USA.

ISO/IEC. (2005). Tecnología de la Información – Tecnicas de seguridad – Sistema de gestión de seguridad de la información – Requerimientos (Primera Edición). ISO/IEC Internacional.

ISO/IEC. (2005). Controles ISO 27002-2005 (Ver. 4.0). Recuperado el 16 de enero del 2011, de http://iso27000.es/download/ControlesISO27002.

López, A. (2005). Guías y publicaciones del Portal de ISO 27001 en español. Recuperado el 6 de abril del 2014, de http://www.iso27000.es

Locke, G., & Gallagher, P. (2011). Managing Information Security Risk NIST SP 800-39 (Rev. March). National Institute of Standards and Technology United States.

Locke, G., & Gallagher, P. (2009). Security, Security Control Mappings for ISO/IEC 27001 (Rev. August). National Institute of Standards and Technology United States.

Navarro, O., & Villalón, A. (2013). Una visión global de la ciberseguridad de los sistemas de control. S2 Grupo España (106), 52-55.

NIST I-CAT. (2014). Vulnerability database. Recuperado el 15 de enero del 2014, de http://icat.nist.gov

Stouffer, K., Falco, J., & Scarfone K. (2013). Guide to Industrial Control Systems (ICS) Security NIST SP 800-82 (r1). National Institute of Standards and Technology United States.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). Guide for Conducting Risk Assessments NIST SP 800-30 (Rev. Julio). National Institute of Standards and Technology United States.

Talib, M., Barchi, M., Khelifi A., & Ormandjieva O. (2012). Guide to ISO 27001:UAE Case Study. Issues in informing Science and Information Technology, 7(2012), 331-349

Tieghi, E. (2007). Introduzione alla protezione di reti e sistema di controllo e automazione. Associazione Italiana per la Sicurezza Informatica, Milano, Italia.

Ureña, E. (2008). Sistema de la gestión de la seguridad de la información – SGSI. Recuperado el 6 de abril del 2014, de http://es.scribd.com/doc/73944170/Gestion-de-Seguridad-de-Informacion-SGSI#scribd.

Vertical-Insight. (2014). Data Breach Investigations Report MANUFACTURING, Verizon Enterprise.

Villamizar, C. (2013). Implementando seguridad de la información en sistemas de control industrial. Magazcitum Internacional de Scitum, 4(2), 20-22.

7. ABREVIATURAS Y ACRONIMOS

DCS Sistema de control distribuido.

FBI Oficina federal de investigación

FedCIRC Centro de respuesta a incidentes de computación federal

ICS-CERT Equipo de respuesta a cyber emergencias de los sistemas de control industrial.

IEC Comisión Electrotécnica Internacional

ISO Organización Internacional de Normalización

NIST Instituto nacional de estándares de tecnología

PLC Controlador lógico programable

RFC Petición de cambios

SCADA Control de supervisión y Adquisición de datos

SCI Sistema de Control Industrial

SP Publicación Especial

TI Tecnologías de Información

8. ANEXOS.

8.1.Anexo 1: Levantamiento de requisitos (PREGUNTAS)

Tabla 2.

Encuesta para levantamiento de requisitos

Levantamiento de Requisitos (PREGUNTAS) - Reunión con Usuarios del SCI			
No. Proyecto	**Fecha**	**Título del Proyecto**	**Administrador del Proyecto**
2	01/11/14	ELABORACION DE UN MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN	Ing. Paúl Díaz, Ing. Fabián Bustamante
Número		**Preguntas**	
1		¿quiénes son los usuario válidos del Sistema de Control Industrial (SCI)?	
2		¿cuál es la misión de la empresa?	
3		¿cuál es el propósito del SCI en relación a la misión	
4		¿Cuan importante es el SCI para la misión de la organización?	
5		¿cuál es el requerimiento de disponibilidad del SCI?	
6		¿Que información de entrada y salida es requerida por la organización?	
7		¿qué información es generada, consumida, procesada, almacenada e ingresada por el sistema?	
8		¿Cuan importante es la información para la misión de la organización?	
9		¿cuáles son los caminos del flujo de información?	
10		¿qué tipo de información es procesada por el SCI y almacenada en él?	
11		¿qué nivel de clasificación tiene la información del SCI?	
12		¿cuál es la información manejada por el SCI que no debe ser revelada y a quien?	
13		¿dónde está específicamente la información procesada y almacenada?	
14		¿cuáles e el tipo de información almacenada?	
15		¿cuál es el potencial impacto en la organización si la información es revelada a personal no autorizado?	
16		¿cuáles son los requerimientos para la disponibilidad e integridad de la información?	
17		¿cuál es el efecto en la misión de la organización si la información si el SCI o información no es confiable?	
18		¿cuánto de tiempo sin funcionar puede tolerar el SCI?	
19		¿En este tiempo sin funcionar que otros procesos u opciones de comunicaciones pueden acceder los usuarios?	
20		¿Puede el SCI o un mal funcionamiento de seguridad o indisponibilidad resultar en heridas o muertes?	

Fuente: Comercializadora San Remigio

8.2. Anexo 2: Levantamiento de requisitos (RESPUESTAS)

Tabla 3.

Respuestas de la encuesta de levantamiento de requisitos

Levantamiento de Requisitos (RESPUESTAS) - Reunión con Usuarios del SCI			
No. Proyecto	**Fecha**	**Título del Proyecto**	**Administrador del Proyecto**
2	01/11/14	ELABORACION DE UN MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO	Ing. Paúl Díaz, Ing. Fabián Bustamante
Número		**Preguntas**	
1		Los usuarios del SCI son los Jefes de Turno, Operadores de máquinas de línea de producción 1 y línea de producción 2	
2		Elaborar soluciones de empaques con excelencia de calidad y servicio para nuestros clientes, manteniendo compromiso con la comunidad y el medio ambiente	
3		Fabricar con calidad el producto, al menor costo y en el menor tiempo	
4		Extremadamente importante, puese de este dependen actualmente los procesos de producción	
5		Solamente 14 días al año el sistema puede estar sin funcionar (este tiempo es por mantenimiento)	
6		Entrada: Pedidos de producción (cantidad, tipo de producto, tiempo de entrega, particularidades del producto) Salida: Pedido producido (Cantidad, tipo de producto, tiempo de producción, datos de calidad)	
7		Velocidad de las 2 líneas de producción, temperatura, presión, comuso de tinta, tipo de troqueles, tipo de scores, cantidad producida por máquina, desperdicio, entre los mas importantes.	
8		Esta información es muy importante, pues ayudan a la parte administrativa a obtener datos para atender a clientes, proveedores y los accionistas de la empresa	
9		Planeación -> Jefe de Producción -> Materias Primas -> Linea de Producción 1 -> Línea de Producción 2 -> Calidad -> Despachos	
10		Magnitudes físicas, químicas, información de cantidades de isumos, cantidades de productos, cantidades de desperdicio, tiempos de parada, turnos de operadores	
11		Información de Producción e información contable	
12		Pedidos, cantidades producidas, Configuración de PLC, Planos de Red de datos y de la red de fuerza. No se lo debe revelar a Otras empresas, Personas no registradas en el SCI, Proveedores, entre otros	
13		En computadoras del proceso, PLCs y en la red de datos del SCI	
14		Cantidad y tipo de insumos, Detalles del pedido, Cantidades producidas	
15		Por el tipo de negocio, el grado de impacto a la organización es medio	
16		El SCI debe estar disponible las 24 horas, los 7 días de la semana, excepto 1 día al mes que se realiza parada de mantenimieinto y 1 vez por 3 días para mantenimiento anual	
17		El problema sería principalmente baja calidad, altos costos y tiempos de entrega elevados	
18		14 días al año puede dejar de funcionar el SCI, fuera de este tiempo existen pérdidas económicas, de imagen y reputación con los clientes	
19		Existen los métodos semi automáticos comandados sólo por PLCs, pero en los cambios de pedidos ya no se los podrá ocupar.	
20		Puede ocurrir, sin embargo no directamente por el SCI sino por algunos de sus componentes.	

Fuente: Comercializadora San Remigio

8.3. Anexo 3: Levantamiento de requisitos (CONTROLES)

Tabla 4.

Lista de controles actuales

Levantamiento de Requisitos (CONTROLES) - Reunión con Usuarios del SCI			
No. Proyecto	**Fecha**	**Título del Proyecto**	**Administrador del Proyecto**
2	01/11/14	ELABORACION DE UN MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO	Ing. Paúl Díaz, Ing. Fabián Bustamante
Número		**Lista de Controles Actuales**	**Comentarios**
1		Revisión de contratos de mantenimiento anuales	Principalmente con proveedores internacionales
2		Revisión anual del índice de capacitaciones realizadas	La norma ISO de la empresa exige llevar un índice de capacitaciones
3		Revisar anualmente con un checklist los lugares críticos para revisión de energía eléctrica	Los equipos electrónicos necesitan un buen sistema eléctrico
4		Guardias no permitan el paso de equipos informáticos sin permiso de Gerencia	Esta disposición fue dada por el gerente debido a robos
5		Proceso de entrevistas a nuevos usuarios del SCI	Recursos humanos al momento de contratar realiza entrevistas
6		Mantenimiento preventivo del SCI	1 vez al mes se hace mantenimiento a todas al máquinas y parte del SCI

Fuente: Comercializadora San Remigio

8.4. Anexo 4: Acta de constitución del proyecto

Tabla 5.

Acta de constitución del proyecto

ACTA DE CONSTITUCION DEL PROYECTO			
N° Proyecto	**Fecha**	**Título del Proyecto**	**Encargado del Proyecto**
2	**01-nov-14**	ELABORACION DE UN MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTANDARES INTERNACIONALES	Ing. Paúl Díaz, Ing. Fabián Bustamante
Identificación de la Problemática	El sistema de Control Industrial de Comercializadora San Remigio a crecido y requiere reducir los incidentes de seguridad informática sin invertir mucho dinero.		
Necesidad del Negocio	Requiere implementar un sistema de gestión de seguridad informática en su sistema de control industrial.		
Justificación del Proyecto	El costo de implementar un SGSI en el SCI de Comercializadora San Remigio es muy bajo en comparación con las pérdidas económicas que se pueden presentar.		
Nivel de Autoridad del Encargado del Proyecto	Los encargados del proyecto deberán planificar las actividades, organizar con las personas encargadas del SCI la coordinación de la elaboración del manual, dirigir las reuniones que requieran para este propósito y controlar que el costo, calidad, alcance y tiempo estén de acuerdo a los requerimientos de la empresa.		
Recursos Pre-asignados	Los recursos financieros teniendo en cuenta el auspicio de la empresa por ser un tema de tesis de maestría es: $300 +/- 10% de imprevistos. Recursos Humanos: Ingenieros de Automatización, Ingenieros de Producción, Ingenieros de Mantenimiento e Ingenieros Informáticos		
Principales Riesgos	Gastar más del presupuesto asignado por cualquier eventualidad, No satisfacer los requerimientos de seguridad de Comercializadora San Remigio y superar el teimpo de entrega establecido		
Principales Oportunidades para la Organización	Con este manual, la empresa tiene la oportunidad de implementar más procesos, tecnología y sistemas informáticos en el SCI, reduciendo problemas de confidencialidad, integridad y disponibilidad		
Interesados del proyecto	**Rol**	**INFLUENCIA**	**INTERÉS**
	Gerente General	3: Alto	3: Alto
	Gerente de Automatización	3: Alto	3: Alto
	Gerente de Producción	2: Medio	2: Medio
	Jefe de Mantenimiento	2: Medio	2: Medio
	Jefe de Tecnologías de Información	3: Alto	3: Alto
	Ingeniero de Automatización	2: Medio	3: Alto
	Administrador del Proyecto	2: Medio	3: Alto
	Ingeniero de Infraestructura Informática	1: Bajo	2: Medio
	Proveedores del SCI	1: Bajo	2: Medio
Entregables	**General:**		
	MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA DE UN SISTEMA DE CONTROL INDUSTRIAL		
	Específicos:		
	Manual de normas y políticas de seguridad basado en controles de Gerenciamiento		
	Manual de normas y políticas de seguridad basado en controles operacionales		
	Manual de normas y políticas de seguridad basado en controles técnicos		

Fuente: Comercializadora San Remigio

8.5. Anexo 5: Políticas con controles de tipo Gerencia

Tabla 6.

Resumen de políticas de nivel gerencial implementadas

RESUMEN DE POLITICAS DE NIVEL GERENCIAL IMPLEMENTADAS							
No. Proyecto	**Fecha**	**Titulo de Proyecto**					**Administrador del proyecto**
1	11/11/14	ELABORACION DE UN MANUAL DE NORMAS Y POLITICAS DE SEGURIDAD INFORMATICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTANDARES INTERNACIONALES					Ing. Paúl Díaz, Ing. Fabián Bustamante
NUMERO	**NIST**	**TEMA**	**POLITICA**	**ROL Y RESPONSABILIDAD**	**APLICABILIDAD**	**CUMPLIMIENTO**	**PUNTOS DE CONTACTO**
1	CA	Valoración de los controles de seguridad de información del Sistema de Control Industrial	Los controles del SCI se evaluarán cada año con el fin de mejorar la gestión	Tecnologías de Información, Automatización, Producción y mantenimiento	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI
2	PL	Mantenimiento del plan de seguridad de información del Sistema de Control Industrial	Cada año se realizará un mantenimiento del plan de seguridad de información	Tecnologías de Información, Automatización, Producción y mantenimiento	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI
3	RA	Valoración de riesgos y mitigaciones del Sistema de Control Industrial	Identificación de riesgos de las operaciones y procesos del SCI anualmente	Tecnologías de Información, Automatización, Producción y	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI
4	SA	Adquisición de recursos para una adecuada protección del Sistema de Control Industrial	Recursos de Automatización, Hardware o Software que se adquieran deben ir con visto bueno de Gerente de Automatización o Jefe de TI	Gerente de automatización o Jefe de Tecnologías de Información	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad e infractores se les descontará de rol de pagos.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI

Fuente: Comercializadora San Remigio

Anexo 6: Políticas con controles de tipo Operativo

Tabla 7.

Resumen de políticas de nivel operacional implementadas

RESUMEN DE POLITICAS DE NIVEL OPERACIONAL IMPLEMENTADAS							
No. Proyecto	**Fecha**	**Titulo de Proyecto**					**Administrador del proyecto**
1	11/11/14	ELABORACION DE UN MANUAL DE NORMAS Y POLITICAS DE SEGURIDAD INFORMATICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTANDARES INTERNACIONALES					Ing. Paúl Díaz, Ing. Fabián Bustamante
NUMERO	**NIST**	**TEMA**	**POLITICA**	**ROL Y RESPONSABILIDAD**	**APLICABILIDAD**	**CUMPLIMIENTO**	**PUNTOS DE CONTACTO**
1	PS	Caracterización de posición del personal, tamizaje, transferencia y terminación del contrato (bajo rol)	Responsables del SCI deben ser Ingenieros electrónicos con conocimientos de informática, telecomunicaciones, 5 años de experiencia y firmar acuerdo de confidencialidad	El ingeniero de automatización estará bajo la dirección del gerente de automatización e implementará proyectos y coordinará con otros involucrados.	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
2	PS	Caracterización de posición del personal, tamizaje, transferencia y terminación del contrato (Contratista).	La empresa proveedora contratada para el SCI presentará documentos de suficiencia de sus empleados y firmar acuerdos de confidencialidad.	El contratista colaborará con implementación de proyectos, mantenimiento preventivo y correctivo del SCI Los Ingenieros de automatización serán responsable de selección y tamizaje.	Unicamente al SCI de producción.	El incumplimiento será considerado no conformidad y causa de sanciones económicas inclusive la expulsión del contratista.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
3	PE	Controles de acceso físico, de transmisión, visualización, ambientales y disposiciones de emergencia.	Cuartos de control deben poseer condiciones adecuadas para su funcionamiento: controles de acceso, cámaras, identificadores, aire acondicionado, ups, cableado estructurado, control de inventario	Ingenieros de automatización y de tecnologías de información son responsables de la protección física y ambiental del SCI	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
4	CP	Restauración de operaciones del negocio e informáticas en eventos de emergencia o fallas.	Realizar un plan de desastre-recuperación y un plan de continuidad del negocio para evitar pérdidas de información	Ingenieros de automatización y de tecnologías de información son responsables de elaborar y mantener los planes de desastre-recuperación y plan de continuidad del negocio	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.

CONTINÚA→

5	CM	Control de modificaciones a hardware, firmware, software y documentación al SCI en contra de modificaciones impropias.	Cambios en la infraestructura del SCI necesitan ser documentados formalmente antes del cambio y con firmas de responsabilidad.	Es responsabilidad de los Ingenieros de Automatización, Tecnologías de la información y de mantenimiento	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
6	MA	Aspectos a considerar en el mantenimiento del Sistema de Control Industrial	El mantenimiento preventivo o correctivo de la infraestructura del SCI debe ser coordinado y aceptado por escrito por el superintendente de producción.	Los ingenieros de mantenimiento, automatización y tecnologías de información son responsables de coordinar por escrito el mantenimiento del SCI.	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
7	SI	Protección de los sistema de información y la integridad de los datos	Cada año se documentará la revisión de los sistemas de antivirus, monitoreo de red y gestión de parches del SCI	Los Ingenieros de tecnologias de información, automatización y mantenimiento son responsables de monitorear, notificar y actuar en proteger la información e integridad de datos.	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
8	MP	Aseguramiento de medios, cubiertas de control de acceso, etiquetado, almacenamiento, transporte, sanitización, destrucción y disposición.	La habilitación de medios, reportes impresos y otros documentos del SCI debe ser autorizada por el gerente de área y gerencia general, previo un visto bueno de Tecnologías de Información.	Tecnologías de información es responsable de recolectar la información de los requisitos de los usuarios y hacerlos aprobar con el respectivo gerente de área, dar el visto bueno y hacerlo firmar al gerente general.	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
9	IR	Respuesta a incientes, pruebas, manejo, monitoreo, reporte y servicios de soporte	Los incidentes se clasifican en graves y leves, los cuales deben estar debidamente establecidos sus acciones de respuesta y recuperación	Ingenieros de automatización, mantenimiento y tecnologías de información serán responsables de elaborar formatos, documentos y procedimientos para la clasificación, acción de respuesta y acciones de recuperación.	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.
10	AT	Capacitación del sistema de seguridad informática del SCI en uso y mantenimiento de registros de asistencia.	Anualmente se hará una capacitación de seguridad informática del SCI y sus componentes con el fin de dar a conocer a los usuarios las nuevas tecnologías enfocadas a la confidencialidad, integridad y disponibilidad.	Es responsabilidad de Automatización, Tecnologías de Información y Recursos Humanos realizar un plan de capacitación anual, registrando la asistencia de los participantes.	Unicamente al SCI de producción.	Incumplimientos considerados no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI.

Fuente: Comercializadora San Remigio

8.6. Anexo 7: Políticas con controles de tipo Técnico

Tabla 8.
Resumen de políticas de nivel técnico implementadas

RESUMEN DE POLITICAS DE NIVEL TECNICO IMPLEMENTADAS							
No. Proyecto	**Fecha**	**Titulo de Proyecto**					**Administrador del proyecto**
1	11/11/14	ELABORACION DE UN MANUAL DE NORMAS Y POLITICAS DE SEGURIDAD INFORMATICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTANDARES INTERNACIONALES					Ing. Paúl Díaz, Ing. Fabián Bustamante
NUMERO	**NIST**	**TEMA**	**POLITICA**	**ROL Y RESPONSABILIDAD**	**APLICABILIDAD**	**CUMPLIMIENTO**	**PUNTOS DE CONTACTO**
1	IA	Procesos de verificación e identificación de usuarios o dispositivos	Cambiar contraseñas cada 6 meses y únicamente en los sistemas que no vayan a tener impacto en el SCI	Tecnologías de información, mantenimiento y automatización llevarán el control de cambio de	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI
2	AC	Conseción o denegación de permisos específicos de la información referente a accesos físicos o servicios	El acceso a cuartos de control, servidores web, vlan y redes inalámbricas que conformen el SCI deben ser pre-	Tecnologías de información y automatización son los responsables del control de acceso documentado y formal.	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI
3	AU	Revisión, examinación de registros y actividades para valorar la adecuación de sistemas de control	Realizar anualmente una auditoría de seguridad informática usando un formato previamente elaborado.	Automatización y Tecnologías de Información son responsables de realizar la auditoriía a procesos, tecnología y usuarios del SCI	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad y deberán los responsables pasar un explicación escrita a Gerencia.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI
4	SC	Mecanismos para proteger los sistemas y componentes de transmisión de datos	Todas las conexiones remotas al sistema de control industrial deben ser encriptadas y protegidas con protocolos seguros.	Tecnologías de Información y automatización son responsables de realizar procedimientos técnicos de protección.	Unicamente al SCI de producción	Incumplimientos consideraros no conformidad e infractores se les descontará de rol de pagos.	Jefe de Tecnologías de Información y asesores de seguridad informática del SCI

Fuente: Comercializadora San Remigio

8.7. Anexo 8: Manual de normas y políticas de seguridad del SCI

COMERCIALIZADORA SAN REMIGIO	Manual de normas y políticas de seguridad del Sistema de Control Industrial	Tipo:	NIST SP800-82 CA
		Revisión:	No. 1
		Hoja:	1 de 18

Elaboración	Revisión	Aprobación
Ing. Luis Rodríguez	Econ. María Peña, Ing. Fernando Pesantez	Ing. Jony Gaviño
Cargo: Jefe de TI	Cargo: Jefe Audit, Jefe Desarrollo Org.	Cargo: Gerente General
Fecha: Noviembre / 2014	Fecha: Diciembre / 2014	Fecha: Diciembre / 2014

3.3.1 Valoración de la seguridad y Autorización:

Declaración del tema:

Valoración de los controles de seguridad de información del Sistema de Control Industrial (SCI)

Declaración de la posición de la organización:

Los controles de seguridad de información del SCI se evaluarán cada año con el fin de mejorar la gestión de seguridad continuamente.

Roles y responsabilidades:

Será responsabilidad del Jefe de Tecnologías de información, Gerente de Automatización, Superintendente de producción y el Jefe de Mantenimiento realizar la valoración de los controles de seguridad de información.

Aplicabilidad:

La valoración de los controles de seguridad se aplicarán únicamente al Sistema de Control Industrial utilizados en las plantas de producción.

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsable, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.3.2 Planeación:

Declaración del tema:

Mantenimiento del plan de seguridad de información del Sistema de Control Industrial (SCI)

Declaración de la posición de la organización:

Cada año se realizará un mantenimiento del plan de seguridad de información del SCI con el fin de detectar nuevos tipos de incidentes, asignando nuevos niveles de seguridad e implementando controles de ser necesario.

Roles y responsabilidades:

Será responsabilidad del Jefe de Tecnologías de información, Gerente de Automatización, Superintendente de Producción y Jefe de Mantenimiento encargarse de realizar una revisión del plan de seguridad.

Aplicabilidad:

El mantenimiento del plan de seguridad se aplicarán únicamente al Sistema de Control Industrial utilizados en las plantas de producción.

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsable, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.3.3 Valoración de Riesgos:

Declaración del tema:

Valoración de riesgos y mitigaciones del Sistema de Control Industrial (SCI)

Declaración de la posición de la organización:

Cada año se realizará un proceso identificación de riesgos de las operaciones y procesos del SCI mediante la determinación de ocurrencia, impacto resultante y determinación de controles adicionales para mitigar dicho impacto.

Roles y responsabilidades:

Será responsabilidad del Jefe de Tecnologías de información, Gerente de Automatización, Superintendente de Producción y Jefe de Mantenimiento encargarse de realizar el análisis y valoración de riesgos.

Aplicabilidad:

La valoración de riesgos y mitigaciones se aplicarán únicamente al Sistema de Control Industrial utilizados en las plantas de producción.

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsable, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.3.4 Sistema y adquisición de servicios:

Declaración del tema:

Adquisición de recursos para una adecuada protección del Sistema de Control Industrial (SCI)

Declaración de la posición de la organización:

Los recursos de Automatización, Hardware o Software que se adquieran para el SCI deben ir con una firma de aprobado por el gerente de automatización o el Jefe de Tecnologías de información previo a la autorización final del gerente general.

Roles y responsabilidades:

Personal de mantenimiento o producción deberán solicitar la autorización necesaria para adquirir cualquier recurso del SCI. Será responsabilidad el Gerente de automatización y del Jefe de Tecnologías de Información aprobar o desaprobar la adquisición de recursos para el SCI. El gerente general autorizará la aquisición de recursos para el SCI una vez que verifique las firmas de aprobación respectivas.

Aplicabilidad:

La adquisición de recursos de automatización, hardware o software se aplicarán únicamente al Sistema de Control Industrial utilizados en las plantas de producción.

Cumplimiento:

El incumplimiento de esta política se considerará como una no conformidad y el valor del recurso adquirido será descontado por rol de pagos al infractor.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.1a Seguridad del Personal - Personal en relación de dependencia

Declaración del tema:

Caracterización de posición del personal, tamizaje, transferencia, penalidades y terminación de contrato del personal contratado bajo rol usuario del SCI.

Declaración de la posición de la organización:

Los empleados de la empresa responsables del Sistema de Control Industrial deberán ser Ingenieros electrónicos con conocimientos de informática y telecomuniaciones con un mínimo de 5 años de experiencia. Junto con el contrato de trabajo el empleado deberá firmar un acuerdo de confidencialidad.

Roles y responsabilidades:

El Ingeniero encargado del SCI tendrá el cargo de Ingeniero de automatización, será responsable del diseño de nuevos proyectos, del mantenimiento preventivo y correctivo de todos los componentes en coordinción con los departamentos de producción, mantenimiento y tecnologías de información. Reportará directamente al Gerente de automatización.

El departamento de Recursos Humanos será responsable de la correcta selección y tamizaje del personal en coordinación con el Gerente de Automatización y Jefe de Tecnologías de Información.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsable, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.1b Seguridad del Personal - Personal sin relación de dependiencia (Contratista)

Declaración del tema:

Caracterización de posición del personal, tamizaje, transferencia, penalidades y terminación de contrato del personal contratado como tercerizado (Contratista)

Declaración de la posición de la organización:

La empresa proveedora contratada para el SCI deberá presentar los documentos de sus empleados que demuestren suficiencia y experiencia profesional en las áreas de Electrónica, informática, automatización y electricidad industrial, los cuales deben firmar acuerdos de confidencialidad.

Roles y responsabilidades:

El proveedor de servicios será denominado contratista y será responsable de colaborar en la implementación de proyectos, mantenimiento preventivo y correctivo del SCI y estará subordinado a los ingenieros de automatización de la empresa.

Los Ingenieros de automatización, de Tecnologías de Información o de mantenimiento serán los responsables de la selección y tamizaje del personal contratista del SCI.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será considerada una no conformidad y causa de sanciones económicas, inclusive la expulsión del contratista.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.2 Protección física y ambiental (PE):

Declaración del tema:

Controles de accesos físicos, de transmisión, vizualización, ambientales y disposiciones de emergencia.

Declaración de la posición de la organización:

Los cuartos de control del SCI deben poseer todas las condiciones adecuadas para su funcionamiento como son: Puertas de acceso con seguridad, equipos electrónicos de control de acceso, cámaras de monitoreo, identificaciones de personal y de equipos, equipos de aire acondicionado, equipos de UPS, control de equipos portátiles y uso de cableado adecuado para fuerza, datos y conexión de PLCs.

Roles y responsabilidades:

Los ingenieros de Automatización y de tecnologías de información son los responsables de que la protección física y ambiental del SCI se cumpla correctamente.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsable, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.3 Plan de Contingencia

Declaración del tema:

Restauración de operaciones del negocio e informáticas en eventos de emergencia o fallas.

Declaración de la posición de la organización:

Los encargados del SCI deberán realizar un plan de desastre-recuperación y un plan de continuidad del negocio debidamente analizado por todas la áreas involucradas y aprobado por la gerencia general con el fin de evitar pérdidas de información y así asegurar la continuidad de las operaciones de la planta.

Roles y responsabilidades:

Los ingenieros de automatización y de Tecnologías de Información son los responsables de elaborar y dar mantenimiento de los planes de desastre-recuperación y plan de continuidad del negocio.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.4 Gestión de configuración

Declaración del tema:

Control de modificaciones a hardware, firmware, software y documentación al SCI en contra de modificaciones impropias.

Declaración de la posición de la organización:

Todos los cambios en la infraestructura del SCI como hardware, software, firmware y documentación, necesitan ser documentados formalmente antes de proceder con la ejecución del cambio o modificación, estos documentos deben estar debidamente firmados por los involucrados.

Roles y responsabilidades:

Es responsabilidad de los Ingenieros de Automatización, Tecnologías de la información y de mantenimiento llevar un procedimiento para control de cambios.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.5 Mantenimiento

Declaración del tema:

Aspectos a considerar en el mantenimiento del Sistema de Control Industrial

Declaración de la posición de la organización:

Cualquier mantenimiento preventivo o correctivo del SCI refentes a: Equipo electrónico, de automatización, hardware o software debe ser debidamente coordinado y aceptado por escrito por el superintendente de producción a cargo, previo a realizarse cualquier trabajo o maniobra considerada de posible impacto.

Roles y responsabilidades:

Los ingenieros de Mantenimiento, Automatización y Tecnologías de información son los responsables de coordinar por escrito los trabajos y maniobras de mantenimiento del SCI.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.6 Integridad del sistema e información

Declaración del tema:

Protección de los sistema de información y la integridad de los datos

Declaración de la posición de la organización:

Cada año se realizará una revisión de los sitemas de antivirus, monitoreo de red y gestión de parches de todo el Sistema de Control industrial y se lo documentará por escrito para las acciones correctivas respectivas.

Roles y responsabilidades:

Es responsabilidad de los ingenieros de Tecnologías de información, automatización y mantenimiento: monitorear, notificar y actuar en la protección de información e integridad de datos.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.7 Protección de medios

Declaración del tema:

Aseguramiento de medios, cubiertas de control de acceso, etiquetado, almacenamiento, transporte, sanitización, destrucción y disposición.

Declaración de la posición de la organización:

La habilitación de floppy disks, cd/dvd drives, usbs, memory sticks, reportes impresos y otros documentos del SCI debe estar autorizada por el gerente de área del usuario que requiere estos accesos y luego del gerente de la empresa con el previo visto bueno de Tecnologías de Información.

Roles y responsabilidades:

Es responsabilidad de Tecnologías de información recolectar la información de los requisitos del usuarios y hacerlos aprobar con el respectivo gerente de área, dar el visto bueno y hacerlo firmar al gerente general.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.8 Respuesta a incidentes:

Declaración del tema:

Respuesta a incientes, pruebas, manejo, monitoreo, reporte y servicios de soporte

Declaración de la posición de la organización:

Los incidentes de seguridad de información del SCI se clasificarán en incidentes graves y leves, los cuales deben estar debidamente establecidos sus acciones de respuesta y acciones de recuperación.

Roles y responsabilidades:

Los ingenieros de Automatización, mantenimiento y tecnologías de información serán los responsables de elaborar formatos, documentos y procedimientos adecuados para la clasificación, acción de respuesta y recuperación luego de un incidentes de seguridad de información.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.4.9 Entrenamiento y concienciación

Declaración del tema:

Capacitación del sistema de seguridad informática del SCI en uso y mantenimiento de registros de asistencia.

Declaración de la posición de la organización:

Cada año se dará una capacitación de seguridad informática del Sistema de Control Industrial y sus componentes con el fin de dar a conocer a los usuarios sobre las nuevas tecnologías en los contextos de Confidencialidad, Integridad y disponibilidad.

Roles y responsabilidades:

Es resonsabilidad de los ingenieros de Automatización, Tecnologías de Información y Recursos Humanos realizar un plan de capacitación anual con los respectivos registros de asistencia en lo referente a la seguridad informática del SCI.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

COMERCIALIZADORA SAN REMIGIO	Manual de normas y políticas de seguridad del Sistema de Control Industrial	Tipo:	NIST SP800-82 IA
		Revisión:	No. 1
		Hoja:	15 de 18

Elaboración	Revisión	Aprobación
Ing. Luis Rodríguez, Ing. Fabián Bustamante, Ing. Paúl Díaz	Econ. María Peña, Ing. Fernando Pesantez	Ing. Jony Gaviño
Cargo: Jefe de TI, Asesores SCI	Cargo: Jefe Audit, Jefe Desarrollo Org.	Cargo: Gerente General
Fecha: Noviembre / 2014	Fecha: Diciembre / 2014	Fecha: Diciembre / 2014

3.5.1 Identificación y autenticación

Declaración del tema:

Procesos de verificación e identificación de usuarios o dispositivos

Declaración de la posición de la organización:

Se realizarán cambios de contraseña cada 6 meses y únicamente en los sistemas que no sean críticos o que no vayan a ser afectados por dicho cambio y teniendo en cuenta que sean de conocimiento para todos los operadores del SCI.

Roles y responsabilidades:

Es responsabilidad de los departamentos de Tecnologías de información, mantenimiento y automatización llevar un control del cambio de contraseñas de tal forma que no interrumpan las labores de los operarios del SCI

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.5.2 Identificación y autenticación

Declaración del tema:

Conseción o denegación de permisos específicos de la información referente a accesos físicos o servicios relacionados con el ambiente del SCI.

Declaración de la posición de la organización:

El acceso a cuartos de control, servidores web, vlan y redes inalámbricas que conformen el SCI deben ser previamente aprobados por Automatización y Tecnologías de Información.

Roles y responsabilidades:

Los Ingenieros de Tecnologías de Información y Automatización son los responsables de realizar procedimientos para controlar los accesos de una manera documentada y formal.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.5.3 Auditoría y rendición de cuentas

Declaración del tema:

Revisión, examinación de registros y actividades para valorar la adecuación de sistemas de control

Declaración de la posición de la organización:

Anualmente se realizará una auditoría de seguridad informática usando un formato previamente elaborado con el fin de evaluar todos los puntos de este manual de normas y políticas de seguridad del sistema de control industrial.

Roles y responsabilidades:

Los ingenieros de Automatización y Tecnologías de información son responsables de realizar una auditoría a todos los procesos, tecnología y usuarios del SCI.

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

3.5.4 Protección del sistema y las comunicaciones:

Declaración del tema:

Mecanismos para proteger los sistemas y componentes de transmisión de datos

Declaración de la posición de la organización:

Todas las conexiones remotas al sistema de control industrial deben ser encriptadas y protegidas con protocolos seguros de comunicación como son conexiones vpn y https.

Roles y responsabilidades:

Es responsabilidad de los ingenieros de Tecnologías de información y Automatización realizar procedimientos técnicos para proteger las conexiones al SCI

Aplicabilidad:

Esta política aplica a toda el área de producción de la empresa en la que intervenga el SCI

Cumplimiento:

El incumplimiento de esta política será tomada como una no conformidad y necesitará una explicación escrita de los responsables, dirigida a la gerencia.

Puntos de Contacto e información suplementaria:

Para cualquier duda sobre esta política se podrá consultar al Jefe de Tecnologías de información de la empresa o a los asesores de seguridad informática del SCI.

8.8. Anexo 9: Diseño de Estrategias de Mitigación, proyecto I.

Tabla 9.
Estrategias de mitigación y controles seleccionados 1er Proyecto.

Estrategias de Mitigación y Controles seleccionados					
No. Proyecto	**Fecha**	**Titulo de Proyecto**		**Administrador del proyecto**	
1	10/09/14	Diseño de Estrategias de Mitigación para mejorar la seguridad de información del SCI en la empresa COMERCIALIZAODRA SAN REMIGIO		Ing. Paúl Díaz, Ing. Fabián Bustamante	
Número	**ESTRATEGIA / CONTROL**		**Seleccionado**	**Comentario**	**Responsables**
1	Implementar antivirus y firewall en la red del SCI		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de Información y Automatización
2	Implementar una aplicación que maneje control de cambios y backups		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de Información y Automatización
3	Implementar un sistema de cámaras de seguridad en cuartos de control y talleres		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de información, Automatización y mantenimiento
4	Implementar una aplicación para gestion de activos e inventarios		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de información, Automatización y mantenimiento
5	Implementar un nuevo sistema para control de corte con equipos de contingencia		NO	El costo de implementación es mucho mayor que el no implementar, Se acepta el riesgo	Tecnologías de información, Automatización y mantenimiento
6	Implementar un nuevo sistema para control de corte con equipos de contingencia		NO	El costo de implementación es mucho mayor que el no implementar, Se acepta el riesgo	Tecnologías de información, Automatización y mantenimiento
7	Adquirir otro PLC para Control de Calidad y respaldar programas		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Automatización y mantenimiento
8	Implementar un sistema de autenticación en equipos del SCI y respaldos diarios		SI	A pesar de que el costo de implementación es menor que el no implementar, la diferencia no es tan alta	Tecnologías de Información y Automatización
9	Implementar controles de acceso en cuartos de control		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de información, Automatización y mantenimiento
10	Implementar un procedimiento de coordinación entre Automatización y Tecnologías de Información		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de información, Automatización, mantenimiento y producción
11	Adquirir otro equipo y licencias de programas principales para el mantenimiento del SCI		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de información, Automatización y mantenimiento
12	Adquirir equipos HMI de repuesto		NO	A pesar de que el costo de implementación es menor que el no implementar, la diferencia no es tan alta	Automatización y mantenimiento
13	Documentar algoritmos y programas para cambios de PLC		SI	El costo de implementación es mucho menor que el no implementar, vulnerabilidad existente	Tecnologías de información, Automatización y mantenimiento
14	Adquirir una pantalla de repuesto		NO	A pesar de que el costo de implementación es menor que el no implementar, la diferencia no es tan alta	Automatización y mantenimiento

Fuente: Bustamante & Díaz, 2015

8.9. Anexo 10: Resultados de la evaluación de aceptación del manual.

Tabla 10.

Cuestionario para evaluación del manual

CUESTIONARIO PARA EVALUACION DEL MANUAL					
No. Proyecto		**Titulo de Proyecto**			**Administrador del proyecto**
1		ELABORACION DE UN MANUAL DE NORMAS Y POLITICAS DE SEGURIDAD INFORMATICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTANDARES INTERNACIONALES			Ing. Paúl Díaz, Ing. Fabián Bustamante
NUMERO	**TEMA**	**NUMERO DE ENCUESTADOS**	**RESUMEN DE RESPUESTAS**	**% DE ACEPTACION**	**FUNCIONARIOS ENCUESTADOS**
1	¿Cree que la empresa necesita de un manual de normas y políticas de seguridad informática para el SCI?. ¿por qué?	10	Si, Incidentes de seguridad en aumento cada año, La competencia obliga a estar actualizados	90%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
2	¿Ha escuchado de NIST o algún otro estándar de seguridad de información?. ¿cuál?	10	NO (La mayoría), El estandar mas escuchado es ISO 27000. Los que han escuchado NIST lo asocian con temas de Industria.	30%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
3	¿Estima que el manual cumple con los objetivos estratégicos de la empresa en cuanto a la confidencialidad de información del SCI?. ¿por qué?	10	SI, Porque toca aspectos de protección de información. La información de producción es muy sensible.	80%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
4	¿Estima que el manual cumple con los objetivos estratégicos de la empresa en cuanto a la integridad de información del SCI?. ¿por qué?	10	SI, Porque habla de manejo del conocimiento y control de cambios. Las configuraciones son críticas en producción.	80%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
5	¿Estima que el manual cumple con los objetivos estratégicos de la empresa en cuanto a la disponibilidad de información del SCI?. ¿por qué?	10	SI, Porque cuida de los procesos de disponibilidad y continuidad del negocio. Los servicios de planta son críticos y no pueden fallar	100%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
6	¿Estima que el manual es objetivo y práctico a la realidad de la empresa?. ¿por qué?	10	SI, Se requiere procesos concienciación para evitar confundir sobre algunos términos técnicos.	90%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
7	¿Estima que este manual genera confianza y es comprensible al personal que lo aplicará?. ¿por qué?	10	SI, Se requiere procesos concienciación para evitar confundir sobre algunos términos técnicos.	90%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
8	¿Cree que este manual puede llegar a ser una camisa de fuerza para el proceso de fabricación?. ¿por qué?	10	SI, porque con referencia a lo actual, estas políticas crearán reacción al cambio en la gente. NO, porque son políticas sencillas de cumplir.	70%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
9	¿Cree Ud. Que las políticas de seguridad de tipo Gerencial podrían reducir los incidentes de seguridad informática?. ¿por qué?	10	SI, Porque irá como disposición gerencial. No, Porque los problemas son más operativos.	60%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
10	¿Cree Ud. Que las políticas de seguridad de tipo Operacional podrían reducir los incidentes de seguridad informática?. ¿por qué?	10	SI, Porque ataca directamente a evitar se den los incidentes de seguridad	90%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos
11	¿Cree Ud. Que las políticas de seguridad de tipo Técnico podrían reducir los incidentes de seguridad informática?. ¿por qué?	10	SI, Porque ataca directamente a evitar se den los incidentes de seguridad	90%	Gerente de Automatización, Ingeniero de automatización, Jefe de Mantenimiento, Superintendente de producción, Jefe de Tecnologías de información, Jefe de Desarrollo Organizacional, Gerente de Desarrollo Organizacional, Jefe de Recursos Humanos, Jefe de Auditoría y Gerente de Proyectos

Fuente: Comercializadora San Remigio

Tabla 11.

Proceso estadístico de la evaluación de aceptación del manual

Porcentaje de Aceptación (%)	Frecuencia	Frecuencia acumulada	Porcentaje de Aceptación - Media	(Porcentaje de Aceptación - Media)^2
30	1	1	-49,09	2409,92
60	1	2	-19,09	364,46
70	1	3	-9,09	82,64
80	2	5	0,91	0,83
90	5	10	10,91	119,01
100	1	11	20,91	437,19

Media:	79,09%
Moda:	90%
Mediana:	75%
Varianza:	569,01
Desviación estandar:	23,85%

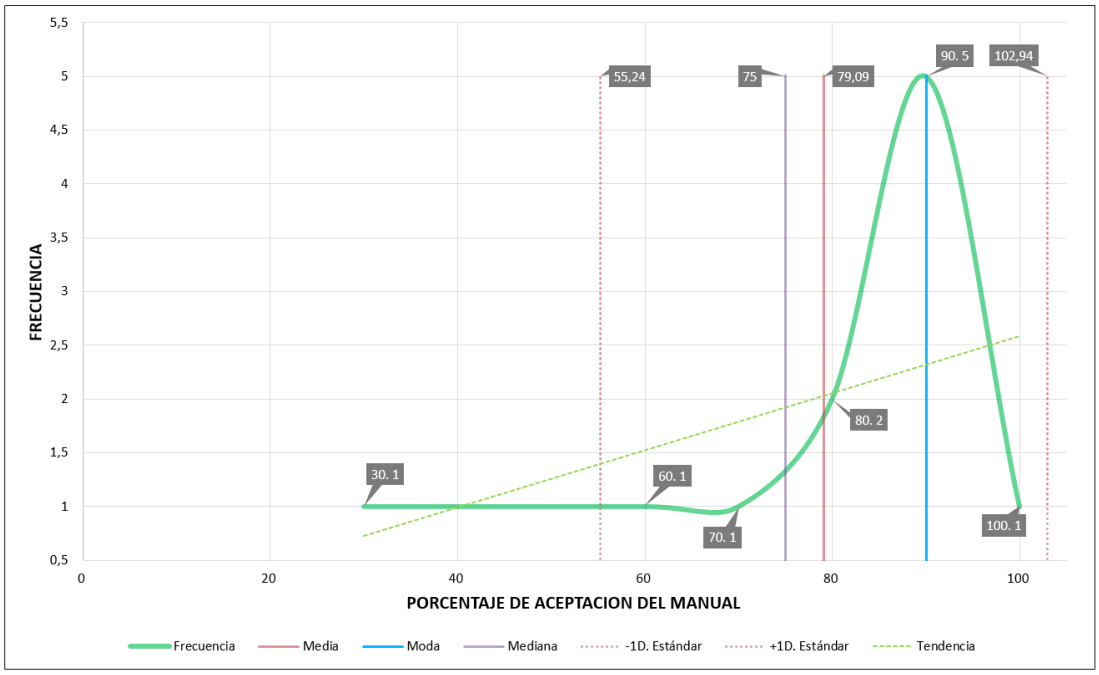

Figura 2. Resultante del proceso estadístico de la evaluación del manual

8.10. Anexo 11: Simulación de uso de manual de normas y políticas de seguridad informática.

Tabla 12.

Resultados de la simulación de aplicar el manual de normas y políticas de seguridad informática

Resultados de la Simulación de implementar el manual de normas y políticas de seguridad en el SCI de Comercializadora San Remigio									
No. Proyecto	**Fecha**	**Titulo de Proyecto**							**Administrador del proyecto**
1	26/12/14	ELABORACION DE UN MANUAL DE NORMAS Y POLITICAS DE SEGURIDAD INFORMATICA DE UN SISTEMA DE CONTROL INDUSTRIAL PARA LA EMPRESA COMERCIALIZADORA SAN REMIGIO USANDO ESTANDARES INTERNACIONALES							Ing. Paúl Díaz, Ing. Fabián Bustamante
NUMERO	**INCIDENTE DE SEGURIDAD**	**ACCION A TOMAR**	**POLITICA QUE SE APLICARIA**	**PERCEPCION DE CUMPLIMIENTO SEGÚN:**					**COMENTARIO**
				Automatiza-ción	**Tecnologías de Información**	**Manteni-miento**	**Producción**	**Promedio**	
1	Infeccionn de virus y malware en red del SCI	Implementar antivirus y firewall en la red del SCI	3.4.6 Integridad del sistema e información	40,0%	55,0%	40,0%	30,0%	41,5%	Producción es pesimista que la política funcione correctamente
2	Pérdida de información y errores de configuraciones en el SCI	Implementar una aplicación que maneje control de cambios y backups	3.4.4 Gestión de configuración	37,5%	45,0%	40,0%	30,0%	38,0%	TI con la experiencia del SGSI ISO, piensa que esta política tendrá acogida.
3	Robo de equipos y dispositivos que conforman el SCI	Implementar un sistema de cámaras de seguridad en cuartos de control y talleres	3.3.4 Sistema y adquisición de servicios	42,5%	45,0%	42,5%	40,0%	42,5%	Mantenimiento y producción por experiencia dicen que esta política no funcionará bien.
4	Infraestructura crítica sin asegurar	Implementar una aplicación para gestion de activos e inventarios	3.3.4 Sistema y adquisición de servicios	42,5%	50,0%	37,5%	30,0%	40,0%	TI con la experiencia del SGSI ISO, piensa que esta política será eficaz
5	Daño de PLC de Control de Calidad en 2da línea de producción	Adquirir otro PLC para Control de Calidad y respaldar programas	3.3.4 Sistema y adquisición de servicios y 3.4.4 Gestión de configuración	40,0%	45,0%	40,0%	41,7%	42,0%	Casi todos acertaron en la percepción que se tiene de esta política.
6	Alteración intencional de información del SCI	Implementar un sistema de autenticación en equipos del SCI y respaldos diarios	3.4.2 Protección física y ambiental	40,0%	48,3%	40,0%	40,0%	42,5%	Mantenimiento cree que esto no funcionará bien.
7	Fallas en la disponibilidad del SCI por sabotaje	Implementar controles de acceso en cuartos de control	3.4.2 Protección física y ambiental	45,0%	45,0%	40,0%	35,0%	41,0%	Producción indica que a pesar de las políticas la gente se da modos de molestar
8	Inversiones en infraestructura de seguridad erroneas	Implementar un procedimiento de coordinación entre Automatización y Tecnologías de Información	3.3.4 Sistema y adquisición de servicios	40,0%	50,0%	35,0%	40,0%	42,0%	Mantenimiento tiene otro método de llevar control de equipos.
9	Falla de computador Laptop para mantenimiento del SCI	Adquirir otro equipo y licencias de programas principales para el mantenimiento del SCI	3.3.4 Sistema y adquisición de servicios y 3.4.4 Gestión de configuración	40,0%	45,0%	40,0%	35,0%	40,0%	Solamente producción estima que para esto debe estar TI en turnos rotativos
10	Falla de PLC Allen Bradley del cuarto de control 3	Documentar algoritmos y programas para cambios de PLC	3.3.4 Sistema y adquisición de servicios y 3.4.4 Gestión de configuración	42,5%	45,0%	40,0%	36,7%	41,0%	Automatización y TI coinciden en que esto evitará incidentes.

Fuente: Comercializadora San Remigio

Tabla 13.

Proceso estadístico de la percepción de cumplimiento del manual

% de Percepción	Frecuencia	Frecuencia Acumulada	%Percepción - Media	(%Percepción - Media)^2
15	4	4	-26,05	678,60
20	5	9	-21,05	443,10
25	13	22	-16,05	257,60
30	10	32	-11,05	122,10
35	8	40	-6,05	36,60
40	16	56	-1,05	1,10
45	11	67	3,95	15,60
50	12	79	8,95	80,10
55	5	84	13,95	194,60
60	9	93	18,95	359,10
65	4	97	23,95	573,60
75	2	99	33,95	1152,60
80	1	100	38,95	1517,10

Media:	41,05%
Moda:	40%
Mediana:	45%
Varianza:	417,83
Desviación estandar:	20,44%

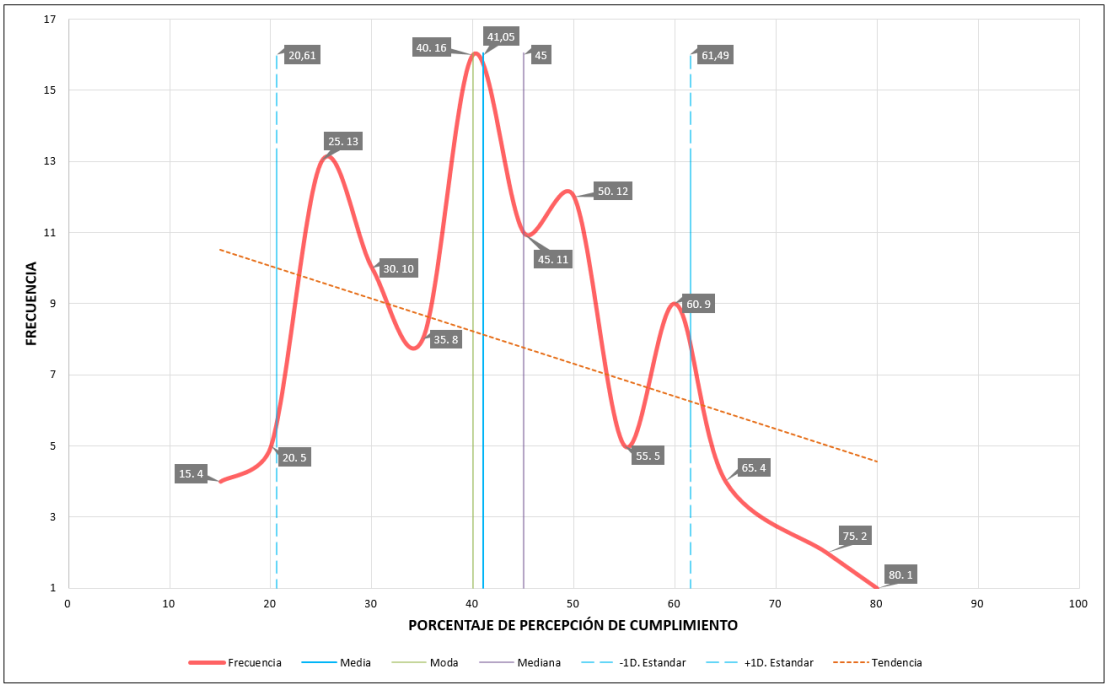

Figura 3. Resultante del proceso estadístico de la percepción de cumplimiento.

8.11. Anexo 12: Resumen ejecutivo de la evaluación y simulación del manual

Resultados de la evaluación y simulación del uso del MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA del Sistema de Control Industrial de Comercializadora San Remigio basado en estándares internacionales.

Autores: Ing. Paúl Díaz, Ing. Fabián Bustamante.
Cuenca, 29 de diciembre del 2014

Resumen Ejecutivo.-

En el siguiente resumen ejecutivo sírvase encontrar los resultados evaluación y simulación del uso del MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA del Sistema de Control Industrial de Comercializadora San Remigio basado en estándares internacionales:

a) **Organizaciones y departamentos involucrados,**
COMERCIALIZADORA SAN REMIGIO, Gerencia General, Gerencia de Automatización, Producción, Mantenimiento y Tecnologías de Información.

b) **Objetivo,**
Informar a la Gerencia General sobre los resultados obtenidos luego de la evaluación y simulación del uso del MANUAL DE NORMAS Y POLÍTICAS DE SEGURIDAD INFORMÁTICA del Sistema de Control Industrial en el área de Producción.

c) **Antecedentes,**
La empresa COMERCIALIZADORA SAN REMIGIO, actualmente cuenta con un Sistema de Control Industrial el cual ha ido implementándose y creciendo desordenadamente en el tiempo, lo cual a provocado que sucedan incidentes de seguridad relacionados con la disponibilidad, confidencialidad e integridad de la información y activos de la empresa, llegándose a reportar hasta 5 incidentes mensualmente al soporte técnico de tecnologías de información. Por lo que se ha elaborado con ayuda de expertos en seguridad informática un manual de normas y políticas de seguridad que ayudarán a gestionar la seguridad de la información del SCI efectivamente.

d) **Resultados de la evaluación,**
Luego de un análisis guiado por los ejecutivos del departamento de desarrollo organizacional de la empresa y encuestado a las áreas de Automatización, Tecnologías de Información, Mantenimiento y Producción, los resultados de la evaluación del manual según: "el porcentaje promedio de aceptación" del anexo 10 es de 79.09%. El total de encuestados fue de 10 personas y un total de 11 preguntas concretas y alineadas con el plan estratégico de la organización. Para evidencia del proceso de evaluación se resumieron y documentaron las respuestas en la columna: "Resumen de respuestas" del mismo anexo. Los resultados de la simulación se adjuntan en el anexo 11 e indican un promedio de 41.05% de percepción de cumplimiento. El procedimiento usado para sacar este resultado fue también sugerido por los ejecutivos de la empresa y consistió en realizar un proceso estadísticos con los porcentajes de percepción de cumplimiento del manual según las experiencias de manuales de políticas ya implementados anteriormente en la empresa (ejemplo: manual de calidad de la empresa). Las áreas que participaron en esta simulación fueron igualmente: Automatización, Tecnologías de Información, mantenimiento y Producción. Se simularon 10 incidentes de seguridad, tomados de los 5 últimos años de entre los que más se repetían y eran considerados un problema para la

empresa. Según se puede observar en este anexo se tiene la mayoría de valores de percepción de cumplimiento en un rango de 15% al 80% y se observa que se aplican máximo 6 políticas de las 18 que contiene todo el manual.

e) **Conclusiones y recomendaciones,**

De acuerdo a los resultados obtenidos y a la necesidad de la empresa COMERCIALIZADORA SAN REMIGIO de mejorar la gestión de seguridad informática, se concluye que el manual de normas y políticas de seguridad de la empresa tendrá un nivel de cumplimiento de 41.05%, el cual depende mucho de la cultura organizacional y las acciones disciplinares que la alta gerencia aprueben y contenidas en dicho manual. Por otro lado se puede que el manual tiene un alto nivel de aceptación (79.09%) entre los stakeholders, por lo que tiene alta probabilidad de ser implementada en un corto o mediano plazo. Por tanto se recomienda la aprobación del manual.

Atentamente,
Ing. Paúl Diaz, Ing. Fabián Bustamante