Revista Colombiana de Computación, Vol. 20, No 2 julio-diciembre 2019, pp. 56-67
http://dx.doi.org/10.29375/25392115-3722

Identificación de elementos de seguridad basados en el modelo C2M2 para la industria manufacturera del sector textil

Identification of safety elements based on the C2M2 model for the textile industry

Jorge Mario Aristizábal Correa[1], Leonel Marín Ramírez[1], Johny Álvarez Salazar[2]

[1]Departamento Sistemas, Instituto Tecnológico Metropolitano, Medellín, Colombia
[2]Departamento Electrónica y Telecomunicaciones, Instituto Tecnológico Metropolitano, Medellín, Colombia
jorgearistizabal212627@correo.itm.edu.co, leonel.marin333@hotmail.com, johnyalvarez@itm.edu.co

(Recibido: 12 junio 2019; aceptado: 13 septiembre 2019)

Resumen

En este trabajo se presenta un estudio de identificación de los elementos de seguridad que afectan a la industria textil –que utiliza sistemas SCADA– los riesgos de fuga, indisponibilidad o alteración no permitida de la información en los ambientes comunes en que operan las tecnologías de la información (TI) y las tecnologías de operación (TO). Para llevar a cabo lo anterior se utilizaron los elementos identificados en la guía de seguridad para los sistemas de control industrial NIST 800-82 y el modelo de madurez en ciberseguridad C2M2. Como resultado se obtuvieron los elementos de seguridad que se ven involucrados en los diferentes procesos, tendencias tecnológicas de la industria analizada; de otra parte, se realizó un comparativo del modelo C2M2 y la NIST 800-82.

Palabras clave: TIC, Desarrollo urbano, Planeación territorial, Gobierno local, Sistemas de información.

Abstract

This paper presents a study based on the identification of the security elements that affect the textile industry where SCADA systems are used, and that may cause risks of leakage, unavailability or unauthorized alteration of information, in common environments in which information technologies (IT) and operating technologies (OT) operate. For this, the elements identified in the safety guide for industrial control systems NIST 800-82 and the cybersecurity maturity model C2M2 were used. As a result, the security elements that are involved in the different processes, technological trends of the analyzed industry were obtained and a comparison of the C2M2 and NIST 800-82 models is made.

Keywords: C2M2, Cibersecurity, SCADA, Security elements, Textile industry.

1. Introducción

El sector industrial está siendo vulnerable a los ataques cibernéticos ocasionados por personas y organizaciones que se aprovechan de los riesgos que se presentan en los Sistemas de Control Industrial (SCI), lo anterior afecta los productos, calidades de producción, reputación de marca y seguridad de las personas. Las intrusiones se han materializado debido a la adopción de las nuevas Tecnologías de la Información (TI) en las que se evidencian las necesidades de integrar los componentes de las TI con los SCI, en lo concerniente a la seguridad (Cherdantseva et al., 2016). Por ejemplo, el informe Índice de Inteligencia de Amenazas (2017) hace referencia a que la seguridad de las redes industriales presenta varias características similares a los estándares de seguridad informática de las empresas (Security Intelligence Staff, 2017).

Para realizar una mitigación de riesgos es necesario evaluar cada uno de los componentes que intervienen en los procesos que están relacionados con las actividades de TI; es un factor clave la identificación

Cite this work as Aristizábal Correa J., Marín Ramírez L., Álvarez Salazar J. (2019). Identificación de elementos de seguridad basados en el modelo C2M2 para la industria manufacturera del sector textil. Revista Colombiana de Computación, 20(2), 56-67. https://doi.org/10.29375/25392115.3722

de los elementos de seguridad para los SCI que pueden ser afectados por las amenazas, vulnerabilidades y ataques. 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 identificar sus debilidades con el fin de poder establecer estrategias que ayuden a mitigar los riesgos que se identifiquen (Johnson, 2012).

El presente artículo pretende reconocer cada uno de los elementos que intervienen en los procesos de los SCI y entender su relación y dependencia. Al identificar tales elementos se pueden conocer los riesgos asociados a las vulnerabilidades que pueden incurrir en pérdidas económicas, información y seguridad laboral.

La metodología aplicada presenta elementos cualitativos y cuantitativos; se realiza una comparación de los diferentes modelos de madurez existentes, se evalúan conceptos, herramientas y elementos existentes en estos, los cuales puedan ser aplicados a la industria manufacturera del sector textil de acuerdo con su impacto en los diferentes procesos y actividades que infieren en la seguridad. En la sección 2 y 3 se presentan las particularidades en la seguridad de los sistemas SCADA y el estándar C2M2 como el modelo de madurez en ciberseguridad. En la sección 4 se presentan las tendencias tecnológicas en la manufactura. Finalmente, en la sección 5 se concluye este artículo.

2. Sistemas SCADA

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) (Candell, Anand, y Stouffer, 2014). Los sistemas SCADA tienen la función de recolectar información de los procesos industriales y de las diferentes formas de interacción con los dispositivos instalados en la maquinaria PLC (*Programmable Logic Controller* o controladores lógicos programables). Los sistemas SCADA están representados en la Figura 1 y 2 por los sensores y actuadores; son capaces, en su nivel básico, de obtener datos como medidas de tamaño, presión, temperatura o posición. En el nivel medio, presentan información de los dispositivos para gestionar a distancia con la supervisión humana, abrir o cerrar compuertas, válvulas, aumentar o disminuir la presión, la temperatura o cualquier otra decisión que requiera la intervención humana, para llevar a cabo esto se utilizan dispositivos HMI (*Human Machine Interface*, Interface Humano – Máquina) que son paneles de visualización o panel de control mediante los cuales se permite interactuar. Los DCS (*Distributed Control System* o Sistemas de Control Distribuido) se encargan de convertir las señales digitales en señales analógicas y viceversa, estas son interpretadas por los PLC; además, se encargan de interactuar con los dispositivos de almacenamiento de las bases de datos, los parámetros de configuración y la iteración con los dispositivos HMI, representado en la Figura 1 como adaptador / convertidor, proceso digital. Cherdantseva et al., (2016) indica 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 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 (Schrecker, 2015).

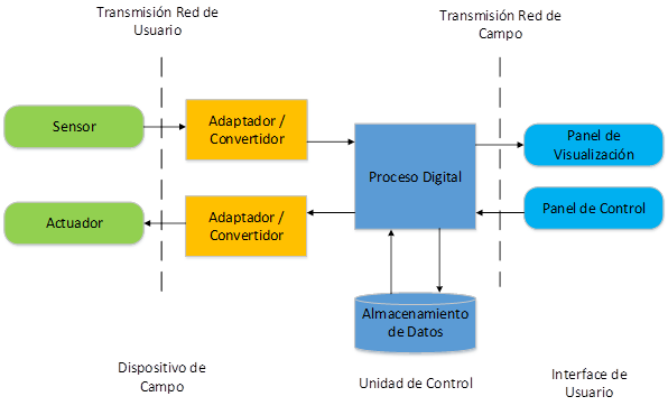

Figura 1. Esquema básico de un sistema SCADA
Fuente: Tomado de (Hernández Cevallos y Ledesma Marcalla, 2010)

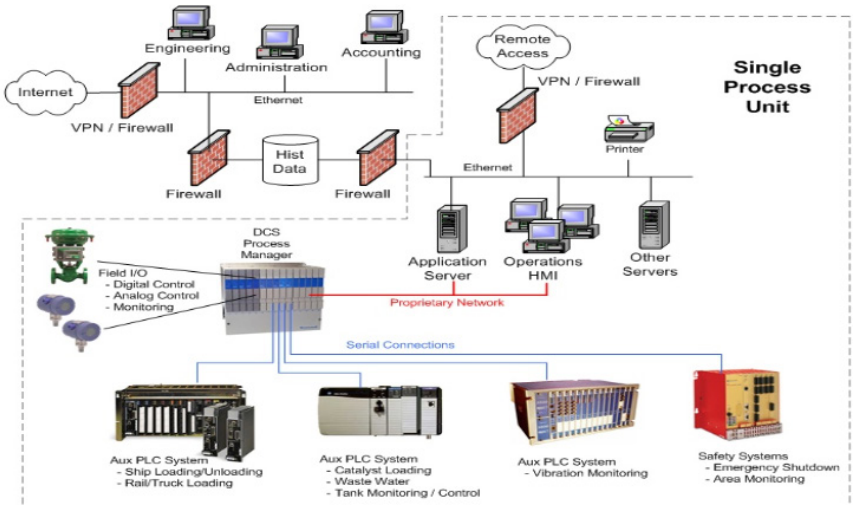

Figura 2. Seguridad en los sistemas de control industrial
Fuente: Tomado de (Kornecki y Zalewski, 2010)

A pesar de que los sistemas SCADA son ampliamente utilizados por su confiabilidad y además de que pueden operar sin pausa durante meses o años (Johnson, 2012), la vulnerabilidad de los sistemas propietarios se presenta a veces en los protocolos de comunicación. El paso de una operatividad local a una gestión remota impulsado por los desarrollos, la interoperatividad y las funcionalidades creadas por los nuevos desarrollos de software para este tipo de sistemas plantean nuevos desafíos de seguridad. Si hay un valor en los datos que se intercambian, los hackers encuentran una manera de acceder a ellos (Proença y Borbinha, 2016).

En ocasiones, los sistemas que soportan estas infraestructuras son 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; sin embargo, 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 muchas ocasiones, se realiza 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 más cuentan con un mayor grado de sofisticación (Cybersecurity and Infrastructure Security Agency, 2018).

Para la transmisión de los datos, los sistemas SCADA utilizan el protocolo Modbus, el cual transmite paquetes sin ningún tipo de cifrado (Bernieri, Etchevés Miciolino, Pascucci, y Setola, 2017). Se espera que estos problemas de seguridad se resuelvan en las capas de transporte (U.S. Department of Energy, 2014).

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, a veces económicamente costosos; 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 y la preservación de la información patentada son vitales para la competitividad de una empresa (Ani, He, y Tiwari, 2017).

Según Johnson (2012), las auditorías de seguridad se realizan probando las políticas, procedimientos y estrategias de acuerdo con el conocimiento de las amenazas y vulnerabilidades conocidas donde comúnmente se emplean cuestionarios y listas de verificación. La preocupación por las amenazas cibernéticas ha generado ciertas publicaciones de estándares y regulaciones de seguridad como NERC CIP, CFATS, ISO/IEC 27002:2005, NRC RG 5.71, y NIST 800-82 que proporcionan controles para administrar los riesgos cibernéticos. Sin embargo, la gran mayoría de estas publicaciones se dirigen a la gestión de los riesgos y protección de la información en un proceso que se conoce como seguridad de la información

(o aseguramiento de la información) (Knapp y Langill, 2015). 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. Sin embargo, en la práctica el término seguridad de la información se utiliza para referirse a ambos procesos. 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 más 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. De acuerdo con Kanpp y Langill (2015), los métodos de evaluación del riesgo de seguridad cibernética para SCADA pueden mejorarse, en términos de estos autores: 1. Abordar el contexto: el establecimiento del proceso de gestión de riesgos; 2. Superación: orientación de ataque o falla; 3. Factor humano; 4 La captura y formalización de expertos; 5. La mejora de la fiabilidad de los sistemas de datos probabilísticos; 6. Evaluación y validación; y 7. Herramientas de soporte.

3. Estándar C2M2

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 de los Estados Unidos (DOE) con el apoyo de la Casa Blanca en asocio con el Departamento de Seguridad Nacional de los Estados unidos (DHS, por sus siglas en inglés), con la colaboración de expertos del sector público y privado (U.S. Department of Energy, 2014). Según McGurk (2008), 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 auditoría y mejoramiento, y progreso en la obtención de los objetivos (McGurk, 2008).

El Modelo C2M2 puede ayudar a las organizaciones de todos los sectores, tipos y 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. El Modelo C2M2 puede utilizarse para que las organizaciones incrementen las capacidades en ciberseguridad, evaluar de manera efectiva y consistente las capacidades en ciberseguridad, compartir los conocimientos, las mejores prácticas y la identificación pertinente de los procesos en las organizaciones como una forma para mejorar las capacidades en ciberseguridad; de otra parte, permite establecer las acciones para priorizar las inversiones y mejorar la seguridad cibernética (Curtis y Mehravari, 2015).

El C2M2 está diseñado para usarse como metodología de autoevaluación de una organización, para medir y mejorar su programa en ciberseguridad o para el desarrollo de un nuevo programa en ciberseguridad. En este modelo se definen varios dominios, los cuales analizan las capacidades de la organización para cumplir con los criterios definidos en cada uno de ellos; para evaluarlos se utilizan los indicadores de nivel de madurez o MIL (ver Tabla 1).

El Instituto Nacional de Estándares (NIST) elaboró una serie de controles con aplicación a los sistemas de control industrial, 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). De acuerdo con Knapp y Langill (2015), NISTSP 800-82 proporciona orientación y desarrollo de los planes de seguridad en los sistemas de control industrial. En la Tabla 2 se realiza una comparación entre los dominios del modelo de madurez C2M2 y los controles de NIST 800-82. Debido a que se deben evaluar los sistemas SCADA, estos modelos son abordados en este tipo de infraestructuras, las cuales integran elementos de TI (Tecnologías de la Información) como de OT (Tecnologías de la Operación).

A pesar de que estas tecnologías son ampliamente conocidas y comprendidas, 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, a veces económicamente costosos. 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

Tabla 1. Hoja Resumen C2M2

Dominio	Descripción
Gestión del Riesgo (RM)	Establecer, operar y mantener un programa de gestión de riesgos de la empresa de seguridad cibernética para identificar, analizar y mitigar los riesgos de seguridad cibernética de la organización, incluyendo sus unidades de negocios, filiales, infraestructura interconectada y las partes interesadas.
Activos, Cambio y Gestión de la Configuración (ACM)	Gestión de las operaciones tecnológicas en la organización (OT) y activos de la tecnología de información (IT) que incluye tanto el hardware como el software, el riesgo de la infraestructura y objetivos de la organización.
Gestión de Identidad y Acceso (IAM)	Crear y gestionar las identidades de acceso lógico o físico a los activos de la organización y las entidades a las que pueden concederse. Controlar el acceso a los activos de la organización, el riesgo de acceso a la infraestructura y objetivos de la organización.
Gestión de las amenazas y las vulnerabilidades (TVM)	Establecer y mantener planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas de seguridad cibernética y vulnerabilidades asociadas con el riesgo de la infraestructura de la organización (por ejemplo, procesos críticos, activos TI críticos, operativos) y objetivos organizacionales.
Conciencia de la situación (SA)	Establecer y mantener las actividades y tecnologías para recoger, analizar, generar alarmas, presentar y utilizar la información operativa y la seguridad cibernética, incluyendo el estado y la información de resumen de los otros dominios del modelo para formar una imagen operativa común (COP).
Intercambio de Información y Comunicaciones (ISC)	Establecer y mantener relaciones con entidades internas y externas para recoger y proporcionar información sobre seguridad cibernética, así como las amenazas y las vulnerabilidades para reducir los riesgos y aumentar la capacidad de recuperación operativa, con el riesgo a la infraestructura y objetivos de la organización.
Eventos y respuesta a incidentes, Continuidad de las Operaciones (IR)	Establecer y mantener planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de seguridad cibernética y mantener las operaciones a lo largo de un evento de seguridad cibernética proporcionadas al riesgo de la infraestructura y objetivos de la organización.
Cadena de Suministro y Gestión de Dependencias externas (CDE)	Establecer y mantener controles para gestionar los riesgos asociados a la seguridad cibernética, servicios y activos que son dependientes de entidades externas acorde con el riesgo a la infraestructura y objetivos de la organización.
Gestión del Personal (WM)	Establecer y mantener planes, procedimientos, tecnologías y controles para crear una cultura de seguridad cibernética y atención a la adecuación permanente y competencia del personal, con el riesgo a la infraestructura y objetivos de la organización.
Gestión de programas de seguridad cibernética (CPM)	Establecer y mantener un programa de seguridad cibernética de la empresa que proporciona el gobierno, la planificación estratégica, y el patrocinio de las actividades de seguridad cibernética de la organización, de manera que se alinee con los objetivos de seguridad cibernética, con los objetivos estratégicos de la organización y el riesgo a la infraestructura.
Fuente: Tomado de (Kornecki y Zalewski, 2010).	

calidad, suministro y personal, acceso a la información por parte de entidades no autorizadas o externas son cruciales en el panorama competitivo actual. La divulgación de negocios, los datos críticos de producción, la información a competidores y adversarios podría causar una pérdida de la ventaja competitiva y la relevancia del mercado. En consecuencia, la protección y la preservación de la información patentada es vital para la competitividad de una empresa (Cybersecurity and Infrastructure Security Agency, 2018).

De acuerdo con Kriz (2011), en todos esos productos se aplican los conocimientos especializados y la creatividad intelectual, este es un valor de capital intelectual para la creación y comercialización de productos; sin embargo, se otorga escasa importancia a la protección de esos activos intelectuales. En

Tabla 2. Comparativo modelo C2M2 y NIST 800-82

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 de 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). Auditoría y responsabilidad (AU).
Gestión de amenazas y vulnerabilidades	Establecer planes, procedimientos y tecnologías para detectar, identificar, analizar, gestionar y responder a las amenazas, vulnerabilidades de la seguridad cibernética en consonancia con el riesgo para los objetivos de infraestructura de la organización (por ejemplo, críticos, informáticos, operacionales), manteniéndolos actualizados.	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, y así formar una imagen operativa común.	Seguridad del personal (PS). Protección física y medioambiental (PE). Conciencia y Entrenamiento (AT).
Intercambio de Información y Comunicaciones	Establecer 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, manteniéndolos actualizados.	
Respuesta a eventos e incidentes, continuidad de las operaciones	Establecer planes, procedimientos y tecnologías para detectar, analizar y responder a eventos de ciberseguridad y, a su vez, para mantener las operaciones a lo largo de un evento de seguridad cibernética proporcional al riesgo para la infraestructura crítica y los objetivos organizacionales, manteniéndolos actualizados.	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).

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 propiedad intelectual para reducir los riesgos que constituye el no registro de los diseños, es una actividad que se debe implementar, ya que con esto se puede impedir que otros los exploten económicamente.

4. Tendencias tecnológicas en la manufactura

En el estudio realizado por CIDETEXCO en 2011 sobre las tendencias tecnológicas para los próximos 10 años en el ciclo de vida del producto (CPV), para la industria fibra textil y confección afirman que 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 limpio y sostenible (ver Tabla 3). El ciclo inicia con la extracción y selección de materiales, posteriormente se pasa a la fase de diseño del 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 este le da al producto. Culminado ese proceso llega la eliminación.

Tabla 3. Tendencias Tecnológicas en la manufactura adaptativa

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 interoperables.	Sistemas híbridos de producción para la fabricación, 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 autoaprendizaje 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 en diseño de sistemas reconfigurables.	Sistemas de sensores para control de planta.	
Instrumentos para la planificación de la producción y la simulación in situ.		

En los procesos de extracción, selección de materiales, diseño de producto, manufactura, empaque y distribución que hacen parte del CVP se desarrollan conceptos ingenieriles con la ayuda de las herramientas tecnológicas que permiten la optimización de los sistemas, haciendo de estos una producción sostenible y de recursos (ver Tabla 4).

Tabla 4. Tendencias Tecnológicas en la Ingeniería digital en manufactura

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 gráfico de usuario para diseño y simulación de productos.	
	Integración y sincronización de la fábrica digital con datos en tiempo real.	

La evolución de la tecnología conlleva la integración de los nuevos avances en productos y las consecuentes modificaciones en el proceso de producción que impulsan hacia una dinámica que debe ser planeada y articulada, lo que requiere la intervención de los diferentes entes para una correcta implementación (ver Tabla 5).

Tabla 5. Tendencias en Tecnologías emergentes

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.

Los nuevos retos que nos propone la tecnología establecen que se debe cambiar el paradigma de producción, optimizar sus aspectos estructurales y funcionales, orientarlo hacia la creación de valor para los productos a lo largo de su ciclo de vida, con el fin de identificar los aspectos cualitativos que deben ser mejorados, nuevos factores de rendimiento, integración con otros procesos y aspectos de la interacción. Lo anterior lleva a la interpretación, tendencias y comprensión de las necesidades de los usuarios en el diseño de los productos, la fabricación y los servicios de valor agregado cerca al usuario junto con las acciones al final de su vida útil (ver Tabla 6).

Según Assante et al., (2018), en los procesos realizados en la industria textil que se encuentran automatizados, en los que se convierte el algodón como fibra natural en un producto fino alargado, resistente y flexible para luego convertirlo en tela; se tienen varias etapas. A continuación, se detallan los siguientes procesos:

Desempacado: consiste en la separación de las fibras y la limpieza de impurezas, esto 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 dirección 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.

Tabla 6. Tips para manufactura

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 validación de la fabricación robótica automatizada, y automatización de los procesos de postproducción.	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.	

Fuente: Tomado de (CIDETEXCO, 2011)

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.

5. Conclusiones

La industria manufacturera del sector textil que utiliza sistemas SCADA son objeto de ataques que afectan la disponibilidad, confidencialidad e integridad; para mitigar esto se deben tener las herramientas necesarias que permitan determinar el nivel de madurez en la gestión de los sistemas de SCADA del sector textil, en donde se identifique, evalúe y califique los elementos de seguridad que puedan causar los riesgos asociados a la seguridad. Al identificar cada uno de los elementos que intervienen en los procesos de estos sistemas, entender su relación, dependencia e importancia se puede identificar el impacto que puede llegar a ocasionar en los factores de seguridad. Una vez se tenga conocimiento de las debilidades en los controles de seguridad, se pueden establecer estrategias que ayuden a mitigar las vulnerabilidades presentes en estos sistemas, ayudando a fortalecer el estado de madurez de los procesos y actividades que se realizan en estos sistemas.

En la evaluación de la seguridad, en los entornos industriales donde se utilizan sistemas SCADA, se identificaron los riesgos asociados a las vulnerabilidades que pueden incurrir en pérdidas económicas, información y seguridad laboral.

Se identificaron los elementos que causan riesgos a la seguridad teniendo como referencia el modelo de capacidades en ciberseguridad C2M2 y la norma NIST 800-82 para la industria manufacturera sector textil. Con esta referencia se lograron identificar los elementos que pueden causar las vulnerabilidades asociadas a estos sistemas.

Al identificar cada uno de los elementos que pueden causar riesgos se tiene el insumo para elaborar las estrategias que ayuden a mitigar las vulnerabilidades, teniendo en cuenta que este proceso es una mejora continua, actualizando continuamente las estrategias y siendo resilientes, identificando nuevos aspectos de mejora.

Declaración de conflicto de intereses

Los autores declaran no tener conflicto de intereses con respecto a la investigación, autoría y/o publicación de este artículo.

Referencias

Ani, U. P. D., He, H. (Mary), y Tiwari, A. (2017). Review of cybersecurity issues in industrial critical infrastructure: manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

Assante, D., Romano, E., Flamini, M., Castro, M., Martin, S., Lavirotte, S., y Spatafora, M. (2018). Internet of Things education: Labor market training needs and national policies. In *2018 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1846–1853). IEEE. https://doi.org/10.1109/EDUCON.2018.8363459

Bernieri, G., Etchevés Miciolino, E., Pascucci, F., y Setola, R. (2017). Monitoring system reaction in cyber-physical testbed under cyber-attacks. *Computers y Electrical Engineering*, *59*, 86–98. https://doi.org/10.1016/j.compeleceng.2017.02.010

Candell, R., Anand, D., y Stouffer, K. (2014). A cybersecurity testbed for industrial control systems. In *Proceedings of the 2014 Process Control and Safety Symposium* (pp. 1–16). Retrieved from https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=915876

Cherdantseva, Y., Burnap, P., Blyth, A., Eden, P., Jones, K., Soulsby, H., y Stoddart, K. (2016). A review of cyber security risk assessment methods for SCADA systems. *Computers y Security*, *56*, 1–27. https://doi.org/10.1016/j.cose.2015.09.009

CIDETEXCO. (2011). *Tendencias tecnológicas ciclo de vida de producto. industria fibra textil confección R2-2011-CIDETEXCO*.

Curtis, P. D., y Mehravari, N. (2015). Evaluating and improving cybersecurity capabilities of the energy critical infrastructure. In *2015 IEEE International Symposium on Technologies for Homeland Security (HST)* (pp. 1–6). IEEE. https://doi.org/10.1109/THS.2015.7225323.

Cybersecurity and Infrastructure Security Agency. (2018). ICS Alert (ICS-ALERT-12-195-01). Retrieved May 30, 2019, from https://www.us-cert.gov/ics/alerts/ICS-ALERT-12-195-01.

Hernández Cevallos, M. I., y Ledesma Marcalla, D. A. (2010). *Desarrollo de un sistema SCADA para la medición de voltajes con sistemas embebidos para el laboratorio de mecatrónica de la facultad de mecánica*. Retrieved from http://dspace.espoch.edu.ec/bitstream/123456789/1137/1/25T00140.pdf.

Johnson, C. (2012). CyberSafety: CyberSecurity and Safety-Critical Software Engineering. In *Achieving Systems Safety* (pp. 85–95). London: Springer London. https://doi.org/10.1007/978-1-4471-2494-8_8.

Knapp, E. D., y Langill, J. T. (2015). *Industrial Network Security* (Second). Elsevier. https://doi.org/10.1016/C2013-0-06836-3.

Kornecki, A. J., y Zalewski, J. (2010). Safety and security in industrial control. In *Proceedings of the Sixth Annual Workshop on Cyber Security and Information Intelligence Research - CSIIRW '10* (p. 1). New York, New York, USA: ACM Press. https://doi.org/10.1145/1852666.1852754.

Kriz, D. (2011). Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity. In *2011 Second Worldwide Cybersecurity Summit (WCS)*. London, UK: IEEE. Retrieved from https://ieeexplore.ieee.org/abstract/document/5978798.

McGurk, S. P. (2008). *Industrial Control Systems Security*. Retrieved from https://csrc.nist.gov/csrc/media/events/ispab-december-2008-meeting/documents/icssecurity_ispab-dec2008_spmcgurk.pdf.

Proença, D., y Borbinha, J. (2016). Maturity Models for Information Systems - A State of the Art. *Procedia Computer Science*, *100*, 1042–1049. https://doi.org/10.1016/j.procs.2016.09.279.

Schrecker, S. (2015). Industrial automation systems cybersecurity. Embedding end-to-end trust and security. Retrieved May 30, 2019, from https://www.isa.org/intech/20150401/.

U.S. Department of Energy. (2014). Cybersecurity Capability Maturity Model (C2M2). Retrieved May 30, 2019, from https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0.