DEPARTAMENTO DE CIENCIAS DE LA COMPUTACION

MAESTRIA EN GERENCIA EN SISTEMAS

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

TEMA: DISEÑO DE ESTRATEGIAS DE MITIGACIÓN PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DEL SISTEMA DE CONTROL INDUSTRIAL EN LA EMPRESA COMERCIALIZADORA SAN REMIGIO.

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 **DISEÑO DE ESTRATEGIAS DE MITIGACIÓN PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DEL SISTEMA DE CONTROL INDUSTRIAL EN LA EMPRESA COMERCIALIZADORA SAN REMIGIO**, 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 **DISEÑO DE ESTRATEGIAS DE MITIGACIÓN PARA MEJORAR LA SEGURIDAD DE INFORMACIÓN DEL SISTEMA DE CONTROL INDUSTRIAL EN LA EMPRESA COMERCIALIZADORA SAN REMIGIO**, 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.

AGRADECIMIENTO

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.

Paul Díaz.

INDICE DE CONTENIDO

Certificación de autenticidad del Director de tesis ii

Autorización y/o restricciones para la publicación de la tesis iv

AGRADECIMIENTO vi

INDICE DE CONTENIDO vii

INDICE DE TABLAS viii

ABSTRACT xi

1. CAPÍTULO I – INTRODUCCION 1
- **1.1. Antecedentes 1**
- **1.2. Justificación e importancia 1**
- **1.3. Planteamiento del problema 1**
- **1.4. Formulación del problema 2**
- **1.5. Hipótesis 2**
- **1.6. Objetivo General 2**
- **1.7. Objetivos Específicos 3**

2. CAPITULO II: FUNDAMENTACION TEORICA 4
- **2.1. Incidentes de seguridad en Sistemas de Control Industrial 4**
- **2.2. Los Sistemas de Control Industrial (SCI) 6**
- **2.3. Evaluación de estándares para el Análisis y Evaluación de vulnerabilidades, amenazas y Riesgos en los SCI. 8**

3. CAPITULO III: DISEÑO DE ESTRATEGIAS DE MITIGACION 10
- **3.1. Caracterización del sistema 10**
- **3.2. Identificación de amenazas 12**
- **3.3. Identificación de vulnerabilidades 15**
- **3.4. Análisis de controles 19**
- **3.5. Determinación de probabilidad 21**
- **3.6. Análisis de impacto 22**
- **3.7. Determinación del riesgo 25**

4. CAPITULO IV: EVALUACION, VERIFICACION Y VALIDACION DE RESULTADOS 27
- **4.1. Recomendaciones de control 27**
- **4.2. Documentación de resultados. 31**
- **4.3. Simulación de solución 31**

5. CAPITULO V: CONCLUSIONES Y RECOMENDACIONES 33
- **5.1. Conclusiones. 33**
- **5.2. Recomendaciones. 33**

6. BLIBLIOGRAFIA 34

7. ABREVIATURAS Y ACRONIMOS 36

8. ANEXOS. 37
8.1. Anexo 1: Encuesta de infraestructura, procedimientos y usuarios del SCI 37
8.2. Anexo 2: Caracterización del sistema 39
8.3. Anexo 3: Lista de fuentes de amenazas 40
8.4. Anexo 4: Fuentes de vulnerabilidad 41
8.5. Anexo 5: Lista de controles 42
8.6. Anexo 6: Riesgos del sistema de control industrial 43
8.7. Anexo 7: Riesgos del hardware y software usados en mantenimiento 44
8.8. Anexo 8: Riesgos del hardware, software y plcs usados en 1ra línea de producción 45
8.9. Anexo 9: Riesgos del hardware, software y plcs 2da línea de producción. 46
8.10. Anexo 10: Ranking de riesgos del sistema de control industrial 47
8.11. Anexo 11: Lista de estrategias de mitigación recomendadas 48
8.12. Anexo 12: Análisis Costo – Beneficio 49
8.13. Anexo 13: Estrategias de mitigación y controles seleccionados 50
8.14. Anexo 14: Resumen Ejecutivo de los resultados 51
8.15. Anexo 15: Resultados de simulación al aplicar estrategias de mitigación y controles en el SCI. 53
8.16. Anexo 16: Diagrama de red del SCI de Comercializadora San Remigio. 54
8.17. Anexo 17: Fotos de infraestructura crítica del SCI. 55
8.18. Anexo 18: Pantallas del software usado en el SCI. 56

INDICE DE TABLAS

Tabla 1. Amenazas, Motivación y acciones de la amenaza 13
Tabla 2. Criterios de Seguridad 18
Tabla 3. Definición de la probabilidad 22
Tabla 4. Definición de Impacto 24
Tabla 5. Escalas de probabilidad e impacto 26
Tabla 6. Caracterización del SCI 39
Tabla 7. Fuentes de amenazas 40
Tabla 8. Fuentes de vulnerabilidad 41
Tabla 9. Lista de controles 42
Tabla 10. Riegos del SCI 43
Tabla 11. Riesgos del hardware y software 44
Tabla 12. Riesgos de hardware y software 1ra línea de producción. 45
Tabla 13. Riesgos de hardware y software 2da línea de producción. 46
Tabla 14. Ranking de riesgos 47
Tabla 15. Estrategias de mitigación recomendadas 48
Tabla 16. Análisis costo - beneficio 49
Tabla 17. Estrategias de mitigación y controles seleccionados 50
Tabla 18. Resultados de simulación. 53

INDICE DE FIGURAS

Figura 1. Respuestas del ICS-CERT en el 2013 por sector. 4
Figura 2. Incidentes de manufactureras vs todas las industrias. 5
Figura 3. Ejemplo de un Sistema de Control Industrial DSC. 7
Figura 4. Metodología valoración de riesgos. 9
Figura 5. Sinóptico de caracterización del sistema 10
Figura 6. Sinóptico de identificación de amenazas 12
Figura 7. Sinóptico de Identificación de vulnerabilidades. 15
Figura 8. Sinóptico del Análisis de controles 19
Figura 9. Sinóptico de la determinación de probabilidad 21
Figura 10. Sinóptico del análisis del impacto 22
Figura 11. Sinóptico de la determinación del riesgo 25
Figura 12. Sinóptico de las recomendaciones de control 27
Figura 13. Metodología la mitigación de riesgos y aplicar controles. 30
Figura 14. Sinóptico de documentación de resultados 31
Figura 15. Diagrama de red del SCI 54
Figura 16. Foto de HMI 1ra línea de producción. 55
Figura 17. Foto de PLC principal 1ra línea de producción. 55
Figura 18. Foto de PLC principal 2da línea de producción 56
Figura 19. Pantalla principal del software utilizado en la 1ra línea de producción. 56
Figura 20. Pantalla principal del software utilizado en 2da línea de producción. 57

RESUMEN

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

PALABRAS CLAVE:

- **SISTEMA DE CONTROL INDUSTRIAL**
- **NIST**
- **ISO**
- **RIESGO,**
- **AMENAZA**
- **VULNERABILIDAD**
- **ISA 99**
- **CONTROLES**
- **SGSI**

ABSTRACT

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

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

Luego de una búsqueda de temas similares o relacionados con este proyecto de tesis se puede indicar que hay algunos artículos y trabajos realizados en Estados Unidos (Francia, 2012), España (Navarro, 2013), Italia (Tieghi, 2007), Brasil (Costa, 2012) y Colombia (Villamizar, 2013) principalmente, en los cuales básicamente hacen recomendaciones y análisis generales sobre los SCI. Es conveniente indicar que en algunos de estos trabajos se menciona la norma NIST SP800-53 e ISA 99.

En cuanto al ámbito Nacional y Local se pudo observar escasos trabajos relacionados a planes de desastre, recuperación y análisis de riesgos únicamente. Sin embargo no presentan propuestas claras de mitigación y mucho menos referentes a empresas Industriales de manufactura. Algunos de estos trabajos se fundamentan en el estándar ISO 27001.

1.3. Planteamiento del problema

La empresa COMERCIALIZADORA SAN REMIGIO a pesar de que posee tecnología, controles y procedimientos en la gestión de la seguridad de la información de su SCI, no consigue reducir y solventar los incidentes relacionados a ataques a la Disponibilidad, Integridad y Confidencialidad.

Además no existen evidencias de haber realizado un análisis completo de las vulnerabilidades, amenazas y riesgos de sus activos y servicios críticos.

1.4. Formulación del problema

La pregunta principal de la investigación es: ¿Cuáles son las estrategias de mitigación para mejorar la seguridad de información del Sistema de Control Industrial en la empresa COMERCIALIZADORA SAN REMIGIO?

Las preguntas orientadoras de la investigación a realizar para presentar solución al problema planteado son las siguientes:

1. ¿Cuáles son los estándares de la industria para evaluar las vulnerabilidades, amenazas y riesgos del SCI de COMERCIALIZADORA SAN REMIGIO?
2. ¿Cuáles son los principales riesgos del SCI de COMERCIALIZADORA SAN REMIGIO?
3. ¿Cómo se puede mitigar estratégicamente los riegos críticos del SCI de COMERCIALIZADORA SAN REMIGIO?
4. ¿Cómo se puede verificar, evaluar y validar los resultados?

1.5. Hipótesis

La Seguridad de la información del Sistema de Control Industrial en la empresa COMERCIALIZADORA SAN REMIGIO se puede mejorar con un conjunto de estrategias de mitigación a riesgos basándose en el estándar NIST 800-82.

1.6. Objetivo General

Diseñar un conjunto de estrategias de mitigación para mejorar la seguridad de información del Sistema de Control Industrial en la empresa COMERCIALIZADORA SAN REMIGIO.

1.7. Objetivos Específicos

- Evaluar estándares para analizar vulnerabilidades, amenazas y riesgos del Sistema de Control Industrial.

- Identificar, analizar y elaborar un documento con el listado de amenazas, vulnerabilidades y riesgos críticos del Sistema de Control Industrial.

- Elaborar un documento con las estrategias de mitigación para mejorar la seguridad de información del Sistema de Control Industrial.

- Evaluar, verificar y validar los resultados obtenidos de la propuesta para mitigar los problemas de seguridad de los sistemas de control Industrial.

2. CAPITULO II: FUNDAMENTACION TEORICA

A pesar de los innumerables incidentes reportados (Verizon, 2014) y experimentados en las empresas industriales en el ámbito mundial, nacional y local, los profesionales de automatización aún no le dan la importancia del caso a la seguridad de la información en los Sistemas de Control Industrial. Actualmente se tiene ya estándares y trabajos realizados por organizaciones y empresas internacionales especializadas en seguridad informática las cuales se basan en los siguientes puntos:

2.1. Incidentes de seguridad en Sistemas de Control Industrial

Dentro de las organizaciones mundiales más importantes en el ámbito de la Seguridad de la Información en Sistemas de Control Industrial, se ha encontrado que el ICS-CERT (Equipo de Respuesta a Emergencias de cómputo en Sistemas de Control Industrial) de Estados Unidos, que en coordinación con el FBI (Departamento de Investigación Federal) son las principales organizaciones que se encargan de prevenir, proteger y mitigar sobre las amenazas y vulnerabilidades de dichos sistemas. En sus informes del ICS-CERT (2013) recibió y respondió a 257 incidentes voluntariamente reportados por propietarios y fabricantes de productos industriales en Norte América.

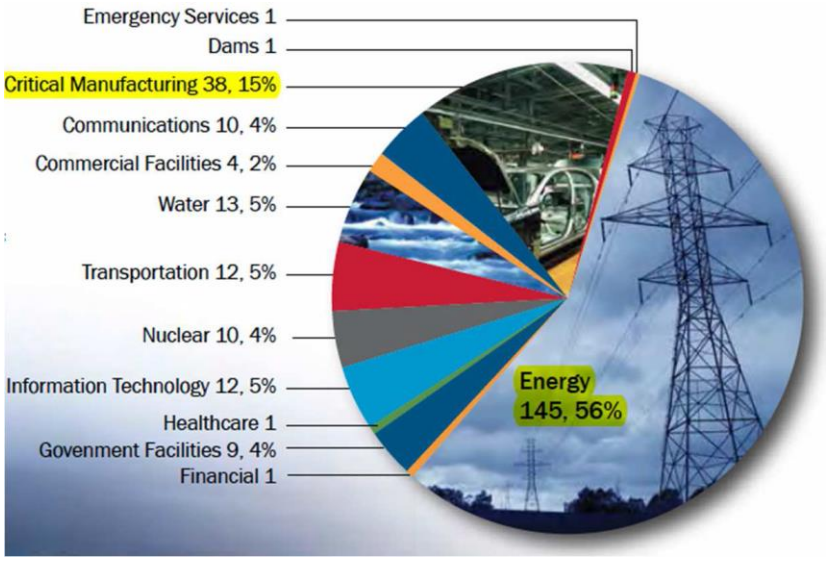

Figura 1. Respuestas del ICS-CERT en el 2013 por sector.

Fuente: ICS-CERT, 2013

Como se puede observar en la Figura 1, luego de las respuestas a incidentes en el área de energía, el que le sigue son las respuestas de incidentes en el sector de manufactura con un 38,15%.

Otros reportes importantes a considerar son los generados por empresas proveedoras de equipos, de sistemas industriales y de soluciones de seguridad informática como son: ABB, Allen Bradley, Verizon, entre otros. De esta última empresa mencionada, la ICS-CERT cita en su página web algunos reportes del 2014, entre los cuales hemos visto conveniente indicar el siguiente:

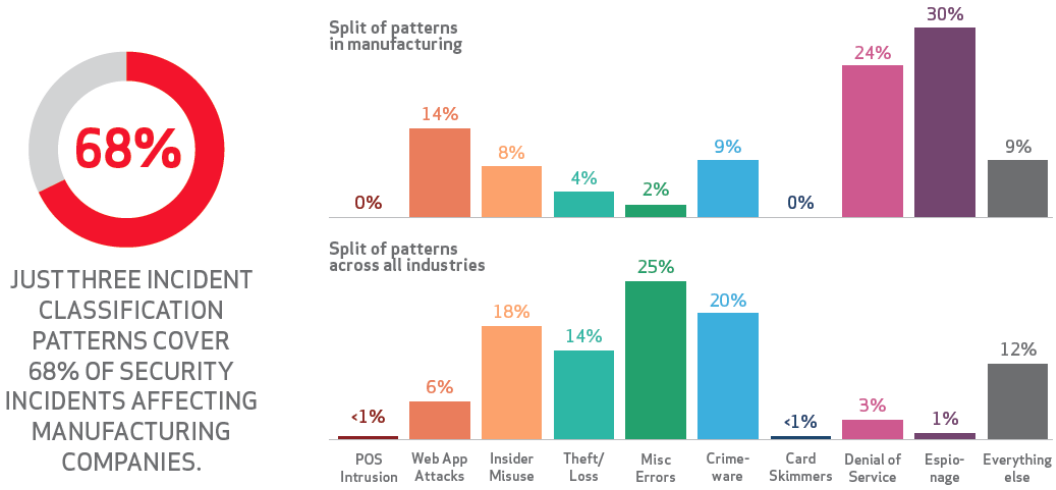

Figura 2. Incidentes de manufactureras vs todas las industrias.
Fuente: Verizon, 2014

El reporte de la Figura 2 es el resultado de 63 mil incidentes de seguridad recolectados en 95 países. Se puede observar también que sólo 9 patrones cubren el 92% de los incidentes de seguridad que se han analizado sobre los 10 últimos años. Por otro lado se puede observar que 3 de los 9 patrones cubren las dos terceras partes de los incidentes experimentados por las industrias de manufactura. Los 3 mayores patrones fueron: 30% de Cyber-Espionaje, 24% de incidentes atribuibles a ataques de negación de servicios y 14% en incidentes de ataques de aplicaciones web.

Al final de estos reportes ICS-CERT y Verizon recomiendan: Usar 2 factores de autenticación (tokens y biometricidad), usar sistemas de manejo de contenido estático en el código de programación de las aplicaciones, políticas de bloqueo de cuentas y monitorear conexiones de outbound.

2.2. Los Sistemas de Control Industrial (SCI)

En general el término de Sistemas de Control Industrial (SCI) engloba algunos tipos de sistemas de control: Sistemas de Adquisición de Datos y Control supervisado (SCADA), Sistemas Distribuidos de Control (DCS) y Controladores Lógicos Programables (PLC). Se debe mencionar que puede haber sistemas híbridos que mezclan por ejemplo características de un SCADA con un DCS.

Según un estudio del Instituto Nacional de Estándares de Tecnología del departamento de Comercio de Estados Unidos (Stouffer, Falco & Scarfone, 2013) los SCI son usados en sectores industriales y en infraestructura crítica tal como: Empresas eléctricas, de agua, de aguas residuales, petróleo, gas natural, químicas, de transportación, farmacéuticas, pulpa y papel, comida y bebida, automotriz, aeroespacial, entre otras. A continuación se explicará brevemente sus características:

SCADA:

- Los sistemas SCADA son sistemas altamente distribuidos usados para controlar geográficamente bienes dispersos.
- Los sistemas SCADA son usados en sistemas distribuidos como distribución de agua, recolección de aguas residuales, conducción de petróleo, conducción de gas natural, redes eléctricas de potencia, sistema de transportación de rieles, entre otros.
- Los SCADA son sistemas específicamente diseñados para manejar comunicaciones a larga distancia.

DSC:

- Los DSC son usados para procesos de control industrial tal como generación de energía eléctrica, refinerías de petróleo, agua, tratamiento de agua, de químicos, de comida, producción de automóviles, entre otros.

- Los DSC son usados extensivamente en industrias basadas en procesos. La figura 3 ilustra un ejemplo de estos sistemas.

PLC:

- Los PLCs son dispositivos basados en computadoras de estado sólido que controlan equipos industriales y procesos.

- Las comunicaciones de DSC y PLC son usualmente realizadas usando red de área local.

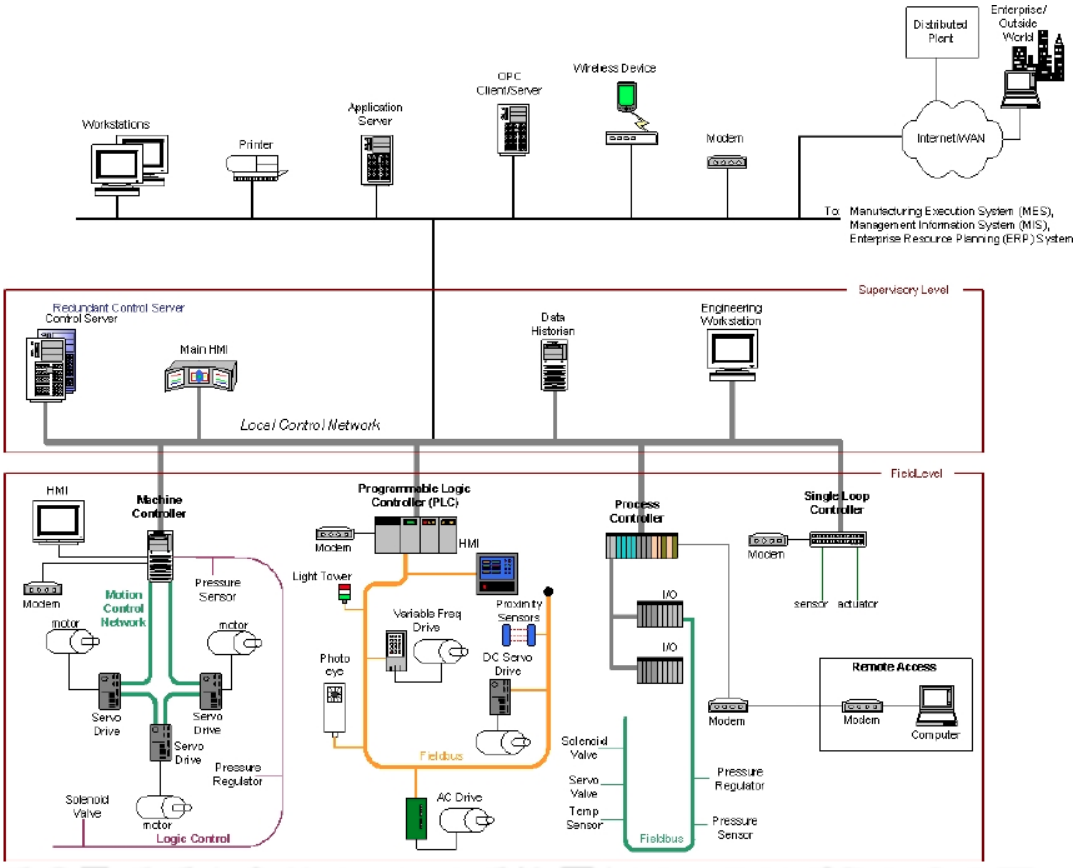

Figura 3. Ejemplo de un Sistema de Control Industrial DSC.
Fuente: Stouffer, Falco & Scarfone, 2013

2.3. Evaluación de estándares para el Análisis y Evaluación de vulnerabilidades, amenazas y Riesgos en los SCI.

El riesgo está en función de la probabilidad de una fuente de amenaza dada, una potencial vulnerabilidad y el impacto resultante de una explotación exitosa de la vulnerabilidad (Stouffer et al., 2013). A su vez la evaluación de riesgos es el proceso de identificar los riesgos de las operaciones de una organización, activos e individuos mediante la determinación de la probabilidad de que una vulnerabilidad identificada será explotada y provocará un impacto. La evaluación de riesgos debe también comparar el costo de la seguridad con el costo asociado con un incidente (Stouffer et al., 2013).

El análisis, la gestión y tratamiento de riesgos de los SCI según la NIST está estructurado de la siguiente manera (Stouffer et al., 2013):

NIST SP 800-82 r1, Documento principal
- |-- NIST SP 800-30 r0, Primer Documento referido
- |-- ISA 99, Segundo Documento referido
  - |-- ISA-62443-2-1, Tercer Documento referido
    - |-- ISO/IEC 27001-2005, Cuarto Documento referido
    - |-- ISO/IEC 27002-2005, Quinto Documento referido

De esta documentación se desprende el cuadro sinóptico de la figura 4.

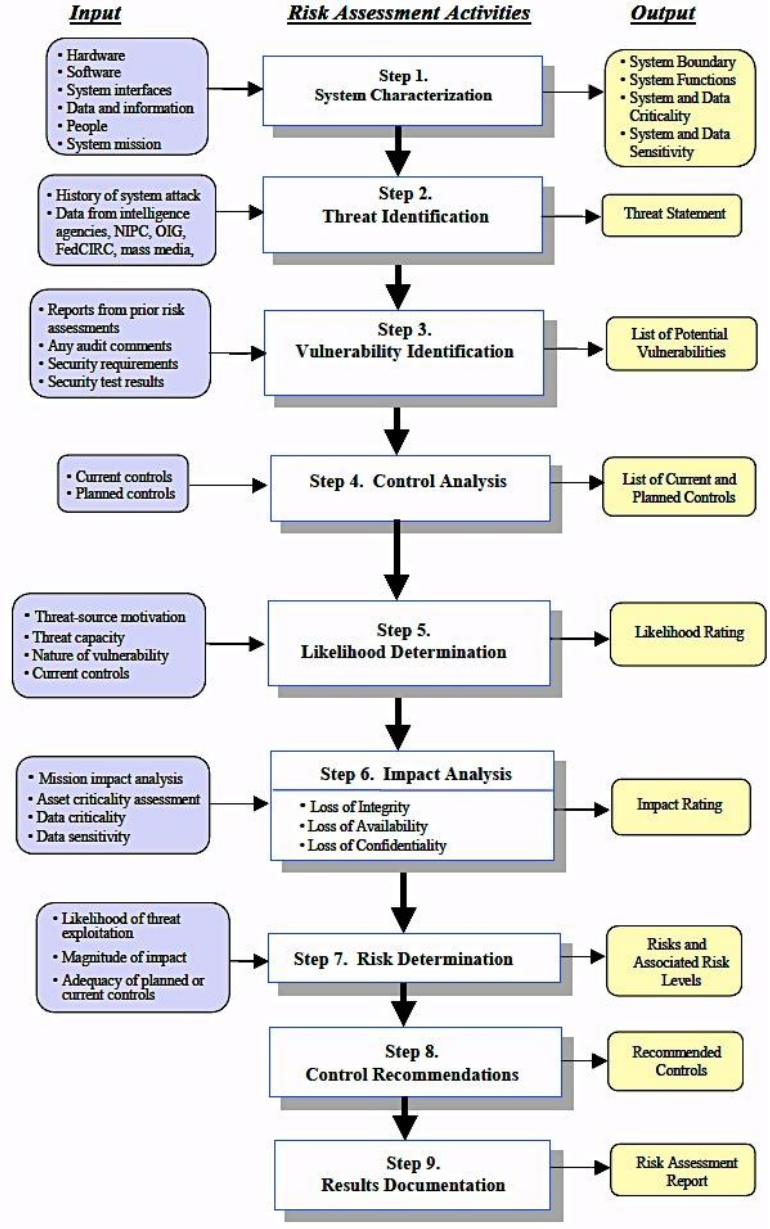

Figura 4. Metodología valoración de riesgos.
Fuente: Stoneburner, Goguen & Feringa, 2002

En la Figura 4 se puede ver el modelo de gestión de riesgos, la cual incluye también los factores claves del riesgo como son: Fuente de Amenaza, Evento de amenaza, Vulnerabilidad, Impacto adverso, riesgos de la organización y controles de seguridad, todo esto configurado para mostrar además las relaciones entre cada uno de estos factores.

3. CAPITULO III: DISEÑO DE ESTRATEGIAS DE MITIGACION

La valoración del riesgo es el primer proceso en la metodología de gestión de riesgos según Stoneburner, Goguen & Feringa (2002). La salida de este proceso ayuda a identificar los controles apropiados para reducir y eliminar riesgos durante el proceso de mitigación. El Riesgo según Stoneburner et al. (2002) es una función de la probabilidad de una fuente de amenaza dada, de ejercer una vulnerabilidad potencial en particular, y el impacto resultante de ese acontecimiento adverso en la organización. Para determinar la probabilidad de un evento adverso futuro, las amenazas a un sistema de Tecnologías de Información debe ser analizado en conjunto con las potenciales vulnerabilidades. El impacto se refiere a la magnitud de daño que puede ser causado por una amenaza sobre una vulnerabilidad. La metodología para valoración de riesgos y diseño de estrategias de mitigación fue desarrollada según Stoneburner et al. (2002), a la cual se agregó un paso más con el fin de comprobar la hipótesis enunciada en el capítulo I. Los 7 primeros pasos se los describe en este capítulo III y los 3 últimos en el capítulo IV:

3.1. Caracterización del sistema

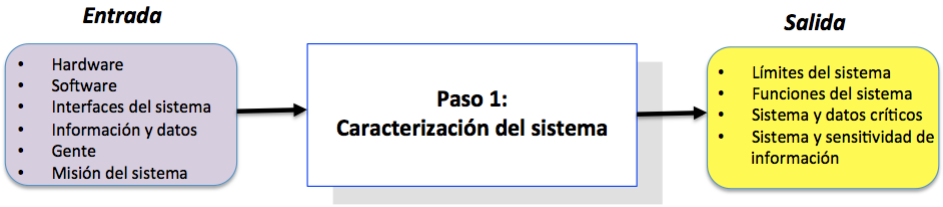

Figura 5. Sinóptico de caracterización del sistema
Fuente: Stoneburner, Goguen & Feringa, 2002

En este paso según Stoneburner et al. (2002) se define el alcance del esfuerzo, los límites del sistema son identificados basados en los recursos e información que lo constituyen. Para realizar la caracterización se necesita describir el sistema de información usado como son:

- Hardware

- Software
- Conectividad interna y externa
- Información y datos
- Personas que dan soporte y usan el sistema
- Procesos realizados por el sistema
- Valor del sistema e importancia para la organización
- Nivel de protección requerido para mantener la integridad, confidencialidad y disponibilidad.

La caracterización además requiere definir las técnicas que se usarán para recolectar la información dentro de las cuales se tiene:

- Cuestionario: Debe ser distribuido al personal técnico y no técnico quienes están diseñando o dando soportando el sistema.
- Entrevistas en sitio: Entrevistas con personal de soporte y de administración del sistema.
- Revisión de documentación: Políticas de la empresa, documentación del sistema y documentación de seguridad relacionada.
- Uso de herramientas automatizadas de escaneo: Pueden ser herramientas de mapeo de la red

En el caso de COMERCIALIZADORA SAN REMIGIO se usó: Entrevistas y revisión de documentación, los cuales se adjuntan en el anexo1. El documento de caracterización del sistema final se puede ver en el anexo 2.

3.2. Identificación de amenazas

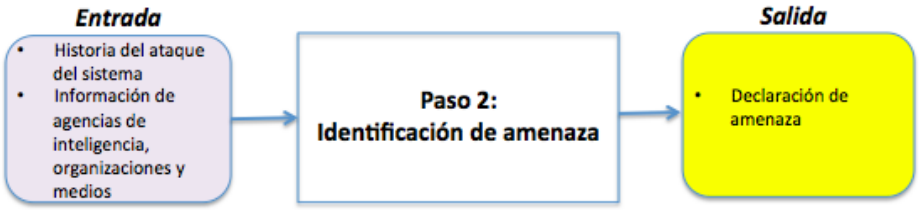

Figura 6. Sinóptico de identificación de amenazas
Fuente: Stoneburner, Goguen & Feringa, 2002

Una amenaza según Stoneburner et al. (2002) es la posibilidad de que una fuente de amenaza se ejecute con éxito (de manera accidental o intencional) en una vulnerabilidad en especial. Una fuente de amenaza no presenta un riesgo cuando no hay vulnerabilidad que pueda ser ejecutada. Para determinar la probabilidad de una amenaza se debe considerar la fuente de amenaza, potenciales vulnerabilidades y los controles existentes.

El objetivo de este paso es identificar las potenciales fuentes de amenazas que pueden ser aplicables al sistema de tecnologías de información que está siendo evaluado. Las fuentes de amenazas comunes según Stoneburner et al. (2002) son:

- Naturales: Inundaciones, terremotos, tornados, deslaves, avalanchas, tormentas eléctricas y otros eventos
- Humanas: Eventos que son habilitados por o causados por seres humanos como: actos no intencionales (ingreso de datos inadvertida) o acciones deliberadas (ataques basados en red, software malicioso, acceso no autorizado a información confidencial)
- Ambientales: Fallas de energía de larga duración, contaminación, química y fuga de fluidos.

La motivación y los recursos para llevar a cabo un ataque, hacen a los humanos una fuente de amenaza peligrosa. Según Stoneburner et al. (2002) se resume en la Tabla1:

Tabla 1.

Amenazas, Motivación y acciones de la amenaza

Amenaza	Motivación	Acciones de la amenaza
Hacker, Cracker	- Desafío - Ego - Rebelión	- Hackeo - Ingeniería Social - Intrusión a sistemas - Acceso a sistemas no autorizados.
Crimen computacional	- Destrucción de información - Divulgación de Información ilegal - Ganancia monetaria. - Alteración de datos no autorizados.	- Crimen computacional (cyber acecho) - Actos fraudulentos - Soborno de información - Engaño - Intrusión al sistema
Terrorismo	- Chantaje - Destrucción - Explotación - Venganza	- Bomba / Terrorismo - Guerra - Denegación de servicios - Penetración al sistema - Manipulación del sistema

CONTINÚA →

Usuarios poco entrenados, descontentos, maliciosos, negligentes, deshonestos o ex empleados	- Curiosidad - Ego - Inteligencia - Ganancia monetaria - Venganza - Errores no intencionales y omisiones (datos ingresados errados, error de programación)	- Asalto a un empleado - Chantaje - Búsqueda de información propietaria - Abuso informático - Fraude y robo - Soborno - Ingreso de información falsa y corrupta. - Interceptación - Código malicioso (virus, bomba lógica, troyano)
Espionaje Industrial	- Ventaja competitiva - Espionaje económico.	- Explotación económica - Robo de información - Intrusión en información personal - Ingeniería Social - Penetración al sistema - Acceso no autorizado al sistema

Fuente: Stoneburner, Goguen & Feringa, 2002

Las fuentes de información de las amenazas más conocidas se podrán obtener de:

- Agencias de inteligencia (FBI)
- Centro de respuesta a incidentes de computación federal (FedCIRC)
- Medio masivos y fuentes web tal como SecurityFocus.com, SecurityWatch.com, SecurityPortal.com y SANS.org

En el anexo 3 se lista las fuentes de amenaza que pueden explotar las vulnerabilidades en el SCI de COMERCIALIZADORA SAN REMIGIO, las cuales se obtuvieron luego de visitar las instalaciones de la empresa y de entrevistas a los usuarios directivos, operativos y técnicos.

3.3. Identificación de vulnerabilidades

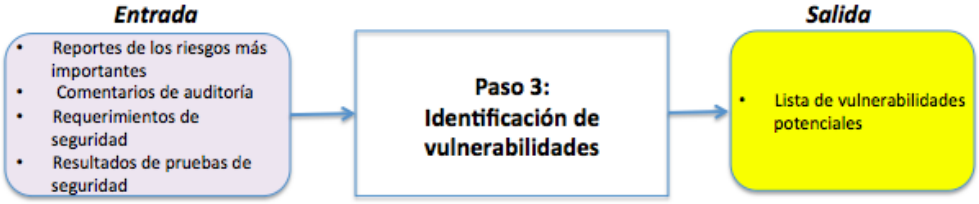

Figura 7. Sinóptico de Identificación de vulnerabilidades.
Fuente: Stoneburner, Goguen & Feringa, 2002

Según Stoneburner et al. (2002), un correcto análisis de amenazas en un SCI debe incluir un análisis de vulnerabilidades asociadas al ambiente en el que este SCI opera, por lo que el objetivo de este paso es desarrollar una lista de las vulnerabilidades del Sistema de Control Industrial de COMERCIALIZADORA SAN REMIGIO, que podrían ser explotadas. Así una vulnerabilidad la definen como una debilidad en procedimientos, diseño, implementación o controles internos que pueden ser ejercidas accidentalmente o intencionalmente explotada y da como resultado una brecha de seguridad o violación de la seguridad.

Los métodos que Stoneburner et al. (2002) recomienda para identificar las vulnerabilidades de un SCI son: el uso de fuentes de vulnerabilidades, pruebas de seguridad de los sistemas y la elaboración de un checklist de requerimientos de seguridad, los cuales se explican con a continuación:

Fuentes de vulnerabilidad: Las vulnerabilidades técnicas y no técnicas pueden ser obtenidas también de las entrevistas, encuestas, revisión de documentación de la empresa y herramientas de escaneo automatizadas. En esta

línea se debe revisar también otras fuentes de la industria que serán útiles como por ejemplo: agujeros de seguridad en aplicaciones y sistemas operativos. El documento de fuentes de vulnerabilidad finalmente debe considerar:

- Documentación previa de la valoración de riesgos, reportes de auditoría a los sistemas, reportes de anomalías, reportes de seguridad y reportes de evaluación y pruebas del SCI.
- Lista de vulnerabilidades tal como el NIST I-CAT (2014) vulnerability database.
- Asesores de seguridad y ventas
- Equipo de respuesta a incidentes de computación como SecurityFocus.com
- Análisis de seguridad del software del SCI.

Pruebas de seguridad del SCI: Los métodos proactivos empleando sistemas de prueba (llamados también testing) son útiles para identificar vulnerabilidades eficientemente. Estos métodos de prueba incluyen:

- Herramientas de escaneo de vulnerabilidades automatizadas: Se usa para escanear un grupo de hosts o una red, sin embargo se deberá tener en cuenta que algunas de las potenciales vulnerabilidades identificadas por las herramientas de escaneo automatizado pueden no representar vulnerabilidades reales por el ambiente en el que el SCI se desarrolla, así se debe tener en cuenta que se pueden presentar los llamados falsos positivos.

- Test de seguridad y evaluación: Este método incluye la elaboración y ejecución de un plan de prueba como por ejemplo: prueba de scripts, prueba de procedimientos y resultados de prueba esperados. El propósito de esta prueba de seguridad del SCI es probar la efectividad de los controles de seguridad.

- Test de penetración: Este test puede ser usado como complemento de la revisión de los controles de seguridad y asegurar que las diferentes facetas del SCI son seguras. El objetivo de este método es probar el SCI desde un punto de vista de una fuente de amenaza e identificar las potenciales fallas en los esquemas de protección.

Elaboración de un checklist de requerimientos de seguridad: En este punto, el personal de valoración de riesgos determina si los requerimientos de seguridad estipulados para el SCI y recogidos durante la caracterización del sistema están siendo cumplidos por los controles de seguridad existentes y planeados. Cada requerimiento debe ir acompañado de una explicación de cómo el diseño del sistema satisface o no ese requerimiento de control de seguridad.

Un checklist de requerimientos de seguridad debe contener los estándares de seguridad básica que pueden ser usados para evaluar sistemáticamente e identificar las vulnerabilidades de los activos (personal, hardware, software, información), procedimientos no automatizados, procesos y transferencia de información en las áreas de seguridad.: Directivas, Operacionales y técnica. La lista del criterio de seguridad sugerido para uso en identificar vulnerabilidades en cada área de seguridad se presenta en la tabla 2.

Tabla 2.

Criterios de Seguridad

AREA	CRITERIO DE SEGURIDAD
Directiva	• Asignación de responsabilidades • Continuidad del soporte • Capacidad de respuesta a incidentes • Revisión periódica de controles de seguridad • Liquidación de personal e investigación de antecedentes. • Valoración de riesgos • Entrenamiento técnico y de seguridad • Separación de funciones • Procesos de autorización y reautorización • Aplicación del plan de seguridad
Operacional	• Control de contaminantes transmitidos por aire (humo, polvo y químicos). • Controles para asegurar la calidad de la energía eléctrica. • Acceso a medio de datos y eliminación • Distribución y etiquetado de datos externos. • Protecciones de instalaciones (cuarto de computadoras, centro de datos y oficina) • Control de humedad • Control de temperatura • Estaciones, portátiles y computadores personales independientes.

CONTINÚA →

Técnica	• Comunicaciones (acceso telefónico, interconexión del sistema, ruteadores) • Criptografía • Control de acceso discrecional • Identificación y autenticación • Detección de intrusos • Reutilización de objetos • Auditoría del sistema

Fuente: Stoneburner, Goguen & Feringa, 2002

El resultado del checklist o cuestionario puede ser usado como entrada para una evaluación de cumplimiento e incumplimiento, estos pasos identifican la debilidad del sistema, procesos y procedimientos, los cuales representan las potenciales vulnerabilidades.

Para COMERCIALIZADORA SAN REMIGIO se consideró entrevistas, revisión y un checklist de requerimientos de seguridad, pues los métodos de escaneo y test de penetración no fueron autorizados ser ejecutados por los riesgos de impactar en la producción. Los resultados se resumen en el anexo 4.

3.4. Análisis de controles

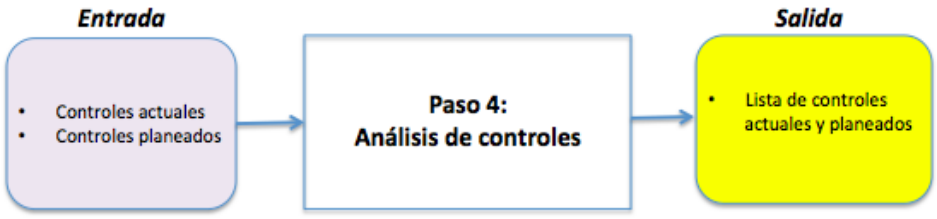

Figura 8. Sinóptico del Análisis de controles
Fuente: Stoneburner, Goguen & Feringa, 2002

El objetivo de este paso según Stoneburner et al. (2002) es analizar los controles que han sido implementados o planeados para la seguridad en la empresa con el fin de minimizar o eliminar la probabilidad de que una amenaza se ejerza sobre una vulnerabilidad. La probabilidad será baja si hay un bajo nivel de interés o capacidad de la fuente de amenaza o si hay un efectivo control de seguridad que puede eliminar o reducir la magnitud del daño.

A continuación se resumen los métodos de control, categorías de control y técnicas de análisis de control según Stoneburner et al. (2002):

Métodos de control: Los controles de seguridad abarca el uso de métodos técnicos y no técnicos. Los controles técnicos son salvaguardas que son incorporados en el hardware de computadoras, software o firmware como por ejemplo: mecanismos de control de acceso, mecanismos de identificación y autenticación, métodos de encriptación, software de detección de intrusos, entre otros. Los controles no técnicos son controles de gestión y operacionales tal como políticas de seguridad, procedimientos operacionales, de personal, físicos y seguridad ambiental.

Categorías de control: Los métodos de control técnicos y no técnicos pueden ser clasificados como preventivos o detectivos. Estas 2 subcategorías son explicadas como sigue:

- Controles preventivos: Previenen de violar políticas de seguridad e incluye controles como aplicación de controles de acceso, encriptación y autenticación.
- Controles detectivos: Advierte de violaciones o intentos de violación de la política de seguridad e incluye controles como rastros de auditoría, métodos de detección de intrusos y checksums.

Técnicas de análisis de control: La elaboración de un checklist de requerimientos de seguridad o el uso de un checklist existente será útil en analizar controles de una manera eficiente y sistemática. Este checklist puede

ser usado para validar no conformidades de seguridad al igual que las conformidades. Además es esencial actualizar este checklist para reflejar cambios en un ambiente de control y así asegurar la validez del mismo.

La lista de controles actuales y planeados usados en el SCI de COMERCIALIZADORA SAN REMIGIO se muestra en el anexo 5.

3.5. Determinación de probabilidad

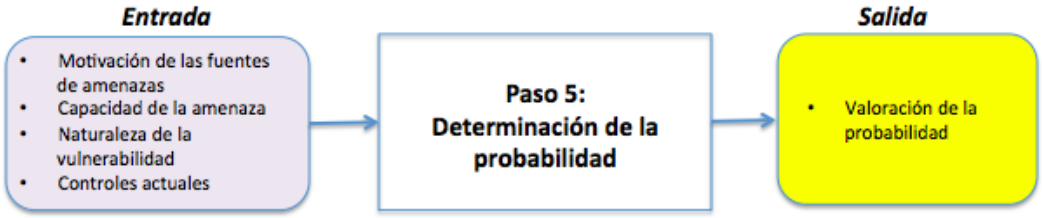

Figura 9. Sinóptico de la determinación de probabilidad
Fuente: Stoneburner, Goguen & Feringa, 2002

Para obtener una completa valoración de la probabilidad que indica la posibilidad de que una potencial vulnerabilidad pueda ser ejercida, los siguientes factores según Stoneburner et al. (2002) deben ser considerados:

- Motivación de la fuente de amenaza y capacidad
- Naturaleza de la vulnerabilidad
- Existencia y efectividad de controles actuales

La probabilidad que una vulnerabilidad potencial puede ser ejercida por una fuente de amenaza dada puede ser descrita como alta, media o baja. Según Stoneburner et al. (2002), la definición de la probabilidad se puede expresar de acuerdo a la tabla 3.

Tabla 3.

Definición de la probabilidad

Valoración	Definición de la probabilidad
Alta (1.0)	La fuente de amenaza es altamente motivada, suficientemente capaz y los controles para prevenir de que la vulnerabilidad sea ejercida son inefectivos.
Media (0.5)	La fuente de amenaza es motivada, capaz, pero los controles impiden que la vulnerabilidad pueda ser ejercida exitosamente.
Baja (0.1)	La fuente de amenaza carece de motivación o capacidad y los controles están puestos para prevenir o al menos impedir significativamente que la vulnerabilidad sea ejercida

Fuente: Stoneburner, Goguen & Feringa, 2002

La valoración de la probabilidad de la infraestructura del SCI de la COMERCIALIZADORA SAN REMIGIO se muestra en los anexos 6, 7 y 8.

3.6. Análisis de impacto

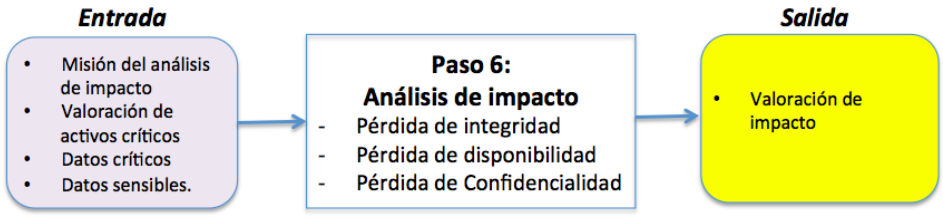

Figura 10. Sinóptico del análisis del impacto
Fuente: Stoneburner, Goguen & Feringa, 2002

En este paso según Stoneburner et al. (2002) el objetivo es determinar impacto adverso resultante de la ejecución exitosa de una amenaza en una vulnerabilidad. Antes de iniciar el análisis de impacto es necesario obtener la siguiente información:

- Misión del sistema (ejemplo: El proceso realizado por el SCI)

- Sistema y criticidad de los datos (ejemplo: El valor del sistema o importancia para una organización)
- Sistema y sensibilidad de los datos

Un análisis del impacto a la misión o conocido también como BIA prioriza los niveles de impacto asociados con los compromisos de los activos de información de la empresa basados en una valoración cualitativa o cuantitativa de la sensitividad y criticidad de esos activos. Entendiéndose por activos a todo el hardware, software, sistemas, servicios y tecnología relacionada.

Si la documentación mencionada no existe el sistema y la sensitividad de los datos puede ser determinada basado en el nivel de protección requerida para mantener el sistema y la disponibilidad, integridad y confidencialidad de los datos. Los propietarios del sistema e información son los responsables de determinar el nivel de impacto de su propio sistema e información. En consecuencia en el análisis de impacto, el enfoque debería ser el entrevistar a los propietarios del sistema e información.

El impacto adverso de un evento de seguridad puede ser descrito en términos de pérdida de los tres objetivos de seguridad: integridad, disponibilidad y confidencialidad. A continuación y según Stoneburner et al. (2002) se describen brevemente los objetivos de seguridad y los impactos de estos no ser cumplidos:

- **Pérdida de Integridad:** Se refiere a los requerimientos de que la información sea protegida de modificaciones impropias. La integridad es perdida en un SCI si cambios no autorizados son realizados en los datos o en el sistema mismo, ya sea intencional o accidentalmente. Hay que tener en cuenta también que la violación de la integridad puede ser el primer paso en un ataque exitoso en contra de la disponibilidad o confidencialidad de la información.

- **Pérdida de disponibilidad:** Si en un sistema de misión crítica, como un SCI, es no disponible para sus usuarios, entonces la misión y operaciones de la organización pueden ser afectados.

- **Pérdida de confidencialidad:** Se refiere a la protección de información de divulgación no autorizada.

Algunos impactos tangibles pueden ser medidos cuantitativamente en la pérdida de ingresos, el costo de reparación del sistema o el nivel de esfuerzo requerido para corregir problemas causados por una acción de amenaza exitosa. Otros impactos (pérdida de confianza pública, pérdida de credibilidad, daño al interés de una organización, etc.) no pueden ser medidos en unidades específicas pero pueden ser calificados o descritos en términos de impactos altos, medios y bajos. De acuerdo a Stoneburner et al. (2002) se describe solamente la valoración de los impactos de una manera cualitativa en la Tabla 4:

Tabla 4.
Definición de Impacto

Valoración	Definición de Impacto
Alto (100)	La ejecución de la vulnerabilidad (1) puede resultar en una pérdida de altamente costosa de los principales activos tangibles o recursos; (2) puede significativamente violar, dañar o impedir las operaciones de una organización, reputación o interés; o (3) puede resultar en la muerte de una persona o heridas graves.
Medio (50)	La ejecución de la vulnerabilidad (1) puede resultar en la costosa pérdida de activos tangibles o recursos; (2) puede violar, dañar o impedir las operaciones de una organización, reputación o interés; o (3) puede resultar en lesiones a personal
Bajo (10)	La ejecución de la vulnerabilidad (1) puede resultar en pérdida de algo de activos tangibles o recursos; (2) puede afectar notablemente las operaciones, reputación o interés de una organización.

Fuente: Stoneburner, Goguen & Feringa, 2002

En el análisis de impacto se debe considerar las diferencias entre la valoración cuantitativa y la cualitativa, por lo que según Stoneburner et al. (2002) se deberá tener en cuenta las ventajas y desventajas de los 2 tipos de valoración:

- Valoración cualitativa: La principal ventaja es que esta prioriza el riesgo e identifica áreas para un inmediato mejoramiento en el direccionamiento de vulnerabilidades. La desventaja es que está no provee medidas cuantificables de magnitud del impacto.

- Valoración cuantitativa: La ventaja es que esta provee una medida de la magnitud del impacto, el cual puede ser usado en el análisis costo beneficio. La desventaja es que dependiendo de los rangos numéricos usados para expresar la medida, el significado del impacto cuantitativo pueden ser no claros y requerir de resultados para ser interpretados en una manera cualitativa. Otros factores adicionales pueden ser tomados en cuenta para determinar la magnitud del impacto, estas son:
  - Frecuencia de ejecución de la fuente de amenaza.
  - Costo de cada ocurrencia
  - Factor de ponderación o peso basado en un análisis subjetivo.

La valoración de impacto para la empresa COMERCIALIZADORA SAN REMIGIO se lo desarrolló tomando en cuenta estos lineamientos y se lo puede observar en los anexos 6, 7 y 8.

3.7. Determinación del riesgo

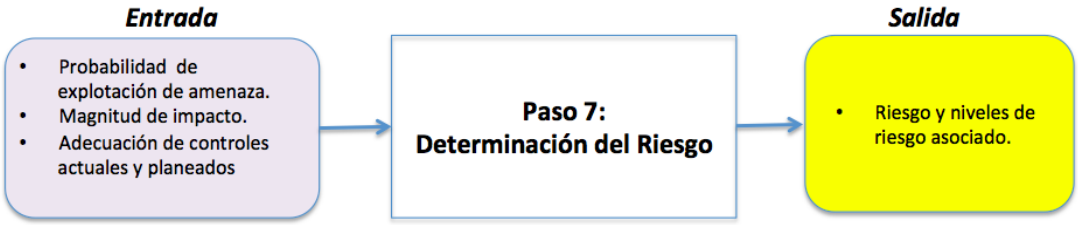

Figura 11. Sinóptico de la determinación del riesgo
Fuente: Stoneburner, Goguen & Feringa, 2002

El propósito de este paso es valorar el nivel de riesgo del SCI. La determinación del riesgo según Stoneburner et al. (2002) puede ser expresada como una función de:

- Probabilidad de una fuente de amenaza dada
- Magnitud de impacto
- La adecuación de controles actuales y planeados para reducir o eliminar el riesgo.

La determinación del riesgo es resultado de multiplicar las valoraciones asignadas por la probabilidad de amenaza y el impacto de la amenaza. La **¡Error! No se encuentra el origen de la referencia.** muestra según Stoneburner et al. (2002) como determinar el riesgo:

Tabla 5.
Escalas de probabilidad e impacto

Probabilidad de amenaza	Impacto		
	Bajo (10)	Medio (50)	Alto (100)
Alto (1.0)	BAJO 10 x 1.0 = 10	MEDIO 50 x 1.0 = 50	ALTO 100 x 1.0 = 100
Medio (0.5)	BAJO 10 x 0.5 = 5	MEDIO 50 x 0.5 = 25	MEDIO 100 x 0.5 = 50
Bajo (0.1)	BAJO 10 x 0.1 = 1	BAJO 50 x 0.1 = 5	BAJO 100 x 0.1 = 10

Fuente: Stoneburner, Goguen & Feringa, 2002

De la tabla anterior las escalas del riesgo se pueden clasificar en:

- Alto: Valor > 50 hasta 100
- Medio: Valor > 10 hasta 50
- Bajo: Valores de 1 hasta 10

Si el nivel indicado es muy bajo y considerado despreciable o no significante (valores menores a 1), se debería no desecharlos del análisis sino más bien tratarlos a un nuevo nivel de riesgos o revalorización.

En los anexos 6, 7, 8 y 9 se muestran las matrices de valoración de riesgos propuestas en la tabla anterior y semaforizando con colores los niveles respectivos. La información de los activos fue recolectada y consultada con los Ingenieros de automatización y de producción de COMERCIALIZADORA SAN REMIGIO.

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

4.1. Recomendaciones de control

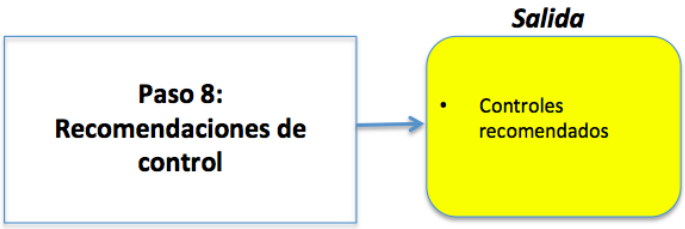

Figura 12. Sinóptico de las recomendaciones de control
Fuente: Stoneburner, Goguen & Feringa, 2002

Los controles pueden mitigar o eliminar la identificación de riesgos. El objetivo del control recomendado es reducir el nivel de riesgo al SCI y sus datos a un nivel aceptable. La eliminación de todo el riesgo es impráctico o casi imposible, por lo cual se debe tener en cuenta la implementación de los controles más apropiados, que tengan el menor costo y que causen el mínimo impacto. En este caso lo que podemos ver es que existe un riesgo residual, el cual resulta luego de haber implementado o ampliado controles. La tendencia debe ser a que este riesgo residual sea lo menor posible.

Las estrategias de mitigación que Stoneburner et al. (2002) sugiere son las siguientes:

- **Cuando la vulnerabilidad existe:** Implementar técnicas de aseguramiento para reducir la probabilidad de que una vulnerabilidad sea ejercida.

- **Cuando una vulnerabilidad puede ser ejercida:** Aplicar capas de protección, diseños arquitectónicos y controles administrativos para minimizar el riesgo.

- **Cuando el costo del atacante es menos que una potencial ganancia:** Aplicar protecciones para decrementar la motivación del atacante ya que se incrementa el costo del ataque.

- **Cuando la pérdida es muy grande:** Aplicar principios de diseño, diseños arquitectónicos y protecciones técnicas y no técnicas para limitar la ampliación del ataque.

Por otro lado, según Stoneburner et al. (2002) los siguientes factores deben ser considerados al momento de recomendar controles:

- Efectividad de opciones recomendadas (ejemplo: compatibilidad del sistema)
- Legislación y regulación
- Política Organizacional
- Impacto operacional
- Seguridad y fiabilidad.

Las recomendaciones de control son el resultado del proceso de valoración del riesgo y provee la entrada al proceso de mitigación del riesgo.

Es necesario conocer que no todos los posibles controles recomendados pueden ser implementados para reducir pérdidas. Según Stoneburner et al. (2002) para determinar cuáles controles son requeridos o apropiados para una organización se debe tener en cuenta un análisis de costo beneficio, el cual mostrará el costo de implementación de controles que pueden ser justificados para la reducción del nivel de riesgo. Además el impacto operacional (efecto en el rendimiento del sistema) y factibilidad (requerimientos técnicos, aceptación de los usuarios) deben ser evaluados cuidadosamente durante el proceso de mitigación del riesgo.

En la figura 13 se puede ver resumida la metodología usada por Stoneburner et al. (2002) para mitigar los riesgos y aplicar controles.

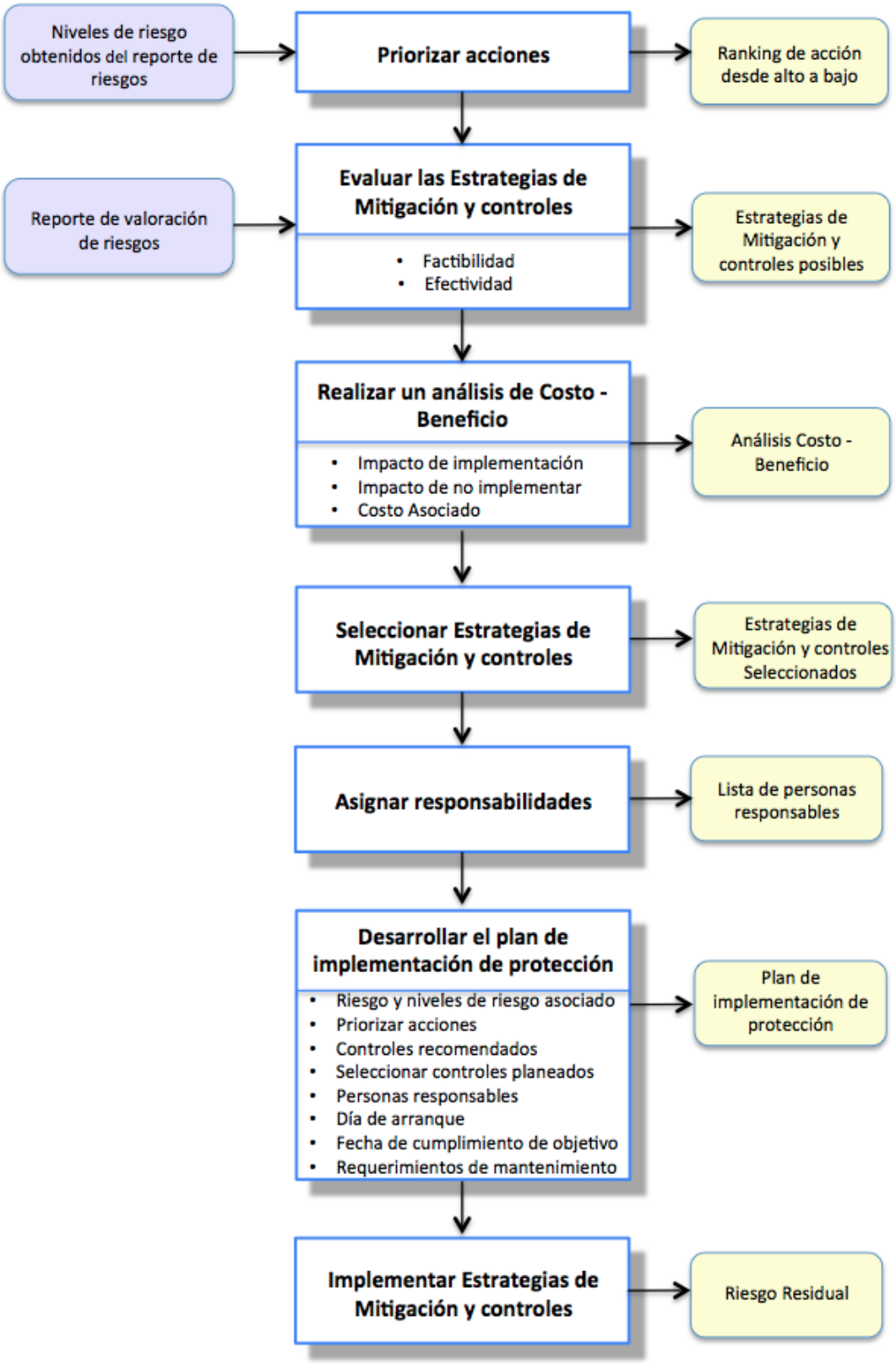

Figura 13. Metodología la mitigación de riesgos y aplicar controles.

Fuente: Stoneburner, Goguen & Feringa, 2002

En el anexo 10, 11, 12 y 13 se pueden observar la aplicación de esta metodología para implementar las estrategias de mitigación y los controles recomendados a COMERCIALIZADORA SAN REMIGIO.

4.2.Documentación de resultados.

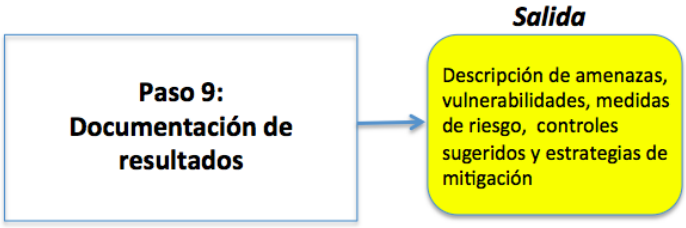

Figura 14. Sinóptico de documentación de resultados
Fuente: Stoneburner, Goguen & Feringa, 2002

Una vez completado todos los pasos indicados por Stoneburner et al. (2002), los resultados fueron documentados en un reporte oficial o en una reunión definitiva con los interesados. Este reporte no fue presentado usando una manera acusatoria, sino con un enfoque sistemático y analítico a la seguridad de información del SCI.

Para COMERCIALIZADORA SAN REMIGIO se procedió a utilizar un formato sugerido por Stoneburner et al. (2002) en el cual se agregaron algunos puntos importantes, quedando al final un reporte que contiene las amenazas, debilidades, medidas de riesgo, controles recomendados y las estrategias de Mitigación a tener en cuenta. Ver el anexo 14.

4.3.Simulación de solución

En este paso se probó los controles recomendados y las estrategias de mitigación, simulando los incidentes de seguridad que ocurrieron en 5 años en el SCI de COMERCIALIZADORA SAN REMIGIO, los resultados de esta prueba se visualizan en cuadros, fotos y gráficos en el anexo 15. Para esta simulación se pidió el criterio de los Ingenieros de: Tecnologías de Información,

Automatización, directivos de producción y operadores de máquinas de producción. Ver anexos 16, 17 y 18.

5. CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones.

Observando los resultados obtenidos se puede concluir que se ha podido diseñar las estrategias de mitigación para el sistema de seguridad industrial para la empresa COMERCIALIZADORA SAN REMIGIO, las mismas que fueron probadas en un procedimiento de simulación conjuntamente con el personal directivo, técnico y operativo de la empresa, comprobando de esta forma que se pudo mejorar la seguridad de la información de una manera integral en sus contextos de la disponibilidad, integridad y confidencialidad. Por otro lado también se concluye que el marco referencial NIST 800-82 sirve para analizar y diseñar estrategias de mitigación de un sistema de control industrial, pues toda la metodología y pasos que se siguieron articularon perfectamente con el funcionamiento, procesos de manufactura y cadena de valor de COMERCIALIZADORA SAN REMIGIO, demostrando y comprobando la hipótesis expuesta en el capítulo I.

5.2. Recomendaciones.

Se recomienda implementar las estrategias de mitigación en la empresa COMERCIALIZADORA SAN REMIGIO en sus 2 líneas de producción y por otro lado se sugiere elaborar un manual de normas y políticas que sirvan como guía y documento maestro en la gestión de la seguridad de la información del sistema de control industrial utilizado en el proceso de producción. Finalmente es recomendable que el departamento de Tecnologías de Información, cada año se actualice con las normas NIST y realice la valoración y ranking de riesgos en la infraestructura del SCI de la empresa.

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

ACP	Acta de constitución del proyecto
DCS	Sistema de control distribuido.
FBI	Oficina federal de investigación
FedCIRC	Centro de respuesta a incidentes de computación federal
FISMA	Gestión de la seguridad de información federal
HMI	Interfaz de usuario
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
SGSI	Sistema de Gestión se Seguridad Informática
SP	Publicación Especial
TI	Tecnologías de Información

8. ANEXOS.

8.1. Anexo 1: Encuesta de infraestructura, procedimientos y usuarios del SCI

1) **PREGUNTA:** ¿Cuál es el tipo de Infraestructura usada en el Sistema de Control Industrial?

   RESPUESTAS:

   a. Controladores lógicos programables (PLCs con sensores y actuadores incluidos)
   b. Drivers para controlar motores.
   c. Human machine Interface (HMI)
   d. Computadoras estaciones de trabajo de monitoreo
   e. Equipos servidores de aplicaciones y bases de datos
   f. Impresoras
   g. Equipos de red (switches y routers)
   h. Equipos de seguridad de red (firewalls, antivirus)

2) **PREGUNTA:** ¿Cuáles son los sistemas, procesos e información usados en el Sistema de Control Industrial?

   RESPUESTAS:

   a. Sistema DCS para la fabricación del producto (2 líneas de producción)
   b. Mantenimiento preventivo y correctivo del SCI electrónico e informático.
   c. Implementación de proyectos electrónicos e informáticos en el SCI

d. La información que maneja el SCI es: Cantidades de materia prima consumida, cantidad de unidades fabricadas, velocidad de fabricación, presión y temperatura de puntos críticos entre los más importantes.

3) **PREGUNTA:** ¿Quiénes son los usuarios del Sistema de Control Industrial?

RESPUESTAS:

a. Operadores de máquina de fabricación de producto
b. Superintendente de producción
c. Ingenieros de mantenimiento
d. Ingenieros de automatización
e. Ingeniero de infraestructura Informática

4) PREGUNTA: ¿Se tiene algún marco referencial para la gestión del SCI?

RESPUESTAS:

- No se tiene ningún marco referencial para la gestión del SCI
- Si se tienen repuestos de los equipos más importantes
- Tienen problemas con la gestión de configuraciones y cambios en los equipos.

8.2. Anexo 2: Caracterización del sistema

Tabla 6.

Caracterización del SCI

CARACTERIZACION DEL SISTEMA			
No. Proyecto	**Fecha**	**Título del Proyecto**	**Administrador del Proyecto**
1	04/09/14	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
Límites del sistema:			
El SCI de la empresa COMERCIALIZAODRA SAN REMIGIO es un conjunto de: - Equipos electrónicos (PLCs, Drivers de motores, sensores y actuadores) - Hardware (Servidores, Computadoras de monitoreo, HMI e impresoras) - Seguridad informática (Firewall y antivirus) - Software (Sistemas operativos, bases de datos, Software de control, Software para programación de PLCs y programas de PLCs) - Procesos (Operación de los DCSs, mantenimiento del SCI e implementación de proyectos en el SCI) - Personas (operadores, técnicos y directivos) que interactuan conjuntamente para la fabricación del producto y que son de alta importancia para las operaciones del negocio.			
Funciones del sistema:			
Las funciones principales del SCI de COMERCIALIZAODRA SAN REMIGIO son: - Fabricación del producto en la línea de producción 1 - Fabricación del producto en la línea de producción 2			
Sistema y datos críticos:			
- Sistema Agnati para línea de producción 1 - DSC de desarrollo propio para línea de producción 2 - Software Rockwel para programación de PLCs y Drivers de motores - Datos críticos: Consumo de materia prima, unidades fabricadas, velocidad de fabricación, presión y temperatura de puntos crítcos			
Sistema y sensitividad de la información:			
Nivel de protección a la Disponibilidad: - Se tiene repuestos de equipos más importantes del SCI Nivel de protección a la Integridad: - Tienen problemas con la gestión de configuraciones y cambios en el SCI Nivel de protección a la Confidencialidad: - No tienen ningún sistema de gestión en el SCI			

Fuente: Comercializadora San Remigio

8.3. Anexo 3: Lista de fuentes de amenazas

Tabla 7.

Fuentes de amenazas

LISTA DE FUENTES DE AMENAZAS				
No. Proyecto	**Fecha**	**Título del 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	
Amenaza		**Motivación**	**Acciones de la amenazas**	**Comentarios**
Hackers, Crackers		Desafío, Ego personal, Rebeldía	Hackeo, Ingeniería social, Intrusión a los sistemas, Accesos no autorizados	Se ha detectado malwares como troyanos, virus, keyloggers instalados en algunos equipos
Crimen computacional		Destrucción de información, Divulgación de información ilegal, Alteración de datos no autorizados	Crimen computacional, Actos fraudulentos, Soborno de Información, Engaño, Intrusión a los sistemas	Los usuarios han detectado borrado de información y alteración de datos
Usuarios poco entrenados		Errores no intencionales y omisiones	búsqueda de información propietaria, abuso informático, Ingreso de información falsa y corrupta, código malicioso	Desconocimiento de usuarios del SCI han llevado a cometer errores los cuales los directivos piensan que son no intencionales y requieren más bien capacitación
Usuarios descontentos, maliciosos, negligentes y deshonestos		Ego, Inteligencia, Ganancia monetaria y venganza	Chantaje, Búsqueda de información propietaria, abuso informático, Fraude, robo, soborno, Ingreso de información falsa y corrupta, código malicioso	Los directivos de COMERCIALIZAODRA SAN REMIGIO indicaron que si se ha dado casos de empleados maliciosos y deshonestos en la empresa
Espionaje industrial		Ventaja competitiva, espionaje económico	Robo de información, intrusión de información personal, Ingeniería Social, Acceso no autorizado al sistema	Personal de TI de la empresa indicaron que han detectado paso de información a la competencia, uso de ingeniería social y accesos no autorizados

Fuente: Comercializadora San Remigio

8.4. Anexo 4: Fuentes de vulnerabilidad

Tabla 8.

Fuentes de vulnerabilidad

FUENTES DE VULNERABILIDAD			
No. Proyecto	**Fecha**	**Título del Proyecto**	**Administrador del Proyecto**
1	18/09/14	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	**Vulnerabilidad Detectada**	**Tipo**	**Comentado en la entrevista**
1	No existe una asignación clara de responsabilidades	Directivo	El organigrama funcional del dpto. de producción y mantenimiento no es claro
2	No hay continuidad del soporte	Directivo	No existe ningún sistema de gestión
3	No se revisa los controles de seguridad	Directivo	El día a día no da tiempo.
4	No existen sansiones e investigación de incidentes	Directivo	No existe personal para estas funciones
5	No se hace evaluaciones de riesgos	Directivo	No se ha visto la necesidad
6	No hay capacitación ni entranamiento de seguridad	Directivo	No se ha visto la necesidad
7	Falta de controles para asegurar calidad de energía eléctrica	Operacional	Existen pocos medidores e indicadores
8	Falta protecciones a instalaciones y cuartos de control	Operacional	No se ha visto la necesidad
9	No existe controles de humedad ni temperatura	Operacional	No se ha visto la necesidad
10	Uso de equipos personal en la empresa	Operacional	No exsite un control de seguridad física
11	Equipos de comunicaciones sin protección	Técnico	No ha existido problemas serios aún.
12	No se usa criptografía	Técnico	Se confía en los usuarios.
13	No se usa controles de acceso, identificaciones ni autenticación	Técnico	Se confía en los usuarios
14	No se usa ningún sistema de detección de intrusos	Técnico	Ha existido pocos incidentes
15	No se hace auditorías al sistema	Técnico	No se ha visto la necesidad

Fuente: Comercializadora San Remigio

8.5. Anexo 5: Lista de controles

Tabla 9.

Lista de controles

LISTA DE CONTROLES					
No. Proyecto	**Fecha**	**Título del Proyecto**		**Administrador del Proyecto**	
1	22/09/14	Diseño de Estrategias de Mitigación para mejorar la seguridad de información del SCI en la empresa COMERCIALIZADORA SAN REMIGIO		Ing. Paúl Díaz, Ing. Fabián Bustamante	
Número	**Actual / Planeado**	**Control**	**Vulnerabilidad**	**Método**	**Categoría**
1	Planeado	Realizar auditorías anuales del organigrama y encuestas a usuarios del SCI	No existe una asignación clara de responsabilidades	No Técnico	Detectivos
2	Actual	Revisión de contratos de mantenimiento anuales	No hay continuidad del soporte	No Técnico	Preventivo
3	Planeado	Revisión anual de los controles de seguridad con los usuarios del SCI	No se revisa los controles de seguridad	No Técnico	Preventivo
4	Planeado	Revisión semestral de incidentes de seguridad y sansiones aplicadas	No existen sansiones e investigación de incidentes	No Técnico	Preventivo
5	Planeado	Revisión anual de los riesgos del SCI de la empresa	No se hace evaluaciones de riesgos	No Técnico	Preventivo
6	Actual	Revisión anual del índice de capacitaciones realizadas	No hay capacitación ni entranamiento de seguridad	No Técnico	Preventivo
7	Actual	Revisar anualmente con un checklist los lugares críticos para revisión de energía eléctrica	Falta de controles para asegurar calidad de energía eléctrica	Técnico	Detectivo
8	Planeado	Revisión semestral del funcionamiento de los controles de acceso a cuartos de control	Falta protecciones a instalaciones y cuartos de control	Técnico	Detectivo
9	Actual	Revisión semestral del funcionamiento de controles de temperatura y humedad	No existe controles de humedad ni temperatura	Técnico	Detectivo
10	Actual	Guardias no permitan el paso de equipos informáticos sin permiso de Gerencia	Uso de equipos personales en la empresa	Técnico	Preventivo
11	Planeado	Revisión semestral de accesos a cuartos de telecomunicaciones.	Equipos de comunicaciones sin protección	Técnico	Preventivo
12	Plaenado	Revisión semestral de llaves criptográficas utilizadas	No se usa criptografía	Técnico	Preventivo
13	Planeado	Revisión anual de controles de acceso a cuartos de equipos	No se usa controles de acceso, identificaciones ni autenticación	Técnico	Preventivo
14	Planeado	Revisión anual de registros y logs de intrusos a la red	No se usa ningún sistema de detección de intrusos	Técnico	Detectivo
15	Planeado	Insertar en la política de seguridad de información auditorías anuales	No se hace auditorías al sistema de control industrial	Técnico	Preventivo

Fuente: Comercializadora San Remigio

8.6. Anexo 6: Riesgos del sistema de control industrial

Tabla 10.

Riegos del SCI

RIESGOS EN EL SISTEMA DE CONTROL INDUSTRIAL - COMERCIALIZADORA SAN REMIGIO				
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
NUMERO	**DESCRIPCION DEL RIESGO**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
1	Infección de virus y malware en red del SCI	1	100	100
2	Alteración intencional de información del SCI	0,5	100	50
3	Pérdida de información y errores de configuraciones en el SCI	1	100	100
4	Fallas en la disponibilidad del SCI por sabotaje	0,5	100	50
5	Robo de información	0,5	50	25
6	Robo de equipos y dispositivos que conforman el SCI	1	100	100
7	Instalación de software sin licencia	0,5	50	25
8	Infraestructura crítica sin asegurar	1	100	100
9	Inversiones en infraestructura de seguridad erroneas	1	50	50

Fuente: Comercializadora San Remigio

8.7.Anexo 7: Riesgos del hardware y software usados en mantenimiento

Tabla 11.

Riesgos del hardware y software

MATRIZ DE RIESGOS DEL HARDWARE Y SOFTWARE USADOS PARA MANTENIMIENTO - SCI SAN REMIGIO												
No. Proyecto		**Fecha**	**Título del 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		
NUMERO	**UBICACIÓN**	**EQUIPO**	**MARCA**	**MODELO**	**#SERIE**	**REPUESTOS**	**SISTEMA OPERATIVO**	**SOFTWARE INSTALADO**	**VERSION SOFTWARE INSTALADO**	**Probabilidad**	**Impacto**	**RIESGO**
1	OFICINA MTTO	COMPUTADOR DESKTOP	HP	HP Pro 3500	MXL31505DR	SI	Windows 7	Autocad 2007	2007	0,1	10	1
2	OFICINA MTTO	COMPUTADOR LAPTOP	LENOVO	T60	L3-M5990	SI	Windows XP	PI7 micro software Telemecanique	4.54	0,5	50	25
3	OFICINA MTTO	COMPUTADOR DESKTOP	LENOVO	ThinkCentre M92p	MJ869DA	SI	Windows 7	Rslogix 500 Allen Bradley software	3	0,1	10	1
4	OFICINA MTTO	COMPUTADOR LAPTOP	Dell	Latitude6440	45T	NO	Windows 8	Software de Mtto.	Varios	0,5	100	50

Fuente: Comercializadora San Remigio

8.8. Anexo 8: Riesgos del hardware, software y plcs usados en 1ra línea de producción

Tabla 12.

Riesgos de hardware y software 1ra línea de producción.

MATRIZ DE RIESGOS DEL HARDWARE, SOFTWARE Y PLC'S EN 1RA LINEA DE PRODUCCION - SCI C. SAN REMIGIO											
No. Proyecto		Fecha	Título del 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		
NUMERO	UBICACIÓN	EQUIPO	MARCA	MODELO	REPUESTOS	SOFTWARE RELACIONADO	LICENCIA SOFTWARE RELACIONADO	FORMA DE COMUNICACION CON EL SOFTWARE	PROBABILIDAD	IMPACTO	RIESGO
1	SPLICER JC LM	PLC	ALLEN BRADLEY	COMPACT LOGIX	SI	Rslogix 5000 Allen Bradley software	SI	ETHERNET	0,1	50	5
2	SPLICER JC LO	PANTALLA TACTIL	PROFACE	AGP3300	SI	GPPROEX 4	NO	ETHERNET	0,1	10	1
3	CONSOLA S90	COMPUTADORA	ALLEN BRADLEY	S/N	SI	RSVIEW 32 ALLEN BRADLEY	VNC	ETHERNET	0,1	100	10
4	CONSOLA S90	FLEX I/O	ALLEN BRADLEY	S/N	SI	ninguno	NO	ETHERNET	0,1	50	5
5	CUARTO DE CONTROL 1	PLC	ALLEN BRADLEY	PLC 5-40	SI	Rslogix 5 Allen Bradley	NO	485 DH+	0,1	100	10
6	SPLICER JD LM	PLC	ALLEN BRADLEY	COMPACT LOGIX	SI	Rslogix 5000 Allen Bradley software	SI	ETHERNET	0,1	50	5
7	SPLICER JD LO	PANTALLA TACTIL	PROFACE	AGP3300	SI	GPPROEX 4	SI	ETHERNET	0,1	10	1
8	SPLICER JA LM	PLC	HITACHI	H-300	SI	ninguno	NO	RS232	0,5	50	25
9	SPLICER JA LO	PANTALLA TACTIL	PROFACE	AGP3300	SI	GPPROEX 4	SI	RS232/ETHERNET	0,1	50	5
10	CUARTO DE CONTROL 1	PLC	HITACHI	H-300	SI	ninguno	NO	N/A	0,1	100	10
11	SPLICER JB LM	PLC	SIN PLC UPGRADE	S/N	SI	ninguno	NO	RS232	0,1	10	1
12	SPLICER JB LO	PANTALLA TACTIL	SIN PLC UPGRADE	S/N	SI	ninguno	NO	RS232/ETHERNET	0,1	10	1
13	ALINEADOR	PLC	SIEMENS	S7 300	SI	SIMATIC MANAGER	NO	PROFIBUS	0,1	50	5
14	ALINEADOR	PANTALLA TACTIL	SIEMENS	SIMATIC PANEL	SI	ninguno	NO	PROFIBUS	0,1	10	1
15	PRECALENTADORES	PLC	ALLEN BRADLEY	PLC 5/20	SI	Rslogix 5 Allen Bradley	SI	485 DH+	0,1	50	5
16	PRECALENTADORES	PANTALLA TACTIL	ALLEN BRADLEY	PV 900	SI	ninguno	NO	485 DH+	0,1	10	1
17	GLUE MACHINE	PLC	SIEMENS	S7-300	SI	SIMATIC MANAGER	NO	PROFIBUS	0,1	100	10
18	SPLICER JE_LM	PLC	ALLEN BRADLEY	COMPACT LOGIX	SI	Rslogix 5000 Allen Bradley software	SI	ETHERNET	0,1	50	5
19	SPLICER JE LO	PANTALLA TACTIL	PROFACE	AGP3300	SI	GPPROEX 4	SI	ETHERNET	0,1	10	1
20	DOUBLE BACKER	PLC	ALLEN BRADLEY	S/N	SI	Rslogix 5 Allen Bradley	NO	485 DH+	0,1	100	10
21	CASETA DE CONTROL	PANTALLA TACTIL	ALLEN BRADLEY	PV900	SI	ninguno	NO	485 DH+	0,5	100	50
22	CUARTO CONTROL 2	FLEX I/O	ALLEN BRADLEY	S/N	SI	ninguno	NO	485 DH+	0,1	50	5
23	CUARTO CONTROL 2	CPU	IEI	PAC-106GWR20	SI	ninguno	NO	RS232	0,5	50	25
24	CASETA DE CONTROL	COMPUTADORA	IEI	PAC-106GWR20	SI	ninguno	NO	RS232	0,5	50	25
25	CASETA DE CONTROL	COMPUTADORA	IEI	PAC-106GWR20	SI	ninguno	NO	RS232	0,5	50	25
26	CUARTO CONTROL 2	CPU1	IEI	PAC-106GWR20	NO	ninguno	NO	RS232	1	100	100
27	CUARTO CONTROL 2	CPU2	IEI	PAC-106GWR20	NO	ninguno	NO	RS232	1	100	100
28	CUARTO CONTROL 3	PLC	ALLEN BRADLEY	MICROLOGIX 1400	SI	Rslogix 500 Allen Bradley software	SI	ETHERNET	0,1	100	10
29	CUARTO CONTROL 3	PLC	ALLEN BRADLEY	SLC 5/02	NO	Rslogix 500 Allen Bradley software	NO	ETHERNET	1	50	50
30	COSINA GOMA	PLC	SIEMENS	S7-300	SI	SIMATIC MANAGER	SI	PROFIBUS	0,1	10	1
31	COSINA GOMA	COMPUTADORA	HP	S/N	SI	ninguno	VNC	PROFIBUS/ETHERNET	0,5	10	5
32	CASETA DE CONTROL	COMPUTADORA	HP	S/N	SI	ninguno	VNC	PROFIBUS/ETHERNET	0,5	10	5
33	CASETA DE CONTROL	COMPUTADORA	ALLEN BRADLEY	1500P	SI	RSVIEW 32 ALLEN BRADLEY	VNC	ETHERNET	0,1	50	5
34	CUARTO CONTROL 2	PLC	ALLEN BRADLEY	PLC 5-40	SI	Rslogix 5 Allen Bradley	SI	485 DH+	0,1	100	10

Fuente: Comercializadora San Remigio

8.9. Anexo 9: Riesgos del hardware, software y plcs 2da línea de producción.

Tabla 13.

Riesgos de hardware y software 2da línea de producción.

MATRIZ DE RIESGOS DEL HARDWARE, SOFTWARE Y PLC'S EN LA 2DA LINEA DE PRODUCCION - SCI SAN REMIGIO												
No. Proyecto		Fecha	Título del 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			
NUMERO	UBICACIÓN	EQUIPO	MARCA	MODELO	REPUESTOS	SOFTWARE RELACIONADO	VERSION SOFTWARE RELACIONADO	LICENCIA SOFTWARE RELACIONADO	FORMA DE COMUNICACION CON EL SOFTWARE	PROBABILIDAD	IMPACTO	RIESGO
1	HOOPER 2	PLC	TELEMECANIQUE	TSC MICRO	NO	PI7 micro software Telemecanique	4.54	SI	RS232	0,5	100	50
2	HOOPER 2	PLC	SIEMENS	SIMATIC 1200	NO	TIA PORTAL SIEMENS	12	NO	ETHERNET	0,1	100	10
3	HOOPER 2	PLC	ALLEN BRADLEY	MICROLOGIX 1400	SI	Rslogix 500 Allen Bradley software	5.5	NO	RS232	0,1	50	5
4	HOOPER 1	PLC	ALLEN BRADLEY	SLC 05/02	NO	Rslogix 500 Allen Bradley software	5.5	SI	NO	0,1	100	10
5	TCY	PLC	ALLEN BRADLEY	SLC 05/02	NO	Rslogix 500 Allen Bradley software	5.5	SI	RS232	0,5	100	50
6	TCY	PLC	ALLEN BRADLEY	SLC 05/02	SI	Rslogix 500 Allen Bradley software	5.5	SI	RS232	0,5	50	25
7	TCY	PLC	MISTUBISHI	FX-3U	SI	GxWorks 2 Mitsubishi Melsoft software	1.492N	SI	RS232	0,1	100	10
8	TCY	PLC	MISTUBISHI	A	SI	ninguno	n/a	NO	RS232	0,1	100	10
9	TCY	PLC	ALLEN BRADLEY	MICROLOGIX 1400	SI	Rslogix 500 Allen Bradley software	5.5	NO	RS232	0,1	50	5
10	TCY	PANTALLA HMI	WEINTECH	MT6601H	SI	ninguno	n/a	NO	NO	0,1	50	5
11	TCY	PC INDUSTRIAL	IEI	PAC-106GWR20	SI	ninguno	n/a	NO	RS232	0,1	50	5
12	TCY	PLC	ALLEN BRADLEY	MICROLOGIX 1400	SI	Rslogix 500 Allen Bradley software	5.5	SI	RS232	0,1	10	1
13	COMPACTADORA	PLC	ALLEN BRADLEY	MICROLOGIX 1200	NO	Rslogix 500 Allen Bradley software	5.5	SI	NO	0,5	100	50
14	COMPACTADORA ACOPIO	PLC	ALLEN BRADLEY	MICROLOGIX 1200	SI	Rslogix 500 Allen Bradley software	5.5	SI	RS232/ETHERNET	0,5	10	5
15	INGENIERIA DE EMPAQUES	PC INDUSTRIAL	SAMPLE MAKER		NO	ninguno	n/a	NO	RS232	0,1	100	10
16	CONTROL CALIDAD	PLC	KOYO	DIRECT LOGIC OS	NO	ninguno	n/a	NO	RS232	1	100	100
17	CORRUGADORA / IMPRENTAS	PANTALLA TIEMPOS PERDIDOS	GSE	SISBAL 662	NO	ACCESS	n/a	NO	RS232	0,5	100	50

Fuente: Comercializadora San Remigio

8.10. Anexo 10: Ranking de riesgos del sistema de control industrial

Tabla 14.

Ranking de riesgos

RANKING DE RIESGOS DEL SCI - COMERCIALIZADORA SAN REMIGIO				
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	
RANKING	**DESCRIPCION DEL RIESGO**		**VALOR DEL RIESGO**	**REFERENCIA**
1	Infección de virus y malware en red del SCI		100	Anexo 6, Número 1
2	Pérdida de información y errores de configuraciones en el SCI		100	Anexo 6, Número 3
3	Robo de equipos y dispositivos que conforman el SCI		100	Anexo 6, Número 6
4	Infraestructura crítica sin asegurar		100	Anexo 6, Número 8
5	Daño de CPU1 que controla corte superior de producto en 1ra línea de producción		100	Anexo 8, Número 26
6	Daño de CPU2 que controla corte inferior de producto en 1ra línea de producción		100	Anexo 8, Número 27
7	Daño de PLC de Control de Calidad en 2da línea de producción		100	Anexo 9, Número 16
8	Alteración intencional de información del SCI		50	Anexo 6, Número 2
9	Fallas en la disponibilidad del SCI por sabotaje		50	Anexo 6, Número 4
10	Inversiones en infraestructura de seguridad erroneas		50	Anexo 6, Número 9
11	Falla de computador Laptop para mantenimiento del SCI		50	Anexo 7, Número 4
12	Falla de HMI tactil de la caseta de control		50	Anexo 8, Número 21
13	Falla de PLC Allen Bradley del cuarto de control 3		50	Anexo 8, Número 29
14	Falla de PLC Telemecanique de la Hooper 2		50	Anexo 9, Número 1
15	Falla de PLC Allen Bradley de la TCY		50	Anexo 9, Número 5
16	Falla de PLC Allen Bradley de la compactadora		50	Anexo 9, Número 13
17	Pantalla de tiempos perdidos		50	Anexo 9, Número 17

Fuente: Comercializadora San Remigio

8.11. Anexo 11: Lista de estrategias de mitigación recomendadas

Tabla 15.

Estrategias de mitigación recomendadas

Lista de Estrategias de Mitigación recomendadas					
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	**DESCRIPCION DEL RIESGO**		**ESTRATEGIA / CONTROL**	**FACTIBILIDAD**	**EFECTIVIDAD**
1	Infección de virus y malware en red del SCI		Implementar antivirus y firewall en la red del SCI	100%	80%
2	Pérdida de información y errores de configuraciones en el SCI		Implementar una aplicación que maneje control de cambios y backups	100%	80%
3	Robo de equipos y dispositivos que conforman el SCI		Implementar un sistema de cámaras de seguridad en cuartos de control y talleres	90%	90%
4	Infraestructura crítica sin asegurar		Implementar una aplicación para gestion de activos e inventarios	90%	90%
5	Daño de CPU1 que controla corte superior de producto en 1ra línea de producción		Implementar un nuevo sistema para control de corte con equipos de contingencia	50%	90%
6	Daño de CPU2 que controla corte inferior de producto en 1ra línea de producción		Implementar un nuevo sistema para control de corte con equipos de contingencia	50%	90%
7	Daño de PLC de Control de Calidad en 2da línea de producción		Adquirir otro PLC para Control de Calidad y respaldar programas	100%	90%
8	Alteración intencional de información del SCI		Implementar un sistema de autenticación en equipos del SCI y respaldos diarios	90%	90%
9	Fallas en la disponibilidad del SCI por sabotaje		Implementar controles de acceso en cuartos de control	100%	80%
10	Inversiones en infraestructura de seguridad erroneas		Implementar un procedimiento de coordinación entre Automatización y Tecnologías de Información	100%	90%
11	Falla de computador Laptop para mantenimiento del SCI		Adquirir otro equipo y licencias de programas principales para el mantenimiento del SCI	70%	90%
12	Falla de HMI tactil de la caseta de control		Documentar algoritmos y programas para cambios de PLC	100%	80%
13	Falla de PLC Allen Bradley del cuarto de control 3		Documentar algoritmos y programas para cambios de PLC	100%	80%
14	Falla de PLC Telemecanique de la Hooper 2		Documentar algoritmos y programas para cambios de PLC	100%	80%
15	Falla de PLC Allen Bradley de la TCY		Documentar algoritmos y programas para cambios de PLC	100%	80%
16	Falla de PLC Allen Bradley de la compactadora		Documentar algoritmos y programas para cambios de PLC	100%	80%
17	Pantalla de tiempos perdidos		Adquirir una pantalla de repuesto	100%	90%

Fuente: Comercializadora San Remigio

8.12. Anexo 12: Análisis Costo – Beneficio

Tabla 16.

Análisis costo - beneficio

Análisis de Costo - Beneficio						
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**		**IMPACTO DE IMPLEMENTAR**	**COSTO ASOCIADO**	**IMPACTO DE NO IMPLEMENTAR**	**COSTO ASOCIADO**
1	Implementar antivirus y firewall en la red del SCI		MEDIO	$8.000	ALTO	$27.250
2	Implementar una aplicación que maneje control de cambios y backups		MEDIO	$5.000	MEDIO	$56.600
3	Implementar un sistema de cámaras de seguridad en cuartos de control y talleres		BAJO	$6.000	ALTO	$20.000
4	Implementar una aplicación para gestion de activos e inventarios		BAJO	$5.000	ALTO	$30.000
5	Implementar un nuevo sistema para control de corte con equipos de contingencia		MEDIO	$200.000	ALTO	$54.500
6	Implementar un nuevo sistema para control de corte con equipos de contingencia		MEDIO	$200.000	ALTO	$54.500
7	Adquirir otro PLC para Control de Calidad y respaldar programas		MEDIO	$4.000	ALTO	$56.600
8	Implementar un sistema de autenticación en equipos del SCI y respaldos diarios		MEDIO	$7.000	MEDIO	$56.600
9	Implementar controles de acceso en cuartos de control		MEDIO	$5.000	ALTO	$67.080
10	Implementar un procedimiento de coordinación entre Automatización y Tecnologías de Información		BAJO	$500	ALTO	$15.000
11	Adquirir otro equipo y licencias de programas principales para el mantenimiento del SCI		MEDIO	$6.000	ALTO	$56.600
12	Adquirir equipos HMI de repuesto		BAJO	$2.000	MEDIO	$8.175
13	Documentar algoritmos y programas para cambios de PLC		BAJO	$2.000	MEDIO	$13.625
14	Documentar algoritmos y programas para cambios de PLC		BAJO	$2.000	MEDIO	$11.000
15	Documentar algoritmos y programas para cambios de PLC		BAJO	$2.000	MEDIO	$11.000
16	Documentar algoritmos y programas para cambios de PLC		BAJO	$2.000	MEDIO	$11.000
17	Adquirir una pantalla de repuesto		BAJO	$1.500	MEDIO	$5.450

Fuente: Comercializadora San Remigio

8.13. Anexo 13: Estrategias de mitigación y controles seleccionados

Tabla 17.

Estrategias de mitigación y controles seleccionados

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: Comercializadora San Remigio

8.14. Anexo 14: Resumen Ejecutivo de los resultados

Resultados de la valoración de riesgos y diseño de estrategias de mitigación del Sistema de Control Industrial de Comercializadora San Remigio basado en el estándar NIST 800-30 y 800-82.

Autores: Ing. Paúl Díaz, Ing. Fabián Bustamante.
Cuenca, 15 de octubre del 2014

Resumen Ejecutivo

En el siguiente resumen ejecutivo sírvase encontrar los resultados de la valoración de riesgos y diseño de estrategias de mitigación del Sistema de Control Industrial de Comercializadora San Remigio basado en los estándares NIST:

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 valoración de riesgos y diseño de estrategias de mitigación 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 esta razón la Gerencia requiere detectar los problemas y proponer una solución para reducir este nivel de incidentes al máximo posible.

d) **Resultados de la evaluación,**
Luego de un análisis estructurado por los estándares NIST 800-82 y NIST 800-30, los resultados obtenidos se resumen en: 5 amenazas visibles, 15 vulnerabilidades detectadas, 17 riegos resultantes y por otro lado 10 estrategias de mitigación seleccionadas, los cuales se pueden observar en los anexos adjuntos a este informe. Este trabajo fue desarrollado en coordinación con el personal de los departamentos involucrados y los datos que se obtuvieron fueron verificados en reuniones antes y después de cada proceso. En la valoración de riesgos se dio énfasis en los riesgos que tuvieron valores de 100 y 50, descartando los que tenían valores inferiores a 50 con el fin de limitar el alcance de este proyecto y al mismo tiempo ser más asertivos en el trabajo solicitado. En el proceso de diseño de las estrategias de mitigación, se debe resaltar el análisis de costo – beneficio el cual sirvió de gran utilidad para seleccionar los controles y estrategias prioritarias que se deben implementar. Amerita mencionar también que en este proceso el staff directivo del departamento de Producción pudo encontrar que el costo mensual por la indisponibilidad del Sistema de Control Industrial en la 1ra línea de producción es de $27.250,00 y $56.600,00 en la 2da línea de producción, estos valores fueron obtenidos por el departamento de presupuestos y talento humano de la empresa. Finalmente se

puede decir que el costo de implementar las estrategias de mitigación y controles seleccionados asciende a: $48.500,00 frente a $426.605,00 que sería el impacto económico de no hacerlo.

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 es indispensable emprender un proyecto de implementación de estrategias de mitigación y controles en el Sistema de Control Industrial para las 2 líneas de producción. Se recomienda elaborar un manual de Normas y Políticas que sirvan como guía y patrón en la correcta gestión de la seguridad informática del Sistema de Control Industrial.

Atentamente,

Ing. Paúl Díaz, Ing. Fabián Bustamante

8.15. Anexo 15: Resultados de simulación al aplicar estrategias de mitigación y controles en el SCI.

Tabla 18.

Resultados de simulación.

Resultados de la Simulación de aplicar Estrategias de Mitigación y Controles en el SCI de Comercializadora San Remigio									
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
NUMERO	**DESCRIPCION DEL RIESGO**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**	**ESTRATEGIA MITIGACION / CONTROL**	**PROBABILIDAD**	**IMPACTO**	**RIESGO RESIDUAL**	**COMENTARIO**
1	Infeccionn de virus y malware en red del SCI	1	100	100	Implementar antivirus y firewall en la red del SCI	0,1	100	10	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación de 5 a 1
2	Pérdida de información y errores de configuraciones en el SCI	1	100	100	Implementar una aplicación que maneje control de cambios y backups	0,1	100	10	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 7 a 2
3	Robo de equipos y dispositivos que conforman el SCI	1	100	100	Implementar un sistema de cámaras de seguridad en cuartos de control y talleres	0,1	100	10	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 4 a 1
4	Infraestructura crítica sin asegurar	1	100	100	Implementar una aplicación para gestion de activos e inventarios	0,1	100	10	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 3 a 0
5	Daño de PLC de Control de Calidad en 2da línea de producción	1	100	100	Adquirir otro PLC para Control de Calidad y respaldar programas	0,1	50	5	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 2 a 0
6	Alteración intencional de información del SCI	0,5	100	50	Implementar un sistema de autenticación en equipos del SCI y respaldos diarios	0,1	100	10	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 5 a 1
7	Fallas en la disponibilidad del SCI por sabotaje	0,5	100	50	Implementar controles de acceso en cuartos de control	0,1	100	10	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 2 a 1
8	Inversiones en infraestructura de seguridad erroneas	1	50	50	Implementar un procedimiento de coordinación entre Automatización y Tecnologías de Información	0,1	50	5	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 10 a 2
9	Falla de computador Laptop para mantenimiento del SCI	0,5	100	50	Adquirir otro equipo y licencias de programas principales para el mantenimiento del SCI	0,1	50	5	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 3 a 0
10	Falla de PLC Allen Bradley del cuarto de control 3	1	50	50	Documentar algoritmos y programas para cambios de PLC	0,1	50	5	Se revisaron los incidentes de seguridad relacionados y se confirmó que pueden ser minimizados en una relación 5 a 1

Fuente: Comercializadora San Remigio

8.16. Anexo 16: Diagrama de red del SCI de Comercializadora San Remigio.

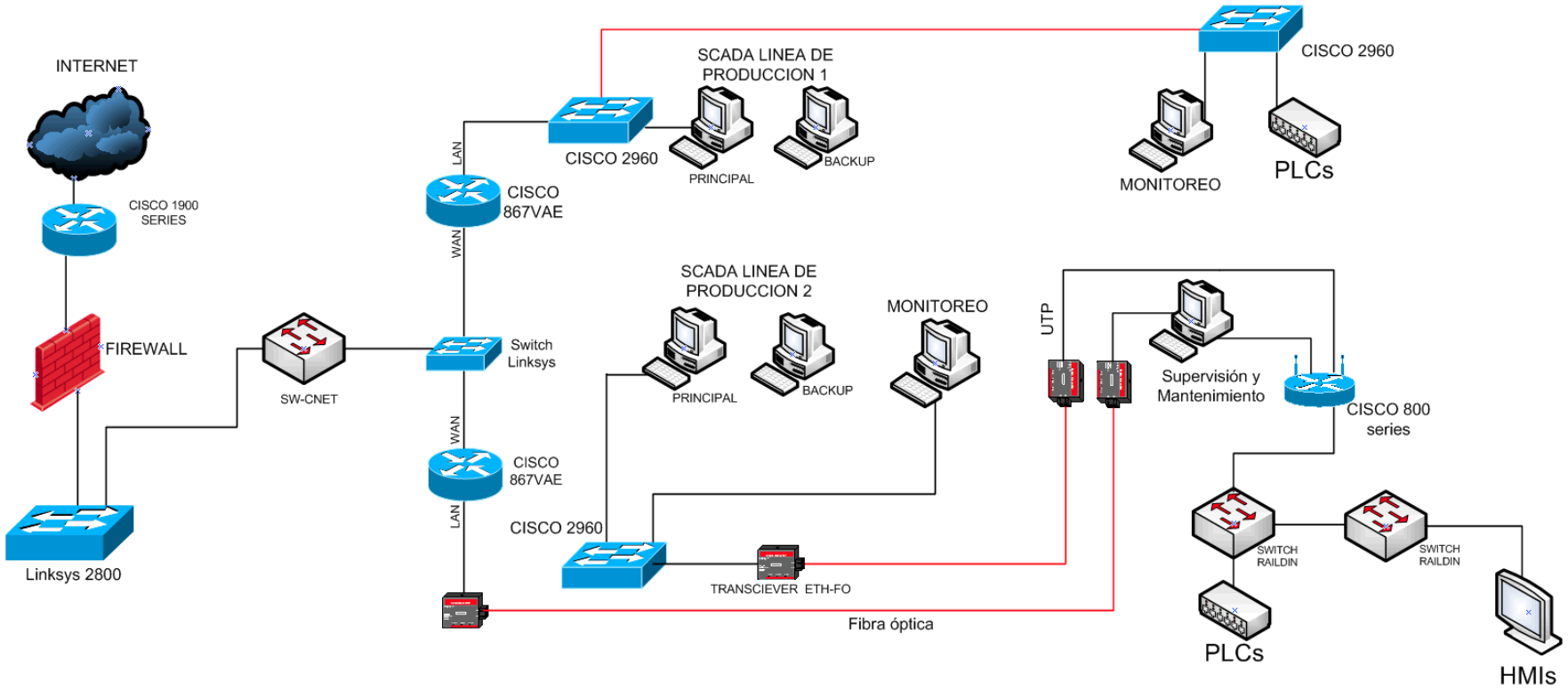

Figura 15. Diagrama de red del SCI

Fuente: Comercializadora San Remigio

8.17. Anexo 17: Fotos de infraestructura crítica del SCI.

Figura 16. Foto de HMI 1ra línea de producción.

Fuente: Comercializadora San Remigio

Figura 17. Foto de PLC principal 1ra línea de producción.

Fuente: Comercializadora San Remigio

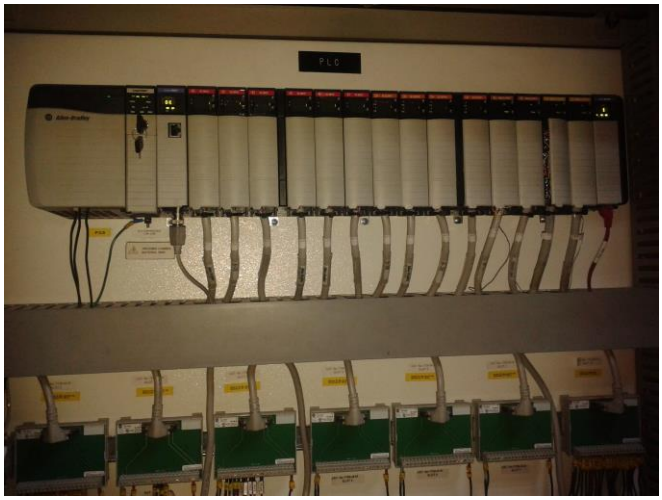

Figura 18. Foto de PLC principal 2da línea de producción

Fuente: Comercializadora San Remigio

8.18. Anexo 18: Pantallas del software usado en el SCI.

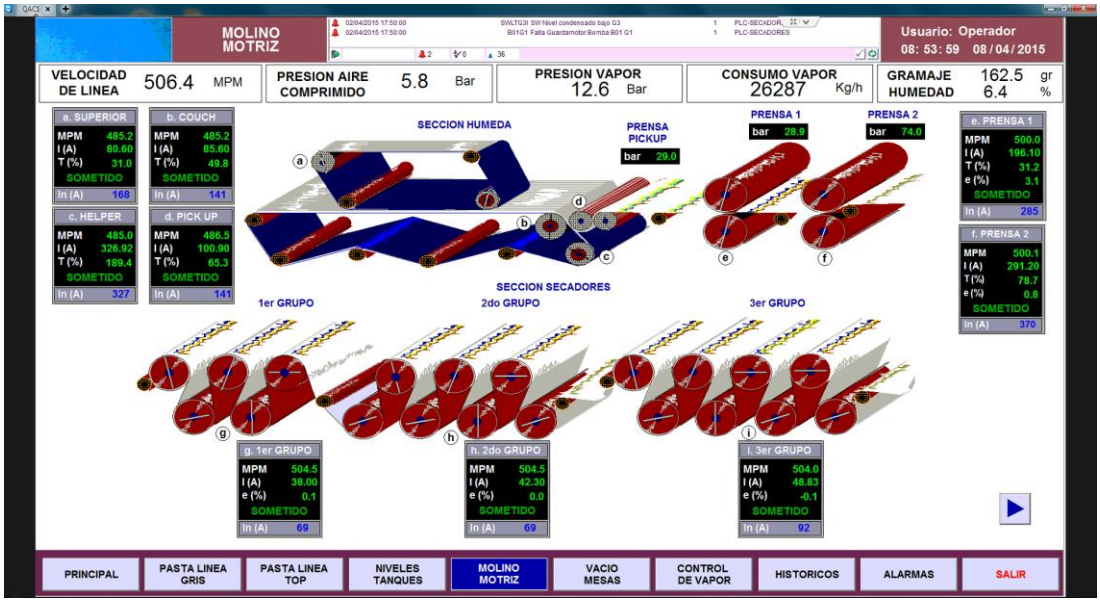

Figura 19. Pantalla principal del software utilizado en la 1ra línea de producción.

Fuente: Comercializadora San Remigio

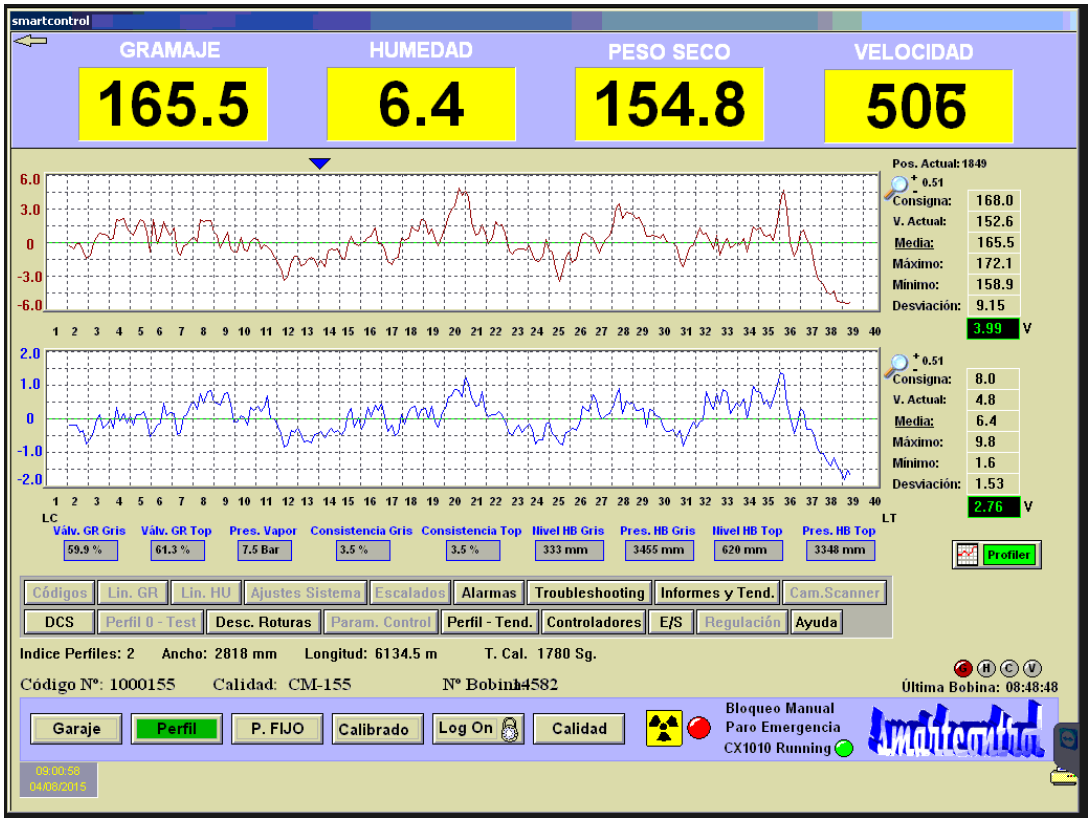

Figura 20. Pantalla principal del software utilizado en 2da línea de producción.

Fuente: Comercializadora San Remigio