Informática Forense, Seguridad y Estándares en Sistemas Industriales e Infraestructuras Críticas

Alumno: Romero, Raúl Oscar

Tutoría Técnica: Kamlofsky, Jorge Alejandro

Profesora de Trabajo Final: Samela, Marcela

Trabajo Final de Carrera presentado para obtener el título de Licenciado en Gestión de Tecnología Informática

Agosto, 2021

Resumen

En la presente investigación se elaboró una metodología de trabajo para disminuir la brecha de seguridad que actualmente existe en los sistemas SCADA. Éstos, permiten controlar de manera remota una instalación recolectando e integrando información desde distintos sensores y autómatas industriales (PLCs o RTUs) por intermedio de diferentes protocolos desde ambos dispositivos. Desde el punto de vista del software se instala y cumple con los requerimientos específicos para ello.

Esta metodología de trabajo se desarrolló ante la falta de aplicación de estándares a redes industriales críticas que puedan establecer seguridad en esta infraestructura.

Se llevó a cabo mediante la realización de la estructura topológica como una solución de laboratorio, simulando un entorno industrial real. Se seleccionó para esta investigación una empresa que produce y comercializa productos plásticos.

El resultado alcanzado y la aplicación de las normativas y estándares o regulaciones actuales aplicadas en países del primer mundo ha sido la adquisición de nuevas tecnologías de hardware y software relevantes para las redes industriales críticas con la finalidad de mermar brechas e incidentes de seguridad en la industria. Demostraron ser efectivas o asertivas a la hora de minimizar la inseguridad en la infraestructura.

Por lo antes mencionado será importante la concientización y capacitación de todos los usuarios interactuantes con los sistemas críticos industriales.

Palabras clave: ciberdefensa, ciberseguridad, estándares, informática forense, redes industriales, seguridad de la información, sistemas SCADA, vulnerabilidad

Abstract

In this research a work methodology was developed to reduce the security gap that currently exists in SCADA systems. These allow remote control of an installation collecting and integrating information from different sensors and industrial automatons (PLCs or RTUs) through different protocols from both devices. From the software point of view, it is installed and meets the specific requirements for this.

The working methodology was developed in the absence of the application of standards to critical industrial networks that can establish security in this infrastructure.

It was carry out by performing the topological structure as a laboratory solution, simulating a real industrial environment. A company that produces and markets plastic products was selected for this research.

The result achieved and the application of current norms and standards or regulations applied in first world countries has been the acquisition of new relevant hardware and software technologies for critical industrial networks to reduce gaps and security incidents in the industry. They proved effective or assertive in minimizing infrastructure. Therefore, the awareness and training of all users interacting with critical industrial systems will be important.

Keywords: cyberdefense, cybersecurity, forensics, industrial network, information security, SCADA systems, standard, vulnerability

Dedicatoria

Este trabajo está dedicado a mis padres (siento la pérdida de mi padre en pleno comienzo de cuarentena por COVID-19), quienes me han brindado una educación y constante apoyo en mis metas profesionales, al resto de mi familia por su apoyo incondicional y amigos por su constante aliento y apoyo en los momentos difíciles.

Agradecimientos o Reconocimientos

Mi especial agradecimiento es para mis padres (siento la pérdida de mi papá en pleno comienzo de cuarentena por COVID-19), quienes me han brindado una educación impecable, logrando ser una persona de bien, de esfuerzo, con objetivos o metas para alcanzarlas.

Al resto de la familia y amigos quienes están presentes y me apoyan en mis metas hasta logarlas.

A mis mentores: docentes y colegas de la Universidad Abierta Interamericana (UAI), a mis docentes y mentores del Consejo de Profesionales de Ciencias Informáticas (CPCI), en mi formación como Perito Informático Forense quienes han participado en mi formación de Investigador y profundización en la utilización de herramientas forenses como aporte para este trabajo final y aspiración para la rama docente.

A mi tutor Jorge Kamlofsky por su tiempo, pasión y dedicación, no solo en la corrección de este trabajo, sino por su trabajo en proyectos previos (es investigador en el CAETI[1]) que permitieron ir dando forma a este trabajo final de carrera.

Mención especial para la empresa Trend Ingeniería, representada por Esteban Carracedo.

A los profesionales externos pertenecientes a la Universidad Fasta, Facultad de Ingeniería el Ejército.

A compañeros de cursada de la carrera con quienes estuvimos hasta último momento en constante apoyo para lograr el gran objetivo del cierre de la carrera.

A todos ellos, y a cada uno de ellos, (no alcanzan los adjetivos calificativos para agradecerles), muchísimas gracias.

[1] CAETI: Centro de Altos Estudios en Tecnología informática. Sitio Web: http://caeti.uai.edu.ar.

Índice General

Índice de Gráficos

Índice de Tablas

Capítulo I - Introducción

"El principal engaño no se dirige solo a los enemigos, sino que empieza por las propias tropas, para hacer que le sigan a uno sin saber adónde van."
(Sun Tzu, *El arte de la guerra*, Siglo V a.c)

1.1. Presentación del problema

Con los avances de la tecnología, el desarrollo de las TICs, de sus siglas en inglés ICTs "Information and Communication Techcnologies", permitió el crecimiento e innovación de la humanidad: su forma de vida y actividades cotidianas. El hombre como miembro de la sociedad tiende a transformarse con el aprovechamiento de la tecnología.

Con el surgimiento de éstas, se entendió su importancia. Gracias a ellas se accede a infinidad de productos y servicios de calidad y de bajo costo. Esta situación fue desencadenante de la Tercera Revolución Industrial mediante la convergencia de las nuevas tecnologías de información y comunicación (TIC).

Según Jorge Kamlofsky, la robustez de los sistemas industriales hizo que se adopten en las infraestructuras críticas que son para la vida contemporánea, por ejemplo, sistemas de distribución de energía, producción y telecomunicaciones. Los sistemas industriales fueron diseñados para controlarlos conectándolos a un computador y redes autómatas industriales a través de una interfaz humana. En la actualidad, éstos ya se pueden comandar desde dispositivos inteligentes e internet, generando cada vez más vulnerabilidades, permitiendo actividades de ciberterrorismo y ciberguerra y además generando incidentes de seguridad a gran escala. (Kamlofsky, 2015, p. 1)

Cabe destacar que los tipos de ataque pueden ser de distintas maneras, a continuación, se detallan algunos ataques importantes:

- Ataques DDoS (Estonia – 2007)
- Virus Stuxnet (Irán – 2010)
- Ciber-ataque Petrolera Aramco (Arabia Saudita – 2012)
- Ciber-espionaje masivo y hacktivismo

Los tipos de ataques antes mencionados quedan en evidencia en la interconexión de redes de los sistemas industriales. (Kamlofsky, 2015, p. 5)

Existen otros tipos de incidentes de seguridad en los sistemas críticos industriales que aún están estudio. Lo cual indica que cuanto menor sea la implementación de la tecnología más exposición ante ataques existe y por consiguiente el riesgo está siempre presente al igual que las pérdidas económicas.

En este trabajo se pretende generar una metodología de trabajo que colabore con la minimización de los riesgos aplicando buenas prácticas de seguridad y análisis forense.

1.2. Hipótesis

Actualmente en los sistemas industriales más conocidos como sistemas SCADA, de sus siglas en inglés “Supervisory Control And Data Acquisition“, o Redes Industriales o Sistemas Críticos, el problema principal se refleja en la seguridad ante las vulnerabilidades existentes que por diversos motivos hacen que sea obsoleta o nula.

La identificación de un problema o incidente que puede generar pérdidas económicas considerables a las empresas se toma como mitigación de estos, basados en la generación de una metodología de trabajo con la implementación de mejores prácticas, desconociéndose la existencia de tal metodología en el país (el problema que se pretende resolver es la existencia de una enorme brecha en la seguridad).

Es importante disminuir las brechas de seguridad en las infraestructuras críticas, no solo a nivel local sino también a nivel país, ya que las consecuencias pueden causar, ante un ciberataque, pérdidas importantes en reputación y en lo económico.

La solución propuesta a dicho problema en el entorno de las redes industriales o sistemas críticos es la creación de una metodología de trabajo aplicando informática forense mediante ingeniería inversa.

El valor teórico de esta investigación es la aplicación de informática forense, la que obtiene resultados generales o particulares según se solicite, pudiendo ser aplicables a otros casos/incidentes o ayudar a explicarlos y/o entenderlos.

La utilidad que se espera de la solución es la mitigación de las brechas o vulnerabilidades utilizando políticas, normas o estándares de seguridad, por medio de la aplicación de la metodología de trabajo antes mencionada, como así también demostrar cuándo dicha solución no es aplicable.

1.3. Objetivo del Trabajo

El objetivo general de la presente investigación es generar una metodología de trabajo para poder demostrar la mitigación de las brechas de seguridad de la información aplicando políticas, normas o estándares de seguridad en las redes industriales críticas.

1.4. Objetivos Particulares

Los objetivos particulares son:

1. Fomentar la metodología de trabajo de mitigación de brechas en seguridad.
2. Mantener y actualizar normas y estándares relacionados con la seguridad de la información y de las redes industriales críticas.
3. Detectar las brechas en seguridad mediante utilización de herramientas, analizarlas y mitigarlas.
4. Generar reportes y monitorear las mitigaciones.
5. Tratar de forma eficiente los incidentes de seguridad.
6. Minimizar los riesgos en seguridad, tanto en los sistemas de información como en las redes industriales críticas.

1.5. Enfoque Metodológico

El enfoque metodológico de este trabajo de investigación es cualitativo. Se orientó hacia el cumplimiento del objetivo principal: generar un plan de trabajo que permita aminorar la brecha de seguridad ante eventuales ciber-ataques, ciberterrorismo, etc., tal cual se describe en el *capítulo 1 punto 1.1 Presentación del Problema*.

El cronograma operativo de las tareas se basó en instancias factibles de ser cumplidas, la misma se puede visualizar en el *capítulo 1 punto 1.7 Cronograma Operativo*.

La forma de realizar las investigaciones consiste en cumplir las siguientes tareas: instalación de software forense, planteo de posibles soluciones al problema, simulación de un escenario industrial real, lo cual se visualiza en el *capítulo 3 Desarrollo Técnico*. Análisis de los datos generados por el ambiente industrial simulado y la validación de los resultados se puede apreciar en el *capítulo 4 Análisis de los resultados*.

La verificación empírica de la hipótesis (ver *punto 1.2 Hipótesis*, de este mismo capítulo) se logró tras el desarrollo, de la metodología de trabajo en los sistemas

operativos (Windows 7 y Windows 10) y de los controles de seguridad, ante las brechas de seguridad detectadas en la comunicación del PLC con el equipo de cómputo, los cuales se pueden apreciar en el *capítulo 4 Análisis de los resultados*.

1.6. Contribuciones Principales

Este trabajo tiene como objetivo promover la aplicación de métodos de trabajo basados en las mejores prácticas, en la concientización de los recursos que operan este tipo de sistemas, mejora en la seguridad para evitar que los sistemas sean vulnerables y/o evitar ataques de hackers.

Además de lograr aportes de conocimiento dentro del proyecto del CAETI denominado "Ciberseguridad en Redes Industriales", también se pretende aportar conocimientos a un incipiente proyecto conjunto entre la UAI, la Universidad Nacional de la Defensa, la Universidad Fasta y la empresa Trend Ingeniería que trata muchos temas desarrollados en este trabajo.

1.7. Cronograma Operativo

Los plazos para la ejecución de la práctica fueron:

	Cronograma Operativo
Armado de la Topología	*Diciembre 2019*
Configuración del Servidor	*Enero 2020*
Instalación Software SCADA	*Febrero 2020*
Puesta en Marcha Topología	*Febrero 2020 – Junio 2020*
Adquisición (obtención y evaluación)	*Julio 2020*
Conclusiones	*Julio 2020*

Tabla 01 - Cronograma Operativo de Tareas

1.8. Recursos Necesarios

	Escenario Servidor
Hardware	*Servidor Físico*
Sistema Operativo	*Microsoft Windows 7 - Starter*
Software Adquisición	*Bento (Live)*

Software SCADA	*Wonderware*
Personal	*Auxiliar de laboratorio y perito informático forense*

Tabla 02 - Recursos necesarios para el escenario práctico.

	Escenario Networking
Router	*TP-Link*
Cableado	*UTP Cat. 5 y 6*

Tabla 03 - Elementos utilizados para comunicación de los equipos

	Escenario Cliente
Hardware	*Equipo Cliente*
Sistema Operativo	*Linux - Mint*
Software de Ataque	*Tsurugui Linux - Acquire*
Personal	*Auxiliar de laboratorio y perito informático forense*

Tabla 04 - Escenario Cliente para búsqueda de vulnerabilidades

	Escenario PLC
Hardware	*PLC DELTA – DVP 12SE*
Software PLC	*ISPSoft*
Software de Conexión	*Wonderware - SMC*
Software de Simulación	*Wonderware - InTouch*
Personal	*Auxiliar de laboratorio y perito informático forense*

Tabla 05 - Escenario SCADA

1.9. Estructura General del Trabajo

La estructura general de este trabajo está compuesta por: seis capítulos, en cada uno de ellos se desarrollan los conceptos principales del trabajo, la elaboración del informe final, líneas futuras de investigación y, por último, los acrónimos y las referencias.

En esta sección de este trabajo, nos vamos a tomar unos pocos minutos para describir el contenido de los siguientes capítulos:

- Capítulo I – Introducción
- Capítulo II – Marco Teórico
- Capítulo III – Limitaciones del uso de la Forensia en los Sistemas SCADA

- Capítulo IV – Desarrollo Técnico
- Capítulo V – Análisis de los Resultados
- Capítulo VI – Conclusiones y Sugerencias
- Elaboración del Informe Final
- Líneas Futuras de Investigación
- Acrónimos
- Referencias

Capítulo II

En el Capítulo II se describe el marco teórico. En el mismo se detallan los conceptos de SCADA, redes industriales, seguridad de la información, seguridad informática, vulnerabilidades, informática forense y ciberseguridad.

Capítulo III

En el Capítulo III se realiza el desarrollo técnico que comprende el armado del tablero del PLC, instalación de los softwares (sistema operativo, aplicaciones que comunican el PLC con el computador, etc.).

Análisis de información de software, tráfico de red y actividades del PLC y los resultados de estos.

Capítulo IV

En el Capítulo IV se detalla el análisis de resultados de la información obtenida en el Capítulo III.

Capítulo V

En el Capítulo V se detallan las conclusiones y sugerencias, basados en el análisis de resultados de la información del Capítulo IV.

Elaboración del Informe Final

Líneas Futuras de Investigación

Acrónimos

Referencias

Capítulo II - Marco Teórico

"Nunca subestimes a tus enemigos"
(Sun Tzu, *El arte de la guerra*, Siglo V a.c)

2.1. Trabajos Relacionados

2.1.1. Disparadores de la Investigación

Un sistema SCADA, es un sistema que permite supervisar y controlar de forma remota una instalación, recolectando datos e integrando dichos datos, desde distintos sensores, autómatas PLCs mediante diferentes protocolos de comunicación desde un solo lugar. Es una aplicación de escritorio instalable que cumple con requerimientos específicos para cumplir su función incluyendo la parte correspondiente al hardware. Aquí se realizó una investigación que permitió obtener una metodología basada en la aplicación de normas y estándares de seguridad. (Alcaraz, 2008, p. 1), (Chandia, 2007, p. 2), (Kalapatapu, SCADA PROTOCOLS AND COMMUNICATIONS TRENDS, 2004, p. 1)

El disparador de esta investigación surge de los ciberataques que ocurren en la actualidad en las infraestructuras críticas.

2.1.2. Aportes a la Comunidad

Se pone énfasis en la metodología de trabajo para achicar la brecha de seguridad en las redes industriales críticas. De esta manera, la aplicación de la metodología de trabajo antes mencionada nos permitirá sustentar la efectividad de éste.

2.2. Bases Teóricas

2.2.1. Sistemas SCADA

Introducción a Sistemas SCADA

Un sistema SCADA (de sus siglas en inglés "Supervisory Control And Data Acquisition"), es un software cuya finalidad es controlar y supervisar redes industriales, mediante comandos a distancia.

Rao Kalapatapu afirma que los sistemas actuales de control de supervisión y adquisición de datos (SCADA) están compuestos de equipos hosts SCADA, equipos

remotos utilizados como unidades terminales (RTU) y otros equipos encargados de monitorear y controlar tales equipos y sistemas de proceso desde distintas ubicaciones e intercambian datos de distintas cantidades de sistemas de control distribuidos a lo largo de las redes.

Los sistemas SCADA operan intercambiando de datos en tiempo real desde los distintos equipos, tales como sucede con otros sistemas de control como los sistemas DCS (sistema de control distribuido) y PI (información de la plataforma).

Un equipo de terminal remota (RTU) está compuesto por procesador central, módulos de E/S (entrada/salida) y equipos de comunicación para conectarse a otros equipos. Los equipos de terminales remota (RTU) son similares a los controladores lógicos programables (PLC). Los controladores lógicos programables (PLC) se usan en un área local, como el piso de la fábrica, y generalmente se conectan entre sí mediante una red de área local (LAN); donde los equipos de terminales remotas (RTU) se utilizan en locaciones remotas y están conectadas por una red de área amplia (WAN); sin embargo, ambos tienen CPU, unidades de E/S (entrada/salida) y puertos de comunicación.

Por lo tanto, la mayor parte de la discusión en este documento también se aplica a los sistemas PLC Estas RTU a su vez están conectadas a los servidores y estaciones de trabajo del sistema de control SCADA, así como a otras redes de área local y remota a través de líneas telefónicas, cables, líneas arrendadas, radios, fibra óptica y/o una combinación de estos según la disponibilidad en cada uno de estos sitios. (Kalapatapu, SCADA PROTOCOLS AND COMMUNICATION TRENDS, 2004, p. 1)

Los softwares más utilizados para este tipo de sistemas son:

- Simatic PC S7, de Siemens. (Siemens, 2021).
- Wonderware, de AVEA. (AVEVA, 2021).
- Monitor Pro, de Schneider Electric. (Electric, 2021).
- SYSMAC SCS, de Omron. (OMRON, 2020).

Arquitectura SCADA

Un sistema SCADA, es un sistema típico para controlar las infraestructuras de servicios públicos como energía, gas, petróleo o agua generalmente consta de un centro de control y numerosos sitios de campo. Los sitios se distribuyen en un área geográfica amplia y están conectados al centro de control mediante diferentes medios de comunicación, como satélites, redes de área amplia (WAN) y redes de radio, microondas o celulares. Los sitios de campo están equipados con dispositivos tales como

controladores lógicos programables (PLC) o equipos terminales remotos (RTU) que controlan las máquinas en el sitio y envían periódicamente información sobre el estado del equipo de campo al centro de control.

El centro de control es el centro del sistema SCADA. Sus componentes principales incluyen una interfaz hombre-máquina (HMI), el sistema de gestión de base de datos (historiador) y el servidor o unidad de terminal maestra (MTU). El equipo terminal remoto (MTU) inicia toda la comunicación con los sitios de campo y recibe los datos enviados desde los dispositivos de campo. Si es necesario, procesa previamente los datos y los envía al historiador para su archivo. La interfaz hombre-maquina (HMI) presenta información al operador humano. (Ahmed, 2012, pp. 44 - 45)

En la ilustración 1 se visualiza un SCADA típico. (Ahmed, 2012, p. 45)

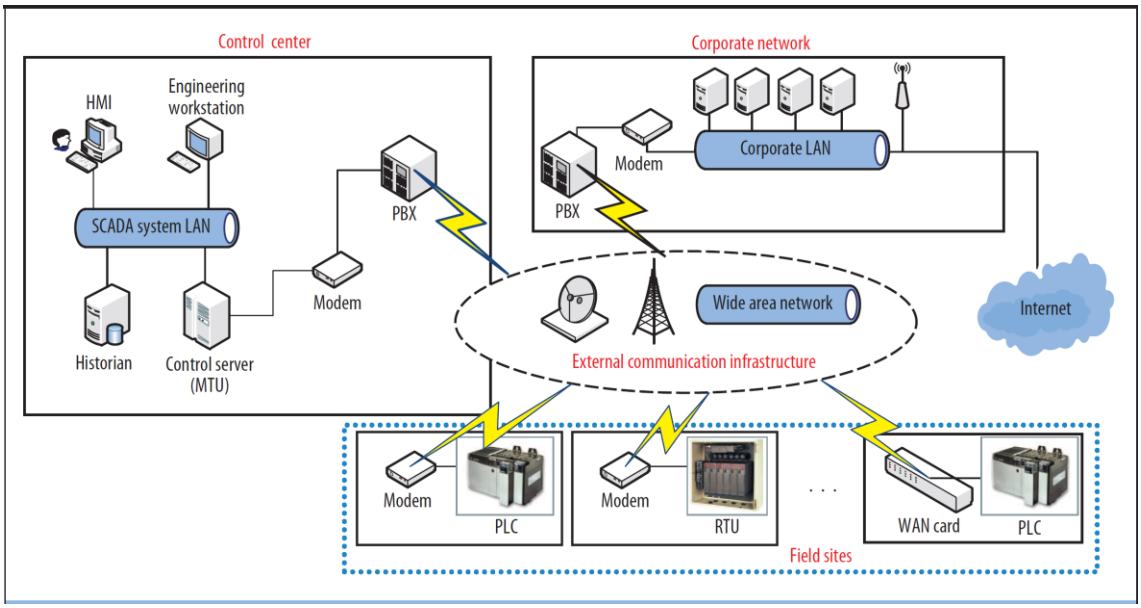


Ilustración 1 – Vista lógica simplificada de arquitectura de control de supervisión y adquisición de datos (SCADA)

Protocolos de Comunicación en Sistemas SCADA

Rao Kalapatapu afirma que los equipos utilizados como unidades de terminales remotas (RTU) están preprogramadas para una comunicarse mediante protocolos de red, entre la estación central SCADA y otros sistemas. Estos sistemas están diseñados para entregar informes sobre el estado de todos los equipos de E/S.

Los protocolos son similares a los idiomas, que permiten que las unidades RTU/SCADA se comuniquen entre sí. Todas las arquitecturas de red se basan en el estándar del modelo ISO (Organización Internacional de Estándares), llamada modelo OSI (Interconexión de sistemas abiertos), el cual cuenta de siete capas, como se detalla a continuación:

- Capa 7 - Aplicación
- Capa 6 - Presentación
- Capa 5 - Sesión
- Capa 4 - Transporte
- Capa 3 - Red
- Capa 2 - Enlace de datos
- Capa 1 - Física

El objetivo del modelo OSI es permita que cualquier sistema o red se conecte e intercambie señales, paquetes de mensajes y direcciones. El modelo permite que las comunicaciones se vuelvan independientes del sistema ideado y protejan al usuario de la necesidad de comprender la complejidad de la red.

En general, las cuatro capas inferiores cubren el cableado físico, la red y los protocolos de comunicación de las redes de área local (LAN) y amplia (WAN), como Ethernet y Frame Relay. TCP/IP (protocolo de control de transporte / protocolos de Internet) es un estándar abierto similar utilizado por todos.

Las capas de Presentación y Sesión se ocupan de establecer la sesión y luego finalizar la sesión entre los dos hosts. No todas las redes usan estas capas.

La Capa de Aplicación (Capa 7) y superior es donde un protocolo típico de PLC/RTU (como Modbus) proporcionará los datos en un equipo local/servidor SCADA típica en un formato de usuario desde las RTU y los sistemas de PLC locales. (Kalapatapu, SCADA PROTOCOLS AND COMMUNICATIONS TRENDS, 2004, pp. 1 - 2)

En la ilustración 2 se visualiza un sistema SCADA en capas. (Ahmed, 2012, p. 46)

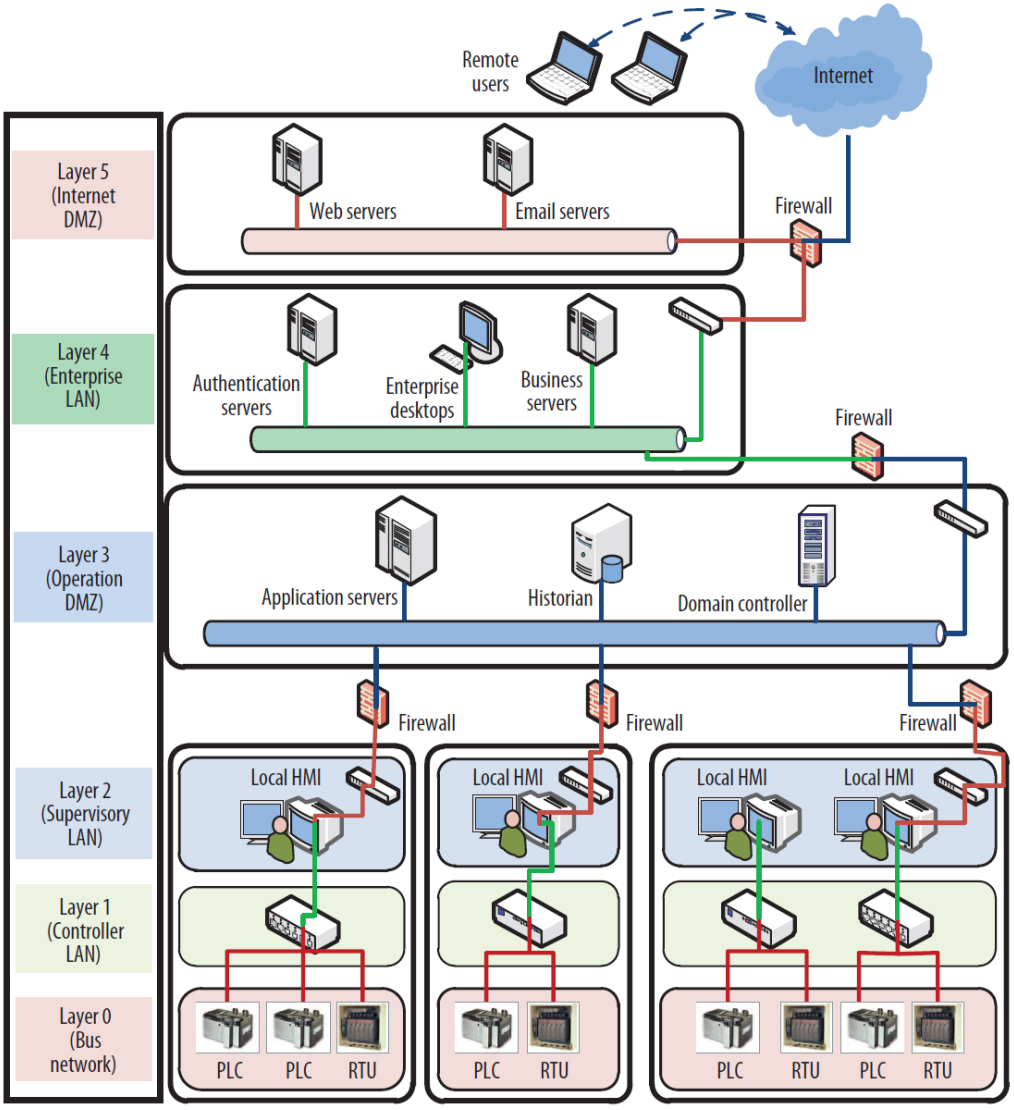


Ilustración 2 - Capas del Sistema SCADA, contiene componentes que controlan procesos industriales subyacentes.

2.2.2. Seguridad de la Información

¿Qué es la Información?

La norma ISO/IEC 27000:2018, establece que la información es un activo fundamental para una organización y que debe protegerse apropiadamente. La información se puede almacenar de muchas formas, incluyendo:

- forma digital (archivos almacenados en medios electrónicos u ópticos),
- forma material (por ejemplo, en papel),
- forma confidencial (información no revelada a los empleados.)

La información puede ser transmitida por distintos medios, tales como: mensajería, comunicación electrónica o verbal. Cualquiera sea el tipo de información, o el medio por el cual se transmita, siempre necesita la protección apropiada.

En las organizaciones, la información depende de la tecnología de la información y las comunicaciones. Esta tecnología es un elemento primordial en la organización y colabora en la creación, procesamiento, almacenamiento, transmisión, protección y destrucción de la información. (27000:2018(E), Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018, p. 12)

Seguridad de la Información

La norma ISO/IEC 27000:2018, establece que la seguridad de la información está representada por la triada CID (CIA de sus siglas en inglés Confidentiality, Integrity and Availability), que garantiza la confidencialidad, disponibilidad e integridad de la información. La seguridad de la información implica la aplicación y gestión de controles apropiados que implica la consideración de una amplia gama de amenazas, con el objetivo de asegurar el éxito y sostener la continuidad del negocio y minimizar las consecuencias de los incidentes de seguridad de la información.

La implementación de la seguridad de la información se realiza con un conjunto de controles aplicables, que se gestionan de un SGSI a través del proceso de gestión de riesgos elegido, que incluye procedimientos, políticas, procesos, estructuras organizativas, hardware y software para la protección de los activos de información identificados. Estos controles deben especificarse, implementarse, monitorearse, revisarse y mejorarse cuando sea necesario, para garantizar que se cumplan los objetivos comerciales y de seguridad de la información específicos de la organización. Se espera que los controles de seguridad de la información relevantes se integren perfectamente con los procesos comerciales de una organización. (27000:2018(E), Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018, pp. 12, 13)

La seguridad de la información se describe como la disciplina que se encarga de la implementación técnica de la protección de la información, de proporcionar la evaluación de riesgos y amenazas, trazar el plan de acción y adecuación para minimizar los riesgos, aplicando las normativas necesarias o con la implementación de las buenas prácticas con el fin de garantizar la confidencialidad, integridad y disponibilidad del manejo de la información de activos de la organización. Seguridad Informática es quien da el soporte o apoyo para obtener los objetivos propuestos por Seguridad de la Información.

2.2.3. Seguridad Informática

Concepto de Seguridad Informática

La norma NIST SP800-128, establece que la seguridad de la información es la protección de la información y los sistemas contra el acceso, uso, divulgación, interrupción no autorizados, modificación o destrucción para proporcionar confidencialidad, integridad y disponibilidad. A los fines de esta publicación, "Seguridad" se usa como sinónimo de "seguridad de la información", y "sistema" se usa como sinónimo de "sistema de información".

La seguridad de tecnologías de la información o seguridad informática es el campo de la informática que debe garantizar el correcto uso de los recursos del sistema de información (material informático o programas) de una organización.

Estas prácticas consisten, en lo general en la restricción del acceso al sistema o parte del sistema y son diversas. El acceso solo es permitido a ciertas personas que se encuentren acreditadas, así como su modificación dentro de los límites de su autorización aplicando táctica y operatividad de la seguridad. (NIST SP 800-128, 2011, pp. 5, 6)

2.2.4. Informática forense

¿Qué es el análisis forense?

Es una ciencia moderna que se aplica a los activos y/o sistemas de información. Permite la reconstrucción de sucesos ocurridos en un sistema en un incidente de seguridad. Este análisis puede determinar quien, desde donde, como, cuando y que acciones ha llevado a cabo un intruso en los sistemas o activos afectados por un incidente de seguridad.

Existen 3 (tres) tipos de análisis forense:

1. ***Análisis Forense de Sistemas***: en este tipo de análisis se tratan los incidentes de seguridad acaecidos en servidores y estaciones de trabajo con los distintos sistemas operativos (Mac OS, Sistemas Operativos Microsoft en todas sus versiones), Sistemas Unix y Sistemas GNU.
2. ***Análisis Forense de Redes***: en este tipo de análisis se engloban las diferentes redes (cableadas, Wireless, bluetooth, etc.)
3. ***Análisis Forense de Sistema embebidos***: en este tipo de análisis se analizan incidentes acaecidos en móviles, PDA, etc. Un sistema embebido es muy similar a un ordenador personal por semejanza en su arquitectura.

Incidente de Seguridad

Un incidente de seguridad se refiere a cualquier acción fuera de la ley o no autorizada: ataques de denegación de servicio, chantaje, posesión de pornografía infantil, envío de correos electrónicos ofensivos, filtraciones de información confidencial dentro de la organización, el cual está involucrado algún sistema telemático o activo de una organización.

La norma ISO/IEC 27035:2011, establece que un incidente de seguridad es indicado por un único o una serie de eventos indeseados o inesperados, que tienen una probabilidad significativa de amenazar la seguridad de la información y comprometer a las operaciones de negocio. (ISO/IEC 27035:2011, 2011)

Los incidentes de seguridad afectaran a cualquiera de los aspectos de la Seguridad de la Información, entre ellos tenemos a la triada de la Seguridad de la Información:

1. ***Disponibilidad***: Interrupción de un servicio o información, que deja de ser accesible a los usuarios autorizados.
2. ***Integridad***: Modificación de información por parte de un usuario no autorizado.
3. ***Confidencialidad***: Acceso a un servicio o información por parte de un usuario no autorizado a ello.
4. ***Autenticidad***: Engaño en la autenticidad de una información, por no ser autentico su contenido o por no provenir de la entidad esperada.
    1. *Categoría 1*: algo que se sabe - Un dato especial, puede tratarse de algo de su persona o bien de un simple o compleja contraseña.

       En la ilustración 3 se visualiza una consola de comandos de Ubuntu. (LINUXCONFIG.ORG, 2020).

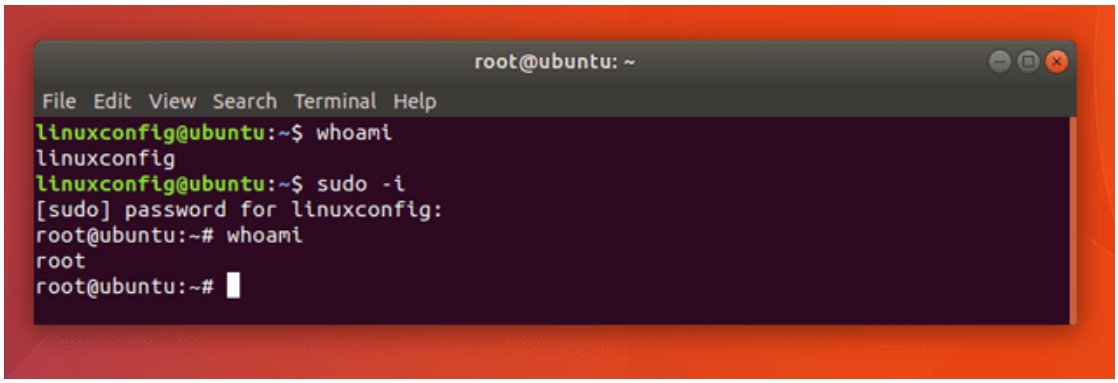


Ilustración 3 – Consola de comandos de Ubuntu

    2. *Categoría 2*: algo que el usuario lleva consigo - Puede ser un documento de identidad, una tarjeta o cualquier otro elemento que uno lleve consigo.

3. *Categoría 3*: propiedad física o acto involuntario - Los datos biométricos (como ser la pupila, voces y huellas dactilares) son ejemplos de propiedades físicas de un individuo_y las firmas son comportamientos involuntarios porque las personas no tienen la intención de realizar cada trazo, sino que los realiza en conjunto.

Ante la presencia de incidentes de seguridad, para hacerles frente de manera rápida y eficiente, hay que contar con el apoyo o colaboración del CSIRT (Computer Security Incident Response).

En nuestro país contamos con el MINSEG-CSIRT (CSIRT gubernamental argentino) (Presidencia de la Nación, 2020), un CSIRT es una organización que tiene por responsabilidad: recibir, revisar y responder a informes y actividad sobre incidentes de seguridad. Este tipo de organizaciones, prestan servicios delimitados en un área, ellas pueden ser empresas, organismos de gobierno o entidades educativas. También pueden delimitarse en una región especifica como ser un país, provincia o estado o bien prestar un servicio a un cliente particular.

Cabe destacar que cada país tiene su propio CERT (Presidencia de la Nacion, 2020).

Informática Forense

Rodney McKemmish define informática forense como una técnica que utiliza un método para capturar, procesar e investigar información procedente de sistemas informáticos para que pueda ser utilizado en los tribunales. (McKemmish, 1999, p. 1)

En lo que respecta al FBI (Federal Bureau of Investigation) (Standardization I. - I., n.d.), dicho organismo define a la informática forense como la ciencia de adquirir, preservar, obtener y presentar datos que han sido procesados de manera electrónica y almacenados en medios informáticos. Se puede apreciar que ambas definiciones coinciden en algunos conceptos y que pueden complementarse. Uno de los objetivos principales del análisis forense es obtener evidencias que permitan llegar a conclusiones sin dar lugar a la duda.

Para finalizar, podemos decir que, la informática forense es la aplicación de técnicas científicas y analíticas especializadas en infraestructura tecnológica que permiten la identificación, preservación, análisis y presentación de datos que sean válidos dentro de procesos preventivos, legales o particulares.

Aplicación de informática forense en SCADA

La informática forense se puede aplicar en entes particulares, empresas de distinta índole, sector público, sector privado, etc.

También se puede aplicar en modo preventivo en carácter proactivo a fin de evitar futuras vulnerabilidades.

Un sistema de red forense captura y almacena el tráfico de red durante las operaciones de la empresa, y proporciona funcionalidad de análisis y consulta de datos para apoyar investigaciones posteriores al incidente, incluida la reconstrucción del incidente.

Sin embargo, un sistema de red forense SCADA también puede mejorar las operaciones industriales y ayudar a monitorear el comportamiento del proceso y verificar las tendencias con el propósito de optimizar el rendimiento de la planta.

El análisis forense en redes de tecnología de la información (TI) a gran envergadura es muy complejo y costoso. Además, el tráfico SCADA es rutinario y predecible, a diferencia de tráfico en redes de TI, que transportan tráfico generado por el usuario con complejos patrones de comunicación Uniformidad de tráfico y bajos volúmenes de tráfico en SCADA. Las redes permiten registrar datos relevantes de procesos/controles asociados con cada mensaje o paquete de información y posteriormente analizar los datos en investigaciones forenses y evaluaciones de rendimiento de la planta y hacer uso de regularidad del tráfico en las redes SCADA para minimizar el volumen de datos recopilados para análisis forenses y respuesta a incidentes. (Chandia, 2007, pp. 125 - 126)

En la ilustración 4 se visualiza una red SCADA con capacidad forense. (Chandia, 2007, p. 126)

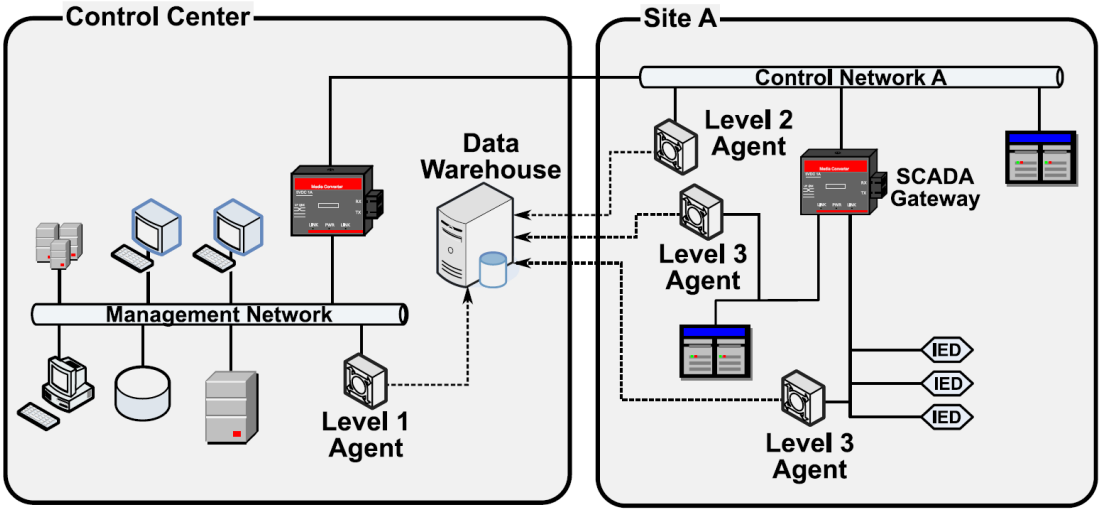


Ilustración 4 – Red SCADA con capacidad Forense

2.2.5. Vulnerabilidades

Definición de Vulnerabilidad

Según TUV NORTH GROUP, la debilidad en una función del sistema, procedimiento, control interno, desarrollo de software o implementación que podría ser explotada o activada por una fuente de amenaza, diseñada intencionalmente en componentes de la computadora (o equipo informático) o insertada accidentalmente en un software en cualquier momento durante su ciclo de vida. (GmbH, p. 3)

Clasificación de Vulnerabilidades

Las vulnerabilidades se clasifican en Muy Alto, Alto, Medio, Bajo e Información. Lo antes mencionado es una clasificación estándar que depende de cada organización y se toma en base a las buenas prácticas que depende de cada herramienta.

Las vulnerabilidades también se pueden clasificar de acuerdo al tipo de riesgo y al impacto que genera el mismo a la organización.

Mitigación de las Vulnerabilidades

La mitigación de las vulnerabilidades requiere de un plan de acción para la remediación de las vulnerabilidades detectadas. El plan de remediación debe ser aprobado por el responsable del área involucrada para luego ejecutarse en los tiempos estipulados.

2.2.6. Estándares de Seguridad, SCADA

Definición de Estándar

Según la Organización Internacional de Normalización (de sus siglas en inglés ISO - International Organization for Standardization) establece la definición de un estándar como una fórmula que describe como es la mejor forma de hacer algo. Esto puede referirse a la manufactura de un producto, administración de un proceso, entrega de un servicio o suministro de materiales. Los estándares cubren un gran abanico de actividades.

Los estándares son conocimientos extraídos de personas que tienen experiencia en el tema y conocen las necesidades de la organización a la que representan. Estas personas incluyen fabricantes, vendedores, compradores, clientes, asociaciones comerciales, usuarios o reguladores. (Standardization I. -I., n.d.)

Los estándares son conocimiento. Son herramientas poderosas que pueden ayudar y aumentar la productividad e impulsar la innovación. Pueden hacer que las organizaciones sean más exitosas y hacer que la vida de las personas sea más fácil, segura y saludable.

Estándares de Seguridad de la Información

Los sistemas información cuentan con varias normas que las regula, ellas son:

- Estándar NIST SP 800-128
- ISO 27000:2018
- ISO 27001:2013

Estándar NIST SP800-128

Según NIST (National Institute of Standard and Technology) 800-128 establece que un sistema está compuesto por componentes que se interconectan para satisfacer en necesidades comerciales y de seguridad de la información. Los componentes del sistema están conectados en red, configurados y administrados, es por ello por lo que, es fundamental para brindar seguridad de la información apropiada y soporte al proceso de gestión de riesgos de una organización o empresa.

Los sistemas cambian de estado constantemente esperando respuesta a nuevos, mejorados, corregidos o capacidades actualizadas de hardware y software, parches para corregir fallas de software y otros errores existentes, nuevas amenazas de seguridad, cambios en las funciones comerciales, etc.

Implementar los cambios en el sistema representa ajustes en la configuración del sistema y para evitar dichos ajustes afectan negativamente a la seguridad del sistema o la organización de la operación del sistema, es necesario un proceso que integre la seguridad de la información, para una gestión de configuración bien definida. (NIST SP 800-128, 2011)

ISO 27000:2018

Según la Organización Internacional de Normalización (de sus siglas en inglés ISO - International Organization for Standardization), las normas internacionales para sistemas de gestión proporcionan un modelo de configuración y operación de un sistema de gestión. ISO / IEC JTC 1 / SC 27 está compuesto por expertos dedicado al desarrollo de normas internacionales de sistemas de gestión para la seguridad de la información,

también conocida como normas del Sistema de Gestión de Seguridad de la Información (SGSI).

Mediante el uso de la familia de estándares ISMS, las organizaciones pueden desarrollar e implementar un marco para administrar la seguridad de sus activos de información, incluida la información financiera, la propiedad intelectual y los detalles de los empleados, o la información que les confían los clientes o terceros. Las mismas se pueden utilizar para la preparación para una evaluación por fuera de un SGSI que se aplique a la protección de la información. (Standardization I. -I., 2018)

ISO 27001:2013

El estándar ISO / IEC 27001 proporciona requisitos normativos para el desarrollo y operación de un SGSI, incluido un conjunto de controles para el control y mitigación de los riesgos vinculados con los activos de información que la organización pretende proteger al utilizar su SGSI. Las organizaciones que utilicen un SGSI pueden tener su acuerdo certificado y auditado.

Su alcance detalla los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar los sistemas de gestión de seguridad de la información (SGSI) en el contexto de los riesgos generales de negocio de la organización. Especifica los requisitos para la implementación de controles de seguridad de la información personalizados para las necesidades de organizaciones individuales o partes de éstos. Este documento puede ser utilizado por todas las organizaciones, independientemente de su tipo, tamaño y naturaleza. (Standardization I. -I., 2013)

Estándar de Sistemas SCADA

Los sistemas SCADA cuentan con varias normas que las regula, ellas son: (API 1164, 2009, p. 120)

- Informes Técnicos ISA-SP99
- Perfil de protección del sistema NIST
- Estándar de seguridad API-1164
- Documentos AGA-12
- Guía de implementación de firewall NISCC
- Documento NIST SP 800-82
- ISA / IEC 62443

Informes Técnicos ISA-SP99

El comité ISA-SP99 propone un enfoque, cuya finalidad es mejorar los componentes de seguridad (la confidencialidad, integridad y disponibilidad) o sistemas de control, para implementar sistemas de control seguros. Hasta la fecha, el comité ha emitido dos Informes técnicos relacionados con la seguridad del sistema de control.

- ***ISA-TR99.00.01-2004 – Security Technologies of Manufacturing and Control Systems***: hace foco en tecnologías de seguridad para sistemas de fabricación y control. Proporciona una encuesta profunda de tecnologías de seguridad electrónica, complementada con guías de uso y evaluaciones de seguridad. El objetivo principal del informe es proporcionar pautas de implementación de seguridad efectivas para los sistemas de control. (Evans, 2005, p. 6)
- ***ISA-TR99.00.02-2004 – Integrating Electronic Security into the Manufacturing and Control System Environment***: hace foco en la integración de componentes de seguridad en entornos de sistemas de fabricación y control. (Evans, 2005, p. 6)

Los informes técnicos de ISA TR99 incorporan una gran cantidad de información de otra seguridad estándares y publicaciones también agrega información específica a los sistemas de control. Los mismos son útiles para identificar los problemas a considerar las opciones de seguridad. No son estándares con requisitos bien definidos que pueden ser probados, certificados o incluidos en las propuestas. (Evans, 2005, pp. 6 - 7)

Perfil de protección del sistema NIST SP

En octubre de 2004, NIST (National Institute of Standard and Technology) lanzó un perfil de protección del sistema (de sus siglas en inglés SPP – Service Protection Profile) para sistemas de control industrial, que proporciona orientación para desarrollar declaraciones formales de requisitos funcionales y de garantía de seguridad para sistemas industriales. El documento NIST adopta perfiles de protección definidos por los Criterios comunes.

El núcleo SPP especifica los requisitos funcionales (control de inicio de sesión, control de acceso basado en roles, autenticación de datos, etc.) y los requisitos de garantía (gestión de configuración, entrega y operación, evaluación de vulnerabilidad, mantenimiento de garantía, etc.). El NIST SPP también proporciona pautas para

desarrollar perfiles de protección enfocados para diversas clases de sistemas de control industrial. (Ron Melton, 2004)

Estándar de seguridad API-1164

Este estándar proporciona pautas, listas de verificación del operador (lista completa de medidas para evaluar el estado de seguridad de los sistemas SCADA) y una plantilla de plan de seguridad para la integridad y seguridad del sistema y se puede usar con modificaciones mínimas, también brinda una descripción de las prácticas de la industria en seguridad SCADA junto con un marco para desarrollar e implementar prácticas de seguridad sólidas.

Las pautas API-1164 también abordan el control de acceso, la comunicación, la distribución y clasificación de la información, la seguridad física, el flujo de datos, el diseño de la red y un sistema de gestión para el personal. (API 1164, 2009)

Documentos AGA-12

Tres semanas después del atentado del 11 de septiembre de 2001, la Asociación Americana de Gas (de sus siglas en inglés AGA - American Gas Association) formó un grupo de trabajo con el fin de recomendar protocolos y mecanismos de protección para los sistemas de control industrial de los ataques cibernéticos.

El documento describe un protocolo basado en sesión con servicios de autenticación que utilizan claves simétricas (AES y SHA1). Presenta un diseño simple que tiene un impacto mínimo en la latencia y fluctúa y usa números de secuencia para proteger contra ataques de repetición. Puede encapsular y transportar otros protocolos, tales como, Modbus y DNP3.

Los documentos AGA, están separados en dos partes:

AGA-12 Parte 1, aborda políticas, evaluaciones y auditorías, describe los requisitos del sistema criptográfico y la planificación de pruebas para dispositivos de seguridad. Requiere cumplir con la norma NIST FIPS 140-2 (Requisitos de seguridad para módulos criptográficos).

AGA-12 Parte 2, aborda la actualización de las comunicaciones en serie y la encapsulación / encriptación de los canales de comunicación en serie.

Hoy en día, AGA se encuentra desarrollando actualmente las Partes 3 y 4, y abordarán la protección de los sistemas en red y la integración de la seguridad en los componentes SCADA. (AGA-12, 2015)

Guía de implementación de firewall NISCC

La Guía de Buenas Prácticas de NISCC sobre Implementación de Firewall para SCADA y Redes de Control de Procesos fue desarrollada por el Instituto de Tecnología de Columbia Británica para el Centro Nacional de Coordinación de Seguridad de Infraestructura (NISCC) del Reino Unido en febrero de 2005. Proporciona configuración, administración y despliegue de un firewall en entornos industriales. Describe y evalúa arquitecturas de segregación desde computadoras de doble alojamiento hasta separación de red basada en VLAN. Cada arquitectura se evalúa en función de la capacidad de administración, la escalabilidad y la seguridad.

También trata sobre las tecnologías futuras que se utilizarán en las redes industriales destaca la importancia de la calidad del servicio y la necesidad de que los dispositivos conozcan los protocolos industriales. (NISCC, 2005)

La ilustración 5 muestra una arquitectura de red SCADA propuesta por NISCC. (Alcaraz, 2008, p. 6)

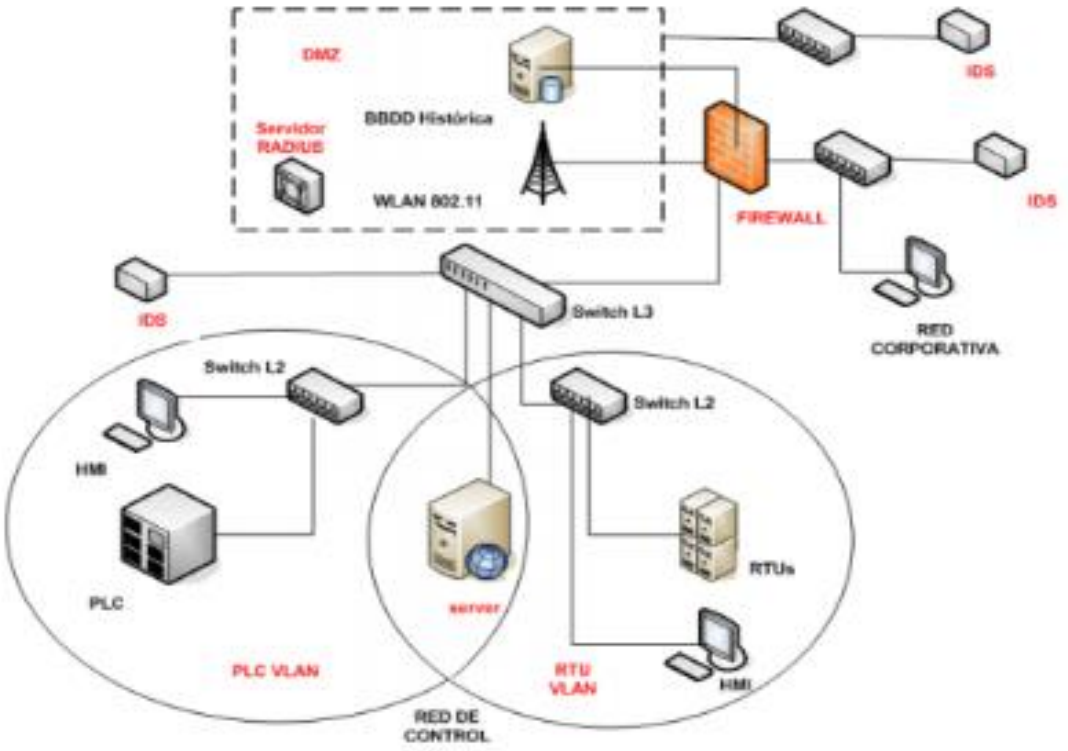


Ilustración 5 – Arquitectura de red SCADA propuesta por NISCC

Documento NIST SP 800-82

El documento NIST presenta un tratamiento integral de los aspectos de seguridad de los sistemas de control industrial (ICS) incluidos en un sistema SCADA, sistemas

distribuidos (DCS) y otros sistemas tales como los controladores lógicos programables (PLC).

En particular, analiza las topologías, amenazas y vulnerabilidades comunes del sistema, y sugiere contramedidas de seguridad que se utilizarán para mitigar el riesgo. Además, reorienta los controles de gestión, seguridad operativa y técnica, que se especificaron originalmente en el contexto de los sistemas de información federales, para entornos de control industrial.

El documento proporciona una visión general de ICS y topologías típicas del sistema, identifica las amenazas y vulnerabilidades típicas de estos sistemas y proporciona contramedidas de seguridad recomendadas para mitigar los riesgos asociados. (NIST SP 800-82, 2011)

ISA / IEC 62443

La norma ISA / IEC 62443, desarrollada por el comité ISA99 y adoptada por la Comisión Electrotécnica Internacional (IEC), proporciona un marco flexible para abordar y mitigar las vulnerabilidades de seguridad actuales y futuras de los sistemas de control y automatización industrial (de sus siglas en inglés IACS – Industrial Automation Control System). El comité ha absorbido las opiniones de los expertos en seguridad de IACS de todo el mundo para desarrollar estándares de consenso aplicables a todos los sectores industriales e infraestructura crítica. (ISA/IEC 62443, 2018)

Estándares de Informática Forense

La informática forense cuenta con varias normas que las regula, ellas son:

- ISO / IEC 27037:2012
- ISO / IEC 27042:2015
- RFC 3227
- RFC 4810
- RFC 4998
- RFC 6283

ISO / IEC 27037:2012

ISO / IEC 27037: 2012 estipula actividades específicas en el manejo de evidencia digital, que son la identificación, recolección, adquisición y preservación de evidencia digital potencial que puede ser de valor probatorio.

Orienta a las personas con respecto a situaciones comunes durante el proceso de manejo de evidencia digital y colabora con las organizaciones en los procedimientos disciplinarios y facilita el intercambio de potencial evidencia digital entre jurisdicciones.

También brinda orientación en Medios de almacenamiento digital utilizados en computadoras estándar como discos duros, disquetes, discos ópticos y magnetoópticos, dispositivos de datos con funciones similares como Teléfonos móviles, asistentes digitales personales (PDA), dispositivos electrónicos personales (PED), tarjetas de memoria, Sistemas de navegación móvil (GPS), Cámaras digitales fijas y de video (incluyendo CCTV), Computadora estándar con conexiones de red, Redes basadas en TCP / IP y otros protocolos digitales, y Dispositivos con funciones similares a las anteriores. (27037:2012, 2012)

ISO / IEC 27042:2015

ISO / IEC 27042: 2015 proporciona orientación sobre el análisis e interpretación de la evidencia digital de una manera que aborda los problemas de continuidad, validez, reproducibilidad y repetibilidad. Encapsula las mejores prácticas para la selección, diseño e implementación de procesos analíticos y registra información suficiente para permitir que dichos procesos sean sometidos a un escrutinio independiente cuando sea necesario. Orienta acerca de los mecanismos adecuados para verificar en el equipo de investigación, el dominio y la competencia.

También proporciona un marco común, para los elementos analíticos e interpretativos del manejo de incidentes de seguridad de los sistemas de información, que se puede utilizar para ayudar a implementar métodos nuevos y brindar un estándar común y mínimo para la evidencia digital producida a partir de esas actividades. (27042:2015, 2015)

RFC 3227

En la solicitud de comentarios 3227 (de sus siglas en inglés RFC3227) propone que un "incidente de seguridad" como se define en RFC2828 “Internet Security Glossary” (Shirey, 2000) es un evento del sistema relevante para la seguridad en el que la política de seguridad del sistema se desobedece o se infringe de alguna otra manera. El propósito de este documento es proporcionar a los Administradores del sistema pautas sobre la recopilación y el archivo de evidencia relevante para dicho incidente de seguridad.

Si la recopilación de pruebas se realiza correctamente, es mucho más útil en deteniendo al atacante, y tiene muchas más posibilidades de ser admisible en caso de enjuiciamiento. (Brezinski, 2002)

RFC 4810

En la solicitud de comentarios 4810 (de sus siglas en inglés RFC4810) se propone que la durabilidad de los datos digitales se ve socavada por el progreso continuo y los cambios en varios frentes. La vida útil de los datos puede exceder la vida útil de los formatos y mecanismos utilizados para almacenar los datos. La vida útil de los datos firmados digitalmente puede exceder los períodos de validez de los certificados de clave pública utilizados para verificar las firmas o el período de análisis criptográfico de los algoritmos criptográficos utilizados para generar las firmas, es decir, el tiempo después del cual un algoritmo ya no proporciona las propiedades de seguridad previstas. Se requieren medios técnicos y operativos para mitigar estos problemas. Una solución debe abordar problemas como la vida útil de los medios de almacenamiento, la planificación ante desastres, los avances en criptoanálisis o las capacidades computacionales, los cambios en el software tecnología y asuntos legales. (C. Wallace, 2007)

RFC 4998

En la solicitud de comentarios 4998 (de sus siglas en inglés RFC4998) se propone un protocolo de seguimiento de estándares de Internet para la comunidad de Internet, y solicita discusión y sugerencias para mejoras. Para mayor información consultar la actual edición de los "Estándares de protocolo oficial de Internet" (STD 1) para conocer el estado del protocolo y de su estandarización.

En muchos escenarios, los usuarios deben poder demostrar la existencia e integridad de los datos, incluidos los datos firmados digitalmente, de una manera común y reproducible durante un período de tiempo largo y posiblemente indeterminado. Este documento especifica la sintaxis y el procesamiento de un Registro de Evidencia, una estructura diseñada para soportar el no repudio a largo plazo de la existencia de datos. (T. Gondrom, 2007)

RFC 6283

En la solicitud de comentarios 6283 (de sus siglas en inglés RFC6283) se propone que, los usuarios deben poder demostrar el (tiempo de) existencia, integridad y validez de los datos, incluidos los datos firmados por períodos de tiempo largos o indeterminados.

Este documento especifica la sintaxis XML y las reglas de procesamiento para crear evidencia para el no repudio a largo plazo de la existencia y la integridad de los datos. El XMLERS de sintaxis de registro de evidencia de lenguaje de marcado extensible proporciona sintaxis alternativa y reglas de procesamiento a la sintaxis de ERN (sintaxis de sintaxis abstracta uno) ASN.1 (sintaxis de registro de evidencia) (RFC4998) mediante el uso de XML. (A. Jerman Blazic, 2011)

2.2.7. Ciberseguridad

Introducción a la Ciberseguridad

El concepto de clasificación de seguridad de la información es variable y algunas veces no informativo. La mayoría de las definiciones son procedentes de estándares y no se actualizaron durante años, incluso si el alcance y los desafíos en seguridad ahora son cada vez mayores con ciberseguridad Basado en una revisión de literatura, proponemos una nueva definición de Clasificación de seguridad de la información.

Como lo explican G. Collard, S. Ducroquet, E. Disson and G. Talens, la información de clasificación de seguridad es un concepto basado en Seguridad informática tradicional. La noción de ciberseguridad genera problemas en este enfoque tradicional. Utilizaremos la Definición de ciberseguridad proporcionada por Craigen y otros en 2014: “La ciberseguridad es la organización y recopilación de recursos, procesos y estructuras utilizados para proteger el ciberespacio y los sistemas habilitados para los sucesos que desalinean de jure de los derechos de propiedad de facto". Esta definición destaca lo interdisciplinario de la seguridad cibernética. Nos muestra que este tipo de seguridad ahora contiene un alcance más amplio que la seguridad informática tradicional. (Collard, 10-12 May 2017)

En la ilustración 6 se visualizan los 3 pilares del Ciber Ataque y Defensa. (singh, 2020).

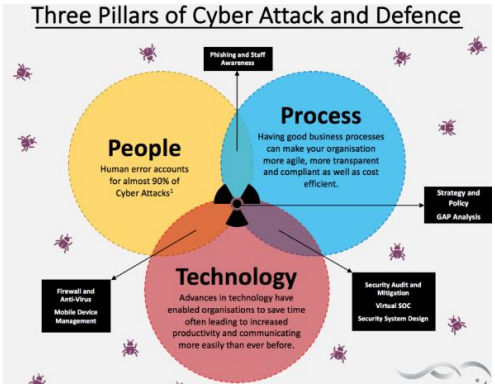


Ilustración 6 - Three Pilar of Cyber Attack and Defense

Aplicación de la Ciberseguridad en Redes Industriales

La aplicación de la Ciberseguridad en Redes Industriales se basa en las mejores prácticas y en los nuevos conceptos de seguridad que se aplican a nivel general. (Collard, 10-12 May 2017)

- ***Disponibilidad***: La disponibilidad de datos se basa en una medida porcentual del grado en que la maquinaria y el equipo están en un estado operable y se puede comprometer en el momento en que es necesario.
- ***Categorías de Seguridad***: Escala de medida, organizada, marcada y claramente definida.
- ***Confidencialidad***: La confidencialidad es el concepto de: asegurar que la información es accesible para leer, escuchar, grabar o remoción física solo a sujetos con derecho a ella, y que los sujetos solo leen o escuchan la información a la medida permitida.
- ***Contextualizar***: las circunstancias que conforman el escenario de una información digital y en términos de las cuales puede ser completamente entendido.
- ***Criticidad***: Mida el potencial para entrar en una crisis.
- ***Evento***: conjunto de resultados de un experimento en el que probabilidad asignada.
- ***Impacto***: la influencia o el efecto de un evento en una organización.
- ***Almacenamiento de Información***: El almacenamiento de información es parte del sistema de información que mantiene los datos accesibles para los procesadores de información.
- ***Integridad***: la integridad implica mantener la consistencia, precisión y confiabilidad de los datos durante todo su ciclo de vida.
- ***Legal***: leyes federales, órdenes ejecutivas, directivas, políticas, regulaciones, estándar.
- ***Propiedad***: una autoridad ejecutoria para emprender acciones particulares en dominios específicos Incluye el acceso correcto, retirada, gestión, exclusión y enajenación.
- ***Perfil del propietario***: Una manera de describir a un propietario categóricamente para que pueda agruparse para la evaluación de riesgos.
- ***Proteger***: restringir el acceso o uso de datos.

- ***Riesgo***: la noción de riesgo implica tanto incertidumbre como algún tipo de pérdida o daño que podría.
- ***Sensibilidad***: Detecta el cuidado especial y el manejo de la información. Especialmente cuando el manejo inapropiado de la información puede generar sanciones, identificar robos, pérdidas financieras, invasión de la privacidad o acceso no autorizado por parte de una o más personas. Parte de la información también está sujeta a regulación por leyes estatales o federales y requiere notificación en caso de divulgación.
- ***Uso***: Cualquier forma de hacer o manejar algo. Uso: Cualquier forma de hacer o manejar algo.
- ***Valor***: la importancia, el valor o la utilidad de algo.

La aplicación de la Ciberseguridad en Redes Industriales se basa en las mejores prácticas y en los nuevos conceptos de seguridad que se aplican según los estándares de seguridad. (Collard, 10-12 May 2017)

- ***Información*** (5) - NIST, ISO, ISA, RFC, NERC
- ***Categorías de Seguridad*** (5) - NIST, CoBiT, ISO, ISA, RFC
- ***Activo*** (4) - ISO, ISA, RFC, NERC
- ***Autorización*** (4) - NIST, ISO, ISA, NERC
- ***Requerimientos Legales*** (4) - NIST, ISO, ISA, NERC
- ***Valor*** (4) - CoBiT, ISO, ISA, RFC
- ***Criticidad*** (3) - CoBiT, ISO, ISA
- ***Propietario*** (3) - NIST, ISO, ISA
- ***Sensibilidad*** (3) - ISO, ISA, NERC
- ***Protección*** (2) - ISA, RFC
- ***Disponibilidad*** (1) - ISA
- ***Ciclo de Vida*** (1) - ISA
- ***Datos*** (1) - CoBiT
- ***Recurso*** (1) - CoBiT

Capítulo III - Desarrollo Técnico

"Los que se anticipan, se preparan y logran llegar primero al campo de batalla y esperan al adversario en posición de descanso. Los que llegan últimos, improvisan y comienzan la lucha agotados."
(Sun Tzu, *El arte de la guerra*, Siglo V a.c)

3.1. Limitaciones del uso de la forensia tradicional en los Sistemas SCADA

Con la creciente amenaza de ataques sofisticados en infraestructuras críticas, es vital que las investigaciones forenses tienen lugar inmediatamente después de un incidente de seguridad. Este trabajo presenta y propone un modelo de proceso forense SCADA estructurado para llevar fuera de las investigaciones forenses, una discusión sobre las limitaciones del uso forense tradicional, de los procesos de investigación y los desafíos que enfrentan los investigadores forenses. Además, fallas en las investigaciones existentes para proporcionar capacidad forense en los sistemas SCADA que se examinan en detalle.

3.1.1. Motivos para hacer un análisis forense

El análisis forense nos permite, mediante la utilización de software y hardware, identificar y luego verificar situaciones de fraude, visualizar funcionamiento de procesos y procedimientos, fuga de información y otros incidentes de seguridad. En este trabajo el análisis forense será utilizado para visualizar las brechas de seguridad de los sistemas industriales.

Hoy en día el análisis forense está siendo pensado como parte del área de Seguridad de la información en las organizaciones; otras lo ofrecen como un servicio privado, ya sea como parte de un juicio o investigación. En ambos casos participan: las partes interesadas, letrados de ambas partes, Escribanos, Peritos Informáticos Forenses, Auxiliares Forenses Informáticos, entre otros.

3.1.2. Tipos de análisis forense

Existen varias modalidades para realizar un análisis forense informático, de los cuales se pueden mencionar algunos de ellos: (CPCI, 2019)

- ***Análisis Forense de Equipos de Cómputo***: computadoras personales, notebooks, netbooks, memoria RAM.
- ***Análisis Forense de Dispositivos Móviles***: teléfonos celulares, Smartphones, tablets.
- ***Análisis Forense de Software***: software enlatado, software a medida, sistemas operativos,
- ***Análisis Forense de Dispositivos Extraíbles***: disco rígido magnético, disco estado sólido, pendrive, memorias flash, medios ópticos (CD, DVD, Blue Ray, Mini-Disc), medios magnéticos (Tape BackUp).
- ***Análisis Forense de Redes***: redes alámbricas e inalámbricas.

3.1.3. Limitaciones del análisis forense para sistemas industriales

Centrándonos en las redes industriales, hoy en día no es frecuente la ejecución de un análisis forense. Uno de los motivos de la escasez de análisis forense en los sistemas de redes industriales se debe a su funcionamiento operativo de 7x24, dado que no es posible detener el proceso producción de la empresa.

El proceso de producción continua impide la interrupción del servidor lo cual no permite el reinicio del equipo ante la instalación de actualizaciones del sistema operativo o en su defecto la instalación de un sistema operativo más reciente. Esto hace que el sistema operativo se mantenga desactualizado y vulnerable ante cualquier tipo de ataque por parte de los hackers, lo mismo sucede para los sistemas operativos que tienen soporte caduco por parte del fabricante. Esto también limita las actualizaciones de hardware haciendo que las mismas se vuelvan vulnerables y obsoletas permitiendo el acceso de los hackers.

Esta situación de no actualización del sistema operativo hace que no se puedan instalar nuevas versiones de los sistemas industriales. Lo mismo sucede al momento de la utilización de las herramientas forenses impidiendo el acceso a las herramientas más sofisticadas en lo que a tecnologías se refiere.

Otro motivo de la desactualización de hardware (no solo equipos de cómputo sino también la infraestructura) y software se debe, en ocasiones, a la negación al cambio, falta de concientización, temas económicos, entre otros, por parte de la organización.

3.2. Desarrollo Experimental

El estudio concluye con una experimentación de una arquitectura de capacidad forense SCADA propuesta en un DELTA DVP-12SP.

Para el desarrollo técnico de este trabajo se toma como escenario industrial o SCADA, un PLC portátil debido a las limitaciones de movilidad por la pandemia, lo cual no permite tener acceso a un escenario industrial o SCADA real.

La industria elegida para la programación del PLC es una fábrica que comercializa artículos plásticos. Para esta tarea se contó con el soporte de un integrante de la empresa Trend Ingeniería. (Carracedo, 2018)

3.2.1. Preparación del escenario

La preparación del escenario para el desarrollo técnico consta de varias etapas, las mismas son:

- Preparación y armado del tablero PLC portátil
- Instalación de Sistema Operativo Windows 7 Starter
- Instalación de la aplicación Wonderware
- Selección de herramientas forenses
- Programación del PLC portátil

Preparación y armado del tablero PLC portátil

El procedimiento de armado del PLC portátil se encuentra documentado en el anexo 1, punto 1 – Preparación y armado del tablero PLC, en el mismo se encuentra adjunto el documento denominado ICS portable - Guía para construcción e instalación. En el mismo se muestra el ensamblado de las partes, configuración e implementación del PLC. Dicho documento es parte de un trabajo practico realizado por Juan Pablo Perdiguizzi, para la asignatura Sistemas de Hardware para la Administración perteneciente a la Carrera de Ingeniería en Sistemas Informáticos de Facultad de Tecnología Informática de la Universidad Abierta Interamericana, a cargo del docente Jorge Kamlofsky quien a la vez es mi tutor en este trabajo.

A su vez, el PLC cuenta internamente con un programa que responde a un circuito electrónico con compuertas, botoneras, luces indicadoras y contactores.

Para este trabajo, se utiliza otro circuito el cual simula en mayor medida el ambiente industrial.

Instalación de Sistema Operativo Windows 7 Starter

El procedimiento de armado del PLC portátil se encuentra documentado en el anexo 1 – Instalación de Sistema Operativo. El proceso muestra el paso a paso de la instalación del SO en su versión Starter.

Instalación de la aplicación Wonderware

El procedimiento de armado del PLC portátil se encuentra documentado en el anexo 1 – Preparación y armado del tablero PLC. El proceso de armado explica el ensamblado de las partes del PLC.

Selección de Herramientas Forenses

Para este trabajo se empleó la herramienta de código abierto (open source):

Bento (portable)

Programación del PLC portátil

Antes de comenzar a programar el PLC hay que tener en cuenta el mapa de direcciones del dispositivo PLC, brindados por el fabricante, en este caso es DELTA. (DELTA, 2011)

En la ilustración 7 se visualiza el mapa de direcciones del dispositivo – Parte 1

Dispositivo	Rango	Rango efectivo			MODBUS Dirección	Dirección
		ES2/EX2	SS2	SA2/SX2		
S	000~255	000~1023	000~1023		000001~000256	0000~00FF
S	256~511				000257~000512	0100~01FF
S	512~767				000513~000768	0200~02FF
S	768~1023				000769~001024	0300~03FF
X	000~377 (Octal)	000~377	000~377		101025~101280	0400~04FF
Y	000~377 (Octal)	000~377	000~377		001281~001536	0500~05FF
T	000~255 bit	000~255	000~255		001537~001792	0600~06FF
	000~255 palabra	000~255	000~255		401537~401792	0600~06FF
M	000~255	0000 ~ 4095	0000~4095		002049~003584	0800~08FF
M	256~511					0900~09FF
M	512~767					0A00~0AFF
M	768~1023					0B00~0BFF
M	1024~1279					0C00~0CFF
M	1280~1535					0D00~0DFF
M	1536~1791				045057~047616	B000~B0FF
M	1792~2047					B100~B1FF
M	2048~2303					B200~B2FF
M	2304~2559					B300~B3FF
M	2560~2815					B400~B4FF
M	2816~3071					B500~B5FF
M	3072~3327					B600~B6FF
M	3328~3583					B700~B7FF
M	3584~3839					B800~B8FF
M	3840~4095					B900~B9FF
C	000~199 (16 bits)	000~199	000~199		003585~003784	0E00~0EC7
		000~199	000~199		403585~403784	0E00~0EC7
	200~255 (32 bits)	200~255	200~255		003785~003840	0EC8~0EFF
		200~255	200~255		401793~401903 (dirección impar válida)	0700~076F

Ilustración 7 - Dirección del dispositivo PLC - Parte 1

En la ilustración 8 se visualiza el mapa de direcciones del dispositivo – Parte 2

Dispositivo	Rango	Rango efectivo			MODBUS Dirección	Dirección
		ES2/EX2	SS2	SA2/SX2		
D	000~255	0000 ~ 9999	0000 ~ 4999	0000 ~ 9999	404097~405376	1000~10FF
D	256~511					1100~11FF
D	512~767					1200~12FF
D	768~1023					1300~13FF
D	1024~1279					1400~14FF
D	1280~1535				405377~408192	1500~15FF
D	1536~1791					1600~16FF
D	1792~2047					1700~17FF
D	2048~2303					1800~18FF
D	2304~2559					1900~19FF
D	2560~2815					1A00~1AFF
D	2816~3071					1B00~1BFF
D	3072~3327					1C00~1CFF
D	3328~3583					1D00~1DFF
D	3584~3839					1E00~1EFF
D	3840~4095					1F00~1FFF
D	4096~4351				436865~440960	9000~90FF
D	4352~4999					9100~91FF
D	4608~4863					9200~92FF
D	4864~5119					9300~93FF
D	5120~5375		N/A			9400~94FF
D	5376~5631					9500~95FF
D	5632~5887					9600~96FF
D	5888~6143					9700~97FF
D	6144~6399					9800~98FF
D	6400~6655					9900~99FF
D	6656~6911					9A00~9AFF
D	6912~7167					9B00~9BFF
D	7168~7423					9C00~9CFF
D	7424~7679					9D00~9DFF
D	7680~7935					9E00~9EFF
D	7936~8191					9F00~9FFF
D	8192~8447				440961~442768	A000~A0FF
D	8448~8703					A100~A1FF
D	8704~8959					A200~A2FF
D	8960~9215					A300~A3FF
D	9216~9471					A400~A4FF
D	9472~9727					A500~A5FF
D	9728~9983					A600~A6FF
D	9984~9999					A700~A70F

Ilustración 8 - Dirección del dispositivo PLC - Parte 2

El PLC se programó en lenguaje Ladder. Para este trabajo la realizo en capas llamadas Networks.

En la ilustración 9 se visualizan las networks correspondientes a la implementación SCADA.

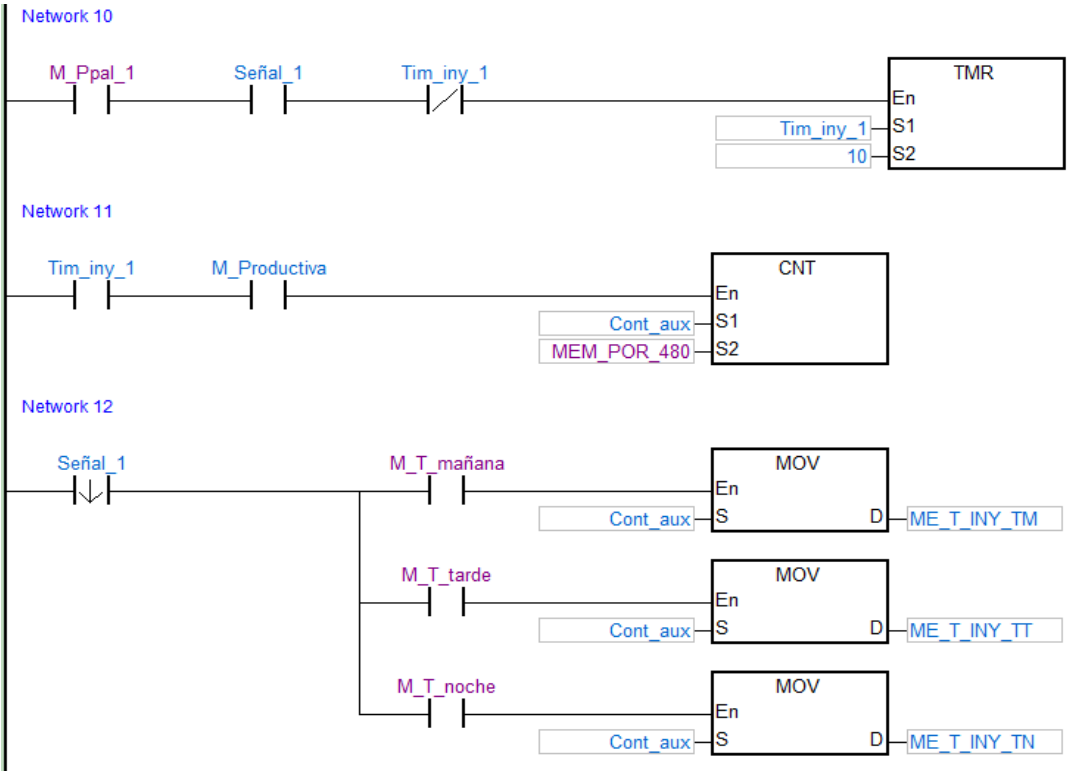


Ilustración 9 - Código de Programación Ladder

Pantallas del Programa del PLC SCADA

En este apartado se visualizan pantallas del Programa utilizado para este Trabajo. Las pantallas son:

- Carátula
- Menú
- Producción
- Totales
- CNC's
- Inyectora 1

Pantalla Carátula

Esta pantalla, es el inicio del programa como parte de este Trabajo, en el cual se menciona a la institución del tesista. Apretando el botón iniciar se accede a la pantalla Menú.

En la ilustración 10 se visualiza la "Pantalla Carátula".

Ilustración 10 - Pantalla Carátula

Pantalla Menú

Esta pantalla es la principal para el sistema ya que es el tablero de comandos, desde el cual se inicia la actividad del PLC y con las luces se puede monitorear el funcionamiento del PLC (flujo de datos), pero no monitorea internamente.

En la ilustración 11 se visualiza la "Pantalla Menú"

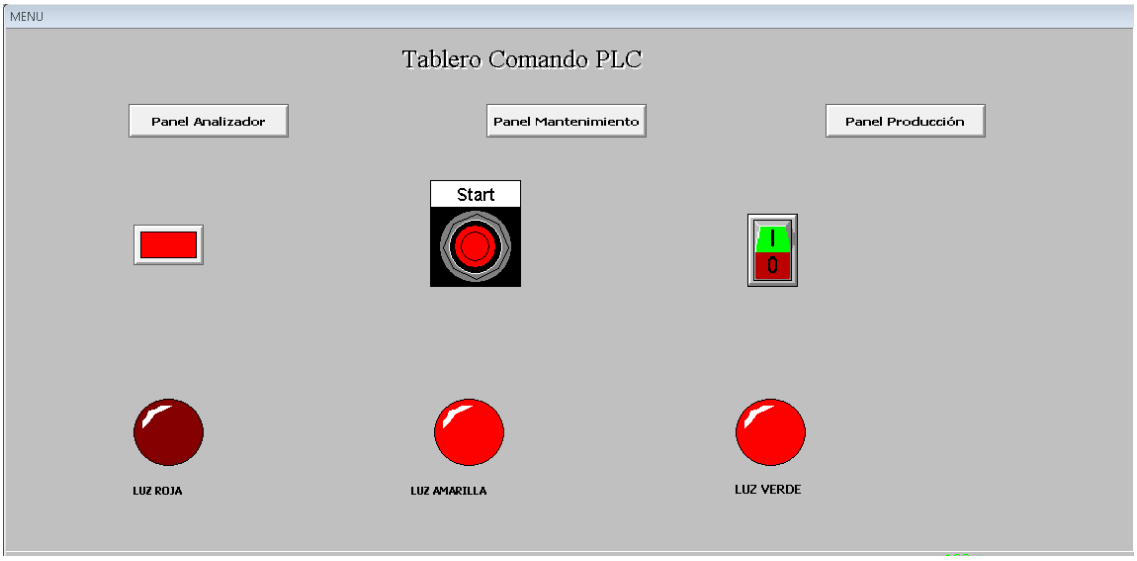


Ilustración 11 - Pantalla Menú

Pantalla Producción

Esta pantalla es la encargada de mostrar el estado de las inyectoras. (Carracedo, 2018)

En la ilustración 12 se visualiza la “Pantalla Producción”

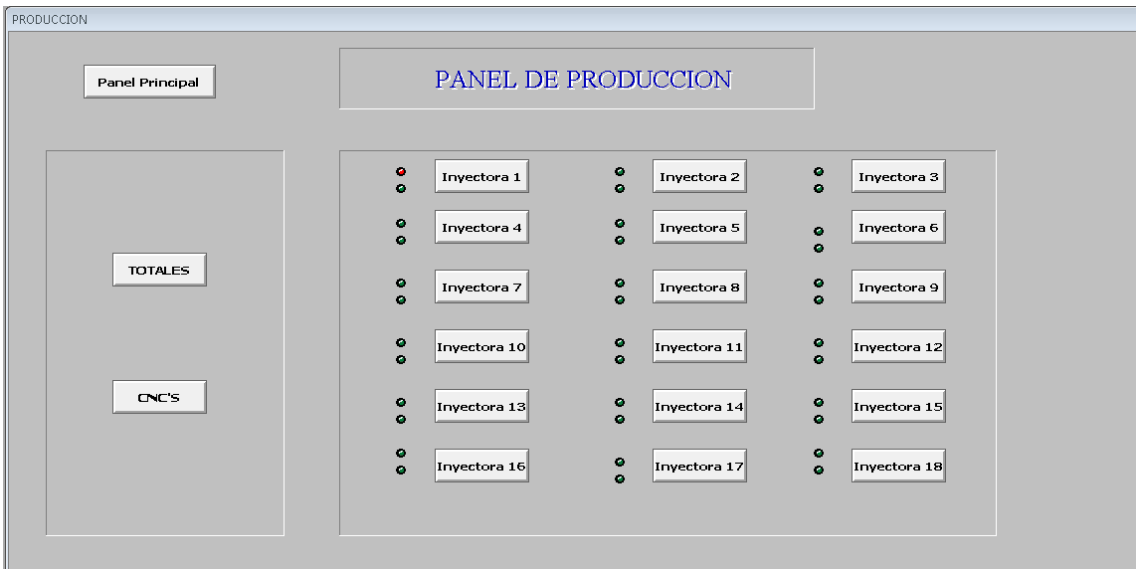


Ilustración 12 - Pantalla Panel de Producción

Pantalla Totales

Esta pantalla es la encargada de mostrar el conteo total de las piezas y los tiempos requeridos por el cliente. (Carracedo, 2018)

En la ilustración 13 se visualiza la “Pantalla Totales”

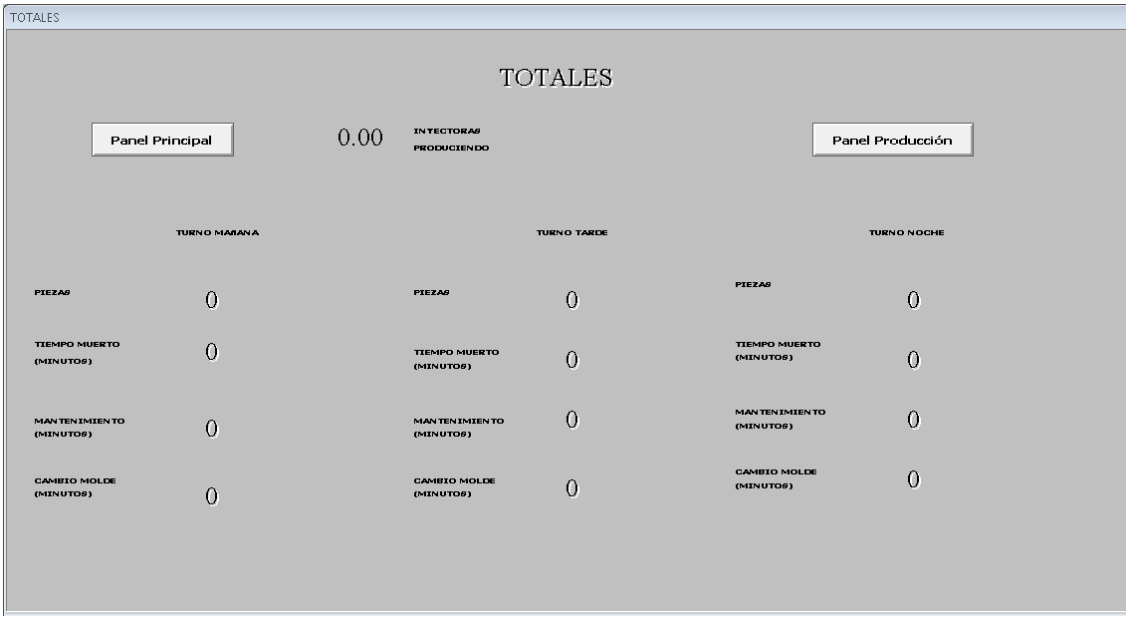
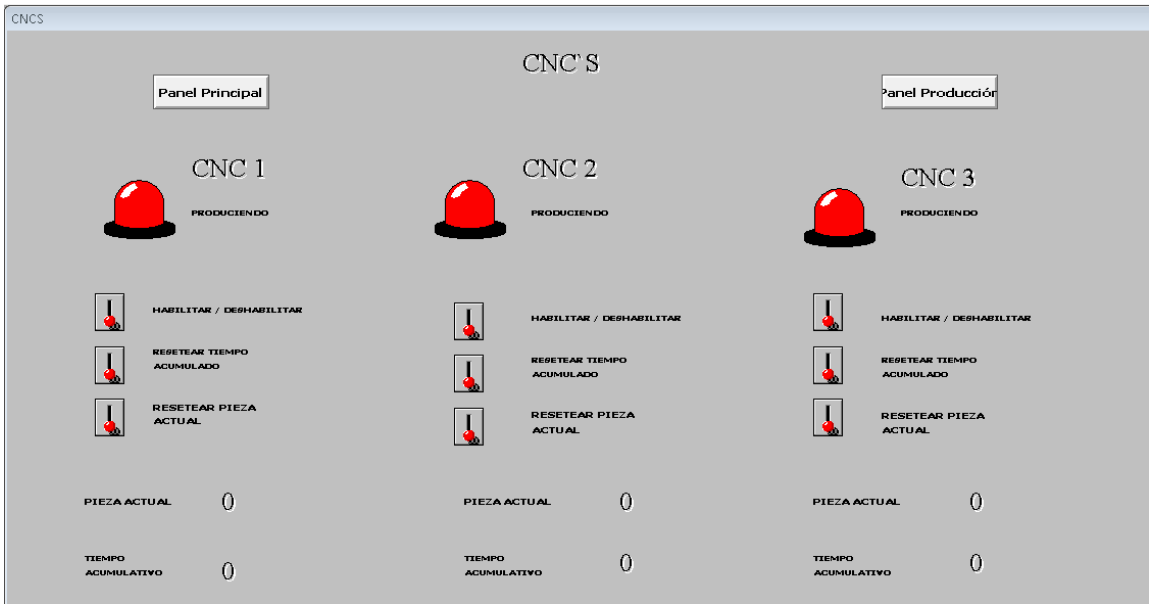


Ilustración 13 - Pantalla Totales

Pantalla CNC’s

Esta pantalla es la encargada de mostrar las variables y luces de estado de los CNC’s. (Carracedo, 2018)

En la ilustración 14 se visualiza la “Pantalla CNC’s”



Pantalla Inyectora 1

Esta pantalla es la encargada de visualizar las variables para la Inyectora 1. (Carracedo, 2018)

En la ilustración 15 se visualiza la “Pantalla Inyectora 1”

Ilustración 15 - Pantalla Inyectora 1

3.2.2. Obtención de la Información

En el laboratorio, la obtención de la información se realizó en vivo (live) tanto al equipo de cómputo como a la red. Para la adquisición de la información se utilizó la herramienta “Bento” mencionada en el punto 4.2.4, la adquisición de la información se tomó de:

- Sistema Operativo
- Red y Trafico de Red
- Actividades del PLC

Información del Sistema Operativo

La obtención de la información se inicia con un análisis de auditoria del sistema operativo para lo cual se utilizó la aplicación WinAudit, ejecutada desde la herramienta Bento. De la misma se obtiene una completa información del equipo de cómputo. La información obtenida se refiere tanto al Sistema Operativo como otras aplicaciones instaladas, puertos de comunicaciones, entre otros.

Desde el sitio web del fabricante del Sistema Operativo se obtiene información de vigencia de soporte y actualizaciones de seguridad entre otros.

Información de Red y Tráfico de Red

Para lectura del tráfico de red y captura de paquetes se utilizaron las aplicaciones NetworkTrafficViewer y SmartSnif, ambas ejecutadas desde la herramienta Bento.

Para el caso del tráfico de red, la aplicación NetworkTrafficViewer, al momento de ejecutar la aplicación, la misma captura las direcciones IP de los dispositivos conectados a la red. Para el caso de la captura de paquetes, la aplicación SmartSnif, al momento de ejecutar la aplicación, la misma captura el paquete de información que se transmite desde el equipo de cómputo al PLC y viceversa.

Información Log de Actividades del PLC

Para leer la trazabilidad de actividades realizadas por el PLC se utilizó la aplicación SMC (Archestra System Management Console), Log Viewer de la herramienta Wonderware InTouch.

3.2.3. Análisis de la Información

De la información obtenida en el punto 4.3 se realizó el análisis de:

- Sistema Operativo
- Red y Trafico de Red
- Actividades del PLC

Análisis del Sistema Operativo

De la herramienta Bento, se ejecutó la aplicación WinAudit, de la misma se obtuvo la información de:

- ***Vista General***

Item	***Value***
Computer Name	*SCADA-PC*
Domain Name	*WORKGROUP*
Site Name	
Roles	*Workstation, Server, Potential Browser, Master Browser*
Description	
Operating System	*Microsoft Windows 7 Starter 32-Bit*
Manufacturer	*Hewlett-Packard*
Model	*HP Pavilion dv5 Notebook PC*
Serial Number	*CNU0450K5S*
Asset Tag	*CNU0450K5S*
Number of Processors	*1*
Processor Description	*Intel(R) Core(TM) i5 CPU M 450 @ 2.40GHz*
Total Memory	*2048MB*
Total Hard Drive	*465.8GB*
Display	*@monitor.inf,%pnpmonitor.devicedesc%;Monitor PnP genérico, 14.5" (32cm x 18cm)*
BIOS Version	*_ASUS_ - 1*
User Account	*SCADA*
System Uptime	*6 Días 23 Hours 45 Minutes*
Local Time	*2020-08-02 16:08:01*

Tabla 06 - Vista General de Información del Sistema Operativo

- ***Sistema Operativo***

Item	***Value***
Name	*7*
Edition	*Starter*
Install Date	*2019-12-28 16:28:33*
Registered Owner	*SCADA*
Registered Organization	
Product ID	*00342-OEM-8992707-00082*
Major Version Number	*6*
Minor Version Number	*1*
Build Number	*7600*
Service Pack	
Service Pack Version	*0.0*
Plus! Version Number	
DirectX Version	*10.0*
Windows Directory	*C:\Windows*
System Directory	*C:\Windows\system32*
Temporary Directory	*C:\Users\SCADA\AppData\Local\Temp*
Operating System Language	*Spanish*
Number of Bits	*32*

Tabla 07 - Información del Sistema Operativo

- ***Sistema Operativo según su fabricante***

El sitio web del fabricante indica que su ciclo de vida y soporte ha caducado. (MICROSOFT, 2020).

- ***Grupos Relevantes***

Item / Grupo	*aaAdministrators*	*Administradores*
Group Type	*Local*	*Local*
Group Name	*aaAdministrators*	*Administradores*
Comment	*ArchestrA administrators*	*Los administradores tienen acceso completo y sin restricciones al equipo o dominio*

Tabla 08 - Información de los Grupos aaAdministrators y Administradores

- ***Grupos Miembro***

Group Name	*Member Name*
aaAdministrators	*SCADA-PC\Tesis*
Administradores	*SCADA-PC\SCADA*
Administradores	*SCADA-PC\Tesis*
Administradores	*SCADA-PC\Administrador*
IIS_IUSRS	*NT AUTHORITY\IUSR*
Invitados	*SCADA-PC\Invitado*
None	*Administrador*
None	*Invitado*
None	*SCADA*
None	*Tesis*
Usuarios	*NT AUTHORITY\Usuarios autentificados*
Usuarios	*NT AUTHORITY\INTERACTIVE*

Tabla 09 - Información de Grupos Miembro

- ***Derechos de Usuarios***

Policy	*Security Setting*
Access Credential Manager as a trusted caller	
Access this computer from the network	
Act as part of the operating system	
Add workstations to domain	
Adjust memory quotas for a process	
Allow log on through Terminal Services	
Back up files and directories	
Bypass traverse checking	
Change the system time	
Change the time zone	
Create a pagefile	
Create a token object	

Policy	Security Setting
Create global objects	
Create permanent shared objects	
Create symbolic links	
Debug programs	
Deny access to this computer from the network	
Deny log on as a batch job	
Deny log on as a service	
Deny log on locally	
Deny log on through Terminal Services	
Enable delegation	
Force shutdown from a remote system	
Generate security audits	
Impersonate a client after authentication	
Increase a process working set	
Increase scheduling priority	
Load and unload device drivers	
Lock pages in memory	
Log on as a batch job	
Log on as a service	
Log on locally	
Manage auditing and security log	
Manage the files on a volume	
Modify an object label	
Modify firmware environment values	
Profile single process	
Profile system performance	
Remove computer from docking station	
Replace a process-level token	
Restore files and directories	
Shut down the system	
Synchronize directory service data	
Take ownership of files or other objects	

Tabla 10 - Información de Derechos de Usuario

- ***Usuarios Relevantes***

Item / Usuarios	Administrador	SCADA
User Account	*Administrador*	*SCADA*
Full Name		
Description	*Cuenta integrada para la administración del equipo o dominio*	
Account Status	*Disabled, Not LockedPassword is required, Can change password, Password never expires, Password has not expired*	*Enabled, Not LockedPassword not required, Can change password, Password never expires, Password has not expired*

Local Groups	*Administradores*	*Administradores*
Global Groups	*None*	*None*
Last Logon	*2020-06-18 15:43:52*	*2020-08-01 01:01:56*
Last Logoff		
Number of Logons	*2*	*61*
Bad Password Count	*0*	*0*
Password Age	*4037 Días*	*39 Días*
Password Expired	*No*	*No*
Account Expires		

Tabla 11 - Información de los usuarios Administrador y SCADA

- ***Aplicaciones instaladas Relevantes***
  - COMMGR 1.11

Item	***Value***
Name	*COMMGR 1.11*
Vendor	*Delta Electronics, Inc.*
Version	*1.11.00*
Software ID	*COMMGR*

Tabla 12 - Información de la Aplicación COMMGR 1.11

  - DAServer Runtime Components Upgrade

Item	***Value***
Name	*DAServer Runtime Components Upgrade*
Vendor	*Invensys*
Version	*3.0.1*
Product Language	*English*
Install Date	*20200502*
Install Location	
Install Source	*C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\WW\DASEngine*
Install State	*The product is installed for the current user.*
Assignment Type	*Per Machine*
Package Code	*{9AB35443-845B-498B-B59D-E241C2A85050}*
Package Name	*Setup.msi*
Local Package	*C:\Windows\Installer\721493d8.msi*
Product ID	*none*
Registered Company	
Registered Owner	*SCADA*
Software ID	*{3F68CA0C-147C-4964-A3F6-0D1F39280F9E}*

Tabla 13 - información de la Aplicación DAServer Runtime Components Upgrade

  - DCISoft 1.22

Item	***Value***
Name	*DCISoft 1.22*

Vendor	*Delta Electronics, Inc.*
Version	*1.22.00*
Software ID	*DCISoft*

Tabla 14 - Información de la Aplicación DCISoft 1.22

- HWCONFIG 4.00

Item	***Value***
Name	*HWCONFIG 4.00*
Vendor	*Delta Electronics, Inc.*
Version	*4.00.09*
Software ID	*HWCONFIG*

Tabla 15 - Información de la Aplicación HWCONFIG 4.00

- ISPSoft 3.10

Item	***Value***
Name	*ISPSoft 3.10*
Vendor	*DELTA ELECTRONICS,INC.*
Version	*3.10*
Product Language	*English*
Install Date	*20200410*
Install Location	
Install Source	*C:\Users\SCADA\AppData\Local\Temp_isE30F*
Install State	*The product is installed for the current user.*
Assignment Type	*Per Machine*
Package Code	*{071AB193-12AA-45A3-A62F-AC8CE890F911}*
Package Name	*ISPSoft 3.10.msi*
Local Package	*C:\Windows\Installer\83fb2.msi*
Product ID	*None*
Registered Owner	*SCADA*
Software ID	*{8E89EEE3-D05E-4C02-B52A-A31FEABAEE9C}*

Tabla 16 - Información de la Aplicación ISPSoft 3.10

- Modicon MODBUS Plus

Item	***Value***
Name	*Modicon MODBUS Plus*
Vendor	*Wonderware*
Version	*8.1.0.0*
Product Language	*English*
Install Date	*20200502*
Install Location	
Install Source	*C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\SC\MBPLUS*
Install State	*The product is installed for the current user.*
Assignment Type	*Per Machine*
Package Code	*{87DF712A-74C3-4E02-B376-895219130CB6}*
Package Name	*Setup.msi*
Local Package	*C:\Windows\Installer\12302c.msi*
Product ID	*1*
Registered Company	
Registered Owner	*SCADA*

Software ID	*{A325F6BD-CAEE-4D25-80CB-BE0C976A035F}*

Tabla 17 - Información de la Aplicación Modicon MODBUS Plus

- Sentinel Protection Installer 7.5.0

Item	Value
Name	*Sentinel Protection Installer 7.5.0*
Vendor	*SafeNet, Inc.*
Version	*7.5.0*
Product Language	*English*
Install Date	*20200604*
Install Location	*C:\Program Files\SafeNet Sentinel\Sentinel Protection Installer\7.5.0*
Install Source	*C:\Users\SCADA\Downloads\DAMBTCP20-20200604T192228Z-001\ DAMBTCP20\Redist\Rainbow*
Install State	*The product is installed for the current user.*
Assignment Type	*Per Machine*
Package Code	*{B0369E3A-3DE6-4DBD-B658-F52334198E6E}*
Package Name	*Sentinel Protection Installer 7.5.0.msi*
Local Package	*C:\Windows\Installer\4b2e06.msi*
Software ID	*{A5A63519-F5C2-4F4A-849A-F28A1AB3D522}*

Tabla 18 - Información de la Aplicación Sentinel Protection Installer 7.5.0

- SuiteLink

Item	Value
Name	*SuiteLink*
Vendor	*Invensys*
Version	*2.0.001*
Product Language	*English*
Install Date	*20200502*
Install Location	
Install Source	*C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\WW\SuiteLink*
Install State	*The product is installed for the current user.*
Assignment Type	*Per Machine*
Package Code	*{1D6CB077-83E8-49A7-9A14-05D43E7CB20A}*
Package Name	*Setup.msi*
Local Package	*C:\Windows\Installer\2a1ce.msi*
Product ID	*none*
Registered Company	
Registered Owner	*SCADA*
Software ID	*{97C680A3-1A53-40ED-AFC2-2FE21D3C4B2B}*

Tabla 18 - Información de la Aplicación SuiteLink

- Virtual COM

Item	Value
Name	*Virtual COM*
Vendor	*Delta Electronics, Inc.*
Version	*2.03*
Software ID	*Virtual COM*

Tabla 19 - Información de la Aplicación Virtual COM

- Wonderware Alarm2U DAServer

Item	Value
Name	Wonderware Alarm2U DAServer
Vendor	Invensys
Version	1.0.0
Product Language	English
Install Date	20200502
Install Location	
Install Source	C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\WW\K2U\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{4888D194-F2AF-43C6-81DA-1781FA8F8DD5}
Package Name	Setup.msi
Local Package	C:\Windows\Installer\2a1c2.msi
Product ID	none
Registered Company	
Registered Owner	SCADA
Software ID	{2988659E-548F-4F02-9378-C2D9875CE5EB}

Tabla 20 - Información de la Aplicación Wonderware Alarm2U DAServer

- Wonderware Common Components

Item	Value
Name	Wonderware Common Components
Software ID	Wonderware Common Component

Tabla 21 - Información de la Aplicación Wonderware Common Components

- Wonderware Compact Panel DAServer

Item	Value
Name	Wonderware Compact Panel DAServer
Vendor	Invensys
Version	1.0.0
Product Language	English
Install Date	20200502
Install Location	
Install Source	C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\WW\DASPanel\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{66286EEB-FB17-439F-AA6E-0C9C0F22E315}
Package Name	Setup.msi
Local Package	C:\Windows\Installer\72149397.msi
Product ID	none
Registered Company	
Registered Owner	SCADA
Software ID	{CC48FCEA-D2FC-4CBC-9497-BDCA5551574D}

Tabla 22 - Información de la Aplicación Wonderware Compact Panel DAServer

- Wonderware FactorySuite Gateway

Item	Value
Name	Wonderware FactorySuite Gateway
Vendor	Wonderware
Version	2.0.0
Product Language	English
Install Date	20200502
Install Location	
Install Source	C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\WW\FSG\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{FC2FE91B-9380-4063-9D75-6FBBBFCF80E9}
Package Name	FSGateway.msi
Local Package	C:\Windows\Installer\721493ed.msi
Product ID	none
Registered Company	
Registered Owner	SCADA
Software ID	{0AEB2C47-7ED7-4F23-B59B-0EB7414CED54}

Tabla 23 - Información de la Aplicación Wonderware FactorySuite Gateway

- Wonderware InTouch

Item	Value
Name	Wonderware InTouch
Vendor	Wonderware
Version	10.1.0
Product Language	English
Install Date	20200303
Install Location	C:\Program Files\Wonderware\InTouch\
Install Source	C:\Users\SCADA\Desktop\Instaladores intouch\Intouch - 10.1\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{E8F8FEAC-93DF-4152-823D-BB12CA5D9062}
Package Name	Setup.msi
Local Package	C:\Windows\Installer\c0772.msi
Product ID	none
Registered Company	
Registered Owner	SCADA
Software ID	{17736C93-2694-488B-9F8A-0CA46E952FDD}

Tabla 24 - Información de la Aplicación Wonderware InTouch

- Wonderware Kontron DAServer

Item	Value
Name	Wonderware Kontron DAServer
Vendor	Wonderware
Version	1.0.0
Product Language	English
Install Date	20200502
Install Location	

Item	Value
Install Source	C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\WW\Kontron\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{85475966-3498-448F-BBAD-392D46FA5F59}
Package Name	Setup.msi
Local Package	C:\Windows\Installer\2a1c7.msi
Product ID	none
Registered Company	
Registered Owner	SCADA
Software ID	{1E515453-E7EE-4D84-8B2D-B038AB9F2168}

Tabla 25 - Información de la Aplicación Wonderware Kontron DAServer

- Wonderware MBSerial DAServer

Item	Value
Name	Wonderware MBSerial DAServer
Vendor	Invensys
Version	2.5.200
Product Language	English
Install Date	20200502
Install Location	
Install Source	C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\SC\DASMBSerial-2.5.200\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{E19D06A3-41D4-4AD9-A1D0-ABB163CB84AC}
Package Name	Setup.msi
Local Package	C:\Windows\Installer\123037.msi
Product ID	none
Registered Company	
Registered Owner	SCADA
Software ID	{8C23365E-A7EB-4313-A198-E2628E29B3F7}

Tabla 26 - Información de la Aplicación Wonderware MBSerial DAServer

- Wonderware MBTCP DAServer

Item	Value
Name	Wonderware MBTCP DAServer
Vendor	Invensys
Version	2.0.0
Product Language	English
Install Date	20200604
Install Location	
Install Source	C:\Users\SCADA\Downloads\DAMBTCP20-20200604T192228Z-001\DAMBTCP20\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{9B41984B-E8A7-481C-9BAA-C2C74395FF6D}
Package Name	Setup.msi
Local Package	C:\Windows\Installer\4b2e12.msi

Item	Value
Product ID	none
Registered Company	
Registered Owner	SCADA
Software ID	{BE4A342E-7295-46CE-8D05-86749FF1B6AD}

Tabla 27 - Información de la Aplicación Wonderware MBTCP DAServer

- Wonderware Modicon MODBUS Ethernet

Item	Value
Name	Wonderware Modicon MODBUS Ethernet
Vendor	Wonderware
Version	8.1.0.0
Product Language	English
Install Date	20200502
Install Location	
Install Source	C:\Users\SCADA\Desktop\Instaladores intouch\Drivers\SC\MBENET\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{591A376C-1CFF-48DF-8780-2C4474A18046}
Package Name	Setup.msi
Local Package	C:\Windows\Installer\123010.msi
Product ID	1
Registered Company	
Registered Owner	SCADA
Software ID	{9FA3A3D2-E5CF-4200-8ED6-4137DADB474B}

Tabla 28 - Información de la Aplicación Wonderware Modicon MODBUS Ethernet

- WonderwareTSInfoTool

Item	Value
Name	WonderwareTSInfoTool
Vendor	Wonderware
Version	1.0.0
Product Language	English
Install Date	20191231
Install Location	
Install Source	C:\Users\SCADA\Desktop\SCADA\WonderwareTSInfoToolSetup\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{5AA27EFB-1436-47E0-BDCE-516E386489C0}
Package Name	WonderwareTSInfoToolSetup.msi
Local Package	C:\Windows\Installer\b47d44d.msi
Software ID	{E7D56D8D-998C-48A8-A06F-3CED1DB1B290}

Tabla 29 - Información de la Aplicación WonderwareTSInfoTool

- WPLSoft 2.49

Item	Value
Name	WPLSoft 2.49
Vendor	DELTA ELECTRONICS, INC.
Version	2.49
Product Language	English
Install Date	20191229
Install Location	
Install Source	C:\Users\SCADA\AppData\Local\Temp_is76E4\
Install State	The product is installed for the current user.
Assignment Type	Per Machine
Package Code	{69651369-3CC2-420E-956B-BA5B5B83A420}
Package Name	WPLSoft 2.49.msi
Local Package	C:\Windows\Installer\35939.msi
Product ID	None
Registered Company	JK
Registered Owner	SCADA
Software ID	{51124DB3-E0FE-45BD-B7FA-A795F783DDB2}

Tabla 30 - Información de la Aplicación WPLSoft 2.49

- ***Dispositivos de Red***

Item / Dispositivo	Intel(R) Centrino(R) Wireless-N 1000	NIC de Gigabit Ethernet PCI-E de la familia Realtek RTL8168D / 8111D (NDIS 6.20)
Adapter Number	2	1
Adapter Name	Intel(R) Centrino(R) Wireless-N 1000	NIC de Gigabit Ethernet PCI-E de la familia Realtek RTL8168D/8111D (NDIS 6.20)
DNS Host Name		SCADA-PC
DNS Servers		
IP Address		192.168.1.20 fe80::3cff:bcd8:29ed:7bea
IP Subnet		255.255.255.0 64
Default IP Gateway		192.168.1.1 fe80::8f5:dfff:fea3:7167
DHCP Enabled	1	0
DHCP Server		
DHCP IP Address		
DHCP Lease Obtained		
DHCP Lease Expires		
Status Code	0	0
Adapter Status	This device is working properly.	This device is working properly.
Adapter Type	Ethernet 802.3	Ethernet 802.3
MAC Address	00:26:C7:CB:2F:AA	1C:C1:DE:BC:E1:22
Connection Status	Media disconnected	Connected
Connection Speed		1000Mbps

Tabla 31 - Información del Dispositivo de Red Wireless y Gigabit Ethernet PCI-E

- ***Puertos de comunicación***

Item / Puertos	*COM1*	*COM2*	*COM3*	*COM4*
Port Number	*2*	*3*	*4*	*5*
Port Name	*COM1:*	*COM2:*	*COM3:*	*COM3:*
Monitor Name	*Monitor Local*	*Monitor Local*	*Monitor Local*	*Monitor Local*
Description	*Puerto local*	*Puerto local*	*Puerto local*	*Puerto local*
Port Type	*Can write, Can read*	*Can write, Can read*	*Can write, Can read*	*Can write, Can read*

Tabla 32 - Información de los Puertos COM1, COM2, COM3 y COM4

- ***Puertos Abiertos Relevantes***
  - TCP ::1:59568

Item	*Value*
Port Protocol	*TCP*
Local Address	*::1*
Local Port	*59568*
Caption	*TCP ::1:59568*
Service Name	
Remote Address	*::1*
Remote Port	*49155*
Connection State	*Connection established (ESTABLISHED)*
Process Name	*C:\Program Files\Wonderware\DAServer\DASMBTCP\Bin\DASMBTCP.exe*
Process ID	*2772*
Process Description	*ServerExe Module*
Process Manufacturer	*Invensys Systems, Inc.*

Tabla 33 - Información del Puerto TCP 59568

- ***Tabla de Ruteo***
  - 0.0.0.0

Item	*Value*
Destination	*0.0.0.0*
Netmask	*0.0.0.0*
Next Hop	*192.168.1.1*
Interface	*192.168.1.20*
Route Type	*Remote*
Protocol	*Static*
Age	*6 Días 23 Hours 45 Minutes*
Metric	*266*

Tabla 34 - Información de la dirección IP 0.0.0.0

- 127.0.0.0

Item	Value
Destination	127.0.0.0
Netmask	255.0.0.0
Next Hop	127.0.0.1
Interface	127.0.0.1
Route Type	Local
Protocol	Static
Age	6 Días 23 Hours 46 Minutes
Metric	306

Tabla 36 - Información de la dirección IP 127.0.0.0

- 127.0.0.1

Item	Value
Destination	127.0.0.1
Netmask	255.255.255.255
Next Hop	127.0.0.1
Interface	127.0.0.1
Route Type	Local
Protocol	Static
Age	6 Días 23 Hours 46 Minutes
Metric	306

Tabla 35 - Información de la dirección IP 127.0.0.1

- 192.168.1.0

Item	Value
Destination	192.168.1.0
Netmask	255.255.255.0
Next Hop	192.168.1.20
Interface	192.168.1.20
Route Type	Local
Protocol	Static
Age	2 Días 21 Hours 40 Minutes
Metric	266

Tabla 36 - Información de la dirección IP 192.168.1.0

- 192.168.1.20

Item	Value
Destination	192.168.1.20
Netmask	255.255.255.255
Next Hop	192.168.1.20
Interface	192.168.1.20
Route Type	Local
Protocol	Static
Age	2 Días 21 Hours 40 Minutes
Metric	266

Tabla 37 - Información de la dirección IP 192.168.1.20

- 192.168.1.255

Item	Value

Destination	192.168.1.255
Netmask	255.255.255.255
Next Hop	192.168.1.20
Interface	192.168.1.20
Route Type	Local
Protocol	Static
Age	2 Días 21 Hours 40 Minutes
Metric	266

Tabla 38 - Información de la dirección IP 192.168.1.255

- ***Configuración de Seguridad***

Item	Name	Setting
Accounts	Administrator account status	Disabled
Accounts	Guest account status	Disabled
Accounts	Rename administrator account	Administrador
Accounts	Rename guest account	Invitado
Account Lockout Policy	Account lockout duration	Not Applicable
Account Lockout Policy	Account lockout threshold	0 Attempts
Account Lockout Policy	Reset account lockout counter after	Not Applicable
AutoLogon	Enabled	
Automatic Updates	Update status	Not configured
Automatic Updates	Update schedule	
Internet Explorer	Run script	Allow
Internet Explorer	Run ActiveX	Allow
Internet Explorer	Run Java	Allow
Internet Explorer	Download files	Allow
Internet Explorer	Install desktop items	Prompt user
Internet Explorer	Launch applications	Prompt user
Network Access	Allow anonymous SID/name translation	Disabled
Screen Saver	Enabled	1
Screen Saver	Timeout	0
Screen Saver	Password protected	

Tabla 39 - Información de la Configuración de Seguridad

Análisis de la Red y Tráfico de Red

Antes de realizar el análisis de red y tráfico de red se realizó una verificación de la configuración de la dirección IP del PLC en la consola de administración de la aplicación Wonderware (ArchestrA System Management Console). En la misma se verifica que la dirección IP del PLC es 192.168.1.5.

En la ilustración 16 se visualiza una captura de pantalla de la consola de administración de la aplicación Wonderware.

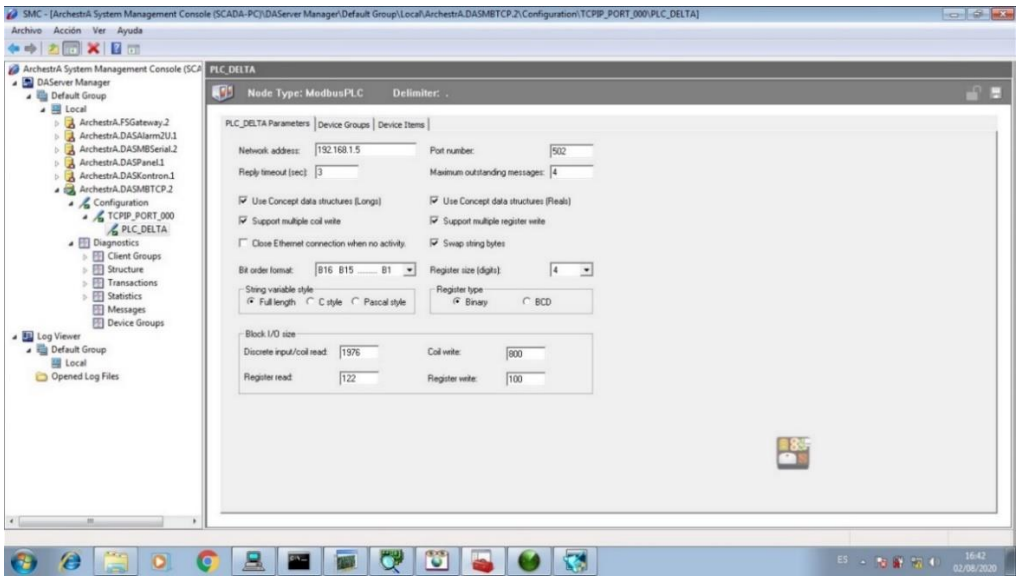


Ilustración 16 - Pantalla de Consola de Administración de la aplicación Wonderware

Luego se verificó la conectividad entre el equipo de cómputo y el PLC, para ello se ejecutó el comando CMD (de sus siglas en inglés, Command Prompt) con privilegios de administrador, lo cual habilitó la consola de comandos (símbolo del sistema) del sistema operativo Windows 7. Los pasos antes ejecutados permitieron el uso del comando PING, lo cual demostró la comunicación satisfactoria entre el equipo de cómputo y el PLC.

En la ilustración 17 se visualiza la ejecución del comando PING y la satisfactoria comunicación entre el equipo de cómputo y el PLC.

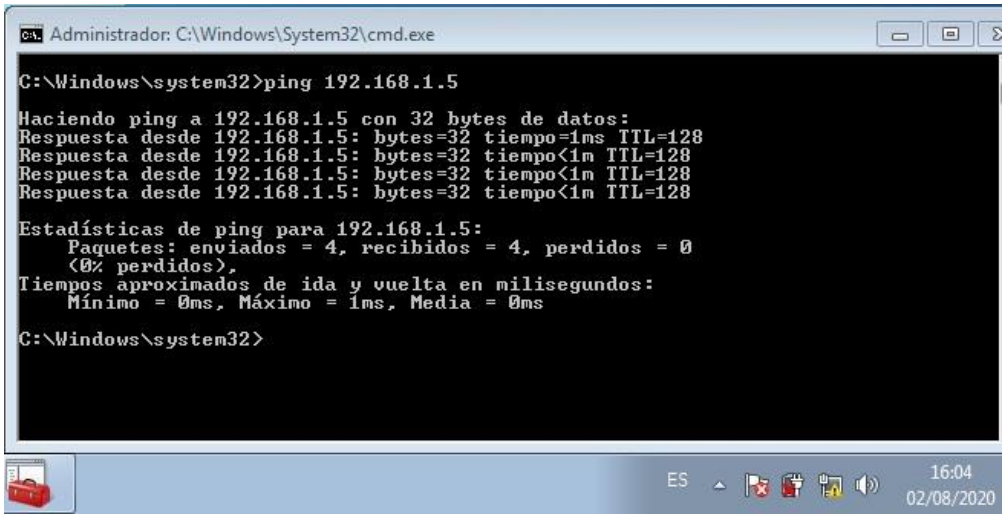


Ilustración 17 – Visualización de comunicación entre el equipo de cómputo y el PLC

La lectura del tráfico de red, a través de la aplicación NetworkTrafficViewer, arrojó resultados satisfactorios de comunicación recíproca entre el equipo de cómputo y el PLC.

En la ilustración 18 se visualiza que en el tráfico de red hay una comunicación recíproca, mediante el protocolo ICMP y TCP, entre el equipo de cómputo y el PLC.

También se verifican las direcciones IP del equipo de cómputo (192.168.1.2) y el PLC (192.168.1.5).

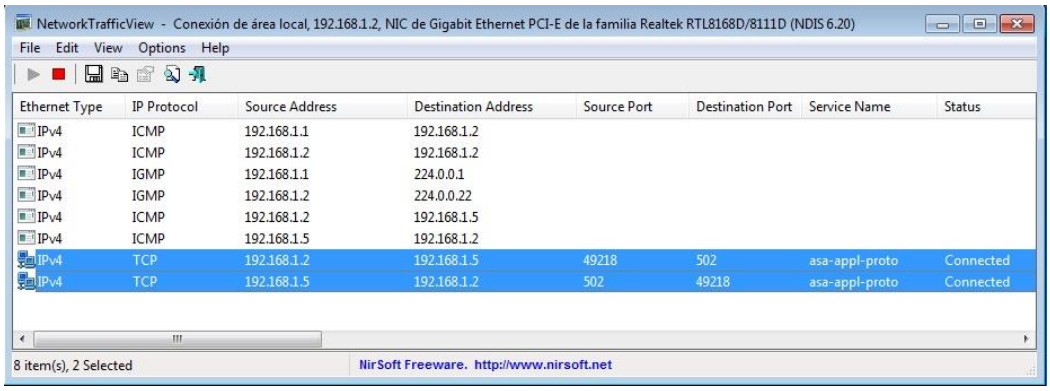


Ilustración 18 - Visualización de comunicación entre el equipo de cómputo y el PLC

Para el caso de la captura de paquetes de datos, la aplicación SmartSniff tiene 3 (tres) modos de visualización de paquetes de datos capturados, ellos son: Automático, Ascii y Hex Dump. Luego de la ejecución de la aplicación se verificó que es posible la captura de paquetes de datos entre el equipo de cómputo y el PLC.

Para el caso del equipo de cómputo en la ilustración 19 se visualiza la captura de paquetes de datos en modo Automático.

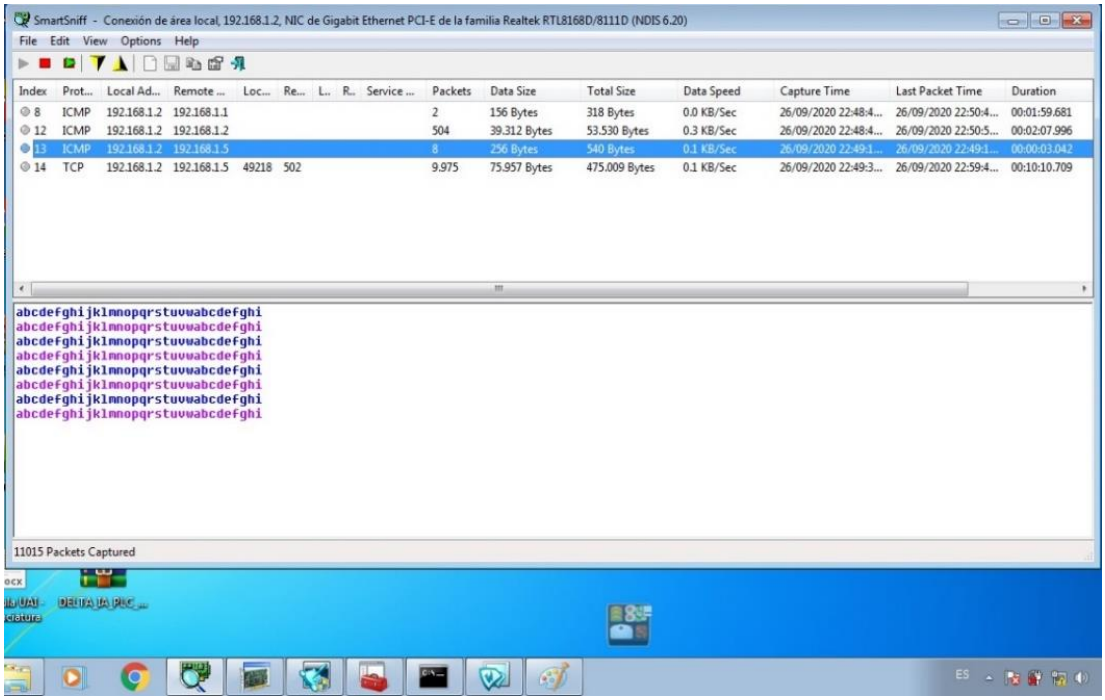


Ilustración 19 - Captura de paquetes de datos en modo Automático

Siguiendo con el equipo de cómputo en la ilustración 20 se visualiza la captura de paquetes de datos en modo Ascii.

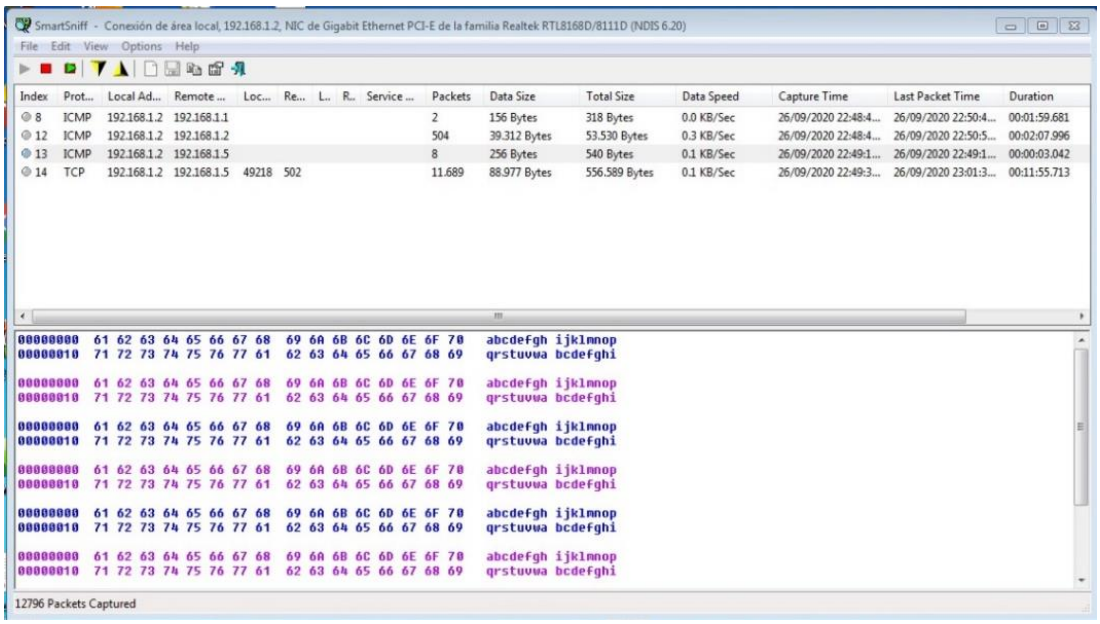


Ilustración 20 - Captura de paquetes de datos en modo Ascii

Para el caso del PCL en la ilustración 21 se visualiza la captura de paquetes de datos en modo Automático.

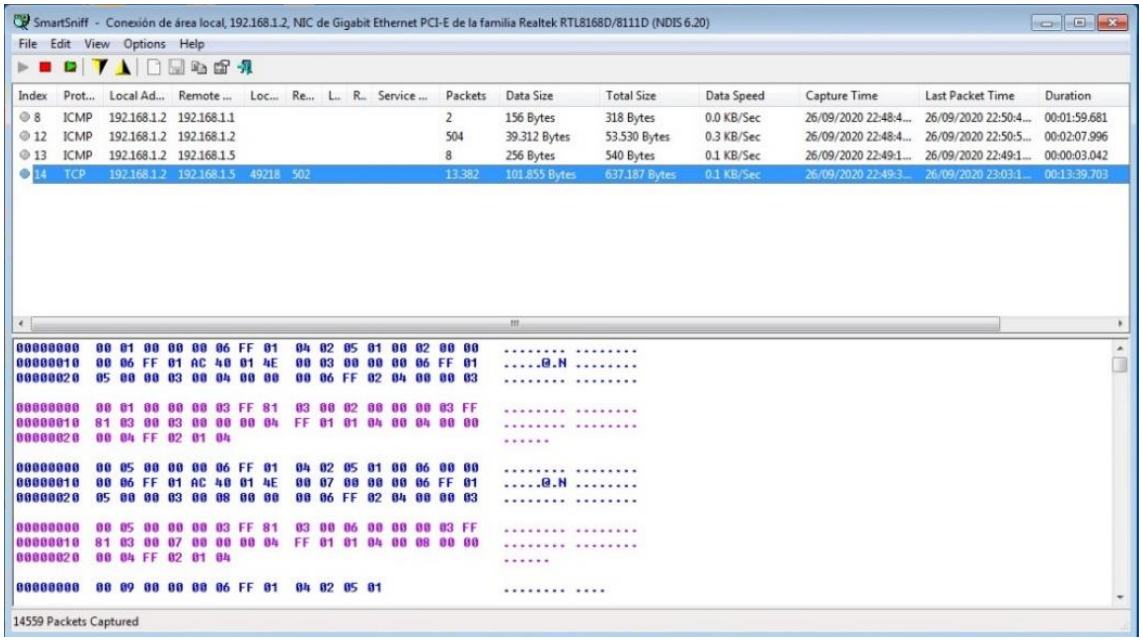


Ilustración 21 - Captura de paquetes de datos en modo Automático

Siguiendo con el PLC en la ilustración 22 se visualiza la captura de paquetes de datos en modo Hex Dump.

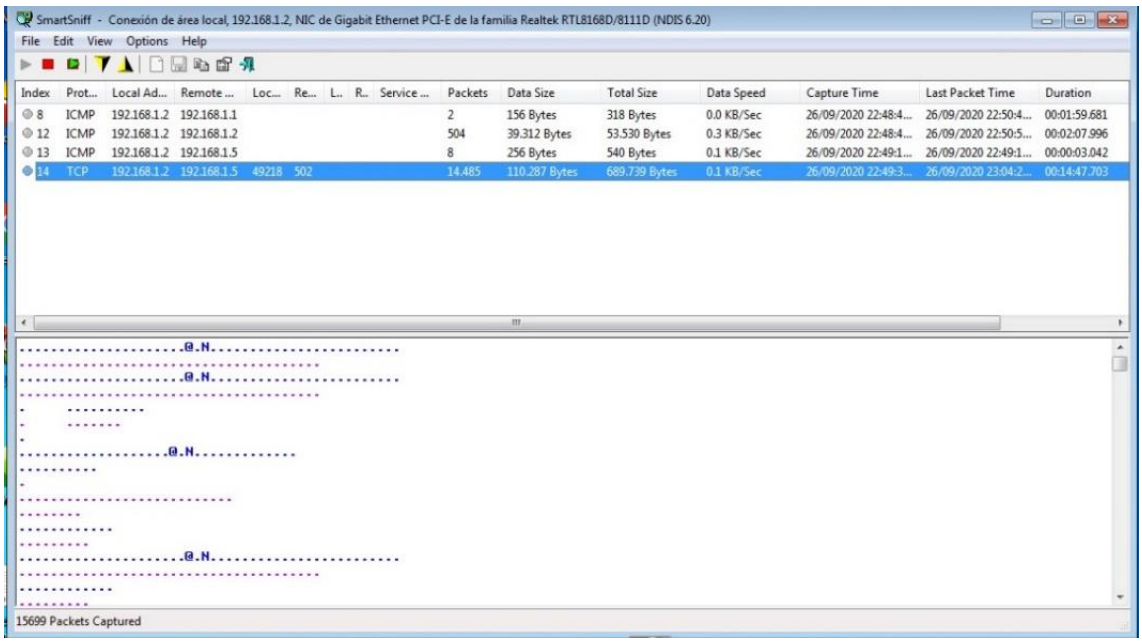


Ilustración 22 - Captura de paquetes de datos en modo Hex Dump

Log de Actividades del PLC

Para leer la trazabilidad de actividades realizadas por el PLC se utilizó la aplicación SMC de la herramienta Wonderware InTouch.

En dicha aplicación se visualizan los eventos satisfactorios y no satisfactorios que ocurren en el PLC.

En la ilustración 23 se visualizan las actividades del Intouch Wonderware, en la cual presenta un evento referido al licenciamiento del software.

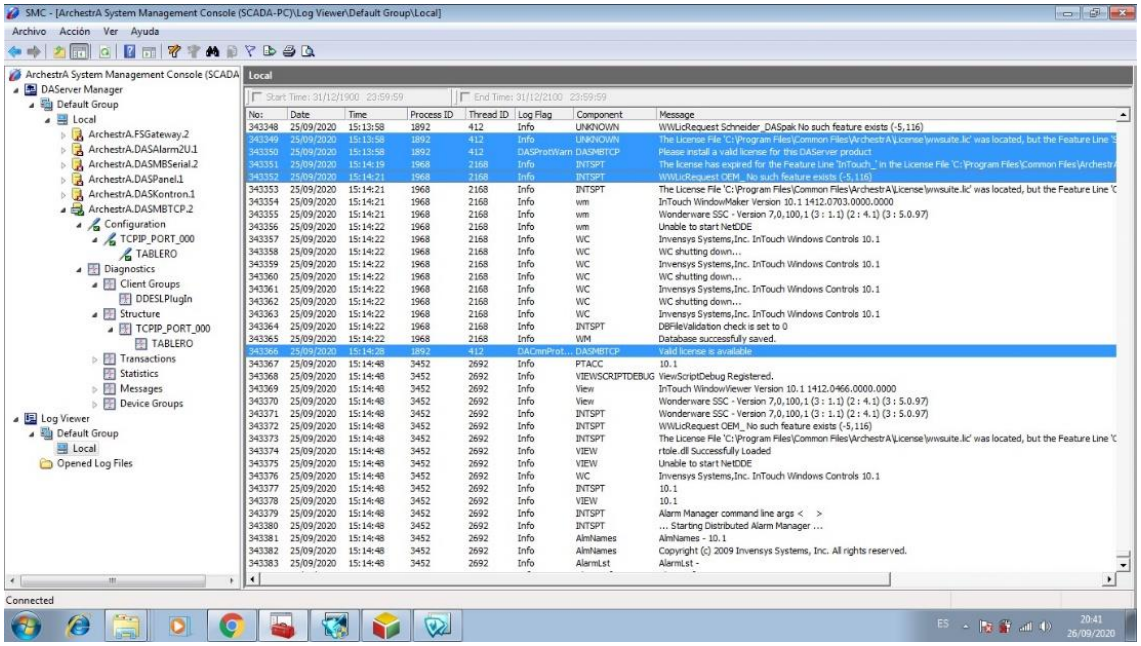


Ilustración 23 – Visor de Eventos de actividad del software Intouch Wonderware - Licenciamiento

En la ilustración 24 se visualizan las actividades del Intouch Wonderware, en la cual presenta un evento referido a la conexión del software.

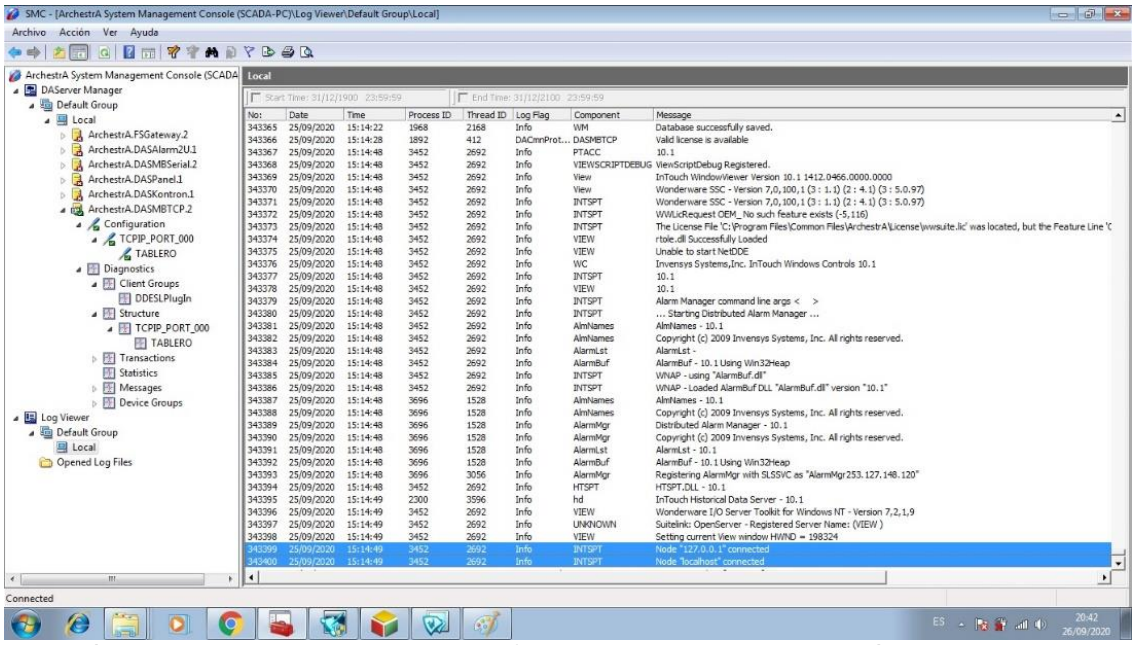


Ilustración 24 - Visor de Eventos de actividad del software Intouch Wonderware - Conexión

3.2.4. Obtención de Resultados

En este apartado vemos los resultados obtenidos en:

- Sistema Operativo
- Red y Tráfico de red
- Log de actividades del PLC

Resultado Análisis del Sistema Operativo

De la herramienta Bento, se ejecutó la aplicación WinAudit, de la misma se obtuvo la información de:

- ***Vista General***: muestra información general del equipo de cómputo, tales como: nombre de equipo, roles, sistema operativo, fabricante modelo, número de serie, memoria ram y hora local entre otros.

- ***Sistema Operativo***: Información específica del sistema operativo, no presenta anomalías.

- ***Sistema Operativo según fabricante***: Según Microsoft, quien es propietario del software, el 14/01/2020, todo equipo de cómputo que

contenga cualquier versión del sistema operativo Windows 7 seguirá funcionando, pero Microsoft ya no proporcionara lo siguiente:

- *Soporte Técnico.*
- *Actualizaciones de software*
- *Actualizaciones de seguridad*

Dado este escenario el equipo de cómputo con este sistema operativo afrontara mayores riesgos de virus, malwares y ranzomware entre otros. (MICROSOFT, 2020).

- ***Grupos Relevantes***: se tomaron los grupos relevantes y no se encontraron anomalías.

- ***Grupos Miembro***: la información encontrada presenta anomalías con el grupo administrador ya que todos los usuarios no deberían ser parte del grupo mismo. El grupo NONE, no se conoce el motivo de su presencia, del cual también son miembros todos los usuarios.

- ***Derechos de Usuarios***: los derechos de usuario no están configurados, lo cual genera una brecha de seguridad.

- ***Usuarios Relevantes***: los usuarios relevantes seleccionados no presentan anomalías.

- ***Aplicaciones instaladas Relevantes***: las aplicaciones relevantes seleccionadas no presentan anomalías.

- ***Dispositivos de Red***: los dispositivos de red no presentan anomalías.

- ***Puertos de comunicación***: los puertos de comunicación seleccionados no presentan anomalías.

- ***Puertos Abiertos Relevantes***: muestra la comunicación con el protocolo ModBus TCP en el puerto TCP: 1:59568.

- ***Tabla de Ruteo***: la tabla de ruteo hallada no presenta anomalías.

- ***Configuración de Seguridad***: muestra que las actualizaciones automáticas del sistema operativo están habilitadas, pero no está configurada y como se mencionó anteriormente este servicio ya no se encuentra disponible por parte del fabricante.

Resultado Análisis de la Red y Tráfico de Red

Se pudo verificar que la configuración del PLC es correcta como así también la comunicación entre el equipo de cómputo y el PLC.

Para el caso del tráfico de red se verificó que existe comunicación recíproca entre el equipo de cómputo y el PLC, en el mismo proceso se visualizaron las direcciones IP de ambos dispositivos.

Para el caso de la captura de paquetes de datos se verificó que es posible la captura de paquetes de datos durante la comunicación entre ambos dispositivos. Para verificar los modos de visualización de los paquetes de datos capturados, se realizó captura de paquetes en sus 3 (tres) modos, tal como se demostró en punto 3.4.2.

También se puede verificar captura de datos cuando el PLC está en pleno funcionamiento.

Para este trabajo, está fuera de alcance el análisis del contenido del paquete de datos.

Resultado Log de Actividades del PLC

Para este caso de estudio no se encontraron vulnerabilidades en los eventos satisfactorios y no satisfactorios ocurridos en el PLC.

Lo que se puede verificar o queda evidenciado son todas las actividades que se registran en el software Intouch Wonderware.

Capítulo IV - Análisis de los Resultados

"Si el enemigo está seguro en todos los puntos, prepárate para su ataque. Si tiene una fuerza superior, evítalo."
(Sun Tzu, *El arte de la guerra*, Siglo V a.c)

4.1. Resumen del Análisis

Se realiza una breve descripción de las limitaciones existentes en el capítulo 3 y del desarrollo técnico.

De acuerdo con la información relevada en el punto 3.4, se realiza el análisis correspondiente a los resultados obtenidos.

4.2. Limitaciones del análisis forense y desarrollo técnico

De acuerdo con lo expuesto en el punto 3.1.3, se verificó que la brecha de seguridad existe debido a las limitaciones antes descriptas en el punto 3.1.

De acuerdo con los resultados obtenidos en el punto 3.2.4, se verificó que la brecha de seguridad existe debido a lo obsoleto del sistema operativo del equipo de cómputo, la negación al cambio por parte de la organización, los tiempos exhaustivos de producción, falta de concientización en actualización de tecnologías, entre otras, a eso, agregarle la captura de los paquetes de datos en el trágico de red.

4.3. Importancia de los resultados

De acuerdo con los resultados obtenidos en los puntos 4.1 y 4.2 se verifica que, ante las brechas de seguridad planteadas en la hipótesis en el punto 1.2 y detectadas en el desarrollo técnico ponen en riesgo los activos de la organización. Estos riesgos pueden ocasionar pérdidas importantes afectando la economía y la reputación de organización entre otras.

4.4. Metodología de Trabajo

De acuerdo con los resultados obtenidos en el punto 4.3, se logró generar una metodología de trabajo basado en estándares y buenas prácticas, lo cual achica en gran medida la amplia brecha de seguridad detectada en el desarrollo técnico.

Para más especificidad, la metodología de trabajo generada hace foco en los puntos mencionados en el desarrollo técnico.

Para este trabajo se desarrollaron 2 (dos) metodologías, una para el sistema operativo Windows 7 y otra para la versión más reciente del sistema operativo Windows 10.

Ambas metodologías están, como ya se mencionó antes, en estándares y buenas prácticas mencionadas en el capítulo 2.

Como conclusión de la metodología de trabajo se desarrollaron controles de seguridad, siempre haciendo foco en los puntos mencionados en el desarrollo técnico. Cabe aclarar el alcance, ya que es muy amplia la variedad de controles aplicables de acuerdos a los últimos estándares y buenas prácticas de seguridad.

4.4.1. Windows 7

Esta versión de metodología de trabajo para Windows 7 es lo que se pudo obtener, ya que el sistema operativo no cuenta con soporte por parte del fabricante. Esta metodología creada no es una buena práctica de seguridad por los motivos antes mencionado. Esta metodología es recomendada ante las limitaciones mencionadas en el punto 3.

Items	*Valores*
Políticas de cuenta	*Política de contraseña*
	Política de bloqueo de cuenta
Políticas locales	*Política de auditoría*
	Asignación de derechos de usuario
	Opciones de seguridad
Registro de eventos	
Grupos restringidos	
Servicios del sistema	
Registro	
Sistema de archivos	
Políticas de red cableada (IEEE 802.3)	
Firewall de Windows con seguridad avanzada	*Perfil de dominio*
	Perfil privado
	Perfil público
Políticas de Network List Manager	

Items	Valores
Políticas de red inalámbrica (IEEE 802.11)	
Políticas de clave pública	
Políticas de restricción de software	
Configuración de cliente NAP de Protección de acceso a redes	
Políticas de control de aplicaciones	
Políticas de seguridad IP	
Configuración avanzada de la política de auditoría	*Inicio de sesión de cuenta*
	Gestión de cuentas
	Seguimiento detallado
	Acceso DS
	Inicio / cierre de sesión
	Acceso a objetos
	Cambio de política
	Uso de privilegios
	Sistema
Plantillas administrativas (computadora)	*Panel de control*
	VUELTAS
	Guía de seguridad de MS
	MSS (Legado)
	Red
	Impresoras
	Menú de inicio y barra de tareas
	Sistema
	Componentes de Windows
Plantillas administrativas (usuario)	*Panel de control*
	Escritorio
	Red
	Carpetas compartidas
	Menú de inicio y barra de tareas
	Sistema
	Componentes de Windows

Tabla 40 - Metodología de Trabajo Windows 7

4.4.2. Windows 10

Esta versión de metodología de trabajo para Windows 10 es lo que se pudo obtener. Esta versión del sistema operativo es la más reciente y actualizada cuenta con soporte por parte del fabricante. Esta metodología creada es una buena práctica recomendada para establecer una configuración segura.

Items	Valores
Políticas de cuenta	*Política de contraseña*
	Política de bloqueo de cuenta

Items	*Valores*
Políticas locales	*Política de auditoría*
	Asignación de derechos de usuario
	Opciones de seguridad
Registro de eventos	
Grupos restringidos	
Servicios del sistema	
Registro	
Sistema de archivos	
Políticas de red cableada (IEEE 802.3)	
Firewall de Windows con seguridad avanzada	*Perfil de dominio*
	Perfil privado
	Perfil público
Políticas de Network List Manager	
Políticas de red inalámbrica (IEEE 802.11)	
Políticas de clave pública	
Políticas de restricción de software	
Configuración de cliente NAP de Protección de acceso a redes	
Políticas de control de aplicaciones	
Políticas de seguridad IP	
Configuración avanzada de la política de auditoría	*Inicio de sesión de cuenta*
	Gestión de cuentas
	Seguimiento detallado
	Acceso DS
	Inicio / cierre de sesión
	Acceso a objetos
	Cambio de política
	Uso de privilegios
	Sistema
Plantillas administrativas (computadora)	*Panel de control*
	Personalización
	Opciones regionales y de idioma
	VUELTAS
	Guía de seguridad de MS
	MSS (Legado)
	Red
	Impresoras
	Menú de inicio y barra de tareas
	Sistema
	Componentes de Windows
Plantillas administrativas (usuario)	*Panel de control*
	Escritorio
	Red

Items	*Valores*
	Carpetas compartidas
	Menú de inicio y barra de tareas
	Sistema
	Componentes de Windows

Tabla 41 – Metodología de Trabajo Windows 10

4.4.3. Controles de Seguridad

Con la metodología de trabajo creada se crearon controles de seguridad que son más extensibles al sistema operativo, información y redes, involucrando temas como: vulnerabilidades, antivirus, entre otros.

Para este trabajo, dentro del alcance, se consideraron como controles de seguridad los siguientes ítems:

- Gestión continua de vulnerabilidades
- Uso controlado de privilegios administrativos
- Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores
- Mantenimiento, monitoreo y análisis de logs de auditoría
- Defensa contra malware
- Limitación y control de puertos de red, protocolos y servicios
- Control de acceso basado en la necesidad de conocer
- Monitoreo y control de cuentas
- Implementar un programa de concienciación y entrenamiento de seguridad

4.4.4. Desarrollo de los Controles de Seguridad

Con los controles ya establecidos en el punto 4.5.3 se procedió a su desarrollo, indicando para cada control su tipo de acción en seguridad, procedimiento y descripción de cada procedimiento. Se estableció crear una tabla explicativa para cada control por separado. Cabe aclarar que los controles establecidos son a modo académico, pero no se descarta la posibilidad de su implementación real en una organización.

Control A: Gestión continua de vulnerabilidades

Descripción Control A: Adquirir, evaluar y tomar medidas de manera continua sobre la nueva información para identificar vulnerabilidades, remediar y minimizar ventanas de oportunidad para los atacantes.

Los detalles del ***Control A***, son:

Sub-control	*Acción*	*Procedimiento*	*Descripción*
A.1	*Detección*	*Ejecución de herramientas de escaneo automatizados de vulnerabilidades*	*Utilice una herramienta actualizada de escaneo de vulnerabilidades compatible con para escanear automáticamente todos los sistemas en la red de forma semanal o más frecuente para identificar todas las vulnerabilidades potenciales en los sistemas de la organización.*
A.2	*Detección*	*Realizar análisis de vulnerabilidades autenticados*	*Realice escaneos de vulnerabilidades autenticados con agentes que se ejecutan localmente en cada sistema o con escáneres remotos que están configurados con derechos elevados en el sistema que se audita.*
A.3	*Protección*	*Proteger las cuentas dedicadas a auditorías*	*Utilice una cuenta dedicada al escaneo de vulnerabilidades autenticado, la cual no debe ser utilizada para otras tareas administrativas y que debe ser vinculada a máquinas específicas en direcciones IPs específicas.*
A.4	*Protección*	*Implementar herramientas de gestión automatizada de parches del sistema operativo*	*Implemente herramientas de actualización de software automatizadas para garantizar que los sistemas operativos cuenten con las actualizaciones de seguridad más recientes provistas por el proveedor del software.*
A.5	*Protección*	*Implementar herramientas de gestión automatizada de parches de software*	*Implemente herramientas de actualización de software automatizadas para garantizar que el software de terceros en todos los sistemas cuente con las actualizaciones de seguridad más recientes provistas por el proveedor del software*
A.6	*Respuesta*	*Comparar escaneos de vulnerabilidades consecutivos*	*Compare regularmente los resultados de escaneos de vulnerabilidades consecutivos para verificar que las vulnerabilidades se hayan remediado de manera oportuna.*
A.7	*Respuesta*	*Utilizar un proceso de calificación de riesgo*	*Utilice un proceso de calificación de riesgo para priorizar la corrección de vulnerabilidades descubiertas.*

Tabla 42 - Control A: Gestión continua de vulnerabilidades

Control B: Uso controlado de privilegios administrativos

Descripción Control B: Los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.

Los detalles del ***Control B***, son:

Sub-control	***Acción***	***Procedimiento***	***Descripción***
B.1	*Detección*	*Mantener un inventario de cuentas administrativas*	*Use herramientas automatizadas para inventariar todas las cuentas administrativas, incluidas las cuentas de dominio y locales, para garantizar que solo las personas autorizadas tengan privilegios elevados*
B.2	*Protección*	*Cambiar contraseñas por defecto*	*Antes de implementar cualquier activo nuevo, cambie todas las contraseñas por defecto para que tengan valores consistentes con las cuentas de nivel administrativo.*
B.3	*Protección*	*Asegurar el uso de cuentas administrativas dedicadas*	*Asegúrese de que todos los usuarios con acceso a la cuenta administrativa utilicen una cuenta dedicada o secundaria para actividades elevadas. Esta cuenta solo se debe usar para actividades administrativas y no para la navegación por Internet, correo electrónico o actividades similares.*
B.4	*Protección*	*Usar contraseñas únicas*	*Cuando no está soportada la autenticación multifactor (como el administrador local, root o cuentas de servicio), las cuentas usarán contraseñas que son únicas de ese sistema.*
B.5	*Protección*	*Usar autenticación multifactor para todo acceso administrativo*	*Utilice autenticación de multifactor y canales encriptados para todos los accesos de cuentas administrativas*
B.6	*Protección*	*Usar máquinas dedicadas para toda tarea administrativa*	*Asegúrese de que los administradores utilicen una máquina dedicada para todas las tareas administrativas o tareas que requieren acceso administrativo. Esta máquina debe estar en un segmento de red diferente al principal de la organización y no se le permitirá el acceso a Internet. Esta máquina no se usará para leer correos electrónicos, manipular documentos o navegar en Internet.*

Sub-control	Acción	Procedimiento	Descripción
B.7	Protección	Limitar el acceso a herramientas de scripts	Limite el acceso a las herramientas de scripting (como Microsoft PowerShell y Python) solo a usuarios administrativos o de desarrollo que necesiten acceder a esas funcionalidades.
B.8	Detección	Registrar y alertar cambios de miembros en grupos administrativos	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos.
B.9	Detección	Registrar y alertar los inicios de sesión fallidos a cuentas administrativas	Configure los sistemas para generar una entrada de registro y una alerta de inicios de sesión fallidos en una cuenta administrativa.

Tabla 43 - Control B: Uso controlado de privilegios administrativos

Control C: Configuración segura de hardware y software en dispositivos: móviles, portátiles, equipos de cómputo y servidores

Descripción Control C: Establecer, implementar y gestionar activamente (rastrear, informar, corregir) la configuración de seguridad de dispositivos: móviles, portátiles, equipos de cómputo y servidores para utilizar una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.

Los detalles del ***Control C***, son:

Sub-control	Acción	Procedimiento	Descripción
C.1	Protección	Establecer Configuraciones seguras	Mantenga estándares de configuración de seguridad estándar documentados para todos los sistemas operativos y software autorizados.
C.2	Protección	Mantener imágenes seguras	Mantenga imágenes o plantillas seguras para todos los sistemas de la organización según los estándares de configuración aprobados por la organización. Cualquier implementación de sistema nuevo o sistema existente que se vea comprometido se debe volver a reconstruido con una de esas imágenes o plantillas.
C.3	Protección	Almacenar las imágenes maestras de forma segura	Almacene las imágenes maestras y las plantillas en servidores configurados de forma segura, validados con herramientas de monitoreo de

Sub-control	Acción	Procedimiento	Descripción
			integridad, para garantizar que solo sean posibles los cambios autorizados en las imágenes.
C.4	*Protección*	*Implementar herramientas de gestión de configuración de sistema*	*Implemente las herramientas de gestión de configuración de sistema que automáticamente fuercen y vuelvan a implementar los parámetros de configuración en los sistemas a intervalos regulares programados.*
C.5	*Detección*	*Implementar sistemas de Monitoreo automatizado de configuración*	*Utilice un sistema de monitoreo de configuración compatible con el Protocolo de automatización de contenido de seguridad para verificar todos los elementos de configuración de seguridad, excepciones aprobadas por catálogo y que alerte cuando ocurran cambios no autorizados.*

Tabla 44 - Control C: Configuración segura de hardware y software

Control D: Mantenimiento, monitoreo y análisis de logs de auditoría

Descripción Control D: Reunir, administrar y analizar registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque.

Los detalles del ***Control D***, son:

Sub-control	Acción	Procedimiento	Descripción
D.1	*Detección*	*Utilizar tres fuentes de tiempo sincronizadas*	*Use al menos tres fuentes de tiempo sincronizadas de las cuales todos los servidores y dispositivos de red recuperan información de tiempo regularmente para que las marcas de tiempo en los registros sean consistentes*
D.2	*Detección*	*Activar registros de auditoría*	*Asegure que los registros locales se han activado en todos los sistemas y equipos de red.*
D.3	*Detección*	*Habilitar registros detallados*	*Habilite el registro del sistema para incluir información detallada, como origen de evento, fecha, usuario, marca de tiempo, direcciones de origen, direcciones de destino y otros elementos útiles.*
D.4	*Detección*	*Asegurar almacenamiento adecuado para registros*	*Asegúrese de que todos los sistemas que almacenan registros tengan el espacio de almacenamiento adecuado para los registros generados.*
D.5	*Detección*	*Gestión centralizada de registros*	*Asegúrese de que los registros apropiados se agreguen a un sistema*

Sub-control	Acción	Procedimiento	Descripción
			central de gestión de registros para su análisis y revisión
D.6	*Detección*	*Desplegar herramientas SIEM o de Análisis de registros*	*Implemente un sistema de Gestión de información de seguridad y eventos (Security Information and Event Management - SIEM) o una herramienta de análisis de registros para la correlación y el análisis de los registros.*
D.7	*Detección*	*Revisar regularmente los registros*	*Regularmente, revise los registros para identificar anomalías o eventos anormales.*
D.8	*Detección*	*Ajustar regularmente el SIEM*	*Regularmente, ajuste el sistema SIEM para identificar mejor los eventos que requieren acción y disminuir el ruido.*

Tabla 45 - Control D: Mantenimiento, monitoreo y análisis de logs de auditoría

Control E: Defensa contra malware

Descripción Control E: Controlar la instalación, propagación y ejecución de código malicioso en múltiples puntos de la organización, al mismo tiempo que optimizar el uso de automatización para permitir la actualización rápida de la defensa, la recopilación de datos y la acción correctiva.

Los detalles del ***Control E***, son:

Sub-control	Acción	Procedimiento	Descripción
E.1	*Protección*	*Utilizar software antimalware de gestión centralizada*	*Utilice software antimalware gestionado centralmente para monitorear y defender continuamente cada una de las estaciones de trabajo y servidores de la organización*
E.2	*Protección*	*Asegurar que el software antimalware y las firmas estén actualizadas*	*Asegúrese de que el software antimalware de la organización actualice su motor de exploración y la base de datos de firmas periódicamente.*
E.3	*Protección*	*Habilitar características antiexplotación de sistemas operativos/implementar tecnologías antiexplotación*	*Habilite las características anti-explotación como la Prevención de ejecución de datos (Data Execution Prevention - DEP) o Address Space Layout Randomization (ASLR) que están disponibles en los sistemas operativos o implemente los kits de herramientas adecuados que pueden configurarse para aplicar protección a un conjunto más*

Sub-control	Acción	Procedimiento	Descripción
			amplio de aplicaciones y ejecutables.
E.4	*Detección*	*Configurar escaneo anti-malware de dispositivos removibles*	*Configure los dispositivos para que automáticamente realicen un análisis anti-malware de los medios extraíbles cuando se inserten o se conecten.*
E.5	*Protección*	*Configurar equipos para no auto-ejecutar contenido*	*Configure los equipos para no ejecutar automáticamente el contenido de medios extraíbles*
E.6	*Detección*	*Centralizar los registros antimalware*	*Envíe todos los eventos de detección de malware a las herramientas de administración antimalware de la organización y a los servidores de registro de eventos para análisis y alertas.*
E.7	*Detección*	*Habilitar registros de consultas DNS*	*Habilitar los registros de las consultas al sistema de nombre de dominio (Domain Name System - DNS) para detectar búsquedas de nombres de host para dominios maliciosos conocidos.*
E.8	*Detección*	*Habilitar registros de auditoría de línea de comandos*	*Habilite el registro de auditoría de línea de comandos para shells de comandos, como Microsoft Powershell y Bash.*

Tabla 46 - Control E: Defensa contra malware

Control F: Limitación y control de puertos de red, protocolos y servicios

Descripción Control F: Administrar (rastrear/controlar/corregir) el uso operacional continuo de puertos, protocolos y servicios en dispositivos en red para minimizar las ventanas de vulnerabilidad disponibles para los atacantes.

Los detalles del ***Control F***, son:

Sub-control	Acción	Procedimiento	Descripción
F.1	*Identificación*	*Asociar puertos, servicios y protocolos activos al inventario de activos*	*Asocie puertos, servicios y protocolos activos a los activos de hardware en el inventario de activos.*
F.2	*Protección*	*Asegurar que solo puertos, protocolos y*	*Asegúrese de que en cada sistema se ejecuten solo los puertos de red, los protocolos y los servicios que se requieran con fines de negocio validados.*

Sub-control	Acción	Procedimiento	Descripción
		servicios aprobados se están ejecutando	
F.3	*Detección*	*Realizar regularmente escaneos automatizados de puertos*	*Realice escaneos automáticos de puertos de forma regular contra todos los sistemas y advierta si se detectan puertos no autorizados en un sistema.*
F.4	*Protección*	*Aplicar firewalls basados en host o filtrado de puertos*	*Aplique firewalls basados en host o herramientas de filtrado de puertos en los sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico, excepto los servicios y puertos que están explícitamente permitidos.*
F.5	*Protección*	*Implementar firewalls de aplicación*	*Coloque firewalls de aplicaciones frente a servidores críticos para verificar y validar el tráfico que va al servidor. Cualquier tráfico no autorizado debe ser bloqueado y registrado.*

Tabla 47 - Control F: Limitación y control de puertos de red, protocolos y servicios

Control G: Control de acceso basado en la necesidad de conocer protección de datos

Descripción Control G: Los procesos y herramientas utilizados para rastrear/controlar/prevenir/corregir el acceso seguro a activos críticos (por ejemplo, información, recursos, sistemas) de acuerdo con la determinación formal de qué personas, computadoras y aplicaciones tienen una necesidad y derecho a acceder a estos activos críticos basado en una clasificación aprobada.

Los detalles del ***Control G***, son:

Sub-control	Acción	Procedimiento	Descripción
G.1	*Protección*	*Segmentar la red basado en sensibilidad*	*Segmente la red según la etiqueta o el nivel de clasificación de la información almacenada en los servidores; ubique toda la información confidencial en redes de área local virtual (VLAN) separadas*
G.2	*Protección*	*Habilitar filtrado de firewall entre VLANs*	*Habilite el filtrado de firewall entre las VLAN para garantizar que solo los sistemas autorizados puedan comunicarse con otros sistemas necesarios para cumplir con sus responsabilidades específicas.*

Sub-control	Acción	Procedimiento	Descripción
G.3	Protección	Deshabilitar comunicaciones entre estaciones de trabajo	Inhabilite todas las comunicaciones de estación de trabajo a estación de trabajo para limitar la capacidad de un atacante de moverse lateralmente y poner en peligro los sistemas vecinos, a través de tecnologías como VLAN privadas o microsegmentación.
G.4	Protección	Cifrar toda la información sensible en tránsito	Cifre toda la información confidencial en tránsito.
G.5	Detección	Utilizar una herramienta de Descubrimiento activo para identificar datos sensibles	Utilice una herramienta de descubrimiento activo para identificar toda la información sensible almacenada, procesada o transmitida por los sistemas de tecnología de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remoto, y actualice el inventario de información sensible de la organización
G.6	Protección	Proteger la información mediante lista de control de acceso	Proteja toda la información almacenada en sistemas con listas de control de acceso específicas para sistema de archivos, uso compartido de redes, aplicaciones o bases de datos. Estos controles harán cumplir el principio de que solo las personas autorizadas deberían tener acceso a la información en función de su necesidad de acceder a la información como parte de sus responsabilidades.
G.7	Protección	Aplicar control de acceso a datos mediante herramientas automatizadas	Utilice una herramienta automatizada, como la prevención de pérdida de datos (Data Loss Prevention - DLP) basada en host, para hacer cumplir los controles de acceso a los datos, incluso cuando los datos se copian de un sistema.
G.8	Protección	Cifrar información sensible en reposo	Cifre toda la información sensible en reposo utilizando una herramienta que requiere un mecanismo de autenticación secundario no integrado en el sistema operativo, para poder acceder a la información.
G.9	Detección	Imponer el registro detallado para acceso o cambios en datos sensibles	Imponga el registro de auditoría detallado para acceder o realizar cambios en datos sensibles (utilizando herramientas como Monitoreo de Integridad de Archivos o sistemas SIEM).

Tabla 48 - Control G: Control de acceso basado en la necesidad de conocer protección de datos

Control H: Monitoreo y control de cuentas

Descripción Control H: Gestione activamente el ciclo de vida de las cuentas del sistema y de aplicaciones (su creación, uso, latencia, eliminación) con el fin de minimizar las oportunidades para que los atacantes las aprovechen.

Los detalles del ***Control H***, son:

Sub-control	***Acción***	***Procedimiento***	***Descripción***
H.1	*Identificación*	*Mantener un inventario de sistemas de autenticación*	*Mantenga un inventario de cada uno de los sistemas de autenticación de la organización, incluidos los ubicados en el sitio o en un proveedor de servicios remoto*
H.2	*Protección*	*Configurar un punto de autenticación centralizado*	*Configure el acceso para todas las cuentas a través de la menor cantidad posible de puntos de autenticación centralizados, incluidos los sistemas de red, de seguridad y en la nube.*
H.3	*Protección*	*Requerir Autenticación Multifactor*	*Requiera autenticación de múltiples factores para todas las cuentas de usuario, en todos los sistemas, ya sea que se administren localmente en la organización o por un proveedor de terceros.*
H.4	*Protección*	*Cifrar o hashear todas las credenciales de autenticación*	*Utilice técnicas de cifrado o hash combinado con salt con todas las credenciales de autenticación cuando se almacenan.*
H.5	*Protección*	*Cifrar la transmisión de nombres de usuario y credenciales de autenticación*	*Asegúrese de que todos los nombres de usuario y las credenciales de autenticación de la cuenta se transmitan a través de redes que utilizan canales cifrados*
H.6	*Identificación*	*Mantener un inventario de cuentas*	*Mantenga un inventario de todas las cuentas organizadas por sistema de autenticación.*
H.7	*Protección*	*Establecer un proceso para revocar el acceso*	*Establezca y siga un proceso automatizado para revocar el acceso a sistemas mediante la desactivación de cuentas inmediatamente después de la terminación o el cambio de responsabilidades de un empleado o contratista. Desactivar estas cuentas, en lugar de eliminar cuentas, permite preservar los registros de auditoría.*
H.8	*Respuesta*	*Deshabilitar cualquier cuenta no asociada*	*Deshabilite cualquier cuenta que no pueda asociarse con un proceso de negocio o un propietario de la organización.*

Sub-control	Acción	Procedimiento	Descripción
H.9	Respuesta	Desactivar cuentas inactivas	Deshabilite automáticamente las cuentas inactivas después de un período de inactividad establecido.
H.10	Protección	Asegurar que todas las cuentas tengan fecha de caducidad	Asegúrese de que todas las cuentas tengan una fecha de vencimiento monitoreada y forzada.
H.11	Protección	Bloquear sesiones de estaciones de trabajo tras inactividad	Bloquee automáticamente las sesiones de la estación de trabajo después de un período estándar de inactividad.
H.12	Detección	Monitorear los intentos de acceso a cuentas desactivadas	Monitoree los intentos de acceso a cuentas desactivadas a través de los registros de auditoria.
H.13	Detección	Alertar sobre desviación de comportamiento de inicio de sesión de cuentas	Alerte cuando los usuarios se desvían del comportamiento normal de inicio de sesión, como la hora y/o el día, la ubicación de la estación de trabajo y la duración.

Tabla 49 - Control H: Monitoreo y control de cuentas

Control I: Implementar un programa de concienciación y entrenamiento de seguridad

Descripción Control I: Para todos los roles funcionales en la organización (priorizando aquellos que son misionales para la organización y su seguridad), identificar los conocimientos, habilidades y capacidades específicos necesarios para soportar la defensa de la empresa; desarrollar y ejecutar un plan integral para evaluar, identificar brechas y remediar a través de políticas, planificación organizacional, capacitación y programas de concienciación.

Los detalles del ***Control I***, son:

Sub-control	Acción	Procedimiento	Descripción
I.1	N/A	Realizar un análisis de brecha de habilidades	Lleve a cabo un análisis de la brecha de habilidades para comprender las habilidades y los comportamientos a los que los miembros de la fuerza de trabajo no se están adhiriendo, usando esta información para construir una hoja de ruta base de educación
I.2	N/A	Realizar capacitación para	Realice capacitaciones para abordar el vacío de habilidades identificado para

Sub-control	Acción	Procedimiento	Descripción
		llenar la brecha de habilidades	*impactar positivamente el comportamiento de seguridad de los miembros de la fuerza laboral.*
I.3	*N/A*	*Implementar un programa de concienciación de seguridad*	*Cree un programa de concientización de seguridad para que todos los miembros de la fuerza laboral lo completen regularmente para asegurarse de que entienden y exhiben los comportamientos y las habilidades necesarias para ayudar a garantizar la seguridad de la organización. El programa de concientización de seguridad de la organización debe comunicarse de manera continua y atractiva.*
I.4	*N/A*	*Actualice el contenido de concienciación con frecuencia*	*Asegúrese de que el programa de concientización de seguridad de la organización se actualice con frecuencia (al menos una vez al año) para abordar nuevas tecnologías, amenazas, estándares y requisitos de negocio.*
I.5	*N/A*	*Entrenar a la fuerza laboral en la autenticación segura*	*Capacite a los miembros de la fuerza de trabajo sobre la importancia de habilitar y utilizar la autenticación segura*
I.6	*N/A*	*Capacitar a la fuerza laboral en la identificación de ataques de ingeniería social*	*Capacite a los empleados sobre cómo identificar diferentes formas de ataques de ingeniería social, como phishing, fraudes telefónicos y llamadas de suplantación.*
I.7	*N/A*	*Capacitar a la fuerza laboral en manejo de datos sensibles*	*Capacite a los empleados sobre cómo identificar y almacenar, transferir, archivar y destruir información confidencial de manera adecuada.*
I.8	*N/A*	*Capacitar a la fuerza laboral sobre las causas de la exposición involuntaria a los datos*	*Capacite a los miembros de la fuerza de trabajo para que conozcan las causas de las exposiciones involuntarias de datos, cómo perder sus dispositivos móviles o enviar correos electrónicos a la persona equivocada debido al autocompletado en el correo electrónico.*
I.9	*N/A*	*Capacite a la fuerza laboral sobre cómo identificar y reportar incidentes*	*Capacitar a los empleados para que puedan identificar los indicadores más comunes de un incidente y poder informar tal incidente.*

Tabla 50 - Control I: Implementar un programa de concienciación y entrenamiento de seguridad

Capítulo V - Conclusiones y Sugerencias

"Estrategia sin táctica es el más lento camino hacia la victoria. Las tácticas sin estrategia son el ruido antes de la derrota."
(Sun Tzu, *El arte de la guerra*, Siglo V a.c)

5.1. Conclusiones

En esta investigación se generó una metodología de trabajo, por medio de la cual, se mostró la minimización de las brechas de seguridad de la información, aplicando políticas de seguridad, normas o estándares de seguridad en las redes industriales críticas.

En este trabajo se detectaron brechas de seguridad en el sistema operativo y en la comunicación con PLC, para ello se utilizaron herramientas forenses. Se analizaron las vulnerabilidades detectadas.

Como parte de la metodología de trabajo antes mencionada, se generó una lista de verificaciones con parámetros de seguridad del sistema operativos utilizado para este trabajo Final y otra lista de verificaciones para un sistema operativo actual.

Para concluir y ser más específico en lo que a seguridad se refiere, se generó una lista de controles de seguridad, en ella se utilizaron normas, estándares y buenas prácticas de seguridad de la información.

5.2. Sugerencias

A la Alta Dirección de la organización se le recomienda alinear la política de negocio en conjunto con el departamento de Tecnología a fin poder implementar esta metodología de trabajo y los controles de seguridad (como así también su mantenimiento y actualización), incitar a la concientización del personal en temas de seguridad de la información para así minimizar riesgos y/o amenazas de los atacantes, como así también contar con un plan de mitigaciones luego del tratamiento y análisis de los incidentes de seguridad ocurridos.

Realizar mantenimiento y actualización de las normas y estándares relacionados con la seguridad de la información y con la seguridad de las redes industriales críticas.

En este trabajo estos controles no fueron ejecutados, pero se pretende generar reportes, monitorear riesgos y un tratamiento eficiente de los incidentes de seguridad.

Elaboración del Informe Final

"Un territorio de igual acceso para ti y para los demás se llama terreno de comunicaciones."
(Sun Tzu, *El arte de la guerra*, Siglo V a.c)

Un sistema SCADA es la herramienta idónea a la hora de supervisar, controlar y administrar sistemas complejos en una industria, dada su gran versatilidad, nos permite implementar (implantar) nuevas áreas de trabajo sin la necesidad de reestructurar todas nuestras instalaciones.

La industria requiere sistemas complejos de fácil acceso y que se lleven la mayor parte del trabajo, realizando análisis, creando registros históricos, permitiendo la automatización y el control de manera sencilla, además del monitoreo remoto de los procesos, que permite a los accionistas y gerentes obtener información relevante del funcionamiento de sus activos.

De los objetivos planteados (Cap. 1.4) y de los resultados obtenidos en el desarrollo técnico se verifica que los resultados fueron los esperados (las brechas de seguridad fueron detectadas). Con la implementación de las buenas prácticas, normas y estándares de cumplimiento, tanto a nivel seguridad como en redes, las brechas de seguridad detectadas disminuirán.

Cabe aclarar que, en el ámbito de seguridad, en las organizaciones el objetivo siempre será disminuir los riesgos o brechas de seguridad o contar con un plan de mitigaciones de estos.

Líneas Futuras de Investigación

Se continuará esa línea de trabajo en el marco del Proyecto titulado “Desarrollo de una Guía para el abordaje de Incidentes de Ciberseguridad en Infraestructuras Criticas Industriales”, presentando para su inclusión en el Banco Nacional de Proyectos de Desarrollo Tecnológico Social, del Ministerio de Ciencia, Tecnología e Innovación de la Nación.

Dicho proyecto se presentó conjuntamente entre las Universidades: Fasta, UAI y Universidad de la Defensa y tiene una duración de 2 (dos) años.

Para este mismo proyecto, en otra etapa se estudiarán con más detalle las topologías y dispositivos de red adecuadas, análisis de bases de datos y licenciamiento de software entre otros.

Anexo I - Software

1. Instalación del Sistema Operativo

2 Instalacion Sistema Operativo.pc

2. Instalación de Wonderware

3 Instalacion Wonderware.pdf

3. Información obtenida con WinAudit

WinAudit_InfoReport_02_08_2020 16_20_

Anexo II - PLC

1. Armado del tablero PLC

1 ICS portable -
Guia para construccic

2. Código del PLC en Lenguaje Ladder

Manual_con_ladder.
ok.pdf

3. Simulación Industrial

Doc PDF.rar

Acrónimos

SCADA	***Supervisory Control And Data Acquisition***
PLC	***Programmable Logic Controllers***
RTU	***Remote Terminal Unit***
DCS	***Distributed Control Systems***
PI	***Platform Information***
WAN	***Wide Area Network***
HMI	***Human Machine Interface***
MTU	***Master Terminal Unit***
OSI	***Open Systems Interconnection***
TCP/IP	***Transport Control protocol / Internet Protocol***
MODBUS	***Industrial Communication Protocol***
CID	***Confidencialidad, Integridad y Disponibilidad***
CIA	***Confidentiality, Integrity and Availability***
NIST	***National Institute of Standard and Technology***
ISO 27000	***International Standard Organization 27000***
ISO 27001	***International Standard Organization 27001***
CSIRT	***Computer Security Incident Response Team***
MINSEG	***CSIRT Gubernamental de la República Argentina***
IT	***Information Technology***
ISO	***International Organization for Standardization***
SGSI	***Sistema de Gestión de Seguridad de la Información.***
ISMS	***Information Security Management System***
ISA-SP99	***International Society of Automation – SP99***
API-1164	***American Petroleum Institute - 1164***
AGA-12	***American Gas Association - 12***
IEC 62443	***International Electronic Commission 62443***
NISCC	***Northern Ireland Social Care Council***
RFC	***Request for Comment***
NERC	***North American Electric Reliability Corporation***
COBIT	***Control Objectives for Information and related Technology***

Referencias

27000:2018(E), I. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Recuperado de Information technology — Security techniques — Information security management systems — Overview and vocabulary: https://www.iso.org/obp/ui#iso:std:iso-iec:27000:ed-5:v1:en - 4.2.2 Information

27000:2018(E), I. (2018). *Information technology — Security techniques — Information security management systems — Overview and vocabulary.* Recuperado de Information technology — Security techniques — Information security management systems — Overview and vocabulary: https://www.iso.org/obp/ui#iso:std:iso-iec:27000:ed-5:v1:en - 4.2.3 Information Security

27037:2012, I. (October de 2012). *Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence*. Recuperado de Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence: https://www.iso.org/standard/44381.html - Reviewed 2018 - https://www.iso.org/obp/ui/#iso:std:iso-iec:27037:ed-1:v1:en

27042:2015, I. (Jun de 2015). *Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence*. Recuperado de Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence: https://www.iso.org/standard/44406.html - https://www.iso.org/obp/ui/#iso:std:iso-iec:27042:ed-1:v1:en

A. Jerman Blazic, S. S. (July de 2011). *RFC6283: Extensible Markup Language Evidence Record Syntax (XMLERS).* Recuperado de RFC6283: Extensible Markup Language Evidence Record Syntax (XMLERS): https://www.hjp.at/doc/rfc/rfc6283.html

AGA-12. (11-13 de March de 2015). Framework for implementation of AGA 12 for secured SCADA operation in Oil and Gas Industry. *2015 2nd International Conference on Computing for Sustainable Global Development* (págs. 1281-1284.). New Delhi, India: IEEE. Recuperado de Framework for implementation of AGA 12 for secured SCADA operation in Oil and Gas Industry: https://ieeexplore.ieee.org/document/7100456/authors#authors

Ahmed, I. &. (23 de January de 2012). *SCADA Systems: Challenges for Forensic Investigators.* Recuperado de SCADA Systems: Challenges for Forensic Investigators: https://www.researchgate.net/publication/234138890_SCADA_Systems_Challenges_for_Forensic_Investigators

Alcaraz, C. F. (2008). *Gestión segura de redes SCADA. Nuevas tendencias en gestión de redes.* Recuperado de Gestión segura de redes SCADA. Nuevas tendencias en gestión de redes: https://www.nics.uma.es/pub/papers/Alcaraz2008a.pdf

API 1164, A. P. (1 de June de 2009). *API STD 1164* . Recuperado de Pipeline SCADA Security: https://standards.globalspec.com/std/10047641/api-std-1164

AVEVA. (2021). *AVEVA.* Recuperado de Wonderware solutions are now AVEVA solutions: https://www.aveva.com/en/solutions/operations/wonderware/

Brezinski, D. &. (February de 2002). *RFC3227: Guidelines for Evidence Collection and Archiving.* Recuperado de RFC3227: Guidelines for Evidence Collection and Archiving.: https://dl.acm.org/doi/pdf/10.17487/RFC3227

C. Wallace, U. P. (March de 2007). *RFC4810: Long-Term Archive Service Requirements.* Recuperado de RFC4810: Long-Term Archive Service Requirements: https://www.hjp.at/doc/rfc/rfc4810.html

Carracedo, E. (12 de Dec de 2018). Implementacion SCADA - Proceso de Produccion . *Tecnicatura Superior en Automatizacion y Control* . Escobar , Buenos Aires, Argentina.

Chandia, R. G. (March de 2007). Security strategies for SCADA networks. *International Conference on Critical Infrastructure Protection* (págs. 117 - 131). Springer, Boston, MA.: DOI: 10.1007/978-0-387-75462-8_9 · Source: DBLP - 5.1 Role of Forensics. Obtenido de SECURITY STRATEGIES FOR SCADA NETWORKS.

Collard, G. D. (10-12 May 2017). A definition of information security classification in cybersecurity context. *In 2017 11th International Conference on Research Challenges in Information Science (RCIS)* (págs. pp. 77-82). Brighton, UK: IEEE.

CPCI. (23 de 08 de 2019). Perito Informático Forense. *ADQUISICIONES FORENSES Y EXTRACCIONES DE DATOS*. Buenos Aires, Buenos Aires, Argentina: CPCI .

DELTA. (30 de June de 2011). *DELTA PLC.* Recuperado de Manual de Operación DVP-ES2-EX2-SS2-SA2-SX2:

www.deltaww;com/filecenter/products/download/06/060301/Manual/DELTA_IA-PLC_DVP-ES2-EX2-SS2-SA2-SX2_PM_SP_20110630.pdf

Electric, S. (2021). *Schneider Electric*. Recuperado de Industrial Automation Software: https://www.se.com/ww/en/product-category/5100-industrial-automation-software/?filter=business-1-industrial-automation-and-control

Evans, R. P. (01 de September de 2005). *A Comparison of Cross-Sector Cyber Security Standards.* Recuperado de A Comparison of Cross-Sector Cyber Security Standards: https://www.osti.gov/biblio/911585 - https://inldigitallibrary.inl.gov/sites/sti/sti/3395027.pdf - 3. STANDARDS - 3.3 ISA SP99 – Manufacturing and

GmbH, T. I. (s.f.). *TUV NORTH GROUP*. Recuperado de Whitepaper Industrial Security based on IEC 62443: https://www.tuvit.de/fileadmin/Content/TUV_IT/pdf/Downloads/WhitePaper/whitepaper-iec-62443.pdf

ISA/IEC 62443, I. (Sep-Oct de 2018). *ISA/IEC 62443 standard specifies security capabilities for control system components*. Recuperado de ISA/IEC 62443 standard specifies security capabilities for control system components: https://www.isa.org/intech/201810standards/

ISA99. (s.f.). *ISA99, Industrial Automation and Control Systems Security*. Recuperado de ISA99, Industrial Automation and Control Systems Security: https://www.isa.org/isa99/

ISO/IEC 27035:2011, N. I. (September de 2011). *Information technology — Security techniques — Information security incident management.* Recuperado de Information technology — Security techniques — Information security incident management: https://www.iso.org/standard/44379.html

Johnson, A. D. (2011). *NIST special publication, 800(128).* Recuperado de Guide for security-focused configuration management of information systems: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf

Kalapatapu, R. (7 de October de 2004). *SCADA PROTOCOLS AND COMMUNICATION TRENDS.* Recuperado de Proc. 2004 ISA Industrial Network Security Symp. (ISA Expo 2004), Instrumentation, Systems and Automation Soc., 2004: http://www.isa.org/journals/intech/TP04ISA048.pdf - 1.0 INTRODUCTION

Kalapatapu, R. (7 de October de 2004). *SCADA PROTOCOLS AND COMMUNICATIONS TRENDS.* Recuperado de Proc. 2004 ISA Industrial

Network Security Symp. (ISA Expo 2004), Instrumentation, Systems and Automation Soc., 2004: http://www.isa.org/journals/intech/TP04ISA048.pdf - 2.0 PROTOCOLS

Kamlofsky, J. C. (November de 2015). Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas. *III Congreso Nacional de Ingeniería Informática/Sistemas de Información (CONAIISI 2015)* (pág. 1). Buenos Aires: ISSN. Recuperado de Un Enfoque para Disminuir los Efectos de los Ciber-ataques a las Infraestructuras Críticas: http://imgbiblio.vaneduc.edu.ar/fulltext/files/TC121046.pdf

LINUXCONFIG.ORG. (26 de 05 de 2020). *LINUXCONFIG.ORG.* Recuperado de How to set a root password on Ubuntu 18.04 Bionic Beaver Linux: https://linuxconfig.org/how-to-set-a-root-password-on-ubuntu-18-04-bionic-beaver-linux

McKemmish, R. (June de 1999). *AUSTRALIAN INSTITUTE OF CRIMINOLOGY TREND & ISSUES IN CRIME AND CRIMINAL JUSTICE N 118.* Recuperado de What is Forensic Computing: https://aic.gov.au/publications/tandi/tandi118

MICROSOFT. (14 de 01 de 2020). *MICROSOFT WINDOWS*. Recuperado de Support for Windows 7 has ended: https://www.microsoft.com/en-us/windows/windows-7-end-of-life-support-information

NISCC. (23 de February de 2005). *Good Practice Guide on Firewall Deployment for SCADA and Process Control Networks.* Recuperado de National Infrastructure Security Co-Ordination Centre: https://www.tofinosecurity.com/professional/good-practice-guide-firewall-deployment-scada-and-process-control-networks

NIST SP 800-128, S. P. (August de 2011). *Guide for Security-Focused Configuration Management of Information Systems.* Recuperado de Guide for Security-Focused Configuration Management of Information Systems: https://doi.org/10.6028/NIST.SP.800-128 - 2.1.2 THE CHALLENGE OF PROTECTING INFORMATION AND MANAGING RISK

NIST SP 800-82, N. S.-8. (June de 2011). *Guide to Industrial Control Systems (ICS) Security* . Recuperado de Guide to Industrial Control Systems (ICS) Security : https://dl.acm.org/doi/pdf/10.5555/2206293

OMRON. (16 de 09 de 2020). *OMRON*. Recuperado de Industrial Automation: https://www.myomron.com/index.php?action=kb&article=147

Presidencia de la Nacion, J. d. (2020). *Programa Nacional de Infraestructuras Críticas de Información y Ciberseguridad*. Recuperado de ICIC - CERT: http://www.icic.gob.ar/paginas.dhtml?pagina=100

Presidencia de la Nación, M. d. (2020). *MINSEG-CSIRT*. Recuperado de MINSEG-CSIRT: https://www.cybersecurityintelligence.com/minseg-csirt-4829.html

Ron Melton, T. F. (29 de October de 2004). *System Protection Profile--Industrial Control Systems Version 1.0.* doi:https://doi.org/10.6028/NIST.IR.7176

Shirey, R. (May de 2000). *RFC2828: Internet security glossary.* Recuperado de RFC2828: Internet security glossary.: https://dl.acm.org/doi/pdf/10.17487/RFC2828

Siemens. (2021). *Siemens Global.* Recuperado de Software for SIMATIC Controllers - The STEP 7 family: https://new.siemens.com/global/en/products/automation/systems/industrial/controller-sw.html

singh, R. (14 de 02 de 2020). *A quick Guide to Cyber Security.* Recuperado de Rakshanda singh: https://medium.com/@rakshandamitthu/a-quick-guide-to-cyber-security-8431336670b5

Standardization, I. -I. (2013). *ISO/IEC 27001:2013.* Recuperado de Information technology — Security techniques — Information security management systems — Requirements: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en - 0 Introduction - 0.1 General

Standardization, I. -I. (2018). *ISO/IEC 27000:2018.* Recuperado de Information technology — Security techniques — Information security management systems — Overview and vocabulary: https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-5:v1:en - Introduction - 0.1 Overview

Standardization, I. -I. (s.f.). *ISO - International Organization for Standardization*. Recuperado de STANDARDS: https://www.iso.org/standards.html

T. Gondrom, R. B. (August de 2007). *RFC4998: Evidence Record Syntax (ERS).* Recuperado de RFC4998: Evidence Record Syntax (ERS): https://www.hjp.at/doc/rfc/rfc4998.html