Institución Universitaria

Adaptación del modelo de madurez en ciberseguridad basado en C2M2, para la industria manufacturera del sector textil que utiliza sistemas SCADA.

Jorge Mario Aristizábal Correa

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2018

Adaptación del modelo de madurez en ciberseguridad basado en C2M2, para la industria manufacturera del sector textil que utiliza sistemas SCADA.

Jorge Mario Aristizábal Correa

Tesis o trabajo de investigación presentada(o) como requisito parcial para optar al título de:

Magister en Seguridad Informática

Director (a):

Magister en administración y dirección de empresas, Leonel Marín Ramírez

Codirector (a):

Magister en automatización y control industrial, Johny Antonio Alvarez Salazar

Línea de Investigación:

Automática, Electrónica y Ciencias Computacionales

Instituto Tecnológico Metropolitano

Facultad de Ingeniería

Medellín, Colombia

2018

Dedicatoria

A Dios

Por darme la oportunidad de poder compartir con aquellas personas que quiero y me apoyan, para la gloria de Dios.

A mi familia

Por su apoyo, enseñanzas, paciencia, entrega y amor que me brindan.

Una locura es hacer la misma cosa una y otra vez esperando obtener resultados diferentes. Si buscas resultados distintos, no hagas siempre lo mismo.

Albert Einstein

Agradecimientos

Por la dedicación, apoyo, sugerencias y orientación brindadas en la ejecución de esta tesis a los directores Leonel Marín Ramírez y Johny Antonio Alvarez Salazar, sin su colaboración no habría sido posible su materialización.

A los profesores, compañeros y amigos por sus valiosos aportes que me brindaron para que este trabajo fuera desarrollado.

Resumen

Los sistemas SCADA, son sistemas de información que reúnen un conjunto de tecnologías, protocolos y plataformas que componen los ICS (Industrial Control System o sistemas de control industrial), recolectan información de los procesos industriales e interactúan con los dispositivos instalados en la maquinaria PLC (Programmable Logic Controller o controladores lógicos programables), son integrados por sensores y actuadores, tienen la capacidad de obtener datos como medidas de tamaño, presión, temperatura o posición, presentan información para la toma de decisiones con la supervisión humana.

Se propone diseñar una adaptación del modelo C2M2 con el fin de establecer un marco de referencia para la protección de la infraestructura crítica de la industria manufacturera del sector textil, apuntando a evaluar la madurez en seguridad de los procesos, políticas y medidas que mitigan el impacto que puedan causar las vulnerabilidades propias de los sistemas de supervisión, control y adquisición de datos (SCADA) integrado por los sistemas de control industrial (ICS), sistemas de control distribuidos (DCS), los controladores lógicos programables (PLC).

Con la adaptación del modelo C2M2 para la evaluación de madurez en ciberseguridad, se pretende determinar el nivel de madurez en la gestión de los sistemas de SCADA del sector textil, en donde se genere una herramienta que pretende identificar, evaluar y calificar los elementos de seguridad que puedan causar los riesgos de fuga, indisponibilidad o alteración no permitida de la información.

Al evaluar estos elementos de seguridad se pretende generar un informe, en el cual se puedan identificar las falencias, los riesgos y debilidades que se tienen, con el fin de que en un futuro este sirva de insumo para establecer políticas, procedimientos o directivas que ayuden a fortalecer la ciberseguridad en los sistemas SCADA.

Palabras clave: Ciberseguridad, Modelo, Madurez, SCADA, ICS, Textil.

Abstract

The SCADA systems are information systems that bring together a set of technologies, protocols and platforms that make up the ICS (Industrial Control System or industrial control systems), collect information from industrial processes and interact with the devices installed in the PLC machinery (Programmable Logic Controller or programmable logic controllers), are integrated by sensors and actuators, have the ability to obtain data such as measurements of size, pressure, temperature or position, present information for decision making with human supervision.

It is proposed to design an adaptation of the C2M2 model to establish a frame of reference for the protection of the critical infrastructure of the textile industry, aiming to evaluate the maturity of the processes, policies and measures that mitigate the impact that can cause the vulnerabilities of the systems of supervision, control and data acquisition (SCADA) integrated by industrial control systems (ICS), distributed control systems (DCS), programmable logic controllers (PLC).

With the adaptation of the C2M2 model for the evaluation of maturity in cybersecurity, it is intended to determine the level of maturity in the management of SCADA systems in the textile sector, where a tool is created that aims to identify, evaluate and qualify the security elements that may cause the risks of flight, unavailability or alteration of the information.

When evaluating these security elements, we intend to generate a report, in which we can identify the shortcomings, the risks and weaknesses that we have, in order that in the future this will serve as an input to establish policies, procedures or directives that help to strengthen cybersecurity in SCADA systems.

Keywords: Cybersecurity, Model, Maturity, SCADA, ICS, Textile.

Contenido

Lista de figuras

Pág.

Lista de tablas

Pág.

Lista de Símbolos y abreviaturas

Abreviaturas

Abreviatura	Término
AGA-12	Estándar para sistemas SCADA
C2M2	*Modelo de madurez en ciberseguridad.*
CFATS	Estándares Antiterroristas para Instalaciones Químicas.
CIA	Agencia central de inteligencia.
DCS	Sistema de control distribuido.
HMI	Interface humano máquina.
ICS	Sistemas de control industrial.
ISACA	Asociación para la auditoría y control de los sistemas de información.
ISO/IEC 27002:2005	Estándar ISO para la seguridad de la información.
MODBUS	Protocolo de comunicación utilizado para PLC, RTU y SCADA.
MTU	Unidad terminal maestra.
NERC CIP,	Estándar del consejo de Confiabilidad Eléctrica de América del Norte para la protección de la infraestructura crítica.
NIST 800-82	Guía para los sistemas de control industrial del instituto nacional de estándares y tecnología.
NRC RG 5.71	Guía regulatoria de la comisión regulatoria nuclear.
OT	Tecnologías de la operación.
PLC	Controladores lógicos programables.
RTU	Unidad terminal remota.
SANS	Organización para la capacitación en seguridad de la información.
SCADA	Sistemas de supervisión, control y adquisición de datos.
TI	Tecnologías de la información.

Introducción

El sector industrial está siendo vulnerable a los ataques cibernéticos ocasionados por personas y organizaciones que se aprovechan de los riegos que se presentan en los sistemas de control industrial, afectando los productos, calidades de producción, reputación de marca y seguridad de las personas. Las intrusiones se han materializado debido la adopción de las nuevas tecnologías de la información, en las que se evidencian las necesidades de integrar los componentes de las tecnologías de la información con los sistemas de control industrial en lo concerniente a la seguridad. Cherdantseva, et al. (2016). En el informe IBM X-Force Research (2016) Índice de Inteligencia en Seguridad Cibernética se evidencia el incremento de los ataques a esta industria y según Knapp (2011) hace referencia a que la seguridad de las redes industriales presentan varias características similares a los estándares de seguridad informática de las empresas.

Para realizar una mitigación de riegos es necesario evaluar cada uno de los componentes que intervienen en los procesos, algunos de estos están relacionados con los procesos de TI, siendo un factor clave la identificación de los elementos de seguridad para los ICS (Sistemas de Control Industrial) que pueden ser afectados por las amenazas, vulnerabilidades y ataques. Los ICS están compuestos por SCADA, HMI, MTU y RTU. Al realizar una evaluación de las políticas de seguridad a este tipo de infraestructuras, se puede determinar el estado de madurez en el que se encuentran, además de poder identificar sus debilidades, con el fin de poder establecer estrategias que ayuden a mitigar los riegos que se pueden identificar. Para realizar dicha identificación se propone una adaptación del modelo C2M2 que evalué la madurez en ciberseguridad, para esto se requiere la elaboración de una herramienta que permita identificar las capacidades y los elementos que pueden causar riesgos de fuga de información, indisponibilidad u alteración de información; los elementos se deben agrupar en dominios, según su relación e impacto, enfocando su estructuración, para la industria manufacturera del sector textil.

A pesar que los sistemas SCADA son ampliamente utilizadas por su confiabilidad y pueden operar sin pausa durante meses o años. Knowles, et al. (2015). La vulnerabilidad de los sistemas propietarios es a veces en los protocolos de comunicación. El paso de una operatividad local a una gestión remota, impulsado por los desarrollos e interoperatividad y funcionalidades creadas por

los nuevos desarrollos de software para este tipo de sistemas, plantea nuevos desafíos de seguridad. Si hay un valor en los datos, que se intercambian, los hackers encuentran una manera de acceder a éllos. Schrecker (2015).

Existe un desafío en la aplicación de soluciones en seguridad que a menudo van más allá de las capacidades técnicas de los sistemas tecnológicos heredados, y a veces económicamente costoso, también se identifican algunas propiedades únicas de los sistemas de control industrial en comparación con los sistemas de TI y variaciones en la seguridad. Se pueden aplicar mecanismos de seguridad para la prevención de ataques, detección, recuperación, resiliencia y disuasión. En la fabricación de productos, los procesos de (diseño, control de calidad, suministro y personal) el acceso a la información por parte de entidades no autorizadas o externas es crucial en el panorama competitivo actual. La divulgación de negocios, datos críticos de producción, información a competidores y adversarios podría causar una pérdida de la ventaja competitiva y la relevancia del mercado. En consecuencia, la protección, la preservación de la información patentada es vital para la competitividad de una empresa. Uchenna, et al (2017).

La metodología aplicada tendrá elementos cualitativos y cuantitativos, teniendo en cuenta los conceptos, herramientas y elementos existentes en el modelo C2M2, adaptándolo al sector textil, que permitan la identificación de otros elementos que puedan ser evaluados y analizados, estableciendo una referencia de las capacidades instaladas en los diferentes procesos que involucran la gestión de los sistemas SCADA. Se propone evaluar los diferentes elementos con el fin de determinar el nivel de madurez en la gestión de estos sistemas e identificar las posibles falencias que se tienen en las políticas, procedimientos o medidas, que puedan causar un riesgo a la seguridad, por medio de un trabajo experimental para evaluar su aplicación en estos ambientes por medio de un caso de estudio. Por medio de un método inductivo se analizarán las necesidades propias de este sector para identificar los elementos que afectan la seguridad y proponer una adaptación del modelo que permita evaluar su madurez en ciberseguridad.

Se va a demostrar el nivel de madurez en ciberseguridad en el cual se pueden evaluar los riesgos de las amenazas, ataques, su impacto e importancia; con los resultados de esta evaluación se pueden establecer estrategias que permitan gestionar y mitigar los riesgos en estos sistemas productivos. Cuando se evalúa el nivel de madurez se crea conciencia en la gestión de estos

sistemas productivos, teniendo como premisa el no perder la confidencialidad, integridad y disponibilidad.

Con la herramienta de evaluación del nivel de madurez se crea una referencia del estado de los procesos, permitiendo así diseñar estrategias y controles eficientes y eficaces, para poder tomar las decisiones correctas, establecer prioridades para la atención de los incidentes, restaurar los servicios afectados a su estado original y evitar los incidentes que impacten el servicio.

Cuando se realiza la auditoria se crea conciencia de los riesgos que generan este tipo de infraestructura, evaluando cada uno de los aspectos que lo afectan, para esto se debe verificar e identificar el estado de madurez que se encuentran los procesos que intervienen en los sistemas SCADA. Al evaluar las actividades que se desarrollan en estos procesos permitirán una adecuada gestión del riesgo, tratamiento y solución ante las amenazas a la seguridad, teniendo en cuenta el impacto que puedan causar cada riesgo, ayudando a las organizaciones a generar un informe que permita identificar las falencias y así establecer medidas de protección, políticas, planes de continuidad y de recuperación de desastres de acuerdo a lo planeado en las capacidades de respuesta con eficiencia y eficacia.

Al diseñar una adaptación del modelo C2M2, se pretende establecer un marco de referencia para la protección de la infraestructura crítica de la industria manufacturera del sector textil, permite evaluar la madurez en seguridad de los procesos, políticas y controles que mitiguen el impacto que puedan causar las vulnerabilidades propias de los sistemas de supervisión, control y adquisición de datos (SCADA) integrado por los sistemas de control industrial (ICS), sistemas de control distribuidos (DCS), los controladores lógicos programables (PLC).

El objetivo general es: Proponer una adaptación del modelo C2M2 de evaluación de madurez en ciberseguridad con la elaboración de una herramienta que permita identificar las capacidades y los elementos que pueden causar riesgos de fuga de información, indisponibilidad u alteración de información.

Los objetivos específicos son: 1) Identificar todos los elementos de seguridad del modelo de madurez que pueden causar los riegos de seguridad, agrupándolos en dominios, según su relación e impacto, tomando como referencia el modelo C2M2, para la industria manufacturera del sector

textil; 2) Crear una adaptación del modelo C2M2, que permita evaluar el nivel de madurez en ciberseguridad para identificar las capacidades instaladas a todos los elementos que puedan afectar la gestión de los sistemas SCADA. 3) Desarrollar una herramienta y las pruebas de la adaptación del modelo por medio de encuestas, para la evaluación del modelo sugerido en un caso de estudio, con el fin de medir el nivel de madurez y capacidades instaladas en ciberseguridad de los elementos que componen la gestión de los sistemas SCADA.

1. Marco Teórico y Estado del Arte

Dentro de los lineamientos de políticas nacionales con respecto al tema a abordar, se encuentra el documento CONPES 3701 de 2011, el cual traza unos lineamientos de política para ciberseguridad y ciberdefensa, la Ley 527 de 1999 en la cual se define la validez jurídica de la información electrónica, Ley 1273 de 2008 donde se establecen los delitos informáticos y protección del bien jurídico tutelado que es la información, Ley 1341 de 2009 Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones TIC. En el año 2016 se publica el documento CONPES 3854, en donde se fortalecen las capacidades de ciberseguridad con un enfoque en gestión de riesgos, evolucionando del documento CONPES 3701, que se alinea con documento OCDE del año 2015, en donde se establece el diseño de estrategias integrales con un conjunto de principios que se enmarca en la gestión de riesgos de seguridad digital.

En el plan nacional de desarrollo 2014 – 2018 se tienen contemplados dos tipos de estrategias TIC, como plataforma para la equidad, la educación y la competitividad; y la Ciencia, Tecnología e Innovación, CTI en donde se integra un único Sistema de Competitividad, CTI, en el marco del cual se adelantará la implementación de la Agenda Nacional de Competitividad, CTI que permitirá agrupar todos los agentes del sector y lograr la institucionalidad necesaria para el desarrollo de las regiones. A nivel departamental se tiene bases del plan de desarrollo de Antioquia 2016 - 2019, en donde se establecen las estrategias como componente importante el desarrollo de la CTI y se orienta a la incorporación de acciones para apoyar el desarrollo de capacidades de gestión, generación de conocimiento, investigación y desarrollo, innovación y emprendimiento, transferencia de conocimiento y tecnología, cultura y apropiación de la CTI, institucionalidad para la CTI, las cuales propiciarán condiciones para agregación de valor y de crecimiento sostenible a largo plazo para las regiones del Departamento. Para impulsar el desarrollo económico y social a través de la ciencia, tecnología e innovación, se establece con base en el análisis de actividades relacionadas con: 1) Capital humano para la CTI; 2) Investigación y desarrollo; 3) Innovación y emprendimiento, 4) Transferencia de conocimiento y tecnología; 5) Cultura y apropiación de la CTI, y 6) Sistema e institucionalidad para la CTI.

El ciberespacio, como se denomina a Internet, es un dominio global e interconectado que no tiene fronteras. Para apoyar el crecimiento, operación, mantenimiento y seguridad, las empresas deben innovar continuamente e invertir en el desarrollo de productos y servicios desplegables a nivel mundial, grupos de interés, consumidores, las empresas, los gobiernos, los propietarios y operadores de infraestructura buscan una experiencia consistente y segura. Kris (2011). Para esta experiencia se ha desarrollado un nuevo concepto que es la ciberseguridad.

El concepto de ciberseguridad aparece por la CIA, SANS (2013) categorizando las consecuencias de la pérdida de confidencialidad, integridad y disponibilidad de la información, dada la importancia que proveen los sectores económicos y sus negativas repercusiones en la competitividad. Este concepto surge ante la necesidad de seguridad en la red internet, en el que se agrupan un conjunto de herramientas, políticas, tópicos de seguridad, esquemas de seguridad, directrices, métodos de gestión de riesgos, acciones, capacitación, programas de sensibilización, buenas prácticas, aseguramiento y técnicas que pueden utilizarse para proteger los activos de las organizaciones y quienes las utilizan.

Según ISACA (2015), (Information Systems Audit and Control Association, Asociación de sistemas de información auditoría y control), la definición más apropiada para ciberseguridad es “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.

La modernidad ha llevado a que los conceptos de modularidad, descentralización, mantenimiento y bajos costos se presenten como un factor importante a la hora de diseñar los sistemas de control, cambiando los protocolos propietarios de cada uno de los fabricantes por el protocolo estándar de red IP que se suelen encontrar en los entornos industriales, domésticos y de oficina Candell y Anand (2014). Aunque estos controles poseen sus propios sistemas propietarios para el control de los dispositivos, anteriormente estos se encontraban aislados de las redes de datos, teniendo como única forma de acceso la física, lo que permitía generar controles de fácil implementación para su utilización, pero con los avances, estos sistemas permitieron conectividad, adaptándose a los protocolos de comunicación como TCP/IP, para su gestión remota o envío de datos atreves de

internet, generando unas vulnerabilidades que además de estos protocolos, los sistemas propietarios no permiten o no se han desarrollado mecanismos de encriptación, los datos viajan sin ninguna protección o seguridad, lo cual puede ocasionar divulgación de los datos de producción, diseños y programación de la maquinaria, en casos en los que esta información es confidencial, viéndose comprometida la propiedad industrial; en otra situación, estos sistemas pueden ser vulnerados y alterados los datos para que los equipos industriales no realicen las tareas para la que en un principio fueron programadas, ocasionando pérdidas de la capacidad operativa, financieras, ambientales y hasta humanas. (Johnson, 2012; Kornecki y Zalewski, 2010)

Para la transmisión de los datos, los sistemas SCADA utilizan el protocolo Modbus, que según Bernieri, et al. (2017) Los datos de paquetes de Modbus son transmitidos sin ningún tipo de cifrado, y se espera que estos problemas de seguridad se resuelvan en las capas de transporte. Según Rezai, Keshavarzi y Moravej (2016). Basándose en el estándar AGA-12, hay aproximadamente 200 protocolos SCADA, dentro de los más populares está el MODBUS, este no contiene formato de seguridad.

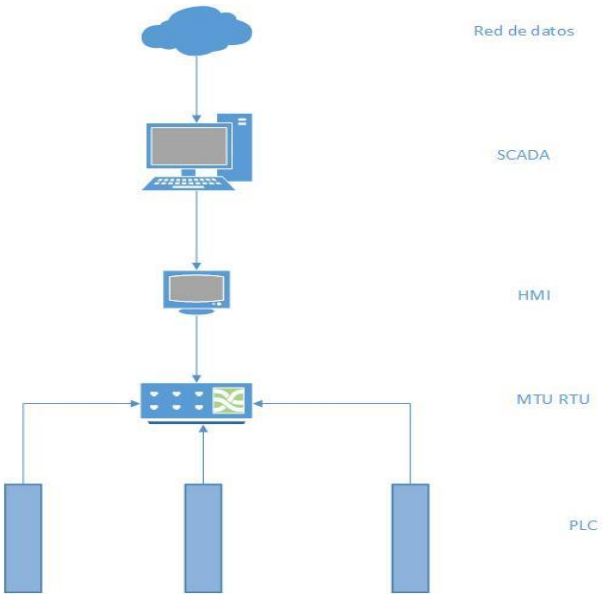
Los sistemas ICS es un término general que abarca varios tipos de sistemas de control, incluyendo los sistemas de control de supervisión y adquisición de datos SCADA, sistemas de control distribuido DCS , y otras configuraciones de sistemas de control , tales como controladores lógicos programables PLC a menudo se encuentra en los sectores industriales y de infraestructuras críticas. Candell, et al. (2014, Octubre).

Los sistemas SCADA, es el nombre que se le da a un sistema de información que reúne un conjunto de tecnologías, protocolos y plataformas integrados que componen un ICS (Industrial Control System o sistemas de control industrial), tienen la función de recolectar información de los procesos industriales y diferentes formas de interacción con los dispositivos instalados en la maquinaria PLC (Programmable Logic Controller o controladores lógicos programables), los sensores y actuadores, ellos son capaces, en su nivel básico, obtener datos como medidas de tamaño, presión, temperatura o posición. En el nivel medio, presentar información de los dispositivos para gestionar a distancia con la supervisión humana, abrir o cerrar compuertas, válvulas, aumentar o disminuir la presión, temperatura o cualquier otra decisión que requiera la intervención humana utilizando dispositivos HMI (Human Machine Interface, Interface Humano –

Máquina). Panel de visualización o panel de control. Los DCS (Distributed Control System o Sistemas de Control Distribuido) se encargan de convertir las señales digitales en señales analógicas y viceversa que son interpretadas por los PLC y de interactuar con los dispositivos de almacenamiento de las bases de datos, los parámetros de configuración y la iteración con los dispositivos HMI. Hernandez y Ledesma (2010).

El grado de penetración del internet, los diversos lugares desde donde se realizan las conexiones, los medios empleados para su distribución y dispositivos a los que se les ha integrado características para su uso, Figura 1, ha hecho que se establezcan formas de penetrar e integrar equipos que permiten realizar transacciones, gestión remota, envío de datos y configuración que ayudan a facilitar las actividades ligadas a la gestión y control de los activos, procesos de producción. Uchenna, et al. (2017); Shin et al. (2016).

Figura 1. Integración de tecnologías de TI con OT. Elaboración Propia.



Cherdantseva, et al. (2016). Indican que los sistemas SCADA modernos son altamente sofisticados y complejos, se basan en sistemas avanzados de tecnología. La sofisticación y modernización, así como la operación en tiempo real y la arquitectura distribuida de sus componentes, el crecimiento de las amenazas cibernéticas a los sistemas SCADA, estos están expuestos a una amplia gama de

amenazas cibernéticas, debido a la estandarización de los protocolos de comunicación y componentes de hardware y a la creciente interconectividad.

Se está operando con un sistema patentado de 20 años de edad, que no es vulnerable a las herramientas y a técnicas de ataque de hoy en día. La vulnerabilidad de los sistemas propietarios es a veces en los protocolos de comunicación. El paso de una operatividad local a una gestión remota, impulsado por los desarrollos e inter operatividad y funcionalidades creadas por los nuevos desarrollos de software para este tipo de sistemas, plantea nuevos desafíos de seguridad. Si hay un valor en los datos, que se intercambian, los hackers encuentran una manera de acceder a éllos. Schrecker (2015).

Los sistemas desarrollados son administrados por sistemas propietarios, que en un principio estaban aislados en una red propia, y que su gestión se realizaba de manera local o en el sitio donde se encontraban los dispositivos Kriaa et al., (2015), no se tenían en cuenta medidas de seguridad o protección de los datos que se transmiten por los protocolos propietarios que utilizan; debido a los avances en telecomunicaciones, éstos se han adaptado a las nueva tecnologías, migrando cada uno de los componentes de software, hardware y sus protocolos de comunicación para ser utilizados en ambientes abiertos, interconectados y de acceso remoto, utilizando internet como medio para su gestión, con la finalidad de darles a estos sistemas adaptabilidad, movilidad, facilidad y bajos costos de mantenimiento, pero estos no cuentan con medidas de protección que mitiguen los ataques, lo que los hace fácilmente vulnerables, haciendo que se produzcan fallos o pérdida de información valiosa para la industria. CockpitCI D 3.1 (2013).

Para la transmisión de los datos, los sistemas SCADA utilizan el protocolo Modbus, que según Bernieri, et al. (2017) los datos de paquetes de Modbus son transmitidos sin ningún tipo de cifrado, y se espera que estos problemas de seguridad se resuelvan en las capas de transporte. Según Rezai, et al. (2016). Basándose en el estándar AGA-12, hay aproximadamente 200 protocolos SCADA, dentro de los más populares está el MODBUS, este no contiene formato de seguridad. Las amenazas a la información pueden clasificarse en perdida de la disponibilidad que significa una interrupción en el acceso a los sistemas, perdida de la integridad siendo una modificación no autorizada o destrucción y perdida de la confidencialidad que es su divulgación no autorizada.

Los sistemas que soportan estas infraestructuras, son en ocasiones antiquísimos, desde el momento en que se instalan no se realizan actividades de actualización ya que por la criticidad y alta disponibilidad de los procesos que soportan, no se quiere correr el riesgo de parar las operaciones por cualquier funcionalidad no tenida en cuenta a la hora de realizar la actualización, pero las actualizaciones se deben realizar para brindar interacción con otros sistemas administrativos o de gestión remota, los cuales son utilizados para dar soporte o monitoreo a dichos sistemas, este monitoreo en mucha ocasiones se realizan desde lugares que están alejados de las instalaciones industriales, obligando a establecer medidas de protección en seguridad para los riesgos y vulnerabilidades modernas que cada vez cuentan con un mayor grado de sofisticación Uchenna, et al. (2017).

Cuando estos sistemas se crearon, la situación era diferente a la que se enfrenta en la actualidad, estos se implementaban en sitios cerrados y de acceso restringido, operados por personal bajo su supervisión, en el sitio, se evidencian muchos casos en los que los sistemas permanecen inalterados desde su instalación por muchos años y asignados a personal técnico especializado. Como se implementaban estos sistemas, presentaban poca probabilidad de intrusiones, ya que no se realizaban conexiones con componentes externos, su gestión se debía desarrollar de manera local, e interactuando directamente con los dispositivos del sistema, haciendo presencia en el sitio para recolectar los datos y definir los controles para su supervisión. En la Tabla 1 se evidencian algunos de los conceptos que deben ser tratados ya que por su implementación estos sistemas presentaban una baja probabilidad de intrusiones o ataques externos ya que no presentaban interacción con otros sistemas, por el desarrollo en las TIC, se permite establecer conectividad con estos sistemas en los que integran diversos dispositivos, arquitecturas y protocolos de comunicación, esto obliga a diseñar estrategias de seguridad que permita tener control y auditar los procesos que se llevaban a cabo en estos sistemas y que utilizan internet como su plataforma de comunicación. McGurk (2008).

Tabla 1. Desafíos en seguridad en los sistemas de control. McGurk (2008).

TEMA DE SEGURIDAD	TECNOLOGÍA INFORMACIÓN	SISTEMAS DE CONTROL
Seguridad Perimetral (Antivirus, Cortafuegos y Sistemas de detección y prevención de intrusos)	Común y ampliamente utilizado	Poco frecuentes y pueden ser difíciles de implementar
Soporte a la Tecnología	3-5 Años	20 años o más
Tercerización	Es común y ampliamente utilizada	Raramente usada, solo hay un vendedor
Aplicación de mejoras o correcciones	Es regular y programada	Es lento y según el proveedor
Gestión del cambio	Es regular y programada	Sistemas heredados no admite actualizaciones – no apto para las medidas de seguridad modernas
Tiempo contención crítico	Los retrasos son generalmente aceptados	Crítico debido a las perdidas
Disponibilidad	Los retrasos son generalmente aceptados	Disponibilidad siempre 7x24
Conciencia de seguridad	Bueno, tanto en el sector privado y público	Generalmente pobre con respecto a la seguridad cibernética
Pruebas de Seguridad / Auditoría	Programado y ordenado	Las pruebas se realizan de vez en cuando en las interrupciones / auditoría para la recreación de eventos
Seguridad física	Segura	Muy bueno, disponibilidad de control remoto

La prioridad que se le da a la protección y seguridad de la infraestructura es importante ya que se depende de las interconexiones de los dispositivos que las monitorean, tales servicios operan en Internet. La fenomenal expansión de esta red ha traído un crecimiento económico sin precedentes, oportunidad y prosperidad. Sin embargo, también presenta malos actores con oportunidades nuevas amenazas y delincuencia. Kriz (2011). Algunos antecedentes de casos documentados con intrusiones de seguridad a estos tipos de infraestructura en la industria son los siguientes:

El 10 de junio de 1999, un oleoducto propiedad de Olympic Pipeline Company, se rompió provocando una fuga de gasolina que se filtró en dos arroyos en Bellingham, Washington. La gasolina se encendió, lo que resultó en una bola de fuego que mató a tres personas, hirió a otros

ocho, y causó importantes daños materiales. Se dio a conocer que aproximadamente ¼ de millón de galones de gasolina fueron arrojados al ambiente. Aunque el daño fue en las tuberías externas, las válvulas de alivio de presión no se instalaron correctamente, y un error de los controles del sistema SCADA fueron los culpables, es una falla de las políticas y procedimientos de la compañía de tubería olímpica que llevaron a esta catástrofe. La evidencia apunta a errores del operador debido a la insuficiencia de los controles de acceso y directivas de auditoría, sin formación en seguridad. Abrams y Weiss (2008).

El Maroochy Servicios de aguas sufrió un incidente de ataque cibernético en abril de 2000 es un buen ejemplo de un ataque interno en un sistema SCADA industrial. Vitek Boden trabajó para la firma Hunter Watertech que instaló el equipo SCADA controlado por radio para la Maroochy Shire Council en Queensland, Australia. Boden dejó su trabajo en el Hunter Watertech y solicitó un trabajo con el consejo del condado de Maroochy, pero fue rechazado. Boden más tarde procedió a hackear el sistema SCADA de Maroochy Servicios de Aguas a través de la red inalámbrica utilizando un ordenador portátil. Él utilizó su conocimiento y experiencia con el sistema SCADA para dar órdenes, desactivar las alarmas, y manipular los datos a través de controladores locales para ocultar los problemas de la vigilancia de los ordenadores centrales del sistema. Su sabotaje provoco el derrame de 800.000 litros de aguas residuales crudas. La falta de control de acceso, políticas y procedimientos de Maroochy para su sistema era la principal causa de este incidente. Adicionalmente, la falta de un plan de respuesta a incidentes, de formación de seguridad y auditoría políticas no ayudaron a mitigar el ataque o los efectos que causaron. Abrams y Weiss. (2008).

En diciembre de 2014 el ICS de la industria de acero alemana Mill, sufre un ataque en el que se comprometen varios componentes críticos de proceso de producción, producto de un software malicioso que ingresa por correo. Assante y Conway (2014).

El 10 de septiembre de 2012 la empresa Telvent Canadá, Ltd, dedicada a proporcionar software y servicios para administrar y supervisar maquinaria del sector industrial, descubre que en los servidores de seguridad se encuentra instalado un malware que les permitió a los atacantes robar archivos de los proyectos relacionados con OASyS SCADA de sus clientes. Goldman (2012).

El 13 de Julio de 2012 y el 15 de Agosto 2012, los investigadores de seguridad independientes Billy Rios y Terry McCorkle identificaron múltiples vulnerabilidades en el software Tridium Niagara AX Framework que pueden ser explotadas remotamente, las cuales fueron publicadas con los documentos ICS-ALERT-12-195-01 e ICSA-12-228-01. Las vulnerabilidades encontradas son el salto de directorio, el almacenamiento de credenciales débiles, debilidades en el inicio de la sesión, y el identificador de sesión predecibles, explotando estas vulnerabilidades se pueden obtener un escalamiento de privilegios. El software de Tridium Niagara AX Framework gestiona controles automatizados para la industria de las telecomunicaciones, seguridad, maquinaria de manufactura, control de iluminación, operaciones de mantenimiento y reparación, y la gestión de las instalaciones, según Tridium, cuenta con más de 300.000 dispositivos instalados con su software. Rios y McCorkle (2012).

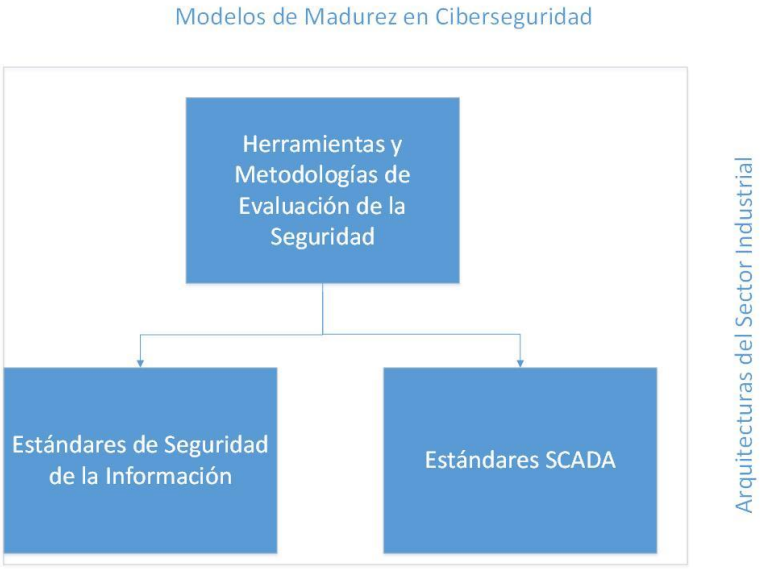
Según Knapp y Langill (2015). Las auditorías de seguridad se realizan probando un sistema en particular en las políticas, procedimientos, normas o reglamentos. Estas son desarrolladas sobre la base del conocimiento de las amenazas y vulnerabilidades "conocidas". Ellas son también complicadas aún más por el hecho de que una vez que una amenaza nueva, emergente o sofisticada es descubierta, puede tomar tiempo para que los documentos se ajusten de cualquier deficiencia que la amenaza puede haber explotado. Las auditorías no suelen revelar vulnerabilidades latentes por este motivo. Las auditorías pueden realizarse utilizando técnicas de recolección activas teniendo acceso directo al (los) sistema (s) considerado (s), o técnicas pasivas que comúnmente emplean cuestionarios y listas de verificación. Por esta razón, las auditorías generalmente no requieren tantos recursos como para llevar a cabo una evaluación o prueba de seguridad más completa.

Según Knapp, et al (2015). Las auditorías de seguridad se realizan probando las políticas, procedimientos y estrategias, teniendo como base el conocimiento de las amenazas y vulnerabilidades "conocidas", donde comúnmente se emplean cuestionarios y listas de verificación. La preocupación por las amenazas cibernéticas ha llevado a unas publicaciones de estándares y regulaciones de seguridad como NERC CIP, CFATS, ISO/IEC 27002:2005, NRC RG 5.71, y NIST 800-82 proporcionan controles para administrar los riesgos cibernéticos. Sin embargo, la gran mayoría de estas publicaciones se dirigen a la gestión de los riesgos, protección de la

información, en un proceso que se conoce más comúnmente como seguridad de la información (o aseguramiento de la información). Para proteger los sistemas de control industrial, hay dos razones predominantes por las que estas publicaciones no pueden aplicarse directamente a entornos de sistemas de control industrial; la primera es que en la aplicación de los controles de seguridad se debe priorizar la disponibilidad que la confidencialidad por razones económicas; la segunda es que un principio de seguridad de los sistemas de control industrial es el diseño para la seguridad humana y protección del medio ambiente, estos sistemas deben ser seguros incluso en un estado de inseguridad. Según Knowles, et al (2015) los métodos de evaluación del riesgo de seguridad cibernética para SCADA pueden mejorarse en términos de abordar el contexto, el establecimiento del proceso de gestión de riesgos; superación orientación de ataque o falla; factor humano; la captura y formalización de expertos; la mejora de la fiabilidad de los sistemas de datos probabilísticos; evaluación y validación; y herramientas de soporte. Cherdantseva et al (2016).

Según Knowles et al (2015). La preocupación por las amenazas cibernéticas ha llevado a unas publicaciones de seguridad que proporcionan orientación y establecen normas para administrar los riesgos cibernéticos. Sin embargo, la gran mayoría de estas publicaciones se dirigen a la gestión de los riesgos protección de la información, en un proceso que se conoce más comúnmente como seguridad de la información (o aseguramiento de la información). En términos precisos, estos son procesos separados: La garantía de la información es el proceso de evaluación y gestión del riesgo para los activos de información a nivel de seguridad de la información es un subproceso dentro del aseguramiento. En la práctica, sin embargo, el término seguridad de la información se utiliza comúnmente para referirse a ambos procesos. Figura 2. Aunque muchos de los paradigmas inherentes a la seguridad de la información son análogos a los requeridos para proteger los sistemas de control industrial, hay dos razones predominantes por las que estas publicaciones no pueden aplicarse directamente a entornos de sistemas de control industrial; la primera es que en la aplicación de los controles de seguridad se debe priorizar la disponibilidad que la confidencialidad por razones económicas; la segunda es que un principio de seguridad de los sistemas de control industrial es el diseño para la seguridad humana y protección del medio ambiente, estos sistemas deben ser seguros incluso en un estado de inseguridad.

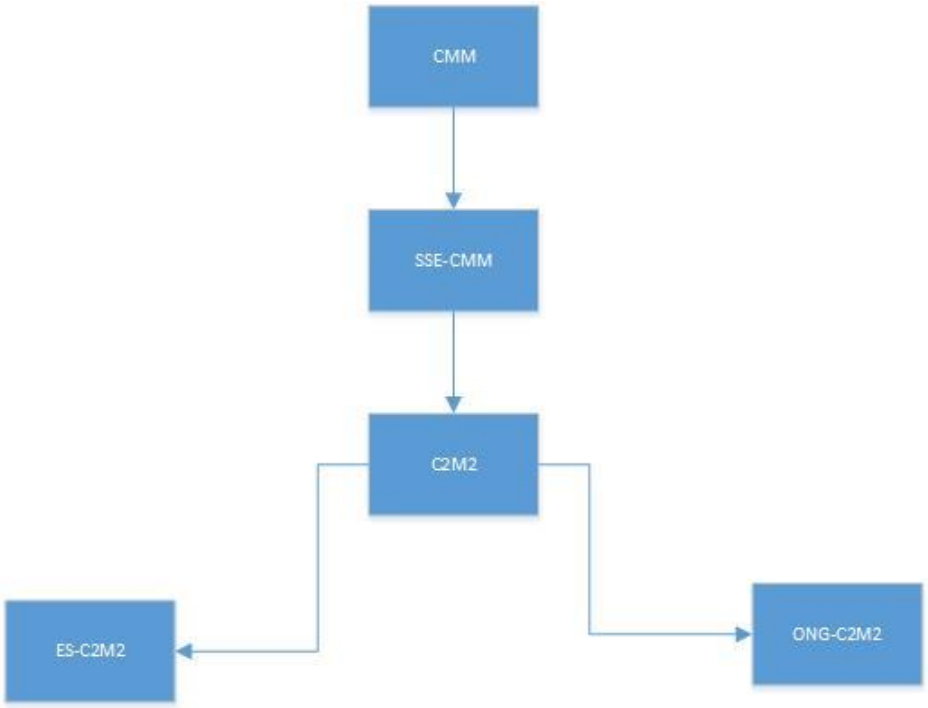
Figura 2. Aplicabilidad de los modelos de madurez en el sector industrial. Elaboración propia.



Según Proençaa, y Borbinhaa (2016). El modelo de madurez es una técnica que provee las herramientas necesarias para evaluar y medir diferentes aspectos de un proceso o una organización, puede ser utilizado para auditoria y mejoramiento, progreso en la obtención de los objetivos.

Según Knowles, et al. (2015). Resaltan que el modelo de madurez CMM (Capability Maturity Model) permite describir la madurez de variados procesos del negocio, originalmente creado para el desarrollo de software, esta ha sido aplicado para crear una multitud de modelos. Un ejemplo es el SSE-CMM utilizado para evaluar los procesos de ingeniería en seguridad, y esta estandarizado como el ISO / IEC 21827, al tener un ámbito universal tiene una serie de limitaciones para ser aplicado a los sistemas de seguridad de control industrial; cómo es que se ignora la heterogeneidad de las organizaciones y consolida en un solo modelo el desarrollo de software, la ingeniería de sistemas, procesos, desarrollo de productos y el abastecimiento de proveedores, teniendo en cuenta estos limitantes se ha creado el modelo C2M2, mediante el cual se ha desarrollado el modelo ES-C2M2 específico para el sector eléctrico y el ONG-C2M2 para el sector de la industria del petróleo y gas Figura 3; en estos modelos se han desarrollado una herramienta de autoevaluación, en donde se realizan una serie de preguntas sobre las capacidades en seguridad y se genera un informe con las potenciales brechas en seguridad.

Figura 3. Evolución de los modelos de madurez. Elaboración propia.



Una mejora del CMMI es el estándar C2M2, Modelo de Madurez en Ciberseguridad, fue propuesto por la universidad Carnegie Mellon en el Instituto de Ingeniería del Software SEI, el origen de este es el modelo ES-C2M2, subsector de energía, desarrollado y liderado por el departamento de energía DOE con el apoyo de la casa blanca y en asocio con el departamento de seguridad nacional DHS, y con la colaboración de expertos del sector público y privado. Muneer (2014).

El instituto nacional de estándares (NIST) elaboró una serie de normas o directrices con aplicación a los sistemas de control la norma NIST 800-82 supervisión Control y adquisición de datos (SCADA) sistemas de control distribuidos (DCS) y otros sistemas de control configurables como los controladores lógicos programables (PLC). Según Knowles, et al. (2015) NISTSP 800-82 proporciona orientación y desarrollo de los planes de seguridad en los sistemas de control industrial.

El Modelo C2M2 puede ayudar a las organizaciones de todos los sectores, tipos, tamaños a evaluar y hacer mejoras en los programas de seguridad de la información; el cual se centra en la implementación y gestión de las mejores prácticas de seguridad cibernética asociados a la gestión de la información, la gestión de las operaciones, los activos y los entornos en los que operan. Este

modelo puede utilizarse para que las organizaciones incrementen las capacidades en ciberseguridad, evaluar de manera efectiva, consistente y capacidades en ciberseguridad, compartir los conocimientos, mejores prácticas y la identificación pertinente de los procesos en las organizaciones como una forma para mejorar las capacidades de ciberseguridad y permite establecer las acciones para priorizar las inversiones y mejorar la seguridad cibernética. Curtis y Mehravari (2015).

Según Knapp y Langill (2015). Las auditorías de seguridad se realizan probando un sistema en particular en las políticas, procedimientos, normas o reglamentos. Estas son desarrolladas sobre la base del conocimiento de las amenazas y vulnerabilidades "conocidas". Ellas son también complicadas aún más por el hecho de que una vez que una amenaza nueva, emergente o sofisticada es descubierta, puede tomar tiempo para que los documentos se ajusten de cualquier deficiencia que la amenaza puede haber explotado. Las auditorías no suelen revelar vulnerabilidades latentes por este motivo. Las auditorías pueden realizarse utilizando técnicas de recolección activas teniendo acceso directo al (los) sistema (s) considerado (s), o técnicas pasivas que comúnmente emplean cuestionarios y listas de verificación. Por esta razón, las auditorías generalmente no requieren tantos recursos como para llevar a cabo una evaluación o prueba de seguridad más completa.

A continuación, en la tabla 2, se describen cada uno de los conceptos que son aplicables a la industria manufacturera y el comparativo de si son abordados por los siguientes modelos de madurez.

Tabla 2. Comparativos modelos de madurez aplicables a la industria manufacturera. Elaboración propia.

Dominio / Modelos	**NICE CMM**	**C2M2**	**ISM3**	**ISO/IEC 21827 SSE CMM**	**COBIT MATURITY MODEL**	**Observaciones**
Evaluación de los procesos	SI	SI	SI	SI	SI	Los procesos analizados son evaluados y describen su nivel de madurez.
Evaluación de las estrategias	SI	SI	SI	SI	SI	Las actividades para la mitigación de los riesgos son evaluadas.
Clasificación de los activos según su criticidad	NO	SI	NO	SI	NO	Se identifican los activos por el impacto, riesgo en seguridad, vulnerabilidad y posibles amenazas.
Evaluación de la infraestructura	SI	SI	SI	NO	NO	Los procesos son evaluados y soportados por un equipo de trabajo en donde se planean las actividades.
Evaluación de las políticas	SI	SI	SI	SI	SI	Las políticas son evaluadas calificadas apropiadamente.
Evaluación de la implementación	NO	SI	SI	NO	SI	Los procesos de implementación son calificados.
Evaluación de las pruebas	NO	SI	SI	SI	SI	Las pruebas de implementación son evaluadas y calificadas.
Evaluación de los riesgos	SI	SI	NO	SI	SI	Los riesgos son evaluados según al programa de administración de riesgos.
Los riesgos son identificados y documentados	NO	SI	NO	NO	NO	Los riesgos tienen un programa de administración de riesgos.
Evaluación capacitación y sensibilización personal.	SI	SI	SI	SI	SI	Las habilidades, capacitación y sensibilización al personal son evaluadas.
Evaluación de los recursos	NO	SI	NO	NO	NO	Los recursos están identificados y evaluado su impacto.
Evaluación de gestión de incidentes	NO	SI	SI	SI	NO	Los incidentes están gestionados y evaluados su impacto.
Evaluación operacional	NO	SI	SI	SI	SI	Las actividades y políticas operacionales son evaluadas.

Tabla 2. Comparativos modelos de madurez aplicables a la industria manufacturera. Elaboración propia.

Dominio / Modelos	**NICE CMM**	**C2M2**	**ISM3**	**ISO/IEC 21827 SSE CMM**	**COBIT MATURITY MODEL**	**Observaciones**
Evaluación Seguridad física	NO	SI	SI	SI	SI	Las medidas de control físicas son evaluadas.
Evaluación control de acceso	SI	SI	SI	SI	SI	Las políticas de control de acceso son evaluadas.
Evaluación Forense.	NO	NO	SI	NO	NO	Las actividades forenses después de un incidente son evaluadas.
Aseguramiento de la calidad	NO	SI	NO	SI	SI	Hay una gestión de aseguramiento de la calidad.
Evaluación de la línea base	NO	SI	NO	SI	SI	Se evalúa la línea base de seguridad de la infraestructura.
Evaluación de continuidad de las operaciones	NO	SI	NO	NO	NO	Se evalúan los procedimientos de continuidad de las operaciones en caso que alguno falle.
Evaluación de la información compartida y las comunicaciones	NO	SI	NO	NO	NO	Se evalúan los datos y la información compartida con otros entes.
Herramienta de autoevaluación con reporte de estado madurez	NO	SI	NO	NO	NO	Se tiene herramienta que permite calificar y evaluar cada uno de los elementos de seguridad involucrados en la seguridad de la infraestructura y genera reporte del estado de madurez.
Indicador Niveles de madurez	3	5	5	5	5	Cantidad de niveles que son evaluados.

En la tabla 3 se realiza un comparativo entre los dominios del modelo de madurez C2M2 y los controles de NIST 800-82, teniendo en cuenta que se deben evaluar los sistemas SCADA, donde estos modelos abordan a este tipo de infraestructuras, las cuales integran elementos de TI como de OT.

Tabla 3. Comparativo modelo de madurez C2M2 y controles NIST 800-82. Elaboración propia.

Dominio C2M2	Descripción	NIST 800-82 Controles
Gestión de riesgos	Definir, gestionar y mantener un programa de gestión de riesgo de seguridad cibernética de la empresa para identificar, analizar y mitigar el riesgo de ciberseguridad para la organización, incluyendo sus unidades de negocios, subsidiarias, infraestructura interconectada relacionada y partes interesadas.	Evaluación de riesgos. (RA) Protección física y medioambiental (PE).
Gestión de activos, cambios y configuración	Administrar los activos de TI y OT de la organización, incluyendo tanto hardware como software, en consonancia con el riesgo para la infraestructura crítica y los objetivos de la organización.	Administración de la configuración (CM). Mantenimiento (MA).
Gestión de Identidad y Acceso	Crear y gestionar identidades para entidades a las que se les puede conceder acceso lógico o físico a los activos de la organización. Controlar el acceso a los activos de la organización, en consonancia con el riesgo para la infraestructura crítica y los objetivos organizacionales.	Evaluación de seguridad y autorización (CA). Adquisición de sistemas y servicios (SA). Seguridad del personal (PS). Identificación y autenticación (IA). Control de acceso (AC). Auditoria y responsabilidad (AU).
Gestión de amenazas y vulnerabilidades	Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas y vulnerabilidades de la seguridad cibernética, en consonancia con el riesgo para los objetivos de infraestructura de la organización (por ejemplo, críticos, informáticos, operacionales).	Protección física y medioambiental (PE). Plan de contingencia (CP). Integridad de los sistemas y la información (SI). Protección medios (MP). Protección de sistemas y comunicaciones.
Conciencia de Seguridad	Establecer y mantener actividades y tecnologías para recopilar, analizar, alarmar, presentar y utilizar información operacional y de ciberseguridad, incluyendo información de estado e información resumida de los otros dominios modelo, para formar una imagen operativa común.	Seguridad del personal (PS). Protección física y medioambiental (PE). Conciencia y Entrenamiento (AT).

Tabla 3. Comparativo modelo de madurez C2M2 y controles NIST 800-82. Elaboración propia.

Dominio C2M2	Descripción	NIST 800-82 Controles
Intercambio de Información y Comunicaciones	Establecer y mantener relaciones con entidades internas y externas para recopilar y proporcionar información sobre seguridad cibernética, incluyendo amenazas y vulnerabilidades, para reducir riesgos y aumentar la resiliencia operacional, proporcional al riesgo para la infraestructura crítica y los objetivos organizacionales.	
Respuesta a eventos e incidentes, continuidad de las operaciones	Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de ciberseguridad y para mantener las operaciones a lo largo de un evento de seguridad cibernética, proporcional al riesgo para la infraestructura crítica y los objetivos organizacionales.	Protección física y medioambiental (PE). Plan de contingencia (CP). Integridad de los sistemas y la información (SI). Respuesta de incidentes (IR).
Gestión de la Cadena de Suministro y Dependencias Externas	Establecer y mantener controles para manejar los riesgos de seguridad cibernética asociados con servicios y activos que dependen de entidades externas, proporcional al riesgo para la infraestructura crítica y los objetivos organizacionales.	
Administración de personal	Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de seguridad cibernética y asegurar la idoneidad y la competencia del personal, en consonancia con el riesgo para la infraestructura crítica y los objetivos organizacionales.	Seguridad del personal (PS). Conciencia y Entrenamiento (AT).
Gestión del Programa de Seguridad Cibernética	Establecer y mantener un programa de seguridad cibernética de la empresa que proporcione gobernabilidad, planificación estratégica y patrocinio para las actividades de seguridad cibernética de la organización de manera que alinee los objetivos de seguridad cibernética con los objetivos estratégicos de la organización y el riesgo a la infraestructura crítica.	Planear (PL). Administración Programa (PM). Plan de contingencia (CP). Integridad de los sistemas y la información (SI).

En la fabricación de productos, los procesos de (diseño, control de calidad, suministro y personal) el acceso a la información por parte de entidades no autorizadas o externas es crucial en el panorama competitivo actual. La divulgación de negocios, datos críticos de producción, información a competidores y adversarios podría causar una pérdida de la ventaja competitiva y la

relevancia del mercado. En consecuencia, la protección, la preservación de la información patentada es vital para la competitividad de una empresa. Uchenna, et al (2017); Shin et al.(2016).

Según la revista de la OMPI (Organización Mundial para la Propiedad Intelectual), en su edición de mayo de 2005. En todos esos productos se aplican los conocimientos especializados y creatividad, siendo este un valor de capital intelectual para su creación y comercialización, sin embargo, las empresas no dan la importancia a la protección de esos activos intelectuales. En el entorno actual la fuente principal de ventajas competitivas para las empresas, viene de la mano de la innovación y de las expresiones creativas originales. La gestión y el uso estratégico de derechos de P.I. (Propiedad Intelectual) para reducir riesgos, que constituye el no registro de los diseños, con esto se puede impedir que otros los exploten económicamente.

En el estudio realizado en 2011 por CIDETEXCO, sobre las tendencias tecnológicas para los próximos 10 años en el ciclo de vida del producto (CPV), para la industria fibra textil y confección. La gestión del CVP corresponde a la implementación de modelos para la práctica moderna de la ingeniería de fabricación, con el objetivo de gestionar el ciclo de vida integral, es decir, de las empresas, sus productos, procesos de fabricación y servicios en un modelo de producción limpia y sostenible Tabla 4, Tabla 5, Tabla 6 y Tabla 7. El ciclo inicia con la extracción y selección de materiales, posteriormente se pasa a la fase de diseño de producto, la cual parte del desarrollo de los conceptos hasta la optimización de los sistemas de final de vida del producto, una vez culminada esta fase se da inicio al proceso de manufactura, empaque y distribución, hasta llegar al usuario final donde se tiene en cuenta el uso y mantenimiento que éste le da al producto. Culminado ese proceso llega la eliminación. Según Pineda y Jara (2010). En los procesos realizados en la industria textil que se encuentran automatizados, en el cual se convierte el algodón como fibra natural en un producto fino alargado, resistente y flexible; convirtiéndolo en tela, para llegar a este estado se detallan los siguientes procesos:

Desempacado: Consiste en la separación de las fibras y la limpieza de impurezas, que se realiza mediante el soplado de aire a alta velocidad.

Cardado: Proceso que termina de separar las fibras, estas pasan entre dos cilindros cada vez a mayor velocidad para adelgazarla.

Peinado: Proceso que se aplican a las cardas largas, se ordenan y orientan en la orientación del hilo.

Trenzado: La carda se pasa por la mecha que hace la primera torsión, se reduce el volumen, el producto entregado es llamado mecha.

Hilatura: La fibra se estira y se unen varios de ellos por medio de la aplicación de torsión.

Acabado: Consiste en retorcer la fibra cuando se unen hilos de varios cabos.

Enconado: El hilo se devana en uno o varios conos.

Engomado: Proceso que aplica químicos a la fibra con el fin de aplicarle una textura determinada para el producto a elaborar.

Urdimbre: Es el proceso de plegar los hilos antes de realizar el tejido.

Tejido: Es el proceso de entrelazar los hilos de acuerdo con la trama, luego este se enrolla como tela.

Teñido: Se impregna colorantes a la tela en forma uniforme, por medio de máquinas de proceso continuo.

Estampado: Proceso de aplicación de tramas de color o diseños a la tela.

Corte: Proceso de elaboración de patrones en la tela para realizar prendas.

Tabla 4. Tendencias Tecnológicas en la manufactura. Manufactura adaptativa. CIDETEXCO (2011).

Corto Plazo	Mediano Plazo	Largo Plazo
Sistemas de fabricación modulares y reconfigurables.	Máquinas de prototipo rápido y equipos de alta precisión.	Fábricas adaptativas y reconfigurables (en tiempo real y en ubicaciones virtuales).
Sistemas de control escalable e inter operables.	Sistemas híbridos de producción para la fabricación y el montaje y desmontaje de productos, con base robótica y / o tecnología de automatización.	Fabricación de alta precisión.
Equipos de producción adaptativa y flexible, sistemas e instalaciones para (re) configuraciones rápidas.	Esquemas de Auto Organización y Auto Optimización de procesos en plantas de manufactura.	Desarrollo de una nueva generación de sistemas de auto-aprendizaje basados en conocimiento.
Nuevas tecnologías de fabricación de alto rendimiento en términos de eficiencia (volúmenes, velocidad, la capacidad del proceso y precisión).	Sistemas electrónicos con monitoreo de las tecnologías digitales.	Integración de modelos de simulación in situ de los procesos de fabricación.
Metodologías y herramientas para la fabricación basada diseño de sistemas reconfigurables.	Sistemas de sensores para control de planta.	
Instrumentos para la planificación de la producción y la simulación in situ.		

Tabla 5. Tendencias Tecnológicas en la manufactura. Ingeniería digital en manufactura.

CIDETEXCO (2011).

Corto Plazo	Mediano Plazo	Largo Plazo
Ingeniería de fabricación digital	Prototipado rápido y virtual.	Modelado y proceso multi-escala para el desarrollo de nuevos productos.
Ingeniería de productos digitales.	Modelos de gestión de datos (Ciclo de Vida de Gestión de Datos).	Simulación y gestión con el enfoque holístico de la ingeniería de fabricación.
Sistemas de integración 3D/CAD en herramientas de ingeniería de producción.	Integración de tecnologías heterogéneas y autónomas.	Producción cero-defectos.

Desarrollo de prototipos digitales para productos virtuales.	Herramientas para la planificación, diseño y fabricación en los estados digitales y virtuales del producto.	Alta capacidad y alto rendimiento mediante simulación basada en la ciencia.
	Sistema avanzado e interactivo de interfaz gráfica de usuario para diseño y simulación de productos.	
	Integración y sincronización de la fábrica digital con datos en tiempo real.	

Tabla 6. Tendencias Tecnológicas en la manufactura. Tecnologías emergentes. CIDETEXCO (2011).

Corto Plazo	**Mediano Plazo**	**Largo Plazo**
Modelos de alto rendimiento en las tecnologías tradicionales.	Desarrollo de superficies funcionales que optimicen los procesos de manufactura basado en el conocimiento de herramientas para la planificación del proceso.	Procesos emergentes y generativos basados en la ingeniería del conocimiento y la innovación.
Sistemas para bajo consumo de energía.	Simulación integrada de manufactura.	Sistemas de control de procesos basados en la cognición de alta precisión.
Tecnologías de recolección de residuos para permitir la implementación de procesos de producción limpia.	Bioprocesos en las cadenas de producción de la industria FTC.	Fabricación 100% confiable, estandarizada, certificada en procesos y con sellos ambientales propios.
	Miniaturización de los componentes con apoyo de ingeniería mecatrónica.	Nueva interfaz humano-máquina para la cooperación en ambientes industriales avanzados.
	Plena integración de los materiales avanzados apoyados en la ingeniería de materiales.	Sistemas de medición inteligente para la fabricación cero defectos.
		Herramientas para toma de decisiones para la fabricación de cero defectos.
		Sistemas de Computación Ubicua y Quántica para producción y manufactura.
		Máquinas de producción inteligente.

Tabla 7. Tendencias Tecnológicas en la manufactura. Tic's para manufactura. CIDETEXCO (2011).

Corto Plazo	Mediano Plazo	Largo Plazo
Automatización de proceso con control para adaptación y tolerancia de fallos.	Desarrollos informáticos y tecnológicos integrados para la fábrica digital y virtual.	Red de fabricación destinada a la migración de las tecnologías de fabricación envolvente.
Sistemas de configuración destinados a la producción y personalización de servicios.	Aplicaciones láser para diseño en manufactura FTC.	Herramientas de producción en red de alta flexibilidad.
Métricas para desarrollo de software en producción específica en FTC.	Pruebas a gran escala y la validación de la fabricación robótica automatizada y automatización de los procesos de post-producción.	Sistemas de adaptación y de respuesta interfaz hombre-máquina.
Sistematización y estandarización de procesos.	Sistemas de simulación, optimización y tecnologías de visualización de productos virtuales.	Computación Ubicua y Quántica.
	Herramientas para convertir la fábrica digital y virtual a la realidad.	
	Bibliotecas digitales y contenidos de la ingeniería de la fabricación para la industria.	
	Tecnologías de modelado y arquitecturas abiertas.	
	Red multimodal de entornos de fabricación destinados a la mejora de las interfaces humano-máquina.	

2. Metodología

2.1 Identificar todos los elementos de seguridad del modelo de madurez que pueden causar los riegos de seguridad, agrupándolos en dominios, según su relación e impacto, tomando como referencia el modelo C2M2, para la industria manufacturera del sector textil.

En el desarrollo de los objetivos en la metodología aplicada se presentan elementos cualitativos y cuantitativos, se realizó un comparativo de los diferentes modelos de madurez existentes, se evalúan conceptos, herramientas y elementos existentes en estos, que puedan ser aplicados a la industria manufacturera del sector textil, adquiriendo su conocimiento con el estudio de los procesos, información, conocimiento organizacional e infraestructura que impactan la seguridad Figura 4.

Figura 4. Conocimiento de la industria manufacturera del sector textil. Elaboración propia.

Se definieron dos procesos en los cuales se trabajaron, el uno fue el identificar y el otro evaluar en un caso de estudio, lo que nos llevó a realizar los siguientes pasos:

Identificar. En el cual se realizó un análisis de cada uno de los elementos de seguridad que impactan la gestión de los sistemas SCADA; se determinó por medio de una calificación cuantitativa cuál de los modelos se cumplió con la mayor cantidad de elementos que se tiene en cuenta para su evaluación Tabla 2; a continuación y teniendo en cuenta que se deben evaluar los sistemas SCADA, se compararon los modelos C2M2 y la NIST 800-82 Tabla 3, que son los modelos de madurez que abordan este tipo de infraestructuras; en este análisis, se encontraron elementos de seguridad que se tuvieron en cuenta para la adaptación del modelo Tabla 8; luego se caracterizaron los elementos, estableciendo relaciones que les permitieran agruparlos en dominios y modelar un borrador del modelo para ser aplicado en la industria manufacturera del sector textil.

2.2 Crear una adaptación del modelo C2M2, que permita evaluar el nivel de madurez en ciberseguridad para identificar las capacidades instaladas a todos los elementos que puedan afectar la gestión de los sistemas SCADA.

Teniendo el borrador del modelo y utilizando el método empírico-analítico; luego se identificaron los elementos que puedan ser evaluados y analizados, por medio de una encuesta a cada una de las áreas involucradas en cada uno de los procesos que se realizan, estableciendo una relación con los elementos definidos en el modelo C2M2, teniendo una referencia de las capacidades instaladas en los diferentes procesos de la industria que se analizó y que involucran la gestión de los sistemas SCADA; para realizar este proceso se llevaron a cabo las siguientes actividades:

Se analizaron y compararon los elementos que afectan la gestión de la ciberseguridad en la industria analizada con el borrador del modelo propuesto.

Se verificó el impacto y la pertinencia de los elementos definidos en el borrador, se clasificaron los elementos en dominios y se modelaron los niveles de evaluación para los elementos definidos.

2.3 Desarrollar una herramienta y las pruebas de la adaptación del modelo por medio de encuestas, para la evaluación del modelo sugerido en un caso de estudio, con el fin de medir el nivel de madurez y capacidades instaladas en ciberseguridad de los elementos que componen la gestión de los sistemas SCADA.

Teniendo los elementos clasificados en dominios y los niveles de evaluación que se van a aplicar a los elementos identificados, se procedió a verificar la evaluación en un caso de estudio mediante el cual se permita identificar la pertinencia de los elementos identificados en el modelo propuesto, debilidades, fortalezas y mejoras a realizarle, con los siguientes procesos:

Se Verificó el modelo propuesto utilizando un caso de estudio con el fin de identificar los elementos que impactan, su pertinencia y la afectación a la seguridad.

Se modelaron las pruebas de validación del modelo.

Se elaboró encuesta a los funcionarios que pueden afectar para identificar la pertinencia de los elementos identificados del modelo propuesto en el caso de estudio.

Se realizaron ajustes a los elementos y dominios, teniendo en cuenta los resultados de la encuesta.

Se realizó evaluación con la herramienta propuesta a un caso de estudio.

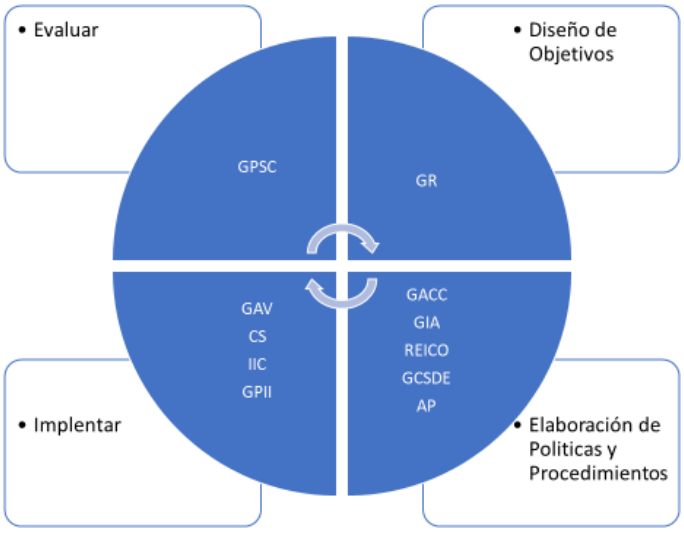
Se analizaron los resultados obtenidos para determinar la madurez, las capacidades instaladas en la gestión de los sistemas SCADA, su pertinencia en el sector y su impacto.

Se evaluaron por medio de un caso de estudio, los diferentes elementos con el fin de determinar el nivel de madurez en la gestión de estos sistemas, identificando las posibles falencias que se tienen en las políticas, procedimientos o medidas correctivas, que puedan causar un riesgo a la seguridad de la información, se definió una herramienta que por medio de un trabajo experimental permitió evaluar su aplicación en estos ambientes en un caso de estudio. Por medio de un método

inductivo se analizaron las necesidades propias de este sector para identificar los elementos que afectan la seguridad y proponer una adaptación del modelo que evaluó su madurez en ciberseguridad.

Se mostró como por medio de la herramienta se puede realizar una auditoría y evaluación del nivel de madurez en ciberseguridad del sector textil, donde se pueden analizar los riesgos de las amenazas, ataques, su impacto e importancia; por medio de un informe que genera los resultados de esta evaluación en donde se plasman las recomendaciones que se deben tener en cuenta para adquirir un nivel de madurez, con este se pueden establecer estrategias que permitan gestionar y mitigar los riesgos en estos sistemas productivos. Cuando se evalúa el nivel de madurez, este debe ser un proceso de ejecución constante iniciando con el diseño de objetivos, elaboración de políticas y procedimientos, implementar y evaluar Figura 5, además se crea conciencia en la gestión de estos sistemas, teniendo como premisa el no perder la confidencialidad, integridad y disponibilidad.

Figura 5. Proceso de evaluación nivel de madurez. Elaboración propia.



Con la herramienta de evaluación del nivel de madurez se creó una referencia del estado de los procesos, permitió así poder identificar las falencias para así tener un insumo para diseñar estrategias y controles eficientes y eficaces, para poder tomar las decisiones correctas, establecer

prioridades para la atención de los incidentes, restaurar los servicios afectados a su estado original y evitar los incidentes que impacten el servicio.

3. Resultados

En la tabla 8 se especifican los elementos identificados para la industria del sector textil, teniendo como referencia el modelo C2M2:

Tabla 8. Relación dominios y objetivos. Modelo C2M2 (2014).

Dominio	Objetivos
Gestión de riesgos.	Establecer la estrategia, gestionar y las actividades.
Gestión de activos, cambios y configuración.	Gestión, administrar la configuración, administrar los cambios y las actividades.
Gestión de Identidad y Acceso.	Establecer y mantener identidades, control de acceso y las actividades.
Gestión de amenazas y vulnerabilidades.	Identificar y responder a las amenazas, reducir las vulnerabilidades y las actividades.
Conciencia de Seguridad.	Registrar, monitorear, establecer línea base y las actividades.
Intercambio de Información y Comunicaciones.	Compartir información y las actividades.
Respuesta a eventos e incidentes, continuidad de las operaciones.	Detectar eventos, escalar, responder, plan de continuidad y actividades.
Gestión de la Cadena de Suministro y Dependencias Externas.	Identificar las dependencias, administrar el riesgo de dependencia y las actividades de gestión.
Administración de personal.	Asignar responsabilidades, control del ciclo de vida de la fuerza de trabajo, desarrollar la fuerza laboral, aumentar la conciencia y las actividades de gestión.
Gestión del Programa de Seguridad Cibernética.	Establecer la estrategia del programa de ciberseguridad, patrocinio, establecer y mantener la arquitectura, realizar el desarrollo de software seguro y las actividades de gestión.

En el análisis del modelo C2M2 y el estándar NIST 800-82, se encontraron los siguientes elementos de seguridad que se tuvieron en cuenta para la adaptación del modelo, específicamente para la industria de la manufactura sector textil, utilizando el método empírico-analítico, se evaluaron cada uno de los elementos de seguridad. Para la identificación de los elementos de seguridad propios de esta industria, se realiza una entrevista Tabla 9, teniendo en cuenta la siguiente plantilla con estas preguntas.

Tabla 9. Plantilla entrevista usuarios. Elaboración propia.

Entrevista Usuarios	
Objetivo: Esta entrevista tiene como propósito lograr que los usuarios expresen las ideas, experiencias y elementos que se logran identificar en sus actividades cotidianas, con el fin de que sirvan de insumo para identificar los elementos que pueden causar riesgos.	
Cargo.	
Área.	
Funciones.	
Casos que se presentan en el área que afectan la operación normal.	
A que otras áreas de la empresa afectan los procesos.	
A que otras entidades externas a la empresa, afectan sus procesos, cuales.	
Si se presenta un inconveniente que procedimiento se sigue.	

En la Tabla 10 se especifican los dominios y elementos de seguridad a evaluar en el modelo de madurez propuesto para la industria manufacturera del sector textil que utiliza sistemas SCADA.

Tabla 10. Dominios y elementos del modelo de madurez propuesto. Elaboración propia.

Dominio	Elementos
Gestión de riesgos	Identificar, Evaluar, Priorizar, Determinar el impacto, Definir estrategias de monitoreo, Definir los niveles de respuesta.
Gestión de activos, cambios y configuración	Identificar, Definir su función, Identificar características, Determinar la línea base de configuración.
Gestión de Identidad y Acceso	Aprovisionamiento, Desaprovisionamiento, Seguimiento y verificación a las identidades y accesos, Definición de requisitos para el acceso, Documentar los accesos, Definir responsables y políticas.
Gestión de amenazas y vulnerabilidades	Definir e identificar las fuentes de información de amenazas, Definir política para la interpretación de la información obtenida y determinar su impacto, Establecer los controles, Definir perfiles de amenazas, su impacto y prioridades.
Conciencia de Seguridad	Definir el registro y monitoreo de la línea base operativa, Establecer los parámetros de comportamiento anómalo, Definir las alarmas y alertas que identifican los eventos.
Intercambio de Información y Comunicaciones	Definir las políticas para compartir información, que, quién, a quienes y como, Establecer los procedimientos para el intercambio de información, proteger y asignar responsables.
Respuesta a eventos e	Definir y revisar periódicamente los procedimientos y planes para la detección de los eventos, Establecer los criterios a tener en cuenta en la que los eventos

incidentes, continuidad de las operaciones	pueden afectar los servicios y correlacionar eventos para identificar patrones, Definir los procedimientos para la atención de los incidentes y su escalamiento, Definir procedimientos y planes de continuidad.
Gestión de la Cadena de Suministro y Dependencias Externas	Identificar los riesgos de los proveedores, Establecer controles que permitan mitigar los riesgos asociados a los proveedores, Definir y verificar los acuerdos de nivel de servicio.
Administración de personal	Definir las políticas de gestión de la seguridad, contratación, capacitación al personal y responsabilidades, Establecer procedimientos para sensibilización.
Gestión del Programa de Seguridad Cibernética	Definir las estrategias de seguridad con políticas y planes, Realiza verificación, mantenimiento y actualización.
Gestión de la Protección de la Propiedad Industrial e Intelectual	Definir las estrategias y procesos para la protección de la propiedad industrial, nombrar los responsables de cada actividad y realizar una revisión periódica de estas, para que estén alineadas con las políticas de la organización.

Los resultados tabulados de las entrevistas se pueden encontrar en el archivo de Excel anexo Entrevista.xls, en donde se detallan cada uno de los temas abordados. En la tabulación de la entrevista se logró establecer los elementos que son importantes a tener en cuenta, todos ellos se agruparon en un nuevo dominio llamado Gestión de la Protección de la Propiedad Industrial e Intelectual con el propósito de establecer y mantener un proceso definido con planificación estratégica para las actividades de registro y protección de la propiedad industrial e intelectual en los diferentes procesos de diseño, modelado y prototipado de los productos que van a ser producidos de tal manera que se alinee con los requisitos, cumpla con las calidades y cualidades en su fabricación.

Un programa de Gestión de la Protección de la Propiedad Industrial e Intelectual es un grupo integrado de actividades diseñadas y administradas para cumplir los objetivos de protección de la propiedad para la organización y / o la función. Un programa de protección de la propiedad puede implementarse en la organización o en el nivel de procesos, pero una implementación de nivel superior y un punto de vista empresarial pueden beneficiar a la organización al integrar actividades y aprovechar las inversiones de recursos en toda la empresa.

El dominio de la Gestión del Programa de Gestión de la Protección de la Propiedad Industrial e Intelectual comprende cuatro objetivos:

Establecer la estrategia de protección del modelado, prototipado y diseño.

Inversión del Programa de protección del modelado, prototipado y diseño.

Establecer y mantener la protección de la propiedad industrial e intelectual.

Actividades de gestión.

Establecer la estrategia de protección del modelado, prototipado y diseño.

La organización tiene una estrategia de programa de protección para la propiedad industrial e intelectual que puede ser desarrollada y administrada.

La estrategia del programa de protección de la propiedad industrial e intelectual define objetivos para cada una de las actividades en la organización.

La estrategia y prioridades del programa de protección de la propiedad industrial e intelectual están documentadas y alineadas con los objetivos estratégicos de la organización y los riesgos a que está expuesto este tipo de información.

La estrategia del programa de protección de la propiedad industrial e intelectual define el enfoque de la organización para proporcionar supervisión y gestión del programa para las actividades de seguridad.

La estrategia del programa de protección de la propiedad industrial e intelectual define la estructura y organización del programa de protección para esta información.

Las estrategias del programa de protección de la propiedad industrial e intelectual es aprobada por la alta dirección.

Las estrategias del programa de protección de la propiedad industrial e intelectual se actualizan para reflejar los cambios en los procesos, diseños y los modelos.

Inversión del programa de protección del modelado, prototipado y diseño.

Los recursos (personas, herramientas y financiación) se proporcionan, para apoyar el programa de protección de la propiedad industrial e intelectual.

La alta gerencia proporciona recursos para el programa de protección de la propiedad industrial e intelectual.

El programa de protección se establece de acuerdo con la estrategia del programa de seguridad.

Se proporcionan recursos adecuados (por ejemplo, personas y herramientas) para establecer, operar y gestionar un programa de protección de la propiedad industrial e intelectual y está alineado con la estrategia del programa.

Los recursos y presupuestos asignados por la alta dirección para el programa de protección de la propiedad industrial e intelectual es visible y es destacado (por ejemplo, es importante y se les da valor a las actividades y son comunicadas por la alta dirección).

Si la organización desarrolla o adquiere software, las prácticas seguras de desarrollo de software tienen recursos asignados para el programa de protección de la propiedad industrial e intelectual.

El desarrollo, mantenimiento y gestión de políticas de la propiedad industrial e intelectual tiene presupuesto asignado.

Se tiene asignado un rol de responsabilidad del programa de protección de la propiedad industrial e intelectual a un funcionario con autoridad.

El desempeño del programa de protección es monitoreado para asegurar que se alinee con la estrategia del programa de la propiedad industrial e intelectual.

El programa de protección es revisado por funcionarios independientes (es decir, por auditores que no están en el programa) para verificar el logro de los objetivos.

El programa de seguridad cumple y permite la consecución de la normatividad para la protección la propiedad industrial e intelectual.

El programa de seguridad monitorea y / o participa en estándares o iniciativas de protección de la propiedad industrial e intelectual de la industria.

Establecer y mantener la protección de la propiedad industrial e intelectual.

Se implementa una estrategia para realizar el registro de la propiedad industrial e intelectual.

Se han definido los requisitos que son necesarios para el registro de la propiedad industrial e intelectual.

Los requisitos se mantienen de acuerdo con un plan documentado.

La estrategia, procedimientos y requisitos se actualizan con frecuencia para mantenerla actualizada.

Actividades de gestión

Se siguen prácticas documentadas para las actividades de gestión del programa de protección de la propiedad industrial e intelectual.

Las partes interesadas en las actividades de gestión del programa de protección de la propiedad industrial e intelectual se involucran y se le asignan responsabilidades.

Se han identificado normas, procedimientos y directrices para informar las actividades de gestión del programa de protección de la propiedad industrial e intelectual.

Las actividades de gestión del programa de protección de la propiedad industrial e intelectual, se guían por políticas documentadas y directivas de la organización.

Las actividades de gestión del programa de protección de la propiedad industrial e intelectual se revisan periódicamente para garantizar que están conforme a las políticas establecidas por la organización.

El personal que realiza actividades de gestión del programa de protección de la propiedad industrial e intelectual, tiene las habilidades y conocimientos necesarios para desempeñar las responsabilidades asignadas.

La herramienta de evaluación se encuentra en el archivo de Excel anexo Evaluación del Caso de estudio – Valoración.xls, donde se definen cada uno de los elementos que pueden impactar cualquiera de los componentes que intervienen en la seguridad.

Los hallazgos encontrados en el caso de estudio en donde se describen las conclusiones y recomendaciones en la Tabla 11.

Tabla 11. Resultado de evaluación del nivel de madurez del caso de estudio. Elaboración propia.

Dominio	Resultados
Gestión de riesgos	En la de gestión de riesgos se presenta una baja madurez, se requiere planear una estrategia que permita evaluar, monitorear los riesgos y que estos se alineen con los objetivos de la organización.
Gestión de activos, cambios y configuración	Se debe realizar una mejor identificación de los activos y configuración, documentar las funciones que desempeñan en cada uno de los procesos para el cual está diseñado, identificar características y caracterizar la línea base de configuración.
Gestión de Identidad y Acceso	Se debe hacer seguimiento y verificación para los procesos de Desaprovisionamiento, identidades y accesos, levantar requisitos para el acceso.
Gestión de amenazas y vulnerabilidades	Se deben identificar las fuentes de información de amenazas, Definir los perfiles de amenazas, determinar su impacto y validarlas con las políticas de la organización, realizar evaluaciones frecuentes de vulnerabilidad para los activos importantes.
Conciencia de Seguridad	Se debe determinar el registro según el riesgo, compartir los registros con otros procesos organizacionales, definir los indicadores de actividad anómala de acuerdo con la línea base operativa, Definir e implementar las alarmas y alertas que identifican los eventos.
Intercambio de Información y Comunicaciones	Se deben establecer las políticas para compartir oportunamente información, definir las entidades externas para compartir y validar la información, documentar las actividades de intercambio de información según las políticas de la organización.
Respuesta a eventos e incidentes, continuidad de las operaciones	Definir el procedimiento y planes para la correlación de eventos, Establecer las políticas para coordinar con otras entidades, recopilación y preservación de pruebas, participar en ejercicios de seguridad con otras entidades.
Gestión de la Cadena de Suministro y Dependencias Externas	Definir las prioridades de las entidades externas, levantamiento de requisitos de seguridad para el desarrollo de software, proveedores y entidades externas, establecer políticas de acuerdos y notificación de incidentes, revisión y pruebas de seguridad a los activos adquiridos.
Administración de personal	Establecer en la evaluación de desempeño el criterio de responsabilidad en seguridad, definir funciones de seguridad a personal alterno, definir los procedimientos de seguridad cuando hay traslado de personal, implementar contenidos de conciencia en seguridad que se basen en los perfiles de amenaza.
Gestión del Programa de Seguridad Cibernética	Definir las estrategias para hacer partícipe a la dirección del patrocinio de las políticas de seguridad en el desarrollo, adquisición de software y mantenimiento, definir las políticas para que el programa de seguridad sea revisado, evaluado y verificado por personal experto que no participe del programa, definir protocolos de actualización periódica de la infraestructura.

Gestión de la Protección de la Propiedad Industrial e Intelectual	Establecer objetivos para cada una de las actividades en el programa de PPII, su supervisión, estructura y organización, definir políticas para que el programa sea revisado, evaluado y verificado por personal experto que no participe del programa.

4. Conclusiones y recomendaciones

4.1 Conclusiones

En el presente trabajo se logró proponer un modelo de evaluación de la madurez en ciberseguridad, mediante el cual se pueden identificar los elementos que pueden causar riesgos en la seguridad de la información, evaluando sus capacidades y su estado actual.

Al identificar y evaluar los elementos que intervienen en un sistema SCADA y su operación e iteración entre los sistemas de TI y TO para la industria manufacturera del sector textil, se puede comprobar su situación y capacidades de madurez en ciberseguridad, recopilando información relevante al estado de los diferentes procesos, controles y actividades que son susceptibles de riesgo y que necesitan ser controlados para mitigar sus vulnerabilidades, teniendo esta información se pueden identificar los aspectos susceptibles de mejora que pueden ser implementados para evitar los riesgos en seguridad.

Teniendo los elementos a ser evaluados se determinó por medio de una calificación cualitativa y cuantitativa, considerando el modelo C2M2, se estableció una escala de evaluación a cada elemento; con lo cual se tiene una referencia de las capacidades instaladas en los diferentes procesos de la industria que se analizó y que involucran la gestión de los sistemas SCADA y así determinar el nivel de madurez en la gestión de estos sistemas, identificando las posibles falencias que se tienen en las políticas, procedimientos o medidas correctivas, al proponer una herramienta por medio de un trabajo experimental permitió evaluar su aplicación en un caso de estudio; y por medio de un método inductivo se analizaron las necesidades propias de este sector para identificar los elementos que afectan la seguridad y proponer una adaptación del modelo que evaluó su madurez en ciberseguridad.

En la metodología aplicada para la elaboración de la herramienta para la evaluación del nivel de madurez en ciberseguridad del sector textil, se analizaron los diferentes modelos de madurez existentes, además de la entrevista y el estudio de caso analizado, luego utilizando un método empírico-analítico se determinaron los elementos que pueden ser aplicados a este sector, luego

estableciendo su relación se establecieron en dominios. Los diferentes elementos identificados permiten evaluar y realizar auditoria a cada uno de los aspectos, procedimientos y actividades que se deben tener en cuenta para la gestión en este tipo de infraestructuras. La gestión adecuada que se le deben dar a cada uno de los dominios identificados es de vital importancia, con el fin de mitigar las posibles falencias en la seguridad que se puedan presentar.

4.2 Recomendaciones

Los resultados de la evaluación pueden servir para generar un informe que permita identificar las fortalezas y debilidades en la gestión de este tipo de infraestructura y servir de insumo para generar mejores controles, establecer las estrategias, políticas y procedimientos que permitan mitigar los riesgos que se puedan presentar en la gestión de seguridad de los sistemas SCADA que se utilizan en la industria analizada.

La verificación de la valoración en cada uno de los elementos que se han evaluado es un proceso por implementar, ya que con él se puede establecer el estado real y su calificación puede ser subjetiva, teniendo en cuenta que en un solo ítem a evaluar se pueden involucrar varios procesos que pueden ser abordados por diferentes individuos.

Si se trata de aplicar esta herramienta y los elementos de seguridad, en otro tipo de industria, es importante tener en cuenta que en cada sector se tienen elementos que son distintivos y de allí se desprenden las diferencias en los elementos que se deben aplicar para su evaluación o auditoria.

A. Anexo: Entrevista.

B. Anexo: Herramienta de evaluación.

C. Anexo: Evaluación caso de estudio.

Bibliografía

Abrams, M., y Weiss, J., (2007). Bellingham, Washington, control system cybersecurity case study. National Institute of Standards and Technology (NIST). Recuperado de http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Bellingham_Case_Study_report%2020Sep071.pdf.

Abrams, M., y Weiss, J., (2008). Malicious control system cyber security attack case study Maroochy water services. Australia: National Institute of Standards and Technology (NIST). Recuperado de http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf.

Bernieri, G., Etchevés, E., Pascucci, F., Setola, R.,(2017) Monitoring system reaction in cyber-physical testbed under cyber-attacks, Computers & Electrical Engineering, Available online 24 February 2017, ISSN 0045-7906, http://dx.doi.org/10.1016/j.compeleceng.2017.02.010. (http://www.sciencedirect.com/science/article/pii/S0045790617303129).

Blowers, M., Iribarne, J., Colbert, E. J., & Kott, A. (2016). In Conclusion: The Future Internet of Things and Security of Its Control Systems. In Cyber-security of SCADA and Other Industrial Control Systems (pp. 323-355). Springer International Publishing.

Candell, R., Stouffer, K., y Anand, D. (2014, Octubre)."A cybersecurity testbed for industrial control systems",2014,"ISA Process Control and Safety Symposium 2014, PCS 2014",,,,"873","888",,,,"http://www.scopus.com/inward/record.url?eid=2-s2.0-84943257571&partnerID=40&md5=9c25cf9427c600fb8b8af503e1a4b55b",Conference Paper,Scopus,2-s2.0-84943257571.

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., Stoddart,K.,(2016) A review of cyber security risk assessment methods for SCADA systems, Computers & Security, Volume 56, February 2016, Pages 1-27, ISSN 0167-4048, http://dx.doi.org/10.1016/j.cose.2015.09.009. (http://www.sciencedirect.com/science/article/pii/S0167404815001388).

CONPES 3701, (2011). Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá D.C.

CONPES 3854, (2016). Política nacional de seguridad digital. Bogotá D.C.

Curtis, P., Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. 2015 IEEE International Symposium on Technologies for Homeland Security, HST 2015, 2015 , art. no. 7225323.

CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2), (2014), Department of Energy (DOE), Estados Unidos.

Cybersecurity on SCADA: risk prediction, analysis and reaction tools for Critical Infrastructures. D3.1- Requirements and Reference Architecture https://www.cockpitci.eu/wp-content/uploads/2015/04/CockpitCI-D3.1-Requirements-and-Reference-Architecture-of-the-Analysis-and-Detection-Layer.pdf.

DANE (2015). Encuesta anual manufacturera EAM. Bogotá D.C.

DAP, (2016). Bases del plan de desarrollo de Antioquia 2016 – 2019. Medellín.

DNP, (2014). Bases del plan nacional de desarrollo 2014 - 2018. Bogotá D.C.

DOE, (2014), Modelo de capacidades de madurez en ciberseguridad C2M2. [Tabla 3].

Goldman, Jeff (2012). Desarrollador de software SCADA fué Hackeado, http://www.esecurityplanet.com/network-security/scada-software-developer-telvent-hacked.html.

Hernandez, M., y Ledesma, D. (2010). Desarrollo de un sistema SCADA para la medición de voltajes con sistemas embebidos para el laboratorio de mecatrónica de la facultad de mecánica. [Figura 1].

Hutchins, M. J., Bhinge, R., Micali, M. K., Robinson, S. L., Sutherland, J. W., & Dornfeld, D. (2015). Framework for identifying cybersecurity risks in manufacturing. Procedia Manufacturing, 1, 47-63., ISSN 2351-9789, http://dx.doi.org/10.1016/j.promfg.2015.09.060.

International Organization for Standardization (ISO) International Electrotechnical Commission (IEC) ISO / IEC 21827:2008 Information technology -- Security techniques -- Systems Security Engineering -- Capability Maturity Model® (SSE-CMM), 2008.

IT Governance Institute COBIT 5. ISACA 2012.

ISACA (2015). Conferencia bSecure Capitulo Monterrey.

ISM3 : Information Security Management Maturity Model (2007) ISBN 1-933284-37-4, 2008.

Johnson C. Cybersafety: on the interactions between cybersecurity and the software engineering of safety-critical systems. Achieving System Safety 2012;85–96.

Knapp, E., Langill, J. (2015).Industrial Network Security (Second Edition), Syngress, Boston, Pages 425-439, ISBN 9780124201149, http://dx.doi.org/10.1016/B978-0-12-420114-9.00027-7. (http://www.sciencedirect.com/science/article/pii/B9780124201149000277).

Knowles, W., Prince, D., Hutchison, D., Ferdinand, J., Disso, P., Jones, K., (2015).A survey of cyber security management in industrial control systems, International Journal of Critical

Infrastructure Protection, Volume 9, June 2015, Pages 52-80, ISSN 1874-5482, http://dx.doi.org/10.1016/j.ijcip.2015.02.002. (http://www.sciencedirect.com/science/article/pii/S1874548215000207).

Kornecki AJ, Zalewski J. Safety and security in industrial control. In: Proceedings of the Sixth AnnualWorkshop on Cyber Security and Information Intelligence Research. ACM, p. 77; 2010.

Kriaa S, Pietre-Cambacedes L, Bouissou M, Halgand Y. A survey of approaches combining safety and security for industrial control systems. Reliab Eng Syst Saf 2015;139:156–78.

Kriz, D. (2011), Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity, Global Cybersecurity Policy, Information Technology Industry Council, Washington, DC, United States ","2011 2nd Worldwide Cybersecurity Summit, WCS 2011, 9780615516080, 5978798, June 1, 2011 - June 2, 2011, Elsevier Inc.","Engineering Village".

Lee, R., Assante, M., Conway, T. (2014). Cyber to Physical or Process Effects case study paper German Steel Mill Cyber Attack. Germany: SANS ICS (Industrial Control System). Recuperado de https://ics.sans.org/media/ICS-CPPE-case-Study-2-German-Steelworks_Facility.pdf.

McGurk, S. (2008). Seguridad en sistemas de control industrial. [Tabla 2],[Figura 2]. Recuperado de http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2008-12/ICSsecurity_ISPAB-dec2008_SPMcGurk.pdf.

National Initiative for Cybersecurity Education Capability Maturity Model NICE-CMM (2012). Recuperado de http://www.tdisecurity.com/about-tdi/cybersecurity_education.pdf.

Pineda L, Jara M. Prospectiva y vigilancia tecnológica en la cadena fibra textil-confecciones. Editorial Universidad el Rosario. Bogotá. 2010. P.71-82. ISBN 9789587380804.

Proençaa, D., Borbinhaa, J.(2016) Maturity Models for Information Systems - A State of the Art.

Rezai, A., Keshavarzi, P., Moravej, Z., (2016) Key management issue in SCADA networks: A review, Engineering Science and Technology, an International Journal, Available online 7 September 2016, ISSN 2215-0986, http://dx.doi.org/10.1016/j.jestch.2016.08.011. (http://www.sciencedirect.com/science/article/pii/S2215098616303482).

Rios, B., y McCorkle, M. (2012). Tridium Niagara Vulnerabilities Alert (ICS-ALERT-12-195-01). Estados Unidos: ICS-CERT Industrial Control Systems Cyber Emergency Response Team. Recuperado de https://ics-cert.us-cert.gov/alerts/ICS-ALERT-12-195-01.

Schrecke, S. (2015). Industrial automation systems cybersecurity of the Analysis and Detection Layer Industrial automation systems cybersecurity Embedding end-to-end trust and security, ISA Publications, InTech Magazine (2015 / Mar-Apr), https://www.isa.org/intech/20150401/.

Shin J, Son H, Heo G. Cyber security risk evaluation of a nuclear i&c system using bayesian networks and event trees. Nuclear Engineering and Technology; 2016.

Stouffer,K., Falcoand, J.,Scarfone, K. (2011) Guide to Industrial Control Systems(ICS) Security ,NIST Special Publication 800-82, National Institute of Standards and Technology, Gaithersburg,Maryland. Recuperado de http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82.pdf.

The MITRE Corporation.ANSI/ISA (2012), Modelo de Diseño de Concepto Purdue ISA-99. [Figura 3].

Uchenna P. Daniel Ani, Hongmei (Mary) He & Ashutosh Tiwari (2017), Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective, Journal of Cyber Security Technology, 1:1, 32-74, DOI: 10.1080/23742917.2016.1252211.

Valenzano, A. (2014), Industrial cybersecurity: Improving security through access control policy models, IEIIT/CNR, Torino 10129, Italy, IEEE Industrial Electronics Magazine, Institute of Electrical and Electronics Engineers Inc., v 8, n 2, p 6-17, June 2014, 2014, 19324529, 10.1109/MIE.2014.2311313, 6839138, Elsevier Inc., Engineering Village.