SEGURIDAD EN LA INTEGRACIÓN DE UN SISTEMA SCADA EN ITS (SISTEMAS INTELIGENTES DE TRANSPORTES) EN COLOMBIA

ROBINSON STIVEN MARTINEZ PEREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
MEDELLIN

2024

SEGURIDAD EN LA INTEGRACIÓN DE UN SISTEMA SCADA EN ITS (SISTEMAS INTELIGENTES DE TRANSPORTES) EN COLOMBIA

ROBINSON STIVEN MARTINEZ PEREZ

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMATICA

EDGAR ROBERTO DULCE VILLAREAL
asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PUERTO BERRIO -ANTIOQUIA
2024

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con amor dedico este trabajo a mi familia, en especial a mi madre Laura, a mi hija Lauren y a mi pareja Helenin, quienes son mi apoyo, mi inspiración y mi motivación constante en la vida.

AGRADECIMIENTOS

Agradezco a todas las personas que me acompañaron en el transcurso de este proceso, por su apoyo, sus palabras de motivación y aliento para continuar formándome como profesional.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

GLOSARIO

AMENAZAS: Son actos maliciosos que buscan dañar equipos, robar datos o interrumpir la vida digital, estas acciones se aprovechan de una vulnerabilidad para atentar contra la seguridad de sistemas de información.

CIBERSEGURIDAD: Es el conjunto de procedimientos y e herramientas que se implementan para proteger la información que se genera y procesa a través de computadoras, servidores, dispositivos móviles, redes y sistemas electrónicos.

HERRAMIENTAS DE AUTOMATIZACIÓN: En procesos empresariales e industriales, son las que permiten a las organizaciones reducir errores humanos al automatizar tareas que son de tipo repetitivo o manejo manual.

INCIDENTE DE SEGURIDAD: Comprende las situaciones que ponen en peligro, la confidencialidad e integridad de un sistema de información y/o violación de normas y políticas de seguridad.

MOVILIDAD: involucra acciones, estrategias, normas, que permiten el manejo, gestión y regulación de la movilidad en un territorio.

PROTOCOLOS DE COMUNICACIÓN: son un tipo de protocolo de red que garantiza la seguridad e integridad de los datos en tránsito a través de una conexión de red como Internet.

RIESGO: Un riesgo es una probabilidad de que se llegue a producir un incidente de seguridad, llegando a convertirse en amenaza y causando perdidas o daños.

SISTEMAS DE INFORMACIÓN: Comprende un conjunto de agentes, códigos, procesos, que interactúan de manera coordinada entre sí para lograr algún fin o propósito.

TRANSFORMACIÓN DIGITAL: Son cambios asociados a la aplicación de tecnologías digitales en diferentes aspectos de la sociedad.

VULNERABILIDADES: Son fallos informáticos o debilidades en un sistema que ponen en peligro y/o riesgo la seguridad de la información, y que pueden ser usadas por atacantes con fines maliciosos.

RESUMEN

En América Latina y específicamente en Colombia, se han venido desarrollando avances significativos en la implementación de sistemas de transporte inteligentes (ITS, siglas en inglés), generando gran impacto en movilidad, infraestructura, desarrollo industrial y sostenibilidad. Para el funcionamiento de estos sistemas se requiere la implementación de herramientas tecnológicas que permitan el adecuado control y manejo de datos para obtener información específica y actualizada de las diferentes operaciones que se realizan en movilidad. Uno de los sistemas usados es el SCADA que permite monitorear y controlar procesos e infraestructuras industriales y se encarga de recopilar datos en tiempo real de sensores y otros dispositivos, analizarlos y enviar señales de control a los procesos industriales, sin embargo, están expuestas a constantes amenazas y vulnerabilidades, que ponen en riesgo el manejo de la información de las organizaciones.

Por lo tanto se pretende generar un análisis de la seguridad en la integración de los protocolos de comunicación de un sistema SCADA en sistemas inteligentes de transporte (ITS) en Colombia mediante una revisión documental, estableciendo la funcionalidad de los protocolos de comunicación con el fin de identificar incidentes de seguridad que puedan poner en riesgo la integridad de la información, categorizando las herramientas de automatización industrial en los ITS determinando las más adecuadas para un proceso de integración articulado con lineamientos de seguridad y finalmente proponer buenas prácticas que permitan salvaguardar la información.

PALABRAS CLAVES: Sistema SCADA, sistemas inteligentes de transporte, vulnerabilidades, herramientas de automatización industrial.

ABSTRACT

In Latin America and specifically in Colombia, significant progress has been made in the implementation of intelligent transportation systems, generating great impact on mobility, infrastructure, industrial development, and sustainability. The operation of these systems requires the implementation of technological tools that allow adequate control and data management to obtain specific and updated information on the different operations performed in mobility. One of the systems used is the SCADA that allows monitoring and controlling industrial processes and infrastructures and is responsible for collecting real-time data from sensors and other devices, analyze them and send control signals to industrial processes, however, they are exposed to constant threats and vulnerabilities, which put at risk the management of information of organizations.

Therefore, it is intended to generate an analysis of security in the integration of communication protocols of a SCADA system in intelligent transportation systems (ITS) in Colombia through a documentary review, establishing the functionality of communication protocols in order to identify security incidents that may jeopardize the integrity of the information, categorizing the industrial automation tools in the ITS, determining the most appropriate for an integration process articulated with security guidelines and finally proposing good practices to safeguard the information.

KEYWORDS: SCADA system, intelligent transport systems, vulnerabilities, industrial automation tools.

INTRODUCCIÓN

El presente trabajo busca presentar una mirada analítica de las características de seguridad que se requieren para el proceso de integración de un sistema SCADA en sistemas inteligentes de transporte (ITS) en Colombia, partiendo de una recopilación y revisión documental sobre la implementación y el desarrollo que ha tenido a nivel mundial y como se viene desarrollando en el país, así mismo se busca identificar las incidencias que ha presentado a lo largo de los años, verificando cuáles han sido los principales, riesgos, amenazas, incidentes, y afectaciones a nivel de ciberseguridad y cuáles han sido las nuevas acciones que se han ido generando para el control y manejo de estos sistemas.

Finalmente, después de contar con el análisis pertinente, se busca proponer algunas buenas prácticas a través de estándares que permitan salvaguardar la información en este tipo de redes de comunicación industrial.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

"Los sistemas Inteligentes de Transporte (ITS) son una amplia gama de sistemas de información y tecnologías electrónicas y de comunicación (inalámbrica o cableada) que mejoran la seguridad vial, la movilidad, la calidad de vida de los ciudadanos, y aumentan la productividad y competitividad del país, a través de la inclusión de tecnologías avanzadas en la infraestructura de transporte y en los vehículos"[1]. En los últimos años a nivel mundial y centrándonos principalmente en Latinoamérica y Colombia, se vienen implementando estas nuevas tecnologías en los mecanismos de control en el transporte logrando ventajas a nivel económico, operacional y de mantenimiento, las cuales buscan satisfacer necesidades de viajes, haciendo uso de varios mecanismos que permiten agilizar y facilitar la movilidad, contribuir al cumplimiento de políticas gubernamentales en cuestión de sostenibilidad económica y ambiental y a brindar seguridad en el funcionamiento y monitoreo de sus operaciones.

Es importante señalar que "cada una de las tecnologías implementadas en las redes de sistemas de transporte debe proporcionar información en tiempo real que permita tener control de datos de forma confiable y que facilite su administración; deben brindar información sobre condiciones de tráfico, trabajos de mantenimiento velocidades de circulación, alarmas ante accidentes, entre otras. Dicho proceso de modernización se debe llevar a cabo de forma gradual teniendo en cuenta que debe suplir las necesidades de movilidad en el presente y se debe acomodar igualmente al volumen de tráfico del futuro"[2] Por tal motivo deben estar basadas en redes de comunicación solidas que por un lado logren una transformación digital

[1] Ministerio de Transporte. ¿Qué es ITS? (2018). [Consultado el 14 de marzo de 2023] disponible en https://www.mintransporte.gov.co/publicaciones/5757/que-es-its/

[2] QUINTERO, Julian; PRIETO, Lina. Sistemas inteligentes de transporte y nuevas tecnologías en el control y administración del transporte. (2015). Disponible en: https://repository.upb.edu.co/bitstream/handle/20.500.11912/7281/SISTEMAS%20INTELIGENTES%20DE%20TRANSPORTE.pdf?sequence=1&isAllowed=y

en los procesos industriales y al mismo tiempo brinde seguridad y protección de los datos.

En este sentido una de las herramientas de automatización para los ITS es el sistema SCADA (Control de Supervisión y Adquisición de Datos) que se utiliza para monitorear y controlar procesos e infraestructuras industriales, encargándose de la recopilación de datos en tiempo real de sensores y otros dispositivos, y tiene como función analizar los datos y enviar señales de control a los procesos industriales para optimizar su rendimiento, también puede proporcionar a los operadores alarmas y alertas si se detectan condiciones anormales[3]. Estos sistemas son fundamentales para el funcionamiento de muchos procesos e infraestructuras industriales, y su seguridad es sumamente importante para evitar el acceso no autorizado o la manipulación.

Sin embargo, estos sistemas están expuestos a diferentes vulnerabilidades, ya que pueden carecer de cortafuegos, mecanismos de cifrado, o software antivirus, en la mayoría de las compañías se utilizan software y hardware estándares que al ser tan conocidos y usados por la mayoría de las empresas representa un aumento en las posibilidades de recibir ataques. así mismo en algunos casos se puede presentar que "el personal de IT no posee el conocimiento o la sensibilización necesaria de que necesita proteger en una red SCADA, es decir en los sistemas SCADA existen vulnerabilidades que normalmente no pueden considerarse de alto impacto en las redes corporativas pero en el marco de este tipo de sistema si lo son"[4], en otros casos se puede presentar también que las medidas de control usadas no han sido adaptadas o su implementación no es lo suficientemente buena para mantener la protección necesaria.

Concretamente en la infraestructura de los sistemas integrados de transporte, los ataques han sido pocos y esporádicos, pero a medida que se avance en herramientas tecnologías implementadas en el transporte, las amenazas

[3] Centro de Formación Técnica para la Industria. Qué es un sistema SCADA, para que sirve y cómo funciona [consultado el 14 de marzo de 2023, de aula 21] Disponible en https://www.cursosaula21.com/que-es-un-sistema-scada

[4] FAJARDO, Franklin. Implementación de Políticas de Seguridad en los sistemas SCADA. Universidad Piloto de Colombia. [Consultado el 17 de marzo de 2023] Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2983/00001484.pdf?sequence=1

aumentarán con el tiempo, especialmente cuando los delincuentes descubran nuevos modelos de especulación, al ser altamente visibles los ataque serán de alto impacto[5].

1.2 FORMULACIÓN DEL PROBLEMA

Si bien muchos sistemas SCADA se han venido actualizando para usar tecnologías más modernas y mejorar su eficiencia y confiabilidad, es pertinente revisar que tanto son afectados por los ataques de ciberseguridad y por las vulnerabilidades a las que pueden estar expuestos, y que impacto generan en a nivel mundial y principalmente en Colombia en relación con los sistemas integrados de transporte, teniendo en cuenta que en el ámbito nacional se vienen implementando estos sistemas desde hace algún tiempo y cada vez son más los entornos donde se requieren, pero es poca la información que se tiene respecto a sus avances y dificultades en los procesos de implementación.

en ese sentido y partiendo de la importancia de la ciberseguridad en estos procesos, surge la pregunta problema del presente trabajo, ¿cuáles son las características de seguridad que se requieren para el proceso de integración de un sistema SCADA en sistemas inteligentes de transporte (ITS) en Colombia?

[5] HUQ, Numan; VOSSELER, Rainer; SWIMMER, Morton (Trend Micro Forward-Looking Threat Research (FTR) Team). Cyberattacks Against Intelligent Transportation System. (2017). Disponible en https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against-intelligent-transportation-systems.pdf

2 JUSTIFICACIÓN

A medida que se generan grandes avances a nivel tecnológico e industrial, también van surgiendo y creciendo situaciones de vulnerabilidad y riesgos que mantienen al acecho las buenas prácticas del manejo de la información en cualquier organización o proceso industrial; en el caso de los sistemas inteligentes de transporte (ITS), se manejan tecnologías avanzadas e innovadoras usadas para salvar vidas, ahorrar tiempo, dinero y contribuir a la sostenibilidad del medio ambiente, que al estar habilitadas para Internet están expuestas a las amenazas de los ciberataques, lo que podría generar interrupciones en comercio, pérdidas económicas, y presentar riesgos de seguridad de datos y manejo de información, así mismo los ciberataques a los que pueden estar abiertos los sistemas de transporte inteligentes pueden generar grandes fallas en las funciones y servicios.

En el caso de Colombia, estos procesos si bien han ido teniendo gran auge y proyección a nivel industrial, y han empezado a implementarse en varios proyectos de movilidad, todavía no logran estar al alcance de las tecnologías a nivel mundial y se enfrentan a diferentes retos a nivel de ciberseguridad que se deben ir revisando y transformando a través de los análisis, avances y recomendaciones que brindan entidades expertas en relación con el funcionamiento adecuado y oportuno de estos sistemas.

En este sentido, el trabajo de la presente monografía busca a través de una revisión documental, dar una mirada analítica a las características que se requieren para el proceso de integración de un sistema SCADA en sistemas inteligentes de transporte (ITS) en Colombia, y así lograr proponer algunas buenas prácticas a través de estándares que permitan salvaguardar la información.

3 OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar la seguridad en la integración de un sistema SCADA en sistemas inteligentes de transporte (ITS) en Colombia, mediante una revisión documental con el fin de proponer buenas prácticas que permitan salvaguardar la información.

3.2 OBJETIVOS ESPECÍFICOS

- Establecer la funcionalidad de un sistema SCADA a partir de una revisión documental con el fin de identificar incidentes de seguridad que puedan poner en riesgo la integridad de la información en sistemas inteligentes de transporte (ITS) en Colombia.

- Identificar herramientas en la integración de un sistema SCADA, en sistemas inteligentes de transporte (ITS), mediante la definición de criterios como funcionalidad, compatibilidad, facilidad de integración.

- Proponer buenas prácticas basadas en el NIST-CSF que permitirá asegurar la integridad, confidencialidad y disponibilidad de la información en el proceso de integración de un sistema SCADA en sistemas inteligentes de transporte (ITS) en Colombia.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Sistemas SCADA. Los sistemas SCADA (supervisión, control y adquisición de datos) son una herramienta fundamental en la automatización de procesos industriales, ya que permiten monitorear y controlar procesos en tiempo real, aumentando la eficiencia y la seguridad de la producción; están diseñados para recopilar datos de sensores y otros dispositivos de campo, y enviarlos a una computadora central donde los datos se pueden visualizar, analizar y controlar, permitiendo que se brinde una atención precisa y rápida a eventos imprevistos[6].

Los principales tipos de sistemas SCADA se dividen según su arquitectura y su distribución:

Por su arquitectura se diferencian por ser:

- Sistemas Clientes/Servidor donde la adquisición y procesamiento lo realiza un servidor al cual se conectan los clientes
- Sistemas Standalone en la que todas las computadoras están conectadas directamente a los controladores de proceso.

Según su distribución se encuentra los siguientes:

- Sistemas distribuidos: los componentes se encuentran físicamente separados y conectados a través de una red de comunicaciones.
- Sistemas centralizados: todos los componentes se encuentran en una misma ubicación.
- Sistemas híbridos: combina las características de los sistemas distribuidos y centralizados.

En la actualidad son sistemas que trabajan formando un conjunto en donde todas las variables controladas hacen un gran sistema de control, pero muchos de los dispositivos que lo conforman no se han actualizado de la misma manera en que ha ido avanzando la tecnología, lo cual empieza a generar nuevos problemas de

[6] Centro de Formación Técnica para la Industria. Qué es un sistema SCADA, para que sirve y cómo funciona [consultado el 14 de marzo de 2023, de aula 21] Disponible en https://www.cursosaula21.com/que-es-un-sistema-scada

seguridad en estos sistemas, presentando brechas en la seguridad lo que puede generar vulnerabilidades al sistema

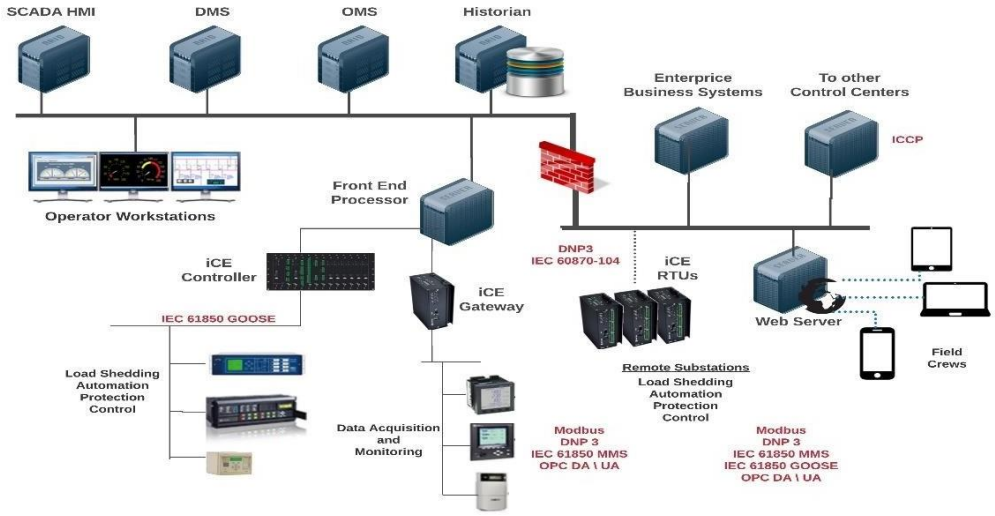

Ilustración 1 Arquitectura de un sistema SCADA. Tomado de https://etap.com/es/product/real-time-system-architecture

4.1.2 Sistemas Inteligentes de Transporte (ITS). Se conoce por sus siglas en inglés como Intelligent Transportation Systems (ITS), y se define "como un sistema avanzado de tecnologías de la información y la comunicación, aplicada en el sector del transporte con el fin de aportar mayor información a los usuarios, mayor seguridad, y gestión para la optimización de recursos"7, buscan mejorar aspectos de seguridad vial, movilidad, calidad de vida de ciudadanos, entre otros, que al diseñarse e implementarse adecuadamente se convierten en herramientas fundamentales en la era de la digitalización, se conforman por un conjunto de soluciones tecnológicas que tienen como fin brindar soporte al transporte terrestre incluyendo vehículos, vías, usuarios etc. también se les conoce como telemáticas porque integra las telecomunicaciones y la informática.

Su funcionalidad consiste en aumentar la seguridad preventiva ante diferentes situaciones de peligro, mediante el uso de estaciones meteorológicas o cámaras,

[7] VELAZCO, Sandra; FERRO, Roberto; CUARTAS, Katherin. Sistemas Integrados de Transporte soportados en el internet de las cosas. (2016). Disponible en https://revistas.udistrital.edu.co/index.php/REDES/article/view/11995

rastreo instantáneo debido a los paneles informativos mediante mensajería, también buscan garantizar que los conductores cumplan las indicaciones, con seguridad reactiva que revisa las acciones, como semáforos, mapas, paneles de mensajería variable, entre muchos más y así facilitar las labores del conductor y controlar lo mejor posible la información obtenida en las carreteras por la seguridad de personas y artículos.

Los sistemas inteligentes de transporte comprenden una amplia cantidad de funciones, entre ellas se encuentran las siguientes[8]:

- Actividad del transporte en tiempo real: Un sistema inteligente puede obtener información del tráfico en tiempo real. En la red se puede encontrar datos de transporte público, flotas de transporte y vehículos personales. Esta información permite tomar decisiones y optimizar rutas para llegar a tiempo, al mismo tiempo se logra minimizar el uso del combustible e incluir en dicho recorrido las zonas más seguras.

- Paneles de mensajería: se colocan en las carreteras y envían información en tiempo real sobre las condiciones de una carretera, por ejemplo: banco de niebla, reduzca la velocidad, y así brindan la posibilidad de un viaje más seguro.

- Notificación de emergencia dentro del vehículo: Este notifica automáticamente cuando hay una probabilidad alta de un potencial accidente. La notificación es enviada al punto de atención de llamadas de emergencia. Esto permite que el mensaje llegue a tiempo a la policía, bomberos y ambulancia.

- Vigilancia automática de infracciones: En el área de seguridad vial, los sistemas inteligentes de transporte también cumplen un papel muy importante. Una de las aplicaciones es el control de exceso de velocidad y el paso del semáforo en rojo.

[8] LOPEZ, Javier. Los Sistemas Inteligentes de Transportes, la tecnología en el transporte terrestre. (2022). Disponible en https://www.eleconomista.com.mx/opinion/Los-Sistemas-Inteligentes-de-Transportes-la-tecnologia-en-el-transporte-terrestre-20220203-0140.html

- Cobro electrónico de peajes: diseñadas para reducir el tiempo de espera en las casetas de cobro y de esta manera mejorar los tiempos de recorrido.

- Información del impacto ambiental: Algunos sistemas también pueden obtener información de las emisiones de dióxido de carbono de los tubos de escape. Su estimación es muy valorada para interpretar el impacto que tiene el transporte en el medio ambiente.

- Conteo de tráfico: Con este sistema se obtiene información de la cantidad de vehículos que pasan por una ruta durante las 24 horas. Con este dato se arman informes útiles para la planeación de nuevas rutas, caminos alternativos o ampliaciones.

  En Colombia la iniciativa ITS busca apoyar y dar lineamientos para el diseño e implementación de los sistemas inteligentes de transporte en todo el país a través del uso de estándares internacionales.

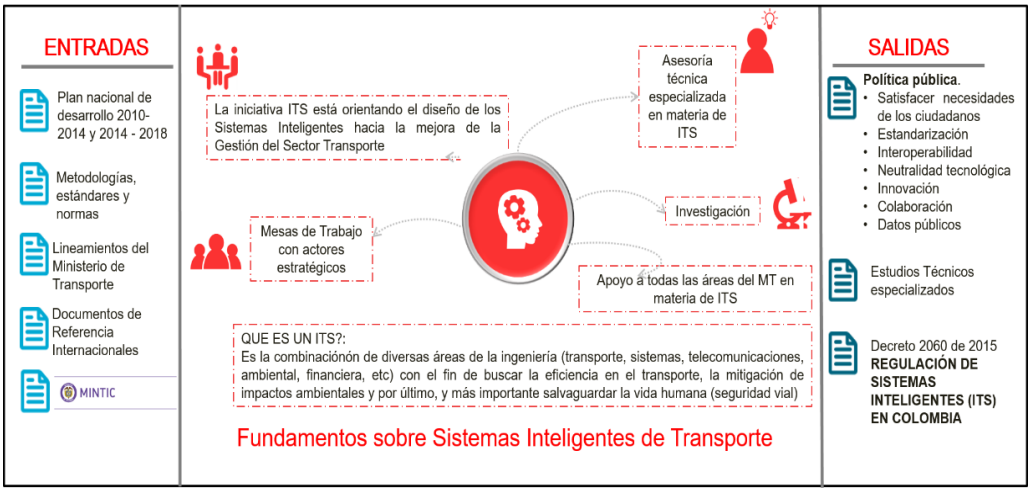

Ilustración 2 Fundamentos ITS en Colombia. Tomado de ministerio de transporte https://mintransporte.gov.co/ ¿Qué es ITS?

4.1.3 Ciberseguridad en Colombia. Se entiende que la ciberseguridad tiene como objetivo principal la protección de la información digital, que se transmite entres dispositivos que se encuentran interconectados, por lo que hace parte de la seguridad informática, que busca reducir los riesgos hasta un nivel aceptable, reduciendo los riesgos y buscando diferentes acciones encaminadas a proteger algún tipo de peligro. En el caso puntual de Colombia “En el año 2011 se realizó el consejo nacional de política económica y social, donde se estableció el conpes

3701, documento que busca generar lineamientos de la política de la ciberseguridad y la ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país"[9], con el fin principal de establecer las causas y efectos que permiten el desarrollo de políticas de prevención y de control. Ante los incrementos de amenazas informáticas, a partir de este documento y otros más se establece el decreto 338 del 2022 que es el más reciente y presenta los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.

4.2 MARCO CONCEPTUAL

4.2.1 Redes de comunicación industrial. Las redes de comunicación industrial son sistemas de interconexión de dispositivos y equipos de automatización industrial para el intercambio de datos y la supervisión de procesos en tiempo real. Estas redes permiten la comunicación entre diferentes equipos y sistemas, lo que permite la optimización de la producción, la mejora de la eficiencia y la reducción de costos. Las redes de comunicación industrial se utilizan en diferentes sectores, como la manufactura, la automatización de procesos, la energía, el transporte y la infraestructura. Algunos ejemplos de redes de comunicación industrial incluyen Ethernet Industrial, PROFIBUS, DeviceNet, Modbus, entre otros. Estas redes son esenciales para la implementación de la automatización industrial y la digitalización de los procesos de producción en la industria moderna. [10]

4.2.2 Protocolos de comunicación. Los protocolos de comunicación son conjuntos de reglas y estándares que definen el formato, la secuencia y el significado de los mensajes intercambiados entre dos o más dispositivos o sistemas de comunicación. Estos protocolos permiten la comunicación eficiente y confiable entre diferentes dispositivos y sistemas en una red de comunicación, independientemente del fabricante o modelo. Los protocolos de comunicación

[9] VALOYES, Amancio. Ciberseguridad en Colombia. (Universidad piloto de Colombia). [consultado el 13 de marzo de 2023] Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

[10] Centro de formación técnica para la industria. (s.f.). *Qué son las redes de comunicación industrial.* Recuperado el 15 de marzo de 2023, de aula 21: https://www.cursosaula21.com/que-son-las-redes-de-comunicacion-industrial/

pueden ser de diferentes tipos, como protocolos de red, protocolos de transporte, protocolos de aplicación, entre otros. Algunos ejemplos de protocolos de comunicación comunes incluyen TCP/IP, HTTP, FTP, Modbus, PROFIBUS, entre otros. Los protocolos de comunicación son esenciales para la interoperabilidad y la integración de diferentes sistemas y dispositivos en una red de comunicación, lo que permite la optimización de la producción, la mejora de la eficiencia y la reducción de costos en diferentes sectores de la industria[11].

4.2.4 NIST-CSF. Marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología, se originó en una orden ejecutiva emitida por el presidente de los Estados Unidos, Barack Obama, en febrero de 2013. La orden ejecutiva (EO 13636) se emitió en respuesta a un número creciente de ciberataques contra los sistemas de información del gobierno, la industria y los ciudadanos estadounidenses[12].

NIST-CSF cuenta con pautas, mejores prácticas y estándares desarrollados para ayudar a las organizaciones a administrar y reducir el riesgo de ciberseguridad. El NIST-CSF está diseñado para ser flexible y adaptable a diferentes industrias, sectores y organizaciones de todos los tamaños, NIST ha sido ampliamente adoptado por organizaciones de todo tipo y tamaño en todo el mundo. Ha sido reconocido como un enfoque efectivo y práctico para la gestión del riesgo de ciberseguridad, y ha sido utilizado por el gobierno de los Estados Unidos como referencia en sus propios programas de ciberseguridad.

4.3 ANTECEDENTES Y ESTADO ACTUAL

El concepto de ITS apareció por primera vez en el manejo y control de flotas de tráfico (compañías de transporte) y fue expuesta como parte de la feria de General Motors en Furama en el año de 1940, en esta misma época, Japón y EE.UU habían

[11] KIO NET WORS. ¿Qué son y para qué sirven los protocolos de comunicación de redes? [Consultado el 12 de marzo de 2023] disponible en https://www.kionetworks.com/blog/data-center/protocolos-de-comunicaci%C3%B3n-de-redes

[12] OEA, AWS. CIBERSEGURIDAD MARCO NIST, Un abordaje integral de la ciberseguridad. (2019). Disponible en https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

alcanzado gran ventaja en la Industria telemática aplicada al sector del transporte, lo que genero un gran reto a la industria Europea y dio paso a investigaciones y creación de programas para la cobertura de los sistemas integrados en las carreteras[13]. De esta manera, se inician programas y proyectos que permiten potenciar los sistemas de transporte a través de la transmisión de datos, sistemas de ayuda de navegación, sistemas de ubicación geoespacial, entre muchos otros, que han estado muy ligadas al desarrollo de las tecnologías inalámbricas abiertas.

Actualmente a nivel mundial existen muchos métodos orientados en planificación y administración de los ITS, que funcionan en pro de aumentar la seguridad preventiva ante posibles dificultades o problemas, mejorar la movilidad y accesibilidad en las ciudades, y están formados por varias soluciones tecnológicas que le brindan soporte al transporte, mediante estaciones meteorológicas, cámaras, rastreos, paneles informativos, mensajería, semaforización, carreteras inteligentes, etc, lo cual permiten controlar información obtenida en las carreteras y le facilita las labores a los conductores.

Específicamente en Colombia, los ITS empezaron a tener auge desde la primera central automatizada de control de semáforos, posteriormente se fueron ampliando e implementando en diferentes procesos a nivel de transporte y en obras de infraestructura vial, con el objetivo principal de crear de vías y ciudades inteligentes[14]. Estos avances van permeados de un crecimiento rápido en informática y robótica, y si bien, en el país muchos de los desarrollos más grandes se dan en las principales ciudades como Bogotá, Medellín, Cali, Barranquilla, con la implementación y ejecución de sistemas creados como estrategia de solución ante deficiencias en los antiguos sistemas de transporte urbano (por ejemplo el SITP y Transmilenio en la ciudad de Bogotá), también se viene desarrollando en gran medida en la creación de vías inteligentes en muchos lugares del territorio nacional.

[13] SUAREZ, Mercedes. Los sistemas inteligentes de transporte ITS. Ciencia e Ingeniería Neogranadina. (2001) Disponible en https://www.redalyc.org/pdf/911/91101006.pdf

[14] VELAZCO, Sandra; FERRO, Roberto; CUARTAS, Katherin. Sistemas Integrados de Transporte soportados en el internet de las cosas. (2016). Disponible en https://revistas.udistrital.edu.co/index.php/REDES/article/view/11995

4.4 MARCO LEGAL

En Colombia se vienen estableciendo las diferentes leyes y lineamientos generales que buscan fortalecer los procesos ciberseguridad, seguridad informática y digital, actualmente se tienen los siguientes referentes legales:

Decreto 338 del 8 de marzo de 2022[15], donde el ministerio de Tecnologías de la Información y las comunicaciones, presenta los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital.

Documento Conpes 3701 del 2011[16], en el cual el Consejo Nacional de Política Económica y Social, presenta los lineamientos de política para ciberseguridad y ciberdefensa en Colombia.

Documento Conpes 3995 del 2020[17], el cual presenta la Política nacional de confianza y seguridad digital.

[15] Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto 338 de 2022 "Lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital". Consultado el [01 de abril de 2023] Disponible en https://www.crossbordertech.com/decreto-338-de-marzo-de-2022-ciberseguridad-en-colombia/#:~:text=El%20Decreto%20338%20de%20marzo,seguridad%20digital%20entre%20otras%20disposiciones.

[16] Consejo Nacional de Política Económica y Social Republica de Colombia. Documento Conpes 3701: lineamientos de política para ciberseguridad y ciberdefensa. (2011). [consultado el 10 de abril de 2023]. Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

[17] Consejo Nacional de Política Económica y Social Republica de Colombia. Documento Conpes 3995: Política nacional de confianza y seguridad digital. (2020). [consultado el 10 de abril de 2023]. Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

4.5 MARCO METODOLÓGICO

La metodología del presente proyecto es de análisis documental, donde se busca generar inicialmente una revisión de diferentes documentos acerca de la funcionalidad de un sistema SCADA en relación con la implementación de estos en sistemas inteligentes de transporte (ITS) en Colombia, se pretende revisar los incidentes, riesgos, vulneraciones, amenazas y demás factores que influyen en las problemáticas de ciberseguridad que pueden presentar estos sistemas.

Para ello se realizará una búsqueda de información general que permita analizar la seguridad en la integración de un sistema SCADA a nivel mundial, identificando que es, como funciona y como se implementa esta herramienta, y así mismo verificar como se integra en los sistemas inteligentes de transporte (ITS) en Latinoamérica y en Colombia, identificando incidentes de seguridad que puedan poner en riesgo la integridad de la información. Luego se categorizarán herramientas de integración de SCADA en los ITS con el fin de determinar cuáles llegan a ser las más adecuadas según su funcionalidad, compatibilidad para un proceso de integración articulado con lineamientos de seguridad.

Finalmente, después de realizar las diferentes búsquedas y análisis correspondientes, se pretende proponer buenas prácticas basadas en la información recolectada y teniendo como base el marco de ciberseguridad NIST-CSF, que permitan salvaguardar la información durante un proceso de integración de un sistema SCADA en sistemas inteligentes de transporte (ITS) en Colombia.

5 DESARROLLO DE OBJETIVOS

5.1 ESTABLECER LA FUNCIONALIDAD DE UN SISTEMA SCADA A PARTIR DE UNA REVISIÓN DOCUMENTAL CON EL FIN DE IDENTIFICAR INCIDENTES DE SEGURIDAD QUE PUEDAN PONER EN RIESGO LA INTEGRIDAD DE LA INFORMACIÓN EN SISTEMAS INTELIGENTES DE TRANSPORTE (ITS) EN COLOMBIA.

Los Sistemas de Control y Adquisición de Datos (SCADA) son herramientas fundamentales en el monitoreo y control de procesos industriales. Estos sistemas permiten la supervisión en tiempo real de los procesos y la adquisición de datos para su posterior análisis, toma de decisiones y configuraciones centralizadas de los equipos que la componen. En el contexto de los Sistemas Inteligentes de Transporte (ITS), los sistemas SCADA juegan un papel crucial en la integración y gestión de los procesos de transporte, desde la infraestructura hasta los vehículos y usuarios.

Sin embargo, los sistemas SCADA pueden estar expuestos a incidentes de seguridad que pueden comprometer la integridad de la información y poner en riesgo la seguridad del sistema en su totalidad. Por lo tanto, es importante establecer la funcionalidad de un sistema SCADA a través de una revisión documental con el fin de identificar posibles incidentes de seguridad y tomar medidas preventivas.

5.1.1 Funcionalidad de un sistema SCADA. La funcionalidad de un sistema SCADA se refiere a las características y capacidades que tiene el sistema para llevar a cabo el monitoreo, control y adquisición de datos en tiempo real. Los sistemas SCADA permiten la recolección de datos de diferentes sensores y dispositivos instalados en el sistema, y luego los procesan para su análisis y toma de decisiones. También permiten la regulación y el control de los procesos de transporte mediante diferentes algoritmos de control, y supervisan los procesos en tiempo real para detectar posibles fallas o incidentes de seguridad.

Algunas características básicas de un sistema SCADA son[18]:

[18] REDONDO, Manel; MORENO Romualdo. Diseño e implementación de un sistema SCADA para una planta de producción y envasado de líquidos. (2008). Consultado en https://core.ac.uk/download/pdf/13284214.pdf

- Adquisición y almacenamiento de datos, para recoger, procesar y almacenar la información recibida de forma continua y confiable.

- Representación gráfica y animada de variables de proceso y monitorización de éstas por medio de alarmas.

- Ejecución de acciones de control, para modificar la evolución del proceso.

- Arquitectura abierta y flexible con capacidad de ampliación y adaptación.

- Conectividad con otras aplicaciones y bases de datos, locales o distribuidas en redes de comunicación.

- Supervisión, para observar desde un monitor la evolución de las variables de control.
- Transmisión de información con dispositivos de campo y otros PC.

- Base de datos, gestión de datos con bajos tiempos de acceso.

- Presentación, representación gráfica de los datos. Interfaz del Operador o HMI (Human Machine Interface).

- Explotación de los datos adquiridos para gestión de la calidad, control estadístico, gestión de la producción y gestión administrativa y financiera.

- Alertas al operador de cambios detectados y que pueden ser almacenados en el sistema para su posterior análisis

5.1.1.1 Funcionalidad En Sistemas De Transporte Inteligente (ITS). La funcionalidad de un sistema SCADA se refiere a las capacidades y características del sistema para integrar y gestionar los procesos de transporte, desde la infraestructura hasta los vehículos y usuarios. Los sistemas SCADA permiten la supervisión en tiempo real de los procesos de transporte, adquiriendo datos de diferentes sensores y dispositivos instalados en las carreteras, vehículos, estaciones, etc. También permiten el control y regulación de los procesos de transporte, como la velocidad de los vehículos, la apertura y cierre de puertas en estaciones, y el control de semáforos, entre otros.

5.1.1.2 Adquisición De Datos. Consiste en la recolección de datos de diferentes sensores y dispositivos instalados en el sistema. Estos datos son enviados al sistema SCADA para su procesamiento y análisis posterior.

5.1.1.3 procesamiento de datos. Proceso donde se lleva a cabo el análisis de los datos adquiridos. El sistema SCADA utiliza diferentes algoritmos y modelos matemáticos para identificar patrones y tendencias en los datos, lo que permite una mejor comprensión del sistema y una toma de decisiones más informada.

5.1.1.4 Control. Es donde se lleva a cabo la regulación y el control de los procesos de transporte. El sistema SCADA utiliza diferentes algoritmos de control para regular la velocidad de los vehículos, la apertura y cierre de puertas en estaciones, el control de semáforos, entre otros.

5.1.1.5 Monitoreo. Es donde se supervisan los procesos en tiempo real y se toman medidas preventivas en caso de incidentes o fallas en el sistema. El monitoreo es fundamental para garantizar la seguridad del sistema y la integridad de la información.

5.1.1.6 Identificar incidentes de seguridad. Los posibles incidentes de seguridad en sistemas SCADA, estos pueden ser causados por fallas en el hardware o software, ataques cibernéticos, errores humanos, entre otros. Algunos de los incidentes de seguridad más comunes incluyen la exposición de contraseñas y credenciales de acceso, la interrupción del suministro eléctrico, la modificación de la configuración del sistema, y la inyección de código malicioso.

Amenazas Internas

- Errores Humanos: Fallos en la operación o configuración del sistema por parte del personal.

- Acceso No Autorizado: Empleados descontentos que podrían abusar de sus privilegios.

Amenazas Externas

- Ciberataques: Ataques dirigidos por hackers que buscan comprometer el control del sistema.

- Malware: Software malicioso que puede infectar el sistema y causar interrupciones.

Fugas de Información

- Accesos No Autorizados: Personas no autorizadas que obtienen acceso a datos críticos.

- Exposición de Datos Sensibles: Datos personales de usuarios o información crítica del sistema.

Impacto:

- Pérdida de Confianza: Daño a la reputación del sistema y pérdida de confianza pública.

- Consecuencias Legales: Posibles sanciones y responsabilidades legales.

5.1.2 Incidentes de seguridad del sistema SCADA en ITS. Los sistemas SCADA utilizados en los ITS pueden ser vulnerables a una serie de incidentes de seguridad o ciberseguridad que podrían poner en riesgo la seguridad y la integridad de los sistemas de transporte y la información relacionada. A continuación, se presentan algunos ejemplos de incidentes de seguridad que pueden afectar a un sistema SCADA integrando ITS:

1. Ataques de denegación de servicio (DDoS): un ataque DDoS puede saturar el ancho de banda del sistema y provocar una interrupción del servicio, lo que podría afectar negativamente la eficiencia del sistema de transporte y la seguridad de los pasajeros.

2. Ataques de malware: los sistemas SCADA integrando ITS pueden ser vulnerables a ataques de malware, que pueden infectar el sistema y robar información confidencial o incluso tomar el control del sistema.

3. Ataques de ingeniería social: los atacantes pueden utilizar técnicas de ingeniería social para obtener información confidencial, como contraseñas, nombres de usuario y otra información sensible, y luego utilizar esa información para acceder al sistema SCADA y causar daños.

4. Vulnerabilidades de red o de interconexión: Los sistemas SCADA están conectados a redes de comunicaciones y con otros sistemas, lo que significa que pueden ser vulnerables a ataques a través de la red. Si un atacante puede infiltrarse en la red, puede controlar los dispositivos y manipular los datos.

5. Vulnerabilidades de autenticación y autorización: Los sistemas SCADA suelen requerir autenticación y autorización para acceder a los datos y los dispositivos. Si un atacante puede comprometer el sistema de autenticación y autorización, puede obtener acceso no autorizado y manipular los datos.

6. Vulnerabilidades en el software y hardware: las vulnerabilidades en el software y hardware pueden ser explotadas por los atacantes para obtener acceso no autorizado al sistema. Los sistemas SCADA suelen utilizar software específico y personalizado, que puede contener vulnerabilidades de seguridad. Si un atacante puede explotar una vulnerabilidad de software, puede controlar los dispositivos y manipular los datos.

7. Acceso físico no autorizado: el acceso físico no autorizado a los sistemas SCADA integrando ITS puede permitir que los atacantes instalen dispositivos maliciosos o alteren el hardware y software del sistema, lo que puede tener consecuencias graves para la seguridad del sistema.

Actualmente no se cuenta con mucha investigación publicada sobre las amenazas de ciberseguridad contra ITS, y aunque los ataques contra esta infraestructura han sido pocos y esporádicos, si es claro que entre más avances de conectividad circulen por las carreteras, las amenazas aumentarán con el tiempo, especialmente cuando los delincuentes descubran nuevos modelos de especulación, debido a que los ITS son altamente visibles y los ataques contra ellos pueden llegar a ser de alto impacto.

5.2 IDENTIFICAR HERRAMIENTAS EN LA INTEGRACIÓN DE UN SISTEMA SCADA, EN SISTEMAS INTELIGENTES DE TRANSPORTE (ITS), MEDIANTE LA DEFINICIÓN DE CRITERIOS COMO FUNCIONALIDAD, COMPATIBILIDAD, FACILIDAD DE INTEGRACIÓN.

Los sistemas SCADA implementados en Sistemas Integrados de Transporte, se utilizan bajo herramientas o sistemas aplicativos de software (cliente-servidor) que, si bien ofrecen un nivel de servicio estándar o general, internamente se establecen manejos según la necesidad de implementación que requiere cada uno, es decir, dependiendo el tipo de operación se debe buscar un SCADA que cumpla con los requerimientos necesarios para sus servicios, a continuación se presentan algunas herramientas importantes para esta integración importantes para el funcionamiento de SCADA en ITS y se realiza una relación de estos respecto a los criterios de funcionalidad, compatibilidad, integración, luego se presentan dos tipos de software realizando un comparativo teniendo en cuenta lo que ofrece cada uno respecto a los criterios y herramientas nombrados anteriormente.

5.2.1 Herramientas de SCADA en ITS

1. Equipos de captación de información. Son definidos como herramientas que permiten la recopilación y transmisión de información importante, son fundamentales para la automatización de procesos y toma de decisiones. En esta ocasión teniendo en cuenta su implementación en los ITS están clasificados en dos grupos:

a. Equipos de información en cielo abierto: son todos aquellos que se encuentran sobre las infraestructuras viales tales como paneles solares, radares, controles de galibo, sos, cámaras, estaciones meteorológicas, paneles, entre otros. Estos están ubicados de manera externa al lugar de control y supervisión y se encuentran a lo largo de las estructuras viales.

Ilustración 3 Sistema SCADA en proyecto de infraestructura vial en Antioquia. Se evidencian algunos equipos de captación a cielo abierto.

b. Redes de comunicación: Son los que se encuentran ubicados en el datacenter o centro operativo ubicados en una estación de trabajo y es desde allí donde se encargan de recibir toda la información en tiempo real de todos los equipos que se encuentran externamente y de llevar a cabo el control y manejo de todo este sistema.

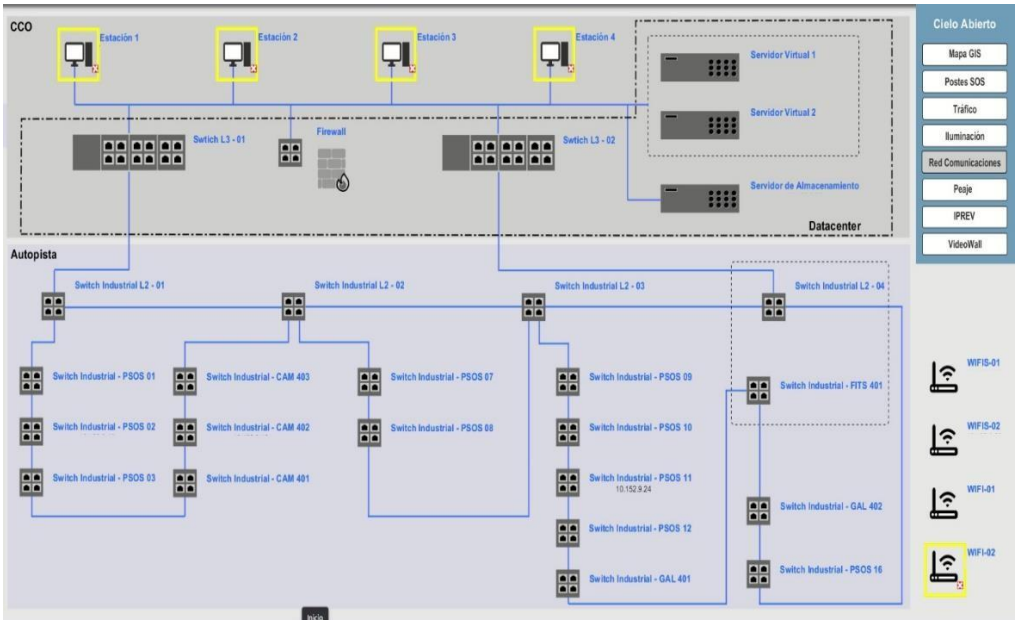

Ilustración 4. Sistema SCADA en proyecto de infraestructura vial en Antioquia

2. Servicios básicos de SCADA en ITS. En este sentido el sistema SCADA en el caso de los ITS debe cumplir con aspectos y servicios básicos contemplados a continuación:

a. Sistemas de gestión y operación: se debe contar con una operación dentro de límites de tolerancia definidos para que el tráfico fluya sin problemas, evitando que se presenten atascos, retrasos, accidentes en los cuales se pueden incluir controles de alumbrado público, gestión de desastres, gestión de datos y almacenamiento de datos, gestión de vehículos.

b. Controles de flujo de tráfico: ayudan a que el tráfico de alto volumen sea más eficiente y que las carreteras sean más seguras, realizando una supervisión del tráfico y las condiciones de la carretera en tiempo real, en estos se incluyen: sistemas de control de señales de tráfico, barreras de cruce de ferrocarril, señales de mensajes dinámicos y cobro de peaje automatizado (telepeaje).

c. Informe de carreteras: ayudan a que el movimiento de tráfico de alto volumen sea más eficiente y se mejore la seguridad vial. Para ello se requiere monitorear constantemente el tráfico y las condiciones actuales de las carreteras, vías, caminos, para lo cual se usa una amplia gama de cámaras, sensores, radares, estaciones meteorológicas, sistemas de detección de vehículos, que se colocan estratégicamente en toda la calzada y que envía información en tiempo real al centro de control.

d. Sistemas de Pago y aplicaciones: aparte de la organización del tráfico y el mejoramiento de la seguridad vial, un objetivo principal en los operadores de ITS es usar los sistemas existentes para aumentar su flujo de ingresos y reducir los costos, en estos se incluyen los pagos/etiquetas RFID, máquinas de pago de quiosco y aplicaciones de boletos electrónicos.

Es importante señalar que los equipos de captación y los servicios básicos se complementan para una adecuada implementación de sistema SCADA en los sistemas integrales de transporte, en la siguiente tabla podemos ver la relación que cumplen cada uno teniendo como base los criterios de funcionalidad, compatibilidad y facilidad de integración.

	FUNCIONALIDAD	COMPATIBILIDAD	INTEGRACIÓN
EQUIPOS DE CAPTACION A CIELO ABIERTO	Recopilan datos ambientales y de tráfico en tiempo real, esenciales para la supervisión y control del tráfico vial.	Deben ser compatibles con diversos sensores y dispositivos de monitoreo, asegurando que puedan integrarse sin problemas con otros componentes del sistema.	Instalados externamente a lo largo de las infraestructuras viales, deben integrarse fácilmente con sistemas de comunicación remota, permitiendo una implementación sencilla y mantenimiento eficiente.
REDES DE COMUNICACIÓN	Transmiten y procesan información de los equipos de campo al centro de control, permitiendo la gestión centralizada de datos y la toma de decisiones en tiempo real.	Necesitan ser compatibles con diversas tecnologías de comunicación (por ejemplo, fibra óptica, inalámbrica, protocolos de comunicación), garantizando la interoperabilidad con otros sistemas ITS.	Deben integrarse con sistemas SCADA y otros subsistemas ITS, facilitando la centralización de la información y el control.
SERVICIOS BASICOS DE SCADA EN ITS	controlan operaciones de tráfico, alumbrado público, gestión de desastres y almacenamiento de datos; supervisan y gestionan el tráfico para mejorar la eficiencia y seguridad; monitorean el estado de las carreteras y proporcionan informes en tiempo real; y facilitan el cobro de peajes y pagos electrónicos para mejorar la eficiencia operativa.	Estos sistemas interactúan con múltiples subsistemas y protocolos, integran sistemas de control de señales, barreras ferroviarias y telepeajes, utilizan cámaras, sensores y estaciones meteorológicas, y son compatibles con sistemas de RFID, quioscos de pago y aplicaciones móviles.	Los sistemas SCADA en ITS permiten una fácil implementación y escalabilidad dentro de los sistemas de transporte inteligente, se comunican en tiempo real con el centro de control, y se integran fácilmente con sistemas de gestión de tráfico y finanzas, asegurando una instalación y mantenimiento eficiente.

Tabla 1. Relación de herramientas de SCADA en ITS. Elaboración propia

5.2.2 Softwares de integración de SCADA en ITS

Actualmente en Colombia se está en la constante búsqueda de herramientas que permitan una óptima integración de sistemas SCADA por lo que se opta por software que sean versátiles, flexibles y potentes. A continuación, se presenta dos opciones de implementación de estas herramientas.

5.2.2.1 Software WinCC OA.

"Es una herramienta muy versátil, que permite personalizar al máximo la infraestructura de automatización y control, está asociado a una base de datos amplia y coherente, que une información de todo tipo, desde la performance de una máquina hasta todo lo que hay que saber durante la integración del sistema como tal"[19]. WinCC OA ofrece una serie de beneficios técnicos y características que lo hacen una solución destacada para integrar sistemas SCADA en entornos de transporte inteligente:

- Orientación a objetos: Su enfoque en la programación orientada a objetos facilita una ingeniería eficiente y escalable, permitiendo la reutilización del código y la construcción de sistemas personalizados.

- Sistema distribuido: WinCC OA descentraliza la información para una mayor seguridad, permitiendo hasta 2048 servidores y garantizando la disponibilidad del sistema.

- Escalabilidad: Se adapta a sistemas de cualquier tamaño o complejidad, desde sistemas locales pequeños hasta grandes sistemas distribuidos, asegurando su flexibilidad ante los cambios.

- Fiabilidad: Con protocolos de redundancia y sistemas de recuperación ante desastres, asegura un alto nivel de disponibilidad y protege contra fallos inesperados.

- Compatibilidad: Es compatible con una amplia variedad de sistemas operativos y dispositivos, permitiendo el monitoreo desde cualquier equipo y ofreciendo funcionalidades móviles tanto para Android como para iOS. Algunos de estos

[19] MEINSA. WinCC OA, tu solución para la integración de sistemas SCADA.S.F. consultado en https://meinsa.com/2021/05/wincc-oa-integracion-sistemas-scada/

son:OPC (OLE for Process Control); Modbus (RTU y TCP); DNP3 (Distribuited Network Protocol); IEC 61850 (para subestaciones eléctricas); BACnet (Building Automation and Control Network); S7 (Siemens S7 Protocol); HTTP/HTTPS; SNMP; MQTT; TCP/IP; UDP.

- Certificaciones oficiales: Cumple con estándares regulatorios como la normativa FDA 21 CFR Part 11 y cuenta con certificaciones de seguridad SIL 3 según la IEC 61508.

Ilustración 5.WinCCOA en una concesión vial en Antioquia

Así mismo WinCC OA, se basa en unas unidades programáticas denominadas 'Manager', las cuales ejecutan funciones específicas del programa de manera autónoma y distribuida y se adaptan dinámicamente según la demanda, ofreciendo una gestión eficiente de recursos y maximizando la compatibilidad, y entre sus herramientas adicionales, este software ofrece funcionalidades como la integración de sistemas de gestión de vídeo, herramientas avanzadas de reproducción y simulación, clientes web basados en HTML5, visualización GIS y generación de informes con plantillas BIRT, entre otras.

5.2.2.1.1 Entorno De Desarrollo – WinccOA

Yunex Traffic ha desarrollado una solución de sistema de gestión de tráfico en WinccOA tomando todos los beneficios al ser una plataforma ABIERTA para desarrollo del SISTEMA DE GESTIÓN DE TRÁFICO la cual cuenta con un conjunto de herramientas y recursos que permite a los desarrolladores crear software de manera eficiente. Esta plataforma ofrece la libertad de crear aplicaciones con una

amplia variedad de widgets desarrollados en el sistema. También permite crearlas desde cero con la posibilidad de desarrollar APIs de integración y funcionalidades graficas mediante QT Dessigner, permitiendo la configuración y entornos de desarrollo de pruebas, depuración y documentación. Esto permite a los desarrolladores crear y distribuir aplicaciones con mayor rapidez, mejorando la calidad del software y reduciendo los costos de desarrollo. Los principales beneficios de WinccOA al ser una plataforma abierta que podrán ser aprovechados por la Concesión Autopista Río Magdalena son: Flexibilidad: Es compatible con la mayoría de los sistemas operativos, dispositivos, motores de bases de datos y protocolos de comunicación industriales. Esto les permite a los usuarios (Desarrolladores y administradores del sistema) crear aplicaciones personalizadas que pueden ser integradas al SISTEMA DE GESTIÓN DE TRÁFICO SITHICC® sin problemas. Facilidad de uso: Es amigable para el usuario ya que ofrece una interfaz intuitiva y fácil de usar. Permitiendo la creación rápida y fácil de aplicaciones nuevas sin necesidad de experiencia previa, basta tener conocimientos básicos de programación. Escalabilidad: Permite a los usuarios añadir más dispositivos y funcionalidades según sea necesario. Esto significa que puede utilizarse para proyectos de cualquier tamaño y complejidad. Soporte: WinccOA cuenta con un equipo de soporte dedicado para ayudar a los usuarios con cualquier problema que puedan tener. Esto significa que los usuarios siempre tendrán ayuda cuando la necesiten. Una plataforma abierta proporciona una solución flexible, escalable y personalizable que permite a los usuarios la creación de nuevas funcionalidades o mejora de las existentes. Esto se logra a través de una interfaz de usuario intuitiva y potente con herramientas de desarrollo. Esta plataforma también proporciona una comunidad en la que los usuarios pueden colaborar para compartir sus conocimientos, experiencias y mejores prácticas. Esto les permite aumentar la productividad, descubrir nuevas oportunidades y mejorar su habilidad para adaptarse a un entorno cambiante. Teniendo en cuenta que cualquier desarrollador con conocimientos básicos en programación puede modificar agregar o crear nuevas herramientas para mejorar el sistema.

se hace aún más atractivo este entorno de desarrollo ya que el personal con el cual deberá contar no necesariamente serán perfiles con especializades que incrementarán el costo de la mantención y actualización del sistema. Como se muestra en la Ilustración 6: Capas de control SISTEMA DE GESTIÓN DE TRÁFICO. El sistema está diseñado para tener 3 capas, teniendo una arquitectura cliente servidor y una comunicación por medio de controladores o protocolos estándar de comunicación para conectarse a todos los equipos del proyecto.

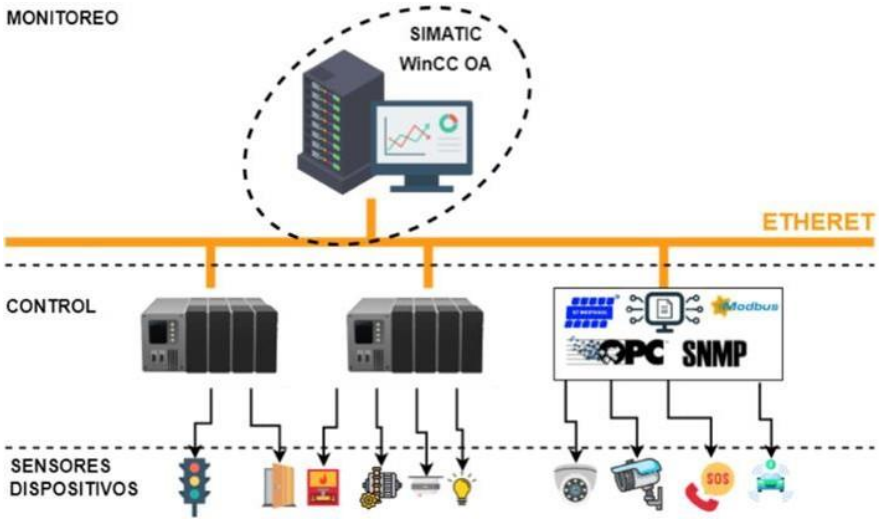

Ilustración 6.Capas de Control Sistema de Gestión de Tráfico
https://www.winccoa.com/

5.2.2.1.2 Arquitectura de Operación WinccOA

WinccOA es un sistema de construcción modular. Las funcionalidades requeridas son manejadas por unidades específicas que fueron creadas para diferentes tareas. En WinccOA estas unidades se denominan gestores - los gestores son procesos de software propios, tal como se describe en la ilustración 7. Por ejemplo, hay un gestor independiente para las conexiones de periferia, almacenamiento de datos de historia, interfaz de usuario, conexión API de terceros, entre otros.

- Event-Manager (EV): El gestor de eventos es el corazón de WinccOA, y quien evalúa el correcto funcionamiento de los demás gestores del proyecto.

- Driver-Manager(D): El gestor de drivers se encarga de controlar los procesos están vinculados a cada uno mediante el número del controlador y su tipo de comunicación.

- Data-Manager (DB): En el gestor de base de datos se ejecutan procesos para base de datos de alta velocidad, almacenamiento consulta y administración.

- Control Manager (CTRL): El gestor de control es un run time de ejecución dedicado, que procesa los programas escritos en el lenguaje de programación de control en una base multitarea orientada a eventos.

- User Interface-Manager (UI): El gestor de interfaz de usuario se encarga de la visualización gráfica de los estados del proceso en cada una de las estaciones de trabajo.

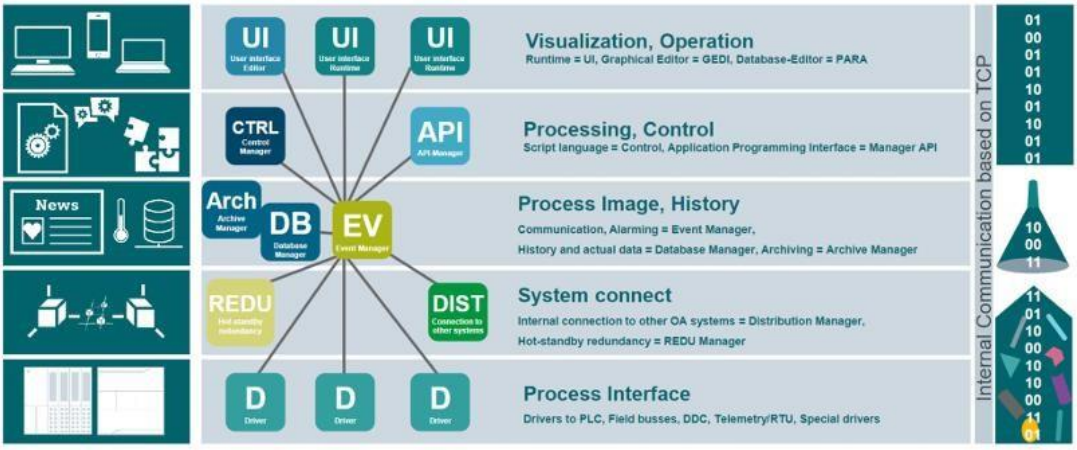

Ilustración 7.Arquitectura de Gestión WinccOA
https://www.winccoa.com/

5.2.2.2 Software FactoryTalk View.

Este software "es una plataforma desarrollada por Rockwell Automation para la supervisión y control de procesos industriales. Es una versátil aplicación de interfaz operador-máquina (HMI) que ofrece una solución robusta y dedicada para dispositivos de interfaz de operador a nivel de máquina"20, está diseñado para proporcionar una solución completa de visualización, monitorización y control en tiempo real para una amplia variedad de aplicaciones industriales, incluyendo manufactura, procesamiento de alimentos y bebidas, y sistemas de energía.

FactoryTalk del líder mundial Rockwell Automation, la cual ha sido ampliamente probada en proyectos complejos (más de 15.000 proyectos por año). Una de las razones por las que el sistema SCADA está basado en FactoryTalk de Rockwell Automation es que, al ser la principal plataforma de automatización a nivel mundial, cuenta con una extensa red de empresas –llamada Encompass Partners- de nivel mundial que fabrican soluciones como cámaras, sistemas de iluminación, sistemas de ahorro de energía, sistemas de georreferenciación, sistemas de comunicaciones, sistemas de gerenciamiento de activos, sistemas de gerenciamiento de mantenimiento de activos etc, que no solo integran sino que desarrollan aplicaciones compatibles, probadas y garantizadas por Rockwell Automation, esto permite a los usuarios y clientes como Consorcios o Concesiones, contar con soluciones probadas en miles de proyectos de igual o mayor complejidad, eliminando el riesgo de desarrollos que generan incertidumbre, tiempos de espera

[20] Rockwell Automation. FactoryTalk View - Software de HMI. (s.f.) Consultado en https://www.rockwellautomation.com/es-co/products/software/factorytalk/operationsuite/view.html#:~:text=El%20software%20FactoryTalk%C2%AE%20View,operador%20a%20nivel%20de%20m%C3%A1quina.

muchas veces fuera del tiempo contemplado, sobrecostos y sorpresas desagradables durante el desarrollo del negocio.

Módulo de Interfaces Graficas.

FactoryTalk View Site Edition es un paquete de software integrado, utilizado para el desarrollo y ejecución de interfaces hombre-máquina (HMI) que involucran múltiples usuarios, servidores y distribución a lo largo de una red, además de proveer todas las herramientas requeridas para crear aplicaciones poderosas, que reflejan el estado de los procesos, le permite monitorearlos, supervisarlos y controlarlos.

En la aplicación FactoryTalk View Studio, es posible crear la red distribuida del aplicativo FactoryTalk View, administrar la estación de red o las aplicaciones para las estaciones locales que presenten la información del proceso, además de crear y probar la aplicación y todos los componentes necesarios de ésta. De esta forma tendrá un sistema integrado desde el cual podrá administrar el sistema y permitirá a los usuarios interactuar con el proceso.

La plataforma de servicios FactoryTalk provee un conjunto de servicios común, tales como mensajes de diagnóstico, monitoreo del estado de los diferentes equipos y componentes del sistema, y brinda acceso en tiempo real a la información de todos los productos FactoryTalk que tenga la autopista y/o túnel. Utilizando estos servicios se puede compartir y obtener simultáneamente acceso a recursos tales como el valor de las variables, displays gráficos que solo necesitará definir una vez en el sistema.

La plataforma de servicios, cuenta con las siguientes aplicaciones embebidas es instaladas junto con el FactoryTalk View Site Edition:

• FactoryTalk Directory**:** Este centraliza el acceso a los recursos del sistema y da nombre a todos éstos para que puedan ser utilizados por todos los aplicativos de software FactoryTalk que corran en el sistema. Directory administra todos los recursos sobre la red de control, así como los recursos locales en cada uno de los clientes del sistema.

• FactoryTalk Security: Centraliza la autenticación de usuarios y los niveles de autorización a los diferentes recursos contenidos en Directory.

• FactoryTalk Live Data: Administra la conección entre los diferentes aplicativos FactoryTalk y los diferentes servidores de datos.

• FactoryTalk Diagnostics: Colecciona y provee acceso a la actividad, estatus, alarmas y mensajes de error generados a través del sistema FactoryTalk.

• Factory Talk Administration Console: Se utiliza como herramienta stand-alone para desarrollar, administrar y configurar los niveles de seguridad de las múltiples aplicaciones del sistema.

• FactoryTalk Alarms and Events: Sistema de la plataforma FactoryTalk con la capacidad para administrar alarmas y eventos provenientes del monitoreo de los dispositivos del sistema, así como de los refelajados en los valores de las variables configuradas en el sistema, generando la trazabilidad sobre los eventos o alarmas identificados, bajo su respectiva estampa de tiempo y responsable por el mismo.

FactoryTalk View SE, como se describe, consiste en muchas piezas de software que trabajando de forma conjunta permiten crear una interfaz gráfica de operación y de interacción entre operaciones y el sistema adaptado a las necesidades del proyecto.

FactoryTalk View SE Server, también llamado servidor HMI, almacena todos los componentes del proyecto HMI (por ejemplo, las interfaces gráficas de operación) y distribuye estás de acuerdo con la demanda hacia los clientes de la aplicación. El servidor contiene además una base de datos de tags, y ejecuta la detección de alarmas y un data logging histórico. Esta plataforma no cuenta con una interfaz de usuario, una vez instalada corre como un conjunto de servicios de Windows que brindan información a los clientes tal como ellos lo requieran.

FactoryTalk View SE Client, es un software para visualización e interacción con el aplicativo FactoryTalk en una estación de operación local, una estación en la red o a lo largo de una red distribuida. Se ejecuta bajo una arquitectura cliente-servidor.

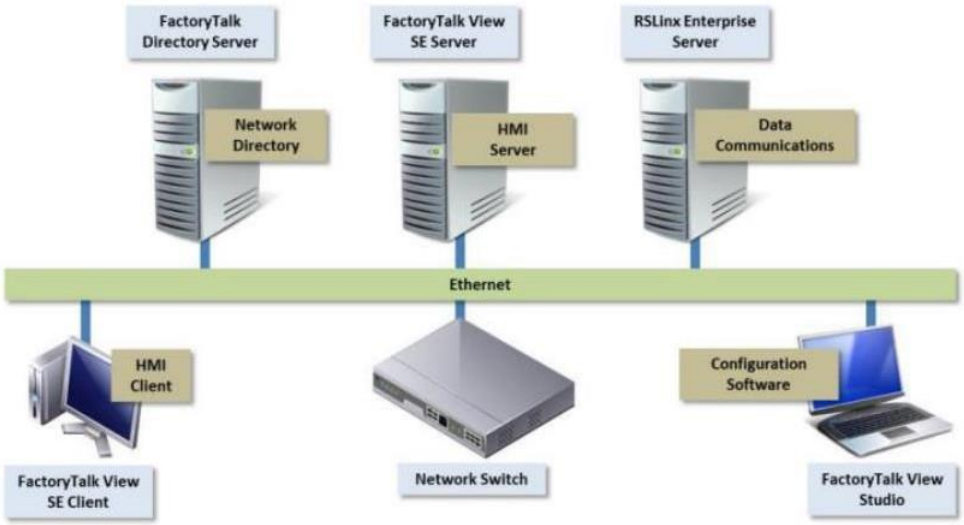

Ilustración 8.Arquitectura Factorytalk View.
https://www.rockwellautomation.com/

Sus características incluyen una interfaz gráfica intuitiva, escalabilidad desde pequeñas máquinas hasta grandes instalaciones industriales, y una integración sólida con otros productos de Rockwell Automation. Además, ofrece herramientas avanzadas de diagnóstico y análisis, y capacidades de acceso remoto a través de FactoryTalk ViewPoint:

- Integración con otros productos de Rockwell Automation: se integra perfectamente con otros productos de Rockwell Automation, lo que facilita la recopilación y el análisis de datos.

- Interfaz de usuario personalizable: Ofrece una interfaz de usuario altamente personalizable que permite a los operadores diseñar pantallas según sus necesidades específicas. Esto incluye la posibilidad de crear gráficos dinámicos, alarmas y reportes personalizados.

- Despliegue en múltiples plataformas: se presenta en dos versiones principales que son FactoryTalk View SE (Site Edition) para aplicaciones de múltiples estaciones y redes, y FactoryTalk View ME (Machine Edition) para aplicaciones de una sola estación; esto permite su uso tanto en grandes instalaciones como en aplicaciones más pequeñas y específicas.

- Seguridad y control de acceso: Incluye características avanzadas de seguridad que permiten controlar el acceso a diferentes niveles de la aplicación. Los usuarios pueden ser autenticados y autorizados mediante la integración con sistemas de seguridad de Windows y FactoryTalk Security.

- Capacidad de análisis y reportes: Integra herramientas para la creación de reportes y análisis de datos históricos. Esto es esencial para la toma de decisiones basada en datos y para mejorar la eficiencia operativa.

- Conectividad y comunicación: Soporta una amplia variedad de protocolos de comunicación, incluyendo OPC (OLE for Process Control), lo que facilita la integración con dispositivos de diferentes fabricantes y la consolidación de datos en un sistema centralizado.

- Escalabilidad: Puede escalarse fácilmente desde aplicaciones pequeñas hasta grandes sistemas distribuidos, permitiendo a las empresas crecer sin necesidad de cambiar su sistema SCADA.

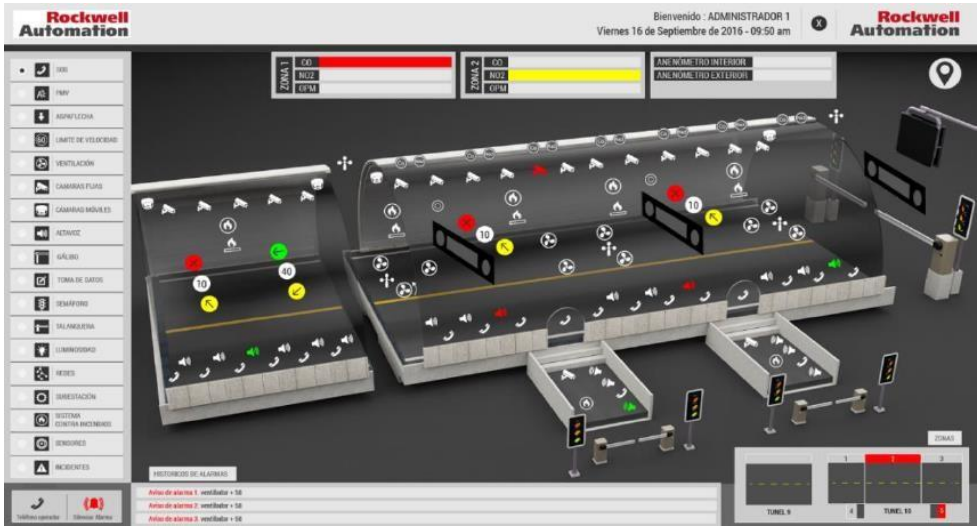

Ilustración 9. Control sistemas electromecánicos de los túneles
https://www.rockwellautomation.com/

Cuadro comparativo de las características entre WinCC OA Vs FactoryTalk View.

	Software WinCC OA	**Software FactoryTalk View**
COMPATIBILIDAD	Compatible con múltiples sistemas operativos y dispositivos, ofrece funcionalidades móviles para Android e iOS. Un soporte amplio y nativo para los protocolos, facilitando la integración en entornos industriales heterogéneos donde se utilizan múltiples dispositivos y tecnologías de diferentes fabricantes.	Es compatible con estándares industriales y protocolos de comunicación ampliamente utilizados, lo que facilita la integración con equipos y sistemas de terceros. Es dentro del ecosistema de Rockwell, pero presenta limitaciones en la compatibilidad con ciertos protocolos industriales estándar, lo que puede complicar su integración en sistemas heterogéneos.
FUNCIONALIDAD	Proporciona un enfoque de programación orientado a objetos, un sistema distribuido y escalabilidad adaptable a diferentes tamaños y complejidades de sistemas.	Herramientas avanzadas de desarrollo que permiten un despliegue rápido y eficiente de aplicaciones SCADA. La reutilización de componentes y la facilidad de configuración son puntos

		destacados en comparación con otros sistemas SCADA.
INTEGRACIÓN	Es una herramienta destacada para la integración de sistemas SCADA en ITS debido a sus características técnicas y beneficios, su diseño modular y flexible permite la personalización y adaptación dinámica a diversas demandas operativas. Además, incluye herramientas adicionales como integración de sistemas de gestión de vídeo, visualización GIS y generación de informes.	Integración nativa con otros productos de Rockwell Automation. Esto reduce significativamente el tiempo de implementación y los problemas de compatibilidad. se destaca por su integración con otros productos de Rockwell Automation, su personalización, seguridad y capacidad de análisis, así como su escalabilidad y soporte. Está diseñado para integrarse perfectamente con otros productos de Rockwell Automation, lo cual puede llevar a una menor prioridad en el desarrollo de compatibilidad con protocolos de otros fabricantes.

Tabla 2. Ejemplo comparativo de software. Elaboración propia

Si bien estos softwares se postulan como soluciones integrales y versátiles para la integración de sistemas SCADA en sistemas de transporte inteligente, destacándose por su flexibilidad, seguridad, fiabilidad y compatibilidad con estándares industriales y tienen en cuenta los equipos de información y redes de comunicación antes nombradas, es necesario siempre mantener acciones que salvaguarden la información y permitan el buen funcionamiento de estos sistemas evitando incidentes como los nombrados con anterioridad, por lo tanto en el siguiente capitulo se proponen algunas buenas prácticas bajo un estándar especifico.

5.3 PROPONER BUENAS PRÁCTICAS BASADAS EN EL NIST-CSF QUE PERMITIRÁ ASEGURAR LA INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD DE LA INFORMACIÓN EN EL PROCESO DE INTEGRACIÓN DE UN SISTEMA SCADA EN SISTEMAS INTELIGENTES DE TRANSPORTE (ITS) EN COLOMBIA

El 12 de febrero de 2013, en respuesta al aumento de incidentes de ciberseguridad en Estados Unidos, el presidente Barack Obama emitió la Orden Ejecutiva 13636. Esta directiva estableció como política nacional el fortalecimiento de la seguridad y resiliencia de las infraestructuras críticas, al mismo tiempo que se promueve un entorno cibernético que fomente la eficiencia, la innovación y la prosperidad económica, respetando la seguridad, la privacidad y las libertades civiles (NIST, 2018)[21].

El Marco de Ciberseguridad del NIST (NIST CSF) se distingue por su enfoque flexible y no restrictivo. A diferencia de los estándares rígidos, el NIST CSF se originó a partir de una iniciativa para proteger las infraestructuras críticas. Similar a cómo la OTAN ha desarrollado manuales para la protección de infraestructuras críticas con fines de defensa nacional, bajo el título “Manual del Marco de Trabajo de Ciberseguridad Nacional” (OTAN, 2012), el NIST CSF busca proporcionar un marco adaptable para mejorar la ciberseguridad de manera integral.

Las buenas prácticas se entienden como las mejores defensas que debe tener cualquier entidad para prevenir y detectar peligros o adversidades en el uso de sistemas de tecnologías de la Información y la comunicación, estas contribuyen a establecer entornos más seguros que puedan cubrir los pilares de la seguridad informática que son confidencialidad, disponibilidad e integridad.

Partiendo de lo recopilado en los capítulos anteriores, es importante establecer estas prácticas a través de estándares normativos que permitan salvaguardas de manera adecuada la información, en este caso se tomara como referente normativo el marco de ciberseguridad NIS- CSF, el cual fue diseñado para establecer medidas o parámetros unificados en torno a la protección de datos, y se centra en aspectos como controles de acceso, controles de seguridad, copias de seguridad de la información y la evaluación de riesgos permanente, entre otros. Tiene como objetivo principal ayudar a las compañías a comprender, administrar y minimizar los riesgos

[21] AGUIRRE, (2023). Diagnóstico integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, para el Programa Nacional de Inversiones en Salud. Disponible en https://hdl.handle.net/20.500.12893/11406

de brechas en su seguridad informática y establece como base fundamental cinco funciones que actúan como pilares para un programa de ciberseguridad exitoso, los cuales son[22]:

Ilustración 10. Funciones o pilares marco NIST

1. Identificar: implica construir una visión integral de la empresa, abarcando la gestión del riesgo cibernético en sistemas, personas, activos, datos y habilidades. Esta comprensión profunda del entorno empresarial, así como de los recursos que sustentan las funciones críticas, y la evaluación de riesgos asociados con la ciberseguridad, capacita a la organización para dirigir y enfocar sus acciones en línea con su estrategia de gestión de riesgos y los objetivos comerciales establecidos. En esencia, se trata de un enfoque estratégico que permite identificar y priorizar las áreas de mayor riesgo en el ámbito de la ciberseguridad.

2. Proteger: involucra desplegar las medidas necesarias para garantizar la continuidad de los servicios proporcionados por infraestructuras críticas. Esto abarca la capacidad de prevenir o reducir el impacto de posibles amenazas cibernéticas. Engloba acciones como el control de acceso a la red, la codificación de datos sensibles, la aplicación de herramientas de protección de datos, la capacitación del personal y usuarios, entre otras estrategias destinadas a preservar la integridad y disponibilidad de los sistemas. En síntesis, se trata de

[22] OEA, AWS. CIBERSEGURIDAD MARCO NIST, Un abordaje integral de la ciberseguridad. (2019). Disponible en https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

un conjunto de iniciativas destinadas a fortalecer la seguridad y robustez de las infraestructuras frente a riesgos potenciales en el ámbito cibernético.

3. Detectar: Busca establecer las acciones requeridas para reconocer la aparición de eventos relacionados con la ciberseguridad, posibilitando su detección temprana. Este proceso se enfoca en una vigilancia continua para prevenir accesos no autorizados a las redes y sistemas empresariales. Conlleva la realización de auditorías de tecnologías de la información de manera regular y la revisión de registros para investigar cualquier actividad inusual. En resumen, se trata de un conjunto de medidas destinadas a identificar de forma proactiva cualquier indicio de amenaza cibernética y responder a ella oportunamente.

4. Responder: implica llevar a cabo las acciones necesarias en respuesta a un incidente de ciberseguridad identificado, desarrollando la capacidad de mitigar el impacto de dicho incidente. Esta etapa es crucial, ya que implica contar con un plan detallado de las acciones que deben emprenderse en caso de amenazas informáticas, tales como ciberataques, intrusiones, robos de datos, entre otros. Esto incluye notificar a empleados, clientes, usuarios y autoridades pertinentes, así como actualizar las políticas de ciberseguridad y aplicar otras prácticas recomendadas para gestionar o reducir los riesgos de seguridad. En resumen, se trata de un conjunto de medidas destinadas a responder de manera efectiva y organizada ante incidentes de seguridad cibernética para minimizar su impacto y restaurar la normalidad operativa lo antes posible.

5. Recuperar: identifica el desarrollo de acciones destinadas a preservar los planes de resiliencia y a restablecer cualquier capacidad o servicio afectado por un incidente de ciberseguridad. Esta tarea se enfoca en la pronta recuperación de las operaciones habituales para minimizar el impacto de dicho incidente. Se trata de garantizar la pronta restauración de la funcionalidad normal, mitigando los efectos adversos del incidente cibernético. En resumen, consiste en un conjunto de actividades orientadas a la recuperación ágil y efectiva de las operaciones tras un evento de ciberseguridad, asegurando así la continuidad del negocio.

5.3.1 Niveles de implementación del NIST CSF

NIST aclara que los niveles establecidos en su marco no representan de manera exacta los niveles de madurez dentro de una organización y, en realidad, tienden a ser bastante similares. Es crucial que cada organización determine el nivel que desea alcanzar, teniendo en cuenta que no es necesario implementar los controles al nivel más alto disponible. En cambio, es fundamental que el nivel seleccionado

se ajuste a los objetivos específicos de la organización y contribuya a reducir el riesgo de ciberseguridad a un nivel que sea aceptable para ella.

Nivel 1 - Parcial:
En este nivel, la gestión de riesgos de ciberseguridad es reactiva. Las organizaciones únicamente responden a eventos específicos de seguridad o incidentes sin una estrategia sistemática en lugar. Las medidas se toman principalmente como reacción a problemas ya ocurridos, sin un enfoque proactivo o planificado.

Nivel 2 - Riesgo Informado:
Aquí, la organización ha adoptado una gestión de riesgos proactiva. Se identifican, analizan y abordan los riesgos de ciberseguridad de manera sistemática. Aunque el enfoque es más organizado que en el Nivel 1, la gestión de riesgos aún depende en gran medida de la información disponible y las amenazas conocidas, con un énfasis en la prevención y preparación.

Nivel 3 - Repetible:
En el Nivel 3, la gestión de riesgos de ciberseguridad está integrada en las actividades diarias de la organización. Los procesos de evaluación y gestión de riesgos están alineados con los objetivos comerciales y la misión de la empresa, permitiendo una evaluación continua del impacto en los objetivos estratégicos. La organización cuenta con procedimientos establecidos que se repiten y mejoran con el tiempo.

Nivel 4 - Adaptable:
Las organizaciones en el Nivel 4 tienen una cultura sólida de ciberseguridad y una capacidad significativa para adaptarse a cambios y nuevas amenazas en tiempo real. La gestión de riesgos es dinámica y continua, con un enfoque en la adaptación constante a las nuevas amenazas y vulnerabilidades. La organización integra la ciberseguridad en todos los aspectos de sus operaciones y está preparada para ajustar sus estrategias de forma proactiva en respuesta a cambios en el entorno de amenazas.

Ilustración 11.National Institute of Standards and Technology (NIST)

5.3.2 Establecimiento o mejora de un programa de ciberseguridad

Según Almagro et al. (2019)[23], el marco de ciberseguridad del NIST se estructura en siete pasos esenciales, que ayudan a crear o mejorar un programa de ciberseguridad. Estos pasos son:

1. Priorización y Alcance: En esta etapa, se identifican los objetivos empresariales y se establecen prioridades a nivel estratégico. Se define el alcance del programa de ciberseguridad, determinando qué sistemas y activos se incluirán en el proceso, así como los sectores de negocio o procesos que se abordarán.

2. Orientación: Aquí, se identifican los sistemas y activos relevantes dentro del alcance definido, así como los requisitos regulatorios o legales aplicables. También se establece un enfoque general de gestión de riesgos.

3. Crear un Perfil Actual: Se lleva a cabo una evaluación exhaustiva de la situación actual de ciberseguridad, que incluye personas, procesos y tecnología. Esta evaluación permite crear un perfil actual que muestra las categorías y subcategorías del marco NIST que ya están en implementación.

[23] Almagro, L., Urrutia, F., Treppel, A., Contreras, B. (2019). Ciberseguridad, Marco NIST, Un abordaje integral de la Ciberseguridad. https://www.oas.org/es/sms/cicte/docs/OEAAWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

4. Realizar una Evaluación de Riesgos: En esta fase, se identifican los riesgos y vulnerabilidades presentes en los activos y sistemas de información frente a amenazas cibernéticas. El objetivo es comprender el impacto y la probabilidad de estos riesgos.

5. Crear un Perfil Objetivo: Las organizaciones desarrollan un perfil objetivo basado en la evaluación de las categorías y subcategorías del marco NIST, con el fin de definir los resultados de ciberseguridad que desean alcanzar. Este perfil puede ajustarse para abordar riesgos específicos y considerar las influencias de partes interesadas externas, como la industria, clientes y socios comerciales.

6. Determinar, Analizar y Priorizar Brechas: Se compara el perfil actual con el perfil objetivo para identificar brechas. La organización debe evaluar los recursos necesarios, incluyendo financiamiento y personal, para abordar estas brechas.

7. Implementar un Plan de Acción: Finalmente, la organización define un plan para eliminar las deficiencias identificadas. Se monitorean las prácticas actuales de ciberseguridad en comparación con el perfil objetivo, actuando proactivamente en áreas como gestión de personal (contratación, formación, etc.), tecnología (soluciones actuales y emergentes), y procesos (políticas, procedimientos y prácticas).

Ilustración 12.Instituto Nacional de Normas y Tecnología, (2023).

5.3.3 NIST 800-82: Guía de Seguridad para Sistemas de Control Industrial (ICS)

Este documento[24] proporciona directrices sobre cómo asegurar los sistemas de control industrial (ICS), que incluyen sistemas de control de supervisión y adquisición de datos (SCADA), sistemas de control distribuido (DCS), y controladores lógicos programables (PLC), entre otros. La guía ofrece una visión general de los ICS y sus arquitecturas, identifica amenazas y vulnerabilidades en la tecnología operativa (OT), y establece medidas de seguridad para mitigar los riesgos asociados.

Los objetivos de control que aborda el documento incluyen:

- Restringir el Acceso Lógico: Limitar el acceso a la red ICS y controlar la actividad dentro de la misma.
- Controlar el Acceso Físico: Restringir el acceso físico a la red y a los dispositivos ICS.
- Proteger Componentes Individuales: Salvaguardar los componentes específicos de ICS contra la explotación.
- Evitar Modificaciones No Autorizadas: Impedir cambios no autorizados en los datos.
- Detectar Eventos e Incidentes: Identificar y responder a eventos e incidentes de seguridad.
- Mantener la Funcionalidad: Garantizar el funcionamiento continuo en condiciones adversas.
- Restaurar el Sistema: Restaurar el sistema tras un incidente de seguridad.

[24] Stouffer, K., Falco, J., & Scarfone, K. (2011). *Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC)*. National Institute of Standards and Technology.

Estos objetivos ayudan a asegurar que las infraestructuras críticas puedan operar de manera segura y eficiente, protegiéndose contra diversas amenazas y vulnerabilidades.

5.3.4 Integración del Marco NIST en un sistema SCADA

Estas tecnologías de la operación se refieren al uso de hardware y software para monitorear y controlar procesos físicos, químicos, equipos y dispositivos en infraestructuras críticas. Esta tecnología abarca un conjunto de herramientas utilizadas en el sector industrial que permite supervisar, controlar y gestionar datos operativos a través de sistemas de control. Estos sistemas influyen en motores, variadores, sensores y otros mecanismos en entornos como plantas nucleares, plantas de tratamiento de agua, plantas eléctricas, sistemas financieros y militares.

Para proteger estas infraestructuras críticas, es esencial implementar controles de ciberseguridad específicos, como se detalla en el documento **NIST 800-82.**

Integrar un sistema SCADA en sistemas inteligentes de transporte (ITS) presenta desafíos específicos de ciberseguridad debido a la naturaleza crítica y compleja de ambos sistemas. A continuación, se detallan recomendaciones específicas basadas en el marco NIST para garantizar la seguridad de esta integración, enfocándose en los aspectos únicos de los sistemas SCADA:

- Evaluación de riesgos: Realiza una evaluación exhaustiva de los riesgos de seguridad asociados con la integración del sistema SCADA en el sistema de transporte inteligente. Identifica las posibles amenazas y vulnerabilidades específicas para desarrollar estrategias de mitigación, dentro de estos:

    - ✓ Identificación de Activos Críticos: Identificar los componentes del sistema SCADA que son críticos para la operación del ITS, como sensores de tráfico, sistemas de control de semáforos y dispositivos de comunicación.

    - ✓ Análisis de Impacto: Evaluar el impacto potencial de diferentes tipos de ciberataques (por ejemplo, denegación de servicio, manipulación de datos) en la operatividad del ITS y la seguridad pública.

- Segmentación de red avanzada: Implementa una arquitectura de red que segmente claramente el sistema SCADA del resto de la red del sistema de transporte inteligente. Esto ayuda a limitar la propagación de ataques y a proteger los datos críticos.

- ✓ Zonas y Conductos: Implementar una segmentación de la red en zonas y conductos, siguiendo algunos estándares como por ejemplo ISA/IEC 62443, teniendo claro que las zonas son agrupaciones de activos con niveles similares de seguridad, y los conductos son los medios seguros de comunicación entre zonas.

- ✓ Firewall y DMZ: Utilizar firewalls para crear una zona desmilitarizada (DMZ) entre el sistema SCADA y otras partes del ITS, limitando el tráfico directo y permitiendo un control más riguroso de los accesos

- Autenticación y control de acceso: Utiliza métodos robustos de autenticación de usuarios y control de acceso para garantizar que solo personal autorizado pueda acceder al sistema SCADA. Considera la implementación de autenticación multifactor y roles de usuario con privilegios mínimos necesarios.

- Monitorización continúa avanzada: Establece sistemas de monitorización continua para detectar actividades sospechosas o intrusiones en el sistema SCADA. Esto puede incluir la implementación de sistemas de detección de intrusiones y análisis de comportamiento de red.

  - ✓ SCADA IDS/IPS: Implementar sistemas de detección y prevención de intrusiones específicos para SCADA, que están diseñados para entender y analizar el tráfico SCADA en busca de patrones anómalos.

  - ✓ SIEM Integración: Integrar un sistema de gestión de eventos e información de seguridad (SIEM) que puede correlacionar eventos de SCADA con otros datos de seguridad en tiempo real para una respuesta más rápida a incidentes.
- Actualizaciones y parches: Mantener actualizados todos los componentes del sistema SCADA con los últimos parches de seguridad y actualizaciones de software. Establece un proceso para gestionar de manera proactiva las vulnerabilidades conocidas.

  - ✓ Validación de Parches: Antes de aplicar parches, se deben realizar pruebas en un entorno que imite el sistema SCADA en producción para asegurar que no interfieran con las operaciones.

- Gestión de Configuraciones: Mantener una base de datos de configuración de todos los dispositivos SCADA para facilitar la rápida restauración de sistemas tras una actualización o incidente

  - ✓ Respaldo y recuperación de datos: Implementa procedimientos de respaldo regulares y sistemas de recuperación de datos para garantizar la disponibilidad y la integridad de la información crítica en caso de un incidente de ciberseguridad.

  - ✓ Plan de Recuperación ante Desastres: Desarrollar un plan de recuperación ante desastres específico para SCADA que incluya procedimientos para restaurar sistemas críticos en el menor tiempo posible

  - ✓ Pruebas Regulares: Realizar pruebas regulares de los procedimientos de respaldo y recuperación para asegurar su efectividad y actualízalos según sea necesario.

- Formación y concienciación del personal: Proporciona formación regular en ciberseguridad para todo el personal involucrado en el mantenimiento y operación del sistema SCADA. Destaca los riesgos específicos asociados con la integración en sistemas de transporte inteligente y las medidas de seguridad correspondientes.

  - ✓ formación específica en protocolos y tecnologías SCADA, así como en los riesgos asociados.

  - ✓ Simulacros de Ciberseguridad: Realizar simulacros de incidentes de ciberseguridad que involucren el sistema SCADA, para mejorar la preparación y la respuesta del personal.

- Colaboración con la comunidad: Fomenta la colaboración con otras organizaciones, agencias gubernamentales y la comunidad de ciberseguridad para compartir información sobre amenazas y mejores prácticas de seguridad en sistemas SCADA integrados en el transporte inteligente.

  - ✓ Participación en ISACs: Participar en Centros de Intercambio y Análisis de Información (ISAC) específicos de SCADA e ITS para compartir información sobre amenazas y mejores prácticas.

- ✓ Estándares y Regulaciones: Mantener actualizados los estándares y regulaciones específicas para SCADA, como por ejemplo NERC CIP, que se pueden aplicar dependiendo de la jurisdicción.

Al seguir estas buenas prácticas basadas en el marco NIST, se puede fortalecer la seguridad de la integración del sistema SCADA en sistemas inteligentes de transporte (ITS) y mitigar los riesgos asociados con posibles amenazas cibernéticas.

6 CONCLUSIONES

La recopilación de información a través del análisis documental sobre la funcionalidad de los sistemas SCADA en el contexto de los Sistemas Inteligentes de Transporte (ITS) en Colombia permitió destacar la importancia que este sistema tiene para supervisar y controlar eficientemente los procesos de transporte, entendiendo que estos sistemas permiten la recolección, procesamiento y análisis de datos en tiempo real, así como la regulación y control de los componentes del sistema de transporte, mejorando la eficiencia operativa y la seguridad. Sin embargo, como su integridad y seguridad se pueden ver comprometidos por diversos incidentes, como vulnerabilidades de hardware y software, ataques cibernéticos, y accesos no autorizados, es sumamente importante contar con las herramientas y las practicas adecuadas para su adecuado funcionamiento.

La integración de sistemas SCADA en ITS es una tarea compleja que requiere una cuidadosa selección de herramientas y medidas preventivas robustas debido al aumento de las amenazas de ciberseguridad. Es por ello por lo que se destaca el software WinCC OA como una solución versátil y robusta para este propósito, ofreciendo características como orientación a objetos, escalabilidad y compatibilidad con diversos sistemas y dispositivos, así como funciones adicionales como gestión de vídeo y visualización GIS. Aunque es necesario aclarar que a medida que se dan avances se van creando software más desarrollados por lo que siempre se deben estar actualizando los procesos según las necesidades.

En cuanto a la ciberseguridad, la implementación de buenas prácticas basadas en el marco NIST-CSF proporciona un camino sólido para garantizar la integridad, confidencialidad y disponibilidad de la información en los sistemas SCADA dentro de ITS en Colombia. Al seguir las cinco funciones clave del marco (Identificar, Proteger, Detectar, Responder y Recuperar), las organizaciones pueden establecer un programa de ciberseguridad robusto y adaptado a sus necesidades particulares, lo que permite una gestión proactiva de riesgos y una respuesta eficaz ante incidentes de seguridad

7 RECOMENDACIONES

Es importante tener en cuenta que proteger completamente los sistemas ITS bajo herramientas como el sistema SCADA, no es una tarea fácil, ya que siempre se presentarán riesgos, amenazas y llegar a ser atacados en algún momento, por lo tanto, uno de los objetivos principales para mitigar y prevenir vulnerabilidades en los procesos, es estar alerta, en un avance continuo, en actualización permanente, buscando las mejores alternativas de protección, disponiendo de compromiso y tomando contramedidas.

Siempre se debe buscar trabajar con las herramientas que sean versátiles, flexibles y potentes y que mejor se adapten a las necesidades de la entidad u organización según el tipo de actividad.

Las buenas prácticas deben contar con un plan de seguimiento y actualización para trabajar siempre bajo las normativas y estándares vigentes o actualizados para evitar vulnerabilidades.

8 BIBLIOGRAFÍA

Almagro, L., Urrutia, F., Treppel, A., Contreras, B. (2019). Ciberseguridad, Marco NIST, Un abordaje integral de la Ciberseguridad. https://www.oas.org/es/sms/cicte/docs/OEAAWS-Marco-NIST-de-Ciberseguridad- ESP.pdf

AGUIRRE, (2023). Diagnóstico integral de Ciberseguridad, basado en estándares internacionales de seguridad de NIST CSF, para el Programa Nacional de Inversiones en Salud. Disponible en https://hdl.handle.net/20.500.12893/11406

ALCARAZ, Cristina; FERNANDEZ Gerardo; ROMAN Rodrigo; BALASTEGUI, Angel; LOPEZ, Javier. Gestión segura de redes SCADA. Edición 196. (2008) Disponible en https://www.nics.uma.es/biblio/citekey/alcaraz2008a

CASTELLANOS, Michelle. Análisis del estado de la ciberseguridad en los sistemas SCADA en el sector eléctrico colombiano. (2022). [consultado el 11 de marzo de 2023] disponible en https://repository.unad.edu.co/bitstream/handle/10596/48925/mcastellanosf.pdf?sequence=3&isAllowed=y

Centro de Formación Técnica para la Industria. Qué es un sistema SCADA, para que sirve y cómo funciona [consultado el 14 de marzo de 2023, de aula 21] Disponible en https://www.cursosaula21.com/que-es-un-sistema-scada

Centro de Formación Técnica para la Industria. Qué son las redes de comunicación industrial. [consultado el 15 de marzo de 2023, de aula 21] Disponible en https://www.cursosaula21.com/que-son-las-redes-de-comunicacion-industrial/

Consejo Nacional de Política Económica y Social Republica de Colombia. Documento Conpes 3701: lineamientos de política para ciberseguridad y ciberdefensa. (2011). [consultado el 10 de abril de 2023]. Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Consejo Nacional de Política Económica y Social Republica de Colombia. Documento Conpes 3995: Política nacional de confianza y seguridad digital. (2020). [consultado el 10 de abril de 2023]. Disponible en https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Digital Security. Los ciberataques, un riesgo real para sistemas de transporte inteligentes. (2018). [consultado el 15 de marzo de 2023, de aula 21] Disponible en https://www.itdigitalsecurity.es/actualidad/2018/02/los-ciberataques-un-riesgo-real- para-sistemas-de-transporte-inteligentes

DUQUE, Francisco. Sistema de gestión de seguridad de la información basado en la familia de normas ISO/IEC 27000. (2021). Disponible en https:// https://repositorio.unal.edu.co/handle/unal/80158

FAJARDO, Franklin. Implementación de Políticas de Seguridad en los sistemas SCADA. Universidad Piloto de Colombia. [Consultado el 17 de marzo de 2023] Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2983/00001484.p df?sequence=1

Instituto Nacional de Normas y Tecnología, (2023). El marco de ciberseguridad 2.0 del NIST. https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework- 20/ipd

KIO NET WORS. ¿Qué son y para qué sirven los protocolos de comunicación de redes? [Consultado el 12 de marzo de 2023] disponible en https://www.kionetworks.com/blog/data-center/protocolos-de- comunicaci%C3%B3n-de-redes

HUQ, Numan; VOSSELER, Rainer; SWIMMER, Morton (Trend Micro Forward- Looking Threat Research (FTR) Team). Cyberattacks Against Intelligent Transportation System. (2017). Disponible en https://documents.trendmicro.com/assets/white_papers/wp-cyberattacks-against- intelligent-transportation-systems.pdf

LOPEZ, Javier. Los Sistemas Inteligentes de Transportes, la tecnología en el transporte terrestre. (2022). Disponible en https://www.eleconomista.com.mx/opinion/Los-Sistemas-Inteligentes-de- Transportes-la-tecnologia-en-el-transporte-terrestre-20220203-0140.html

MEINSA. WinCC OA, tu solución para la integración de sistemas SCADA.S.F. consultado en https://meinsa.com/2021/05/wincc-oa-integracion-sistemas-scada/

Ministerio de Tecnologías de la Información y las Comunicaciones. Decreto 338 de 2022 "Lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras criticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital". Consultado el [01 de abril de 2023] Disponible en https://www.crossbordertech.com/decreto-338- de-marzo-de-2022-ciberseguridad-en-colombia/#:~:text=El%20Decreto%20338%20de%20marzo,seguridad%20digital%20entre%20otras%20disposiciones.

Ministerio de Transporte. ¿Qué es ITS?. (2018). [Consultado el 14 de marzo de 2023] disponible en https://www.mintransporte.gov.co/publicaciones/5757/que-es- its/
OEA, AWS. CIBERSEGURIDAD MARCO NIST, Un abordaje integral de la ciberseguridad. (2019). Disponible en https://www.oas.org/es/sms/cicte/docs/OEA- AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

QUINTERO, Julian; PRIETO, Lina. Sistemas inteligentes de transporte y nuevas tecnologías en el control y administración del transporte. (2015). Disponible en: https://repository.upb.edu.co/bitstream/handle/20.500.11912/7281/SISTEMAS%20INTELIGENTES%20DE%20TRANSPORTE.pdf?sequence=1&isAllowed=y

REDONDO, Manel; MORENO Romualdo. Diseño e implementación de un sistema SCADA para una planta de producción y envasado de líquidos. (2008). Consultado en https://core.ac.uk/download/pdf/13284214.pdf

RODRIGUEZ, Aquilino. Sistemas SCADA. 3ra edición. Barcelona. (2012) Marcombo. Disponible en https://books.google.es/books?hl=es&lr=&id=cNQfjbBcUq8C&oi=fnd&pg=PA1&dq=integracion+de+protocolos+de+comunicaci%C3%B3n+en+sistemas+scada&ots=

4HRVtEQNZD&sig=PgVqO4Z8ihu4tIJ9oIr5rjPcHXo#v=onepage&q=integracion%20de%20protocolos%20de%20comunicaci%C3%B3n%20e

SUAREZ, Mercedes. Los sistemas inteligentes de transporte ITS. Ciencia e Ingeniería Neogranadina. (2001) Disponible en https://www.redalyc.org/pdf/911/91101006.pdf

Stouffer, K., Falco, J., & Scarfone, K. (2011). Guide to Industrial Control Systems (ICS) Security - Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). National Institute of Standards and Technology.

TORRES, Ricardo; MEDINA, Fabian; MENDOZA, Miguel. Propuesta metodológica para la auditoría de ciberseguridad aplicada a un sistema SCADA. Ingenierías USBMed, vol. 11, No 2, pp. 62–70 (2020). Disponible en http://revistas.usbbog.edu.co/index.php/IngUSBmed/article/view/4307/3735

VALOYES, Amancio. Ciberseguridad en Colombia. (Universidad piloto de Colombia). [consultado el 13 de marzo de 2023] Disponible en http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6370/CIBERSEGURIDAD%20EN%20COLOMBIA.pdf?sequence=1&isAllowed=y

VELAZCO, Sandra; FERRO, Roberto; CUARTAS, Katherin. Sistemas Integrados de Transporte soportados en el internet de las cosas. (2016). Disponible en https://revistas.udistrital.edu.co/index.php/REDES/article/view/11995

AL GHAZO, Alaa; KUMAR, Ratnesh. ANDVI: Automated Network Device and Vulnerability Identification in SCADA/ICS by Passive Monitoring. (2024). Disponible en https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2- s2.0-85182934426&origin=resultslist&sort=plf-f&src=s&sid=ed0d7a8db8a08e4209c5d74141bf583b&sot=b&sdt=cl&cluster=scola ng%2C%22English%22%2Ct%2Bscoexactkeywords%2C%22SCADA+Systems%

BRIONES, Lenin; ORTIZ, Ivan; SINGO, Marlon; ECHEVERRÍA, Aarón.
Implementación de un Modelo de Ciberseguridad de una Arquitectura de Sensores de Monitoreo IoT en la Niebla. (2023). Disponible en https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2-s2.0-85162916626&origin=resultslist&sort=plf-f&src=s&sid=ed0d7a8db8a08e4209c5d74141bf583b&sot=b&sdt=cl&cluster=scola ng%2C%22Spanish%22%2Ct&s=%28TITLE-ABS-KEY%28%22ciberseguridad

DAMING, Ge. Remote Monitoring System of Expressway Mechanical and Electrical Facilities Based on SCADA-HMI. (2022). Disponible en https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2-s2.0-85151554361&origin=resultslist&sort=plf-f&src=s&sid=99ed5429127d17035827ef4e85504f32&sot=b&sdt=b&cluster=scolan g%2C%22English%22%2Ct%2Bscoexactkeywords%2C%22Transportation+

FERNANDEZ, Susel; ITO, Tkayuki. Using SSN ontology for automatic traffic light settings on inteligent transportation systems. (2016).Disponible en https://www- scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?origin=recordpage&eid=2- s2.0-85013674066&noHighlight=false&sort=plf-f&src=s&sid=99ed5429127d17035827ef4e85504f32&sot=b&sdt=b&sl=68&s=TITL E-ABS-KEY%28inteligent+transportation+systems*

INFANTE, Alfonso; INFANTE, Juan; GALLARDO, Julia. Factores claves para concienciar la ciberseguridad en los empleados. (2022). Disponible en https://www- scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2-s2.0-85135410339&origin=resultslist&sort=plf-f&src=s&sid=ed0d7a8db8a08e4209c5d74141bf583b&sot=b&sdt=cl&cluster=scola ng%2C%22Spanish%22%2Ct&s=%28TITLE-ABS-KEY%28%22ciberseguridad

MAYORGA, Tannia, ARMIJOS, Maria; POZO, Diana; PÉREZ, Mario. Seguridad de la información aplicada a un caso de estudio de red SCADA. (2023). Disponible en

https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2- s2.0-85162747610&origin=resultslist&sort=plf-f&src=s&sid=ed0d7a8db8a08e4209c5d74141bf583b&sot=b&sdt=cl&cluster=scolang%2C%22Spanish%22%2Ct&s=%28TITLE-ABS-KEY%28%22ciberseguridad

MUÑOZ, Angelo; GARIBAY, Alexis; WONG, Lenis. Cybersecurity framework for SMEs in Peru based on ISO/IEC 27001 and CSF NIST controls. (2023). Disponible en https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2- s2.0-85169811956&origin=resultslist&sort=plf-f&src=s&sid=99ed5429127d17035827ef4e85504f32&sot=b&sdt=b&s=%28TITLE- ABS-KEY%28marco+de+ciberseguridad*%29+AND+ALL%28NIST*%29%29&sl=9

ORTIZ, Iván; CADENA, César; NEGRETTE, Gustavo; VILLEGAS, William. Marco de Referencia de Gestión de Riesgos de Ciberseguridad de Ecosistemas IoT en Ciudades Inteligentes. (2023). Disponible en https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2-s2.0-85162928734&origin=resultslist&sort=plf-f&src=s&sid=ed0d7a8db8a08e4209c5d74141bf583b&sot=b&sdt=cl&cluster=scolang%2C%22Spanish%22%2Ct&s=%28TITLE-ABS-KEY%28%22ciberseguridad

OSPINA, Alexandra; GARCES, Luis; VALENCIA, Alejandro; BERMEO, Maria; GOMEZ, Ledy; PATIÑO, Juan; GARCIA, Raul. Tendencias investigativas en ciberseguridad del Internet de las Cosas (IoT). (2023). Disponible en RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao: https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2-s2.0-85174747247&origin=resultslist&sort=plf-f&src=s&sid=ed0d7a8db8a08e4209c5d74141bf583b&sot=b&sdt=cl&cluster=scolang%2C%22Spanish%22%2Ct&s=%28TITLE-ABS-KEY%28%22ciberseguridad

SRIVASTAVA, Animesh; SAINI, Parveen; TIWARI, Shweta, SAWAN, Vikash; GARG, Navin. Securing SCADA System from DDoS Attack. (2024). Disponible en 2nd International Conference on Computer, Communication and Control, IC4 2024: https://www-scopus-com.bibliotecavirtual.unad.edu.co/record/display.uri?eid=2- s2.0-85190519682&origin=resultslist&sort=plf-f&src=s&sid=ed0d7a8db8a08e4209c5d74141bf583b&sot=b&sdt=cl&cluster=scolang%2C%22English%22%2Ct%2Bscoexactkeywords%2C%22SCADA+Systems%