Universidad Nacional del Nordeste

Facultad de Ciencias Exactas y Naturales y Agrimensura

MAESTRÍA EN SISTEMAS Y REDES DE COMUNICACIONES

VULNERABILIDADES DE CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL Y ACCESIBILIDAD A TRAVÉS DE REDES PÚBLICAS

Maestrando: Ing. Oscar A. Cossio
Director: Mgtr. Ing. Oscar G. Lombardero

Este trabajo es dedicado con profundo amor a:

Aura,

Martina

y a mis padres

Con un agradecimiento muy grande a los docentes de la maestría por su apoyo constante, en especial al Ing. Guillermo Lombardero por su guía y consejo.

VULNERABILIDADES DE CIBERSEGURIDAD EN SISTEMAS DE CONTROL INDUSTRIAL Y ACCESIBILIDAD A TRAVÉS DE REDES PÚBLICAS

Índice

Resumen 1

1. Introducción 3

1.1 Generalidades de sistemas de control industriales 3

1.2 Generalidades de SCADA 7

1.3 DCS: Sistemas de control distribuido 11

1.4 Ciberseguridad para sistemas de control industriales 14

1.5 Elementos generales de ciberseguridad [10] 18

1.6 Servicios de seguridad 24

1.7 Mecanismos de seguridad 26

1.8 Aplicaciones de ciberseguridad a sistemas industriales 27

2. Objetivos 33

3. Materiales y métodos 33

3.1 Metodología general de tests de penetración 33

3.1.1 Parámetros de análisis 35

3.1.2 Reconocimiento de red 37

3.1.3 *Portscanning* 39

3.1.4 *Fingerprinting* de sistemas 41

3.1.5 Sondeo de servicios 41

3.1.6 Exploración automatizada de vulnerabilidades 42

3.1.7 Investigación de *exploits* 42

3.1.8 Exploración manual de vulnerabilidades y verificación de resultados automatizados 43

3.1.9 Exploración de aplicaciones 44

3.1.10 Sondeo de Firewall y Listas de control de acceso 45

3.1.11 Sistemas de detección de intrusión (IDS) 46

3.1.12 Verificación de sistemas confiables 47

3.1.13 Password cracking 48

3.1.14 Pruebas de denegación de servicio 49

3.1.15 Revisión de logs de IDS y servidores 50

3.2 Metodología de detección 50

3.2.1 Análisis de vulnerabilidades de dispositivos expuestos a Internet 52

3.2.2 Verificación con nmap 54

3.2.3 Herramientas alternativas 57

4 Resultados obtenidos 58

4.1 Resultados del análisis de vulnerabilidades 58

4.2 Resultados de investigación bibliográfica 73

4.3 Vulnerabilidades de ICS por año: 75

4.4 Clasificación de vulnerabilidades:..... 76

4.5 Vulnerabilidades en protocolos de comunicación industriales de alta relevancia 78

5 Discusión de resultados..... 78

6 Conclusiones..... 81

6.1 Propuestas de solución a las vulnerabilidades encontradas..... 82

6.2 Líneas futuras de investigación 86

7 Bibliografía..... 88

Índice de tablas

Tabla 1 - Queries de shodan para detección de sistemas industriales 54

Tabla 2 - Cantidad de objetivos detectados por tecnología 59

Tabla 3 - Datos de reconocimiento de red por tecnología 72

Tabla 4 - Posibles casos de sistemas industriales vulnerables a fallas conocidas de TLS/SSL 73

Índice de figuras

Figura 1 - Diagrama de bloques de ICS 4
Figura 2 - Layout general de un SCADA 9
Figura 3 - Implementación de una red SCADA 10
Figura 4 - Implementación de un sistema SCADA (control ferroviario) 11
Figura 5 - Implementación de sistema de control distribuido 14
Figura 6 - Diagrama de proceso de detección 51
Figura 7 - Casos principales detectados por tecnología 60
Figura 8 - Vulnerabilidades de ICS por año 75
Figura 9 - Vulnerabilidades de ICS por industria 76
Figura 10 - Vulnerabilidades de ICS por componente 77
Figura 11 - Vulnerabilidades de ICS por severidad 77

Abreviaturas

COTS: *Commercial off-the-shelf*

CVSS: Common Vulnerability Scoring System

DCS: Sistema de control distribuído

HMI: Interfaz hombre máquina

ICS: Sistema de control industrial

IDS: Sistema de detección de intrusiones

IED: Dispositivo electrónico inteligente

IP: Protocolo de interred

IT: Tecnologías de la información

LAN: Red de área local

MAN: Red de área metropolitana

MTU: Unidad terminal maestra

PBX: *Public branch exchange*

PKI: Infraestructura de clave pública

PLC: Controlador lógico programable

RTU: Unidad terminal remota

SCADA: Control supervisor y adquisición de datos

SSH: *Shell* segura

TCP: Protocolo de control de transmisión

UDP: Protocolo de datagrama de usuario

VPN: Red privada virtual

WAN: Red de área amplia

Resumen

El objetivo de este trabajo es obtener información sobre las características y la prevalencia de las principales vulnerabilidades de ciberseguridad en redes de control industrial, sistemas de control industrial, protocolos de comunicación de dispositivos de campo y SCADA.

Para esto inicialmente se realizó un relevamiento bibliográfico de estudios y trabajos académicos internacionales, a fin de acotar el espectro de vulnerabilidades a estudiar y obtener datos preliminares. Posteriormente se ejecutó un análisis de vulnerabilidades a nivel global y argentino en sistemas expuestos a Internet. Para este fin se seleccionaron algunas herramientas de uso común en tests de penetración. El criterio de selección fue su especialización para trabajar con grupos grandes de objetivos y su nivel bajo de intrusividad.

Se obtuvo un gran volumen de datos: un universo de 119.190 sistemas y dispositivos expuestos a Internet en todo el mundo, de los cuales 61 pertenecen a organizaciones argentinas. El 56,2% del total corresponden a PLC, y menos del 1% a otros dispositivos de campo como variadores de velocidad e interfaces hombre-máquina. Se encontró que un 58,9% de los sistemas descubiertos trabajan sin encriptación ni autenticación y adicionalmente un 6,9% utiliza protocolos criptográficos deprecados con vulnerabilidades de seguridad conocidas y con vectores de explotación simples. Complementariamente, a partir del relevamiento bibliográfico se obtuvo una progresión anual de vulnerabilidades descubiertas, una clasificación por industria, por componente del sistema y por severidad.

A partir de los datos de la investigación bibliográfica se concluye que la cantidad de vulnerabilidades que se descubren se incrementa año a año, lo que significa que éste área está en crecimiento. La industria más vulnerable es la de energía, lo que resulta especialmente preocupante por el impacto ambiental y el peligro para la vida que esto constituye. Los PLC, junto con los SCADA y dispositivos de comunicaciones, representan las superficies de ataque más vulnerables de un sistema de control industrial. Esta conclusión se ve soportada por la preeminencia de PLC y otros dispositivos de campo encontrados en la investigación online expuestos a Internet, con vulnerabilidades conocidas, y en muchos casos sin ningún tipo de seguridad.

Como conclusión final, la cantidad muy alta de dispositivos de campo expuestos a Internet, revela la inexistencia de un diseño de arquitectura de red con la

ciberseguridad en mente. Además el acceso sin autenticación ni encriptación en muchos casos, y en otros con sistemas obsoletos fácilmente vulnerables, nos muestra que la ciberseguridad aplicada a los sistemas industriales es una cuenta pendiente de muchas organizaciones, a pesar de los riesgos para ambientales, financieros y para la vida en general que esta negligencia acarrea.

Palabras clave: sistemas de control industrial, ciberseguridad, vulnerabilidades, PLC, SCADA

1. Introducción

1.1 Generalidades de sistemas de control industriales

Sistema de control industrial (*ICS, Industrial Control System*) es un término general que cubre varios de tipos de sistemas de control, incluyendo sistemas SCADA (*Supervisory control and data acquisition*), sistemas de control distribuido (DCS, *distributed control systems*) y otras configuraciones a menudo encontradas en todos los sectores industriales y de infraestructura crítica. Un ICS consiste de la combinación de [1] una serie de componentes de control (eléctricos, mecánicos, hidráulicos, neumáticos, etc.) que actúan de manera coordinada para lograr un objetivo industrial, como por ejemplo, una capacidad de manufactura o de transporte de materia o energía. La parte del sistema que se encarga principalmente de la producción de un resultado o salida, se denomina *proceso*. La parte controladora del sistema, denominada *control*, incluye la especificación de la salida o rendimiento deseado y también las herramientas para mantener la conformidad con estas especificaciones. El control puede ser completamente automático o incluir una intervención humana dentro del lazo. Los sistemas de control pueden configurarse para operar en lazo abierto, lazo cerrado o modo manual, dependiendo de la operación deseada. En lazo abierto, la salida del sistema de control es totalmente determinada por parámetros preestablecidos, mientras que en lazo cerrado, la salida tiene un efecto en la entrada a través de un camino de realimentación de manera tal que se obtengan resultados dentro de un rango aceptable. En caso de operación en modo manual, el sistema es controlado completamente por operadores humanos. Un ICS típico puede contener numerosos lazos, interfaces con operadores (*HMI, Human Machine Interface*), y herramientas de diagnóstico y mantenimiento construidas por sobre una cantidad de protocolos de comunicaciones. Los ICS se usan típicamente desde hace años en todos los sectores industriales, incluyendo el eléctrico, de agua potable y cloacas, aceite y gas natural, químico, transporte, farmacéutico, papelero, manufactura discreta, control de tráfico aéreo, etc. Por lo general son críticos para su operación, altamente interconectados e interdependientes. La figura 1 ilustra un diagrama de bloques general de un ICS:

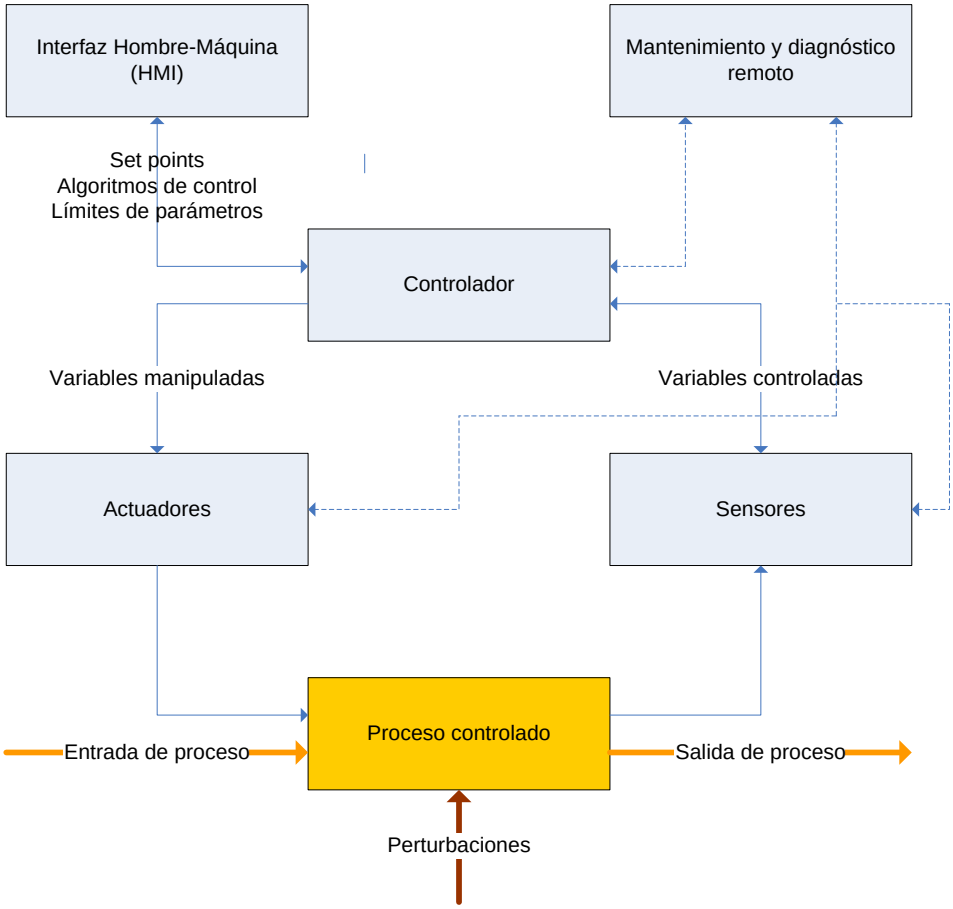

Figura 1 - Diagrama de bloques de ICS

Muchos de los ICS de hoy día evolucionaron de la inserción de capacidades de IT (*Information Technologies*) en sistemas físicos pre-existentes, a menudo reemplazando o suplementando mecanismos físicos de control. Por ejemplo, muchos controles digitales embebidos reemplazaron controles mecánicos analógicos en máquinas rotativas y motores. Las mejoras en costo y performance han estimulado este proceso evolutivo, resultando en muchas de las hoy llamadas tecnologías "*smart*" (inteligentes), tal como las redes eléctricas inteligentes (*smart grid*), transporte urbano inteligente, *smart buildings*, etc. Esto produce un incremento de hecho de la conectividad y criticidad de los sistemas de control, pero además exige una mayor necesidad de adaptabilidad y seguridad. La ingeniería de ICS continúa evolucionando para proveer estas y otras capacidades al mismo tiempo que intenta mantener el largo ciclo de vida asociado a los sistemas industriales [1]. Mientras tanto, la incorporación de dispositivos y capacidades de IT a los sistemas físicos presenta comportamientos no previstos con implicaciones de seguridad considerables. El problema central que estudia el presente trabajo es la consecuencia directa de este "choque de culturas" entre la industria y los sistemas de información. La intersección de estas dos áreas es el hábitat de los ICS.

El estudio de sistemas de infraestructura crítica merece atención especial, en primer lugar por el impacto económico, medioambiental y social sin precedente que tienen los problemas de seguridad cuando suceden en ellos, y por otro lado por las particularidades que le concede el alto nivel de interconectividad e interdependencia que poseen [2], [3]. A menudo la relación entre ellos es compleja, tanto físicamente como a través de redes de información y comunicaciones. Un incidente en una infraestructura puede directa e indirectamente afectar a las demás a través de fallas en cascada, muchas veces escalando en severidad. Tanto las redes de transmisión como de distribución de energía eléctrica utilizan sistemas SCADA distribuidos geográficamente para operar sistemas dinámicos de gran interconectividad consistentes de distribuidoras públicas y privadas, y cooperativas rurales. Los SCADA monitorean y controlan la distribución de energía recolectando datos y enviando comandos a estaciones de control remotas en el campo desde una central de operaciones. Esto es cierto también para otros grandes usuarios de SCADA, como las empresas de agua potable y cloacas, gas y combustible, etc. Por lo general los SCADA y DCS se interconectan. Este es el caso para centrales de producción, transformación y control de energía. Por ejemplo, la operación de una instalación de generación de energía es controlada por un DCS, pero la producción se coordina en base a datos de demanda de transmisión y distribución del SCADA. La energía eléctrica es considerada a menudo como una de las fuentes más prevalentes de disrupciones en sistemas interdependientes de infraestructura crítica. Por ejemplo, una pérdida de monitoreo y comando de una unidad de generación ocasionada por interrupción de un enlace de microondas podría causar un desbalanceo disparando múltiples fallas en cascada en toda la red eléctrica. Si el desbalanceo es suficientemente grande como para causar la salida de servicio de sectores de la red, podrían afectarse otras industrias que dependan de ella, como la producción y transporte de gas, tratamiento de agua, etc.[2]

Un ICS típico contiene numerosos lazos de control, interfaces humanas y herramientas remotas de diagnóstico y mantenimiento construidas con una variedad de protocolos y arquitecturas de comunicaciones. Un lazo de control utiliza sensores, actuadores y controladores para manipular un proceso controlado. Un sensor es un dispositivo que produce una medición de una propiedad física y envía esta información como una variable al controlador. El controlador interpreta las señales y genera variables manipuladas en función de ellas, basado en un algoritmo de control y parámetros preexistentes o *target set-points*. Las variables manipuladas son transmitidas a los actuadores. Los actuadores, tales como válvulas, contactores, switches o motores son utilizados para la manipulación directa del proceso controlado a partir de los comandos

del controlador. Los operadores e ingenieros utilizan las interfaces humanas para manipular y configurar *set-points*, algoritmos de control, y ajustar otros parámetros del controlador. La interfaz humana además muestra información del estado del proceso, y también información histórica. Las utilidades de diagnóstico y mantenimiento se usan para prevenir, identificar y recuperarse de circunstancias de operación anormal o fallos. A veces los lazos de control se diseñan de manera anidada o en cascada, de manera tal que el *set-point* de un lazo se basa en una variable de proceso determinada por otro lazo. Por lo general, tanto los lazos de nivel supervisor como los de más bajo nivel operan continuamente a lo largo de la duración del proceso, con tiempos de ciclo en un rango de entre milisegundos a minutos.[4]

Las consideraciones de diseño fundamentales de un ICS son [1]:

- **Requerimientos de timing de proceso**: Los procesos controlados por los ICS tienen un espectro variado de requerimientos temporales, incluyendo velocidad de respuesta, consistencia, regularidad y sincronización. Muchas veces los seres humanos no somos capaces de cumplir estos requisitos de manera consistente, y ello implica la necesidad del control automático. En algunos sistemas inclusive se busca que el dispositivo encargado de la computación de las variables de salida se instale lo más cerca posible de sensores y actuadores para reducir la latencia de comunicación al mínimo posible.
- **Distribución geográfica**: Existen muchos niveles de distribución geográfica, desde pequeños sistemas implementados como controles locales con un PLC, hasta sistemas distribuidos que se extienden a lo largo de cientos de kilómetros, como acueductos o redes eléctricas de distribución. Una mayor extensión espacial implica una complejidad añadida a nivel de red de datos, a veces implicando líneas alquiladas, redes de conmutación de circuitos o paquetes, comunicaciones móviles, y otros.
- **Jerarquización**: El control supervisor se utiliza para proveer una ubicación central que pueda funcionar como acumulador de datos de múltiples ubicaciones. A su vez este agregado de datos permite soportar decisiones de control basadas en el estado actual del sistema. A menudo, un control jerárquico/centralizado permite proveer al operador humano con una visión general y comprensiva de un sistema de grandes dimensiones espaciales.
- **Complejidad de control**: A menudo algunas funciones de control se pueden ejecutar con controladores simples y algoritmos preestablecidos. Sin embargo, a medida que aumenta la complejidad del proceso a controlar, se incrementa la sofisticación de los controladores. En casos especiales de alta complejidad y severidad crítica, es

imposible obviar la supervisión humana constante para resguardar el cumplimiento de los objetivos superiores del sistema, por ejemplo en el control de tráfico aéreo.

- **Disponibilidad**: Los requisitos de disponibilidad o confiabilidad del sistema fundamentalmente determinan la redundancia e implementaciones alternativas a través de toda la infraestructura de comunicaciones y control.
- **Impacto de fallos**: El fallo de una función de control puede implicar impactos sustancialmente diferentes a lo largo de todo el espectro de aplicaciones. Los sistemas con mayor impacto de falla por lo general se diseñan desde su concepción con la habilidad de continuar las operaciones a través de redundancia, o la capacidad de operar en estado degradado.
- **Seguridad**: Los sistemas deben poder detectar condiciones inseguras de funcionamiento y disparar acciones para reducirlas a condiciones seguras. En la mayoría de las aplicaciones críticas de seguridad, la supervisión humana y control de los procesos peligrosos es una parte esencial del sistema de seguridad.

1.2 Generalidades de SCADA

Los sistemas SCADA son una clase particular de ICS, de gran ubicuidad en sistemas de infraestructura crítica. Esencialmente se utilizan para controlar sistemas de gran dispersión espacial en los que la adquisición centralizada de datos es tan importante como el control [5], [6]. Tienen gran aplicación en áreas de sistemas de distribución, por ejemplo de agua y cloacas, gasoductos, oleoductos, transmisión y distribución eléctrica, y transporte público. Un sistema SCADA típicamente integra adquisición de datos con transmisión de datos y software HMI para proveer una monitorización centralizada y control para procesos de numerosas entradas y salidas. El sistema recolecta la información de campo, la transfiere a un sistema central de computación y la representa de manera organizada. De esta manera permite el monitoreo o control de un sistema completo prácticamente en tiempo real desde una central de operaciones. Dependiendo de la configuración general del SCADA, el control de cada sistema individual, operación o tarea puede ser automático o ejecutarse bajo los comandos del operador. El *hardware* típico para una instalación de este tipo incluye un servidor de control ubicado en el centro de operaciones, equipos de comunicaciones (de área local y área amplia, considerando la gran extensión geográfica que abarcan mayoritariamente estos ICS), y uno o más sitios de campo distribuidos consistentes de RTU (*remote terminal unit*) que controlan a los actuadores y monitorean sensores. El

servidor de control almacena y procesa la información de las entradas y salidas de las RTU, mientras la misma controla los procesos locales. El hardware de comunicaciones permite la transferencia de la información desde y hacia el servidor de control. El software es programado para saber qué y cuándo monitorear, qué rangos son aceptables para cada parámetro, y qué respuesta iniciar ante cada desviación de los mismos. Un IED (*intelligent electronic device*) puede comunicarse directamente con el servidor de control, por ejemplo un relé de protección, o un PLC puede interrogar al IED y reenviar esa información al servidor de control para su tratamiento. Por lo general un sistema SCADA se diseña con alto nivel de tolerancia a fallas y alta redundancia.

La Figura 2 muestra los componentes y la configuración general de un sistema SCADA. El centro de control contiene principalmente un servidor central y hardware de red, aunque también suelen incluir interfaces HMI, *workstation* de ingeniería, y el servidor histórico. Todos estos componentes se conectan a través de una LAN. El centro de control recolecta la información generada por los sitios de campo, muestra la información en el HMI y puede disparar acciones en base a eventos. Además, el centro de control es responsable de la generación de alarmas, estadísticas y reportes. Los sitios de campo se encargan del control local de actuadores y monitoreo de sensores. Generalmente se diseñan con algún tipo de capacidad de acceso remoto para permitir que los operadores ejecuten tareas de diagnóstico y mantenimiento. Esta particularidad suele ser la fuente de innumerables problemas de seguridad. La información del sistema se transporta por sobre un gran número de protocolos de comunicaciones, de red y serie, abiertos y propietarios. Es muy común que cada sistema utilice una combinación de tecnologías y protocolos de comunicaciones, en cascada y en paralelo. También hay gran variabilidad entre las topologías de red usadas en los diferentes puntos del sistema, normalmente en combinación entre sí.

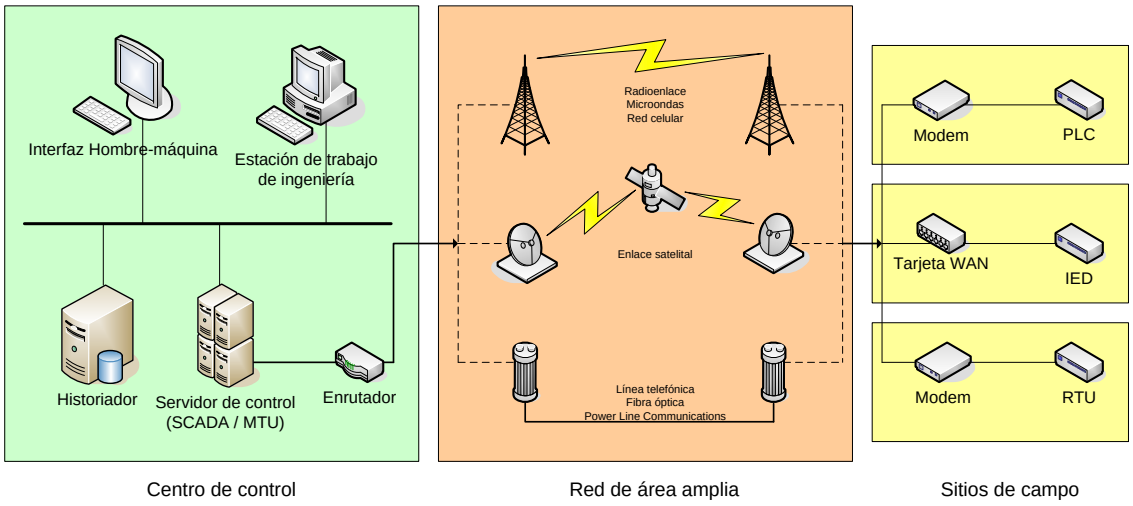

Figura 2 - Layout general de un SCADA

Funcionalmente, la topología punto a punto es la más simple. Sin embargo, puede ser más costosa debido al gran número de canales individuales necesarios para cada conexión. En la configuración serie, se reduce el número de canales, sin embargo compartir canales puede tener un efecto en la eficiencia del sistema. La figura 3 ilustra un ejemplo de implementación de un sistema SCADA. Este sistema en particular consiste de un centro de control y tres sitios de campo. Un centro de control de backup provee redundancia en la eventualidad de un fallo en el centro de control primario. Se usan conexiones punto a punto para la conexión interred entre la red de campo y la red del centro de control, dos de ellas funcionando por sobre radioenlace serie. La tercera estación de campo es local al centro de control, por lo que utiliza la WAN para comunicaciones. Un centro de control regional se ubica por sobre el centro primario para un nivel más alto de control supervisor. La red corporativa tiene acceso a todos los centros de control a través de la WAN, y los sitios de campo pueden ser accedidos remotamente para diagnóstico y mantenimiento. El centro de control primario encuesta (*polling*, es la técnica para recopilación de información por parte de un nodo central en la cual el nodo central es el que solicita en intervalos periódicos a los nodos remotos que informen su estado, los cuales permanecen pasivos hasta que reciben la interrogación del nodo central) a los dispositivos de campo en intervalos definidos, obteniendo así los valores de la variables que representan el estado de los sensores, y a su vez actualiza las variables de ajuste o *set-points* para que los dispositivos de campo corrijan la posición de los actuadores. De manera adicional el servidor central puede recibir interrupciones de alta prioridad provenientes del sistema de alarma de los sitios de campo.

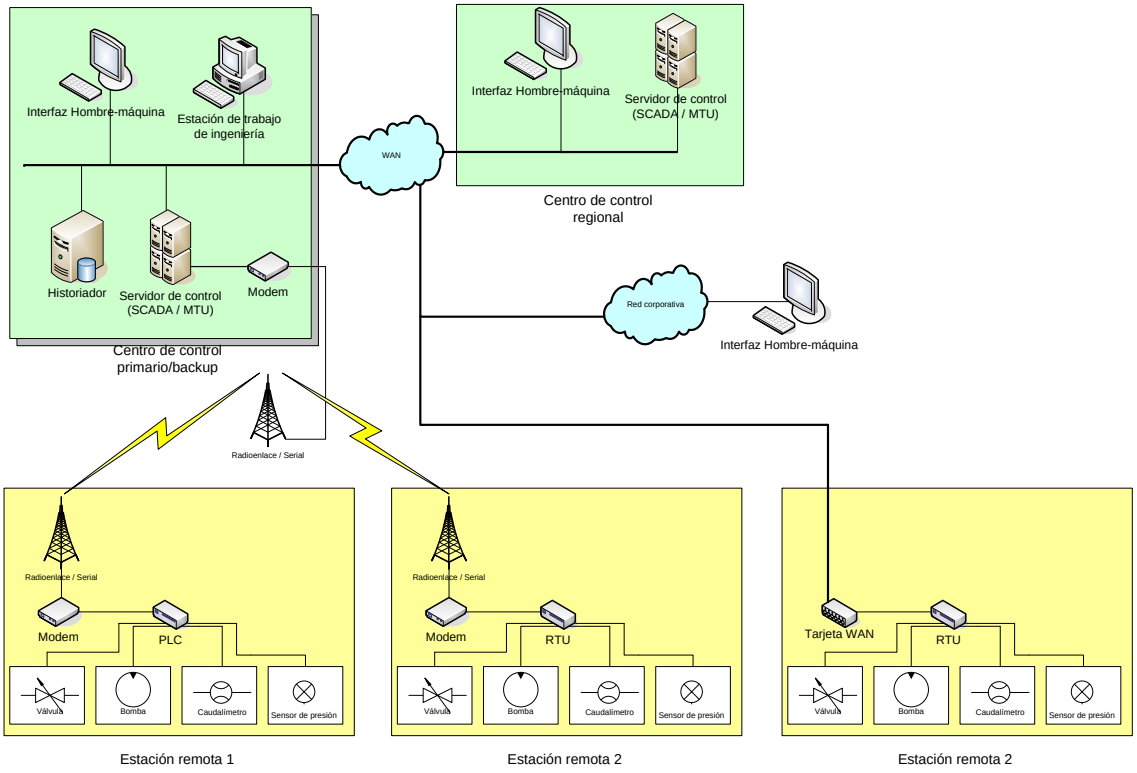

Figura 3 - Implementación de una red SCADA

La figura 4 muestra una implementación de ejemplo para un sistema de monitoreo y control de transporte ferroviario. El ejemplo incluye un centro de control que contiene un sistema SCADA y tres secciones de sistema de control ferroviario. El SCADA encuesta a los dispositivos de campo sobre el estado de los trenes, sistemas de señales, eléctrico, venta de tickets, y cualquier otro parámetro que sea considerado relevante al momento del diseño. Estos datos alimentan las consolas de operación en la estación HMI dentro del centro de control. El SCADA también recibe la entrada de los operadores en el centro de control y monitorea las condiciones en cada sitio remoto.

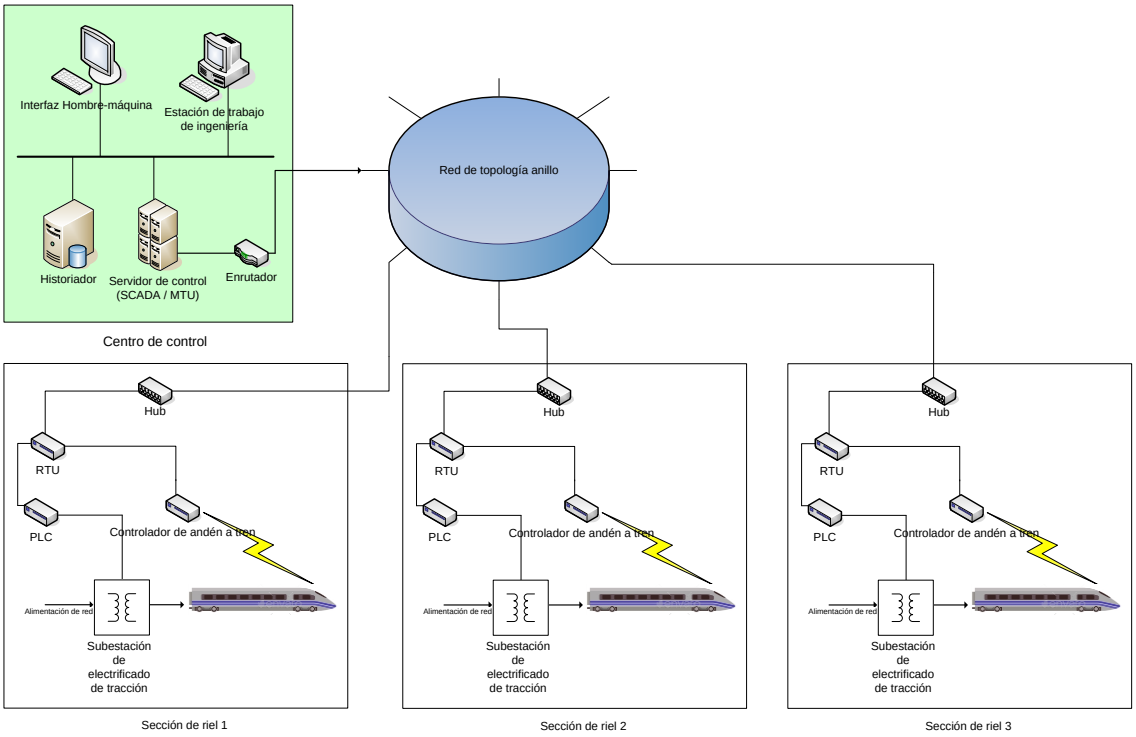

Figura 4 - Implementación de un sistema SCADA (control ferroviario)

1.3 DCS: Sistemas de control distribuido

Los DCS se utilizan para controlar sistemas de producción dentro de la misma ubicación geográfica para todas las áreas de la industria. Estos sistemas pueden efectuar tanto control de procesos continuos como de manufactura discreta. En líneas generales un DCS es un tipo de arquitectura de control compuesta por un nivel superior de control supervisor y múltiples subsistemas integrados controladores de procesos localizados. A nivel de control. Un DCS utiliza un lazo supervisor centralizado para mediar a uno o varios grupos de lazos de control de tareas específicas que componen el proceso productivo completo [7]. Se aplican lazos de todas las clases descritas en el apartado anterior, buscando mantener las variables de salida dentro de la tolerancia predefinida alrededor de un *set-point*. La modularización que incorpora el DCS puede ser beneficioso en reducir el impacto de fallas en el sistema general.

Es simple de ver que los DCS y SCADA poseen componentes, configuraciones y *layout* muy similares, sin embargo existen diferencias esenciales entre ambos. En un sistema SCADA los dispositivos de campo ejecutan los lazos de control cerrado y centro de control se encarga fundamentalmente de recolectar información y hacer interfaz con los operadores. Su participación en las tareas de control del proceso es limitada. Por el contrario en un DCS el controlador centralizado participa activamente en el lazo maestro

de control, realizando tareas de corrección automática y manteniendo los puntos de funcionamiento de los lazos de menor jerarquía a través de un ajuste de una variable de error. Podríamos resumir esta y otras diferencias conceptuales de la siguiente manera:

- DCS tiene orientación a proceso, mientras que SCADA está orientado a recolección de datos. DCS tiene énfasis en control de procesos, e incorpora un nivel de control supervisor. Por otra parte el foco de SCADA está puesto en la adquisición de datos del proceso y presentación al operador y centro de control.

- Desde un punto de vista de distribución espacial, como se mencionó anteriormente un DCS por lo general se aplica a un proceso contenido en un espacio geográfico limitado, como por ejemplo una fábrica. En cambio los sistemas SCADA pueden extenderse a lo ancho de sistemas muy amplios, como redes de distribución. Esto tiene relación con lo descrito en el punto anterior, dado que una red de área tan amplia implica un nivel de potencialidad de falla y una latencia inaceptables para un lazo de control, pero compatibles con una tarea de recolección de datos.

- Desde un punto de vista de arquitectura, como se mencionaba un DCS aplica un lazo de control cerrado que abarca desde la central de control hasta las unidades terminales remotas. SCADA se limita a la recolección de datos. Sin embargo, los avances tecnológicos en comunicaciones han logrado tales mejores en ancho de banda, latencia y confiabilidad que la industria está propulsando las capacidades de los SCADA para incorporar ajuste de *set-points*, es decir agregar funciones de control en lazo abierto o *feedforward*. Este solapamiento de usos y funciones entre SCADA y DCS es una tendencia general, y es probable que a corto y mediano plazo continúe.

- DCS es conducido por estado de proceso (*process state driven*), lo que significa que encuesta el estado de todas las variables de importancia del proceso en un intervalo de tiempo despreciable con respecto al tiempo mínimo de variación significativa o constantes de tiempo físicas del proceso. Este capacidad de respuesta virtualmente inmediata es lo que denominamos “tiempo real”, e implica que el DCS mantiene una modelización o abstracción del proceso representativa en todo momento de su estado actual. Inicialmente SCADA es conducido por eventos, por lo que no monitorea el proceso secuencialmente si no que los dispositivos de campo se configuran para esperar un evento particular y en ese momento transmitir los valores de variables. Al igual que el punto anterior, esta diferencia tiene que ver con el uso de SCADA en redes de área amplia, en los que el ancho de banda es mucho más caro que redes de área local, haciendo prohibitivos los costos de mantener al SCADA sincronizado en tiempo real. Esta consideración de diseño acarrea algunas desventajas, principalmente retardos y desfasajes entre la representación del proceso que mantiene el sistema y el proceso en sí mismo, además de problemas de inconsistencia en caso de que haya

servidores o bases de datos redundantes recibiendo datos al mismo tiempo. Sin embargo, como se comentaba en el punto anterior, con la enorme disminución de costos que han tenido las redes de comunicación en los últimos años, cada vez se hace menos necesario esta salvedad, y todos los SCADA actuales pueden ser configurados para funcionar en modo de estado proceso (en la práctica simplemente denominado *polling*).

- En términos de aplicaciones, los DCS se utilizan en procesos de área confinada, como plantas o fábricas, y para procesos de control complejos. Por el contrario los SCADA ven mayor aplicación en sistemas de gran extensión espacial.

sLa figura 5 muestra una implementación de DCS de ejemplo, evidenciando los componentes y la configuración general. Este DCS abarca espacialmente la instalación entera desde el nivel base de proceso productivo hasta la capa corporativa o de negocios. El control supervisor se comunica con sus subordinados a través de la red de control. El supervisor envía *set-points* y solicita datos de los controladores de campo distribuidos. Estos últimos controlan los actuadores de proceso basados en los comandos de control del servidor central y la realimentación de sensores de sus procesos. Los controladores de bajo nivel encontrados el DCS del ejemplo mostrado son algunos de los más comunes. En la práctica general estos diferentes controles se implementan como algoritmos en un PLC. La red de campo incorpora cableado punto a punto, la técnica más básica y limitada para que los controladores accedan a los sensores y actuadores, y también el protocolo de campo Fieldbus (IEC61158), que se usa para reducir el cableado entre controladores y sensores individuales. Además permite una funcionalidad más allá del control, incluyendo diagnóstico de dispositivos de campo. A menudo se utilizan protocolos de campo diseñados por grupos de la industria, como Fieldbus y Modbus.

A parte de los lazos de nivel supervisor y nivel de campo, pueden existir lazos de nivel intermedio. Por ejemplo en el caso de manufactura de partes discretas, podría haber un nivel de supervisión intermedio en cada celda dentro de la planta. Esta supervisión englobaría un área productiva completa, conteniendo un controlador de máquina que procesa una parte, y un controlador de robot para el manejo de stock y productos terminados. Podrían existir una serie de estas celdas por debajo del lazo supervisor general del DCS.

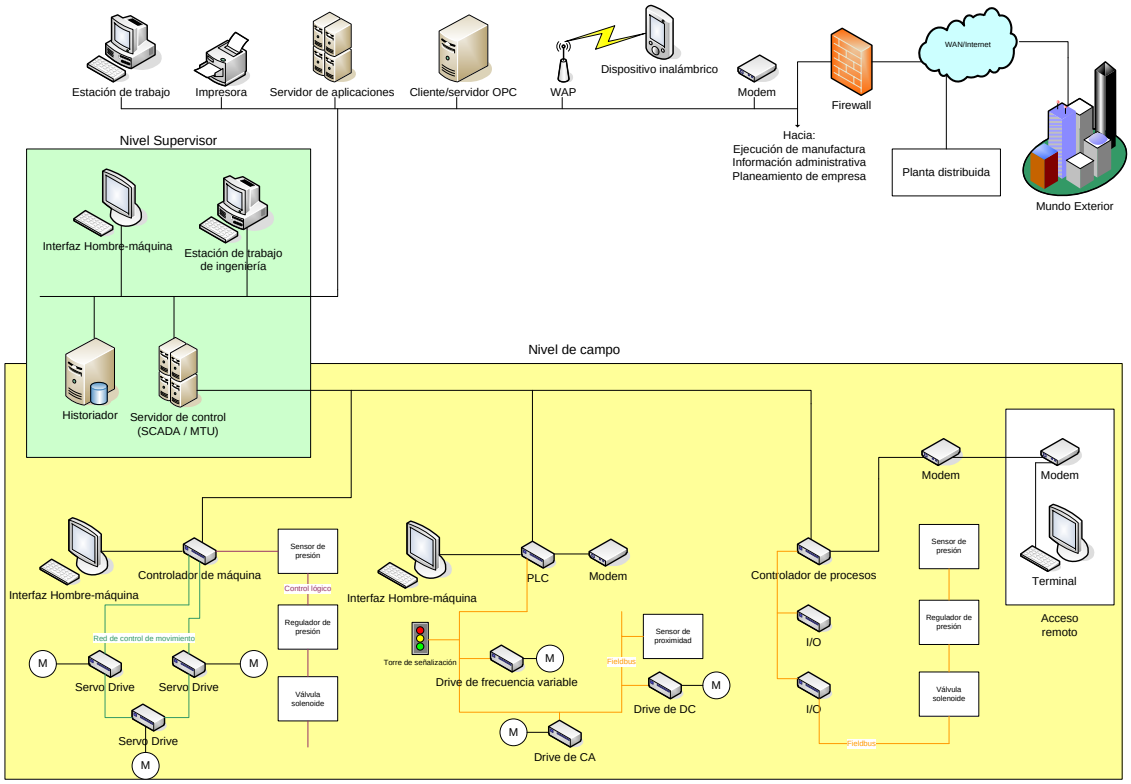

Figura 5 - Implementación de sistema de control distribuido

1.4 Ciberseguridad para sistemas de control industriales

Un ICS controla el mundo físico, a diferencia de los sistemas de IT que manejan datos. Esto implica que existen una serie de diferencias fundamentales en las que un ICS difiere de un sistema de IT tradicional, incluyendo diferentes riesgos y prioridades. Entre estas diferencias se incluye un riesgo significativo a la salud y la vida humanas, daños serios medioambientales, financieros como pérdidas de producción y lucro cesante, e impactos en la economía de una nación. Los ICS tienen diferentes requerimientos de performance y confiabilidad, y utilizan tecnologías, como sistemas operativos y aplicaciones, poco convencionales para un ambiente de red de IT típico. Las protecciones de seguridad deben implementarse de una manera que mantenga la integridad del sistema durante tanto operaciones normales como bajo un ataque [8].

Inicialmente, las diferencias entre ambos eran aún mayores. Los ICS eran sistemas aislados basados en protocolos propietarios de control, y usaban hardware y software especializados. Hoy día estas tecnologías antiguas propietarias están siendo reemplazadas por dispositivos IP y Ethernet, de bajo costo y gran utilización, lo que incrementa la posibilidad de incidentes y vulnerabilidades de seguridad. Los ICS modernos adoptan soluciones de IT para promover la conectividad corporativa,

capacidades de acceso remoto y otras funcionalidades, y se diseñan basados en base a computadoras, sistemas operativos y protocolos de red estandarizados. Esta tendencia implica que a medida que pasa el tiempo, la diferencia entre un ICS y un sistema típico de IT se difumina. Como consecuencia se han ampliado las capacidades de IT de los ICS, pero ha disminuido en gran medida la aislación de los sistemas industriales del resto del mundo interconectado, creando una gran necesidad de mejorar la seguridad de los ICS. Ya existen soluciones de seguridad diseñadas para lidiar con este tipo de situaciones en sistemas de IT típicos, aunque al aplicar estas mismas soluciones a un ambiente de ICS deben tenerse en cuenta una serie de precauciones especiales [9].

Los ambientes en los que operan los sistemas de IT y los sistemas industriales están cambiando todo el tiempo. Estos ambientes se definen a partir de una serie de características, como por ejemplo el espacio de amenaza, la función de negocio/misión, la arquitectura de seguridad de la empresa y de la información, las tecnologías de información, las relaciones de cadena logística, la cultura organizacional, los procesos de adquisición, las políticas/procedimientos organizativas, la tolerancia a fallas, las limitaciones, y otros.

Considerando que el conocimiento de seguridad de datos atañe principalmente a los sistemas de IT, resulta útil definir el alcance y las consideraciones de seguridad en un sistema industrial a partir de estas definiciones. Las consideraciones de seguridad fundamentales para ICS definidas a partir de su relación con los sistemas típicos de IT son [1]:

- **Requerimientos de performance y *timing***: Por lo general los sistemas industriales son críticos en tiempo. El criterio de retardo y *jitter* aceptable varía en función de cada aplicación. Mayormente los sistemas requieren respuestas deterministas de alta confiabilidad, pero no requieren gran ancho de banda o capacidad de datos. Al contrario, los sistemas típicos de IT priorizan la capacidad de transmisión, y pueden funcionar con un cierto grado de latencia y *jitter*. Para algunos ICS, el tiempo de respuesta automática o la respuesta del sistema a la interacción humana es muy crítica. Algunos ICS se diseñan alrededor de sistemas operativos de tiempo real (RTOS) para dar atención específica a esta cuestión.
- **Requerimientos de disponibilidad**: Muchos procesos sujetos a sistemas de control industriales son de naturaleza continua. Esto implica que cortes de servicio de los sistemas controladores pueden generar complicaciones y por tanto no son aceptables. Las salidas de servicio debe ser planeadas y programadas con anticipación. Es esencial que se ejecuten pruebas de aceptabilidad exhaustivas previas y posteriores al despliegue en campo, a fin de asegurar el nivel de disponibilidad esperado. En

general, es muy difícil detener e iniciar un sistema de control sin afectar el proceso productivo. En algunos casos, los productos en la línea de producción o el equipamiento en uso son mucho más importantes que los datos que se están enviando, por lo tanto no es aceptable el uso de estrategias típicas de IT tales como reiniciar componentes o software, debido al impacto negativo que tienen en la producción y los requerimientos de disponibilidad y confiabilidad. Algunos sistemas de control se despliegan con redundancia en sus componentes críticos corriendo en paralelo, para proveer continuidad al trabajo en caso de una salida de servicio de los componentes primario.

- **Requerimientos de gestión de riesgo**: En un sistema de IT típico, la confidencialidad de datos y la integridad son de importancia máxima. En un ICS, la seguridad de las personas y la tolerancia a fallos para resguardar la vida humana, la salud pública, cumplimiento de regulaciones, pérdida de equipamiento, y pérdida o daño a productos son las preocupaciones centrales. El personal responsable de operar, asegurar y mantener un ICS debe comprender la relación fundamental entre seguridad del sistema y seguridad de las personas.

- **Efectos físicos:** Los dispositivos de campo de un sistema de control afectan y conducen procesos físicos. Es posible que ocurran eventos físicos que sean la manifestación de interacciones complejas entre los procesos físicos y el sistema de control. Lograr un entendimiento completo de estos efectos físicos potenciales a menudo requiere una comunicación entre expertos en sistemas de control y expertos en el área a la que atañe el proceso físico particular bajo control.

- **Operación del sistema:** Los sistemas operativos y las redes de control de un ICS por lo general son significativamente diferentes a sus equivalentes de IT, requiriendo un conocimiento, habilidades y experiencia diferentes. Las redes de control son manejadas típicamente por ingenieros de control, no personal de IT. No dimensionar esta diferencia puede tener consecuencias desastrosas para la operación del sistema.

- **Limitación de uso de recursos:** Los sistemas de control y los sistemas operativos de tiempo real usados en ellos son por lo general sistemas de recursos limitados que no incluyen las capacidades de seguridad típicas de los sistemas de IT modernos. El largo ciclo de vida asociado al mercado industrial implica que muchas veces los ICS operen sobre sistemas antiguos que han quedado relegados en funcionalidad y recursos del sistema. En algunos casos pueden carecer de características deseadas de mucha ubicuidad, como registro de fallas, encriptación, protección por contraseña, etc. El uso indiscriminado o poco criterioso de prácticas comunes de seguridad de IT en un sistema de control puede tener consecuencias inesperadas, como fallas de disponibilidad o latencia. Puede que un sistema de control

no tenga recursos disponibles de manera suficiente para hacerles una readaptación y equiparlos con capacidad de seguridad actualizadas.

- **Comunicaciones:** Los protocolos y medios de comunicación utilizados en entornos industriales para control de dispositivos de campo y redes intermedias pueden ser diferentes a la mayoría de los ambientes de IT. En muchos casos se usan protocolos cerrados y propietarios.

- **Gestión de cambios:** Para mantener la integridad de sistemas de control y de IT, la gestión de cambios es muy importante. El software desactualizado representa una de las principales vulnerabilidades de un sistema. Las actualizaciones de software en un sistema de IT, incluyendo parches de seguridad, se aplican típicamente de manera ordenada y a tiempo, en base a los dictámenes de las políticas y procedimientos de seguridad. Además, estos procedimientos a menudo son automatizados a través de herramientas del lado del servidor. En un sistema de control es mucho más complejo administrar la instalación de parches y actualizaciones, y mantener el sistema al día. Además cada actualización debe ser probada exhaustivamente tanto por el fabricante de la aplicación ICS como por el usuario final. Adicionalmente, el operador del ICS debe planear cada salida de servicio con mucha anticipación, haciendo más engorrosa la situación. También existe el problema de que el ciclo de vida de los productos de IT es mucho menor que el esperado de los sistemas industriales, implicando que en ocasiones los sistemas operativos o hardware de computadora aplicados a un ICS queden fuera de soporte y dejen de ser mantenidos, dejando de recibir actualizaciones para futuros problemas. Nuevamente, la práctica recomendada es la creación de un equipo interdisciplinario entre expertos en sistemas de control y personal de IT para lograr una solución a medida que contemple todos los puntos de vista.

- **Soporte**: La naturaleza abierta de gran cantidad de software de uso moderno en sistemas de IT y la expansión de la cultura *open-source* al mundo corporativo ha permitido una diversificación de estilos y procedimientos para dar soporte a una gran variedad de arquitecturas y tecnologías interconectadas. Para los sistemas industriales en cambio el servicio de soporte es generalmente a través de un único proveedor, que probablemente no posee una solución de soporte diversificada e interoperable para los otros sistemas. En algunas instancias, por cuestiones de licenciamiento y acuerdos de servicio no se permiten soluciones de seguridad de terceros, pudiendo incurrir en pérdida o nulidad de servicio en ese caso.

- **Vida útil de componentes:** En caso de sistemas de IT, el ciclo de vida está en el orden de 3 a 5 años. En sistemas industriales, en los que en muchos casos la tecnología ha sido desarrollada para un uso e implementación muy específicos, el ciclo

de vida de los sistemas desplegados está en el orden de entre 10 a 15 años, y algunas veces más.

- **Locación de componentes:** La mayoría de los componentes de IT se ubican en instalaciones comerciales o empresariales, en centros urbanos o de fácil acceso. Para sistemas industriales, por el contrario, la norma son los lugares aislados, remotos y que requieren un esfuerzo de transporte considerable, siendo esto especialmente cierto para procesos de extracción primaria como minería, gas, petróleo, agroindustria, etc. Esta salvedad es importante para considerar las medidas de seguridad físicas y ambientales que deben implementarse.

En resumen, las diferencias operacionales y de características de riesgo entre sistemas industriales y sistemas puramente informáticos han creado la necesidad de una sofisticación mayor en la aplicación de estrategias de ciberseguridad y operativas. Resulta fundamental el trabajo coordinado y cercano de un equipo interdisciplinario de ingenieros de control, operadores del sistema y profesionales de seguridad de IT para entender las posibles implicaciones de la instalación, operación y mantenimiento de las soluciones de seguridad en conjunto con el sistema de control. Antes del despliegue de las soluciones de seguridad debe comprenderse exactamente el impacto en confiabilidad y performance que tendrán en los sistemas productivos. Además, debido a las arquitecturas especializadas de los ambientes de ICS, muchos los sistemas operativos y aplicaciones que ejecutan no operan correctamente con soluciones de ciberseguridad de IT del tipo COTS (*commercial-off-the-shelf*).

1.5 Elementos generales de ciberseguridad [10]

Los requerimientos de seguridad de la información dentro de una organización han sufrido dos cambios mayoritarios en las últimas décadas. Antes del uso generalizado de equipamiento de proceso de datos, la seguridad de la información considerada valiosa por una organización se proveía primariamente por medios físicos y administrativos. Por ejemplo, el uso de gabinetes de archivo robustos con cerraduras de combinación para almacenar documentos sensibles, o los procedimientos de verificación de personal durante el proceso de contratación. Con la introducción de las computadoras, la necesidad de herramientas automatizadas para proteger arhivos y otra información digital se hizo evidente. Esto es especialmente cierto para el caso de sistemas compartidos, y aún más para sistemas de acceso público a través de redes telefónicas, redes de datos o la Internet. El nombre genérico para el grupo de

herramientas y técnicas diseñadas para proteger los datos y frustrar a los atacantes es ciberseguridad.

El segundo cambio mayoritario que afectó la seguridad de datos fue la introducción de sistemas distribuidos y el uso de redes e instalaciones de comunicaciones para transportar datos entre terminales de usuario y computadoras, y entre computadoras y computadoras. Considerando el alcance del presente trabajo, debemos considerar además los sistemas de transporte de datos entre computadoras y controladores, sensores, actuadores, etc. Para proteger los datos durante su transmisión deben aplicarse medidas comprendidas en el área denominada seguridad de redes. En realidad, el término seguridad de redes es algo confuso, porque virtualmente todos los negocios, gobierno, y organizaciones académicas interconectan sus equipos de procesamiento de datos con un arreglo de redes interconectadas. Tal arreglo se denomina internet o interred, por lo que el término exacto sería seguridad de interredes. No hay un límite claro entre estas dos formas de seguridad. Por ejemplo, uno de los ataques a sistemas de información en general, y que de hecho ha visto un uso bastante común en sistemas industriales también, es el virus de computadora. Un virus puede introducirse en un sistema físicamente cuando llega en un disco óptico, o en un pendrive USB, técnica que cobra preponderancia para saltar los *air-gap* que se diseñan siempre para dar aislación a las redes de control. Además los virus pueden llegar a través de una interred. En cualquier caso, una vez que el virus es residente en un sistema de computadoras, se necesitan herramientas interna y un proceso especial para detectarlo y recuperar el sistema. Existen otros casos generales de violación de ciberseguridad, por ejemplo:

- El usuario A transmite un archivo al usuario B. El archivo contiene información sensible que debe protegerse y mantener su confidencialidad. El usuario C, que no posee autorización para leer el archivo, consigue monitorear la transmisión y capturar una copia del archivo durante su transmisión.
- Un administrador de red, D, transmite un mensaje a la computadora E, la cual está bajo su administración. El mensaje instruye a la computadora a actualizar un archivo de autorización para incluir las identidades de un número de usuarios nuevos que deben ser concedidos acceso a esta computadora. El usuario F intercepta este mensaje, altera su contenido para añadir o borrar entradas, y luego lo reenvía a E, que lo acepta como proveniente del administrador, D, y actualiza su archivo de autorización correspondientemente.
- En vez de interceptar el mensaje, el usuario F construye su propio mensaje con las entradas que él desea y lo transmite a E como si viniera del manager D, suplantando

su identidad. La computadora E acepta el mensaje como proveniente de D y actualiza su archivo de configuración de manera acorde.

- Un empleado es despedido sin aviso. El administrador de personal envía un mensaje al servidor central para invalidar la cuenta del empleado. Cuando la invalidación ha terminado, el servidor debe distribuir un aviso al archivo de empleados como confirmación de la acción. El empleado logra interceptar este mensaje y retardarlo lo suficiente para acceder una última vez al servidor y hacerse con información sensible. El mensaje es entonces reenviado, y el aviso distribuido. La acción del empleado puede pasar inadvertida durante un tiempo considerable.
- Un cliente envía un mensaje a un corredor de bolsa con instrucciones para varias transacciones. Subsecuentemente, las inversiones pierden valor y el cliente niega haber enviado el mensaje.

Esta lista no es exhaustiva, aunque ilustra el rango de situaciones que competen a la seguridad de redes.

Una definición de seguridad de computadoras, o ciberseguridad, que tiene aceptación general en la comunidad de investigadores y la industria es [11]):

Ciberseguridad: La protección dada a un sistema de información automatizado de manera tal de preservar o lograr los objetivos aplicables de mantener la integridad, disponibilidad y confidencialidad de los recursos de información del sistema (incluyendo hardware, software, firmware, datos y comunicaciones).

Esta definición introduce los tres objetivos fundamentales de la ciberseguridad tanto para datos, información como para servicios:

- Confidencialidad: Este término cubre dos conceptos relacionados
  - Confidencialidad de datos: Asegura que la información privada, confidencial o secreta no se haga pública o se comparta con individuos no autorizados.
  - Privacidad: Asegura que los individuos controlen o influencien qué información relacionada a ellos es recolectada y almacenada, y por quién y con quién esa información puede ser compartida.
- Integridad: Este término cubre dos conceptos relacionados:
  - Integridad de datos: Asegura que la información y los programas son cambiados solo de las maneras especificadas y autorizadas.
  - Integridad del sistema: Asegura que un sistema ejecute su función planeada sin impedimentos, libre de manipulaciones no autorizadas, sean deliberadas o inadvertidas.

- Disponibilidad: Asegura que el sistema trabaje puntualmente y no se niegue el servicio a usuarios autorizados [12].

Para evaluar las necesidades de seguridad de una organización de manera efectiva y para evaluar y escoger las políticas y productos de seguridad a aplicar, el administrador responsable de los sistemas informáticos y de las redes de datos necesita de una forma sistemática de definir los requerimientos de seguridad y caracterizar la manera de afrontar estos desafíos. Este problema presenta una dificultad considerable en sistemas de procesamiento de datos centralizados; si además agregamos el uso extendido de redes de área local y de área amplia, y las particularidades del medio industrial, los problemas se multiplican.

El abordaje sistemático para esta cuestión se define en la recomendación ITU-T X.800 La arquitectura de seguridad OSI es útil para los administradores e ingenieros como una manera de organizar la tarea de proveer seguridad. Además, debido a que esta arquitectura fue desarrollada como un estándar internacional, los fabricantes de computadoras y sistemas de comunicaciones se han encargado de desarrollar características de seguridad en sus productos y servicios que se basan en esta definición estructurada [12].

Para propósitos del trabajo presente, la arquitectura de seguridad OSI provee una vista general, aunque un poco abstracta, de muchos de los conceptos útiles sobre los que nos vamos a referir al describir y analizar la ciberseguridad de sistemas industriales. De manera breve, los conceptos principales de la arquitectura OSI son:

- **Ataque de seguridad:** Cualquier acción que comprometa la seguridad de la información propiedad de una organización.
- **Mecanismo de seguridad:** Un proceso, o dispositivo que incorpora tal proceso, que se diseñó para detectar, prevenir o recuperarse de un ataque de seguridad.
- **Servicio de seguridad:** Un servicio de procesamiento o comunicaciones que aumenta la seguridad de los sistemas procesadores de datos y las transferencias de información de una organización. Los servicios se diseñan para evitar ataques de seguridad, y se utilizan uno o más mecanismos de seguridad para proveer el servicio.

En la literatura, los términos ataque y amenaza se utilizan a menudo de manera intercambiable. Se definen de la siguiente manera [13]:

- **Amenaza:** Una violación de seguridad potencial, que existe cuando hay una circunstancia, capacidad, acción o evento que pudiera infringir la seguridad y causar daño. Es decir, una amenaza es un posible peligro que podría explotar una vulnerabilidad.
- **Ataque:** Un asalto a la seguridad de un sistema que deriva de una amenaza con inteligencia. Es decir, un acto inteligente que es un esfuerzo deliberado (especialmente en el sentido de usar un método o técnica) para evadir los servicios de seguridad y violar la política de seguridad de un sistema.

Los ataques de seguridad pueden clasificarse en términos de ataques pasivos y ataques activos [13], [14]. Un ataque pasivo intentará descubrir o utilizar información del sistema, pero no afectará los recursos del mismo. Un ataque activo por el contrario intentará alterar o afectar la operación de los recursos del sistema.

Los ataques pasivos son, en esencia, una escucha a escondidas o monitoreo, de transmisiones de datos. El objetivo del atacante es obtener la información que está siendo transmitida. Existen dos tipos generales de ataque pasivo: por un lado, está el acceso al contenido del mensaje. Una conversación telefónica, un correo electrónico o un archivo transferido pueden contener información sensible o confidencial. Es importante que se prevenga que personas no autorizadas accedan al contenido de estas transmisiones. Por otra parte, existe el segundo tipo de ataque pasivo, el análisis de tráfico. Supongamos que se tiene una manera de enmascarar el contenido de los mensajes u otra información de tráfico de manera tal que el atacante, incluso si capturara el mensaje, no pudiera extraer la información del mensaje. Esta técnica común de enmascarar el contenido de los mensajes se denomina encriptación. Si tuviéramos esta técnica implementada, un atacante aún podría observar el patrón de los mensajes. Además podría determinar la ubicación e identidad de los sistemas comunicantes, y observar la longitud y frecuencia de los mensajes intercambiados. Esta información podría ser útil para descubrir la naturaleza de esa comunicación en particular. En general, los ataques pasivos son muy difíciles de detectar, porque no involucran la alteración de datos. Típicamente, el tráfico de mensajes es enviado y recibido de manera normal, y ni el transmisor ni el receptor están al tanto de que un tercero ha leído los mensajes y observado el patrón de tráfico. Sin embargo, es posible prevenir el éxito de estos ataques, fundamentalmente a través de la encriptación. Por esto, el énfasis al lidiar con ataques pasivos es en la prevención y no en la detección.

Los ataques activos involucran alguna modificación del flujo de datos, o la creación de un flujo de datos falso, y pueden subdividirse en cuatro categorías: falsificación de

identidad, retransmisión, modificación de mensajes y denegación de servicio. Estos tipos de ataques representan el grueso de los problemas de seguridad en los sistemas industriales, debido a que es a través de ellos que pueden alterarse el estado del sistema y modificar su comportamiento. Sin embargo, veremos que muchas veces el ataque pasivo representa un escalón anterior al ataque activo, funcionando como tarea de reconocimiento previa, como preparativo o accesorio.

Un ataque de falsificación de identidad ocurre cuando una entidad pretende ser otra. Un ataque de falsificación de identidad usualmente incluye una de las otras formas de ataque activo. Por ejemplo, las secuencias de autenticación pueden ser capturadas y retransmitidas después de que una secuencia de autenticación válida ha tenido lugar, habilitando a una entidad autorizada con pocos privilegios a escalar a una identidad falsa con mayores niveles de acceso. Un ataque de retransmisión involucra la captura pasiva de unidades de datos y sus reenvíos subsecuentes para producir un efecto no autorizado. Un ataque de modificación de mensajes simplemente indica que alguna porción de un mensaje legítimo es alterado, o que los mensajes son retrasados o reordenados para producir un efecto no autorizado. Por ejemplo, un atacante podría modificar el envío de un valor de *set-point* a un controlador de caldera para configurarlo a una temperatura que destruya ese lote de producción. La denegación de servicio (DoS, *denial of* service) previene o inhibe el uso normal o la administración de alguna utilidad de comunicaciones. Este ataque puede tener un objetivo específico, por ejemplo un atacante podría intentar suprimir todos los mensajes dirigidos a un destino en particular. Otra forma de denegación de servicio es la disrupción de una red completa, ya sea deshabilitando la red o sobrecargándola con mensajes de manera tal que la performance de la red se degrade al punto de inutilizarla. Existen ataques de denegación de servicio de complejidad muy baja o nula para el atacante, haciéndolos uno de los problemas de seguridad más vistos en las redes y sistemas de todo el mundo. Además, en el caso de sistemas industriales adquieren una importancia mucho mayor, porque que un controlador o dispositivo inteligente no pueda recibir un *set-point* u orden de detención a tiempo puede significar una catástrofe. Esto está relacionado con los requerimientos de confiabilidad y latencia que introdujimos para las redes industriales en el apartado anterior.

Los ataques activos presentan las características opuestas a los ataques pasivos. Mientras que los ataques pasivos son difíciles de detectar, existen medidas que podemos tomar para prevenir su éxito. Por otro lado, es bastante difícil la prevención absoluta de los ataques activos debido a la amplia variedad de vulnerabilidades físicas, de software y de red que existen.

El enfoque típico de sistemas de IT hace foco en la detección de ataques activos, y en la recuperación de cualquier disrupción o retardo causado por ellos. Además, se considera que si la detección tiene un efecto disuasorio también contribuye a la prevención [10]. Es la opinión de este autor que este paradigma puede resultar inaplicable a sistemas industriales, debido a lo expuesto en el párrafo anterior: en sistemas críticos de tiempo, como RTOS o sistemas de control de un proceso físico, puede no existir la posibilidad de recuperación luego de un ataque. Por esto es importante el desarrollo de criterios de diseño que consideren estas posibilidades.

1.6 Servicios de seguridad

Un servicio de seguridad se define [14] como un servicio provisto por una capa de protocolos de comunicaciones que permite la seguridad de un sistema o una transferencia de datos. Alternativamente se define como [13]: un servicio de comunicaciones o procesamiento que es provisto por un sistema para dar un tipo específico de protección a recursos del sistema; los servicios de seguridad implementan políticas de seguridad y son implementados por mecanismos de seguridad. La definición de mayor uso en la industria [14] divide estos servicios en cinco categorías y catorce servicios específicos:

- El servicio de autenticación es el encargado de asegurar que una comunicación es auténtica. En el caso de un mensaje individual, tal como una advertencia o señal de alarma, la función del servicio de autenticación es asegurar al receptor que el mensaje proviene de la fuente que dice provenir. En el caso de una interacción en curso, tal como una conexión de un terminal a un sistema, dos aspectos están involucrados. Primero, en el momento del inicio de la conexión, el servicio asegura que las dos entidades sean auténticas (es decir, que cada una sea la que asegura ser). Segundo, el servicio debe asegurar que la conexión no sea interferida de manera tal que un tercero pueda falsificar su identidad como una de las partes legítimas para propósitos de recepción o transmisión no autorizadas. Se definen dos servicios específicos de autenticación [14]:

- Autenticación de entidad par: Provee corroboración de la identidad de una entidad par en una asociación. Dos entidades se consideran pares si implementan el mismo protocolo en sistemas diferentes (por ejemplo dos módulos TCP en dos sistemas de comunicación). La autenticación de entidad par se provee para su uso en el establecimiento de la conexión, o durante la fase de transferencia de datos. Intenta

proveer confianza en que la entidad no está intentando suplantar la identidad de otra, o intentando un reenvío no autorizado de una conexión previa.

- Autenticación de origen de datos: Verifica la fuente de una unidad de datos. No provee protección contra la duplicación o modificación de las unidades de datos. Soporta aplicaciones como el correo electrónico, en la que no hay interacciones previas entre las entidades comunicantes.

- En el contexto de la seguridad de redes, control de acceso es la habilidad de limitar y controlar la llegada a los sistemas y aplicaciones a través de enlaces de comunicaciones. Para lograr esto, cada entidad que trate de ganar acceso debe ser primero identificada o autenticada, de manera tal que los derechos de acceso sean personalizadas para cada entidad individual.

- La confidencialidad es la protección de los datos transmitidos contra ataques pasivos. Con respecto al contenido de una transmisión de datos se pueden identificar varios niveles de protección. El servicio más amplio protege todos los datos transmitidos entre dos usuarios por un período de tiempo. Por ejemplo, cuando se inicia una conexión TCP entre dos sistemas esta protección amplia previene el acceso al contenido de los mensajes intercambiados. También pueden definirse protecciones más específicas, como para un solo mensaje, o un campo particular dentro del mensaje. Estos refinamientos son menos versátiles que el enfoque amplio, y pueden incorporar una complejidad técnica y un costo mayor. El otro aspecto de la confidencialidad es la protección del flujo de tráfico contra el análisis. Esto implica que un atacante no tenga posibilidad de observar la fuente, el destino, frecuencia, longitud y otras características del tráfico en un canal de comunicaciones.

- Como con la confidencialidad, la integridad de datos puede aplicarse a un flujo de mensajes, a un mensaje individual, o a campos específicos dentro del mensaje. Nuevamente, la forma de mayor uso y simpleza es la protección del flujo completo. Un servicio de integridad orientado a la conexión se encarga de un flujo de mensajes y asegura que los mensajes son recibidos tal como se enviaron, sin duplicación, inserción, modificación, reordenamiento o retransmisión. Además el servicio previene contra la destrucción de datos. Por tanto, el servicio de integridad orientado a la conexión trata tanto con la modificación del flujo de mensajes como con la denegación de servicio. Por otra parte, un servicio no orientado a la conexión trata con mensajes individuales sin considerar ningún contexto, y generalmente provee una protección contra modificación del mensaje exclusivamente. Podemos además establecer una distinción entre servicios con y sin recuperación. Dado que el servicio de integridad se relaciona con ataques activos, desde el punto de vista de IT clásico nos preocupamos más por la detección que por la prevención. Si se detecta una violación de integridad el servicio puede

simplemente reportar este hecho, requiriendo un software específico o intervención humana para recuperarse de la violación, o puede tratarse de un servicio con recuperación automática. Es claro que resulta más atractiva en un contexto de uso típico la opción con recuperación automática.

- El servicio de no-repudio (*non-repudiation*) previene que tanto al receptor como al emisor les sea denegado un mensaje transmitido. Es decir que cuando un mensaje es enviado el receptor puede probar que el supuesto emisor envió efectivamente el mensaje. De manera similar, cuando un mensaje es recibido, el emisor puede probar que el receptor haya recibido el mensaje.
- La propiedad de disponibilidad se define [13], [14] como la capacidad de un sistema o un recurso de sistema de ser accesible y utilizable en función de la demanda por parte de una entidad autorizada del sistema, de acuerdo a las especificaciones de performance del sistema. Existe una variedad de ataques que pueden resultar en la pérdida o reducción de disponibilidad. Algunos de estos ataques pueden ser prevenidos con contramedidas automatizadas, tales como autenticación o encriptación, mientras que otros requieren algún tipo de acción física para prevenir o recuperarse de la pérdida de disponibilidad. Este servicio responde a los riesgos de un ataque de denegación de servicio. Depende a su vez de una buena administración y control de los recursos del sistema, y por tanto depende del servicio de control de acceso y otros.

1.7 Mecanismos de seguridad

Los mecanismos se dividen en aquellos que están implementados en una capa de protocolo específica, como TCP o un protocolo de capa de aplicación, y aquellos que no son específicos de ninguna capa de protocolo ni de ningún servicio de seguridad [14]. Los mecanismos de seguridad específicos, es decir los que pueden ser incorporados en la capa de protocolo apropiada para proveer un servicio son:

- **Cifrado**: El uso de algoritmos matemáticos para transformar los datos en una forma que no sea inteligible de manera inicial. La transformación y la recuperación de los datos dependen de un algoritmo y en algunos casos de una serie de llaves de encriptación.
- **Firma digital**: La firma es una serie de datos adjuntos a la información, o bien una transformación criptográfica de la misma. Permite que un receptor pruebe la fuente y la integridad de los datos transmitidos contra cualquier falsificación.

- **Control de acceso**: Una variedad de mecanismos que regulan que entidad, sistema o usuario pueden hacer uso de ciertos recursos.
- **Integridad de datos:** Aseguran que los datos recibidos no sean alterados o modificados en el **transporte.**
- **Intercambio de autenticación (*handshake*):** Asegura la identidad de una entidad por medio del intercambio de cierta información.
- ***Padding* de tráfico**: la inserción de segmentos de datos en el flujo de una comunicación a fin de dificultar el uso de técnicas de análisis de tráfico.
- **Control de enrutamiento:** Permite la selección de ciertas particulares físicamente seguras para algunos datos, y permite modificación a las rutas especialmente cuando se sospecha una violación de seguridad.
- **Notarización:** El uso de terceros para asegurar ciertas propiedades de un intercambio de datos.

Además existen mecanismos de seguridad que no son específicos a ningún servicio de seguridad o capa de protocolos, sino que son generalizados:

- **Funcionalidad confiable**: Propiedad de los servicios y sistemas que los hace compatibles con un criterio de seguridad, especialmente con el establecido por las políticas de seguridad.
- **Etiquetas de seguridad**: Señalan los atributos de seguridad de los recursos, que pudieran ser unidades de datos.
- **Detección de eventos**: Control permanente de sucesos esperados y no esperados que sean pertinentes a la seguridad de los sistemas, y su registro para análisis futuro.
- ***Security audit trail***: Registro cronológico, o conjunto de registros que provee evidencia documental de las secuencias de actividades que hayan afectado a la operación específica del sistema.

1.8 Aplicaciones de ciberseguridad a sistemas industriales

Los sistemas SCADA se diseñaron originalmente en la década de 1960 cuando la preocupación por las medidas y protocolos de seguridad de la información era mínimos. En aquel tiempo los sistemas operaban en un ambiente completamente aislado y confiaban principalmente en software, hardware y tecnología de comunicaciones propietarios. Los sistemas de hoy en día son distribuidos e interconectados, y dependen

de protocolos abiertos lo que los hace vulnerables a diferentes prácticas de ciberterrorismo. A fin de comprender la importancia y la urgencia de estudiar los problemas específicos de ciberseguridad de sistemas industriales, se analizan algunos casos interesantes de violaciones a la seguridad de sistemas industriales que tuvieron gran resonancia en la prensa internacional, especialmente al tratarse de sistemas de infraestructura crítica con posibles consecuencias en para grandes grupos de personas.

Históricamente los desarrolladores de sistemas SCADA basaron la seguridad de sus sistemas en dos conceptos fundamentales: por un lado redes con “espacio de aire” (air-gapped network, es decir una subred de propósito especial sin conexión en línea con las demás partes de la red) [15], y por otro lado el uso de protocolos no estandarizados, cerrados y propietarios. A medida que se produjeron demandas de usabilidad, la conexión on-line de las redes industriales con las redes corporativas y la Internet fue tomando cada vez mayor preeminencia. Este fenómeno trae aparejada la mayor apertura de los sistemas de control a ataques, particularmente desde otros partes del mundo y en especial al ser considerados objetivos muy valiosos por los atacantes debido a su alto nivel de criticidad. Además, como veremos algunos atacantes de mayor nivel de sofisticación han logrado acceder a sistemas con redes que aún mantienen el principio de establecer un air-gap como medida de protección. Los incidentes se presentan en orden cronológico.

Explosión del gasoducto transiberiano (1982)

Este es el primer incidente de ciberseguridad conocido que involucra a sistemas de infraestructura crítica. En 1982, unos intrusos instalaron un troyano en el sistema SCADA que controlaba el gasoducto transiberiano, lo cual causó una explosión equivalente a 3.000 toneladas de TNT [16].

Sistema de alerta de emergencias de Chevron (1992)

Un empleado despedido de Chevron deshabilitó el sistema de emergencia de alerta ingresando sin autorización y saltando la seguridad de servidores en Nueva York y San Jose, California, produciendo la caída del sistema. Esta situación no se detectó hasta que ocurrió una emergencia en la refinería de Chevron ubicada en Richmond, California, y el sistema no se pudo utilizar para notificar a la comunidad adyacente de la liberación al ambiente de un producto nocivo. Durante el período de diez horas en el que el sistema estuvo fuera de servicio, miles de personas en veintidós estados de EEUU y seis áreas no especificadas de Canadá fueron puestas en riesgo [17].

Proyecto Río Salado (1994)

Entre julio y agosto de 1994 un atacante ganó acceso no autorizado a la red de computadores del Proyecto Río Salado, un conglomerado que une a la cooperativa eléctrica y de mejoramiento agrícola y la cooperativa de agua potable de la ciudad de Phoenix, Arizona en EEUU. El atacante utilizó una conexión dial-up para acceder a la información de facturación, e instaló un backdoor para retener sus privilegios de acceso en el futuro. En ese momento, el sistema SCADA del Proyecto Río Salado operaba un acueducto y sistema de canales de un total de 210 Km de longitud utilizado para entregar agua potable al área metropolitana de Phoenix. El atacante mantuvo al menos una sesión de 5 horas con máximos privilegios en sistemas de misión crítica de control de los canales, accedió a los datos de monitoreo de agua y energía, y datos financieros, comerciales y personales de los clientes [18].

Aeropuerto de Worcester, Massachussets (1997)

En marzo de 1997, un atacante penetró y deshabilitó una computadora de la compañía telefónica que daba servicio al aeropuerto de la ciudad de Worcester. Como resultado el servicio de teléfono de la Administración Federal de la Aviación de EEUU, la torre de control, el departamento de bomberos del aeropuerto, el servicio de meteorología y demás se quedaron sin conexión durante seis horas. Durante el transcurso del día, el mismo atacante deshabilitó otra computadora del servicio telefónico, causando pérdidas financieras y amenazando la seguridad y la salud pública en el área de la ciudad de Rutland [17].

Gazprom (1999)

Los atacantes ingresaron a los sistemas de Gazprom, una compañía rusa de gas. El ataque se orquestó en colaboración con un elemento interno de la empresa (un empleado descontento). A través de un troyano obtuvieron acceso a la computadora que controla el conmutador central, que opera el flujo de gas en los gasoductos [19].

Oleoducto de Bellingham, Washington (1999)

En junio de 1999, 897.000 litros de combustible se filtraron de un oleoducto de 16 pulgadas de diámetro en un arroyo cercano a la ciudad. Aproximadamente luego de una hora y media de la ruptura, la nafta se incendió causando tres muertes y ocho heridos graves que se conozcan. El accidente fue causado por la incapacidad de los sistemas de control de monitorear correctamente los parámetros de la cañería. Un reporte elaborado por la National Transportation Safety Board de EEUU en octubre de 2002 cita como una de las causas principales del accidente la práctica por parte de la empresa operadora del oleoducto de realizar tareas de desarrollo de base de datos en el sistema SCADA mientras éste operaba en tiempo real sobre el oleoducto [20]. Aunque no se trate de un ataque estrictamente, la pérdida de vidas humanas en este accidente ilustra los peligros de una falla en un sistema de infraestructura crítica.

Sistema de Agua de Maroochy (2000)

En Maroochy Shire, Queensland, Australia un ex empleado descontento penetró en el sistema de control de la red de aguas y cloacas, e inundó el predio de un hotel y un río cercano con un millón de litros de agua de cloaca. Este no fue un ataque aislado, sino que fueron varias intrusiones a lo largo de un período de tiempo prolongado [21].

Cal-ISO (2001)

Un grupo de atacantes, según presumen los investigadores de origen chino, logró acceder a una de las redes de computadoras el California Independent System Operator (Cal-ISO), el ente operador del mercado eléctrico mayorista del estado de California, en mayo de 2001. Cal-ISO tiene control jerárquico sobre una serie de redes operadas por sus miembros. Este ataque no generó ningún daño directo, pero se extendió por un período superior a dos semanas [22].

Planta de energía nuclear Davis-Besse (2003)

En enero de 2003, el gusano SQL Slammer infectó la planta de energía ubicada en Ohio, EEUU. Como resultado de la infección, el sistema de monitoreo de parámetros de seguridad y la computadora de procesos de planta estuvieron fuera de línea durante varias horas [19].

Corporación CSX (2003)

En un caso similar al anterior, un virus denominado Sobig desactivó los sistemas de señalización de la red ferroviaria en Florida, EEUU. Este virus explotó con gran éxito la propagación como archivo adjunto de email, siendo uno de los que llegó a mayor velocidad de expansión en su época. Deshabilitó los sistemas de señalización, despacho y otros de la corporación CSX, uno de los más grandes proveedores de servicio de transporte en los EEUU. Sin embargo, el único daño que causó fue la demora en la salida de algunos trenes [23].

Tehama Colusa Canal Authority (2007)

Un supervisor técnico de la junta de empresas de agua potable de California Tehama Colusa Canal Authority (TCAA) instaló software no autorizado en el sistema SCADA. Según el relato oficial, el empleado fue despedido luego de 17 años, y en su último día de trabajo introdujo el software extraño. La TCAA no reveló datos ni análisis del software, ni tampoco si se produjo algún incidente a causa de este hecho [23].

Stuxnet (2010)

En junio de 2010 se descubrió que un gusano denominado Stuxnet había ingresado en la instalación nuclear de Natanz, en Irán. El gusano utilizó cuatro vulnerabilidades zero-day para obtener privilegios, así como las contraseñas por defecto de Siemens para acceder a las computadoras que corren WinCC y PCS7, las aplicaciones SCADA de bandera de la empresa. Su objetivo era hallar los conversores de frecuencia marca Fararo Paya (Irán) y Vacon (Finlandia), que alimentaban los centrífugos utilizados para el enriquecimiento de la concentración del isótopo uranio-235. Alterando los parámetros de frecuencia de los conversores logro una condición de funcionamiento anormal que hizo fallar a los centrífugos a mayor frecuencia que lo normal [24].

Night dragon (2011)

En febrero de 2011 la empresa de seguridad McAffee reportó que cinco empresas mundiales de energía y petróleo estaban siendo atacadas con una combinación de ingeniería social, troyanos y vulnerabilidades de Windows. Los ataques, denominados “Night dragon” por los investigadores, se mantuvieron durante más de dos años y

especulan que sean de origen chino. Puede ocurrir que simplemente los atacantes hayan estado utilizando computadoras chinas comprometidas y software de ataque chino para enmascarar su verdadera identidad. Aunque no se atacó directamente a ningún sistema SCADA, los segmentos de red corporativa que fueron objetivo de los agresores pertencen a compañías que operan grandes sistemas industriales. Los atacantes se concentraron en el robo de información, en particular planos técnicos de operaciones, constituyendo un caso de ciberespionaje industrial [23].

DUQU (2011)

En 2011 una serie de investigadores especializados en virus encontraron una nueva forma de malware que utilizaba varias de las técnicas innovadoras que antes habían solo vistas en Stuxnet. Se denominó Duqu, y no era autoreplicante ni tenía una carga útil. Aparentemente habría sido diseñado para llevar a cabo tareas de reconocimiento en un sistema de control industrial desconocido [25].

Flame (2012)

Algunos grupos de investigación descubrieron un malware especial operativo en zonas de Irán, Líbano, Siria, Sudán y otras partes del medio oriente y noráfrica durante al menos dos años. Este malware denominado “Flame” aparentemente ha sido generado por el mismo grupo detrás de Stuxnet. Los análisis tempranos indicaron que su función principal era espiar a los usuarios, robando datos, credenciales, documentos, conversaciones, etc. Además mantenía una comunicación con servidores centralizados de comando y control que permitían a los atacantes modificar y aumentar las capacidades del malware. [26]

La lista precedente, si bien es claramente incompleta, sirve para dimensionar algunos de los riesgos a los que las organizaciones se exponen al no considerar las cuestiones de seguridad de manera integral, sienta un precedente y justifica el esfuerzo de investigación en el área.

2. Objetivos

1) Ofrecer un informe del estado del arte de los métodos de análisis de seguridad de redes y sistemas industriales, pruebas de penetración y caracterización de vulnerabilidades y superficies de ataque.

2) Efectuar una evaluación de vulnerabilidades de sistemas industriales expuestos a Internet: utilizando las herramientas shodan.io, nmap y metasploit, se efectuará un reconocimiento de red consistente en una exploración de puntos de presencia en Internet, identificación de servicios y análisis de vulnerabilidades simple en dispositivos de campo como PLC, interfaces hombre-máquina, *drives AC*, y otros.

3) Identificar y caracterizar los riesgos más significativos y las superficies de ataque de los sistemas en el contexto estudiado.

3. Materiales y métodos

Una evaluación de vulnerabilidades es una etapa inicial de un test de penetración, cuyo objeto es ejecutar un mapeo de la red y los sistemas conectados, identificar los servicios y versiones que ejecutan, y catalogar los sistemas vulnerables [27].

Inicialmente se comentarán los elementos fundamentales de la metodología de tests de penetración, para luego acotar la misma al nivel de análisis de vulnerabilidades, que corresponde al alcance del estudio presente. Los limitantes fundamentales son los riesgos de los tests de penetración y las implicaciones legales debido a que un test de penetración sin un acuerdo explícito con la organización analizada constituye un ataque, y en menor medida de orden práctico debido a que la gran cantidad de objetivos encontrados expuestos en Internet requeriría de un tiempo y esfuerzo que excede el alcance del presente trabajo para que se haga un análisis exhaustivo sobre cada uno de ellos [28].

3.1 Metodología general de tests de penetración

El test de seguridad fundamental para redes y sistemas interconectados, conocido en la jerga como test de penetración, o *pentesting*, es un proceso de abundante complejidad y muy variable, por lo que se resiste su sistematización. Requiere mucha participación por parte del ejecutor, o *tester*, y es muy dependiente de la experiencia y conocimiento del mismo. Además, como se menciona en el párrafo anterior, existe un sinfín de cuestiones legales a tener en cuenta cuando se encaran los análisis de seguridad, fundamentalmente si se trata de auditorías externas. Los posibles problemas

legales escapan al alcance de este trabajo y por tanto no serán estudiados aquí, si no que se limitará la discusión a lo estrictamente técnico [29].

Como se comentaba en el apartado anterior, un test de seguridad consta de dos tipos de ataque. Un ataque pasivo, generalmente lo que hace es recolectar datos de manera tal que no influencia o invade el sistema o red objetivo. Un ataque activo, o intrusivo, intenta invadir el sistema, y puede ser detectado y registrado [30].

El proceso de un test de seguridad se concentra en evaluar las siguientes áreas[31]:

- Visibilidad: La visibilidad es lo que puede ser visto de la presencia en redes abiertas (especialmente Internet) de la organización objetivo del test. Esto incluye puertos abiertos o filtrados, sistemas y tipos de sistemas, arquitectura, aplicaciones, direcciones de email, nombres de empleados, productos de seguridad utilizados, sitios visitados por los empleados, etc. Estos datos y otros forma la “huella digital” de la organización, y pueden usarse como punto de partida para diseñar un ataque.
- Acceso: El acceso se constituye de la suma de los servicios que ofrece la organización al público a través de redes abiertas. Incluye páginas web, e-business, servidores DNS, video streaming, y cualquier otro servicio o aplicación con capacidad de ser accedido remotamente e interactuar con otras computadoras dentro de la red privada. En el caso de sistemas industriales, las capacidades de acceso remoto para supervisión, configuración, lectura de datos y estadísticas para el sector de negocio de la organización, soporte del fabricante, y otros puntos de ingreso a la red industrial, implican un vector muy significativo en la estructura de seguridad. Limitación de acceso significa controlar todos los vectores y denegar todo punto de acceso excepto aquellos que están expresamente justificados en el plan de negocios de la organización.
- Confianza: La confianza (*trust*) es el concepto más importante en seguridad de Internet. Es una medida de cuánto pueden depender las personas de lo que ofrece el sistema. La confianza depende del tipo y nivel de autenticación, no repudio, control de acceso, confidencialidad, integridad de datos y otros mecanismos de seguridad implementados por el sistema. En algunos casos la confianza es la base del servicio, por ejemplo en el caso de sistemas intermediarios de información. Por ejemplo, servidores que implementan conectores VPN, PKI, SSH, conexiones de servidor a base de datos, o cualquier otra comunicación entre dos computadoras que cause interdependencia entre ellas.
- Alarma: Es la notificación apropiada y a tiempo de actividades que violen o intenten violar la visibilidad, acceso, o confianza de una organización. Por ejemplo,

análisis de archivos de registro, monitoreo de tráfico, sistemas de detección de intrusión. A menudo la alarma es el eslabón más débil entre las medidas de seguridad.

3.1.1 Parámetros de análisis

La metodología se divide en parámetros y tareas. Los parámetros no deben entenderse en el sentido matemático de la palabra, sino que representan el flujo de la metodología desde un punto de presencia hacia el siguiente. Cada parámetro tiene una entrada y una salida, consistentes de la información que consume y devuelve cada etapa. La salida de uno puede ser en algunos casos datos que sirvan de entrada para otro parámetro. En este caso se denomina inteligencia. Inclusive puede tratarse de un dato que alimente a varios otros parámetros, tales como direcciones IP o nombres de dominio. Algunas tareas no devuelven ninguna salida, esto significa que existirán parámetros para los cuales no hay entrada. Estos pueden ser ignorados durante el proceso de test. No son indicativos de un test inferior, sino que puede ser que indiquen un nivel superior de seguridad. Los parámetros que no tengan salida pueden significar una de tres cosas: las tareas no se ejecutaron correctamente, las tareas demostraron un nivel de seguridad superior al esperado, o los datos resultantes de las tareas han sido analizados equivocadamente.

La cantidad de tiempo que se invierte antes de dar por finalizada una tarea y considerar los datos de salida como finales, depende del alcance del análisis. Un test apropiado es un balance de tiempo, dinero, mano de obra y recursos computacionales a invertir por parte de la organización[32].

El análisis de seguridad es un esfuerzo estratégico. Aunque puede haber diferentes métodos y herramientas para verificar los mismos parámetros, hay pocas variaciones en cuanto al orden en el que deben ser ejecutados los test. Algunos de los parámetros mencionados en esta lista no son puntos de presencia en Internet, aunque se mencionan de igual manera por la importancia que tienen para la seguridad.

A continuación se ofrece una lista de los parámetros fundamentales. Muchos de los nombres se muestran en inglés debido a la importancia de mantener la coherencia con la literatura internacional:

1. Reconocimiento/inspección de redes
2. *Portscanning*

3. *Fingerprinting* de sistemas
4. Fugas en redes inalámbricas
5. Prueba de servicios: web, mail, servidores de nombre, documentos visibles, antivirus y antimalware.
6. Verificación de vulnerabilidades automatizado redundante
7. Investigación de *exploits* preexistentes.
8. Verificación de vulnerabilidades manual
9. Test de aplicaciones
10. Test de *firewall* y listas de control de acceso (ACL)
11. Revisión de política de seguridad
12. Test de IDS (sistemas de detección de intrusiones)
13. Test de PBX (*wardialing*)
14. Verificación de documentación descartada
15. Ingeniería social
16. Verificación de sistemas confiables
17. *Password cracking*
18. Test de denegación de servicio
19. Revisión de política de privacidad
20. Análisis de seguridad web y *cookies*
21. Revisión de registros de servidores e IDS

Esta metodología fluye desde el reconocimiento inicial de la red, hasta el reporte final. Debe tenerse en cuenta una separación entre las etapas de recolección de datos y verificaciones y test de los datos recolectados, y a partir de ellos. También debe tenerse en claro los puntos precisos para la inserción y extracción de datos en el flujo.

Al definir la metodología de test, es importante no constreñir la creatividad del *tester* mediante la introducción de estándares muy formales o estrictos de manera tal que la calidad del análisis se vea afectada. Hay que tener en cuenta que el análisis de ciberseguridad trata con un objeto de estudio muy impredecible, por lo que la flexibilidad metodológica es de suma importancia. Por ejemplo, en el ítem de verificación de encriptación no se especifica qué técnicas deben ser usadas para verificar, ni de qué encriptación estamos hablando. Esto permite que se contemplen los conceptos de manera amplia e incorpora espacio para la variabilidad. Este punto es especialmente importante durante el testeo de vulnerabilidades, debido a la naturaleza dinámica de los *exploits*.

Como se comentaba en el párrafo anterior, cada parámetro se relaciona con el anterior y con el posterior en la estructura del método. El test de seguridad comienza con una entrada que es fundamentalmente la dirección de cada uno de los sistemas que componen la red a verificar. De igual manera, el test termina con el inicio de la etapa de análisis, sumarización e interpretación de la información y el reporte final.

Las tareas son las pruebas individuales relacionadas con la seguridad que se ejecutarán, dependiendo de la entrada para cada parámetro. Los resultados de la tarea pueden ser analizados inmediatamente y considerarse un resultado procesado, o dejarse en “crudo”. De cualquier manera se consideran la salida del parámetro correspondiente La salida a menudo es considerada la entrada del parámetro siguiente, o en algunos casos como por ejemplo si se descubrieran nuevos nodos o *hosts* en la red, pueden ser la entrada de otro parámetro previo. Algunos parámetros se denominan “no tradicionales”, en el sentido de que pueden existir condiciones bajo las cuales los componentes a testear no definan un punto de presencia en Internet. Por ejemplo, una LAN inalámbrica puede filtrarse más allá de las inmediaciones del sitio de la organización, constituyendo un punto de acceso liberado a recursos restringidos, pero por la cuestión del rango de la señal inalámbrica no puede considerarse un acceso público del mismo nivel que un servicio en Internet. Estos puntos son importantes sin embargo, y deben ser considerados en el test y análisis.

Existe una interdependencia entre muchos parámetros, pero no entre todos. Esto permite que muchas pruebas individuales puedan ejecutarse en paralelo. Es importante verificar de antemano las posibilidades de interdependencia para diseñar un plan de pruebas acorde.

3.1.2 Reconocimiento de red[33]

Un reconocimiento de red sirve como una introducción a los sistemas a ser estudiados. Es una combinación de recolección de datos y análisis de la información. Aunque a menudo es recomendable desde un punto de vista legal definir contractualmente con exactitud qué sistemas serán testeados, tanto si se trata de una auditoría externa como interna, lo típico es que no se tengan a disposición nombres de *host* o direcciones IP. En este caso el reconocimiento de red cobra mayor importancia aún. El punto de esta tarea es encontrar los sistemas alcanzables a ser testeados, teniendo siempre en consideración los límites legales de la operación.

Es normal que se detecten muchos objetivos a medida que progresan las etapas del método. En este caso, estos datos son realimentados a las etapas anteriores y sus resultados son compilados junto con el resto. Puede requerir flexibilizar el flujo de trabajo para incorporar la nueva información previamente oculta, y hasta modificar los objetivos descartando o agregando hipótesis.

Se espera que un reconocimiento de red devuelva la siguiente información:

- Nombres de dominio
- Nombres de servidores
- Direcciones IP
- Mapa de redes
- Información de ISP
- Propietarios de sistemas y servicios
- Posibles límites del test

Tareas a ejecutar:

Respuestas de servidores de nombre

- Examinar información de registro de dominios
- Buscar bloque IP propiedad de la organización
- Verificar las respuestas de servidores de nombre primarios, secundarios y de ISP

Superficie exterior de red

- Utilizar trazas múltiples hacia la puerta de enlace para definir la capa exterior de la red y *routers*

Examinar pistas de la organización

- Buscar logs web y logs de intrusión con trazas de la red objetivo

Fugas de información

- Examinar código fuente de sitios web y scripts de la organización buscando links internos y servidores de aplicación

- Examinar cabeceras de email, email rechazados y confirmaciones de lectura a la búsqueda de trazas de servidores.
- Examinar grupos de noticias y redes sociales
- Buscar bases de datos de búsqueda de trabajo, buscando posiciones de IT para la organización, relacionadas a hardware y software. Este ítem es especialmente importante en el caso de tests a sistemas industriales.

3.1.3 *Portscanning*[34]

Portscanning, o exploración de puertos es el sondeo invasivo de los puertos del sistema a nivel de capa de transporte y capa de red. Se incluye también en esta tarea la validación de la recepción del sistema a protocolos bajo túneles, encapsulamiento y de enrutamiento. Este parámetro enumera los servicios “vivos” o accesibles desde Internet, como también más allá del *firewall*. Cada dispositivo con conectividad IP soporta 65536 puertos TCP y UDP. Existen diferentes criterios para reducir el número de puertos a sondear, pero deben aplicarse cuidadosamente y siempre dando prioridad a que la información sea lo más completa posible.

Los resultados esperados de esta tarea son:

- Puertos abiertos, cerrados o filtrados
- Direcciones IP de sistemas en línea
- Lista de protocolos de túnel y encapsulamiento descubiertos
- Lista de protocolos de enrutamiento soportados
- Servicios activos
- Mapa de redes

Tareas a ejecutar:

Verificación de errores

- Comprobar pérdida de paquetes en la ruta a la red objetivo
- Medir el *round trip time* de paquetes
- Medir la relación de aceptación y respuesta de paquetes en la red objetivo
- Medir la cantidad de denegación de conexiones en la red objetivo

Enumeración de sistemas

- Recolectar respuestas de broadcast de la red objetivo
- Sondear más allá del firewall con paquetes de TTL específico (*firewalking*) para todas las direcciones IP
- Utilizar ICMP y verificaciones de nombre reverso para determinar la existencia de todos los *hosts* de la red
- Utilizar puerto de origen 80 y bandera ACK en los puertos de destino 3100-3150, 10001-10050, 33500-33550 y 50 puertos aleatorios por encima de 35000 para sondear todos los *hosts* de la red. De esta manera se logra enmascarar el sondeo como respuestas legítimas de servidores web, engañando reglas poco rigurosas de filtrado.
- Utilizar fragmentos TCP en orden inverso con escaneos de tipo FIN, NULL y XMAS a los puertos 21,22,25,80 y 443 para todos los *hosts* de la red
- Utilizar pruebas TCP SYN a los puertos 21, 22, 25, 80 y 443 para todos los *hosts*.
- Utilizar intentos de conexión DNS en todos los *hosts*
- Utilizar saltos a través de proxy y FTP para ejecutar verificaciones dentro de la DMZ en puertos 22, 81, 111, 132 137 y 161 para todos los *host*

Enumeración de puertos

- Utilizando paquetes TCP SYN (conexión semi abierta) enumerar los puertos de cada sistema como abierto, cerrado o filtrado
- Utlizar fragmentos TCP en orden inverso para enumerar puertos y servicios de un subconjunto de puertos.
- Utlizar escaneo UDP para enumerar puertos como abierto o cerrado. Primero es recomendable hacer una verificación de filtrado con un subconjunto pequeño, dependiendo de los recursos disponibles.

- Verificar y explorar el uso de los siguientes protocolos de túnel y encapsulamiento: SMB-over-IP, NBT, IPX, RPC, DCE RPC, PPTP, L2TP, IP-over-IP, SNMP, GRE, IPSEC y Radius.
- Verificar y explorar el uso de los siguiientes protocolos de enrutamiento: ARP, RIP, OSPF, LSA y BGP

3.1.4 *Fingerprinting* de sistemas[35]

Se denomina *fingerprinting* al sondeo activo de un sistema, buscando obtener respuestas específicas que puedan distinguir entre diferentes sistemas operativos y versiones.

Tareas a ejecutar:

1. Examinar respuestas del sistema para determinar tipo de sistema operativo, versión y nivel de parches instalados.
2. Examinar respuestas de aplicaciones para determinar versiones y nivel de parches.
3. Verificar la predicción de números de secuencia TCP para cada *host* vivo en la red
4. Examinar fugas de información de sistemas y aplicaciones instaladas en grupos de noticias y otros sitios de Internet
5. Comparar la información indirecta obtenida de Internet con las respuestas del sistema

3.1.5 Sondeo de servicios[36]

El sondeo de servicios es el probado activo de las aplicaciones escuchando detrás de cada puerto. En algunos casos, puede existir más de una aplicación por cada servicio, por ejemplo si una cumple el rol de *listener* y las otras funcionan como otros componentes. Esta situación es recurrente por ejemplo en bases de datos, o sitios web con soporte para algunos lenguajes de scripts.

Resultados esperados: Tipos de servicios, tipos de aplicaciones de servicios y nivel de patch, mapa de red.

Tareas a ejecutar: Identificar cada puerto abierto con un servicio y un protocolo

Identificar el *uptime* de los hosts

Identificar, si existe, el atraso entre versiones de las aplicaciones instaladas y las últimas versiones disponibles

Verificar las aplicaciones detrás de cada servicio y el nivel de patch por medio de análisis de *banners* de servicio

Identificar los componentes externos de cada servicio

3.1.6 Exploración automatizada de vulnerabilidades

Buscar vulnerabilidades utilizando herramientas automáticas es una manera eficiente de determinar agujeros de seguridad existentes y niveles de parche del sistema. Aunque muchos *scanners* automáticos existen en el mercado hoy día, es importante que el *tester* identifique e incorpore los últimos desarrollos a las pruebas[j].

Resultados esperados: lista de vulnerabilidades del sistema
Tipo de aplicaciones y servicios por vulnerabilidad
Niveles de patch de sistemas y aplicaciones

Tareas a ejecutar:

1. Medir la organización del objetivo contra herramientas populares de exploración
2. Intentar determinar vulnerabilidades por tipo de sistema
3. Intentar identificar vulnerabilidades por aplicación
4. Intentar determinar tipo de aplicación y servicio por vulnerabilidad
5. Es recomendable hacer una exploración auomática cruzada con al menos 2 herramientas diferentes

3.1.7 Investigación de *exploits*

Este parámetro cubre la investigación básica involucrada en encontrar vulnerabilidades hasta la entrega del reporte. Es importante hacer esta distinción porque por la naturaleza dinámica de la comunidad investigadora de vulnerabilidades pueden aparecer en cualquier momento. Además es importante incluir en la búsqueda no solo las bases de datos web generales y específias de los sistemas a verificar si no también canales heterodoxos como IRC, grupos de noticias y sitios FTP.

Resultados esperados: niveles de patch de sistemas y aplicaciones

Lista de posibles vulnerabilidades de denegación de servicio

Tareas a ejecutar:

1. Identificar todas las vulnerabilidades de acuerdo a las aplicaciones

2. Identificar todas las vulnerabilidades de acuerdo a los sistemas operativos

3. Identificar todas las vulnerabilidades para sistemas similares o acordes que pudieran también afectar a los sistemas objetivos.

3.1.8 Exploración manual de vulnerabilidades y verificación de resultados automatizados

Este parámetro es necesario para filtrar falsos positivos de la exploración automatizada, expandir el alcance del estudio, descubrir el flujo de datos hacia dentro y fuera de la red, y encontrar vulnerabilidades que las herramientas automáticas pasen por alto.

Resultados esperados:

Lista de áreas aseguradas por “oscuridad”

Acceso visible

Lista de vulnerabilidades verificadas, es decir sin falsos positivos

Lista de sistemas internos y DMZ

Lista de convenciones de nombre, email y servidores

Mapa de red

Tareas a ejecutar

Verificar todas las vulnerabilidades encontradas durante la fase de investigación de *exploits*

Verificar todos los positivos obtenidos en etapas anteriores.

Es importante tener en cuenta que durante esta fase hay una probabilidad importante de que las vulnerabilidades se comprueben mediante su explotación. Esto

significa que la seguridad de los sistemas será violada efectivamente, por ejemplo causando una denegación de servicio. Debe verificarse de antemano los detalles contractuales y planificarse las posibles salidas de servicio con anticipación y acuerdo de las partes.

3.1.9 Exploración de aplicaciones[37]

Este parámetro se refiere a la verificación de aplicaciones accesibles desde Internet. A menudo se trata de scripts que proveen un proceso de negocio, y puede tener mecanismos de acceso de muchos tipos diferentes.

Resultados esperados:

1. Lista de aplicaciones
2. Lista de componentes de aplicación
3. Lista de vulnerabilidades
4. Lista de sistemas confiables para cada aplicación

Tareas a ejecutar:

1. Descomponer las aplicaciones en sus partes de ser necesario para el análisis
2. Examinar el proceso de cada aplicación
3. Verificar los mecanismos de saneamiento de entrada de las aplicaciones
4. Examinar las salidas de las aplicaciones
5. Examinar las relaciones de confianza y comunicaciones
6. Determinar los límites de autenticación y control de acceso
7. Medir las limitaciones de las variables definidas
8. Examinar el uso de caché

3.1.10 Sondeo de Firewall y Listas de control de acceso[38]

El *firewall* y el enrutador de filtrado son dos defensas encontradas a menudo en redes corporativas. Su función es controlar el flujo de tráfico entre la red interna y la Internet. Ambas operan en base a una política de seguridad y se basan en listas de control de acceso (ACL). Este parámetro está diseñado para asegurar que solamente aquello que esté expresamente permitido pueda cruzar hacia la red interna, y todo lo demás sea denegado. Sin embargo lograr esta tarea puede ser difícil cuando no existe una política de seguridad explícita en la organización, y el *tester* puede encontrarse haciendo asunciones acerca del nivel de riesgo aceptable. Esto no es parte del rol ni del alcance de un análisis de seguridad, sino que es encontrar los límites de las defensas de red tanto en aplicaciones como en servicios.

Resultados esperados:

Información del firewall como servicio y como sistema

Información de enrutadores como servicio

Contorno de la política de seguridad de redes por ACL

Lista de tipos de paquetes que pueden entrar a la red

Lista de tipos de protocolos con acceso a la red interna

Lista de sistema en línea encontrados más allá del firewall

Tareas a ejecutar:

Verificar el tipo de firewall con información recolectada a través de inteligencia

Verificar tipos de enrutadores y configuraciones

Probar las ACL contra la política de seguridad o contra una regla “denegar todo”

Probar que el firewall filtra también el tráfico saliente y no solo el entrante (*egress filtering*)

Probar que el firewall o enrutadores filtran paquetes con direcciones falsificadas (*spoofing*)

Verificar las penetraciones completadas a través de exploración inversa en el parámetro de exploración de puertos

Verificar las penetraciones con paquetes con TTL estratégicamente calculado (*firewalking*) completadas en el parámetro de exploración de puertos

3.1.11 Sistemas de detección de intrusión (IDS)[39]

Esta prueba está enfocada en la performance y la sensibilidad de los IDS que se ejecutan en la red. Una parte importante de ella es difícil de lograr sin acceso a los log de IDS. Otras partes están sujetas a otras variables, como ancho de banda del atacante, distancia en saltos y latencia.

Resultados esperados:

Tipo de IDS

Peformance del IDS bajo alta carga

Tipos de paquetes no verificados por el IDS

Tipos de protocolos no verificados por el IDS

Tiempo de reacción del IDS

Sensibilidad del IDS

Mapeo de reglas del IDS

Tareas a ejecutar:

Verificar el tipo de IDS con información recolectada en la exploración de inteligencia

Verificar las reacciones configuradas para muchos y variados ataques

Verificar las reacciones configuradas para URLs ocultas

Verificar las reacciones configuradas a ajustes en el volumen de tráfico en el envío de paquetes

Verificar las reacciones configuradas a ajustes en el puerto de origen

Verificar la habilidad del IDS de manejar paquetes fragmentados

Verificar los estados de alarma

Verificar la sensibilidad de detección de firmas en ventanas de tiempo de varias longitudes

Verificar el efecto y las reacciones del IDS contra diferentes direcciones de origen

3.1.12 Verificación de sistemas confiables

El propósito de este test es afectar la presencia en Internet de la red o la organización objetivo a través de suplantar la identidad de un sistema confiable. Es difícil de lograr en la práctica. Conceptualmente, este parámetro reside a media distancia entre el test de vulnerabilidades y el test de Firewall.

Tareas a ejecutar:

Verificar posibles relaciones determinadas a partir de recolección de inteligencia, sondeo de aplicaciones y servicios

Verificar las relaciones entre varios sistemas falsificando direcciones de origen o buscando disparar eventos especiales

Verificar qué sistemas pueden ser falsificados

Verificar qué aplicaciones pueden ser falsificadas

3.1.13 Password cracking[40]

Este parámetro hace referencia al proceso de validar la fortaleza de las contraseñas usadas en el sistema a través de herramientas que exponen algoritmos criptográficos débiles, implementación incorrecta de los algoritmos, o contraseñas débiles debido a factores humanos. No debe confundirse con captura de contraseñas a través de escucha en canales de texto plano, que puede ser más simple pero prueba un aspecto diferente de la seguridad del sistema. Ocurre a menudo en la práctica que resultan útiles también pruebas manuales con combinaciones derivadas de información personal de los usuarios. En caso de obtener archivos de contraseña encriptados, es posible intentar ataques de fuerza bruta en función del tiempo y recursos computacionales disponibles, pero para servicios en línea, como Telnet o ssh resulta demasiado engorroso debido a los valores de timeout de la entrada de datos.

Es importante hacer notar que en el caso de sistemas industriales, que suelen ser instalados y configurados por personal sin formación en seguridad informática, y además que suelen confiar la seguridad del sistema en su totalidad a la inaccesibilidad, es muy común encontrar contraseñas débiles, por defecto o directamente inexistentes como veremos más adelante.

Resultados esperados

1. Archivo de contraseñas, encriptado o en texto plano
2. Lista de ID de login con contraseñas de usuario o del sistema
3. Lista de sistemas vulnerables a este tipo de ataques
4. Lista de documentos o archivos vulnerables
5. Lista de sistemas con usuarios o ID de login del sistema usando las mismas contraseñas

Tareas ejecutar

1. Obtener el archivo de contraseñas del sistema
2. Ejecutar un ataque de diccionario sobre el archivo
3. Ejecutar un ataque de fuerza bruta en función del tiempo y recursos disponibles
4. Utilizar las contraseñas obtenidas para acceder a sistema adicionales y aplicaciones

5. Verificar el envejecimiento de las contraseñas

3.1.14 Pruebas de denegación de servicio [41]

La denegación de servicio (*denial of service, DoS*) es una situación en la que una circunstancia intencional o accidental previene el funcionamiento correcto del sistema y el cumplimiento de su labor esperada. En algunos casos, el sistema puede estar trabajando de manera correcta pero una sobrecarga, o parámetros extraños, que impiden que dé respuesta a nuevas solicitudes a tiempo. Nuevamente estamos ante un ensayo que puede resultar peligroso para la organización, por lo que resulta fundamental el planeamiento y monitoreo muy cercano de las actividades.

Resultados esperados

Lista de puntos débiles en la presencia en Internet, incluyendo puntos únicos de fallo

Establecer un nivel basal de uso normal

Listar comportamientos del sistema bajo carga alta

Listar sistemas vulnerables a DoS

Tareas a ejecutar:

Verificar que las cuentas administrativas, archivos de sistema y recursos estén apropiadamente asegurados y todo acceso se provea siempre considerando el criterio de mínimos privilegios

Chequear las restricciones de exposición de los sistemas a redes no confiables

Verificar que las líneas de base establecidas sean adecuadas para la actividad normal del sistema

Verificar qué procedimientos están establecidos para responder a actividad irregular del sistema

Comprobar funcionamiento de servidores y redes bajo cargas altas

3.1.15 Revisión de logs de IDS y servidores

La revisión de los logs de servidores es necesaria para verificar las pruebas ejecutadas en los puntos de presencia en Internet, especialmente en casos en los que los resultados de los tests no son inmediatamente visibles para el tester. Para el analista que no tiene acceso a los logs quedan muchos interrogantes sin responder.

Resultados esperados:

1. Lista de falsos positivos de IDS
2. Lista de alarmas no detectadas de IDS
3. Lista de paquetes que entraron a la red por número de puerto
4. Lista de protocolos que entraron a la red
5. Lista de caminos sin monitoreo hacia la red

Tareas a ejecutar:

1. Verificar el proceso de log del firewall, IDS y servidores
2. Relacionar alertas de IDS con exploraciones de vulnerabilidades
3. Relacionar alertas de IDS con *password cracking*
4. Relacionar alertas de IDS con pruebas de sistemas confiables
5. Verificar exploraciones de puertos TCP y UDP con logs de servidores
6. Verificar exploraciones automáticas de vulnerabilidades con logs de servidores
7. Verificar deficiencias de log de servicios

3.2 Metodología de detección

La metodología de detección utilizada en este estudio se diseñó específicamente para el mismo. Partiendo del proceso de test de penetración explicado en la sección 3.1 se lo adaptó para cumplir con una serie de requisitos

Requisitos:

- Bajo nivel de intrusividad: debido a que no existe una relación contractual con las organizaciones o personas propietarias de los sistemas que son objeto de análisis en este estudio, las pruebas efectuadas deben limitarse a obtener información pública, recolección pasiva de datos y mantener la cantidad de pruebas activas al mínimo.
- Tiempo de ejecución por objetivo reducido: el universo de objetivos esperado es de muy gran volumen, al tratarse de sistemas expuestos a Internet. Esto significa que por cuestiones prácticas no se pueden ejecutar pruebas exhaustivas.
- Capacidad de automatización: al igual que el caso previo, este requisito está relacionado al gran volumen de objetivos esperado.

En base a estos criterios se seleccionó un grupo de pruebas, de manera tal que el diagrama de proceso del estudio es el siguiente:

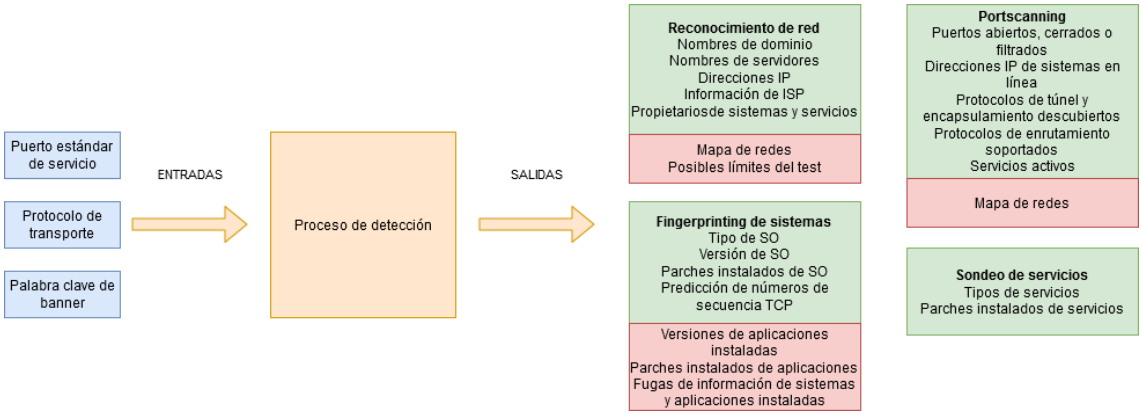

Figura 6 - Diagrama de proceso de detección

El diagrama muestra los parámetros de entrada y salida del proceso de detección diseñado para este estudio. Los parámetros de salida son los detallados en la sección 3.1, agrupados según la tarea a la que pertenecen. Los recuadros verdes muestran los parámetros de interés que entran dentro del alcance de este estudio. Los parámetros recuadrados en rojo se descartan, debido a que no cumplen con los criterios detallados en el punto anterior y por lo tanto exceden el alcance de este trabajo.

Los parámetros de entrada son:

- Puerto estándar de servicio: es normal que en redes seguras los sistemas sensibles se diversifiquen, o configuren para trabajar en puertos no estándar. Por este motivo hallar servicios críticos trabajando en sus puertos por defecto constituye un indicio de una red probablemente poco segura.
- Protocolo de transporte: debido a la dificultad y baja confiabilidad de la detección en UDP, este parámetro se fija para todos los análisis de este estudio en TCP.
- Palabra clave de banner: el análisis de banners o “banner grabbing” es uno de los métodos más utilizados para identificación de servicios remotos. El método consiste en establecer una conexión al servicio o aplicación remota para luego enviar diferentes “estímulos” y evaluar las respuestas. Mediante una clasificación de las respuestas y una base de conocimiento pueden inferirse detalles de la implementación del servicio remoto, como ser fabricante, versión, sistema operativo, arquitectura, etc. En algunos casos estos datos funcionan como antecedentes para el análisis de vulnerabilidades, y en otras pueden ser directamente evidencia de un sistema vulnerable [42].
-

3.2.1 Análisis de vulnerabilidades de dispositivos expuestos a Internet

Como se comentaba en la sección 1, para que la arquitectura de una red industrial sea considerada segura, las subredes de servidores SCADA, bases de datos, dispositivos de campo y todos los demás equipos que provean servicios de control y auxiliares deben segmentarse y aislarse de las subredes comerciales y administrativas. Resulta particularmente importante que se aíslen además de todos los equipos que tengan acceso a Internet.

A través de las herramientas mencionadas en la sección 2, se efectúa un reconocimiento de red en Internet, a la búsqueda de sistemas específicos industriales. La primer herramienta utilizada es el motor de búsqueda online Shodan.io. Shodan es un *web-crawler* de dispositivos conectados a Internet, orientado principalmente al descubrimiento de nodos IoT, SCADA, y otros sistemas. Para esto utiliza diferentes técnicas de *crawling* que obtienen banners de servicios online en puertos comunes y otros metadatos, almacenándolos en una base de datos y correlacionándolos con información geográfica y corporativa para trazar un mapa de los sistemas conectados e identificar protocolos y tipos de dispositivos. Estos metadatos incluyen información acerca del software de los servidores, opciones soportadas por los servicios, mensajes de bienvenida o cualquier otro dato que el cliente puede obtener antes de interactuar

con el servidor. Shodan recolecta datos mayoritariamente de servidores web (HTTP/HTTPS en puertos 80, 8080, 443, 8443), FTP/SFTP (puerto 21), SSH (puerto 22), telnet (puerto 23), SNMP (puerto 161), y otros, aunque la base de puertos testeados ha crecido mucho a medida que el sistema ha progresado en el tiempo.

A fin de tener mayor flexibilidad se generaron las consultas a través de la herramienta automatizada de testeo de penetración *opensource* Metasploit 4.1.4.2. Esta es una herramienta de uso libre que cuenta con un sistema de plugins programados en el lenguaje Ruby para lograr automatizar y simplificar diferentes tareas de rutina durante el proceso de una auditoría de seguridad, por ejemplo escaneo de puertos TCP/UDP, verificación de credenciales no diversificadas y, en el caso de este trabajo particular, consultas al motor de búsqueda Shodan. Además cuenta con un motor de base de datos PostgreSQL que permite el registro y organización de los datos recolectados.

La elección de esta herramienta responde a la necesidad práctica de acopiar y registrar los datos obtenidos de manera organizada y automática en un *framework* especializado. Trabajando con información muy dispar de gran cantidad de objetivos es fundamental el control de los datos automatizado. Metasploit mantiene en su base de datos un registro de todas las tareas y resultados, y permite clasificarlos y ordenarlos de forma simple.

El módulo de Metasploit utilizado se denomina "auxiliary/gather/shodan_search" y se ejecutó con las opciones por defecto, excepto que se configuró la APIKEY a una cuenta de uso profesional, el número de páginas de retorno en 5 y el acceso a base de datos para guardar los datos. A continuación se presentan algunas de las keywords más significativas utilizadas para consultar y una breve referencia. Estas consultas fueron repetidas a nivel global y argentino:

port:502	MODBUS
port:102	SIEMENS S7
port:20000 source address	DNP3
port:1911,4911 product:Niagara	NIAGARA FOX TRIDIUM
port:47808	BACNET
port:44818 device	ETHERNET/IP (Industrial Ethernet)
port:18245,18246 product:”general electric”	GENERAL ELECTRIC SRTP
port:5094 hart ip	HART IP
port:1962 PLC	PC WORX

port:5006,5007 product:mitsubishi	MELSEC-Q
port:789 product:\Red Lion Controls\""	CRIMSON v3.0 / RED LION CONTROLS G306A
port:2455 operating system	CODESYS
port:2404 asdu address	IEC 60870-5-104
port:20547 PLC	PROCONOS

Tabla 1 - Queries de shodan para detección de sistemas industriales

Además de estas consultas específicas por protocolo, se realizaron consultas generales por keywords que pudieran contener otras descripciones de dispositivos.

Con esta herramienta se obtuvo una lista de direcciones IP públicas de Internet y puertos de escucha de los diferentes servicios.

3.2.2 Verificación con nmap [43]

Nmap (*Network* Mapper) es una herramienta *open-source* especializada en exploración de redes y auditoría de seguridad. La primera versión de uso popular en la comunidad de seguridad informática data de 1997, por lo que es una herramienta de ubicuidad probada y muy reputada. Es el estándar *ad-hoc* de referencia en exploración de redes. De forma común se usa para descubrimiento y caracterización de sistemas y servicios remotos, mediante el envío de paquetes especialmente diseñados y el análisis de las respuestas.

Se seleccionó para su uso en este estudio por los siguientes criterios:

- Confiabilidad y ubicuidad: es una aplicación *open-source* de muchos años de uso común, continuado y recomendado.
- Costo: al ser *open-source* tiene costo cero.
- Flexibilidad: con el correr de los años ha crecido muchísimo en cantidad de funciones y parámetros configurables, dándole la capacidad de adaptarse a gran cantidad de situaciones y requerimientos
- Capacidad de trabajar con grandes cantidades de objetivos: es uno de sus criterios de diseño, y está relacionado con el punto siguiente
- Consumo de recursos de sistema: bajo costo en CPU y RAM para su ejecución sin degradación de performance al ser una aplicación *standalone* de consola desarrollada en C y C++.

Nmap se aplicó en el presente estudio como una forma de verificar los resultados obtenidos en el paso anterior. Las técnicas de exploración que utiliza Shodan pueden

dar falsos positivos a veces, porque la base de datos tiene un período de actualización y puede ocurrir que un servicio o sistema sea sacado de servicio, se interrumpa su conectividad u otras situaciones que impidan su detección. A fin de mantener los criterios de intrusividad y tiempo de ejecución definidos en el apartado 3.2, nmap se configuró para solamente verificar la escucha del servicio en el puerto determinado por shodan con el envío de un paquete SYN y espera de un SYN/ACK en la ventana de *timeout*.

Como entrada del proceso se utilizó una exportación de la base de datos de Metasploit, poblada en el apartado 3.2.1 con el universo de direcciones IP, hostnames, puertos y servicios posiblemente vulnerables detectados por shodan. Se descartaron todos los datos excepto dirección IP y puerto, y se generó un archivo de entrada para nmap. Los criterios de configuración de la aplicación para esta verificación se basaron en los criterios generales comentados en el apartado 3.2. En esta etapa de exploración directa fue muy importante mantener el nivel de intrusividad bajo para evitar causar interferencias con la operación de los sistemas probados, por esto se determinó la elección de una exploración tipo SYN que impide obtener muchos detalles o capturar *banners* de servicios, pero garantiza la detección un puerto TCP en escucha y al mismo tiempo tiene la menor posibilidad de interferencia con el sistema remoto.

Por otra parte, desde el punto de vista del sigilo de la detección, es decir la capacidad del sistema remoto de determinar que está bajo exploración o ataque, no es muy avanzada para los estándares de hoy y existen técnicas más modernas. Sin embargo es la opinión del autor que un riesgo permanente al hacer exploración de sistemas industriales es causar una denegación de servicio involuntaria durante la etapa de análisis de vulnerabilidades, porque muchas veces por cuestiones de recursos limitados en PLC y otros dispositivos de campo no se implementan las pilas TCP/IP al completo de las especificaciones, y esto puede causar fallas al recibir paquetes extraños usados durante la exploración. Es decir que fue primordial utilizar un mecanismo de detección que esté garantizada su implementación en cualquier sistema, aunque el sistema esté fuera de especificaciones.

Finalmente fue de importancia mantener el criterio de *performance* o tiempo de exploración lo más bajo posible, para acotar el tiempo de trabajo sobre una cantidad grande de objetivos.

A partir de estos criterios se definieron las siguientes opciones de configuración:

- Versión utilizada: 7.80

- Resolución de DNS: desactivada para mejorar el tiempo de exploración por objetivo
- Ping scan: desactivado para mejorar el tiempo de exploración por objetivo. Por otra parte, al tratarse de un estudio general y masivo no nos interesa el estado particular de cada objetivo, si no la comprobación de la escucha en el puerto y eventualmente la existencia del servicio. En otras palabras, no fue de interés discriminar entre un host no vulnerable online, y un host offline.
- Tamaño de grupos de exploración paralela: nmap tiene la capacidad de dividir el universo de objetivos en grupos, y ejecutar las pruebas de manera paralela entre grupos. A mayor tamaño de grupo, mayor rendimiento en la ejecución general, pero los resultados de individuales no se presentan hasta terminada la totalidad del grupo, por lo que lleva más tiempo presentarlos. Por defecto, la aplicación comienza con un tamaño de 5 para obtener los primeros resultados de manera más rápida, y a medida que progresa el trabajo se incrementa hasta 1024. Como valor de referencia se recomienda un tamaño de 256 para redes clase C. Para este trabajo se utilizó un valor mínimo y máximo de 1024 al no tener requerimientos de visualización en tiempo real.
- Reintentos máximos: al escanear mayoritariamente dispositivos de campo, es importante tener en cuenta que en la mayoría de los casos estaremos trabajando sobre dispositivos muy alejados, muchas veces directamente conectados en sitio de una explotación industrial. Es decir, redes de latencia y ancho de banda mucho peor que lo normal en Internet. Por esto, y de forma contraria a nuestro criterio básico de alto rendimiento, se incrementaron los reintentos máximos a 20.
- *Host timeout*: Se incrementó a un máximo de 2 minutos por host, para compensar los efectos mencionados en el punto anterior y teniendo en cuenta que no se verifican más de dos puertos por objetivo.
- Tipo de detección: SYN scan, acorde lo comentado en el párrafo anterior de este apartado
- Puertos objetivo: estrictamente los referidos a los servicios analizados, y comentados en el apartado 3.2.1

Por ejemplo, considerando estos criterios, la línea de comando para la ejecución del proceso en un grupo de objetivos de Modbus y su salida correspondiente será:

```
# nmap -n -Pn –sS --min-hostgroup 1024 --max-hostgroup 1024 --max-retries 10 --host-timeout 2m -p 502 -i ./modbus2.txt

Warning: You specified a highly aggressive --min-hostgroup.
```

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-07-11 15:51 EDT

Nmap scan report for 127.0.0.1

Host is up (0.000034s latency).


PORT    STATE  SERVICE

502/tcp closed mbap


Nmap scan report for [redacted]

Host is up (0.32s latency).


PORT    STATE SERVICE

502/tcp open  mbap
```

Esto es un ejemplo ilustrativo en un grupo reducido, que además incluye el host local como referencia de puerto cerrado primero en la lista.

3.2.3 Herramientas alternativas

Durante el proceso de selección de herramientas se evaluaron algunas alternativas a nmap, pero en las pruebas preliminares mostraron que no hubo mejor significativas de performance o exactitud, y además, como se comentaba en el apartado previo, nmap se ha convertido en el estándar ad-hoc de uso común para muchos tipos de análisis de redes [44], por lo que su elección responde a su ubicuidad, flexibilidad y confiabilidad probadas.

4 Resultados obtenidos

4.1 Resultados del análisis de vulnerabilidades

El universo de resultados obtenidos resultó ser mucho más grande de lo esperado. Este hecho introdujo nuevas complejidades al tratamiento de datos, debido a que herramientas de uso común de planilla de cálculos no están preparados para manejar conjuntos de datos de tal volumen.

El total de hosts encontrados en Internet asciende a 119.190. De estos, 61 se ubican dentro de la Argentina. Lógicamente estos números son mucho más manejables, permiten una verificación uno por uno de los hosts encontrados, y un gran nivel de detalle.

Para todos los hosts descubiertos en Internet se obtuvo la siguiente información:

- direcciones IP y puertos
- información geográfica
- identificación de servicios
- identificación de sistema operativo
- dominio / organización propietaria
- autenticación y control de acceso
- producto, en caso de sistemas embebidos
- versión de servicio y sistema operativo
- encriptación
- información de implementación SSL: versión, expiración de certificados, longitud de cadena

En caso de sistemas conectados con poco nivel de seguridad, haciendo un análisis fino puede obtenerse aún más información. Se comenta el siguiente caso, que si bien cae en lo anecdótico está muy lejos de ser excepcional y sirve como ejemplo ilustrativo: se encontró un PLC SIEMENS Simatic 1200 conectado a Internet sin ningún tipo de seguridad, ubicado en Juan Jose Paso, provincia de Buenos Aires y perteneciente a una empresa de construcciones**.** El dispositivo está conectado a una red de campo con una serie de sensores y se denomina **“Controlador de reactor”**. Se descubrió que por un error de configuración, su interfaz de control es accesible a

cualquier persona que conozca su dirección, es decir que puede alterarse sus parámetros, detener su funcionamiento, cambiar su punto de trabajo, y recuperar la información de los sensores en su totalidad.

Total de ICS encontrados: 119.190 a nivel mundial, 61 en Argentina. (Abril 2018)

Vulnerabilidades principales esperadas

- Credenciales por defecto del fabricante, muchas conocidas “hardcoded”
- Cuentas de visitante sin autenticación habilitadas
- Software y servicios no utilizados (incrementa superficie de ataque)
- SO y servicios deprecados
- Elementos de seguridad básicos de IT faltantes (firewall, IDS, etc)
- Bajo nivel de log
- Dispositivos de campo conectados a Internet

Los primeros problemas de seguridad detectados son en sí mismas la accesibilidad y conectividad a la totalidad de los 119.190 casos verificados a través una red pública como Internet. La visibilidad de una red crítica en Internet o cualquier otra red pública, es evidencia de que no existe o no está configurado correctamente un Firewall, no hay IDS/IPS, no hay segmentación de subredes la arquitectura de red no ha sido diseñada con seguridad en mente y de que probablemente la organización no tiene o no respeta buenas políticas de seguridad de datos. En palabras simples, es indicio de una presa fácil para un atacante.

De la totalidad de los resultados, se muestran a continuación las principales tecnologías encontradas;

TECNOLOGÍA	CASOS
SIEMENS S7	3165
MODBUS	18784
NIAGARA	31553
BACNET	15808
DNP3	507
ETHERNET INDUSTRIAL	8740

Tabla 2 - Cantidad de objetivos detectados por tecnología

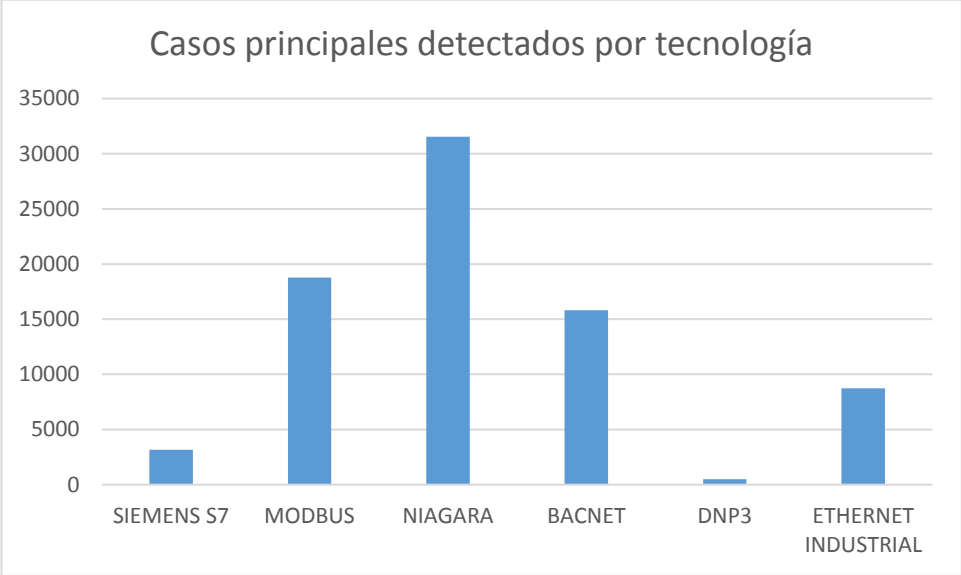

Figura 7 - Casos principales detectados por tecnología

A continuación se presenta la tabla completa con los datos de reconocimiento de red para las tecnologías más relevantes categorizados:

SIMENES S7		
Consulta shodan	port: 102 "basic"	
Resultados totales:	3165	
Top países		
Alemania	721	22,78%
España	530	16,75%
Italia	337	10,65%
Turquía	164	5,18%
Estados Unidos	152	4,80%
Polonia	95	3,00%
Francia	94	2,97%
Brasil	87	2,75%
Austria	83	2,62%
Hungría	76	2,40%

Top ISP		
Deutsche Telekom AG	434	13,71%
Vodafone España	295	9,32%
Telefonica de España	113	3,57%
Turkcell	102	3,22%
Deutsche Telekom Business	88	2,78%
Orange	79	2,50%
Telecom Italia	68	2,15%
Envia Tel Gmbh	62	1,96%
Magyar Musorszoro es Radiohirkozl	62	1,96%
Top dominios		
t-ipconnect.de	270	8,53%
airtel.net	220	6,95%
rima-tde.net	195	6,16%
telecomitalia.it	90	2,84%
skydsl.it	61	1,93%
wanadoo.fr	59	1,86%
vivozap.com.br	52	1,64%
ttnet.com.tr	38	1,20%
mycingular.net	38	1,20%
myvzw.com	36	1,14%
MODBUS		
Consulta shodan	port:502	
Resultados totales:	18784	
Top países		
Estados Unidos	3227	17,18%
Francia	1304	6,94%
España	1154	6,14%
Italia	113	0,60%
Alemania	1043	5,55%
Australia	933	4,97%
Turquía	830	4,42%
Canada	821	4,37%

Suecia	798	4,25%
Taiwan	700	3,73%
Top ISP		
Verizon Wireless	1491	7,94%
Telstra Internet	876	4,66%
Orange	735	3,91%
Deutsche Telekom AG	730	3,89%
Turkcell	640	3,41%
Telefonica de España	462	2,46%
Telecom Italia Mobile	368	1,96%
HiNet	299	1,59%
Korea Telecom	295	1,57%
TeliaSonera AB	270	1,44%
Servicios HTTP con negociación de contenido		
HTTP 1.1	2	0,01%
HTTP/2	1	0,01%
Top Hardware		
BMX P34 2020	562	2,99%
BMX NOE 0100	180	0,96%
TM221CE40T	161	0,86%
SAS TSXETY4103	145	0,77%
TM221CE40R	98	0,52%
BMX P34 20302	62	0,33%
TM251MESE	53	0,28%
TM221CE24T	51	0,27%
TM221ME16R	48	0,26%
TM241CE24T_U	44	0,23%
Top Versiones (Hardware)		
V1.0	515	2,74%
V2.5	200	1,06%
V2.6	136	0,72%
V2.2	90	0,48%
V4	74	0,39%

V2.8	73	0,39%
V2.4	48	0,26%
V2.1	48	0,26%
V3.1	48	0,26%
Top Dominios		
myvzw.com	1491	7,94%
rima-tde.net	725	3,86%
wanadoo.fr	664	3,53%
hinet.net	360	1,92%
telia.com	341	1,82%
t-ipconnect.de	257	1,37%
vivozap.com.br	244	1,30%
mycingular.net	223	1,19%
telecomitalia.it	193	1,03%
sfr.net	187	1,00%
Versiones SSL		
TLS v1.2	2	0,01%
TLS v1.1	2	0,01%
TLS v1	2	0,01%
Top Sistemas Operativos		
Windows 7 / 8	23	0,12%
Linux 2.6.x	18	0,10%
Linux 2.4-2.6	14	0,07%
Linux 3.x	13	0,07%
Linux 2.4.x	8	0,04%
Windows XP	3	0,02%
NIAGARA		
Resultados totales:	31553	
Consuta shodan	port:1911,4911 product:"Niagara"	
Top Paises		
Estados Unidos	21550	68,30%
Canada	1867	5,92%

Italia	1646	5,22%
Gran Bretaña	1053	3,34%
Australia	1034	3,28%
Países Bajos	818	2,59%
Francia	739	2,34%
Noruega	352	1,12%
Dinamarca	225	0,71%
Taiwan	221	0,70%
Encriptación con túnel SSL		
No	26883	85,20%
Si	4670	14,80%
Top ISP		
Comcast	3526	11,17%
Verizon Wireless	2155	6,83%
AT&T Internet Services	1278	4,05%
CenturyLink	1177	3,73%
Time Warner Cable	986	3,12%
Frontier Communications	775	2,46%
Telstra Internet	764	2,42%
AT&T U-verse	722	2,29%
Cox Communications	639	2,03%
Telecom Italia Mobile	606	1,92%
Top Versiones		
Fox protocol 1.0.1	21614	68,50%
Niagara 4 Framework	7939	25,16%
Fox protocol 1.0	1997	6,33%
Top dominios		
comcastbusiness.net	3480	11,03%
myvzw.com	2150	6,81%
sbcglobal.net	1475	4,67%
rr.com	876	2,78%
verizon.net	829	2,63%
cox.net	583	1,85%

charter.com	455	1,44%
frontiernet.net	435	1,38%
optonliine.net	426	1,35%
comcast.net	323	1,02%
Versiones SSL		
TLSv1	4501	14,26%
TLSv1.2	3693	11,70%
TLSv1-1	3606	11,43%
SSLv3	121	0,38%
Certificados SSL expirados		
Expirados	3234	10,25%
No expirados	1379	4,37%
Longitud de cadena SSL		
1	4476	14,19%
2	54	0,17%
3	35	0,11%
4	33	0,10%
5	10	0,03%
6	3	0,01%
9	2	0,01%
Top Sistemas Operativos		
Windows 7 / 8	54	0,17%
HP UX 11.x	38	0,12%
Windows XP	32	0,10%
BACNET		
Resultados totales:	15808	
Consulta shodan	port:47808	
Top Paises		
Estados Unidos	9770	61,80%
Canada	2617	16,55%
Francia	396	2,51%
Australia	271	1,71%
España	265	1,68%

Reino Unido	252	1,59%
Alemania	206	1,30%
Suecia	178	1,13%
Italia	152	0,96%
Corea del Sur	131	0,83%
Top ISP		
Comcast Business	1498	9,48%
AT&T Internet Services	898	5,68%
Time Warner Cable	612	3,87%
Verizon Wireless	535	3,38%
AT&T U-verse	508	3,21%
Telus Communications	485	3,07%
Bell Canada	376	2,38%
Frontier Communications	367	2,32%
Shaw Communications	353	2,23%
CenturyLink	327	2,07%
Top Productos		
NiagaraAX Station	1465	9,27%
MACH-ProWebSys	741	4,69%
MACH-ProWebCom	656	4,15%
Niagara4 Station	650	4,11%
Tracer SC	567	3,59%
LGR25	440	2,78%
MACH-ProSys	412	2,61%
DSM_RTR	382	2,42%
MACH-ProCom	375	2,37%
eBMGR	282	1,78%
Top Version string		
0.0	1124	7,11%
189697	575	3,64%
2.6.30_HwVer12AB-hydra	562	3,56%
3.8.111	373	2,36%
7.76	237	1,50%

159693	219	1,39%
4.2.36.38	215	1,36%
1.2	214	1,35%
7.0.0.4400	175	1,11%
535847	171	1,08%
Top dominios		
comcastbusiness.net	1492	9,44%
sbcglobal.net	960	6,07%
rr.com	534	3,38%
myvzw.com	533	3,37%
charter.com	299	1,89%
bell.ca	278	1,76%
verizon.net	277	1,75%
telus.net	260	1,64%
cox.net	227	1,44%
wanadoo.fr	224	1,42%
DNP3		
Consulta shodan	port:20000 source address	
Resultados totales:	507	
Top países		
Estados Unidos	245	48,32%
Brasil	64	12,62%
Italia	28	5,52%
Hungría	23	4,54%
Canada	15	2,96%
Australia	13	2,56%
Turquía	12	2,37%
Argentina	9	1,78%
Alemania	9	1,78%
Mexico	9	1,78%
Top ISP		
Verizon Wireless	104	20,51%
Sagenet LLC	65	12,82%

Vivo	40	7,89%
Vodafone Hungary	23	4,54%
AT&T Wireless	18	3,55%
WIND Telecomunicazion	15	2,96%
Telstra Internet	11	2,17%
MPInet	11	2,17%
Turkcell	10	1,97%
Telecom Italia Business	9	1,78%
Top Dominios		
myvzw.com	103	20,32%
vivozap.com.br	40	7,89%
vodafone.hu	23	4,54%
mycingular.net	15	2,96%
telecomitalia.it	9	1,78%
claro.net.br	6	1,18%
amazonaws.com	6	1,18%
ufinet.com.gt	5	0,99%
uninet-ide.com.mx	4	0,79%
timbrasil.com.br	4	0,79%
ETHERNET INDUSTRIAL		
Consulta shodan	port:44818 device	
Resultados totales:	8740	
Top países		
Estados Unidos	4703	53,81%
Corea del Sur	737	8,43%
Canada	690	7,89%
España	456	5,22%
Italia	234	2,68%
Taiwan	201	2,30%
Australia	194	2,22%
Portugal	157	1,80%
Dinamarca	110	1,26%
China	102	1,17%

Top ISP		
Verizon Wireless	2758	31,56%
SK Telecom	713	8,16%
AT&T Wireless	395	4,52%
Telefonica de España	213	2,44%
Bell Mobility	210	2,40%
Telstra Internet	166	1,90%
Comcast Business	161	1,84%
Telecom Italia Mobile	123	1,41%
HiNet	105	1,20%
Vodafone Spain	101	1,16%
Top Fabricantes		
Rockwell Automation/Allen-Bradley	4795	54,86%
OPTO-22	389	4,45%
Reservado	63	0,72%
Omron Corporation	62	0,71%
Wago Corporation	54	0,62%
Red Lion Controls	32	0,37%
Delta Power Electronics	30	0,34%
Schneider Automation	26	0,30%
ABB Industrial Systems	20	0,23%
1301	18	0,21%
Top Productos		
SNAP-PAC-R2	375	4,29%
9-L24ER-QBFC1B/A LOGIX5324ER	284	3,25%
1756-L61/B LOGIX5561	264	3,02%
1769-L33ER/A LOGIX5333ER	233	2,67%
1769-L32E Ethernet Port	190	2,17%
1769-L30ER/A LOGIX5330ER	177	2,03%
1766-L32BXBA B/15.00	115	1,32%
1756-ENBT/A	114	1,30%
1766-L32BXB B/B15.00	112	1,28%
1766-L32BXBA B/11.0	98	1,12%

Top dominios		
myvzw.com	2757	31,54%
rima-tde.net	318	3,64%
mycingular.net	300	3,43%
comcastbusiness.net	156	1,78%
hinet.net	113	1,29%
telus.com	86	0,98%
sbcglobal.net	74	0,85%
rr.com	73	0,84%
frontiernet.net	65	0,74%
airtel.net	52	0,59%
PC WORX		
Consulta shodan	port:1962 PLC	
Resultados totales:	1190	
Top Paises		
Italia	465	39,08%
Alemania	176	14,79%
Paises bajos	159	13,36%
Turquía	83	6,97%
España	76	6,39%
Francia	57	4,79%
Rumania	26	2,18%
Estados Unidos	24	2,02%
Canada	24	2,02%
Bélgica	16	1,34%
Top ISP		
WIND Telecomunicazion	229	19,24%
Telecom Italia Mobile	166	13,95%
Deutsche Telekom AG	162	13,61%
Vodafone-Libertel NV	137	11,51%
Turkcell	73	6,13%
SFR	33	2,77%
Telefonica de España	24	2,02%

Telefonica de España estática	21	1,76%
Vodafone Italia	20	1,68%
GGSN/APN	20	1,68%
Top Dispositivos		
ILC 151 GSM/GRPS	402	33,78%
ILC 150 GSM/GPRS	222	18,66%
ILC 151 ETH	144	12,10%
ILC 191 ETH 2TX	101	8,49%
ILC 131 ETH	61	5,13%
AXC 1050	56	4,71%
ILC 150 ETH	47	3,95%
ILC 171 ETH 2TX	46	3,87%
ILC 191 ME/AN	37	3,11%
ILC 130 ETH	21	1,76%
Top Model Number		
2700977	402	33,78%
2916545	222	18,66%
2700974	144	12,10%
2700976	101	8,49%
2700973	61	5,13%
2700988	56	4,71%
2985330	47	3,95%
2700975	46	3,87%
2700074	37	3,11%
2988803	21	1,76%
Top dominios		
sfr.net	49	4,12%
rima-tde.net	45	3,78%
t-ipconnect.de	28	2,35%
kpn-gprs.nl	19	1,60%
telecomitalia.it	14	1,18%
proximus.be	10	0,84%
kyivstar.net	9	0,76%

centertel.pl	8	0,67%
airtel.net	8	0,67%
vodafone.pt	6	0,50%

Tabla 3 - Datos de reconocimiento de red por tecnología

De la totalidad de resultados mostrados en las tablas precedentes el 56,2% corresponden a PLC. Además hay un 1% de dispositivos de campo misceláneos, como controladores de motores AC, variadores de velocidad, interfaces HMI, etc. El resto de los dispositivos encontrados no fueron posibles de identificar.

En términos de vulnerabilidades de seguridad, como se comentó en el párrafo anterior la visibilidad y accesibilidad de sistemas industriales a través de Internet, y en particular su registro y análisis por un buscador público como Shodan, en sí mismos constituyen un riesgo. Es decir que la totalidad de los sistemas estudiados son clasificables como vulnerables desde que son accesibles por cualquiera a través de Internet.

En segundo término, el problema de seguridad más frecuente y grave encontrado es el uso masivo de comunicaciones sin SSL/TLS. SSL y su versión actual, TLS, son protocolos de seguridad para conexiones TCP basados en tecnología de criptografía asimétrica que permiten encriptar y autenticar las comunicaciones, de forma corriente usados para navegación Web segura en el protocolo HTTPS. En la actualidad TLS provee seguridad y privacidad a todos los sistemas de interfaces de usuario Web como homebanking, gestiones gubernamentales, e-commerce, redes sociales, etc., y su funcionamiento se consideraría imposible si no se pudiera garantizar la autenticidad de los servidores a los que accedemos, y la privacidad de la información que intercambiamos con ellos. Desde la primera versión de SSL en el año 1995, han aparecido numerosas versiones que solucionan problemas de seguridad anteriores y dan soporte a nuevos cifrados y algoritmos más fuertes. La última versión es TLS 1.3, aprobada por la IETF en Marzo de 2018. Apple, Google, Microsoft y Mozilla conjuntamente deprecaron hasta TLS 1.1 inclusive en Marzo de 2020 [45].

Sin embargo, al menos el 58,9% de la totalidad de los sistemas descubiertos operan sin esta tecnología ni ninguna otra que cumpla este rol, lo cual es consistente con la conclusión parcial de que los sistemas industriales carecen muchas veces de políticas de seguridad adecuadas, y en sí mismo representa una gran superficie de ataque, exponiendo a estos sistemas a los siguientes tipos de ataques:

- ataques “man in the middle”: un atacante podría interceptar las comunicaciones y modificar la información intercambiada.
- suplantación de identidad: utilizando técnicas de DNS *poisoning* por ejemplo, podría hacerse pasar por un servidor legítimo y recolectar credenciales
- “packet sniffing”: o simplemente escuchar en el canal de comunicaciones y registrarlo todo, accediendo así a información privilegiada o sensible incluyendo credenciales de acceso

Todos estos ataques, y muchas variantes de cada uno, podrían implementarse con muy baja dificultad y con casi nulas probabilidades de detectarlos ni prevenirlos, en sistemas sin encriptación del canal.

Adicionalmente el 6.9% funciona con protocolos obsoletos, es decir SSLv2, SSLv3, TLSv1 y TLSv1.1. Estos protocolos son vulnerables a las siguientes vulnerabilidades:

Vulnerabilidad de TLS/SSL	**Versión afectada**	**Casos potenciales**	**CVE (ref.)**
POODLE	SSLv3	121	CVE-2014-3566
BEAST	SSLv3, TLSv1	4624	CVE-2011-3389
CRIME	TLSv1.2 y anteriores	8228	CVE-2012-4929
BREACH	N/A	N/A	CVE-2013-3587
Heartbleed	N/A	N/A	CVE-2014-0160

Tabla 4 - Posibles casos de sistemas industriales vulnerables a fallas conocidas de TLS/SSL

Como referencias para la elaboración de esta tabla se tomaron datos de la organización MITRE.

4.2 Resultados de investigación bibliográfica

De la investigación bibliográfica se desprenden los siguientes resultados en cuanto a vulnerabilidades descubiertas en sistemas industriales. La clasificación se realiza por año, por sector industrial, por componente del sistema y por severidad acorde al puntaje CVSS v3. [46], [47], [48]

Los datos de vulnerabilidades fueron tomados de recomendaciones del ICS-CERT (Industrial Control Systems Cyber Emergency Response Team) y NIST NVD (National Institute for Standards and Technology Vulnerability Database)

4.3 Vulnerabilidades de ICS por año:

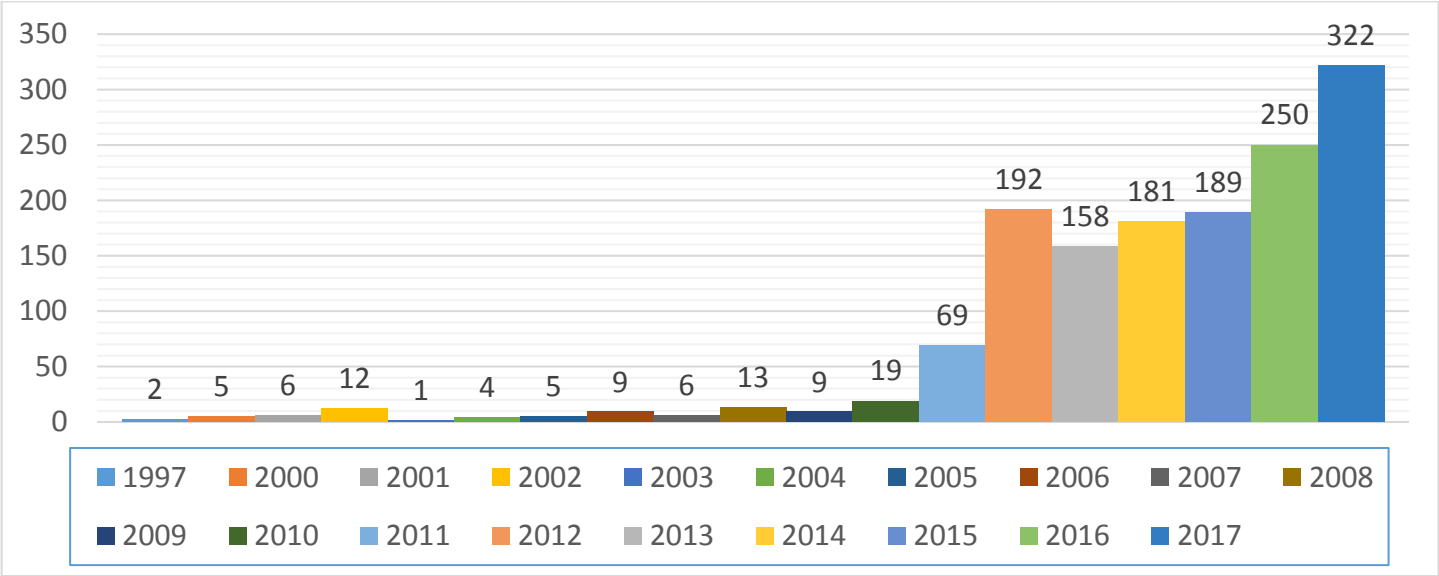

Figura 8 - Vulnerabilidades de ICS por año

CVSS v3 (*Common Vulnerability Scoring System*) es un estándar libre y abierto de la industria para medir la severidad de distintas vulnerabilidades. El sistema intenta asignar un puntaje de severidad, posibilitando que los organismos de respuesta prioricen los recursos en base al nivel de amenaza. Los puntajes se calculan a partir de una fórmula que depende de varias métricas que aproximan la facilidad de explotación y el impacto potencial de una vulnerabilidad. Los puntajes van del 1 al 10, donde 10 es el más severo. La versión 3 del estándar, que es la más actualizada, fue hecha pública en junio de 2015.

Los datos presentados en el trabajo presente datan de hasta 2017 inclusive para la revisión anual, y en la clasificación por características se limitan a este año, para dar una imagen general del estado actual del conocimiento público sobre vulnerabilidades de sistemas industriales.

4.4 Clasificación de vulnerabilidades:

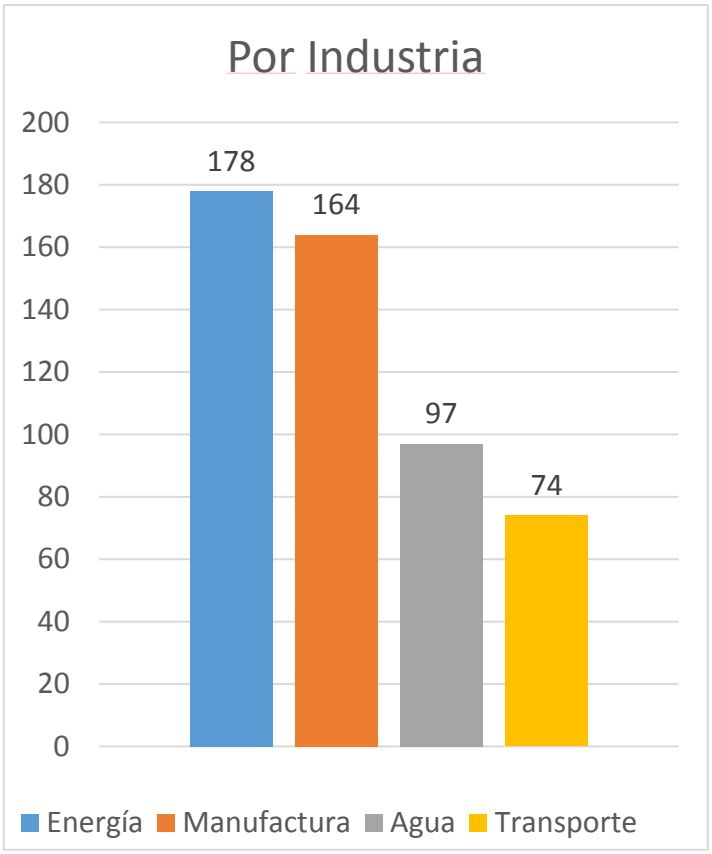

Figura 9 - Vulnerabilidades de ICS por industria

De todos los casos de agujeros de seguridad analizados se eligieron tres de los más relacionados con el objeto de estudio del presente trabajo, y de mayor gravedad, descubiertos durante el último año. Se presentan como ejemplo con una breve descripción, para ejemplificar y dimensionar la gravedad de los problemas que ocurren. [49]

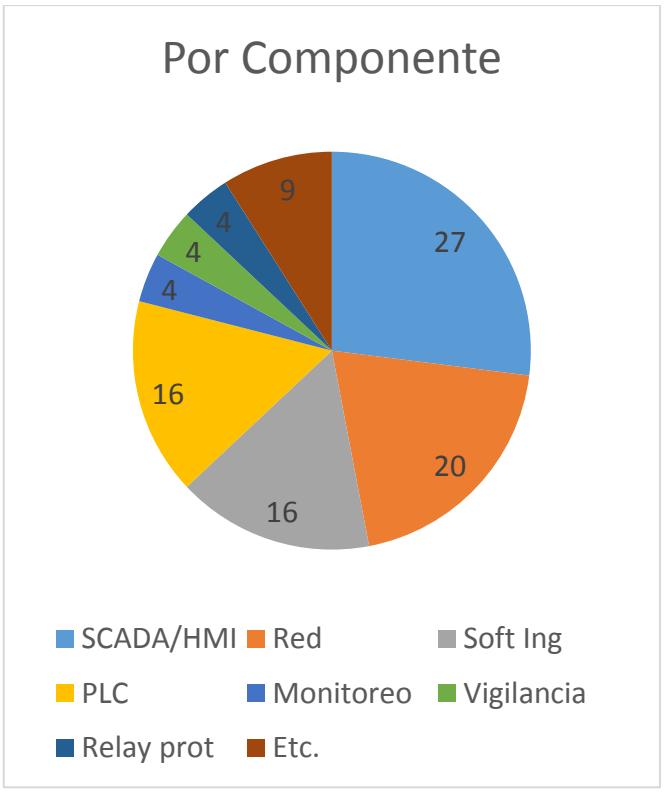

Figura 10 - Vulnerabilidades de ICS por componente

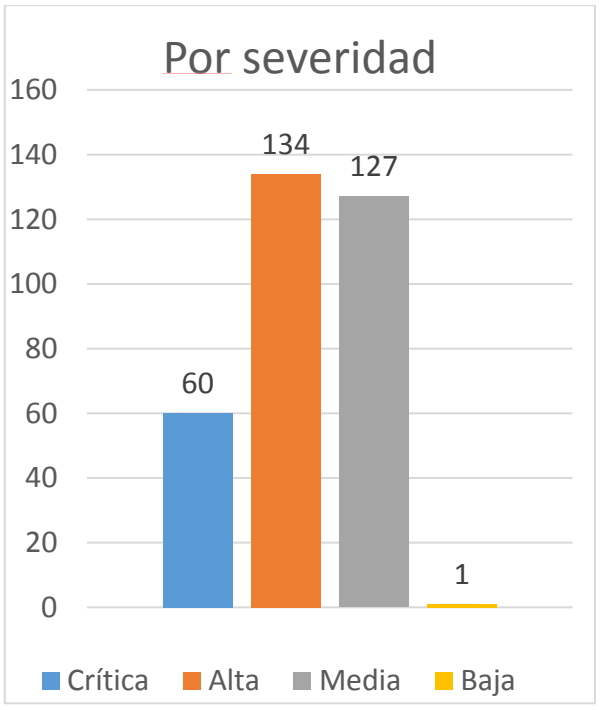

Figura 11 - Vulnerabilidades de ICS por severidad

4.5 Vulnerabilidades en protocolos de comunicación industriales de alta relevancia [50], [51], [52]

- Schneider Electric Modicon Modbus Protocol
  - CVSS v3 score: **10 (Crítica)**
  - Remota, bajo nivel
  - Bypass de autenticación, información sensible en texto plano, mala implementación de check de seguridad permite ataque de fuerza bruta
- Siemens pila de protocolos OPC UA
  - CVSS v3 score: **8,2 (Crítica)**
  - Remota, bajo nivel
  - Envío de paquetes especialmente diseñados al OPC Discovery Server (TCP 4840)
- Siemens protocolo PROFINET Discovery and configuration
  - CVSS v3 score: **6,5 (Mediana)**
  - Denial of service, improper input validation

5 Discusión de resultados

A continuación se comentan los resultados concretos obtenidos en el relevamiento y pruebas ejecutados, que constituyen los aportes a la generación de conocimiento realizados por el presente estudio.

El primer resultado del este trabajo es la confirmación de que es posible, con un nivel de dificultad técnica no muy elevado, acceder a través de Internet a miles de sistemas industriales privados que operan sobre infraestructura crítica en muchos casos.

En segunda instancia, se comprobó que es posible extraer una gran cantidad de información de estos sistemas. Las tareas de reconocimiento de red dieron resultados de servicios, versiones, sistemas operativos, arquitectura de red, configuraciones, etc., lo cual constituye un problema de fuga de información muy grave. Resulta aún más grave teniendo en cuenta que estos resultados se obtuvieron ateniendo las pruebas a

requisitos estrictos de rendimiento e intrusividad, y sin los cuales los resultados hubieran sido mucho más completos y exactos.

En tercera instancia, se encontró que el 65,8% de los sistemas analizados trabajan con protocolos criptográficos deprecados, o directamente sin los mismos. Esto representa una evidencia muy importante de que estas organizaciones no tienen una política funcional de actualización de software y firmware. En particular, que exista un porcentaje tan alto de sistemas trabajando con versiones obsoletas nos permite inferir con un nivel de confianza razonable que la seguridad directamente no ha sido tenida en cuenta durante el proceso de diseño de arquitectura y de que no existen procesos ni políticas establecidas de seguridad de datos, especialmente a la luz de la gran cantidad de vulnerabilidades relacionadas con estos protocolos conocidas, explotadas y estudiadas de modo corriente en la industria de la seguridad informática.

Se encontró que el protocolo industrial de mayor exposición a Internet en el mundo es Tridium Fox, con casi 32.000 sistemas conectados. Este es un sistema de automatización de edificios que se integra al framework Niagara, diseñado para articular la comunicación entre las estaciones remotas y la central de control. Es un protocolo de aplicación que corre sobre TCP. En la arquitectura de Tridium, las estaciones ejecutan una máquina virtual Java.

Lo sigue MODBUS TCP/IP, de gran ubicuidad en el mundo industrial en general, con cerca de 19.000 sistemas conectados. Este protocolo, cuya versión original data de 1979, tiene uno de los problemas más constantes en la seguridad de sistemas industriales: simplemente no fue diseñado para usarse en una red abierta accesible públicamente por millones de usuarios alrededor del mundo. Carece de consideraciones de seguridad totalmente, no tiene control de acceso. La realidad es que si uno puede llegar a un dispositivo MODBUS en una red, uno puede leer y escribir cualquier dato del sistema. En el caso de interfaces gráficas de control vía HTTP relacionadas con controladores Modbus se encontró que la gran mayoría carece de autenticación. El sistema más expuesto es el PLC Schneider Electric BMXP342020, y los siguientes 4 pertenecen al mismo fabricante. Un punto importante a analizar es si existe alguna configuración por defecto u otra circunstancia que hace a los controladores de este fabricante tan fáciles de acceder, si hay algún sesgo inadvertido en los datos, si son más fáciles de utilizar o más ubicuos por cualquier otro motivo. Otra circunstancia interesante que se descubrió en el caso particular de MODBUS, es que existe un enorme porcentaje de servidores relacionados corriendo sistemas operativos muy

antiguos como Windows XP. Esto representa un riesgo de seguridad enorme, debido a las múltiples vulnerabilidades conocidas de estos sistemas operativos.

6 Conclusiones

Como resultado de este trabajo es evidente que existe un enorme trabajo a realizar para asegurar que tanto las compañías industriales como los servicios públicos de infraestructura estén protegidos de la mejor manera posible contra el riesgo permanentemente y creciente de brechas de ciberseguridad que vulnera los entornos de control industrial. Los incidentes de ciberseguridad ocurren de manera frecuente, y resulta de una complejidad técnica relativamente baja explotarlos para obtener algún beneficio. A pesar de la toma de conciencia y la supuesta preparación por parte de las organizaciones, a menudo son subestimados tanto la fuente como el alcance de estos incidentes. Es esencial que se lleven a cabo los pasos necesarios para identificar los riesgos a los entornos de sistemas de control industriales, con políticas y procesos rigurosos y bien definidos para administrar el riesgo de manera tal que la organización esté en la mejor posición posible para asegurar su tecnología operacional. Adicionalmente a las pérdidas financieras muy significativas, el impacto de un ataque, intencional o accidental, puede ser considerable para el proceso industrial de una organización, para los productos, información propietaria o reputación. En los peores casos, estos pueden resultar en la pérdida de vidas humanas, daños irreversibles al medio ambiente o el fin de una empresa.

Los enfoques que toman las organizaciones de manera general para administrar la ciberseguridad industrial son bastante desestructurados y pueden ser mejorados. A pesar de que muchas empresas ofrezcan soluciones de seguridad, su eficacia sólo puede garantizarse si se trata de soluciones de seguridad específicas para entornos de ICS, y son soportadas con procesos robustos y lineamientos de trabajo claros. Contra el trasfondo de las amenazas concretas a los sistemas industriales, confiar en un producto de seguridad estándar "*out-of-the-box*" resulta totalmente subestimativo.

Existe además una alta probabilidad de que los incidentes reportados y detectados sean una fracción pequeña de todo el universo de violaciones de seguridad en sistemas de control industrial (especialmente cuando hablamos de infraestructuras no críticas), sumado a que los métodos de los que disponemos para analizar la exposición de los sistemas a redes públicas son limitados. Esto significa que el verdadero impacto en empresas y servicios de los problemas de seguridad de ICS se mantiene aun relativamente desconocido, al haber muy pocos casos de reportes de brechas de seguridad obligatorios entre las organizaciones. Por otra parte, hay antecedentes [53] de un número significativo de compañías internacionales que manifestaron su apoyo a introducir algún nivel de información obligatoria en su área de negocios, dejando una

oportunidad clara para los órganos regulatorios tales como CERT, ISAC, ISO y otros. Esto aportaría transparencia a los problemas de seguridad y ayudaría a generar un marco de trabajo para administrar el riesgo.

El problema de la ciberseguridad, tanto para sistemas industriales como para otras áreas de negocio, comienza con las personas. Para ejemplo, basta ver las estadísticas de sistemas expuestos a redes públicas por errores de configuración encontrados en el trabajo presente. Las compañías que ejecutan programas de *security awareness* para el personal, contratistas y proveedores típicamente experimentan menores pérdidas financieras [53] relacionadas a problemas de ciberseguridad. Los negocios industriales basados en tecnologías de operación requieren personal preparado con las habilidades necesarias y entrenamiento para proveer protección especializada a su infraestructura. Por esto resulta fundamental la preparación de profesionales que comprendan las necesidades de los dos mundos, de los sistemas de control industrial y de la ciberseguridad.

6.1 Propuestas de solución a las vulnerabilidades encontradas

A continuación se comentarán algunas posibles soluciones generales a los problemas encontrados. Las propuestas son técnicas generales de la industria de la seguridad informática, relacionadas con el *hardening* de redes y sistemas. Si bien se presentan clasificadas por vulnerabilidad, muchas se interrelacionan. La mayoría de estas recomendaciones parten de la base del criterio de “acceso estrictamente necesario”, que dice que para proveer el mayor nivel posible de seguridad debemos limitar el acceso a todos los servicios y recursos para cualquier solicitud o cliente, y solamente crear permisos de acceso a partir de una necesidad estricta para el funcionamiento u operación. Para expresarlo coloquialmente, podríamos decir que consideramos a todo intento de acceso a un recurso: culpable (o sospechoso) hasta que demuestre lo contrario.

Las soluciones se comentan a modo de recomendación ya que un trabajo completo de técnicas de mitigación está fuera del alcance del estudio presente. Además es importante tener en cuenta que si no se definen procesos permanentes de revisión, actualización y auditoría, por la naturaleza siempre cambiante del panorama de seguridad y la rápida evolución de la tecnología y técnica de los atacantes, las soluciones serán siempre temporales:

- **Visibilidad / detección a través de Internet:**
    - Rediseñar arquitectura de red con criterios de seguridad en mente: deben analizarse puntualmente los casos y necesidades de cada implementación, pero en general no debe escatimarse en gastos ni buscar reducir la complejidad de los procesos y sistemas a costa de la seguridad.
    - Implementar criterios de *defense in depth* a la arquitectura de red: *defense in depth* es una aproximación al diseño de seguridad basado en la definición de capas de seguridad con diferentes técnicas de mitigación a los riesgos conocidos y posibles. Este tipo de diseño permite que cada riesgo individual se vea abordado desde diferentes puntos de vista, y provee un nivel de redundancia de seguridad en el sentido de que un atacante tiene que superar muchas barreras individuales para explotar un único vector de ataque.
    - Segmentar subredes en niveles de seguridad: definir criterios de segmentación para los sistemas y dispositivos conectados a la red, establecer una DMZ para el acceso a sistemas de *front end*, interfaces de usuario, servicios expuestos, etc. Establecer filtrado de paquetes con firewall IP y WAF entre capas
    - *Air-gapping* completo de redes de control y redes de dispositivos de campo: las redes de control y dispositivos de campo no deben ser accesibles directamente desde fuera de sus segmentos. Para comunicaciones autorizadas, se recomienda diseñar una arquitectura con un firewall NAT que funcione como punto único de acceso a la subred y permita concentrar todas las solicitudes a través de sí.
    - Implementación de firewall IP: los firewalls IP deben configurarse con políticas de acceso estrictamente necesario a servicios, filtrado por dirección de origen, nivel de log detallado y tiempo de rotación coordinado con auditorías, y políticas en caso de acceso denegado de tipo DROP para limitar fugas de información.
    - Implementación de sistemas de detección tipo IDS/IPS: los *Intrusion Detection / Prevention Systems* envían alertas en caso de detectar tráfico malintencionado. Para que sean efectivos deben coordinarse con procesos de monitoreo y auditoría.

- Implementación de *honeypots:* para asegurar las capas exteriores de la arquitectura deben instalarse *honeypots*, es decir sistemas especialmente diseñados para dar la apariencia de ser muy vulnerables y fácilmente explotables, a fin de atraer a un atacante mientras emiten una alerta y guardan la información relacionada al ataque para su análisis. Nuevamente, si no existen procesos de monitoreo y auditoría dentro de la organización no se pueden aprovechar con efectividad.
- Implementación de acceso autorizado por VPN con autenticación multifactor: partiendo siempre del criterio de "acceso estrictamente necesario", para el acceso de usuarios y servicios remotos y en casos en los que por ejemplo por cuestiones presupuestarias o prácticas debe recurrirse al acceso a través de Internet, es fundamental la utilización de un túnel/VPN encriptada con autenticación multifactor. Por ejemplo existen soluciones con usuario y contraseña, más generación de un token de acceso de 30 o 60 segundos de duración, más autenticación con un certificado digital almacenado en una *smartcard*. Además, muchas veces proveen un cierto nivel de verificación de conformidad de políticas de seguridad por parte del *endpoint*.
- Implementación de acceso a interfaces web estrictamente a través de WAFs: un WAF o *Web Application Firewall* es un sistema que permite un nivel agregado de seguridad para las interfaces de usuario y webservices expuestos mediante el análisis de las solicitudes realizadas a nivel HTTP, y permite prevenir y detectar ataques web conocidos como inyección SQL, XSS, XSRF, etc. Son totalmente compatibles con HTTPS.

- **Fugas de datos:**
  - Implementar políticas de actualización de software y firmware: la naturaleza permanentemente cambiante de la tecnología y técnicas de los atacantes, las nuevas vulnerabilidades, vectores de ataque y herramientas desarrolladas hacen que la seguridad más invulnerable de hace 6 meses sea un blanco fácil hoy. Es la opinión del autor que el no tener en cuenta este concepto de ciclo de actualización y obsolescencia tan rápido es a veces la causa de muchos problemas de seguridad de sistemas industriales que son diseñados por ingenieros de áreas con ritmos de obsolescencia

más lentos como el control industrial, electricidad, infraestructura, automatización, etc.

- Seleccionar implementaciones basadas en sistemas operativos seguros, probados y certificados: Algunos sistemas operativos tienen certificaciones por parte de organizaciones de auditoría de seguridad y estándares internacionales, como por ejemplo la *Common Criteria for Information Technology Security Evaluation* (ISO/IEC 15408) o *Federal Information Processing Standard Publication* FIPS 140-2.
- Denegar acceso a puertos TCP/UDP no esenciales para el servicio a nivel de firewall: surge de la aplicación directa del criterio de "acceso estrictamente necesario". Para establecer una regla de acceso a un puerto a un cliente determinado debe justificarse claramente la necesidad de acceso para el funcionamiento, y en caso contrario filtrarse las solicitudes de conexión y registrarse en los log de control de acceso con todo detalle.
- Denegar uso de protocolos y servicios de red no esenciales: al igual que el ítem anterior, pero extensivo a protocolos y servicios de capas inferiores. Por ejemplo, el caso más típico es la denegación de ping ICMP, o de IGMP, por la posibilidad de su explotación para hacer reconocimiento de red o generar un ataque de denegación de servicio.
- Denegar acceso de paquetes anómalos usados para *fingerprinting* de sistemas operativos: para detectar el tipo de sistema operativo y versión ejecutada se envían paquetes especialmente diseñados a puertos abiertos y cerrados, y se analizan las respuestas a la búsqueda de particularidades en la implementación de la pila TCP/IP. Muchas veces estas particularidades no se encuentran en los mecanismos de uso común de la pila TCP/IP, si no en la implementación de funciones oscuras o poco utilizadas, y esto se relaciona con que la definición de protocolos TCP/IP deja ciertos parámetros liberados a la implementación del sistema operativo. Por lo tanto, muchos firewalls proveen detección y filtrado de paquetes exóticos para prevenir el *fingerprinting*.

- **Protocolos de conexión segura obsoletos:**
  - Actualizar a última versión de TLS

    - Implementar procesos y políticas permanentes de auditoría interna y externa: el proceso de auditoría permanente permite detectar vulnerabilidades de antemano, y generar requerimientos de actualización para prevenir la obsolescencia.
    - Implementar autenticación mutua y políticas de administración de certificados digitales: de esta forma puede garantizarse la confiabilidad y autenticidad de las comunicaciones, y mantener un ciclo de vida para los certificados digitales
- **Recomendaciones generales:**
    - Definir a nivel de organización un equipo responsable de seguridad: puede subcontratarse en casos de tratarse de organizaciones pequeñas, y hoy día las posibilidades de trabajo remoto permiten hacer *outsourcing* con mucha flexibilidad
    - Establecer políticas de entrenamiento de seguridad de datos continuo para el personal técnico: resulta fundamental que el personal responsable de comunicaciones, arquitectura de redes y sistemas de control esté en conocimiento pleno de las necesidades de seguridad de la organización
    - Implementar sistemas de *Endpoint Detection and Response*: muchas veces las fugas de información, o robo de credenciales, ocurren no a nivel de servidores, sino que son comprometidas las PC utilizadas por el personal que cuentan con un nivel de seguridad mucho menor. Para prevenir esto existen herramientas que verifican la conformidad de las PC que el personal utiliza para conectarse con las políticas de seguridad, por ejemplo que tengan un antivirus actualizado, encriptación de disco duro, etc.

6.2 Líneas futuras de investigación

Las principales líneas de investigación futuras a partir de este estudio que se proponen son las siguientes:

- **Vulnerabilidades de TLS/SSL en sistemas industriales:** Una de las conclusiones principales que derivan del estudio presente es que los protocolos de comunicaciones seguras son uno de los puntos débiles en las redes industriales. Por ello, es la opinión del autor que sería interesante

profundizar sobre este ítem en particular, analizando los siguientes parámetros:

- Expiración de certificados
- Longitud de cadena de certificación
- Certificados autofirmados
- Certificados de tipo “wildcard”

Para lograr este tipo de análisis podría diseñarse una metodología de detección un poco más intrusiva que la del estudio actual, porque requeriría completar la conexión TCP, completar el handshake TLS/SSL y recuperar la información del certificado del servidor.

- **Vulnerabilidades en servicios auxiliares**: El estudio presente se enfoca fundamentalmente en problemas de seguridad de los servicios de control industrial, y sus protocolos. Sin embargo, para la operación de una red industrial hacen falta muchos otros servicios y protocolos, que proveen o contribuyen a la infraestructura de red necesaria, pero también aportan a la superficie de ataque de las redes con sus propias vulnerabilidades. Podría diseñarse un estudio que partiera de la detección de sistemas y redes industriales en Internet de forma similar al trabajo presente, pero que enfocara la etapa de análisis de vulnerabilidades no solamente a los pertinentes a servicios de control industrial, si no al resto de servicios detectados en cada sistema. Podría diseñarse de manera previa una lista de puertos y servicios a buscar, o de forma más completa pero también más intrusiva, hacer un barrido de completo de rangos de puertos a la búsqueda de identificar cualquier tipo de servicio.
- **Vulnerabilidades en servidores de redes de control**: El trabajo presente aporta datos sobre problemas de seguridad en todo tipo de sistemas industriales sin discriminación. Sin embargo algunos componentes fundamentales de los sistemas de control que son los servidores donde corren servicios fundamentales como SCADA, bases de datos, historiadores, etc. requieren de una atención especial y el diseño de una metodología específica que tenga en cuenta sus particularidades para detectarlos y analizarlos desde una perspectiva de seguridad.

7 Bibliografía

1. Stouffer, K., Pilliteri, V., Lightman, S., Abrams, M. & Hahn, A. (2015, Mayo). Guide to Industrial Control Systems Security. National Institute of Standards and Technology
2. Peerenboom, James, (2001, Junio). “Infrastructure Interdependencies: Overview of Concepts and Terminology,” NSF/OSTP Workshop on Critical Infrastructure: Needs in Interdisciplinary Research and Graduate Training, Washington.
3. Rinaldi, Steven, et al., (2001, Diciembre). “Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies,” IEEE Control Systems Magazine,
4. Myers, D., Radke, K., Suriadi, S., & Foo, E. (2017, Mayo). Process Discovery for Industrial Control System Cyber Attack Detection. In IFIP International Conference on ICT Systems Security and Privacy Protection. Springer, Cham.
5. Bailey, D., Wright, E., (2003) Practical SCADA for Industry, Vancouver: IDC Technologies,
6. Boyer, S. (2010). SCADA: Supervisory Control and Data Acquisition. 4th ed. Research Triangle Park, North Carolina: International Society of Automation, 2010.
7. Erickson, K., Hedrick,J. (1999) Plantwide Process Control, New York: John Wiley & Sons, Inc.
8. Knapp, E., (2011) Industrial Network Security: Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems, Waltham, Massachusetts: Syngress,
9. Korman, M., Välja, M., Björkman, G., Ekstedt, M., Vernotte, A., & Lagerström, R. (2017, Abril). Analyzing the Effectiveness of Attack Countermeasures in a SCADA System. Proceedings of the 2nd Workshop on Cyber-Physical Security and Resilience in Smart Grids (pp. 73-78). ACM.
10. Stallings, W., (2011), Network Security Essentials: Applications and standards, 4ta ed. Prentice Hall
11. Guttman, B., Roback, E., (1995, Octubre). An Introduction to Computer Security: the NIST Handbook. NIST Special Publication
12. FIPS PUB 199, (2004) Standards for security categorization of Federal Information and Information Systems. Computer Security Division, Federal Information Processing Standards Publication, USA.

13. Shirey, R., (2000), RFC 2828, Internet Security Glossary

14. ITU-T Recomendación X.800, Security architecture for Open Systems Interconnection for CCITT Applications. (1991), CCITT, ITU-T
15. B. Miller, D. C. Rowe, (2012, Octubre) “A Survey of SCADA and Critical Infrastructure Incidents”, Proceedings of the 1st Annual conference on Research in information technology
16. Daniela, T. (2011). Communication security in SCADA pipeline monitoring systems. Roedunet International Conference
17. Denning, D.E. (2000). Cyberterrorism: The Logic Bomb versus the Truck Bomb - Centre for World Dialogue. Global Dialogue.
18. Turk, R.J. (2005). Cyber Incidents Involving Control Systems. Contract.
19. Remenyi, E. by D.D. et al. (2006, Junio). Proceedings of the 5 th European Conference on Information Warfare and Security: National Defence College, Helsinki, Finland
20. Tsang, R. Cyberthreats, Vulnerabilities and Attacks on SCADA Networks
21. Mustard, S., (2005). Security of distributed control systems: the concern increases. Computing & Control Engineering Journal.
22. Stamp, J. et al. (2003). Common vulnerabilities in critical infrastructure control systems. Sandia National Laboratories.
23. Nicholson, A. et al. (2012). SCADA Security in the light of Cyber-Warfare. Computers & Security.
24. Farwell, J.P. and Rohozinski, R. (2011). Stuxnet and the Future of Cyber War.
25. Zetter, K. (2011). Son of Stuxnet Found in the Wild on Systems in Europe. Wired
26. Zetter, K. (2012). “Flame” spyware infiltrating Iranian computers - CNN.com. Wired.
27. Xynos, K., Sutherland, I. et al (2010). “Penetration Testing and Vulnerability Assessments: A Professional Approach” (Proceedings of the 1st International Cyber Resilience Conference).

28. 28. Türpe, S., Eichler, J., (2009). “Testing Production Systems Safely: Common Precautions in Penetration Testing” (2009 Testing: Academic and Industrial Conference - Practice and Research Techniques).

29. 29. Babu, B., Ijyas, T., Muneer, P., & Varghese, J. (2017, Marzo). Security issues in SCADA based industrial control systems. Anti-Cyber Crimes (ICACC), 2017 IEEE.

30. Taormina, R., Galelli, S., Tippenhauer, N. O., Salomons, E., & Ostfeld, A. (2017). Characterizing Cyber-Physical Attacks on Water Distribution Systems. Journal of Water Resources Planning and Management.

31. Herzog, P. (2001). “Open-Source Security Testing Methodology Manual” (Institute for Security and Open Methodologies ISECOM).

32. Chiem, T. P. (2014). A study of penetration testing tools and approaches (Doctoral dissertation, Auckland University of Technology).

33. Shaikh, S. A., Chivers, H., Nobles, P., Clark, J. A., & Chen, H. (2008). Network reconnaissance. *Network Security*, *2008*(11), 12-16.

34. Wolfgang, M. (2002). Host Discovery with nmap. *Exploring nmap's default behavior*, *1*, 16.

35. Spangler, R. (2003). Analysis of remote active operating system fingerprinting tools. *University of Wisconsin*.

36. Na, S., Kim, T., & Kim, H. (2018). Service Identification of Internet-Connected Devices Based on Common Platform Enumeration. *Journal of Information Processing Systems*, *14*(3).

37. Huang, Y. W., Tsai, C. H., Lee, D. T., & Kuo, S. Y. (2004, November). Non-detrimental web application security scanning. In *15th International Symposium on Software Reliability Engineering* (pp. 219-230). IEEE.

38. Zhang, X., Knockel, J., & Crandall, J. R. (2015, April). Original SYN: Finding machines hidden behind firewalls. In *2015 IEEE Conference on Computer Communications (INFOCOM)* (pp. 720-728). IEEE.

39. Lupták, P. (2011). Bypassing Web application firewalls. In *Proceedings of 6th International Scientific Conference on Security and Protection of Information* (pp. 79-88).

40. Raza, M., Iqbal, M., Sharif, M., & Haider, W. (2012). A survey of password attacks and comparative analysis on methods for secure authentication. *World Applied Sciences Journal*, *19*(4), 439-444.

41. Bonguet, A., & Bellaiche, M. (2017). A survey of denial-of-service and distributed denial of service attacks and defenses in cloud computing. *Future Internet*, *9*(3), 43.
42. Kondo, T. S., & Mselle, L. J. (2014). Penetration testing with banner grabbers and packet sniffers. *Journal of Emerging Trends in computing and information sciences*, *5*(4), 321-327.
43. Pale, P. C. (2012). *Nmap 6: Network Exploration and Security Auditing Cookbook*. Packt Publishing Ltd.
44. El-Nazeer, N., & Daimi, K. (2011). Evaluation of Network Port Scanning Tools. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).
45. Dowling, B., Fischlin, M., Günther, F., & Stebila, D. (2015, October). A cryptographic analysis of the TLS 1.3 handshake protocol candidates. In *Proceedings of the 22nd ACM SIGSAC conference on computer and communications security* (pp. 1197-1210).

46. 46. Milinkovic, S., (2012, Noviembre). Industrial PLC security issues. Telecommunications forum TELFOR 2012.
47. 47. Sami, A., (2013, Diciembre). Era of insecure industrial control systems and calamities to come. Journal of Electronic Systems Volume III, Number 4.
48. 48. Yang, A., Li, J., Bian, Y., & Wang, X. (2016, Abril). The Cyber Security Evaluation of China's Nuclear Power Plant DCS System. In International Confernece Pacific Basin Nuclear Conference . Springer, Singapore.
49. 49. Nguyen, T., Irvine, C., (2018) Development of industrial network forensics lessons- Cybersec 2018
50. 50. Schneider Electric Security Notification SEVD-2018-074-01, (2018, Marzo). https://www.schneider-electric.com/en/download/document/SEVD-2018-074-01/
51. 51. ICS-CERT Advisory ICSA-17-243-01B (2017, Octubre). https://ics-cert.us-cert.gov/advisories/ICSA-17-243-01B
52. 52. ICS-CERT Advisory ICSA-17-129-01 (2017, Mayo). https://ics-cert.us-cert.gov/advisories/ICSA-17-129-01
53. 53. Schwab, W., Poujol, M., (2018, Junio). The state of industrial cybersecurity 2018. Kaskpersky Lab, CXP Group,