Esquema de seguridad para la planta de control de presión del laboratorio de control de procesos basado en el Estándar ISA-99

Pablo Alejandro Pantoja Otero
Laura Marcela Segura Rosas

Universidad del Cauca
Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Electrónica, Instrumentación y Control
Ingeniería en Automática Industrial
Popayán, Marzo de 2013

Esquema de seguridad para la planta de control de presión del laboratorio de control de procesos basado en el Estándar ISA-99

Documento Final de Trabajo de Grado para optar al título de
Ingeniero en Automática Industrial

Pablo Alejandro Pantoja Otero
Laura Marcela Segura Rosas

Director: Ing. Diego Alfonso Aguilar Cardona
Codirector: Ing. Vladimir Trujillo Arias

Universidad del Cauca

Facultad de Ingeniería Electrónica y Telecomunicaciones
Departamento de Electrónica, Instrumentación y Control
Ingeniería en Automática Industrial
Popayán, Marzo de 2013

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE IMAGENES

LISTA DE TABLAS

INTRODUCCION

El laboratorio de control de procesos del Departamento de Electrónica, Instrumentación y Control DEIC de la Universidad del Cauca, cuenta con siete plantas[1]utilizadas por los estudiantes del programa Ingeniería en Automática Industrial, en materias como: laboratorio de control de procesos, instrumentación industrial, software para aplicaciones industriales II, redes y sistemas computarizados de control, además de ser empleadas en proyectos de trabajo de grado. Lo que se desea en un futuro es poder realizar prácticas sobre las plantas del laboratorio de manera remota vía web. Por lo tanto el análisis de seguridad que se hace en el presente trabajo tiene esto en consideración.

Los laboratorios remotos (a veces llamados "laboratorios controlados vía Web o, simplemente, WebLabs), ofrecen acceso remoto a los verdaderos equipos de laboratorio e instrumentos en tiempo real. La principal ventaja de los WebLabs radica en la realidad de los sistemas con los que trabajan los alumnos. Su principal inconveniente se basa en una pérdida de la observación y control de manera directa

Cuando se tiene un sistema de supervisión y control hay riesgos y amenazas intrínsecas que lo pueden dañar por intrusión, alteración o mal manejo de la información. Además, internet provee una infinita librería de información técnica que describe en detalle los pasos necesarios para penetrar la red de un computador, al igual que la documentación necesaria para mapear o navegar a través de los sistemas de control y automatización industrial (IACS por sus siglas en inglés).

Los sistemas de control y manufactura habían sido ajenos hasta hace un tiempo a los riesgos y amenazas de las tecnologías de la información (TI) por sus siglas en ingles. Sin embargo la utilización de protocolos de comunicación o tipos de red estándar han hecho que sean cada vez más vulnerables a ataques informáticos. Hay marcadas diferencias entre abordar un problema de seguridad cibernética en las TI y en los sistemas de control y manufactura. El estándar ISA-99 define una serie de pasos y reglas a tener en cuenta en el momento de diseñar e implementar un sistema de seguridad cibernético sobre los sistemas de control [1].

El estándar ISA-99 se desarrolla para ser aplicado en un entorno industrial. El presente trabajo busca adaptar dicho estándar y formular una serie de lineamientos para el diseño de un esquema de seguridad cibernético en un laboratorio de control de procesos académico. Finalmente estos lineamientos

[1]Planta de control de temperatura, planta de sistema de eventos discretos, planta de control de presión, planta de control nivel, planta de clasificación, planta multivariable y planta de control de movimiento.

serán aplicados en la planta de control de presión del laboratorio de control de procesos de la Universidad del Cauca.

1. DESCRIPCION DEL ESTANDAR ISA 99

La seguridad de la información y del control de los procesos de producción es una parte integral de la seguridad en las empresas, cada vez se aumenta la necesidad de contar con mecanismos o estrategias que garanticen la integridad de los sistemas de control y manufactura.

Hasta hace unos años, el sector industrial había sido ajeno a los riesgos presentes en las tecnologías de la información, entre otras cosas, por utilizar soluciones y redes cerradas, las cuales eran de conocimiento exclusivo del fabricante o proveedor. La industria contaba con sistemas operativos y comunicación de datos propietarios, un flujo de información segmentado, soluciones hardware y software monolítico y arquitecturas cerradas, lo cual trajo consigo varios inconvenientes, entre los más destacados estaba el hecho de mantenerse atado por siempre al proveedor que suministraba la solución, debido a que no era compatible con otras marcas [2][3].

Para atender a esta necesidad se empezaron a proponer soluciones con sistemas operativos abiertos, comunicación de datos estándar, flujo de información integrado, soluciones hardware y software modulares y arquitecturas abiertas, haciendo que la seguridad de la información fuese aún más importante que antes y que los riesgos y vulnerabilidades propios de las TI emigrasen hacia los sistemas de control y manufactura [4].

Podría pensarse en utilizar las diferentes herramientas de seguridad diseñadas en las TI para atender las necesidades de los sistemas de control, sin embargo, estos últimos presentan vulnerabilidades que impiden su uso directo:

- Requieren una velocidad o frecuencia de respuesta que descarta el uso de técnicas tradicionales en informática, como encriptado de bloques.
- No fueron diseñados pensando en la seguridad informática.
- El requisito de fácil de usar para los operadores impide el uso de contraseñas más seguras.
- La necesidad de verificaciones rigurosas de todos los cambios dificulta la actualización periódica de parches de seguridad en los sistemas operativos.
- Una vez que se rompe la protección de sus cortafuegos de seguridad es sencillo comprometer su correcta operación en sistemas abiertos.
- Los sistemas se diseñaron asumiendo que todos los usuarios son de confianza.
- Los procesadores de control fueron diseñados para maximizar su rendimiento y no su seguridad.

- Los datos son casi siempre texto sin codificar
- Los protocolos son abiertos con mínima seguridad
- Hay analizadores de protocolos disponibles en Internet
- Los parches de seguridad no se instalan inmediatamente
- Las redes inalámbricas pueden ser un problema

Además las TI y el control industrial han sido diseñados buscando objetivos diferentes en cuanto a fiabilidad, integridad, y disponibilidad.
Entre las diferencias más destacadas entre las TI y el control industrial se encuentran [2]:

Tecnología de la Información	Control Industrial
Respuesta debe ser fiable	Tiempo de respuesta critico
Demanda de una tasa alta de datos	Tasa de datos modesta es aceptable
Se aceptan grandes retrasos	Los retrasos son un grave problema
Operación programada	Operación continua 24x7x365
Fallos ocasionales son tolerados	Los apagones son intolerables
Lo importante: seguridad de los datos	Lo importante: seguridad de las personas
Riesgos: perdida de datos o de la operación del negocio	Riesgos: perdida de la vida, equipos o productos
Recuperación por arranque del sistema	Esencial la tolerancia a fallos

Tabla 1.1 Diferencias entre TI y control industrial

Con el fin de atender estos nuevos requerimientos de seguridad, han surgido una gran variedad de estándares para la seguridad cibernética; reduciendo al máximo dichos riesgos por medio de recomendaciones para el uso de la información en todos los niveles del sector industrial.

El comité de ISA-99 establece estándares, practicas recomendadas, reportes técnicos e información relacionada que define procedimientos para implementar sistemas de control y manufactura electrónicamente seguros, prácticas de seguridad y evaluación del desempeño de la seguridad cibernética. Está dirigida a aquellos responsables de diseñar, implementar o manejar sistemas de control y manufactura y debe aplicar también a usuarios integradores de sistemas, practicantes de seguridad y vendedores de sistemas de control [5].

El enfoque del comité es mejorar la confidencialidad, integridad y disponibilidad de componentes o sistemas utilizados para el control o la manufactura y proveer criterios para la adquisición e implementación de sistemas seguros de control. El cumplimiento de las actividades propuestas por el estándar mejorará la seguridad cibernética de los sistemas de control y manufactura y ayudará a identificar y abordar vulnerabilidades, reduciendo así el riesgo de comprometer información

confidencial o causar degradación o falla de los sistemas de control y manufactura.

El estándar ISA-99 está dividido en cuatro partes, hasta la fecha algunas ya han sido publicadas mientras que otras están aún en fase de desarrollo [5].

Parte 1: Conceptos, modelos y terminología.
Es un glosario de términos utilizado por el comité encargado del estándar.

Parte 2: Establecimiento de un programa de seguridad para un sistema de control y manufactura.
Orienta sobre cómo establecer un programa de seguridad para un sistema de control y manufactura

Parte 3: Operación de un programa de seguridad para un sistema de control y manufactura. Parte en desarrollo

Parte 4: Requerimientos específicos de seguridad para un sistema de control y manufactura. Parte en desarrollo
Cada una de las cuatro partes que conforma el estándar está orientada a los niveles 0, 1, 2 y 3 del modelo jerárquico funcional descrito en el estándar ISA-95, presentado en la figura 1.1 [6]. Planeación del negocio y el sistema de logística (nivel 4) no está incluido dentro del alcance de este estándar, sin embargo la integridad de los datos en las comunicaciones de dominio de los sistemas de control y manufactura que van hacia las unidades de negocio si deben estar incluidos.

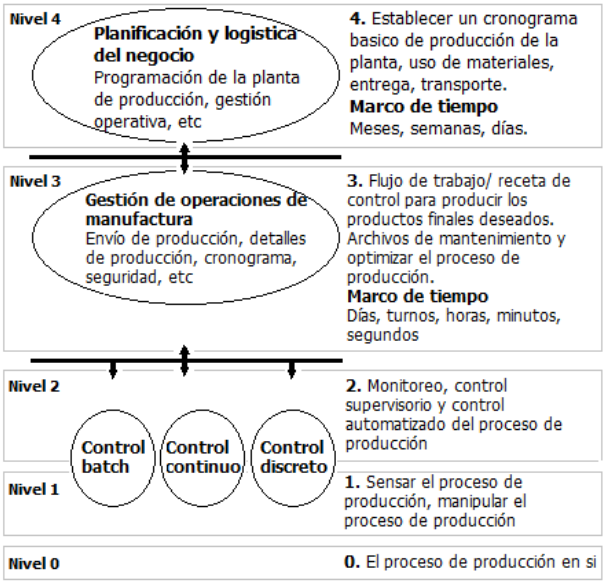


Figura 1.1. ANSI/ISA 95 Modelo jerárquico funcional.

Un esquema de seguridad es un conjunto de políticas de seguridad y procedimientos que deben ser usados colectivamente para impulsar la seguridad cibernética a lo largo de la compañía. Los pasos para desarrollar este esquema son descritos en la parte dos del estándar, razón por la cual, será la base para desarrollar el presente trabajo [1].

El esquema de seguridad se obtiene al desarrollar 18 actividades enmarcadas en las 4 fases del ciclo de Deming: *Planear, Hacer; verificar, Actuar*. [7]

Planear: Establece el alcance y las políticas del esquema de seguridad, identifica, clasifica y evalúa los riesgos.

Hacer: Implementar y operar el esquema de seguridad y todos sus procesos.

Verificar: Monitorear, evaluar y medir el desempeño y reportar los resultados para una posterior inspección.

Actuar: Tomar acciones correctivas y preventivas y mejorar continuamente el desempeño.

El presente trabajo abarca las fases *Planear – Hacer,* omitiendo las actividades cuyo objetivo sea una implementación u operación física sobre el sistema de control debido a que están fuera del alcance del mismo.

A continuación, en la figura 1.2, se presenta el grafico de las 19 actividades propuestas por el estándar ISA-99. Las actividades marcadas con una estrella son aquellas pertenecientes a las fases *Planear – Hacer* incluidas en el trabajo. El eje X representa el tiempo y el eje Y indica la madurez del esquema de seguridad [1].

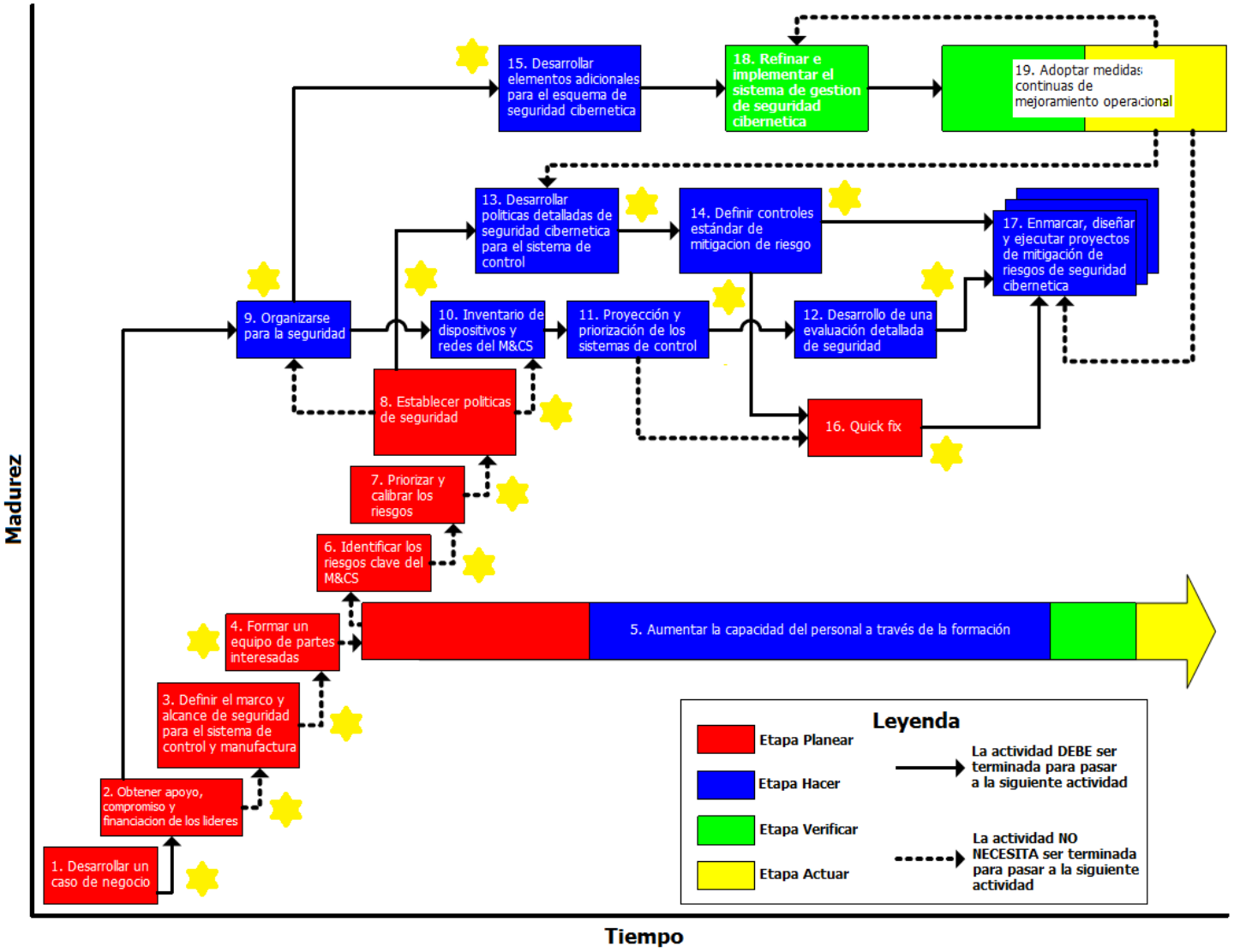


Figura 1.2. Actividades del Estándar ISA-99.

1.1. ACTIVIDADES DEL ESTANDAR ISA-99

A continuación se presenta una breve descripción de cada una de las actividades establecidas por el estándar [1], con el fin de lo lograr un primer acercamiento hacia lo que se debe desarrollar.

- **Desarrollar un caso de negocio.**
  El caso de negocio proporciona la justificación financiera y de negocio para crear un programa integrado de seguridad cibernética.

- **Obtener apoyo, compromiso y financiación de los líderes.**
  El caso de negocio se presenta a las personas que lideran las tecnologías de la información y los sistemas de control y manufactura. Los líderes serán responsables de aprobar y dirigir políticas de seguridad cibernética, asignar roles de seguridad e implementar el programa de seguridad cibernética a lo largo de la compañía.

- **Definir el marco y alcance de seguridad para el sistema de control y manufactura.**
  Decidir y documentar el objetivo del esquema de seguridad cibernética, las organizaciones afectadas, todos los sistemas de computación y redes involucrados, presupuesto, recursos necesarios y división de responsabilidades

- **Formar un equipo de partes interesadas.**
  El equipo de partes interesadas lo conforman las personas responsables de las operaciones de fabricación, gestión de seguridad en los procesos, soporte de red, control de procesos, seguridad física del sitio, mantenimiento y soporte de las TI. Las partes interesadas son responsables de sacar adelante la iniciativa de seguridad cibernética.

- **Aumentar la capacidad del personal a través de la formación.**
  Diseñar programas de entrenamiento efectivo y vehículos de comunicación para ayudar a los empleados a entender porque se requieren nuevos procedimientos de acceso y control, ideas que se puedan usar para reducir riesgos y el impacto sobre la compañía si los métodos de control no son incorporados.

- **Priorización y calibración de riesgos.**
  Las partes interesadas deben considerar un amplio rango de amenazas en la seguridad cibernética y un amplio rango de vulnerabilidades potenciales

en la operación de los sistemas de control y manufactura de la compañía. Las partes interesadas necesitan entender como estas amenazas podrían afectar los activos de la compañía para causar daño.

- **Identificar los riesgos clave del sistema de control y manufactura**
  Una vez las amenazas, vulnerabilidades y consecuencias son aclaradas, cada escenario necesita ser priorizado y calibrado frente al nivel de tolerancia del riesgo corporativo que ha sido desarrollado por otros sistemas de gestión de riesgo.

- **Establecer políticas de seguridad**
  Desarrollar políticas de seguridad y obtener apoyo de los líderes. Comunicar las políticas para que todos entiendan el objetivo de esta, como y quien debe cumplirlas.

- **Organizarse para la seguridad.**
  Establecer la estructura organizacional responsable de manejar la seguridad física y cibernética dentro de la compañía.

- **Inventario de los dispositivos y redes del sistema de control y manufactura.**
  Identificar las aplicaciones, sistemas de cómputo, redes dentro de las áreas de tecnología de la información y sistemas de control y manufactura.

- **Proyección y priorización de los sistemas de control.**
  Evaluar cada clase de sistema para entender las consecuencias financieras y de seguridad en el caso en que la confidencialidad, integridad o disponibilidad del sistema estén comprometidas.

- **Desarrollo de una evaluación detallada de seguridad.**
  La evaluación del riesgo ayuda a identificar cualquier debilidad que pueda estar presente en el sistema y que podría permitir acceso inapropiado al mismo y a los datos. Además se identifican los riesgos relacionados con la seguridad cibernética y qué enfoques de mitigación pueden ser usados para reducir los riesgos.

- **Desarrollar políticas detalladas de seguridad cibernética para el sistema de control.**
  Después de que los riesgos del sistema han sido claramente entendidos, se deben examinar las políticas de seguridad existentes para comprobar que

estos se aborden adecuadamente. Si es necesario, se deben desarrollar políticas adicionales suficientemente detalladas y procedimientos para abordar sistemas administrativos, sistemas de control y manufactura y cadenas de valor.

- **Definir controles estándar de mitigación de riesgo.**
  Analizar la evaluación detallada de riesgos, identificar los costos de mitigación de cada riesgo, comparar los costos con la ocurrencia del riesgo y seleccionar los controles de mitigación donde el costo es menor que el riesgo potencial.

- **Desarrollar elementos adicionales para el esquema de seguridad cibernética.**
  Se deben buscar formas de incorporar mejoras a los procesos existentes para lograr los objetivos del esquema de seguridad en vez de empezar desde cero y desarrollar un conjunto de prácticas completamente nuevo. Buscar maneras de apalancar y evolucionar las prácticas existentes con el fin de satisfacer las necesidades de seguridad.

- **Soluciones Rápidas.**
  Mientras se desarrolla el plan de seguridad es posible identificar algunos riesgos que pueden ser mitigados con soluciones “rápidas” a bajo costo, y reducir además el nivel de riesgo.

1.2. ELEMENTOS CLAVE EN EL DESARROLLO DE UN ESQUEMA DE SEGURIDAD

Además de las actividades descritas anteriormente, existen 18 elementos clave que pueden ser tenidos en cuenta en el desarrollo de un esquema de seguridad [1]. Se presentan a continuación en una breve descripción:

- **Importancia de la seguridad cibernética en el negocio.**
  Señala que es importante establecer que la compañía conozca y entienda la importancia que tienen los riesgos asociados a las TI sobre su negocio. Estos riesgos se extienden a los sistemas de control y manufactura, empresa conjunta, terceros y subcontratación.

- **Alcance del esquema de seguridad cibernética.**
  El alcance puede incluir todos los aspectos de los sistemas de control y manufactura, puntos de integración con socios comerciales, clientes y proveedores.

- **Políticas de seguridad.**
  Aborda el compromiso de los líderes de la organización con la mejora continua a través de la publicación de políticas. Las políticas deben ser expuestas a los empleados y se revisarán periódicamente para asegurar que siguen siendo apropiadas.

- **Seguridad organizacional.**
  Establece una organización, estructura o red con responsabilidades sobre la seguridad en general teniendo en cuenta que los componentes tanto físicos como cibernéticos.

- **Seguridad del personal.**
  Comprende responsabilidades de seguridad en la fase de selección de personal, incluyendo estas responsabilidades en los contratos, y monitoreo del desempeño de los empleados.

- **Seguridad física y ambiental.**
  Abarca la protección de activos físicos o tangibles (computadores, redes, equipos de manufactura, etc.) de daños, pérdida, acceso no autorizado o uso incorrecto. Los activos o información crítica deben estar ubicados en un área segura, protegida por un perímetro de seguridad y controles de entrada. Estos controles de seguridad física, trabajan en conjunto con las medidas de seguridad cibernética para proteger la información.

- **Identificación, clasificación y evaluación de riesgos.**
  Establece que identificar, realizar y analizar amenazas potenciales de seguridad, vulnerabilidades y consecuencias usando metodologías apropiadas, de tal forma que las compañías protegen su organización y la capacidad para cumplir con su misión.

- **Gestión de riesgo e implementación.**
  Abarca el desarrollo e implementación de medidas de seguridad acordes con los riesgos identificados. La importación de la mitigación del riesgo es convertir todos los planes de gestión del riesgo en acciones y contar con un plan que permita monitorear su efectividad.

- **Planeación y respuesta de los incidentes.**
  Establece la necesidad de estar alerta, para determinar y detectar cualquier incidente de seguridad. Si ocurre un incidente, la empresa debe identificar y responder prontamente de acuerdo con las prácticas establecidas por la misma, las cuales pueden incluir procesos de notificación, procesos de documentación, investigación y prácticas de seguimiento.

- **Comunicaciones, operaciones y gestión de cambios.**
  Abarca políticas y procedimientos que deben ser desarrollados y seguidos para mantener la seguridad en los sistemas de cómputo e instalaciones de

manufactura. Estas políticas y procedimientos generales deben articular claramente todos los aspectos de seguridad operacional.

- **Control de acceso.**
  Abarca la administración de cuentas, autenticación y autorización. La administración de cuentas debe establecer reglas para asegurar que el acceso de los usuarios a los datos y sistemas sea controlado. La autorización comprende la necesidad de los negocios de establecer y emplear un conjunto de procedimientos de autenticación acorde con los riesgos para evitar que usuarios no autorizados, hosts, aplicaciones, servicios y recursos accedan a los sistemas críticos. La autenticación describe los procesos para identificar correctamente usuarios de redes, hosts, aplicaciones, servicios y recursos para algunos tipos de transacciones computarizados utilizando una combinación de factores de identificación o credenciales. La autenticación es el prerrequisito para permitir el acceso a los recursos de un sistema.

- **Gestión de información y documentación.**
  Comprende los procedimientos asociados con la clasificación de todos los datos y salvar información y documentos asociados con los esquemas de seguridad cibernética

- **Desarrollo y mantenimiento del sistema.**
  En los ambientes de los sistemas de control y manufactura, el desarrollo de sistemas es frecuentemente una tarea de configuración de aplicaciones para llevar a cabo los requerimientos del sistema. El mantenimiento es la actividad que apoya los cambios en las aplicaciones asociadas a los procesos así como parches y actualizaciones en los sistemas.

- **Entrenamiento del personal y concientización de seguridad.**
  Un entrenamiento efectivo en seguridad cibernética y concientización de seguridad se basa en proveer a cada empleado la información necesaria para identificar, revisar y ayudar a asegurar sus propias prácticas de trabajo.

- **Cumplimiento.**
  Comprende la programación y ejecución de auditorías y el cumplimiento de requerimientos legales, regulatorios y de seguridad. Establece que las compañías deben evaluar periódicamente sus programas y procesos de seguridad para confirmar que estos programas y procesos estén trabajando adecuadamente y que las acciones correctivas se estén ejecutando apropiadamente.

- **Plan de continuidad del negocio.**
  Se debe contar con un plan de acción para responder a consecuencias de desastres, fallas de seguridad y pérdida del servicio en la compañía. Es

necesario desarrollar planes de contingencia, implementarlos y probarlos para asegurarse que los procesos pueden ser recuperados en el momento oportuno.

- **Monitoreo y revisión del esquema de seguridad.**
  Se emplean métodos internos de control tales como auditorias del sistema, auditorías de cumplimiento e investigación de incidentes, permite a la compañía verificar la efectividad del sistema y si está operando de acuerdo con las expectativas.

- **Mantenimiento e implementación de mejoras.**
  Las compañías deben continuamente hacer seguimiento, mediciones, y mejoras en la seguridad para mantener a las personas, propiedades, productos, procesos, información y sistemas de información más seguros.

2. LINEAMIENTOS DE SEGURIDAD PARA UN LABORATORIO ACADÉMICO UNIVERSITARIO CON ACCESO REMOTO.

Las actividades del estándar ISA-99 mencionadas en el capítulo anterior no están diseñadas para ser aplicadas directamente a un entorno académico, por tal razón es necesario adaptarlas para dicho uso. Lo que se busca al plantear lineamientos de seguridad para un laboratorio académico universitario con acceso remoto es estudiar cada una de las actividades propuestas por el estándar y adaptarlas con el fin de que estas recomendaciones puedan ser seguidas por cualquier institución universitaria que preste este tipo de servicios.

Los lineamientos desarrollados en este capítulo definen una serie ordenada de pasos a seguir para que al diseñar un esquema de seguridad cibernética para un laboratorio académico con acceso remoto se tengan en cuenta las necesidades y características del mismo.

A continuación se describe en detalle las actividades que deben seguirse para diseñar el esquema de seguridad.

2.1. Desarrollo de un caso de negocio

Dentro de cada universidad, el camino para desarrollar un programa de seguridad cibernética efectivo en sus sistemas de control y manufactura comienza con individuos que reconocen los riesgos que está tomando la universidad o la facultad, después articulan estos riesgos internamente, no solo en términos técnicos, sino también en términos económicos que sean de prioridad para la universidad.

El objetivo de esta actividad es justificar la necesidad de diseñar un esquema de seguridad, para ello se debe conocer el funcionamiento del laboratorio universitario con acceso remoto con el fin de poder identificar las vulnerabilidades, riesgos y consecuencias que están presentes en él. Las diferentes vulnerabilidades pueden ser explotadas por:

- Individuos que buscan penetrar sistemas informáticos a través de ataque directos (hacking) o indirectos (virus y gusanos), para robar o destruir información o interrumpir las actividades de una organización.
- Empleados, contratistas o estudiantes disgustados quienes roban información por venganza para ganar beneficio personal.
- Empleados o estudiantes bien intencionados quienes por descuido realizan cambios en el proceso o controlador incorrecto.

- Empleados o estudiantes que incumplen las políticas o procedimientos para obtener los resultados de laboratorio esperados.
- Ladrones profesionales que roban información para venderla

De la misma manera se deben tener en cuenta los equipos (PLC, sensores, actuadores, etc.), procedimientos y herramientas (laboratorio remoto) que generan riesgos para la seguridad virtual y física del laboratorio.
Por otro lado dentro de las consecuencias se puede incluir:

- Lesión o muerte de estudiantes o empleados.
- Lesión o muerte de las personas de la comunidad.
- Daño de equipos.
- Daño medioambiental.
- Contaminación de producto.
- Pérdida de información confidencial.
- Pérdida de imagen de la universidad.
- Pérdidas económicas.

Las vulnerabilidades, riesgos y amenazas reconocidas en esta etapa inicial no son las únicas existentes ya que en etapas posteriores pueden aparecer más. Por lo tanto el esquema de seguridad no debe limitar su alcance a las listadas en este ítem.

A partir de las vulnerabilidades, riesgos y consecuencias reconocidas en el laboratorio, se debe escribir un documento en el que se exponga y justifique la necesidad de desarrollar un esquema de seguridad cibernética para el mismo.

2.2. Obtener apoyo, compromiso y financiación de los directivos

El compromiso con un programa de seguridad comienza en la parte superior de la organización. Los programas de seguridad cibernética, con un apoyo notable por parte de los líderes de la organización; tienen más probabilidad de cumplir con los objetivos además de tener un mejor funcionamiento [1].

Generalmente las Universidades están organizadas con una estructura piramidal, en donde están de abajo hacia arriba, la coordinación, el departamento, la decanatura y el consejo de facultad.

A modo de ejemplo se utiliza el organigrama mostrado en la figura 2.1, para el laboratorio de control de procesos del programa de Ingeniería en Automática Industrial, en este ejemplo, el caso de negocio se presentaría al departamento de

electrónica, instrumentación y control (DEIC) y si recibe aprobación se informa al ente superior.

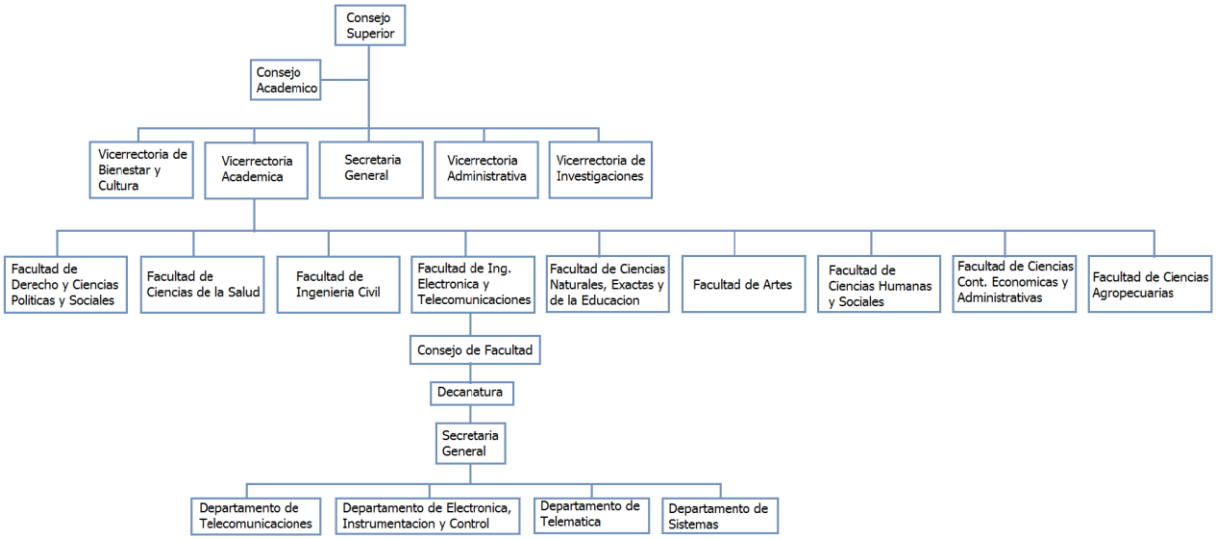


Figura 2.1. Organigrama parcial de la Universidad del Cauca.

Esta actividad inicia con identificar, empezando por la base de la estructura, a quien debe ser presentado el caso de estudio con el fin de obtener el apoyo al trabajo siguiendo el conducto regular establecido por la Universidad.

Una vez identificados los directivos de la Universidad a quien dirigirse, se presenta el caso de estudio, el enfoque debe estar orientado en exponer y argumentar los beneficios que el esquema de seguridad generaría al laboratorio y a la Universidad en términos operativos y académicos.

De la misma manera se debe mostrar la comparación entre el costo de contar con un esquema de seguridad versus el costo de convivir con los riesgos, vulnerabilidades y sus consecuencias. Si en esta temprana etapa del proyecto no se dispone de un valor aproximado de presupuesto es necesaria una segunda reunión para tratar este requerimiento.

2.3. Definición del marco y alcance de seguridad para el sistema de control y manufactura.

Una vez realizado el caso de estudio y recibido el apoyo, compromiso y financiación por parte de los directivos de la Universidad; el siguiente paso consiste en definir formalmente el alcance y delimitar el marco bajo el cual será desarrollado el proyecto. El marco debe establecer que es lo que se va a lograr en términos académicos, de arquitectura y funcionales y cuando se alcanzarán. Se recomienda que el desarrollo del esquema de seguridad sea encargado a un grupo interdisciplinar de personas, esto será tratado más adelante, sin embargo en

esta etapa se establece la persona que dirige el proyecto. Ella será responsable de que el mismo se ejecute, además de asegurar su correcta financiación, auditoria y retroalimentación entre todas las partes interesadas.

El alcance de seguridad para el sistema de control y manufactura debe responder a tres diferentes aspectos: académico, de arquitectura y funcional.

En el aspecto académico se deben responder las siguientes preguntas:

- ¿Qué departamentos de facultad o programas están incluidos?
- ¿Qué materias o proyectos se verán afectados?
- ¿Qué sitio físico será incluido, el laboratorio está centralizado o distribuido?

En cuanto a la arquitectura se debe responder a:

- ¿Qué sistemas de computación y redes serán incluidos?
- ¿Qué Sistemas de Control y Adquisición de Datos (SCADA por sus siglas en ingles) y sistemas de monitoreo serán incluidos?
- ¿Qué sistemas de computación que no participan en las prácticas de laboratorio pero si son necesarios para su funcionamiento serán incluidos (aquellos limitados a las TI)?
- ¿Qué Sistemas Instrumentados de seguridad (SIS) serán incluidos?
- ¿Qué sistemas robóticos serán incluidos?
- ¿Si el laboratorio no es de uso exclusivo de la Universidad y presta servicios a terceros, quienes estarán incluidos?

Para referirse al aspecto funcional se deben considerar las siguientes preguntas:

- ¿De qué manera se relaciona el alcance de este proyecto con los sistemas de administración de riesgo existentes?
- ¿De qué manera se relaciona el alcance de este proyecto con las políticas de seguridad de la información que ya están siendo aplicadas en el laboratorio?
- ¿De qué manera se relaciona el alcance del proyecto con estándares técnicos y procedimientos que ya están siendo aplicados a componentes de arquitectura específicos (sistemas de control de proceso, SCADA, SIS, sistemas robóticos, etc.)?
- ¿De qué manera se relaciona el alcance con proyectos ya existentes?
- ¿De qué manera se relaciona el alcance con servicios existentes?

Es muy importante que se defina qué tan abierto va a ser el laboratorio remoto. ¿Sera implementado para uso exclusivo de la universidad o como un servicio más

abierto para ser ofrecido a otras instituciones? Esto influye directamente sobre los riesgos y vulnerabilidades a las que se enfrenta el laboratorio y será analizado más adelante.

Dar respuesta a estas preguntas es necesario para que el esquema de seguridad que se proponga vaya acorde con el funcionamiento existente de la Universidad, y no genere conflictos o peligro para otros sistemas.

2.4. Formación de un equipo con las partes interesadas

El equipo de partes interesadas debe estar formado por un grupo interdisciplinar con el fin de reunir las habilidades y conocimientos que generalmente no se encuentran en una sola persona. Dependiendo de las necesidades que vayan surgiendo en el tiempo durante el desarrollo de actividades y fases al desarrollar el esquema de seguridad, este equipo está sujeto a cambios, con el fin de entregar soluciones más completas y eficaces.

El equipo de partes interesadas puede estar conformado por:

- Estudiantes de trabajo de grado.
- Estudiantes de grupos de investigación.
- Estudiantes de otros programas que utilicen el laboratorio
- Docentes del programa al que pertenece el laboratorio.
- Docentes de programas que trabajen las TI.
- Docentes de programas de control y automatización.
- Personal de apoyo y mantenimiento de la Universidad.
- Proveedores de la Universidad.

Además de definir los integrantes del equipo, se debe establecer con cada uno el horario de trabajo que será destinado para el desarrollo del esquema de seguridad. El compromiso y disposición por parte del equipo es esencial para el éxito del proyecto.

2.5. Aumento de la capacidad del personal de seguridad a través de la formación.

El entrenamiento de uno u otro tipo es una actividad que se extiende en todo el desarrollo del proyecto. Inicia después de haber definido el marco y alcance del proyecto y el equipo de partes interesadas. Las actividades de formación pueden ser descritas basándose en la fase del ciclo Planear - Hacer – Verificar- Actuar en que se encuentren [1].

Debido a que el alcance del presente trabajo llega hasta las fases Planear – Hacer, la adaptación del estándar ISA-99 se hace en este marco.

Planear — El equipo de partes interesadas necesitara formación en temas específicos del marco y alcance del trabajo. Por ejemplo, documentarse sobre las redes presentes en el laboratorio, sistemas computarizados de control, políticas de seguridad en laboratorios remotos de control, etc.
De la misma manera, se debe tener información sobre trabajos en otras universidades, incidentes que se hayan presentado, aplicaciones de estándares de seguridad cibernética en sistemas de control de procesos como ISA-99, etc. Se debe contar además con información concerniente a los riesgos que fueron considerados en el desarrollo del caso de negocio.

Hacer — Montar un esquema de seguridad cibernética al laboratorio con acceso remoto trae cambios en su funcionamiento y en la manera de realizar las prácticas. En la fase “hacer” la formación debe estar dirigida a los estudiantes, docentes y personal involucrado con el laboratorio para lograr el entendimiento de los cambios que el esquema conlleva. Por ejemplo, si los estudiantes cuentan con guías de laboratorio, incluir en esta, información sobre el esquema de seguridad montado en el laboratorio, publicación de las políticas de seguridad y sobre la nueva forma de operar las diferentes plantas, entre otros.

2.6. Identificación de los riesgos clave del sistema de control y manufactura.

Para identificar la naturaleza de los riesgos asociados a un laboratorio de control de procesos con acceso remoto es necesaria la utilización de técnicas para el análisis de riesgo (PHA). Actualmente se encuentran en el mercado una gran variedad de estas y para hacer una correcta selección es necesario saber en qué fase del ciclo de vida del proyecto se encuentra [8]. Las fases del ciclo de vida son:

1. Investigación y desarrollo
2. Diseño conceptual
3. Ingeniería básica o definición del diseño
4. Ingeniería detallada
5. Operación rutinaria
6. Proceso de modificación
7. Investigación de incidentes
8. Construcción y puesta en funcionamiento

9. Cierre o desmantelamiento

A continuación se presentan las características de cada una de las fases para la elección de la técnica PHA más adecuada:

1. Investigación y desarrollo I+D.
   En esta fase se encuentran aquellos proyectos que se diseñan a partir de nuevas tecnologías o innovaciones de alguno existente. Normalmente no se dispone de suficiente información sobre el proceso para hacer recomendaciones para controlar peligros y carece sobre todo de experiencia en la operación del proceso.
   En esta fase todos los resultados son cualitativos.

2. Diseño conceptual.
   En esta fase del proyecto se intentan identificar los principales peligros asociados al mismo. Normalmente no se dispone de la suficiente información sobre el proceso para hacer recomendaciones de alternativas para controlar los peligros.
   Todos los resultados son cualitativos.

3. Ingeniería básica o definición del diseño.
   En esta fase, si la información disponible lo permite, es posible realizar un análisis más profundo de aquellos escenarios de accidente cuyo peligro percibido es alto. También cobran importancia las alternativas planteadas para eliminar o controlar los peligros identificados en las etapas anteriores.
   Todos los resultados son cualitativos.

4. Ingeniería detallada.
   A esta altura del proyecto, lo más habitual es que se hayan identificado todos los peligros generales, por ello los resultados están más enfocados en identificar y evaluar escenarios de accidente, a recomendar alternativas para controlar los peligros y escenarios de accidente y a generar información para poder realizar análisis cuantitativos de riesgo. En esta fase ya se dispone de información necesaria para utilizar las técnicas PHA más detalladas (ETA, FTA).
   La carencia más importante es la referente a información sobre experiencia en la operación, aunque en ocasiones, se puede suplir con la información de procesos similares ya existentes.

5. Operación rutinaria.
   En esta fase se identifican nuevos peligros, escenarios de accidente, que surgen debido a la operación continua del proceso y a las modificaciones del diseño original, se hacen recomendaciones sobre las alternativas para controlar los anteriores y se genera información para poder realizar análisis cuantitativos de riesgo. Para la evaluación de escenarios de accidente

complejos y de los errores humanos se generan resultados cuantitativos para tener una idea sobre la probabilidad de que sucedan y sobre las causas y/o efectos de los mismos.

6. Proceso de modificación.
   En esta fase se realizan evaluaciones de las modificaciones o mejoras del diseño original del proceso, con el objetivo de no introducir nuevos peligros. En función del peligro potencial percibido asociado a la modificación o al tipo de fallo que puede introducir la misma, se utilizarán técnicas que pueden cubrir la identificación de un gran rango de peligros o aquellas que se centran en escenarios específicos.
   En esta fase se dispone de suficiente información del proyecto para poder aplicar cualquier técnica PHA, incluida la experiencia en la operación del proceso.

7. Investigación de incidentes.
   En esta fase se recomienda utilizar las técnicas que permiten revisar y/o evaluar de forma detallada aquellas zonas o áreas del proceso que han sufrido algún tipo de accidente/incidente con el objetivo de identificar el fallo que lo originó y sugerir alterativas que permitan eliminar reducir la probabilidad de que se vuelva a producir dicho accidente.
   El resultado que se obtiene es una lista del fallo/os o error/es que han producido el accidente, así como un listado de las recomendaciones o alternativas para eliminar o reducir la probabilidad de que vuelva a suceder el mismo.

8. Construcción y puesta en funcionamiento.
   El objetivo de realizar un estudio PHA en esta fase del proyecto es verificar que la instalación se ha construido según lo diseñado y cumpliendo las prácticas de la industria y que los peligros para la seguridad no han sido ignorados. Por todo ello, se aconseja utilizar técnicas que puedan identificar una amplia gama de peligros.

   En esta fase cobra especial interés la información relacionada con los materiales y procedimientos de construcción y los requisitos o estándares de la compañía que operará el proceso.

9. Cierre y/o desmantelamiento.
   El cierre y/o desmantelamiento de una instalación o parte de la misma puede exponer al personal a diferentes peligros, por ello se recomienda utilizar una técnica que pueda examinar una gran variedad de peligros y que permita generar recomendaciones para reducir su impacto. La técnica seleccionada debe ser apta para procesos que no están en operación.
   En esta fase cobra especial interés toda la información relacionada con los posibles materiales de desecho que pueden tener impacto medioambiental sobre la zona cercana a la ubicación de la instalación clausurada.

Para cada una de las fases de un proyecto, se han definido una serie de técnicas PHA (Process Hazard Analysis) que son las más utilizadas de forma general en la industria debido a su metodología de aplicación y al nivel de detalle de la información que se requiere [8].

En la tabla 2.1 se muestra la clasificación:

FASE DEL CICLO DE VIDA	TÉCNICA PHA RECOMENDADA
Investigación y desarrollo	PrHA, What if, Relative ranking
Diseño conceptual	prHA, What if, Checklist, Relative ranking
Ingeniería básica o definición del diseño	PrHA, What if, Checklist, HAZOP, FMEA
Ingeniería detallada	What if, Checklist, HAZOP, FMEA, FTA, ETA
Construcción	What if, Checklist, Safety review
Operación rutinaria	Checklist, HAZOP, FMEA, Safety review, FTA, ETA HRA, CCA
Proceso de modificación o expansión	What if, Checklist, HAZOP, FMEA, FTA, ETA, Safety review, HRA, CCA
Cierre o desmantelamiento	What if, Checklist, Safety review

Tabla 2.1. Técnicas PHA más utilizadas en cada fase del ciclo de vida

A continuación se presenta una breve descripción:

- **Análisis preliminar de riesgos PrHA**
  El propósito de esta técnica consiste en evaluar los peligros en las primeras fases del ciclo de vida de un proceso para tener una visión general de las áreas de mayor peligro, donde puede ser conveniente realizar estudios posteriores más detallados.
  Los resultados son cualitativos y se tabulan en una tabla que contiene para cada peligro considerado:
  - Las causas del peligro.
  - Las consecuencias o efectos principales.
  - La categoría del peligro, con lo que se realiza una clasificación cualitativa que se puede usar para priorizar las recomendaciones.
  - Las acciones correctivas y medidas preventivas recomendadas.

- **What-if.**
  Su propósito es identificar los peligros y situaciones potenciales de accidente asociados a una instalación industrial, con el objetivo de recomendar alternativas que puedan controlar las consecuencias de los mismos.
  Los resultados son cualitativos y se presentan en forma de tabla, la cual contiene para cada pregunta con el formato ¿qué pasaría sí? los siguientes campos:

- Consecuencias o peligros que pueden aparecer si se cumplen las condiciones enunciadas en la pregunta.
- Medidas de seguridad existentes para evitar las consecuencias.
- Recomendaciones para reducir las consecuencias.

- **Checklist.**
  Busca garantizar que se cumplen las prácticas estándar, a través de la identificación de peligros conocidos, de deficiencias de diseño y de consecuencias de accidentes asociados al equipo y operación del proceso.
  Los resultados son cualitativos e incluye:
  - Una lista de respuestas a las preguntas estándar de la checklist, las cuales se basan en diferencias o deficiencias.
  - Algunas veces genera una lista de peligros identificados y las acciones sugeridas para resolverlos.

- **Relative Ranking.**
  El propósito es hacer una clasificación de las áreas del proceso y/o de las operaciones del mismo, comparando las características de las sustancias químicas, las condiciones del proceso y los parámetros de operación. Otro objetivo puede ser determinar si las características peligrosas del proceso son suficientemente significativas para realizar un estudio posterior.
  Los resultados dependen del tipo de técnica utilizada para hacer la clasificación. Pueden incluir una lista de procesos, equipos, operaciones o actividades ordenados por su nivel de peligrosidad.

- **Safety Review.**
  El propósito es garantizar que una instalación se está operando y manteniendo según los estándares de diseño.
  Los resultados son cualitativos e incluyen:
  - Lista de deficiencias identificadas.
  - Lista de áreas de problema.
  - Lista de acciones recomendadas y justificaciones de las mismas, adicionalmente puede contener una lista que ayuda a realizar el seguimiento del estado de la implementación de las acciones.

- **FMEA.**
  Tiene como propósito identificar los modos de fallo del equipo del proceso o sistema para poder evaluar las consecuencias potenciales asociados a cada uno de ellos. Normalmente genera recomendaciones para aumentar la fiabilidad del equipo y mejorar la seguridad del proceso.

Los resultados son cualitativos, normalmente se documentan en forma de tabla, la cual incluye los siguientes campos de información para cada componente del equipo del proceso o sistema estudiado:

- Identificación del equipo: Se relaciona el equipo en cuestión con los planos del sistema y su localización.
- Descripción del equipo: incluye el tipo de equipo, configuración de operación y otras características de servicio (presión elevada, temperatura elevada) que pueden influir sobre los modos de fallos y sus consecuencias.
- Modos de fallo: se consideran todos los posibles modos de fallo del equipo después de estudiar las condiciones normales de operación del mismo.
- Efectos para cada modo de fallo: se describen los efectos inmediatos en el lugar del fallo y los efectos esperados del fallo sobre el resto del equipo.
- Medidas de seguridad existentes que pueden evitar los efectos de cada modo de fallo: descripción de las medidas de seguridad o procedimientos asociados al sistema que pueden reducir la probabilidad de que ocurra un fallo o las consecuencias del mismo.
- Acciones para corregir los efectos de cada modo de fallo: listado de sugerencias de acciones correctivas para reducir la probabilidad de los efectos asociados a cada modo de fallo.

- **HAZOP.**
  Revisar cuidadosamente un proceso y su operación, con el objetivo de determinar si las desviaciones del mismo pueden conducir a consecuencias no deseadas y de este modo poder identificar los peligros del proceso y los problemas de operación del mismo.
  Los resultados son cualitativos y se documentan en una tabla que contiene para cada nodo o sección del proceso:
  - La desviación.
  - La causas que provoquen la desviación.
  - Efectos de la desviación.
  - Medidas de seguridad presentes para evitar las consecuencias.
  - Acciones correctivas a implementar para evitar las consecuencias.

- **FTA (Fault Tree Analysis).**
  El propósito consiste en identificar las combinaciones de fallos del equipo y errores humanos que pueden provocar un accidente.

Produce un modelo lógico de los fallos del sistema, el cual utiliza puertas lógicas para describir los fallos del equipo y los errores humanos que se pueden combinar para causar un fallo principal del sistema. El número de modelos para un proceso complejo depende de cómo se seleccionó el suceso iniciador.

El resultado obtenido es que normalmente se soluciona cada modelo lógico para generar una lista de las secuencias mínimas de fallos que pueden provocar el suceso iniciador, estas listas se pueden ordenar cualitativamente por el número y tipos de fallos de cada una. La inspección de estas listas revela la debilidad del diseño/operación del sistema para lo que se sugieren alternativas para mejorar la seguridad.

- **ETA (Event Tree Analysis)**

  El propósito de esta metodología es identificar las combinaciones de fallos que pueden provocar un determinado accidente y la secuencia de consecuencias o accidentes que este puede provocar.

  El resultado son diagramas en forma de árbol de los fallos o errores (se representan con puertas lógicas) que conducen a un accidente, las secuencias del accidente (las cuales describen las consecuencias posibles de los accidentes en términos de secuencia de sucesos que siguen al suceso iniciador).

  Los resultados se utilizan para identificar la debilidad del diseño y de los procedimientos de operación y normalmente proporcionan recomendaciones para reducir la probabilidad y consecuencias de los accidentes potenciales analizados. Si se usa este método para evaluar una secuencia de accidente, proporciona una lista con las secuencias mínimas.

- **HRA (Human Reliability Analysis)**

  El propósito es identificar los errores humanos potenciales para poder determinar las causas de los mismos.

  El resultado es una lista de los posibles errores humanos que pueden aparecer durante la operación normal o de emergencia del proceso, factores que contribuyen a dichos errores y las modificaciones para reducir la probabilidad de los mismos (cambios en el equipo y en los procedimientos para corregir las deficiencias identificadas).

  También incluye una descripción detallada de las tareas del operador en forma de lista o gráfico, que puede usarse para establecer procedimientos, políticas de formación. Adicionalmente, puede incluir la identificación de las interfaces del sistema afectadas por errores particulares y una clasificación de éstas basándose en su probabilidad de ocurrencia.

- **CCA (Cause and Consequence Analysis)**
  El propósito es identificar las causas y consecuencias de los accidentes potenciales.
  El resultado es diagramas que representan las secuencias mínimas de causas que provocan un accidente y descripciones cualitativas de las consecuencias de los mismos.

Para seleccionar la técnica más adecuada, además de identificar en qué etapa del ciclo de vida se encuentra el proyecto, se tienen en cuenta las siguientes recomendaciones:

- Tipo de resultados necesitados o buscados
  1. Descripción cualitativa de un amplio rango de peligros generales identificados.
  2. Clasificación de los peligros identificados.
  3. Descripción cualitativa de las causas y/o consecuencias de los peligros identificados.
  4. Descripción de un determinado escenario de accidente; cálculo de la probabilidad de que suceda y la representación gráfica de sus consecuencias y/o causas.
  5. Alternativas para eliminar o controlar los peligros y escenarios de accidente identificados.
  6. Entrada de información para un análisis cuantitativo del riesgo.

- La información o documentación técnica disponible
  Que tanto detalle de información, conocimiento y experiencia necesita la técnica PHA.

- Características del problema a analizar.

En resumen, esta actividad se inicia con la identificación de la fase del ciclo de vida en que se encuentra el proyecto. Con esto definido y teniendo en cuenta los resultados buscados y la información disponible, se selecciona la técnica PHA más conveniente para el proyecto [2].

Una vez elegida la técnica que se va a utilizar y de acuerdo a la información obtenida en las actividades anteriores, el equipo de partes interesadas procede a identificar los riegos. Se deben evaluar basándose en aspectos como:

- Dispositivos.
- Las interfaces de comunicación.

- El software y código de programación.
- Redes de comunicación.

2.7. Priorización y calibración de los riesgos.

Para entender el esfuerzo que se debe tomar sobre cada uno de los riesgos, primero deben ser identificados y priorizados. En esta actividad se describen los pasos necesarios para desarrollar un marco en donde se prioricen los riesgos individualmente con el fin de poder justificar adecuadamente las acciones correctivas sobre cada uno de ellos [1].
Inicialmente se deben definir dos términos que permiten la priorización del riesgo.

- Probabilidad (*likelihood* en inglés).
- Riesgo.

La Probabilidad de que una acción es especifico ocurra se calcula por medio de la multiplicación de la *probabilidad de la amenaza* por la *probabilidad de la vulnerabilidad*

Probabilidad = Probabilidad Amenaza X Probabilidad Vulnerabilidad

Donde Probabilidad Amenaza: es la probabilidad de que una amenaza en específico ocurra. Y Probabilidad Vulnerabilidad: es la probabilidad de que una vulnerabilidad en específico sea explotada.

El riesgo está conformado por la probabilidad y la consecuencia. Donde la consecuencia es el impacto negativo que experimenta la Universidad debido al daño de algún activo causado por alguna amenaza o vulnerabilidad.

Riesgo = Probabilidad X Consecuencia

Para priorizar los riesgos se deben hacer las escalas de medición para la probabilidad y la consecuencia, estas varían dependiendo de la información disponible (aspectos económicos, medioambientales, legales, entre otros).

A continuación se presenta un ejemplo de una escala de probabilidad (Tabla 2.2) y una de consecuencia (Tabla 2.3).

PROBABILIDAD	
Categoría	**Descripción**
Alta	Una amenaza/vulnerabilidad cuya ocurrencia es probable en el próximo año
Medio	Una amenaza/vulnerabilidad cuya ocurrencia es probable en los próximos diez años
Bajo	Una amenaza/vulnerabilidad cuya ocurrencia es probable en los próximos cien años
No aplica	Una amenaza/vulnerabilidad para la cual no hay historial de ocurrencia y por lo tanto la probabilidad se considera extremadamente improbable

Tabla 2.2. Escala de probabilidad

CONSECUENCIAS	
Grado	**Parámetros de evaluación**
Leve	Pequeñas heridas, lesiones no incapacitantes o daños menores.
Medio	Lesiones con incapacidad no permanentes o daños superiores al 20% de las instalaciones
Grave	Lesiones con incapacidad permanente o daños superiores al 60% de instalaciones.
Catastrófica	Muerte o daños superiores al 90% de las instalaciones

Tabla 2.3. Escala de consecuencias

Las tablas que se presentan son solo un ejemplo, la categoría, descripción, grado y parámetros de evaluación cambian ajustándose al laboratorio que se esté trabajando.

Una vez se tiene la escala de consecuencia y la escala de probabilidad, se define el nivel de riesgo haciendo uso de la matriz de clasificación de riesgos. En la tabla 2.4 se presenta un ejemplo:

PROBABILIDAD	CLASES DE RIESGOS			
	CONSECUENCIA CATASTRIFICA	CONSECUENCIA GRAVE	CONSECUENCIA MEDIA	CONSECUENCIA LEVE
Alto	I	I	I	II
Medio	I	I	II	II
Bajo	I	II	II	II
No aplica	II	II	II	III

Tabla 2.4. Matriz de clasificación de riesgos

El tamaño de la matriz está determinado por las escalas de probabilidad y consecuencias definidas previamente.

A partir de la información organizada se procede a ejecutar la técnica PHA seleccionada en la actividad *"2.6. Identificación los riesgos claves del sistema de control y manufactura".*

2.8. Establecimiento de políticas de seguridad.

Dentro de cada sistema de gestión de riesgo, hay un conjunto de reglas que describen que acciones deben ser tomadas para manejar un riesgo en particular y que sistemas y unidades organizativas están sujetas a estos requerimientos; estas reglas se llaman políticas [1]. Establecer políticas es el primer paso en la creación de soluciones y acciones de seguridad, estas deben ser desarrolladas con énfasis en cubrir en mayor medida los riesgos calificados con mayor prioridad en la actividad anterior.

El planteamiento de políticas de seguridad depende directamente de los riesgos identificados y priorizados. Algunos de los aspectos que pueden abordar las políticas son:

- Políticas para los estudiantes.
- Políticas para los docentes.
- Políticas para los administradores del Laboratorio con acceso remoto.
- Políticas de mantenimiento.
- Entre otros

En el momento de redactar las políticas se recomienda incluir [9]:

- La declaración de la política (cuál es la posición de la administración o que es lo que se desea regular).
- Especificar quien debe acatar la política (es decir, a quien está dirigida) y quien es el responsable de garantizar su cumplimiento.
- Referencias a otras políticas y regulaciones en las cuales se soporta o con las cuales tiene relación.
- Explicar que acciones se seguirán en caso de contravenir la política.
- Fecha a partir de la cual tiene vigencia la política.

Estas políticas deben ser notificadas la comunidad universitaria, con el fin de que se entienda el objetivo de las mismas, como y quien debe cumplirlas. Es importante que estas vayan agrupadas en subgrupos para hacerlas más accesibles a los lectores que traten un tema en específico.
Es de resaltar que si la universidad comparte recursos con otras instituciones, se deben establecer políticas de seguridad para el uso compartido de los recursos y ser acordes a los servicios prestados.

2.9. Organizarse para la seguridad.

Se recomienda una estructura organizacional responsable de manejar la seguridad física y cibernética dentro de la universidad. Las responsabilidades organizacionales deben ser definidas claramente, los empleados involucrados necesitan recibir el entrenamiento adecuado preparándolos para su función.
Las personas aquí involucradas se encargan del correcto funcionamiento del esquema de seguridad, cumpliendo funciones como:

- Definición de metas estratégicas para el esquema de seguridad y para el equipo encargado.
- Seguimiento de resultados.
- Obtención de recursos adicionales si es necesario.
- Evaluar riesgos y desarrollar políticas.
- Formación para los empleados, estudiantes y profesores.
- Mantenimiento del esquema de seguridad.

Es importante aclarar que este equipo de personas no está encargado en la etapa inicial de diseño del esquema de seguridad (el responsable es el equipo de partes interesadas), sino del funcionamiento una vez esté en operación.
La estructura organizacional es creada de acuerdo a las necesidades que presente el laboratorio remoto, según la disponibilidad y recursos de la universidad. Esta estructura puede ser representada por un grupo de investigación ya existente o uno que se necesite crear, comités, semilleros, entre otras comunidades integradas de aprendizaje.

2.10. Inventario de los dispositivos y redes del sistema de control y manufactura.

En esta actividad se conocen en detalle los dispositivos y redes del sistema de control y manufactura que están dentro del alcance del proyecto. Tiene tres elementos importantes:

- Localizar los dispositivos de control y manufactura usados en el laboratorio con acceso remoto:
  Ubicar la disposición física que tienen las diferentes plantas de control y los dispositivos que hacen parte de ellas.
- Identificar los dispositivos de control y manufactura usados en el laboratorio con acceso remoto:
  Registrar la información sobre cada dispositivo identificado en un formato estándar como: fabricante, rango de trabajo, señal de entrada, señal de salida, span, etc.

- Agrupar los dispositivos de control y manufactura para elaborar un inventario.
  Debido a la cantidad sistemas de control que pueda estar presente en el laboratorio, es de utilidad organizarlos de tal forma que sea más fácil acceder a la información. Esta clasificación se puede hacer de acuerdo a la función de los dispositivos, a sus características, entre otros.

El desarrollo de esta actividad está enfocado en los sistemas en vez de limitarse a sus dispositivos, con el fin de lograr un entendimiento mucho más amplio e identificar los puntos clave del sistema de control sobre el cual se está trabajando.
Los sistemas de control y manufactura pueden incluir los siguientes componentes:

- Sistemas de Control Distribuido (DCS) y dispositivos asociados.
- Sistemas de Supervisión Control y Adquisición de Datos (SCADA) y dispositivos asociados.
- Controlador Lógico Programable PLC y dispositivos asociados.
- Interfaz Hombre Maquina HMI
- Sistemas Instrumentados de Seguridad SIS.
- Máquinas de control numérico CNC.
- Dispositivos de protección de redes (firewalls, sistemas de detección de intrusos, etc).

Así mismo, esta actividad, establece la necesidad de hacer un diagrama general de las redes. Este paso es de vital importancia debido a las condiciones de red con que pueda contar el laboratorio, ya que los laboratorios universitarios de control de procesos tienen fines académicos, se pueden encontrar diferentes tipos de redes y protocolos en la misma instalación.

Finalmente, puede ser de utilidad realizar un diagrama de flujo para las prácticas que se realizan en el laboratorio, con el fin de identificar los activos (cualquier cosa que tenga valor para el laboratorio) críticos del mismo.

2.11. Proyección y priorización de los sistemas de control

Una vez se tiene el inventario de los dispositivos y redes, se necesita saber de qué manera se enfocarán los esfuerzos para asegurar el laboratorio con acceso remoto. Para ello se realiza una proyección y priorización de los sistemas estudiados en la actividad anterior. Se debe comenzar definiendo una escala para valorar cualitativa o cuantitativamente la vulnerabilidad y el riesgo asociado a cada sistema, esta escala va acompañada de los criterios que se tienen en cuenta para cada nivel.

Se recomienda que en esta actividad se reciba el apoyo de docentes o estudiantes con amplios conocimientos en las TI y en sistemas de control y manufactura. Los primeros aportaran conocimiento sobre los dispositivos que están siendo usados en el laboratorio y los segundos aportan el conocimiento sobre las consecuencias que puede traer un incidente de seguridad.

Cuando se esté definiendo el nivel de riesgo asociado a cada sistema, se deben evaluar las consecuencias financieras y de seguridad en el caso de que se vea comprometida la integridad (medida de confianza en la precisión de los datos que están siendo accedidos), disponibilidad (medida de la confiabilidad y facilidad con que cada dato puede ser obtenido cuando se necesite) o confidencialidad (medida de la importancia de los datos) del sistema.

Además de la escala de valoración de riesgos, deben tener en cuenta consideraciones adicionales como:

- El aspecto más importante para la universidad: ambiental, salud, seguridad, financiero, etc.
- Medidas menos costosas para implementar.
- Requerimientos de la universidad.
- Antecedentes de problemas de seguridad cibernética.

2.12. Desarrollo de una evaluación detallada de seguridad.

Con las actividades anteriores se identificaron los dispositivos y redes del sistema de control y manufactura y el riesgo asociado a cada uno de ellos. Con esta información es posible realizar una evaluación mucho más detallada arrojando información más completa en comparación con la actividad *“2.6 Identificación de los riesgos clave del sistema de control y manufactura”.*

El primer paso para desarrollar una evaluación detallada de seguridad es escoger la metodología apropiada para el caso de estudio. En el mercado se encuentran gran cantidad de metodologías que pueden ser utilizadas y que emplean diferentes tipos de información, sin embargo los resultados esperados deben ser los mismos: identificar la información y dispositivos particulares que son vulnerables y que deben ser abordados con estrategias de mitigación de riesgos apropiadas.

Para seleccionar la metodología acorde al caso de estudio se recomienda tener en cuenta los siguientes factores:

- Criterios como facilidad de uso, complejidad, alcance, recursos necesarios y tipo de metodología (cualitativa o cuantitativa).
- Después de listar las metodologías que podrían encajar con las necesidades del laboratorio, se deben evaluar para identificar aquella que cumple con los requerimientos del sistema de control. La evaluación se puede realizar basado en los siguientes criterios:
  - Metodología para la evaluación de la vulnerabilidad de la seguridad cibernética.
  - Observaciones generales.
  - Fortalezas y limitaciones.
  - Como se utiliza la metodología.
  - Información en la página web.

Para encontrar más información sobre metodologías para evaluación detallada de riesgos, refiérase al anexo A.

Una vez seleccionada la mejor metodología, es importante tener en cuenta los siguientes aspectos durante la evaluación detallada de seguridad:

- La evaluación debe ser desarrollada por un equipo interdisciplinar para tener una solución global, puede ser conformado por una persona de seguridad física, seguridad en los sistemas de control, mantenimiento, seguridad de la información y un representante de redes.
- La evaluación debe ir más allá del proceso en funcionamiento, un aspecto fundamental es analizar los riesgos que pueden provenir de mantenimiento o cambios en la configuración del sistema.

Las áreas que generalmente pueden ser vulnerables deben ser previamente identificadas y examinadas. Entre estas áreas se encuentran:

- Puntos de acceso wireless.
- Puntos de módems.
- Software de acceso remoto.
- Conexiones de internet e intranet.
- Cualquier conexión de red que no haga parte directa del sistema de control y manufactura.
- Redes que se extiendan más allá del área físicamente segura.

Al realizar la evaluación se debe evitar las siguientes situaciones:

- Diseñar la solución durante la evaluación.
- Minimizar o exagerar las consecuencias por conveniencia.

- No llegar a un consenso en los resultados de la evaluación de riesgos por parte del equipo encargado.
- Evaluar el sistema sin considerar los resultados de evaluación de otros sistemas similares.

2.13. Desarrollo de políticas detalladas de seguridad cibernética para el sistema de control.

A partir de las políticas de seguridad que se establecieron en la actividad *"2.8. Establecimiento de políticas de seguridad"* y de la evaluación detallada de seguridad desarrollada en la actividad *"2.12. Desarrollo de una evaluación detallada de seguridad",* se obtiene información que permite definir nuevas políticas de seguridad con el fin de ampliar el alcance de las mismas. Para plantear estas nuevas políticas, se debe tener en cuenta las recomendaciones presentadas en la actividad *2. 8.*

2.14. Definición de controles estándar de mitigación de riesgos.

En esta actividad las medidas de seguridad se diseñan con el fin de tratar el riesgo. El diseño debe ser acorde a los resultados obtenidos en la actividad *"2.12. Desarrollo de una evaluación detallada de seguridad"* Los pasos anteriores han sido llevados a cabo para reconocer y priorizar los riesgos que existen en el LCP y deben ser mitigados por el esquema de seguridad que se está proponiendo; esta actividad consiste en el diseño del esquema como tal para dar respuesta a las necesidades previamente establecidas.

A partir de la priorización de los riesgos, se debe definir de qué manera afrontar el riesgo. Según el estándar ISO 27005 (*Information technology, security techniques, information security risk management*) [10] hay cuatro decisiones que pueden ser tomadas:

- Reducir el nivel de riesgo: El nivel de riesgo debe ser reducido a través de los controles seleccionados hasta que el riesgo residual tenga un nivel aceptable. Es importante tener en cuenta también que esta solución se puede realizar siempre que su costo sea menor al costo de asumir el riesgo. Se deben tomar acciones para reducir la probabilidad y/o las consecuencias asociadas a este.

- Retener el riesgo: Si el nivel de riesgo coincide con el nivel de aceptación del riesgo, o si el costo de asumir el riesgo es menor al costo de la solución no

	hay necesidad de implementar controles adicionales y el riesgo debe ser retenido.
• Evitar el riesgo.	Cuando el riesgo identificado se considera muy alto, o los costos de implementar opciones para tratar el riesgo superan los beneficios, la decisión debe ser evitar el riesgo completamente, ya sea retirándose de una actividad o un conjunto de actividades o cambiando las condiciones bajo las cuales la actividad funciona.
• Transferir el riesgo.	Un riesgo debe ser transferido a un tercero que puede manejar más efectivamente dicho riesgo. Cabe aclarar que transferir el riesgo puede generar nuevos riesgos o modificar los existentes, por lo tanto se necesita realizar una evaluación de riesgos nuevamente.

Es importante aclarar que la decisión sobre cómo se va a tratar el riesgo corresponde a las directivas de la universidad, de acuerdo a los costos que para la institución representan y al plan de negocio que se sigue.

2.15. Desarrollo de elementos adicionales para el esquema de seguridad cibernética

Las medidas de seguridad definidas durante las actividades anteriores, dan respuestas a los riesgos y amenazas existentes al implantar un laboratorio de control de procesos con acceso remoto. Sin embargo se debe tener en cuenta que teniendo protección para el sistema de control siempre existe la posibilidad de que éste se vea comprometido, bien sea porque logran pasar las barreras de seguridad, porque se implementan cambios en los sistemas o por la adición de nuevos proyectos sobre el mismo.

Por tal razón es necesario contar con un plan de continuidad, donde se contemplan los asuntos relacionados con mantener o restablecer la producción en caso que ocurra una interrupción indeseada.

Antes de crear este plan es importante especificar los objetivos de restauración para el sistema, basándose en las necesidades del laboratorio. Hay dos enfoques diferentes: restablecimiento del sistema y restablecimiento de los datos. Restablecimiento del sistema abarca restablecer todos los enlaces de comunicación y capacidades de procesamiento. Restablecimiento de los datos

abarca restablecer los datos que describen el funcionamiento de las plantas (código de programación, HMI, valores PID, entre otros).
Un plan de continuidad está dividido en cuatro fases así [11]:

Fase1. Análisis del negocio

Como se mencionó previamente, en esta fase se busca obtener un conocimiento de los objetivos del laboratorio y de los procesos que se consideran críticos para el funcionamiento de la facultad. También se debe tener en cuenta el análisis de riesgos realizado en actividades anteriores, con el fin de identificar en éste, dichos procesos críticos definidos y sus respectivos riesgos.

Para desarrollar esta fase es de utilidad dar respuesta a los siguientes interrogantes:

- ¿Cuáles son las actividades más importantes para el laboratorio?
- ¿Cómo afectaría económicamente una interrupción de los servicios a medida que va pasando el tiempo sin reanudar el servicio?
- ¿Cuál es el plazo máximo para volver a la normalidad sin llegar a incurrir en graves pérdidas?
- ¿Cuál sería la capacidad operativa del laboratorio a medida que pasa el tiempo?

Fase 2. Selección de estrategias

En esta fase se seleccionan los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente que provoque una interrupción en el funcionamiento del laboratorio. El método seleccionado deberá garantizar la restauración de los procesos afectados en los tiempos que se establezcan (definidos previamente). Algunas estrategias que se pueden tomar son:

- Reubicación de personal con funciones no urgentes en tareas más importantes
- Teletrabajo
- Sitio alternativo subcontratado a terceros

De todas las alternativas existentes se debe elegir la más adecuada en el caso del laboratorio con acceso remoto para el cual se está diseñando el plan, dependerá de las necesidades del mismo, en cuanto a tiempos de recuperación, costos económicos, recursos, etc.

Fase 3. Desarrollo del plan

Luego de seleccionar la estrategia de respaldo hay que desarrollarla e implantarla dentro del laboratorio. Esta es la fase de llevar el plan a la acción, y para ello se debe definir:

- Los equipos (de personas) y materiales necesarios para el desarrollo del plan.
- Las responsabilidades y funciones de cada uno de los equipos.
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el plan.
- Los procedimientos de actuación ante incidentes.
- La estrategia de vuelta a la normalidad.

Fase 4. Pruebas y mantenimiento

Es importante tomar en cuenta que no todo termina con la implementación del plan. Luego se debe evaluar para determinar si realmente funciona y es efectivo, qué aspectos hay que mejorar o eliminar del todo, además de cómo mantenerlo en el tiempo.

Se debe definir qué tipo de pruebas se van a utilizar (reales o de exposición mínima), realizar ejercicios técnicos (ejecución de procedimientos de notificación y operativos, el uso de equipos de hardware, software y posibles centros y métodos alternativos para asegurar un rendimiento adecuado) y un test completo (implica la restauración real de la capacidad de proceso en un centro alternativo).

Además, al estar agregando elementos de seguridad al laboratorio, el tipo de mantenimiento que se le da se ve afectado, por tal razón en esta actividad se consideran los cambios a introducir para los trabajos de mantenimiento.

Se recomienda realizar auditorías periódicamente para determinar que el laboratorio con acceso remoto y las plantas funcionan adecuadamente, para ello se deben tener en cuenta los siguientes ítems:

- Los controles de seguridad implementados en el laboratorio funcionan correctamente
- Los cambios realizados son abordados de la manera establecida.

2.16. Soluciones rápidas

A medida que se desarrolla el esquema de seguridad, es posible identificar varios riesgos que pueden ser mitigados por una "solución rápida", soluciones de bajo costo, prácticas de alto valor que pueden reducir significativamente el riesgo. Algunos ejemplos de actividades que entran en la categoría incluyen la restricción de acceso a Internet y la eliminación de acceso al correo electrónico desde los computadores de las plantas, restricción de acceso al código de programación, entre otros.

3. DESCRIPCION DE LA PLANTA DE CONTROL DE PRESION DEL LABORATORIO DE CONTROL DE PROCESOS DE LA UNIVERSIDAD DEL CAUCA

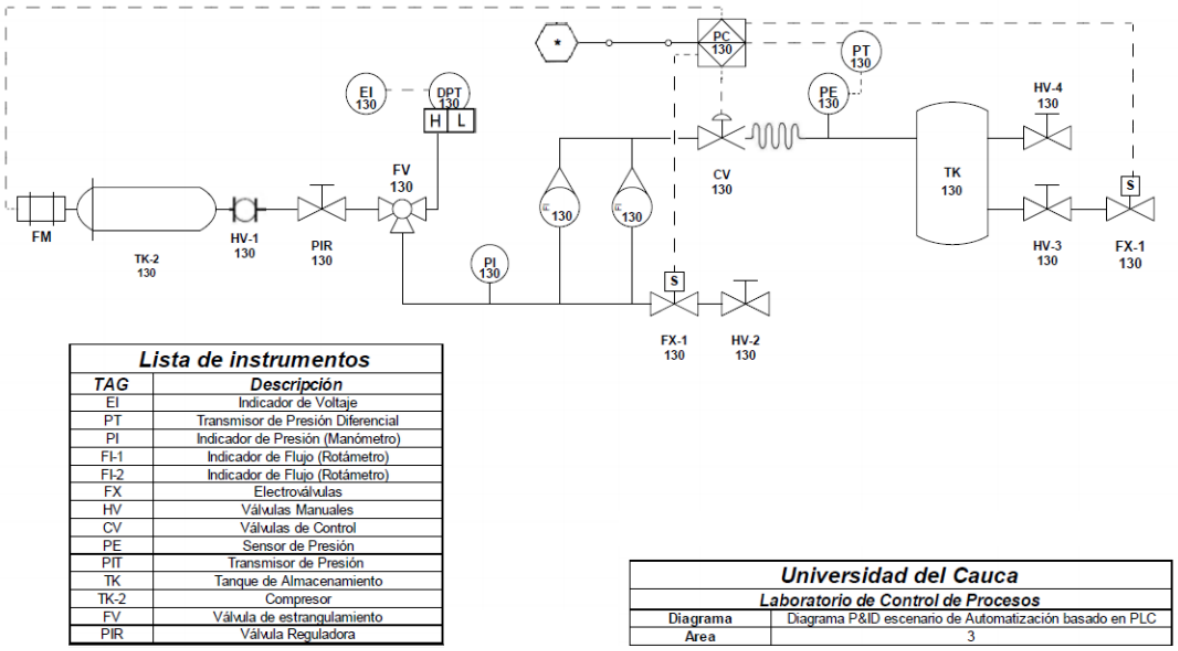
Los lineamientos de seguridad definidos en el capítulo 2 serán ejemplarizados en la planta de control de presión del laboratorio de control de procesos de la Universidad del Cauca. El presente capitulo busca informar al lector sobre la instrumentación, funcionamiento y características de dicha planta

La planta de presión es una planta académica concebida como un tanque de almacenamiento de aire a presión. Este tanque tiene una tubería de entrada y una tubería de salida. El flujo de aire siempre está en continuo movimiento. Tanto en la tubería de entrada como en la de salida, se encuentran válvulas manuales y una válvula de control. Con las válvulas manuales se puede inhabilitar la entrada o salida de aire del tanque y con la válvula de control se puede manipular el caudal de aire que ingresa o sale al tanque, según la tubería donde se instale. Las perturbaciones externas son dos: el caudal de entrada y el caudal de salida. Estas suceden cuando se presentan cambios no esperados en el caudal de aire suministrado al tanque y en el flujo demandado al tanque en el caudal de salida, respectivamente. En la imagen 3.1 se muestra la planta.

Imagen 3.1. Planta de control de presión

Entrando en detalles con la planta de presión y flujo de aire del laboratorio de control de procesos, se observa que la misma se encuentra organizada en dos paneles. El primero representa la planta ubicada en campo, mientras que el segundo es el panel donde se encuentran cableados los dos escenarios de automatización: Stand Alone y basado en PLC [12].

A continuación, en la figura3.1 se presenta el diagrama P&ID del proceso con el escenario de automatización basado en PLC:



Lista de instrumentos	
TAG	Descripción
EI	Indicador de Voltaje
PT	Transmisor de Presión Diferencial
PI	Indicador de Presión (Manómetro)
FI-1	Indicador de Flujo (Rotámetro)
FI-2	Indicador de Flujo (Rotámetro)
FX	Electroválvulas
HV	Válvulas Manuales
CV	Válvulas de Control
PE	Sensor de Presión
PIT	Transmisor de Presión
TK	Tanque de Almacenamiento
TK-2	Compresor
FV	Válvula de estrangulamiento
PIR	Válvula Reguladora

Universidad del Cauca	
Laboratorio de Control de Procesos	
Diagrama	Diagrama P&ID escenario de Automatización basado en PLC
Area	3

Figura 3.1. P&ID planta de control de presión

En el panel de campo (imagen 3.2) el proceso empieza con la activación del motor, el cual toma aire del ambiente y lo encierra a presión en el contenedor del compresor. Este aire viaja por una manguera que lo comunica con la tubería de la planta donde se ha instalado una válvula manual que permite su paso o no hacia los instrumentos. El aire proveniente del compresor tiene una presión aproximada de 80 psi, éste pasa por un filtro que se encarga de extraer las gotas de agua que se puedan producir en el interior de la tubería. Para obtener aire de instrumentos, el aire para por un primer regulador con su respectivo indicador que se encarga de disminuir la presión de 80 psi a 40 psi y una válvula de estrangulamiento que la reduce finalmente a 20 psi. Una de las salidas del último reductor va a un transmisor de presión diferencial ciego conectado a un voltímetro, como indicador, la otra salida va hacia un manómetro y de este a los dos rotámetros, en cuya parte

inferior se encuentra una electroválvula encargada de generar los disturbios. En la parte superior de los rotámetros, el aire se dirige a una servoválvula de control que es la encargada de manipular la cantidad de aire que entra o no al tanque, el aire que entra al tanque es medido por un sensor de placa de orificio el cual envía la señal de presión para posteriormente realizar el control. Finalmente el tanque tiene una salida que continuamente permite el paso de aire y otra salida que se activa como disturbio por medio de una electroválvula.

Imagen 3.2. Panel de Campo

En el panel de cableado (imagen 3.3) o control se implementa el cableado de los dos escenarios de automatización que dispone la planta: basado en PLC y Stand Alone. Toda la instrumentación que se encuentra en campo se reúne por medio de un sistema de borneras (JB - junction box) en campo y se llevan hasta el panel de control por medio de cables. En el panel de cableado otro grupo de borneras reciben las señales de campo y las envía hacia un bloque de relés electromecánicos quienes las distribuyen hacia los dos escenarios de automatización, según disponga la posición de una llave selectora que gobierna la activación de los relés. Los cables se instalan al interior de canaletas ranuradas distribuidas según se necesite en el panel de control.

Cuando la llave selectora indica Stand Alone, la servo-válvula y el transmisor-indicador de presión quedan conectados a un controlador industrial de proceso

Omron, mientras la instrumentación restante: circuito de mando del compresor y electroválvulas de disturbio quedan para activación manual desde pulsadores [12].

Cuando el control se realiza por medio del PLC, se utiliza el HMI mostrado en la imagen 3.4

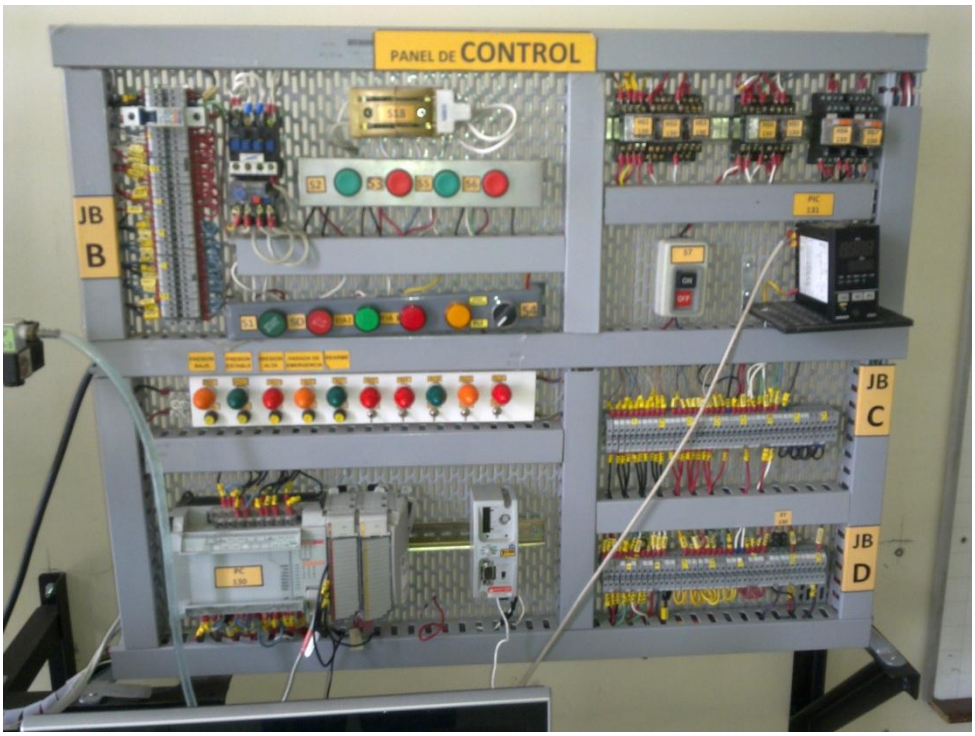


Imagen 3.3. Panel de Control

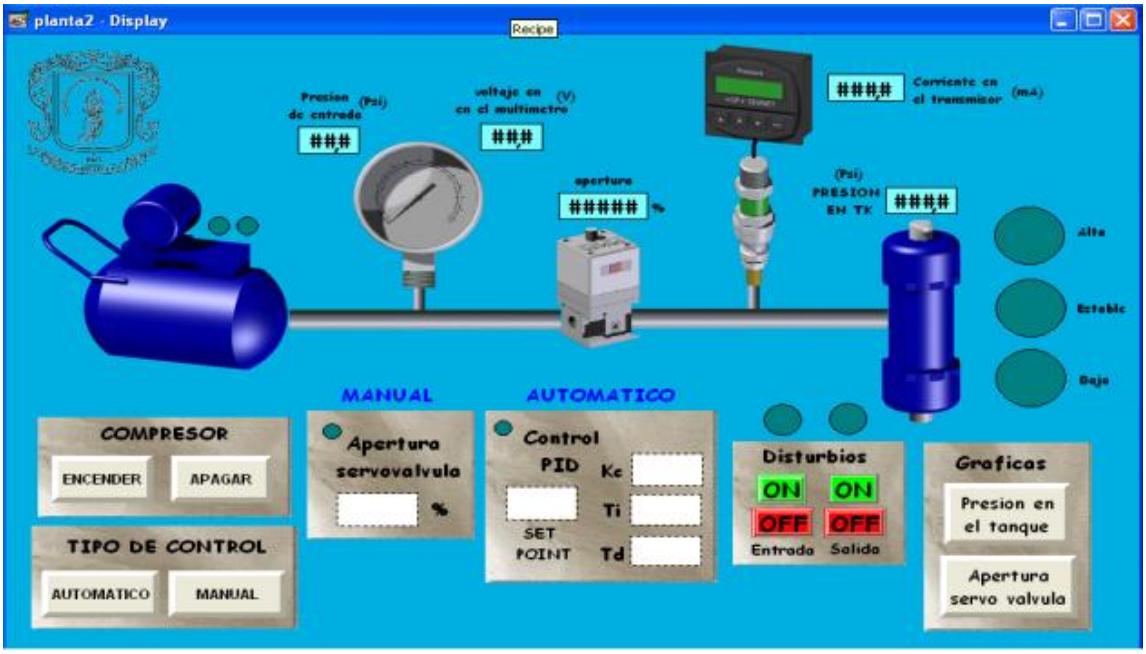


Imagen 3.4. HMI planta de control de presión

En el primer piso del edificio de la Facultad de Ingeniería Electrónica y Telecomunicaciones FIET, en el cuarto de la subestación eléctrica se encuentra el compresor que proporciona el aire a la planta con una presión determinada. La imagen 3.5 muestra la imagen de este.

Imagen 3.5. Compresor de aire

4. ESQUEMA DE SEGURIDAD CIBERNETICA PARA LA PLANTA DE CONTROL DE PRESION

A partir de los lineamientos de seguridad descritos anteriormente y del conocimiento de las necesidades puntuales del laboratorio que se esté trabajando, se debe seleccionar cuales de las dieciséis actividades aplican y cuales deben o pueden ser omitidas.

4.1. Actividades específicas para la planta de control de presión del laboratorio de control de procesos LCP.

En la tabla 4.1 se presentan las actividades que no se seleccionaron para el laboratorio de control de procesos de la FIET de la Universidad del Cauca:

Actividad	Justificación
2. Obtener apoyo, compromiso y financiación de los directivos	Esta actividad no es incluida dentro del esquema de seguridad a desarrollar puesto que al ser un trabajo de grado se da por cumplida en el momento en que la propuesta y el anteproyecto son aprobados, siguiendo el conducto regular por los directivos de la FIET, ya que en ellos se incluyen aspectos como presupuesto y se expone el caso de negocio.
9.Organizarse para la seguridad	Debido al alcance del esquema de seguridad, y la etapa en que se encuentra el proyecto, no es necesario llevar a cabo esta actividad. Una vez el acceso remoto al laboratorio sea habilitado y se implemente este esquema de seguridad las personas responsables de velar por su buen funcionamiento serán el laboratorista y los docentes involucrados
11. Proyección y priorización de los sistemas de control	En esta actividad, se define el riesgo asociado a cada uno de los sistemas de control, para establecer de qué manera van a ser orientados los esfuerzos de mitigación de riesgos. En el presente trabajo, únicamente se encuentra un sistema de control, la planta de control de presión, por tal motivo, no es necesario ningún tipo de priorización.

Tabla 4.1. Selección de actividades para el LCP

4.2. Ejemplarización del esquema de seguridad cibernética sobre la planta de control de presión del LCP

En este numeral se hace uso de la planta de control de presión para aplicar sobre esta los lineamientos de seguridad desarrollados en el capítulo 2. Es importante tener en cuenta que debido a las dos actividades no seleccionadas, la numeración original de los lineamientos de seguridad se ve alterada para este ejemplo.

4.2.1. Desarrollo de un caso de negocio

En el LCP (laboratorio de control de procesos) del DEIC de la Universidad del Cauca se quiere habilitar el acceso de manera remota a cada una de sus siete plantas con el fin de ampliar la capacidad del mismo en tiempo adicional en las horas de clase. Paralelo a este proyecto se está desarrollando un trabajo de grado titulado “Sistema de acceso remoto a través de internet a la planta sistema a eventos discretos (sed) del laboratorio de control de procesos (LCP) del programa de ingeniería en automática industrial (PIAI)” desarrollado por los estudiantes Jhessica Jaramillo Caicedo y Víctor Iván Joaqui Tandioy. En el cual el usuario accede desde internet al PLC de la planta a través de una interfaz montada en un servidor web que permite cambiar el estado de las variables sin necesidad de acceder ni manipular el código de programación. La solución es pensada de tal manera que el usuario, una vez tiene habilitado el acceso remoto a la planta, solo puede interactuar con esta por medio de la interfaz que se despliega.

Para garantizar el buen funcionamiento de la instrumentación, la correcta realización de las prácticas por parte del estudiante y la integridad de la infraestructura, es necesario tener toda una serie de medidas que aseguren los activos dentro del laboratorio.
Algunas de las consecuencias que pueden ocurrir cuando se implemente LCP remoto son:

- **Daño de los equipos**:
  Daño del PLC o de sus componentes como el relé interno que conmuta a la salida, suprimiendo su acción de control sobre la planta y permitiendo que las variables alcancen valores para los que no fue diseñado el sistema de control. Lo anterior también puede provocar daños o desajustes en la calibración de instrumentos, como el tanque de presión y el regulador electro-neumático, debido a que trabajan en un rango de 0-20 y de 0-25psi, respectivamente.

- **Perdida de información confidencial:**

  La encuesta de seguridad y delitos informáticos del CSI/FBI de 2003 indica que el robo de información exclusiva ha sido invariablemente la causa más común de pérdidas económicas desde 1999 [13].

  A nivel industrial, referirse a pérdida de información confidencial, hace alusión a casos como: publicación y modificación de bases de datos que contengan información sobre clientes y proveedores, pérdida de confidencialidad de los récipes de fabricación de los productos, pérdida de confianza de los consumidores por el uso ilícito de su información.

  Al referirse al caso académico del LCP, la información confidencial que puede ser vulnerada es la disposición física de las plantas y sus equipos en el laboratorio. De esta manera se facilita el robo de instrumentación por parte de personas ajenas. También, se incluye en este apartado, la modificación de las bases de datos, alteración de las contraseñas y adición o eliminación de personas con acceso al LCP.

- **Perdidas económicas**

  El mal funcionamiento de la instrumentación, los equipos de control, o del software existente en el LCP, pueden ser causantes de pérdidas económicas, sin embargo se deben tener en cuenta otros factores como: denegación del servicio haciendo que la inversión realizada para habilitar el acceso remoto al laboratorio se vea afectada por la incapacidad para utilizarlo.

De la misma manera, puede haber amenazas provenientes de fuentes diferentes como por ejemplo:

- **Intrusión de personas ajenas a las habilitadas para el uso remoto del LCP.**

  Robo de cuentas de usuarios. Debido a que el control de acceso al LCP debe contar con un administrador de cuentas, la intrusión de personas ajenas puede ocasionar suplantación de usuarios; como cuentas de estudiantes, docentes o administradores del LCP.

- **Mal manejo de los equipos e instrumentación por parte del estudiante.**

  La planta de control de presión trabaja con una presión de aire de 20 psi; el compresor que la alimenta lo entrega a 80 psi, para acondicionar

el aire a la presión requerida se utilizan dos válvulas reguladoras que la reducen a 40 y 20 psi respectivamente; dichos reductores de presión, son operados de forma manual, un cambio en la posición del vástago puede provocar daños o desajustes en la calibración de instrumentos, como el tanque de presión y el regulador electro-neumático, debido a que trabajan en un rango de 0-20 y de 0-25psi, respectivamente.

En el panel de campo la planta cuenta con un PLC, si a este se le envían órdenes de abrir y cerrar repetida y rápidamente cualquiera de las dos electroválvulas de la planta durante un tiempo prolongado, se exige un esfuerzo de control de alta frecuencia haciendo que el relé interno del PLC, que conmuta a la salida, se dañe.

- **Caída de la red, rompiendo la conexión cliente-servidor.**

La caída de la red se puede provocar por diferentes escenarios, dentro ellos están:

- Fallos en el servicio de energía tanto el en laboratorio como el sitio donde esté trabajando el usuario
- Caída del proxy, Gateway y/o enrutadores de la Universidad bien sea por daño, ataque o falta de energía
- Desconexión del medio de transmisión (cable par trenzado).
- Daño de la tarjeta de red.
- Falla en el proveedor de servicios de internet.

Además de presentarse situaciones como la perdida de paquetes de datos o un ancho de banda limitada que dificulte la correcta comunicación.

- **Propagación de virus y gusanos**

Al ser un servicio de uso público para la comunidad del DEIC, la aparición de virus y gusanos es una amenaza potencial debido al amplio número de computadores que pueden conectarse con el servidor y la cantidad de dispositivos de almacenamiento masivo que se utilizan; habilitando un camino para la propagación en los sistemas de control del laboratorio.

Anteriormente, a nivel mundial las redes industriales tenían características definidas por el fabricante proveedor del sistema de control logrando sistemas aislados de la TI. Las amenazas de virus y gusanos han ido en aumento debido a que en la actualidad la tendencia es implementar estándares de

comunicación como Ethernet introduciendo en los sistemas de control y manufactura vulnerabilidades propias de las IT.

El caso más reciente y de mayor impacto es Stuxnet, un gusano informático que apunta a los sistemas industriales de control que se utilizan para controlar instalaciones industriales como plantas de energía eléctrica, represas, sistemas de procesamiento de desechos entre otras operaciones industriales. Stuxnet busca sistemas de control industriales y luego modifica el código en ellos para permitir que los atacantes tomen control de los sistemas sin que los operadores lo noten. En otras palabras, esta amenaza está diseñada para permitir a los hackers manipular equipamiento físico, lo cual lo hace extremadamente peligroso [14].

Cabe aclarar que en el caso del LCP remoto no se contempla la posibilidad de ser afectado por un gusano como Stuxnet, sin embargo no está exento de este tipo de ataques y debe ser protegido.

Los esfuerzos más comunes por parte de quienes han implantado laboratorios académicos de control remoto son dos principalmente. El primero es contar con un control de acceso en donde administran las cuentas de usuario y los horarios de trabajo. El segundo es la utilización de firewall (cortafuego), para restringir el flujo de información a través de la red.

Teniendo en cuenta las amenazas y consecuencias que genera habilitar el acceso remoto al LCP, es necesario el planteamiento de un esquema de seguridad que contenga medidas más allá de un control de acceso y un cortafuego.

4.2.2. Definición del marco y alcance de seguridad para el sistema de control y manufactura

El esquema de seguridad que se planteará en este trabajo tiene como objetivo sentar las bases teóricas para asegurar cibernéticamente los niveles 0, 1 y 2 de la planta de control de presión, el cual será utilizado una vez haya sido habilitado el acceso remoto al LCP. Para el planteamiento del esquema se contará con un tiempo aproximado de nueve meses.

El esquema de seguridad está dirigido a la planta de control de presión (los paneles de control y campo están ubicados en el laboratorio de control de procesos y el compresor que alimenta el suministro de aire en el primer piso del edificio de la FIET) perteneciente al DEIC de la Universidad del Cauca,

debido a la pequeña escala del proyecto, este es el único departamento involucrado con esta primera ejemplarización.

La planta de control de presión es utilizada principalmente por estudiantes de Ingeniería en Automática Industrial que cursan las siguientes materias: Instrumentación industrial, Laboratorio de control de procesos, Software para aplicaciones industriales II, redes y sistemas computarizados de control además de ser empleada en proyectos de trabajo de grado.
Aunque se cuenta con el apoyo de los docentes del DEIC, las personas responsables del desarrollo y cumplimiento del proyecto son los autores del documento.

Lo que se busca con este trabajo es permitir a los estudiantes de Ingeniería en Automática Industrial de la Universidad del Cauca acceder de forma segura a la planta de control de presión de manera remota.

El alcance del esquema de seguridad abarca aspectos de arquitectura tales como:

- SCADA de la planta de control de presión.
- Red LAN de la Universidad.
- Internet
- PC con conexión al PLC y a la red Ethernet
- Los dispositivos utilizados para conectarse a Internet.

Actualmente la División de Tecnologías de Información y Comunicación de la Universidad del Cauca, en cabeza del Ingeniero Giovanni Andrés de los Reyes se encuentra implementando la serie del estándar ISO 27000, la cual abarca aspectos como: requisitos del sistema de gestión de seguridad de la información y directrices para la gestión del riesgo en la seguridad de la información, entre otros [15].

En la definición del marco y alcance del proyecto es necesario contar con una estimación del presupuesto y recursos necesarios para éste fin. Esta información se encuentra detallada en la Tabla 4.2

RUBROS	**FUENTES**		**TOTAL($)**
	ESTUDIANTES($)	**DEPARTAMENTO($)**	
Personal	19`720.800	1.643.400	21.364.200
Hardware	0	680.712	680.712

Software	0	0	0
Varios	440.000	0	440.000
Comunicaciones	0	429.698	429.698
AUI	0	4.296.982	4.296.982
Total	20.160.800	7.040.392	27.201.192

Tabla 4.2. Presupuesto del trabajo

Los gastos correspondientes a la Universidad del Cauca, serán asumidos por el Departamento de Electrónica Instrumentación y Control (DEIC). Los gastos restantes serán asumidos por los desarrolladores del proyecto.

4.2.3. Formación de un equipo con las partes interesadas

El equipo formado para desarrollar el proyecto lo integran:

Los estudiantes de X semestre de Ingeniería en Automática Industrial

- Laura Marcela Segura Rosas
- Pablo Alejandro Pantoja Otero
- Victor Ivan Joaqui Tandioy
- Jhessica Jaramillo Caicedo

Además se cuenta con la ayuda en temas de control e instrumentación con los docentes

- Ing. Diego Alfonso Aguilar Cardona
- Ing. Vladimir Trujillo Arias

En lo concerniente a seguridad informática aplicada en las TI está presente:

- Ing. Siler Amador Donado

La persona responsable del funcionamiento, operación y gestión del esquema de seguridad una vez este implementado, es la misma que atiende las necesidades del LCP, es decir el laboratorista

4.2.4. Aumento de la capacidad del personal de seguridad a través de la formación

Para la fase PLANEAR las personas pertenecientes al equipo de partes interesadas se documentan sobre el funcionamiento de la planta de control de presión y las redes de la Universidad del Cauca, esto último con la colaboración de personal del área de Contacto 55 como los ingenieros Fabián Mera y Jaime Martínez. Para comprender el estándar ISA-99 se emplearon

artículos sobre ésta disponibles en la página web de ISA [16][17][18[19][20][21][22] y documentación sobre laboratorios remotos desarrollados en universidades de diferentes países[23][24][25][26][27][28][29][30][31].

Además, la socialización del esquema con la comunidad estudiantil se hace a través del artículo de divulgación del trabajo de grado, la monografía y la sustentación final para informar sobre las necesidades y cambios que deben ser incorporados en la planta de control de presión.

En la fase HACER, cuando el laboratorio con acceso remoto sea puesto en marcha, se recomienda que los administradores del laboratorio, reciban capacitación de la mano de quienes implementan el esquema de seguridad en éste. De igual forma, cuando el esquema de seguridad sea implementado sobre la planta de control de presión en trabajos futuros, se generarán cambios en ella y en la forma de realizar las distintas prácticas. Para familiarizar y formar a la comunidad estudiantil sobre dichos cambios, se adicionará la información necesaria en las guías del laboratorio.

4.2.5. Identificación de los riesgos clave del sistema de control y manufactura

De acuerdo con las fases mencionadas, el esquema de seguridad que se propone se encuentra en *Ingeniería básica o definición del diseño*. En esta fase, si la información disponible lo permite, se debe realizar un análisis más profundo de aquellos escenarios de accidentes cuyo peligro percibido es alto. También cobran importancia las alternativas planteadas para eliminar o controlar los peligros identificados en las fases anteriores.

La característica del problema a analizar consiste en que es un proceso productivo controlado de manera remota, las técnicas PHA cualitativas como HAZOP o FMEA realizan un estudio minucioso, sin embargo sus resultados se limitan a los riesgos presentes en el proceso productivo, excluyendo además los riesgos por errores humanos. Es claro que aunque se dispone de la información necesaria para realizar estas técnicas, los resultados que se obtienen no son suficientes para el logro de la actividad.

De acuerdo a lo anterior se decide seleccionar la técnica PrHA-Preliminary Hazard Analisys (Análisis preliminar de riesgo). Esta técnica, busca los resultados (1), (3) y (5) referenciados en *“2.6. Identificación de los riesgos clave del sistema de control y manufactura”*, motivos por los cuales se hace la

actividad (*4.2.5 Identificación de los riesgos claves del sistema de control y manufactura*). Esta técnica es recomendada para proyectos nuevos en donde no se cuenta con información previa o historial sobre acontecimientos pasados, sirviendo como base para estudios más detallados ya que identifica las áreas de peligro que deben evaluarse de forma más específica cuando se disponga de más información.

Una vez elegida la técnica que se va a utilizar y de acuerdo a la información obtenida en las actividades anteriores, los riesgos identificados por el equipo de partes interesadas son:

- Presión de aire de entrada a la planta > 20 psi.
- Control de acceso débil.
- Ausencia de controles para garantizar la correcta realización de las prácticas de laboratorio.
- Planta en operación de manera remota, sin supervisión.
- Falta de programación de cronogramas de trabajo
- Desconocimiento del estado en que se encuentra la planta.

Se consideró como riesgo importante el acceso remoto, por parte del usuario, al código de programación del PLC, sin embargo en el proyecto “Sistema de acceso remoto a través de internet a la planta sistema a eventos discretos (sed) del laboratorio de control de procesos (LCP) del programa de ingeniería en automática industrial (PIAI)” que se desarrolla paralelo a este proyecto, se definió que el sistema de acceso remoto permite manipular los estados de las variables de control, sin tener acceso alguno al código de programación.

4.2.6. Priorización y calibración de los riesgos

En la actividad *“4.2.5. Identificación de los riesgos clave del sistema de control y manufactura”* se identificaron los riesgos a trabajar y se definió la técnica PrHA con lo cual se hará el análisis de riesgo cuyo resultadlo permitirá priorizarlos. De acuerdo con las tablas 4.3, 4.4 y 4.5 presentadas a continuación se realiza en análisis preliminar de riesgos consignado en la tabla 4.6.

Descripción	Categoría	Definición
Catastrófica	I	Perdidas de muertos o sistemas
Crítica	II	Heridas severas, daño severo al sistema
Marginal	III	Heridas menores, daños menores al sistema
Despreciable	IV	Menos que heridas menores o daño al sistema

Tabla 4.3. Niveles de severidad de la norma MIL-STD-882B.

Descripción	Nivel	Especificaciones individuales
Frecuente	A	Probable de ocurrir frecuentemente
Probable	B	Ocurre varias veces en la vida del equipo
Ocasional	C	Probable que ocurra alguna vez en la vida del equipo
Remota	D	Improbable, pero posible que ocurra
Improbable	E	Tan improbable que ocurra, que es imposible

Tabla 4.4. Niveles de probabilidad de la norma MIL-STD-882B.

PROBABILIDAD	CLASES DE RIESGOS			
	CONSECUENCIA CATASTROFICA	CONSECUENCIA CRITICA	CONSECUENCIA MARGINAL	CONSECUENCIA DESPRECIABLE
Frecuente	I	I	I	II
Probable	I	I	II	II
Ocasional	I	II	II	II
Remoto	II	II	II	III
Improbable	II	III	III	III

Tabla 4.5. Matriz de clasificación de riesgos

Análisis preliminar de riesgos (APR)									
Universidad del Cauca									Fecha: 31-08-2012
Laboratorio de control de procesos con acceso remoto									Planta de control de presión
Vulnerabilidad	Amenaza	Barreras de protección	Tipos de efecto	Consecuencia	Prob.	Sev.	Riesgo	No de escenario de amenaza	Recomendaciones/ Sugerencias
Presión de aire de entrada a la planta > 20 psi	Apertura de cualquiera de los dos reguladores manuales de presión	NA	Impactos operacionales	Daño o des calibración de la instrumentación	D	II	II	1	Proteger los dos reguladores por medio de una caja sellada del cual solo tiene llave el laboratorista
Control de acceso débil	Intrusión en la cuenta de usuario del docente o del estudiante	NA	Impacto social	Uso inadecuado de la planta	A	II	I	2	Preguntas personales para permitir el acceso y utilizar SSL para encriptar los datos.
	SQL Injection	NA							Incluir código de seguridad en la programación de la base de datos.
Ausencia de controles para garantizar la correcta realización de las prácticas de laboratorio	Caso omiso a las guías de laboratorio diseñadas para cada practica	NA	Impacto Operacional	Daño de la instrumentación de la planta y de los equipos del laboratorio	B	III	II	3	Sanción por incumplimiento de políticas de seguridad
Planta en operación, de manera remota, sin supervisión	Estudiante	NA	Impacto operacional	Aprovechamiento incorrecto de los recursos del LCP	B	II	I	4	Llevar un registro de eventos importantes ocurridos durante la práctica.
Falta de programación de cronogramas de trabajo	Dos o más usuarios con acceso a la planta simultáneamente	NA	Impacto Operacional		A	IV	II	5	Definición de horarios de disponibilidad de la planta para trabajos remotos y locales

Desconocimiento del estado en que se encuentra la planta	(local-remoto, remoto-remoto)	NA							Implantar instrumentos de visualización que indiquen de qué manera está siendo operada la planta

Tabla 4.6. Análisis preliminar de riesgos

Uno de los objetivos de la presente actividad, es tener priorizados los riesgos para conocer de qué manera se deben orientar los esfuerzos para la mitigación del riesgo. Como “control de acceso débil” y “planta en operación de manera remota sin supervisión” tienen nivel de riesgo “I”, es necesario utilizar criterios adicionales para priorizarlos correctamente.

Teniendo en cuenta el significado de disponibilidad (acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran), confidencialidad (acceso a la información únicamente por personas que cuenten con la debida autorización), integridad (en este caso incluye la integridad de los datos: propiedad que busca mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados e integridad mecánica: tiene por objeto garantizar que todo equipo de proceso sea diseñado, instalado, operado, inspeccionado, mantenido y/o remplazado oportunamente para prevenir fallas, accidentes o potenciales riesgos a personas, instalaciones y al ambiente [32]), y las condiciones del laboratorio descritas anteriormente, se propone una escala de 0 a 100% donde se define el nivel de importancia de dichos criterios para el laboratorio.

Con el fin de obtener dicho nivel, se realizó una encuesta a los docentes cuya materia está relacionada con el LCP. El documento de la encuesta se encuentra en el anexo B. Los porcentajes que asignaron cada uno de los docentes son ponderados y el resultado arrojado se presenta en la tabla 4.7:

Integridad	Al ser un LCP con acceso remoto es de suma importancia que la información suministrada y recibida por el usuario sea confiable, y también que los equipos e instrumentación sean instalados y operados de manera que permitan una ejecución remota segura ya que los horarios de trabajo incluyen horas no laborales, impidiendo alguna intervención humana en caso de fallo. Con base en lo anterior el equipo de partes interesadas concertó en definir que la disponibilidad aporta en un 52% en la seguridad del LCP.
Disponibilidad	Contrario al sector industrial en donde la disponibilidad de los sistemas de control debe ser 24x7, el LCP funciona en un entorno académico para un programa presencial donde la disponibilidad debe estar sujeta al uso local por parte de los estudiantes. Por otro lado, existe la posibilidad de que se presenten casos en los que la red de la universidad no esté disponible o se caiga, lo cual no representa en sí un problema critico puesto que no se está hablando de un servicio a una empresa o negocio. Con base en lo anterior el equipo de partes interesadas concertó en definir que la disponibilidad aporta en un 30% en la seguridad del LCP.

Confidencialidad	El LCP es una herramienta académica que busca fortalecer el conocimiento en sistemas de control, por tal razón el esquema de seguridad debe ser pensado de tal manera que permita compartir la mayor cantidad de información sobre el proceso sin llegar a comprometer su integridad. Con base en lo anterior el equipo de partes interesadas concertó en definir que la confidencialidad aporta en un 18% en la seguridad del LCP.

Tabla 4.7. Nivel de importancia de los criterios de seguridad cibernética para el LCP

El siguiente paso consiste en puntuar (de 0 a 10) que tanto afecta cada uno de los riesgos identificados a la *Integridad, Disponibilidad y confidencialidad* del LCP. Finalmente se multiplica el valor de la calificación con el porcentaje establecido para los tres criterios por el equipo de partes interesadas. Y con este valor se priorizan los riesgos organizándolos de mayor a menor, siendo 1 el valor más bajo y 10 el valor más alto. El resultado se presenta en la tabla 4.8

Riesgo	Integridad %	Disponibilidad %	Confidencialidad %	Puntuación
1	10	7	0	73
2	10	0	10	70
3	8	0	0	41
4	6	0	0	32
5	3	10	0	45

Tabla 4.8. Priorización de riesgos

4.2.7. Establecimiento de políticas de seguridad

De acuerdo con los riesgos identificados y priorizados por el equipo de partes interesadas, encargado del esquema de seguridad, se define un conjunto de reglas que describen qué acciones deben ser tomadas para manejar dichos riesgos en particular y qué sistemas y unidades organizativas están sujetas a estos requerimientos. Este conjunto de reglas llamado políticas que se presenta a continuación representa el compromiso que tiene el equipo de partes interesadas con la seguridad cibernética durante las prácticas remotas en el laboratorio.

Para su publicación y divulgación primero deben ser aprobadas por el DEIC y las directivas de la facultad. De ser aprobadas, entraran en vigencia a partir del momento en que se habilite el acceso remoto al laboratorio y se implemente el esquema de seguridad.

POLITICAS PARA EL USO ADECUADO DE LA PLANTA

- Las guías diseñadas para desarrollar las prácticas de laboratorio sobre la planta de control de presión deben ser seguidas rigurosamente por parte del estudiante.
- Los recursos del laboratorio han sido dispuestos con fines académicos, por tal motivo el estudiante debe hacer un uso responsable de cada uno de ellos.
- El reconocimiento de la planta de manera presencial por parte del estudiante es un requisito para poder realizar prácticas de manera remota y/o local.
- El laboratorio de control de procesos cuenta con una aplicación para programar el horario y fecha en que el estudiante realizará las prácticas de manera remota. Es responsabilidad del estudiante reservar su turno con veinte minutos de antelación.
- Las condiciones con que el estudiante recibe y entrega la planta deben ser las mismas (estado de los instrumentos, configuración de los equipos, etc.)
- La única persona autorizada para hacer cambios, mejoras o actualizaciones a la planta es el laboratorista.
- La única persona que puede abrir la caja de seguridad y manipular las dos válvulas de presión a la entrada de la planta de control de presión es el laboratorista, este último debe revisar periódicamente que la planta esté siendo alimentada con aire a 20 psi de presión.
- La distribución de los equipos, instrumentos, y demás recursos del laboratorio deben mantenerse como lo instaure la persona encargada del laboratorio.
- El acceso remoto a la planta debe tener única y exclusivamente fines académicos establecidos por el docente que dicta la materia cursada por el estudiante
- El uso inmediato de la planta sin necesidad de hacer reservación se puede hacer únicamente de manera local, verificando previamente que los instrumentos de visualización indiquen que no está siendo utilizada de manera remota.
- El estudiante debe cerrar su sesión de usuario al terminar la práctica remota

POLITICAS DE CONTROL DE ACCESO

- La persona autorizada para realizar prácticas remotas cuenta con un nombre de usuario y contraseña para acceder al laboratorio remoto. Este nombre de usuario y contraseña son personales e intransferibles.
- La única persona autorizada para cambiar la lista de usuarios habilitados para acceder remotamente al laboratorio es el docente, a través de su cuenta con privilegios.
- Las únicas personas que deben ser habilitadas para acceder remotamente al laboratorio son aquellas que aparecen matriculadas en la materia que hace uso del laboratorio remoto.
- Para reservar localmente la planta de presión se debe dirigir al laboratorista quien es el encargado de realizar dicha operación.

El incumplimiento de estas políticas ocasionara la suspensión del servicio del acceso remoto al estudiante por un tiempo determinado (definido por el docente) dependiendo de la gravedad de la falta. En el caso del laboratorista las medidas a tomar serán definidas por su jefe inmediato.

4.2.8. Inventario de los dispositivos y redes de la planta de control de presión.

Los dispositivos de control y manufactura de la planta de control de presión están ubicados en el LCP a excepción del compresor de aire ubicado en el cuarto de la subestación de voltaje de la FIET. En la tabla 4.9 se consignaron los dispositivos y redes de la planta de presión y algunos datos sobre los mismos.

Instrumento	Variable de proceso	Rango de trabajo	Señal de entrada	Señal de salida	Ubicación
Sensor de presión	Presión	0-17 bar 0-250 psi	Aire a presión	Voltaje	Panel de campo
Válvula manual de perilla redonda	Caudal de aire	0-100%	Aire a presión	Aire a presión	Panel de campo
PLC Micrologix 1500 serie c	Presión y caudal de aire	0-120 AC – 24VDC	Fuente de poder de 100- 240 VAC/ 50-60 Hz/12 entradas 120 VAC/4-20 mA	12 Salidas de relé a 24 VDC	Panel de control
Botonera	No aplica	No aplica	No aplica	No aplica	Panel de control
Medidor de voltaje	Presión del transmisor ciego	1 – 5V	1 – 5V	Indicador de voltaje	Panel de campo

Válvula manual de vástago recto	Flujo de aire	0 – 100%	Caudal de aire	Caudal de aire	Panel de campo
Relé electromecánico	No aplica	5 – 200 VDC	Voltaje	Estado del relé	Panel de control
Servovalvula	Flujo de aire	0.5-10 Kg-f/cm^2	0 – 10V	Porcentaje de posición	Panel de campo
Tanque de presión	Presión	0 – 25 psig	0.7 – 20 psig	0.7 – 20 psig	Panel de campo
Manómetro	Presión	0 – 160 psi	0 – 20 psi	0 – 20 psi	Panel de campo
Controlador digital Omron ESEK	Presión	No aplica	4 - 20 mA, 0 - 12 mA/ 1 - 5V, 0 - 5 V, 0 - 10 V	4 - 20 mA, 0 - 20 mA/ 0 - 10 VDC	Panel de control
Sensor y transmisor ciego de presión Honeywell ST3000	Presión	0 – 25 psi	Diferencial de presión	4 - 20 mA	Panel de campo
Regulador electro neumático	Flujo de aire	0 – 25 psig	0 - 10Vcc,0 - 5Vcc / 4 - 20mAcc,0 - 20mAcc	0.7 - 70PSI, 1 – 5Vcc	Panel de campo
Válvula manual de bola	Presión	0 – 600 psig	0 – 25 psi	Paso o no de aire	Panel de campo
Rotámetro	Caudal de aire	0 – 200 ft^3/min	Caudal de aire	Posición del indicador de 0 - 0.2 ft3/m fluid=nitrógeno	Panel de campo
Transmisor de presión GF+Signet 8450	Presión	0 – 25 psi	4 – 20 mA	4 – 20 mA	Panel de campo
Compresor de aire	Presión de aire	110/220 VAC 8.4-4.3 a 60HZ	110/220 VAC	Aire comprimido 80 psi	Subestación eléctrica primer piso edificio FIET
Módulo de comunicación DH 485					Panel de control
Llave selectora	No aplica	No aplica	No aplica	No aplica	Panel de control
Filtro de aire	No aplica	No aplica	No aplica	No aplica	Panel de campo
Reductor de presión	No aplica	No aplica	No aplica	No aplica	Panel de campo
Válvula de estrangulamiento	No aplica	No aplica	No aplica	No aplica	Panel de campo
Switch	No aplica	No aplica	No aplica	No aplica	Panel de campo
Contactor lc1d1810	No aplica	No aplica	No aplica	No aplica	Panel de control
Relé térmicolr2d1312	No aplica	5.5 a 8A	Voltaje	Estado del relé	Panel de control
Cuchilla	No aplica	No aplica	No aplica	No aplica	Panel de control

Pulsadores	No aplica	No aplica	No aplica	No aplica	Panel de control
Luces piloto	No aplica	No aplica	No aplica	No aplica	Panel de control
HMI	No aplica	No aplica	No aplica	No aplica	PC
PC	No aplica	No aplica	No aplica	No aplica	Lugar de trabajo del estudiante, perteneciente a la planta de control de presión
Código de programación del PLC	No aplica	No aplica	No aplica	No aplica	PLC

Tabla 4.9. Inventario planta de control de presión

Sin embargo no todos los dispositivos listados anteriormente se consideran activos críticos, ya que la planta de control de presión con acceso remoto puede funcionar sin su presencia. Para definir la criticidad de los activos (en cuanto al funcionamiento físico de la planta) se utilizó un diagrama de flujo de las dos prácticas de laboratorio que se realizan en la planta de control de presión (identificación y sintonización del PID) que utilizarían el acceso remoto, presentado en la figura 4.1.

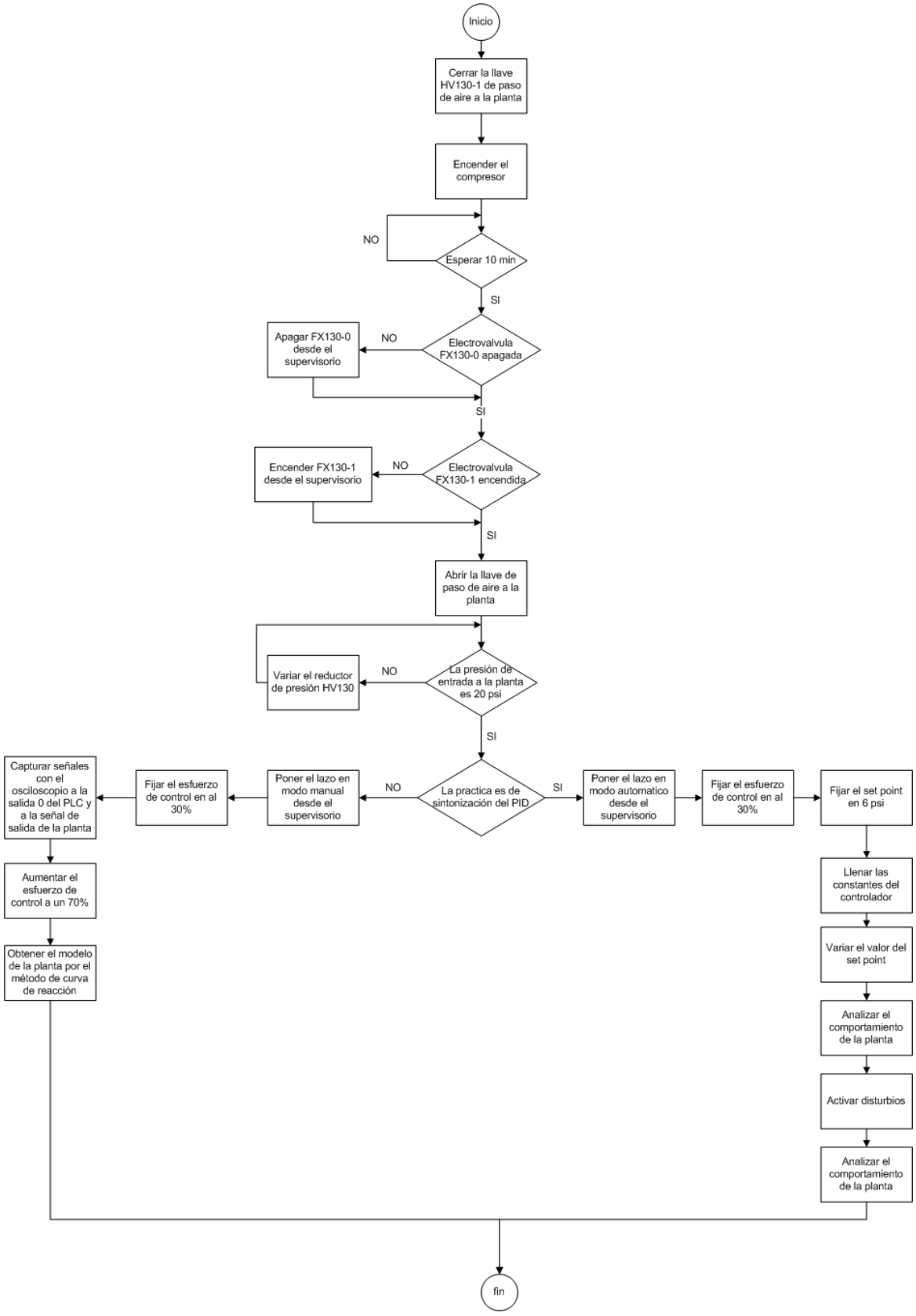


Figura 4.1. Diagrama de flujo de las prácticas en la planta de control de presión

De acuerdo con el diagrama de flujo se definen los siguientes activos críticos:

- Compresor de Aire (TK 2)
- Llave de entrada de aire a la planta (HV130-1)
- Tanque de almacenamiento de aire (TK 130)
- Sensor y transmisor ciego de presión diferencial (PT 130)
- Sensor de presión (PE 130)
- Transmisor de presión (PIT130)
- Servovalvula (FX 130-0)
- Electrovalvulas para activar disturbios (FX 130-1 y FX 130-2)
- Reductor de presión (HV 130)
- PLC Micrologix 1500 serie C Allen Bradley (PC 130)
- Información Cliente-Servidor

Por otro lado, el acceso remoto vía web, se está desarrollando en el trabajo de grado “Sistema de acceso remoto a través de internet a la planta sistema a eventos discretos (sed) del laboratorio de control de procesos (LCP) del programa de ingeniería en automática industrial (PIAI)” por medio de un servidor OPC, un servidor Web y un HMI. Por tal motivo estas tres herramientas son incluidas dentro de la lista de activos críticos para las prácticas remotas.

Diagrama de redes del LCP

El inventario realizado anteriormente incluye los instrumentos existentes en la planta de control de presión necesarios para hacer prácticas de laboratorio en dos escenarios de automatización (basado en PLC o Stand Alone). En el caso del escenario Stand Alone algunos instrumentos deben ser activados de manera manual, como es el caso de los disturbios a la entrada y salida del tanque que deben ser activados por medio de pulsadores. Esta condición limita la capacidad del laboratorio remoto, por lo cual se descarta este escenario y el esquema de seguridad que se propone está dirigido al escenario basado en PLC.

De la misma manera se incluyen los equipos necesarios para llevar la información del servidor del LCP a internet. Este diagrama se muestra en la figura 4.2.

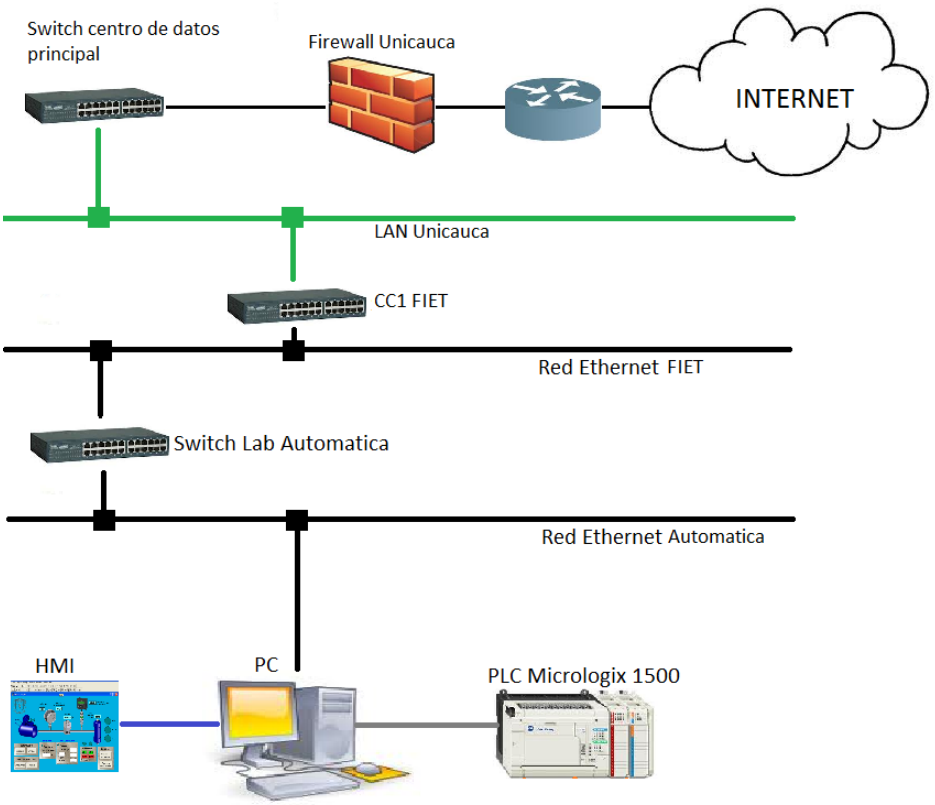


Figura 4.2. Diagrama de redes de la planta de control de presión

4.2.9. Desarrollo de una evaluación detallada de seguridad.

En los lineamientos de seguridad se mencionan diferentes técnicas y software para el análisis de riesgos. Debido a que en *"4.2.6 Priorización y calibración de riesgos"* se utilizó la técnica PrHA, en esta actividad se continúa con su utilización para que los resultados finales sean basados en los mismos criterios y no se genere ningún tipo de conflictos por utilizar técnicas o software diferentes.

A Partir de los activos listados en *"4.2.8. Inventario de dispositivos y redes de la planta de control de presión"* se procede a identificar los riesgos particulares a cada uno de ellos, estos eran mostrados en la tabla 4.10:

Análisis preliminar de riesgos PrHA										
Universidad del Cauca									Fecha: 11-02-2013	
Laboratorio de control de procesos con acceso remoto									Planta de control de presión	
Activo	Vulnerabilidad	Amenaza	Barreras de protección	Tipos de efecto	Consecuencia	Prob.	Sev.	Riesgo	No. de escenario de amenaza	Recomendaciones/ Sugerencias
Compresor TK2	Ausencia de control de presión en el compresor de aire	Exceso de presión de aire	Breaker de 120V de la planta de control de presión	Impacto operacional	Daño del motor del compresor	A	II	I	6	Remplazar el compresor existente por uno nuevo Implantar un circuito de protección de presión en el compresor que lo apague cuando alcance su máxima capacidad
PLC Micrologix 1500serie C Allen Bradley (PC130)	Ausencia de protección contra picos de voltaje	Altos voltajes en la red de energía	Subestación de energía para el edificio de la FIET	Impacto operacional	Daño de equipos	D	II	II	8	UPS
NA	Mala instalación o ausencia de dispositivos de comunicación o instrumentos	Empleado	NA	Impacto operacional	Planta fuera de servicio	C	IV	II	9	Creación de políticas de mantenimiento de la planta
NA	PC que trabaja como servidor es utilizado también para las practicas presenciales o es de dominio publico	Estudiante	Antivirus	Impacto operacional	Alteración del código de programación para el uso remoto del PLC Denegación del servicio (DoS) Introducción de código malicioso	A	II	I	10	Equipo dedicado a los servidores al cual solo tenga acceso el administrador

					Daño o eliminación total/ parcial intencional de software					
NA	Ausencia de un número máximo de intentos para acceder a una cuenta	Robot	NA	Impacto operacional	Personal no autorizado tenga acceso al LCP con acceso remoto	C	II	II	11	Utilización de captcha
INFORMACION CLIENTE-SERVIDOR	Comunicación a través de internet	Hacker	Firewall	Impacto operacional	Robo o uso inadecuado de información	C	II	II	12	VPN
					Denegación de servicio DoS					Nuevo Firewall

Tabla 4.10. Análisis preliminar de riesgos detallado

Los dos reductores de presión representan un riesgo para la planta, pero el tratamiento de los mismos fue desarrollado en el primer análisis. Por tal razón no se tienen en cuenta en esta etapa.

De la misma manera como se hizo en la actividad *"4.2.6 Priorización y calibración de riesgos"* se utiliza la tabla 4.11 como una herramienta adicional para la priorización de los riesgos.

Escenario de amenaza	Integridad %	Disponibilidad %	Confidencialidad %	Porcentaje de afectación seguridad
6	10	8	0	76
7	7	9	0	63
8	10	0	0	52
9	0	8	0	24
10	8	8	8	80
11	2	5	10	43
12	0	10	10	48

Tabla 4.11. Priorización detallada de riesgos

4.2.10. Desarrollo de políticas detalladas de seguridad cibernética para el sistema de control

A partir de los nuevos riesgos identificados en la actividad anterior, se complementa la lista de políticas establecida en la actividad *"4.2.7. Establecimiento de políticas de seguridad"* siguiendo los parámetros para redacción de políticas de la actividad *"2.8.Establecimiento de políticas de seguridad".*

POLITICAS PARA EL USO ADECUADO DE LA PLANTA

- El estudiante y/o laboratorista no debe interactuar con la válvula manual de salida del tanque TK130, ésta debe permanecer abierta.
- El laboratorista, al terminar su horario laboral, debe asegurarse que el paso de aire del compresor este dirigido hacia la planta de control de presión.
- El estudiante al realizar una práctica de manera presencial debe verificar que el suministro de aire no esté siendo utilizado por la planta de clasificación.
- El mantenimiento de la planta de control de presión debe realizarse según un cronograma establecido con anticipación, y su instrumentación y dispositivos no pueden ser cambiados ni removidos en horarios diferentes a los establecidos en el mismo.

- El laboratorista es la única persona autorizada para manipular el software para el acceso remoto (código de programación, interfaz gráfica o servidores).
- Los turnos de trabajo asignados para las prácticas remotas en la planta de control de presión no deben coincidir con los asignados para trabajar en la planta de visión de máquina.
- El compresor de aire debe recibir mantenimiento preventivo periódico revisando el nivel de aceite drenando el líquido acumulado en el tanque, inspeccionando y limpiando el filtro de aire y revisando la válvula de seguridad por sobrepresión con el fin de mantener y/o alargar la vida útil del compresor.
- El laboratorista debe realizar periódicamente backups del servidor Web y OPC, así como tener en un disco duro de máquina virtual estos dos servidores para ser montados en otro equipo en caso de emergencia.

4.2.11. Definición de controles estándar de mitigación de riesgos.

La información obtenida hasta el momento contempla los riesgos operativos implicados en el laboratorio con acceso remoto. Es necesario que la decisión que se tome sobre qué tipo de control de mitigación (reducir, evitar, transferir o retener el riesgo) utilizar en cada riesgo, esto se hace teniendo en cuenta la relación entre los costos que genera el riesgo y su solución.

El presente trabajo analiza la parte funcional pero no se cuenta con la información financiera y de presupuesto que maneja la facultad. Para dicha decisión se recomienda tener en cuenta además del aspecto financiero, el nivel de importancia de los criterios de seguridad cibernética para el LCP (tabla 12) y la priorización de los riesgos presentados en las tablas 13 y 16.
Es por ello que se proponen las siguientes recomendaciones como medidas de control pero deben ser evaluadas por las partes administrativas encargadas.

Transferir no es una opción porque no hay terceras partes involucradas en el laboratorio. No podemos tomar decisión sobre *retener* el riesgo debido a que se necesita información financiera para tomarla.

Las opciones que se escogieron teniendo en cuenta el aspecto operativo del laboratorio fueron *reducir* o *evitar el riesgo.* A continuación se presentan las soluciones propuestas:

- **Compresor de aire TK2**

Actualmente el compresor de aire trabaja sin ningún mecanismo de seguridad dedicado. El control de alta presión lo efectúa el breaker de 110V ubicado en el panel de control de la planta de control de presión. Cuando el compresor está en si máxima capacidad, no hay nada que detenga su funcionamiento, el motor debe hacer sobresfuerzo en su operación aumentando la corriente a través del mismo, es aquí cuando el breaker de 110V de la planta actúa y abre el circuito apagando todos los dispositivos conectados a la fuente de voltaje.

Esta situación desgasta el motor y reduce su vida útil. Así mismo, pensar en un uso continuo de la planta de manera remota bajo este escenario no es posible debido a que el breaker dejaría fuera de servicio el compresor y el PLC, quienes se alimenta de la fuente de 110V. En caso de una falla en el breaker la integridad de la planta se vería seriamente comprometida si se permite el ingreso de más aire al compresor.

Por otro lado, tanto la instalación de la tubería de aire como el compresor no están siendo sometidos a ningún tipo de mantenimiento ocasionando que hayan fugas de aire y que la presión a la salida del compresor este por debajo de los 80 psi necesarios. Esto impide que se tenga una presión y un caudal de aire constante.

Por lo anterior se recomienda minimizar el riesgo a través de un control redundante de la siguiente manera:

- Remplazar el compresor y la tubería de aire hasta la planta de control de presión.
- En caso de que el nuevo compresor no la traiga consigo, implementar una válvula de seguridad por sobrepresión: Esta válvula tiene como función proteger el circuito contra una presión excesiva. Si existiera una avería en el circuito, por la que la presión sobrepasara el valor de 235 psi (capacidad máxima del compresor actual), la válvula se abriría descargando el aire a la atmosfera.
- Es importante contar con un sistema de supervisión para la presión en el compresor, por ello se recomienda acoplar a la salida del compresor un sensor y transmisor de presión que envié la señal al PLC para que pueda ser monitoreada y controlada. En el código de programación del PLC se debe crear una subrutina que apague el compresor cuando la presión exceda los 235 psi (pensado para la máxima capacidad del compresor actual).

- **Autenticación de usuario.**

El control de acceso es pensado para evitar que haya intrusión en las cuentas de usuario tanto del docente, administrador y estudiante. Para ello se recomienda lo siguiente:

- Los datos de usuario deben ser encriptados con SSL (Secure Sockets Layer).
- Durante el registro de un nuevo usuario, este debe definir una serie de preguntas personales que cada vez que intenta acceder remotamente al laboratorio saldrán aleatoriamente y deben ser respondidas correctamente para autorizar el acceso.
- Una de las amenazas más comunes en los sistemas de control de acceso son los llamados “robots”, un algoritmo que a través de la prueba y error descifra la contraseña del usuario. Para evitar que el laboratorio sea vulnerable a los robots, se debe utilizar CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans are Apart) consiste en que el usuario introduzca correctamente un conjunto de caracteres que se muestran en una imagen distorsionada que aparece en la pantalla, con el fin de corroborar que es el humano quien intenta el acceso.

Por otro lado, la base de datos de los usuarios está expuesta comúnmente a un ataque llamado SQL injection: se inserta o "inyecta" código SQL invasor dentro del código SQL programado, a fin de alterar el funcionamiento normal del programa y lograr así que se ejecute la porción de código "invasor" incrustado, en la base de datos. Esto lo puede evitar el programador de la base de datos incluyendo código de seguridad que varía dependiendo del lenguaje que se esté utilizando.

- **Uso inadecuado de la planta.**

La planta está diseñada para trabajar a 20 psi, por ello es importante restringir el valor del set point desde el código de programación. Si el usuario pide un valor de set point por encima del límite máximo de trabajo de la planta, el PLC debe hacer caso omiso a esta orden y la aplicación web debe mostrar un mensaje de advertencia sobre dicha acción de control.

El laboratorio remoto ha sido planeado para operar de manera remota en horas adicionales al horario laboral, es importante contar con un sistema de supervisión que permita al docente y al administrador hacer un seguimiento al desarrollo de las prácticas sobre la planta. Es necesario registrar las variables y las acciones tomadas (como apertura o cierre de una electroválvula) durante la práctica de laboratorio.

Tener los dos reguladores manuales de presión sin ninguna medida de seguridad puede ocasionar que cambien la posición de este y permitan que la planta trabaje a una presión mayor a los 20 psi de diseño, es por esto que se recomienda proteger estos dos instrumentos en una caja sellada la cual solo podrá abrir el laboratorista.

- **Dos o más usuarios con acceso a la planta simultáneamente (local-remoto, remoto-remoto).**

El laboratorio de control de procesos hace parte de un entorno académico, en donde tiene múltiples usuarios (tanto remotos, como locales). Se deben organizar los turnos de trabajo en un horario teniendo prioridad los usuarios locales. Adicionalmente, se debe contar con un tiempo límite para cada práctica con el fin de tener una mayor cobertura.

Del mismo modo es necesario contar con ayudas visuales (como luces piloto) en el laboratorio que permitan al estudiante reconocer si la planta está siendo utilizada de manera remota por otro usuario.

- **Servidor.**

Los servidores web y OPC deben estar en equipos diferentes al utilizado para las practicas presenciales y solo pueden tener acceso a ellos el administrador del laboratorio remoto. Para su adecuación se recomienda contar con:

  - UPS para protegerse contra picos de voltaje y para tener abastecimiento de energía en caso de que se caiga el servicio.

- **PLC**

Para proteger al PLC contra picos de voltaje, se recomienda conectarlo a la UPS destinada a los servidores.

Por otro lado es importante que dentro del algoritmo de programación se cuente con subrutinas de seguridad que eviten que el usuario pueda hacer oscilar las salidas digitales del PLC (conectadas a las electroválvulas FX 130-1 y FX 130-2) lo cual afecta la integridad del controlador.

- **VPN**

Una VPN (Virtual Private Network) por sus siglas en inglés, es una tecnología de red que permite una extensión segura de la red local sobre una red pública o no controlada. Esto con el fin de aprovechar en nuestro caso la infraestructura que ofrece internet, pero con la privacidad de una red cerrada. Algunas de las aplicaciones más típicas de una VPN son: la posibilidad de conectar dos o más sucursales de una empresa utilizando como vínculo Internet, permitir a los miembros del equipo de soporte técnico la conexión desde su casa a una planta de industrial, entre otros.
Para emular un vínculo punto a punto en una VPN, los datos se encapsulan o empaquetan con un encabezado que proporciona la información de enrutamiento que permite a los datos recorrer la red pública hasta alcanzar su destino. Para emular un vínculo privado, los datos se cifran para asegurar la confidencialidad. Los datos interceptados en la red compartida o pública y no se pueden descifrar si no se dispone de las claves de cifrado

Los componentes básicos de una VPN son [33]:

  - Servidor VPN.

- Túnel.
- Conexión VPN.
- Red pública de tránsito.
- Cliente VPN.

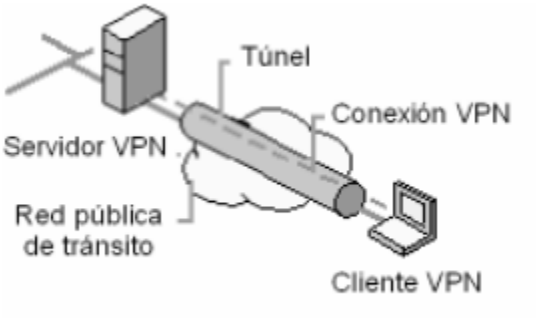


Figura 4.3. Componentes de una VPN. Fuente [12]

El uso de una red privada virtual ofrece las siguientes ventajas al proyecto:

- Autenticación de usuarios.
- Control de acceso.
- Administración de direcciones.
- Cifrado de datos.
- Administración de claves.
- Ancho de banda.

- **Firewall**

Además de ser vulnerable a una intercepción de los datos por utilizar una red pública como internet, también se puede presentar un ataque de Denegación de Servicio (DoS) por sus siglas en ingles. Este ataque tiene lugar cuando un atacante desactiva o corrompe las redes, los sistemas o los servicios para denegar el servicio a los usuarios. Se puede lograr enviando datos no validos a aplicaciones o servicios de red, lo que puede hacer que el servidor se bloquee. Otro ataque DoS, consiste en inundar de tráfico toda una red hasta hacer que se sature y sea imposible utilizarla o también se puede estropear un router con el fin de que los usuarios legítimos no puedan acceder a la red.

Por lo anterior es necesario que además de contar con una VPN, se utilice un Firewall tanto para el acceso desde internet como desde la red LAN de la Universidad que restrinja tanto el número de paquetes que se recibe por host como el número de host que se atiende en simultaneo [34].

Las recomendaciones que se proponen no necesariamente generan sobrecostos por talento humano debido a que se pueden desarrollar como trabajos de grado, trabajos de investigación o incluso en las materias que se cursan en los diferentes programas de pregrado de la facultad.

4.2.12. Desarrollo de elementos adicionales para el esquema de seguridad cibernética.

Finalmente se propone un plan de continuidad para la planta de control de presión de acuerdo con las necesidades del laboratorio:

De acuerdo con el análisis de riesgos y la encuesta realizada a los docentes, se definieron dos aspectos que son críticos para el funcionamiento y serán tratados en esta etapa:

- Equipo que soporta el servidor web y OPC.
  A pesar de los controles para mitigar los riesgos sobre este activo, puede llegar o sufrir daños o quedar fuera de servicio.
- Perdida de conexión cliente – servidor.
  Al estar conectados a través de internet, puede presentarse la situación de que el cliente o el servidor web pierdan dicha conexión.

Estas dos situaciones influyen fuertemente sobre la disponibilidad del laboratorio, sin embargo los resultados de las encuestas hechas a los docentes que trabajan en el laboratorio arrojo que no es muy importante y horas o días de suspensión del servicio de acceso remoto son tolerados.

A continuación se presentan las estrategias de solución para cada situación:

- Equipo que soporta el servidor web y OPC
  A. Hacer uso de los back ups de cada uno de los servidores.
  B. Si se necesita restablecer rápidamente el servicio, se puede tener el servidor en una máquina virtual de tal manera que si el equipo es considerado como perdida, esta se puede montar rápidamente sobre otro equipo alterno.

  La persona encargada de llevar a cabo estas estrategias es el laboratorista, quien tendrá en su poder los back ups y el disco duro de la máquina virtual.

- Perdida de conexión cliente – servidor.
  A. Si la planta dura 10 minutos sin recibir ningún tipo de orden por parte del cliente, el PLC debe proceder a liberar todo el aire al interior de la planta abriendo las electroválvulas FX 130-1 y FX 130-2, apagar el compresor y dejar todos los instrumentos en su estado inicial.

4.2.13. Soluciones rápidas

Algunas de las soluciones rápidas que deben ser implementadas para el correcto funcionamiento de la planta con acceso remoto son las siguientes:

- La llave HV130-1 que permite el paso de aire a la planta es manual, es necesario que sea remplazada por una electroválvula para que se pueda abrir o cerrar el paso de aire remotamente.

- Actualmente la manera de elegir entre la planta de visión de maquina o la planta de control de presión para que realice el control del compresor de aire se hace a través de una cuchilla ubicada en el panel de control de la planta de presión. Es necesario que esta acción pueda hacerse desde el HMI para acceso remoto, para ello se deben incluir en el interfaz botones para esta acción.
- Interfaz para encender o apagar el compresor de aire remotamente.

5. REQUERIMIENTOS DEL ESQUEMA DE SEGURIDAD CIBERNÉTICA DE LA PLANTA DE CONTROL DE PRESIÓN.

La ejemplarización de los lineamientos de seguridad (propuestos en el capítulo 2) sobre la planta de control de presión (desarrollados en el capítulo 4) permitió realizar un análisis del funcionamiento de dicha planta, con acceso remoto. En estos pasos se realizó un análisis de riesgos y los controles necesarios para tratarlos se ven sintetizados, a manera de lista, en este capitulo

Basados también en las tablas *11. Análisis preliminar de riesgos* y *16. Análisis preliminar de riesgos detallado*. Se definen los siguientes requerimientos para contar con un adecuado esquema de seguridad cibernética para la planta de control de presión del laboratorio de control de procesos de la Universidad del Cauca:

Para el software de la planta

- Sistema de supervisión de presión en el compresor.
- Subrutinas de seguridad en el algoritmo de programación del PLC contra malas prácticas.
- Interfaz para encender o apagar el compresor de aire remotamente y para definir cuál de las dos planta realiza el control (planta de visión de maquina/planta de control de presión).

Para el software de los servidores:

- Preguntas personales para autenticación de usuario.
- Captcha durante la autenticación de usuario.
- Código de seguridad en el algoritmo de la base de datos contra SQL Injection.
- VPN.
  - Autenticación de usuarios.
  - Control de acceso.
  - Administración de direcciones.
  - Cifrado de datos.
  - Administración de claves.
  - Ancho de banda.

Para el hardware de la planta:

- Remplazar el compresor de aire y la tubería de acople a la planta de control de presión.

- Válvula de seguridad por sobrepresión en el compresor de aire.
- Caja de seguridad para los reguladores manuales de presión a la entrada de la planta.
- Luces piloto para indicar si la planta está siendo operada remota o presencialmente.
- Remplazar la llave HV130-1 por una electroválvula.

Para el hardware de los servidores:

- Equipo dedicado para el servidor web y OPC.
- UPS

Para la gestión y administración del laboratorio:

- Políticas de seguridad.
- Historial de los eventos ocurridos durante las prácticas remotas.
- Cronograma de trabajo para las prácticas remotas.

6. CONCLUSIONES Y RECOMENDACIONES

- El esquema de seguridad debe ser diseñado por un equipo interdisciplinar de personas con el fin de abarcar todos los aspectos presentes en un laboratorio
- Los lineamientos de seguridad diseñados en este proyecto permiten seguir de forma organizada una serie de actividades que llevan a un esquema de seguridad para un laboratorio académico acorde con las necesidades del mismo
- Un esquema de seguridad exitoso se logra no solo con un correcto diseño del mismo, sino con el compromiso de las personas para quienes el laboratorio es una herramienta de trabajo, en cuanto al cumplimiento de políticas de seguridad y buen uso de los recursos que tienen a su disposición. El laboratorio de control de procesos no presenta las condiciones hardware y software para ser habilitado el acceso remoto.
- El análisis de riesgos debe realizarse repetidamente después de cada cambio, adaptación o mejoras al laboratorio.
- El análisis de riesgos y las medidas de control de mitigación deben ser desarrolladas por expertos en los sistemas de control, seguridad cibernética, y el personal involucrado en la operación y mantenimiento del laboratorio.
- La toma de decisiones durante los controles de mitigación de riesgo es llevada a cabo por los directivos del departamento o de la Universidad ya que se contempla además del aspecto operativo del laboratorio, las políticas y finanzas de la institución.
- Las medidas aquí recomendadas deben ser realizadas por un equipo con conocimientos en redes, instrumentación industrial, programación de PLC's y seguridad informática.
- El análisis de riesgos debe ser realizado de nuevo, una vez hayan sido implementadas las recomendaciones aprobadas por las directivas ya que se pueden presentar nuevos riesgos.

Se recomienda, que basados en este proyecto se realicen trabajos futuros como:

- Implementación de los controles recomendados para mitigar los riesgos aprobados por las directivas.
- Aplicación de los lineamientos de seguridad sobre las demás plantas del laboratorio de control de procesos.
- Completar el ciclo Planear-Hacer-Verificar-Actuar propuesto por el estándar ISA-99 en la planta de control de presión.

7. BIBLIOGRAFIA

[1] ISA International, “ISA S99.00.02 Manufacturing and Control Systems Security Part 2: Establishing a Manufacturing and Control System Security Program” Septiembre, 2005

[2] Puyosa, Héctor. “Vulnerabilidad de sistemas de control”, ISA Seccion Española, Madrid y Cartagena. [En internet]. Disponible en http://www.isa-spain.org/images/biblioteca_virtual/rt%200801%20-%20vulnerabilidad%20de%20sistemas%20de%20control%20publicar%20rev3.pdf. [Accedido Junio 13, 2012].

[3] Sanchez, Javier, “Ethernet Indsutrial,” Hirschmann Automation and Control. ISA Sección Española. [En internet]. Disponible en http://www.isa-spain.org/images/biblioteca_virtual/rt%20isa%20ethernet%20industrial.pdf. [Accedido Junio 16, 2012]

[4] Departamento de Ingenieria de Sistemas y Automatica, “Industrial Ethernet Comunicaciones Industriales” Escuela Superior de Ingenieros del Pais Vasco. [En internet]. Disponible en http://www.disa.bi.ehu.es/spanish/ftp/material_asignaturas/Laboratorio%20de%20Comunicaciones%20Industriales/Documentaci%F3n/04%20%20Industrial%20Ethernet.pdf. [Accedido Junio 16, 2012].

[5] ISA International, “ISA-99” [En Internet]. Disponible: http://www.isa.org/Template.cfm?Section=Standards2&template=/Ecommerce/ProductDisplay.cfm&ProductID=7552 [Accedido Junio 25, 2012]

[6] ISA International, “ANSI/ISA 95.00.01-2000 Enterprise Control System Integration Part 1: Models and Terminology” Julio 2000.

[7] Implementación Sistemas Integrados de Gestión SIG, “El ciclo de Deming”. [En internet]. Disponible en http://www.implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-deming. [Accedido Octubre 7, 2012]

[8] Puerta, Fernando Alonso de la, “Guía para la selección y aplicación de las técnicas de PHA (análisis de peligros de procesos)”, Universitat Politécnica de Catalunya. [En internet]. Disponible en

http://upcommons.upc.edu/pfc/handle/2099.1/4187. [Accedido Noviembre 21, 2012].

[9] Guía para elaboración de políticas de seguridad. Universidad Nacional de Colombia Dirección Nacional de Informática y Comunicaciones, 2003. [Accedido Enero 14, 2013].

[10] ISO 27005, "Desarrollo de una evaluación detallada de seguridad," 2008. [Accedido Enero 14, 2013]

[11] Pino, Laura del, "Guía de desarrollo de un plan de continuidad de negocio", Universidad Politécnica de Madrid. [En internet]. Disponible en http://www.criptored.upm.es/guiateoria/gt_m001r.htm. [Accedido Enero 23, 2012]

[12] Flórez, Juan Fernando. "Planta de Presión y Flujo de Aire: Reconocimiento de la Planta," Guía de Laboratorio. Universidad del Cauca.

[13] Conferencia de la OEA sobre la seguridad cibernética. Buenos Aires, Argentina. Julio 28 y 29, 2003. [En internet]. Disponible en http://www.afcea.org.ar/cursos/conferenciaOEA.htm. [Accedido Febrero 7, 2013]

[14] Symantec Corporation, "El gusano Stuxnet". [En internet]. Disponible en http://www.symantec.com/es/mx/theme.jsp?themeid=stuxnet [Accedido Febrero 7, 2013]

[15] ISO 27000, "Familia de normas 27000 Seguridad de la información," ISO 27000 el portal de ISO 270001 en Español, 2005. [En Internet]. Disponible en http://iso27000.es/iso27000.html. [Accedido Febrero 10, 2013]

[16] National Institute of Standars and Technology "ISA 99 foundational requirements," 2009. [En internet]. Disponible en http://www.isa.org/Template.cfm?Section=Products_and_Services&Template=/Ecommerce/EcomDefault.cfm. [Accedido Mayo 21, 2012]

[17] Lessig, Bill, "Chemical Facility Integrates Security and Process Control to Reduce Risk and increase Safety," Julio, 2005 [En internet].Disponible: http://hpsweb.honeywell.com/Cultures/enUS/NewsEvents/SuccessStories/success_geismar.htm [Accedido Mayo 21, 2012]

[18] Tofino Security, “Using ANSI/ISA-99 Standars to Improve Control System Security,”2012. [En internet]. Disponible en http://www.tofinosecurity.com/professional/using-ansiisa-99-standards-improve-control-system-security. [Accedido Mayo 23, 2012]

[19] Langill, Joel, T. Ü. V. FSEng, and CCNA Staff Engineer. “INCORPORATING CYBER SECURITY INTO THE EXECUTION METHODOLOGY OF AUTOMATION PROJECTS." [Accedido Mayo 23, 2012]

[20] Langill, Joel, “securing the analyzer network – working with OPC analyzer devices integration”. [En internet]. Disponible en http://www.isa.org/Template.cfm?Section=Products_and_Services&Template=/Ecommerce/EcomDefault.cfm. [Accedido Mayo 23, 2012]

[21] Fouad, M. “Successful Implementation of ISA-99 Recommendations in Saudi Aramco,” 2010. [En internet]. Disponible en http://www.isa.org/Template.cfm?Section=Products_and_Services&Template=/Ecommerce/EcomDefault.cfm. [Accedido Mayo 24, 2012]

[22] Chemical Industry Data Exchange, “The Cybersecurity Journey—How to Begin an Integrated Cybersecurity Program,” 2005. [Accedido Mayo 24, 2012]

[23] Zerpa, Sergio, “Desarrollo de un Laboratorio Remoto de Automatización de Procesos vía Internet” Seventh LACCEI Latin American and Caribbean Conference for Engineering and Technology. 2009. [En internet]. Disponible en http://www.laccei.org/LACCEI2009-Venezuela/Papers/ELDE179_Zerpa.pdf. [Accedido Junio 3, 2012]

[24] Jimenez, Luis, “Laboratorios remotos para las prácticas de ingeniería de sistemas y automática en la universidad Miguel Hernández” Universidad Miguel Hernandez Elche- Alicante. [En internet]. Disponible en http://www.uv.es/eees/archivo/UMH-LaboratoriosRemotos03.pdf. [Accedido Junio 3, 2012]

[25] Khamis, A. "Interacción remota con robots móviles basada en Internet." PhD Tesis. Universidad Carlos de Madrid. Madrid. 2003. [Accedido Junio 3, 2012]

[26] Matalobos, Juan “Análisis de riesgos de seguridad de la información,” 2009. Universidad politécnica de Madrid. [En internet]. Disponible en http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf. [Accedido Junio 5, 2012]

[27] Cendagorta, Juan “Seguridad en servidores web,” 2004. Universidad Nacional de Comahue - Argentina [En internet]. Disponible en http://www.criptored.upm.es/guiateoria/gt_m148u.htm. [Accedido Junio 5, 2012]

[28] Ariza, Carlos “Laboratorio remoto para la enseñanza de la programación de un robot industrial,” 2011. Universidad Militar Nueva Granada. [En internet]. Disponible en http://web.usbmed.edu.co/usbmed/fing/v2n1/v2n1a7.pdf. [Accedido Junio 5, 2012]

[29] Nourdine, Aliane, “Un Laboratorio de Ingeniería de Control Basado en Internet,” 2007. Universidad Europea de Madrid. [En internet]. Disponible en http://www.scielo.cl/scielo.php?pid=S071807642007000600004&script=sci_arttext. [Accedido Junio 5, 2012]

[30] Dikai, Liu, “Remote laboratories in Engineering Education: Trends in Students’ Perceptions” University of Technology Sydney-Australia. [En internet]. Disponible en http://www.labshare.edu.au/media/img/remote_lab_education_trends.pdf. [Accedido Junio 6, 2012]

[31]Casallas, Ricardo “Desarrollo básico de un laboratorio virtual de control de proceso basado en internet,” 2005. Universidad de Los Andes Táchira – Venezuela. [En internet]. Disponible en http://www.saber.ula.ve/bitstream/123456789/17233/2/articulo6.pdf. [Accedido Junio 6, 2012]

[32] Reliability and Risk Management, “Inspección basada en riesgo e integridad mecánica”. [En internet]. Disponible en http://www.reliarisk.com/r2m/mariangela/%28Microsoft%20Word%20-%20Inspecci_363n%20Basada%20en%20Riesgo%20_IBR_-Contenido.doc%29.pdf. [Accedido Febrero 26, 2013]

[33] González, Alexandro, “Redes Privadas Virtuales”, Universidad Autónoma del Estado de Hidalgo, Mayo 2006. [En internet]. Disponible en

http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20privadas%20virtuales.pdf [Accedido Febrero 23, 2013]

[34] FUNDESEM Bussiness School, “Técnicas de defensa contra ataques DoS”. [En internet]. Disponible en http://www.efundesem.com/_Recursos/Curso00099/Convocatoria000115/Recurso0000643/Comentario1G5.pdf [Accedido Febrero 28, 2013]