GRADO EN INGENIERÍA EN TECNOLOGÍAS INDUSTRIALES

TRABAJO FIN DE GRADO

Análisis de criterios de ciberseguridad en una planta de generación renovable

Autor: Luis Lázaro Trasobares

Director: Emilio Manuel Domínguez Adán

Madrid

Declaro, bajo mi responsabilidad, que el Proyecto presentado con el título

“Análisis de criterios de ciberseguridad en una planta de generación renovable”

en la ETS de Ingeniería - ICAI de la Universidad Pontificia Comillas en el

curso académico 2022 es de mi autoría, original e inédito y

no ha sido presentado con anterioridad a otros efectos.

El Proyecto no es plagio de otro, ni total ni parcialmente y la información que ha sido

tomada de otros documentos está debidamente referenciada.

LÁZARO TRASOBARES, LUIS (AUTENTICACIÓN)

Firmado digitalmente por LÁZARO TRASOBARES, LUIS (AUTENTICACIÓN)
Fecha: 2022.06.29 16:20:05 +02'00'

Fdo.: Luis Lázaro Trasobares Fecha: 29/ 06/ 2022

Autorizada la entrega del proyecto

EL DIRECTOR DEL PROYECTO

DOMINGUEZ ADAN EMILIO MANUEL - 02620715A

Firmado digitalmente por DOMINGUEZ ADAN EMILIO MANUEL - 02620715A
Fecha: 2022.06.29 16:30:36 +02'00'

Fdo.: Emilio Manuel Domínguez Adán Fecha: 29/ 06/ 2022

GRADO EN INGENIERÍA EN TECNOLOGÍAS INDUSTRIALES

TRABAJO FIN DE GRADO

Análisis de criterios de ciberseguridad en una planta de generación renovable

Autor: Luis Lázaro Trasobares

Director: Emilio Manuel Domínguez Adán

Madrid

ANÁLISIS DE CRITEROS DE CIBERSEGURIDAD EN UNA PLANTA DE GENERACIÓN RENOVABLE

Autor: Lázaro Trasobares, Luis.
Director: Domínguez Adán, Emilio Manuel.
Entidad Colaboradora: ICAI – Universidad Pontificia Comillas.

RESUMEN DEL PROYECTO

Este TFG lleva a cabo una labor de investigación exhaustiva de los elementos más plausibles de sufrir ciber ataques en una planta solar fotovoltaica. Además, demuestra mediante tres prácticas, lo sencillo que puede llegar a ser encontrar vulnerabilidades y aprovecharlas. Por último, propone modelos y soluciones para mejorar la ciberseguridad de la planta solar.

Palabras clave: Ciberseguridad, Planta solar, Energía renovable.

1. Introducción

Este proyecto se basa en el análisis de la ciberseguridad de una planta de generación solar fotovoltaica.

La red eléctrica es un elemento de máxima importancia para el correcto funcionamiento de un país. Sabiendo pues su importancia, nos encontramos ante una infraestructura que ha de ser protegida en todos sus puntos ante posibles ataques externos. Con la ampliación y descentralización de las energías y la creciente introducción de dispositivos inteligentes conectados a Internet en el sistema, se está derivando hacia un panorama en el que el riesgo de sufrir ciberataques es cada vez mayor.

Se ha escogido una planta solar dado que las energías renovables están en proceso de expansión y son necesarias para proporcionar un futuro próspero a las generaciones venideras. La importancia de la energía solar ha sido identificada por grandes potencias mundiales cómo China o India y jugará un papel muy importante en las próximas décadas. España tiene el clima indicado para la proliferación de este tipo de plantas de generación de energía y ha de ser capaz de adaptarse a las nuevas tendencias tecnológicas de forma ciber-segura.

2. Definición del Proyecto

Se presenta la arquitectura de una planta solar fotovoltaica, analizando tanto los componentes eléctricos como los principales protocolos de comunicaciones que se utilizan. Entre ellos se incluyen: inversores solares, cajas de corriente continua, servidores SCADA, el protocolo Modbus/TCP, etc. Es muy importante conocer el funcionamiento interno de estos elementos y los protocolos más utilizados para posteriormente, ser capaces de implementar las medidas de ciberseguridad necesarias de forma eficaz.

Más adelante, se tratan los criterios de ciberseguridad y robustez en su totalidad. Se comienza comprendiendo las diferencias entre el entorno IT y el entorno OT, que coexisten en una planta de generación, además de aportar soluciones de ciberseguridad en ambos. A modo de conclusión se proponen tanto guías generales de organismos

internacionales para la ciberseguridad de plantas industriales cómo modelos de referencia estructural para la seguridad de la red de comunicaciones.

El esquema de trabajo seguido ha sido el siguiente.

Figura 1: Esquema de Trabajo

3. Descripción del modelo/sistema/herramienta

A lo largo del proyecto se han utilizado tres (3) herramientas distintas con el fin de demostrar como un hacker puede obtener información sensible en un entorno industrial y utilizarla a su favor.

Se puede comprender la utilización de estas herramientas como parte de una buena práctica de ciberseguridad conocida como “pentesting”. Este proceso consiste en atacar de forma controlada y autorizada diferentes entornos o elementos con el objetivo de detectar y prevenir posibles fallos. Así se es capaz de solucionarlos antes de que puedan suponer una vulnerabilidad.

La primera herramienta se llama “Nmap”, un software de código abierto muy utilizado para realizar auditorías de seguridad dentro de una red. En concreto se ha utilizado la versión de Windows que tiene un sencillo interfaz gráfico. Su función principal es conocer con detalle todo lo que está ocurriendo dentro de una red a la que se tiene acceso. Monitorizar una red es necesario dado que permite conocer lo que está pasando en tiempo real, qué dispositivos están conectados, qué IPs y puertos se están utilizando y cualquier otra información importante para mantener la seguridad de la red.

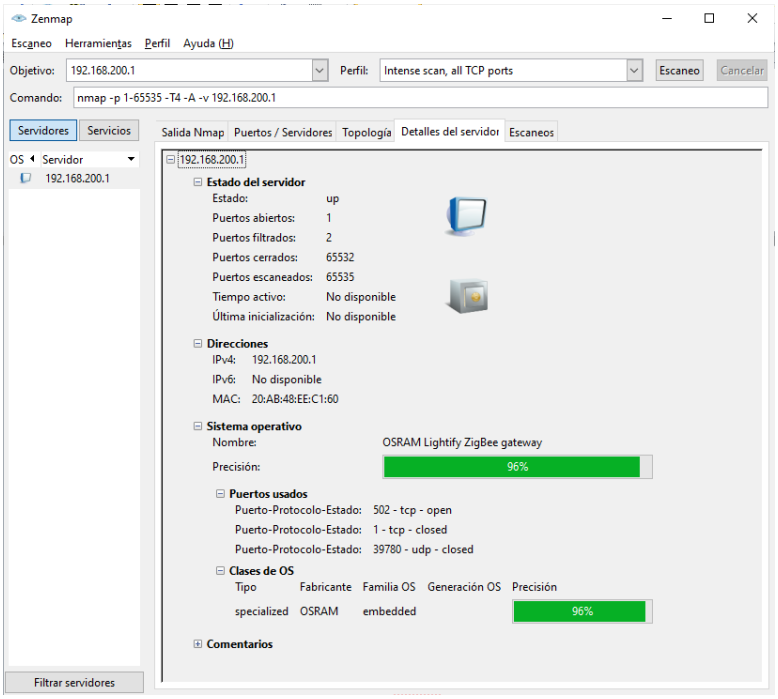


Figura 2: Información obtenida con Nmap

En segundo lugar, se ha utilizado "Shodan Search Engine", un buscador web que tiene como objetivo ubicar todo tipo de objetivos que están conectados a internet. Una vez localizado un dispositivo, puede mostrarnos los servicios abiertos e incluso posibles vulnerabilidades presentes.

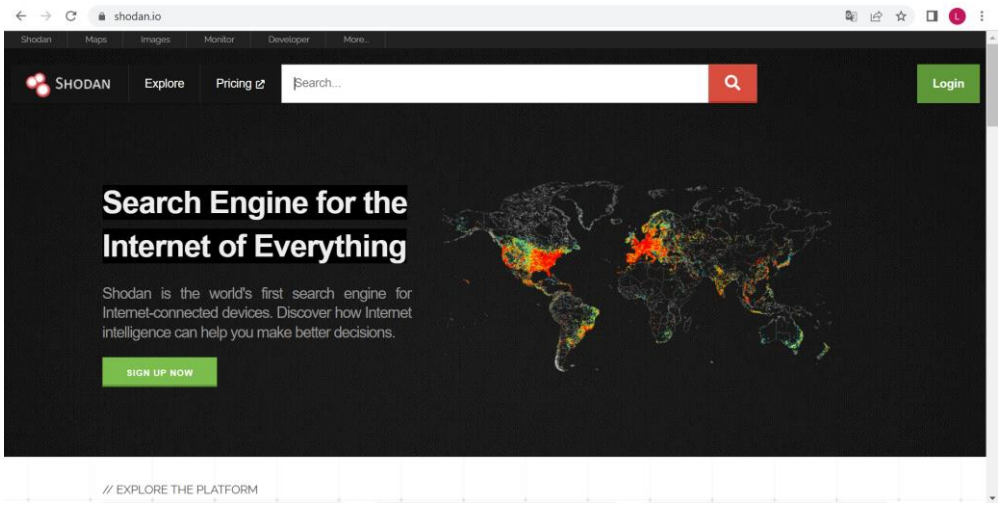


Figura 3: Pantalla de inicio de Shodan

La ventaja principal de Shodan es que lleva a cabo una búsqueda silenciosa, ajena al usuario que está siendo atacado ya que busca en una base de datos como si fuera Google, no se conecta directamente a la red de la víctima

La última herramienta utilizada es Metaesploit, una aplicación muy popular para realizar tests de penetración y sistemas de detección de intrusos. Metaesploit nos permite ejecutar distintos exploits para ver cómo actúan. Esta herramienta la utilizamos en Kali Linux,

una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática.

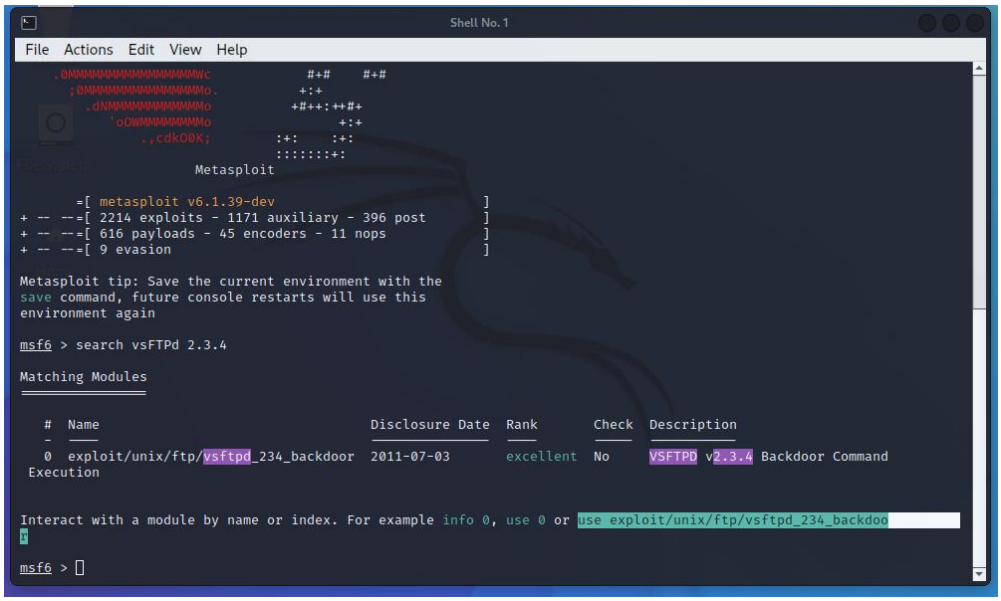


Figura 4: Exploit a utilizar en Metaesploit

Se va a intentar acceder a una máquina virtual que tienen vulnerabilidades previamente identificadas utilizando Metaesploit. En este caso, se logrará gracias a una vulnerabilidad no parcheada, acceder por una puerta trasera sin necesidad de identificación.

4. Resultados y Conclusiones

La realización de las prácticas de ciberseguridad demuestra como gracias a Internet, con las herramientas adecuadas y unos conocimientos básicos se puede obtener y aprovechar información sensible de distintos sistemas y dispositivos. Este hecho aumenta las preocupaciones acerca de lo que puede ser capaz de hacer un hacker con conocimientos y prácticas avanzadas en algún punto la red eléctrica.

La conclusión principal que se obtiene tras la realización de este proyecto nos lleva a afirmar que lograr un entorno completamente ciberseguro en el mundo moderno hiperconectado en el que nos encontramos es imposible. La cadena de la ciberseguridad tiene demasiados eslabones y con que uno se rompa el sistema puede venirse abajo. Aún así, es indispensable seguir un modelo o una guía de buenas prácticas para ser capaz de detectar las brechas y solventarlas con rapidez. Por otro lado, se deduce que la mayoría de los ataques provienen de fallos humanos y de ahí la necesaria labor de formación en ciberseguridad que se ha de realizar en los entornos industriales en los próximos años.

La dependencia de los países de las energías renovables para proporcionar un futuro próspero a las nuevas generaciones solo aumentará de la mano de los intereses de los hackers en atacar este tipo de infraestructuras. Por ello, se subraya la importancia de adaptar estas platas renovables a un modelo ciberseguro y fiable.

ANALYSIS OF CYBERSECURITY CRITERIA AT A RENEWABLE GENERATION PLANT

Author: Lázaro Trasobares, Luis.
Supervisor: Domínguez Adán, Emilio Manuel.
Collaborating Entity: ICAI – Universidad Pontificia Comillas

ABSTRACT

This TFG carries out an exhaustive investigation of the most sensitive elements to suffer cyber-attacks in a photovoltaic solar plant. It also demonstrates, through three practical exercises, how easy it can be to find vulnerabilities and exploit them. Finally, it proposes models and solutions to improve the cybersecurity of the solar plant.

Keywords: Cybersecurity, P.V. Plant, Renewable energy.

1. Introduction

This project is based on the analysis of the cybersecurity of a solar photovoltaic generation plant.

The electricity grid is an element of the utmost importance for the correct functioning of a country. Knowing its importance, we are faced with an infrastructure that must be protected at all points against possible external attacks. With the expansion and decentralization of energy and the increasing introduction of internet-connected smart devices into the system, the risk of cyber-attacks is growing.

A solar plant has been chosen as renewable energies are in the process of expansion and are necessary to provide a prosperous future for generations to come. The importance of solar energy has been identified by major world powers such as China and India and will play a very important role in the coming decades. Spain has the right climate for the proliferation of this type of energy generation plants and must be able to adapt to new technological trends in a cyber-safe way.

2. Project Definition

First, the architecture of a solar PV plant is presented. Analyzing both the electrical components and the communications protocols used. These include solar inverters, string box, SCADA servers, the Modbus/TCP protocol, etc. It is very important to know the inner workings of these elements and protocols in order to be able to implement the necessary cybersecurity measures effectively.

Later, the cybersecurity and robustness criteria are discussed. It starts by understanding the differences between the IT environment and the OT environment, which coexist in a power plant. In addition to providing cybersecurity solutions in both. Proposing both general guidelines from international organizations for the cybersecurity of industrial plants and structural reference models for network security.

The working outline was as follows.

Figure 1: Work scheme

3. Description of the model/system/toll

Throughout the project, 3 different tools have been used to demonstrate how a hacker can obtain sensitive information from an industrial environment and use it to his advantage.

The use of these tools can be understood as part of a good cybersecurity practice known as pentesting. This process consists of attacking different environments or elements in a controlled and authorized manner with the aim of detecting and preventing possible failures. In this way, it is possible to fix them before they become a vulnerability.

The first tool is called "Nmap", an open-source software widely used to perform security audits within a network. Specifically, the Windows version has been used, which has a simple graphical interface. Its main function is to know in detail everything that is happening within a network to which you have access. Monitoring a network is necessary because it allows you to know what is happening in real time, what devices are connected, what IPs and ports are being used and other important information to maintain the security of the network.

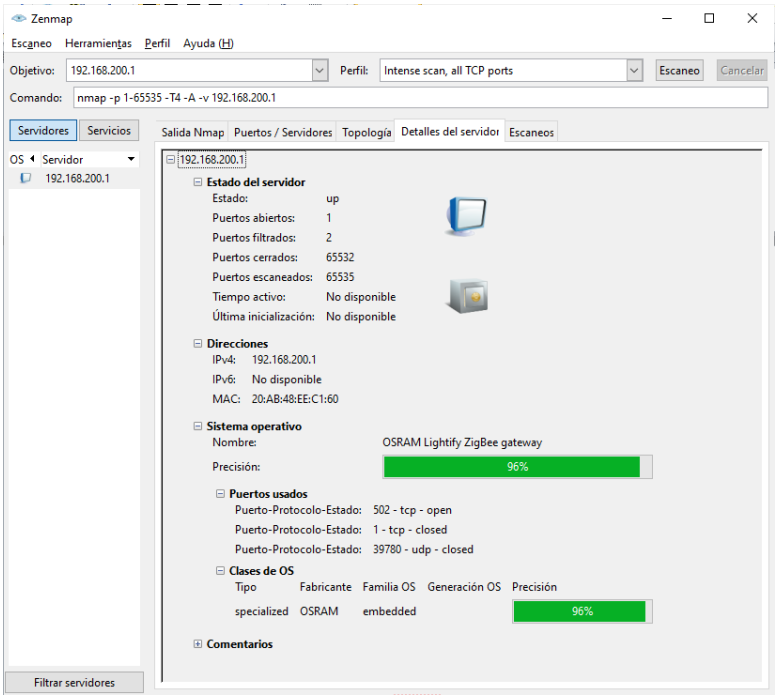


Figure 2: Results obtained with Nmap

Secondly, "Shodan Search Engine" has been used, a web search engine that aims to locate all types of targets that are connected to the internet. Once a device has been located, it can show us the open services and even possible vulnerabilities.

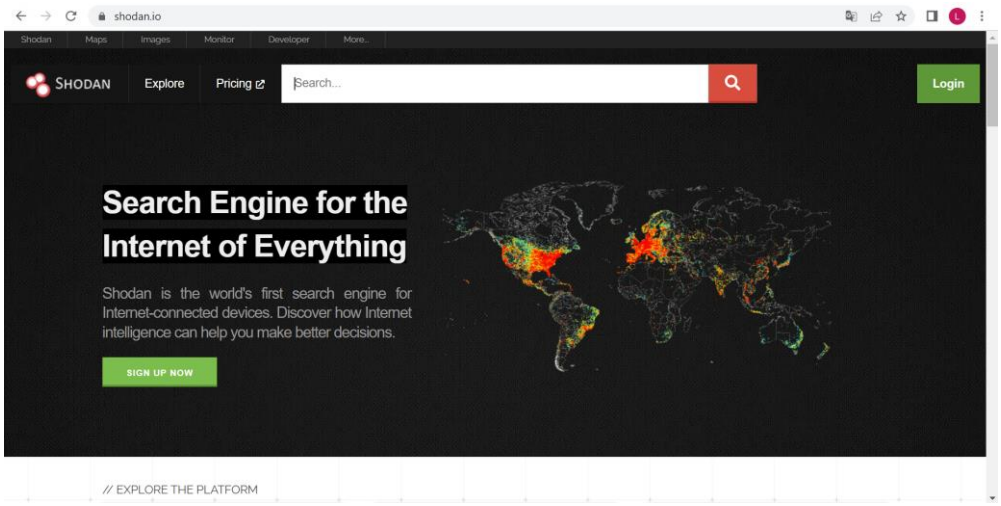


Figure 3: Shodan main browser

The main advantage of Shodan is that it performs a silent search, oblivious to the user being attacked as it searches a database like Google, not connecting directly to the victim's network.

The last tool used is Metaesploit, a very popular application for penetration testing and intrusion detection systems. Metaesploit allows us to run different exploits to see how

they work. We use this tool on Kali Linux, a Debian GNU/Linux-based distribution designed primarily for computer security and auditing.

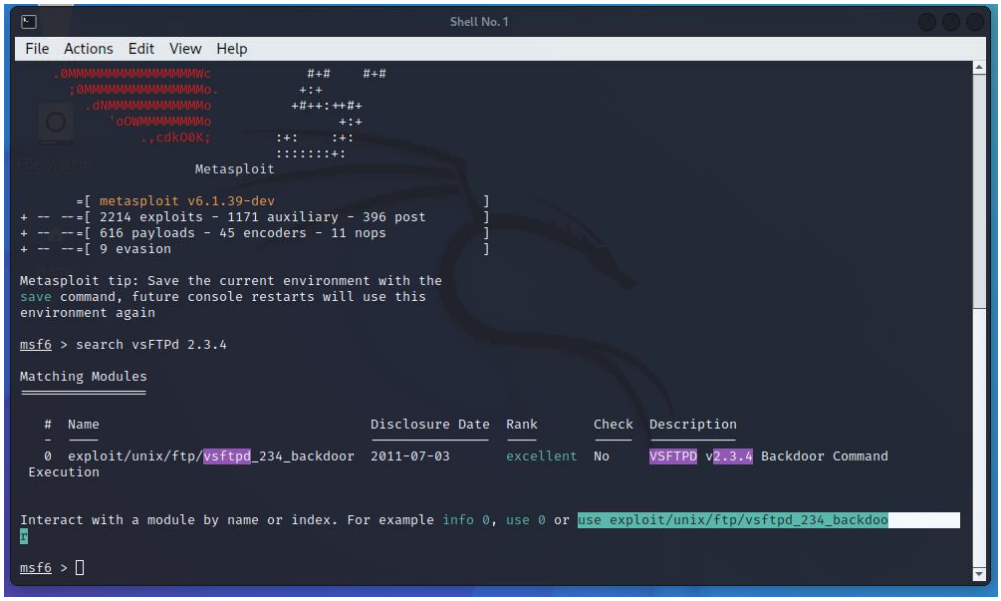


Figure 4: Metasploit screen capture

An attempt will be made to access a virtual machine that has previously identified vulnerabilities using Metaesploit. In this case, an unpatched vulnerability will be used to gain access through a backdoor without the need for identification.

4. Results & Conclusions

The completion of the cybersecurity practices demonstrates how using the Internet, with the right tools and basic knowledge, sensitive information can be obtained and exploited from different systems and devices. This fact raises concerns about what a hacker with advanced knowledge and practices might be able to do at some point in the power grid.

The main conclusion to be drawn from the completion of this project is that achieving a fully cyber-secure environment in the modern hyper-connected world in which we find ourselves is impossible. The cyber security chain has too many links and if one link breaks, the system collapses. Even so, it is essential to follow a model or best practice guide to be able to detect breaches and address them quickly. On the other hand, most attacks come from human error, hence the need for cybersecurity training in industrial environments in the coming years.

The dependence of countries on renewable energies to provide a prosperous future for new generations will only increase with the interest of hackers in attacking this type of infrastructure. It therefore underlines the importance of adapting these renewables to a cyber-secure and reliable model.

Índice de la memoria

Índice de figuras

Índice de tablas

Capítulo 1. INTRODUCCIÓN

1.1 CIBERSEGURIDAD Y SU ESTADO ACTUAL

La ciberseguridad engloba el conjunto de medidas y operaciones que se aplican a un equipo o una red para protegerlos frente posibles ataques externos, intentos de robo de información o control del dispositivo.

El ser humano, a lo largo de la historia siempre ha tratado de proteger sus bienes de forma efectiva. La seguridad es la ausencia de riesgo, y por ello la ciberseguridad es la disciplina encargada de evaluar, estudiar y gestionar los riesgos asociados al mundo digital.

En los últimos años, con la transformación digital que ha sufrido el mundo moderno, el número de ciberataques ha aumentado exponencialmente suponiendo pérdidas millonarias para muchas empresas. El desarrollo de la ciberseguridad ha sido muy lento en comparación al desarrollo tecnológico. La tecnología buscaba avanzar a cualquier coste, es decir, al inventar o desarrollar un producto lo importante era su correcto funcionamiento, pero nadie se paraba a pensar si al mismo tiempo se estaba protegiendo el producto contra ataques externos. Por ello, hoy en día las carencias en el sector de la ciberseguridad son abismales y hay una evidente falta de formación en los trabajadores. Afortunadamente la industria se ha percatado de ello, la ciberseguridad es un sector en auge que experimentará fuertes inversiones en las próximas décadas. Desafortunadamente todavía nos encontramos muy lejos de la situación óptima y de ahí la importancia de analizar el contexto de la ciberseguridad en distintos sectores claves de la sociedad.

1.2 IMPORTANCIA DE LA CIBERSEGURIDAD EN EL SECTOR ELÉCTRICO

Un reto clave al que se va a enfrentar el ser humano en las próximas décadas es el desarrollo de un modelo energético sostenible, seguro y eficaz. El sol es una fuente de energía que siempre va a estar a nuestra disposición y a la que sacamos un partido ínfimo en comparación a su potencial. Con la ampliación y descentralización de las energías que constituyen el sistema de aprovisionamiento y con la creciente introducción de dispositivos inteligentes en el sistema se está derivando hacia un escenario en el que el riesgo de sufrir ciberataques es cada vez mayor.

La red eléctrica es uno de los sistemas más complejos desarrollado por el ser humano y es un elemento de máxima importancia para el correcto funcionamiento de un país. Sabiendo pues su importancia, nos encontramos ante una infraestructura que ha de ser protegida ante posibles ataques externos.

Cada vez son más los incentivos para instalar plantas de producción de energía renovable dentro de la red eléctrica y nos encontramos en un punto de transición hacia el futuro. España entre muchos otros países de la Unión Europea se encuentra en un punto de rápida ampliación del número de plantas fotovoltaicas para hacer frente al aumento de la demanda energética y ser capaz de proveer esta energía de forma renovable. El mayor ejemplo de implantación de plantas solares es China, líder mundial en energía solar, un país que hace años supo identificar la importancia de esta tecnología y comprender que de cara al futuro iba a ser clave. Algunos ejemplos de plantas solares a gran escala son el Parque Solar del Desierto de Tengger con una capacidad de 1.547 MW que se conectó a la red en 2016. Otras potencias emergentes cómo la India también han sido capaces de identificar el papel capital que jugarán este tipo de energías y en marzo de 2020 finalizó la construcción de Bhadla Solar Park con una capacidad de 2.245 MW. Para entender la magnitud de estas construcciones hemos de entender que por ejemplo la planta solar de Totana en Murcia tiene una potencia autorizada de 85MW.

Figura 1:Bhadla Solar Park (https://www.flickr.com/photos/cifaction/43943012564)

1.3 MOTIVACIÓN

Es una realidad que el ritmo de consumo de recursos que de la sociedad moderna es insostenible a largo plazo con el modelo energético actual. Las plantas de producción de energía tradicional han de ser sustituidas poco a poco por plantas renovables y en España el potencial de la energía fotovoltaica es esperanzador.

La integración de la red de plantas de energía solar fotovoltaica a gran escala representa muchos desafíos que afectan a la estabilidad, confiabilidad y calidad de la energía del sistema debido a la naturaleza intermitente de la radiación solar y a los problemas de acceso físico a los lugares donde la mayoría de las plantas de energía fotovoltaica están ubicadas.

Garantizar el funcionamiento confiable y seguro de las redes eléctricas es fundamental para la economía y la seguridad nacional de cualquier país. Durante las últimas décadas hemos creado una dependencia absoluta a la electricidad para poder desarrollar nuestra vida de

forma normal. Más allá, del funcionamiento de todos los aparatos eléctricos, Internet depende de esta energía, un apagón global que dejara algún territorio sin conexión sería un absoluto desastre económico y social. A medida que aumenta la cantidad de energía solar en la red, esta energía se convertirá en una parte integral del sistema y proporcionará resistencia adicional al suministro de electricidad porque las instalaciones solares están dispersas, lo que las hace más resistentes a interrupciones generalizadas.

Sin embargo, los desafíos de la ciberseguridad se complican por la gran cantidad de propietarios y operadores involucrados en la energía solar. Cuanto más abarque la infraestructura del sistema, más vulnerabilidades pueden aparecer. Las plantas solares deben ser más conscientes y ciberseguras, con capacidad para prevenir, identificar, detectar, responder y recuperarse de los ciberataques. También es fundamental concienciar a los operadores de sistemas solares sobre los estándares de ciberseguridad y las mejores prácticas para la gestión de riesgos. Este aspecto se tratará también en este trabajo ya que muchas veces el factor humano es el más peligroso. En resumen, si las plantas no son ciberseguras, no son fiables y la fiabilidad es un elemento clave en la ingeniería.

La motivación de este TFG es realizar un trabajo de investigación que logre analizar la situación y colaborar a un futuro mejor.

La ingeniería siempre ha buscado solucionar problemas de forma práctica y eficaz. En la sociedad moderna la ingeniería tiene un papel determinante analizando soluciones tecnológicas a los retos de la sociedad. Como ingeniero tengo una grave preocupación por el futuro de nuestro planeta y las energías renovables pueden ser una gran oportunidad para el ser humano. De ahí mi concienciación con la necesidad de proteger las plantas solares fotovoltaicas para su correcto funcionamiento.

1.4 ALINEACIÓN CON LOS OBJETIVOS DE DESARROLLO SOSTENIBLE (ODS)

Los objetivos de desarrollo sostenible (ODS) establecidos por las naciones Unidas en la Agenda 2030 creada en 2015 buscan prosperidad compartida en un mundo sostenible: un mundo en el que todas las personas puedan llevar una vida productiva, vibrante y pacífica en un planeta sano.

Al tratar la ciberseguridad de una planta solar de producción de energía renovable, este TFG se alinea de forma directa con varios ODS.

El ODS número 3 es "Garantizar una vida sana y promover el bienestar de todos a todas las edades". Ha quedado ampliamente demostrado por infinidad de estudios en los últimos años que la contaminación afecta gravemente a la salud general de todos los seres humanos. Con la implantación de plantas renovables se produce una transición hacia un futuro dónde los combustibles fósiles juegan un papel minoritario y la contaminación del aire se ve reducida. Para que esta transición sea efectiva las plantas han de ser fiables y ciberseguras. De ahí la importancia de la ciberseguridad en este tipo de centros de producción para garantizar una vida más saludable.

Este razonamiento se alinea además con el ODS número 13 "Adoptar medidas urgentes para combatir el cambio climático y sus efectos".

El ODS número 7 propone "Garantizar el acceso a una energía asequible, fiable, sostenible y moderna para todos". Cuando se comenzó a introducir la energía solar uno de sus mayores problemas era su elevado coste. Por eso varios países cómo Alemania incorporaron tarifas para bonificar a los consumidores si implantaban placas solares. Afortunadamente, hoy en día la energía solar es mucho más barata y asequible para todo el mundo. Respecto a la fiabilidad exigida por este objetivo de desarrollo sostenible, es ahí dónde la ciberseguridad es capital. Las plantas de producción han de ser seguras y capaces de resistir los incesantes ataques de los hackers para hacer que estas dejen de funcionar.

Por último, el ODS número 12 esta relacionado con la producción y consumo responsables y busca "Garantizar modalidades de consumo y producción sostenibles". La huella material esta creciendo descontroladamente y los recursos del planeta son limitados, de ahí la importancia de controlar el consumo de estos y limitar en la mayor medida de lo posible su utilización. El sol es un bien ilimitado que nos proporciona constantemente energía, el uso de la energía solar es una solución perfecta para no consumir los recursos de nuestro planeta. Fomentar la introducción de plantas fotovoltaicas para aportar energía al sistema es una forma práctica y eficaz de arreglar el problema de la huella material.

1.5 OBJETIVOS DEL PROYECTO

1. Analizar los riesgos existentes asociados a los ciberataques en plantas fotovoltaicas. Se busca comprender y evaluar el riesgo de distintos ciberataques que pueden sufrir las plantas de generación de energía fotovoltaicas. Por otro lado, también se analizarán las medidas que existen actualmente para mitigarlos llevando a cabo un estudio sobre su fiabilidad y cómo mejorar la infraestructura para prevenir irrupciones externas en el sistema.

2. Estudio de la arquitectura de una planta solar fotovoltaica desde el punto de vista de los sistemas de control y gestión remota, comunicaciones utilizadas y los aspectos principales referidos a su ciber-riesgo.

3. Análisis de herramientas y técnicas de hacking utilizados contra plantas de generación de energía solar fotovoltaica, incluyéndose las instalaciones tanto grandes como pequeñas. Para comprender un problema en su totalidad hay que analizarlo desde perspectivas distintas. En este caso se analizará la situación desde el punto de vista de un hacker cuyo objetivo es obtener información sensible sobre la infraestructura.

4. Recopilación de normativas y hojas de ruta para la implantación de ciberseguridad en este tipo de instalaciones. Análisis de la situación actual y los requerimientos que establece España para el correcto funcionamiento de una planta de generación de energía renovable de forma cibersegura.

Capítulo 2. ARQUITECTURA Y ELEMENTOS DE UNA PLANTA SOLAR FOTOVOLTAICA

2.1 ELEMENTOS QUE COMPONEN UNA PLANTA SOLAR FOTOVOLTAICA

2.1.1 EFECTO FOTOELÉCTRICO, FOTOVOLTAICO Y CÉLULAS SOLARES

La energía solar fotovoltaica basa su funcionamiento en el efecto fotoeléctrico. El efecto fotoeléctrico consiste en la emisión de electrones por un material al incidir sobre él una radiación electromagnética (luz visible o ultravioleta).

Gracias al efecto fotoeléctrico podemos conseguir el efecto fotovoltaico, que consiste en la transformación parcial de la radiación electromagnética del sol en energía eléctrica. Esto ocurre cuando los fotones provenientes del sol impactan en unos dispositivos electrónicos llamados células fotovoltaicas. Una cierta porción de estos fotones es absorbida por el material semiconductor y otra parte sale rebotada, con esto, la energía absorbida se transfiere al semiconductor, esta energía hace que los electrones se puedan separar de los átomos y fluir libremente.

Las células fotovoltaicas tienen uno o más campos eléctricos cuya función principal es obligar a los electrones, liberados por la absorción de la energía lumínica, a fluir en una dirección determinada, este flujo de electrones produce una corriente y al colocar contactos de metal en la parte superior e inferior de la célula, podemos extraer esta corriente continua (CC) para un uso externo.

Las células fotovoltaicas están constituidas por materiales semiconductores, básicamente silicio enriquecido, complementado con fósforo y boro. Las capas de silicio y el fósforo suministran una carga negativa (semiconductor tipo N) y la de boro aporta la carga positiva (semiconductor tipo P).

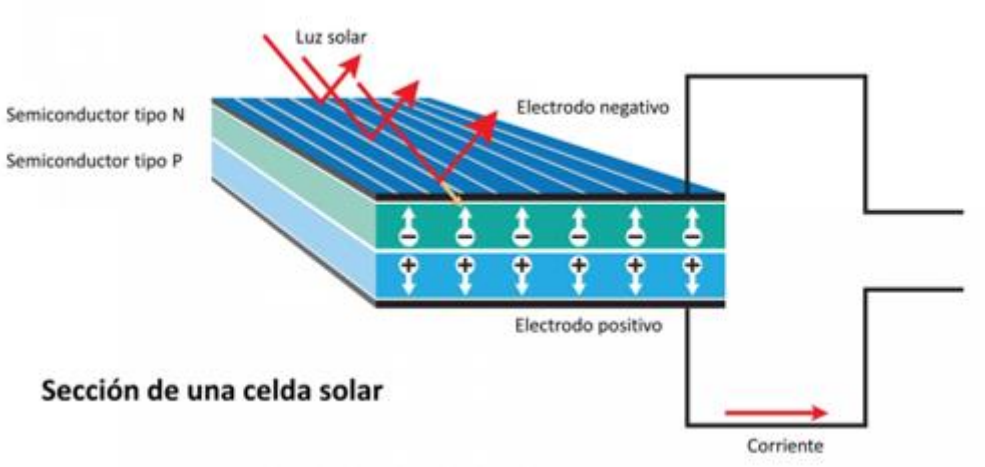


Figura 2: Efecto fotoeléctrico en una célula solar (https://www.inntecsol.mx/instalaciones-electricas/)

2.1.2 PANELES Y MESAS SOLARES

Las células solares se interconectan en serie o en paralelo formando un módulo fotovoltaico, que tiene como objetivo para cumplir con los requisitos de tensión y corriente establecidos en el diseño.

A su vez varios módulos se ensamblan en una estructura sencilla que permita su manejo, conexionado y transporte, son los paneles solares fotovoltaicos. Por último, en las plantas de generación, múltiples paneles solares forman un "string" que se monta encima de lo que se denominan mesas solares, que generalmente tienen sistemas de seguimiento solar para mejorar el rendimiento.

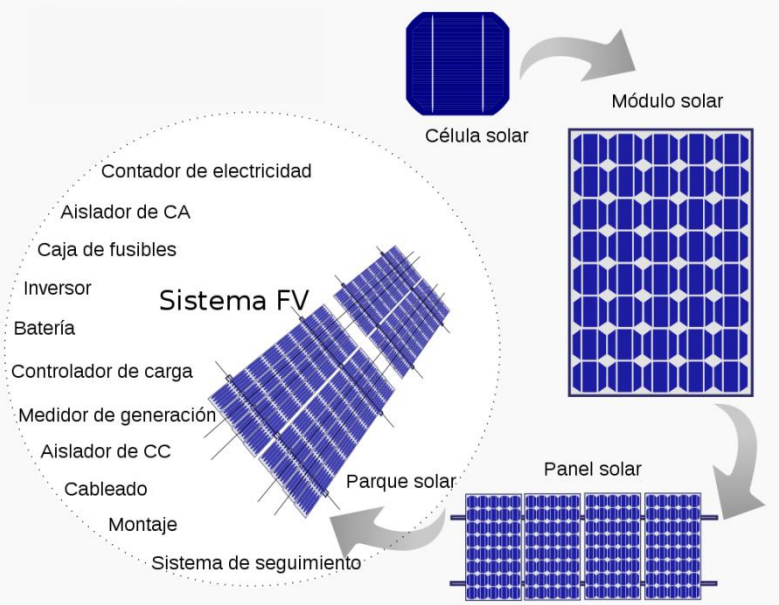


Figura 3: Célula, módulo y panel solar (Wikipedia)

Figura 4: Mesas solares

Los paneles solares, suelen tener una potencia unitaria pico entre 325 Wp y 550 Wp. La tecnología utilizada en plantas de generación fotovoltaica puede ser monocristalina o

policristalina. Hoy en día, se han introducido también las placas fotovoltaicas bifaciales que se caracteriza por ser sensible a la luz por ambas caras.

Los módulos monocristalinos poseen los índices de eficiencia altos y funcionan mejor que los policristalinos en condiciones de baja radiación solar. Se elaboran a partir de bloques de silicio enteros, lo que hace más costosa su fabricación. Sin embargo, su vida útil es más larga. Se distinguen por su color negro.

Los policristalinos se caracterizan porque su estructura cristalina no es uniforme en toda su extensión, siendo menos eficientes que los monocristalinos y se requiere una mayor cantidad de ellos para lograr la misma potencia. Son de color azul.

Figura 5: Panel con módulos monocristalinos de 550WP (https://www.amazon.es)

2.1.3 SEGUIDORES SOLARES

Los seguidores solares son mecanismos de orientación de los paneles solares que permiten aumentar el rendimiento de éstos según la posición del sol.

En función del eje y sus ajustes respecto al sol, los seguidores solares se pueden clasificar en seguidores solares en un eje (horizontal, polar o azimutal) y seguidores solares de dos ejes (siempre perpendiculares al sol). Por razones económicas y de disminución de su

complejidad, la tendencia actual es montar seguidores en un eje de giro en dirección Norte-Sur con movimiento de giro en dirección Este-Oeste para seguir el movimiento diario del sol.

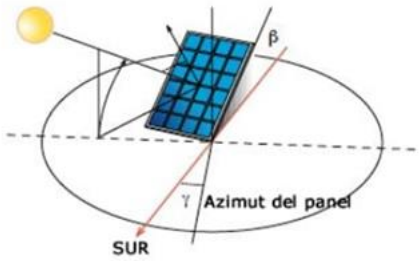


Figura 6: Orientación panel solar

Se estima que la instalación de seguidores solares mejora el rendimiento hasta un 20% - 30% en algunos casos de alta incidencia de luz solar.

Hay varios tipos de seguidores según los paneles han de moverse durante el día o solamente al cambiar de estación.

2.1.4 CAJAS DE CORRIENTE CONTINUA

Las cajas de nivel o "stringbox" son gabinetes metálicos preparados y protegidos para su instalación en el exterior (protección mínima IP54). Combinan las cadenas o "strings" de paneles solares y envían por un solo cable de CC toda la energía producida por estas a un inversor de CC/CA. La finalidad de las cajas de corriente continua es la reducción de pérdidas y disminución de costes en el cableado de CC.

Van equipadas además con diferentes tipos de protecciones eléctricas (seccionador en carga bipolar y fusibles, para tensión de hasta 1.500 V en corriente continua).

2.1.5 INVERSORES DE CORRIENTE

Los inversores son los elementos encargados de cambiar el voltaje de entrada de corriente continua proveniente de las mesas a un voltaje de salida de corriente alterna con la magnitud

y frecuencia necesaria para conectarse a los transformadores internos de las estaciones de transformación.

Figura 7: Isla de inversores de CC a CA

Los inversores disponen de microprocesadores que les permite controlar y almacenar gran cantidad de datos. Tanto parámetros eléctricos (tensión, intensidad, frecuencia, potencia, armónicos, rizados de intensidad, etc.) como parámetros externos (radiación, temperatura exterior, seguidores solares, etc.) e internos (temperaturas de trabajo, protecciones, etc.).

Existen diferentes configuraciones para la interconexión de los strings con los inversores: Inversores centrales, cadena de inversores o inversores en string y, por último, cadena múltiple o múltiple string. La selección de una u otra alternativa se basa en el tipo de planta, el coste y la fiabilidad deseada.

En la configuración de inversores centralizados (figura 8), todos los paneles fotovoltaicos están conectados a un inversor central de alta potencia. Son equipos grandes que en la mayoría de los casos precisan de una base sólida sobre la que asentarse, se utilizan en las grandes plantas de generación fotovoltaica.

En este tipo de configuración, las mesas solares se agrupan en matrices. Cada matriz fotovoltaica consta de muchas cadenas conectadas en paralelo y cada cadena consta de muchos paneles fotovoltaicos conectados en serie.

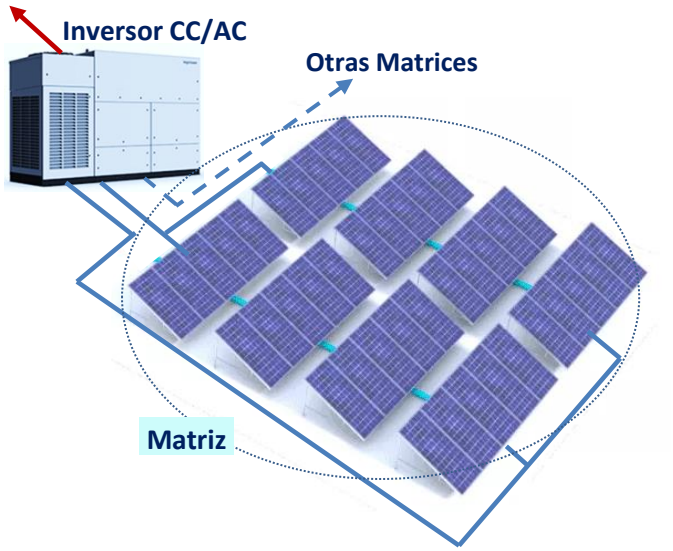


Figura 8: Configuración de inversores centralizados

En este tipo de configuración es imprescindible utilizar cajas de corriente continua ya que las entradas al inversor están preparadas para conectar intensidades muy altas, lo que implica cables más gruesos. Por un lado, esto facilita la instalación, pero el inversor no es capaz de saber lo que pasa a nivel de cadena, sólo lo ve a nivel de caja de nivel.

En la configuración de cadena (figura 9), cada cadena está conectada directamente al inversor. Esto permite que el inversor pueda monitorizar cada uno de los "strings" conectados a él. Además, este tipo de inversores llevan incorporados el algoritmo de funcionamiento conocido como MPPT (Maximum Power Point Tracker o seguidores del punto de máxima potencia), lo que posibilita optimizar la producción a nivel de cadena.

Esto es muy útil en instalaciones donde las mesas tienen diferente orientación, inclinación o sombras. Esto suele ocurrir en plantas comerciales orientadas a autoconsumo industrial o en grandes instalaciones de generación solar (250 MW o más).

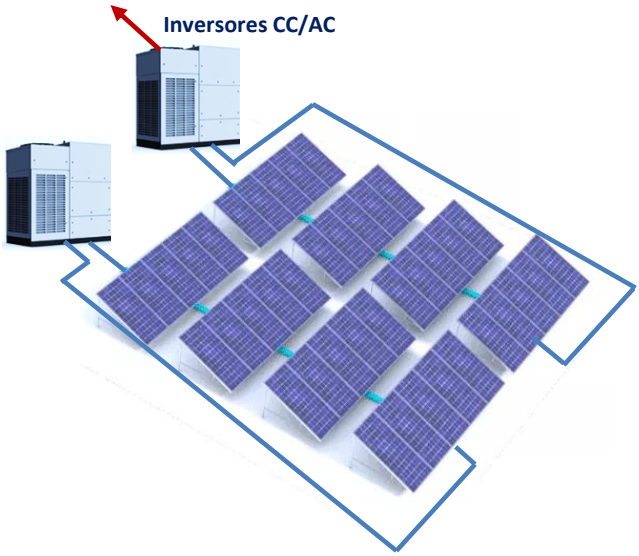


Figura 9: Configuración de cadena de inversores

En el caso de una configuración de cadenas múltiples (figura 10), las cadenas están conectadas a un conversor de CC/CC y cada grupo de conversión CC/CC está conectado un Inversor CC/CA.

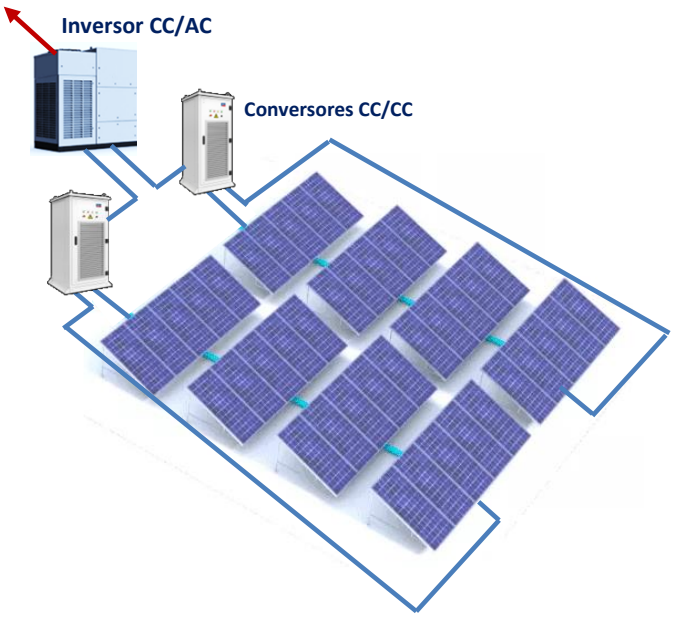


Figura 10: Configuración de cadenas múltiples

2.1.6 CENTRO DE TRANSFORMACIÓN

En las plantas de generación de energía fotovoltaica el centro de transformación de media tensión se encuentra integrado con el inversor, en lo que se denomina estación de potencia. Su misión es elevar la tensión de salida de los inversores para minimizar las pérdidas, antes de enviar la energía generada por la instalación fotovoltaica al centro de seccionamiento y posteriormente a la línea de media tensión (11, 22, 30 KV) que permite la interconexión con las redes de transporte de energía eléctrica.

También se incluye equipamiento de protección, monitorización y control y panel de conexiones eléctricas entre los diferentes elementos. En la figura 11 se ven los diferentes elementos de una estación de potencia (Panel auxiliar, Batería, Transformador, Inversor)

Figura 11: Estación de potencia (https://www.power-electronics.co.nz)

En la siguiente tabla se ven las características del controlador de la estación de potencia, cabe destacar la capacidad de comunicaciones mediante una conexión Ethernet con conectividad Modbus TCP/IP

MODO DE INSTALACIÓN	OUTDOOR
FUNCIONALIDADES	CONTROL DE VOLTAJE POI
	CONTROL Y LIMITACIÓN DE POTENCIA ACTIVA Y REACTIVA
	RAMPA
ADICIONALES	CONTROLADOR PPC
	ANALIZADOR DE POTENCIA
	REGLETA TERMINALES INTERCONEXIÓN
INTERFACE	CONEXIÓN ETHERNET RJ45
COMUNICACIONES	MODBUS TCP/IP (ETHERNET)

Tabla 1: Características del controlador de la estación de potencia

2.1.7 SISTEMAS DE CONTROL Y MONITORIZACIÓN

Estos sistemas permiten recopilar los datos de funcionamiento de la planta solar fotovoltaica y enviar las órdenes necesarias para asegurar su correcto funcionamiento, consiguiendo aumentar su rendimiento, reducir los costes de mantenimiento y prolongar su vida útil.

Para ello, cada planta solar fotovoltaica cuenta con un sistema local de control SCADA (Supervisory Control And Data Acquisition), el cual se describirá en el siguiente capítulo con más detalle. Este sistema informático recibe información del estado de toda la planta de forma continuada, se obtienen datos de: inversores, estaciones meteorológicas, sensores de radiación, seguidores solares y equipos auxiliares inteligentes.

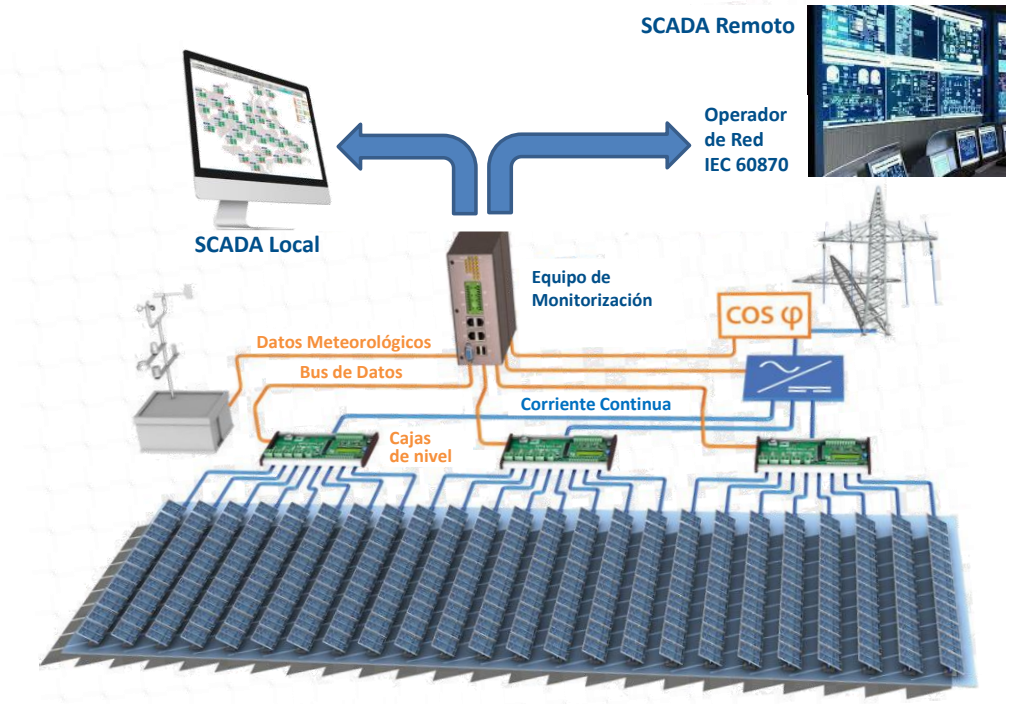


Figura 12: Sistemas de monitorización y SCADA local y remoto

Estos datos se envían a través de diferentes medios y redes de comunicaciones locales.

Además, se pueden utilizar redes inalámbricas Wi-Fi, redes locales Ethernet junto con otros protocolos de control, que describiremos más adelante, para que el sistema SCADA en planta pueda realizar las siguientes funciones básicas:

- ✓ Control automático de los elementos del sistema, siguiendo un procedimiento determinado.
- ✓ Detección de anomalías de los parámetros preestablecidos para un funcionamiento normal del sistema.
- ✓ Actuar sobre el sistema para llevarlo a sus condiciones normales de funcionamiento, en caso de detectar desviaciones. Esto permite minimizar pérdidas de producción, al detectar rápidamente el posible problema que pueda existir en un elemento de la planta.
- ✓ Presentar los datos de funcionamiento del sistema al usuario u operario de mantenimiento. Esto proporciona la información más importante de todos los parámetros de la planta, con lecturas detalladas que se muestran en tiempo real.
- ✓ Almacenado de estadísticas y de datos históricos de funcionamiento de la planta.

2.2 SCADA

Las siglas SCADA significan Control de Supervisión y Adquisición de Datos. El sistema SCADA es un tipo de Sistema de Control Industrial (ICS), es decir, un sistema controlado por un ordenador que se encarga de gestionar y supervisar los procesos industriales que existen en el mundo físico. Mientras que los ICS suelen estar limitados a distancias cortas y a lugares concretos, SCADA puede llevar procesos a gran escala que implican múltiples localizaciones y largas distancias.

Los sistemas SCADA evolucionaron desde la industria (fabricación, refinado, etc.…) a otras instalaciones, como infraestructuras de energía (parques eólicos, oleoductos, gasoductos, transmisión de energía eléctrica) e incluso a edificios, aeropuertos y barcos, controlando los sistemas de calefacción, ventilación, aire acondicionado, consumos energéticos, etc.

En un proceso industrial distribuido geográficamente, como es la generación de energía fotovoltaica, un sistema centralizado de control remoto y gestión del rendimiento en tiempo real es fundamental para mejorar la rentabilidad de los activos y la calidad de las operaciones. Los sistemas SCADA son cada vez más importantes en el sector fotovoltaico, ya que permiten a las empresas ahorrar costes de personal y de explotación

Existen varios tipos de sistemas SCADA, dependiendo del tipo de fabricante y la finalidad con la que se va a hacer uso del sistema. La selección correcta del software SCADA es de suma importancia tanto para el adecuado manejo de los flujos de datos entrantes como para el posterior análisis de estos. La representación gráfica e intuitiva en forma de gráficos, tablas y diagramas de todos esos flujos de datos (primarios y derivados) permite una fácil observación y control del sistema.

Los sistemas SCADA están formados por los siguientes componentes:

1. **Hardware de las estaciones externas:** son los componentes cómo transformadores de corriente, transformadores de tensión, válvulas de combustible, el estado de carga

(SOC), transportadores y disyuntores que pueden ser controlados localmente o de forma remota.

2. **Procesadores de las subestaciones locales:** recogen los datos de los instrumentos y equipos de hardware. Esto incluye la unidad terminal remota (RTU), el controlador lógico programable (PLC) y los dispositivos electrónicos inteligentes (IED), como relés y contadores digitales. El procesador local será responsable de docenas de entradas y salidas tanto analógicas como digitales de los IED y de los equipos de conmutación.
3. **Instrumentos digitales:** suelen instalarse en el campo o en una instalación que detecta condiciones como la corriente, el voltaje, la irradiación, la temperatura, la presión o la velocidad del viento.
4. **Dispositivos de comunicación:** pueden ser comunicaciones de corto alcance o de largo alcance. Las comunicaciones de corto alcance se instalan entre las RTUs, instrumentos y equipos de operación. Se trata de una distancia relativamente corta o conexiones inalámbricas que transportan señales digitales y analógicas utilizando señales eléctricas, como la tensión y la corriente, o utilizando otros protocolos de comunicaciones industriales. Las comunicaciones de largo alcance se instalan entre los procesadores locales RTU/PLC. Esta comunicación suele utilizar métodos como líneas telefónicas alquiladas, microondas, satélite, redes de datos celulares.
5. **Ordenadores/servidores:** serían tanto los ordenadores centrales, como el servidor de adquisición de datos DAC que actúa como punto central de supervisión y control. Estarán en la sala de control o estación maestra. La estación de trabajo de operación es donde un ingeniero u operador puede supervisar el proceso, así como recibir alarmas del sistema, revisar los datos y ejercer el control remoto.

2.3 INFRAESTRUCTURA DE COMUNICACIONES

En una planta fotovoltaica, la infraestructura de la red de comunicaciones se implementa con diferentes tecnologías muy diferentes entre sí. Por un lado, a nivel físico (cables de pares, fibras ópticas, WiFi, GPRS/3G/4G), pero también a nivel de los protocolos de

comunicaciones que se utilizan para llevar y recibir la información de control desde los diferentes dispositivos inteligentes hacia los SCADAs locales y remotos (Modbus, Modbus/TCP, IEC61850, IEC60870-104).

Para el troncal de comunicaciones se utilizan fibras ópticas, que permite alcanzar mayores distancias que el resto de las soluciones basadas en pares de cobre o la propia WiFi. La topología física utilizada es de anillo, ya que ofrece alta disponibilidad y fiabilidad, sobre todo cuando se utiliza una estructura de doble anillo aumentando la resiliencia de la red.

El acceso remoto se realiza mediante una VPN (Virtual Private Network) y otros elementos de seguridad como firewalls, sistemas de detección de intrusos, diodos de datos, así como equipos especializados que ofrecen mejoras en la ciberseguridad de la instalación.

En la siguiente figura puede verse un esquema parcial y simplificado de la red de comunicaciones que se suele utilizar. En ella se diferencian claramente los sistemas de generación de energía de los sistemas de control y gestión que utiliza la red de comunicaciones para el envío de mensajes de información, control, alarmas, fallos, recuperación, etc.

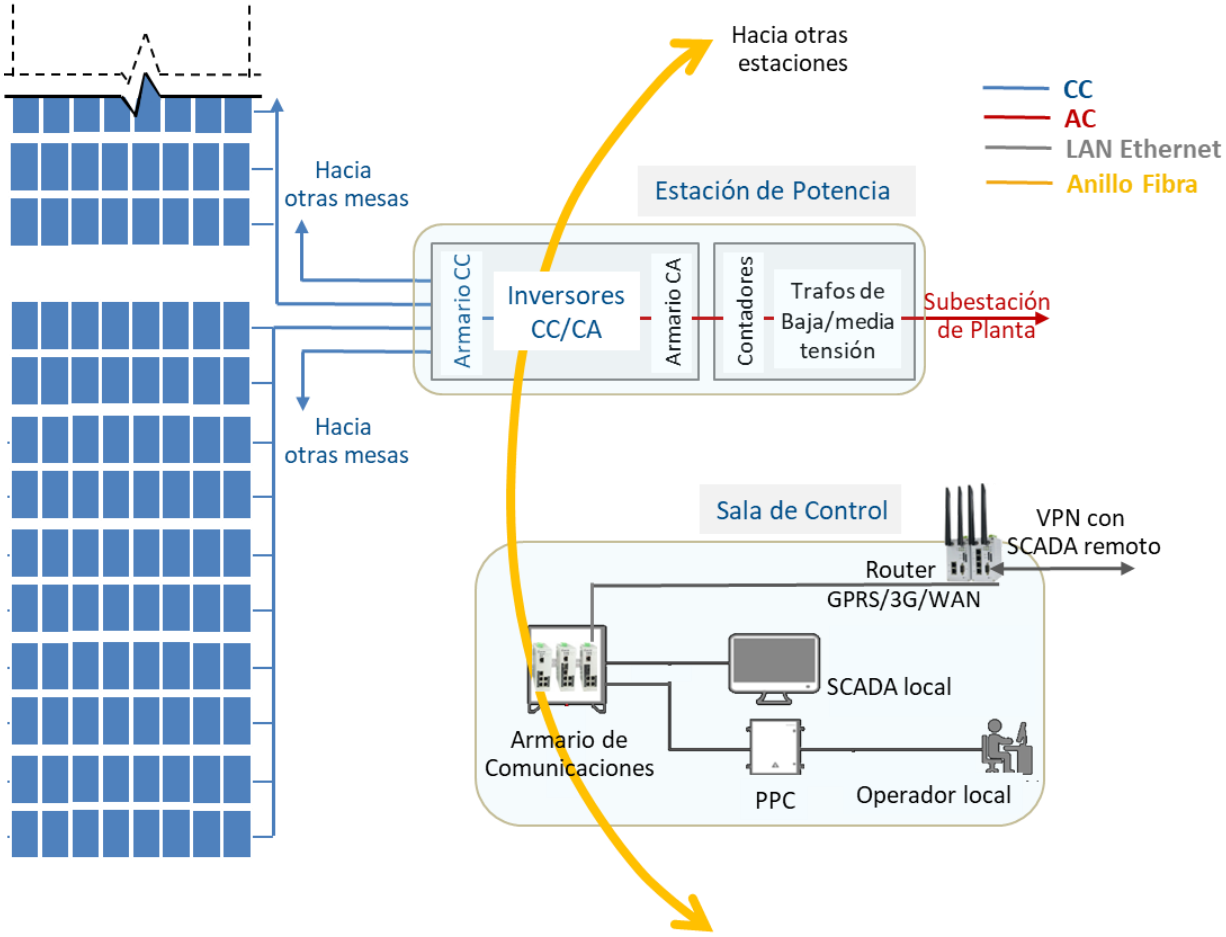


Figura 13: Esquema de la red de comunicaciones

La electrónica de la red de comunicaciones está basada en conmutadores LAN, con soporte para conexiones de enlaces de fibra y de conexiones Ethernet, que son los enlaces que se utilizan en las redes ofimáticas de las empresas y en nuestra propia casa. Estos equipos son gestionables, es decir tienen capacidades de control remoto para su configuración, operación y mantenimiento. Además, esto permite la obtención de información del tráfico que circula por la red, control de errores y recuperación de fallos, y el uso de herramientas ampliamente utilizadas para la gestión de redes de comunicaciones, etc.

El equipamiento utilizado es de tipo industrial, con equipos más robustos y especificaciones más exigentes en cuanto a su temperatura de funcionamiento, aislamiento eléctrico y medioambiental, etc. Pero desde el punto de vista de su operativa, son análogos a los que se

utilizan en las instalaciones clásicas de edificios de oficinas, campus, etc. Debido a la diversidad y elevado número de dispositivos que precisa una planta solar fotovoltaica, nos encontraremos con elementos inteligentes que tienen muy baja capacidad de proceso y necesiten enviar un bajo tráfico de datos, como por ejemplo los captadores solares, sensores de temperatura, estaciones meteorológicas, etc. En el caso de las estaciones de potencia, formadas por uno o varios inversores y un transformador de baja/media tensión, tendremos mayor necesidad de proceso informático y de envío/recepción de información y control. La razón de esto es muy simple, su monitorización detallada permite identificar y actuar de forma rápida sobre las incidencias que puedan surgir en los equipos de potencia, permitiendo mejorar el rendimiento y alargar la vida útil de la planta fotovoltaica.

Cada planta solar es distinta, pero a efectos prácticos de monitorización y control se pueden cuantificar tres zonas distintas en la arquitectura de la red de comunicaciones, con distintas necesidades y por lo tanto precisan diferentes soluciones. Estás zonas son: la zona de generación fotovoltaica, zona de estaciones de potencia y zona de control y subestación de planta.

En la figura 14 se ven claramente estas tres zonas de la red en una planta solar fotovoltaica y los medios de acceso a la red de comunicaciones que normalmente se suelen utilizar (RS-485, WiFi, Ethernet y fibra óptica).

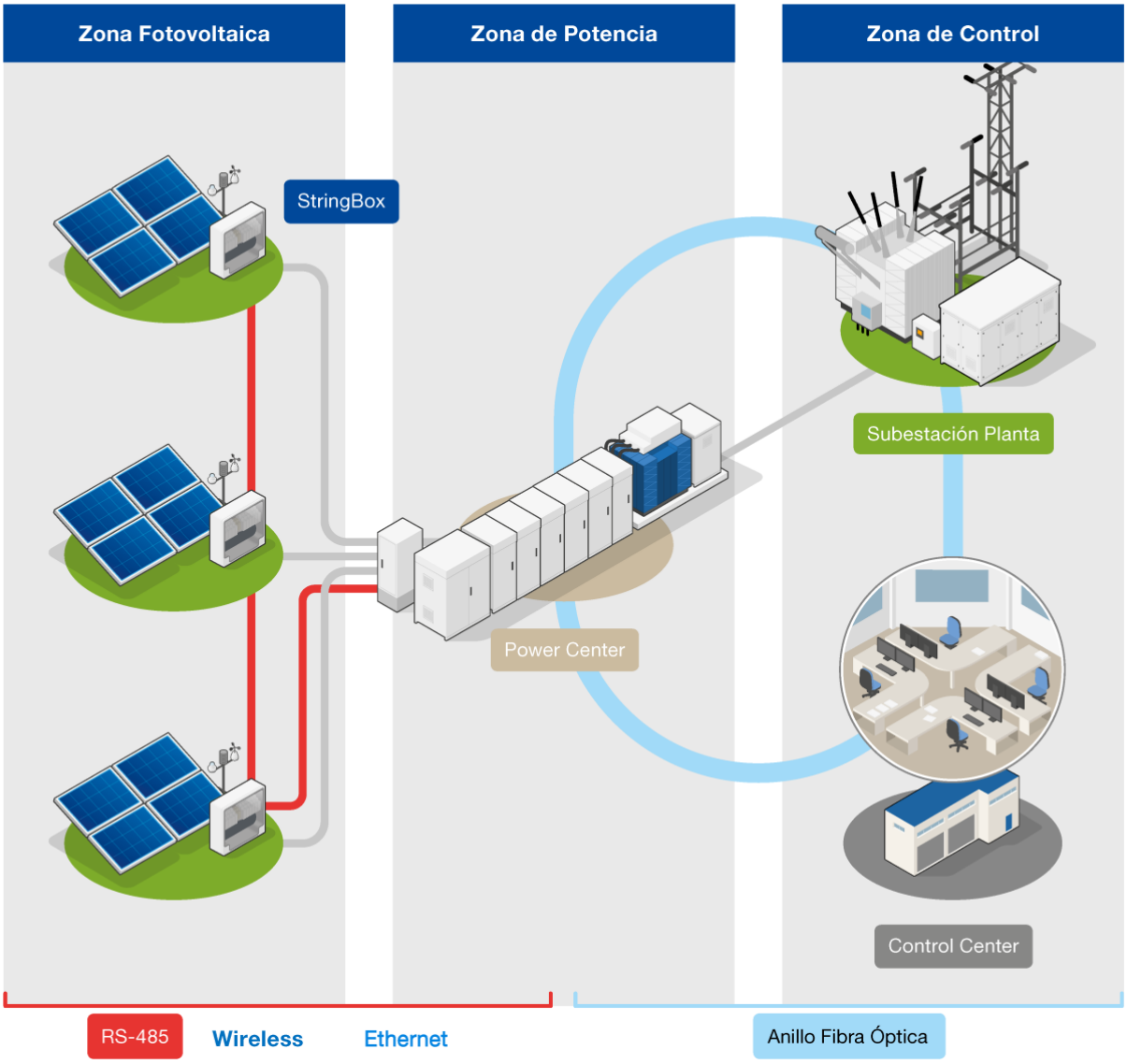


Figura 14: Zonas de monitorización (www.circutor.com)

2.3.1 COMUNICACIONES EN LA ZONA DE GENERACIÓN FOTOVOLTAICA

En esta zona se encuentran múltiples equipos de control que envían información relevante de la instalación fotovoltaica. Estos dispositivos se interconectan mediante enlaces serie tipo RS-485 de corto alcance y baja velocidad. Estos enlaces se concentrarán en hubs y se canalizan hacia el armario de comunicaciones situado en la estación de potencia, donde se adaptarán a conexiones del tipo Ethernet mediante dispositivos como Gateway o adaptadores

específicos. Existen diferentes alternativas, en función del producto y fabricante que estemos utilizando. El protocolo de comunicaciones utilizado y que describiremos más adelante es el Modbus o el Modbus/TCP.

En la figura siguiente se ven las comunicaciones serie tipo RS-485, y además, en este caso el fabricante también ofrece la posibilidad de utilizar conexiones inalámbricas WiFi entre las cajas de nivel (string box) y la estación de potencia.

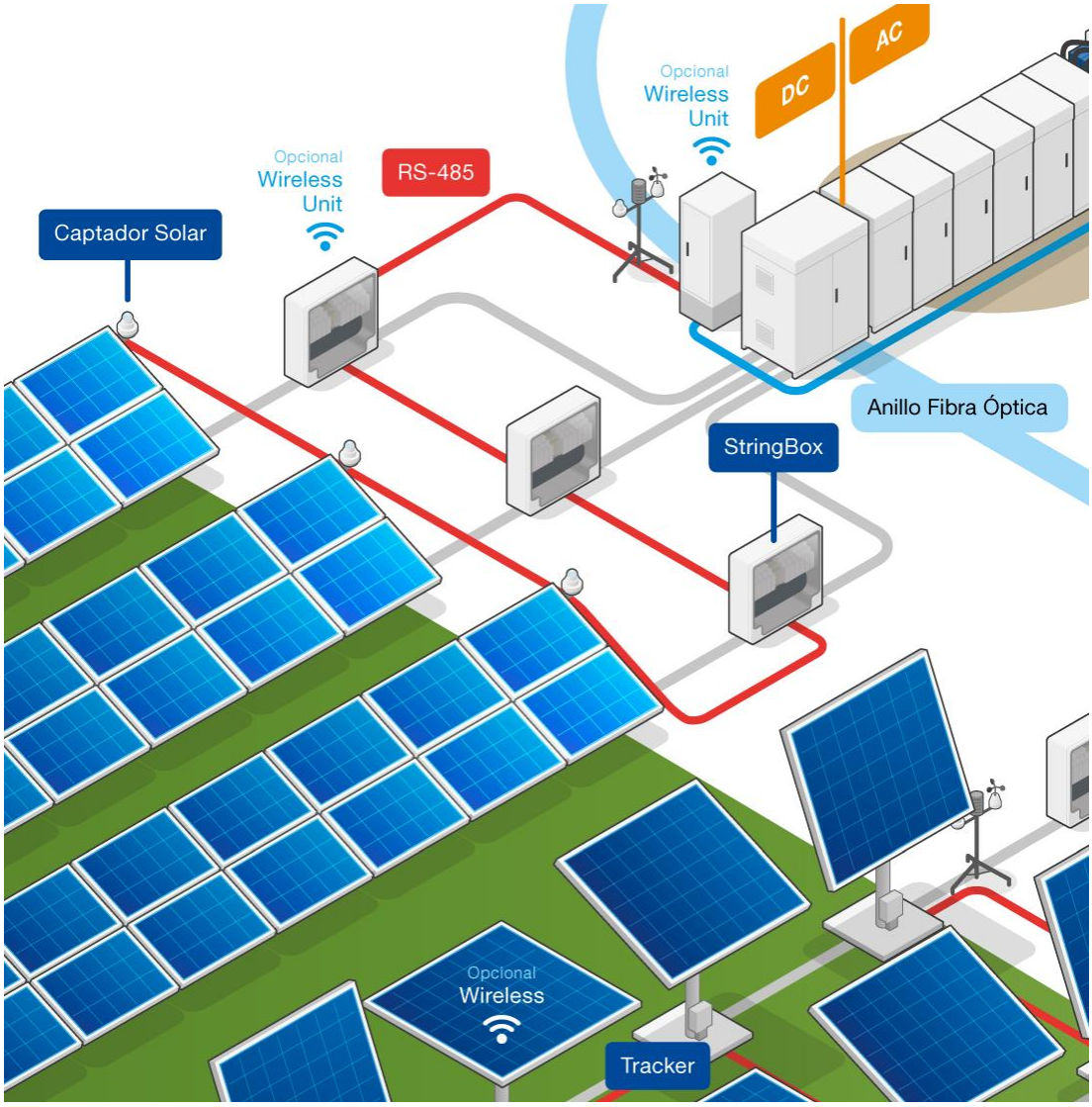


Figura 15: Esquema de la zona de generación fotovoltaica (www.circutor.com)

2.3.2 COMUNICACIONES EN LA ZONA DE LAS ESTACIONES DE POTENCIA

Esta zona en un área crítica a nivel comunicaciones, ya que además de concentrarse aquí todos los datos que provienen de los elementos de control de la zona fotovoltaica, se añaden los datos de monitorización y gestión de los inversores que son críticos en la generación de energía. También es necesario medir, monitorizar y controlar los elementos de protección del transformador, las protecciones de la red de media tensión y las entradas de CC de los "strings" agregados por las diferentes cajas de nivel de CC.

Toda esta información se transmite a través de la red de fibra óptica al centro de control, donde están instalados los diferentes servidores SCADA y los terminales de control de los operadores de estos sistemas.

El anillo de fibra troncal puede estar formado por varios anillos físicos, con objeto de llevar separados por cada anillo los distintos tráficos de información y control. También puede ser un único anillo físico de fibra, en este caso la separación de tráficos se realiza mediante técnicas de VLANs (Virtual LANs). Para ello es necesario definir las diferentes VLANs en los conmutadores LAN. Existen diferentes alternativas para implementar las VLANs, la más sencilla consiste en definir, en cada puerto físico del conmutador, la VLAN a la que va a pertenecer dicho puerto. Cabe indicar, que desde el punto de vista de la ciberseguridad se considera más seguro una separación física de las redes, es decir varios anillos, que la separación lógica por VLANs, ya que en este último caso todo el tráfico de datos va por la misma fibra.

La Figura 16 ilustra los elementos y necesidades de medidas y monitorización en esta zona. Generalmente el acceso de todos los equipos se realiza mediante conexiones Ethernet, que a su vez se canalizan a los conmutadores ópticos que se encuentran en el armario de comunicaciones, donde se realiza la interconexión al anillo o anillos de fibra troncal.

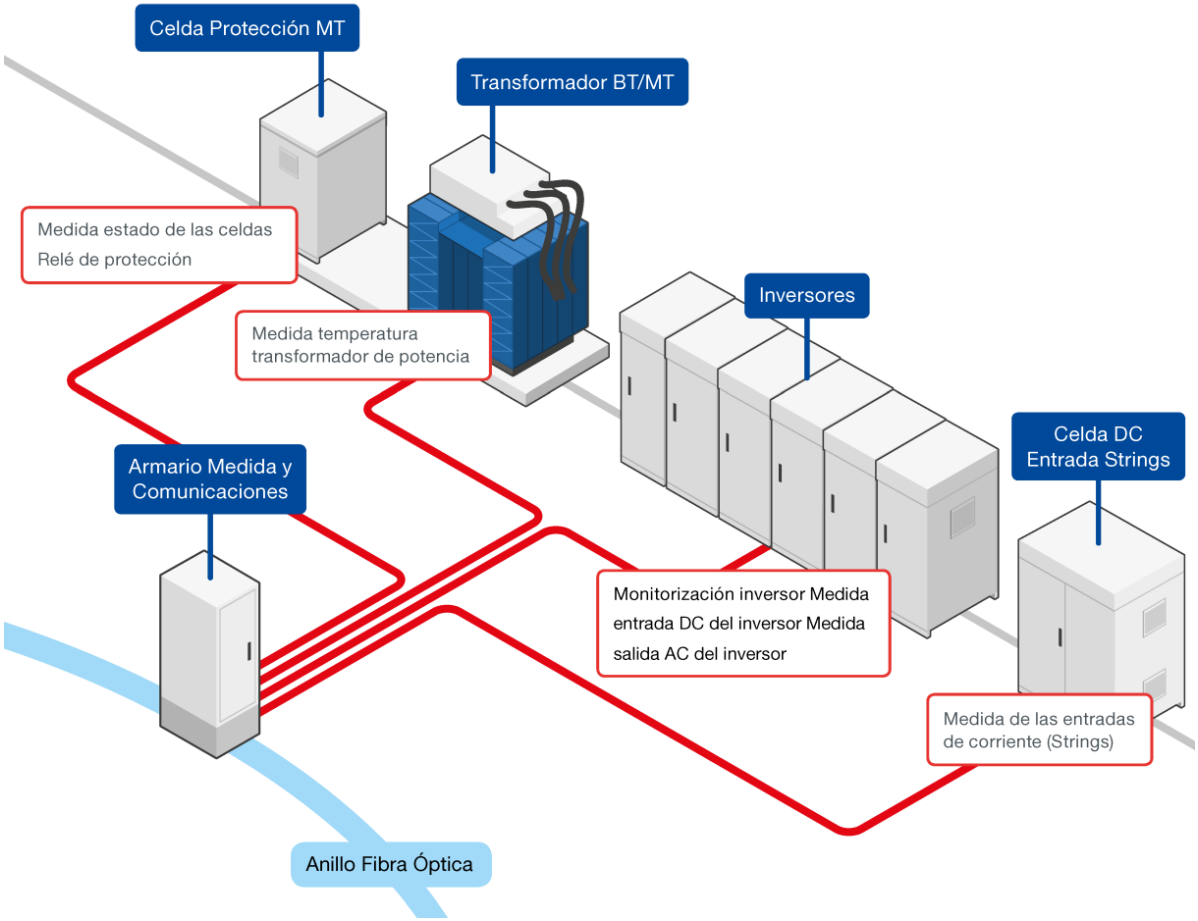


Figura 16: Esquema de la zona de potencia (www.circutor.com)

2.3.3 COMUNICACIONES EN LA ZONA DE CONTROL Y SUBESTACIÓN DE PLANTA

En esta última zona, todo el tráfico de datos del resto de zonas se recibe en el centro de control, para ser analizado y en su caso almacenado en los servidores SCADA locales. El operador de cada SCADA podrá enviar órdenes y comandos de actuación a los dispositivos que sea necesario. Además, en el centro de control se encuentra el router con la VPN de salida hacia un sistema de supervisión superior ubicado fuera de la planta, para la supervisión externa del sistema.

Desde el punto de vista de la ciberseguridad, este centro es el más importante a proteger y detectar posibles ataques, sobre todo a los terminales de los operadores, ya que, si un hacker tomase el control de este, estaría en una posición de producir graves daños a la instalación.

Por ello, los dispositivos de ciberseguridad, tales como firewalls o sistemas de detección de intrusos deben implementarse en esta zona y sobre todo tiene que existir una metodología adecuada que permita identificar y corregir los posibles fallos de ciberseguridad. Todos estos aspectos se desarrollan más adelante en el capítulo de ciberseguridad.

La subestación de planta es el punto de interconexión con la compañía eléctrica para la distribución de la energía generada. En este punto se suele instalar el Power Plant Controller (PPC), que es la herramienta de control para la regulación de la potencia de la planta. El PPC recibe los parámetros desde el SCADA local e interactúa con los inversores instalados en planta para cumplir con las exigencias de la compañía eléctrica, modulando la inyección de energía a la red. El PPC tiene como objetivo asegurar el buen funcionamiento de la instalación de generación de energía eléctrica regulando parámetros como tensión, control de frecuencia, limitación de producción, limitación de potencia o regulación de potencia reactiva.

En la figura 17 se ve el centro de control con los puestos de operación de los SCADAs y la subestación de elevación de media/alta tensión con el PPC, todos ellos interconectados al troncal de fibra.

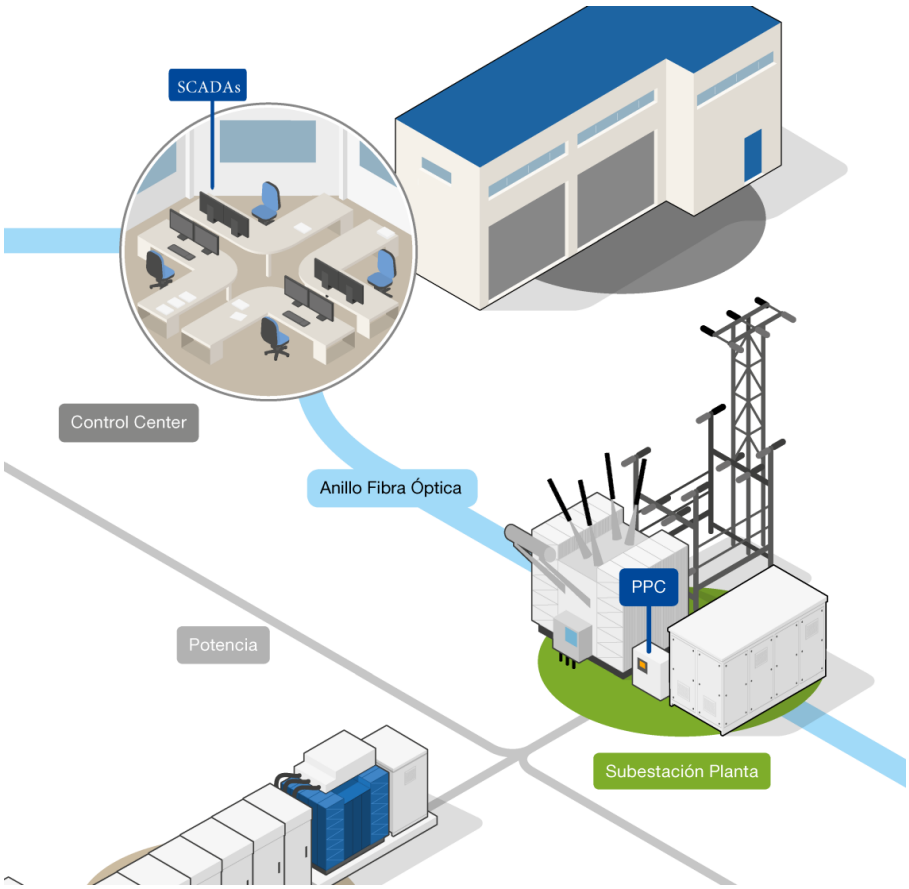


Figura 17: Esquema de la zona de control y subestación de planta (www.circuitor.com)

2.4 PROTOCOLOS DE COMUNICACIÓN

2.4.1 INTRODUCCIÓN A LA ARQUITECTURA DE COMUNICACIONES ESTRATIFICADA EN NIVELES

Actualmente las comunicaciones de datos utilizan como modelo de referencia la arquitectura que se definió para Internet, prácticamente el 100% de los equipos informáticos vienen preparados para poder conectarse a redes IP. Esta arquitectura tiene cuatro niveles, que se describirán más adelante.

La utilización de un modelo de arquitectura en niveles jerárquicos permite agrupar funciones relacionadas e implementar el hardware y software modularmente, lo que presenta grandes

ventajas en el desarrollo y evolución de estas tecnologías de comunicaciones, a parte de su mejor comprensión por parte de todas las personas que trabajan en este campo.

En la siguiente figura se aprecian los distintos niveles y como se implementan, ya sea mediante un programa software o un determinado hardware.

- ✓ Nivel de **Aplicación**: Son los procesos de usuario final, sirve como soporte, a nivel de comunicaciones, de las aplicaciones diseñadas para Internet
- ✓ **Nivel TCP** (Transmission Control Protocol): Ofrece la conectividad extremo a extremo a través de la red TCP/IP
- ✓ **Nivel IP** (Internet Protocol): Comunica los ordenadores a través de las diferentes redes, interconectadas mediante routers IP, que forman la Internet
- ✓ Interface de **Red:** Corresponde al servicio de acceso a la red (local LAN o remota WAN)

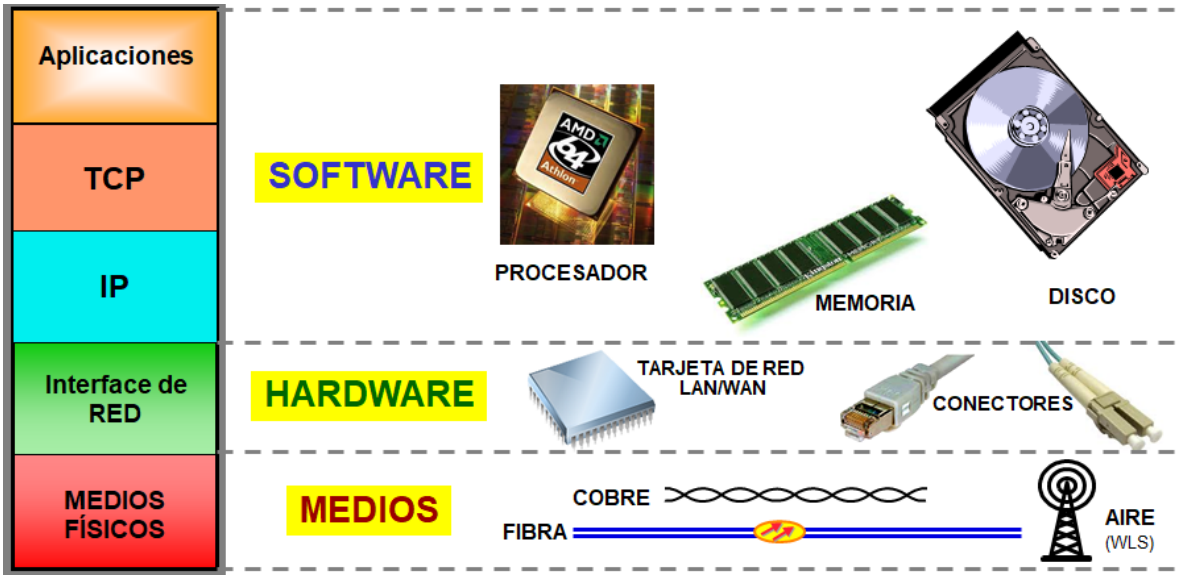


Figura 18: Arquitectura de comunicaciones (www.lmdata.es)

Por último, están los diferentes medios físicos que podemos utilizar para transmitir los bits o fotones de información (pares de cobre, fibra óptica, medios inalámbricos como Wifi, LTE, etc.), y que no forma parte de la arquitectura.

Los protocolos de comunicaciones son los intercambios entre niveles iguales de distintos sistemas interconectados mediante el TCP/IP. Por ejemplo, un protocolo a nivel de aplicación permite que un ordenador local intercambie datos de forma fiable con otro equipo situado en cualquier parte de una red TCP/IP. Para conseguir esto, la aplicación construye un mensaje de información, con una determinada estructura de datos que entenderá el equipo remoto, y lo pasa al nivel inferior (TCP) a través de un punto de intercambio. Estos puntos de intercambio corresponden a lo que en programación se denominan sockets.

Cabe destacar que es muy importante, en el ámbito de la ciberseguridad, conocer cómo opera la arquitectura de comunicaciones TCP/IP, ya que todos los ataques (robos de información, virus, troyanos, denegaciones de servicio, etc.) utilizan estos protocolos para propagarse, infectarse y comunicarse con el hacker, incluso aunque el atacante este físicamente en la misma instalación o cuando un troyano se halla instalado vía memoria USB. Las comunicaciones son imprescindibles para que el ataque se produzca y por lo tanto es vital tener en cuenta este tema.

2.4.2 PROTOCOLOS DE COMUNICACIONES UTILIZADOS EN UNA PLANTA SOLAR FOTOVOLTAICA

Según se vio en anteriormente en el apartado “Infraestructura de Comunicaciones”, los protocolos de comunicación usados en este tipo de instalaciones se basan en estándares internacionales definidos por el IEC (International Electrotechnical Commission) y el protocolo Modbus y su adaptación a redes TCP/IP denominado Modbus/TCP.

2.4.2.1 ModBus y ModBus/TCP:

Modbus es un protocolo industrial abierto utilizado para transmitir información entre dispositivos electrónicos conectados a un mismo bus. Es decir, Modbus es un protocolo ampliamente aceptado, de dominio público, que requiere una licencia, pero es gratis. Así

pues, es un sistema de comunicación muy popular en entornos industriales y se usa generalmente para transmitir señales de los dispositivos de instrumentación y control a un controlador principal o a un sistema de recolección de datos, es decir al PLC. Este protocolo es esencial para la comunicación con los inversores y los seguidores solares.

Hay distintos tipos de protocolos Modbus, pero los más interesantes en las comunicaciones de una planta fotovoltaica son el Modbus RTU y el Modbus TCP/IP

En el Modbus RTU se produce la comunicación entre dos dispositivos. El dispositivo que solicita la información sería el maestro y el que la envía el esclavo. Cada dispositivo tiene un ID para poder referirse a él. El maestro puede hacer frente a esclavos individuales, o puede iniciar un mensaje a todos los esclavos. Los esclavos devuelven una respuesta a todas las consultas dirigidas a ellos de forma individual, estos no pueden iniciar los mensajes por su cuenta, solo responden a las preguntas del maestro. En nuestro caso el PLC podría ser el maestro y los inversores conectados a él los esclavos.

Este protocolo necesita conexiones físicas directas, clásicamente 3 opciones distintas. RS232, permite la comunicación punto a punto entre el maestro y el esclavo a una distancia de unos 15 metros. Por otro lado, el RS485 o el RS422 permiten la conexión entre un maestro y varios esclavos que se conectan en serie entre sí hasta un máximo de 247 esclavos cada uno con distinta ID.

El Modbus TCP/IP es simplemente el protocolo Modbus RTU con una interfaz TCP que se ejecuta en Ethernet. Es decir, las bases sobre las que se da la interpretación de los datos son las mismas. En este protocolo se pierde la arquitectura maestro/esclavo que sería sustituida por la comunicación cliente/servidor del protocolo TCP/IP. Cada dispositivo de la red tiene una dirección IP que sirve para su identificación. El cliente está conectado a un switch al que a su vez se conectan uno o varios servidores. La función principal de TCP es asegurar que todos los paquetes de datos se reciben correctamente, sin errores, mientras que el IP permite de que los mensajes llegan a su destino.

Cabe destacar que el Modbus TCP/IP utiliza la puerta 502, es importante saber que esta puerta no puede estar cerrada por un firewall para que la comunicación funcione.

2.4.2.2 Estándares IEC

Los protocolos IEC que nos podemos encontrar en una planta de generación de energía solar fotovoltaica son los siguientes:

Estándares del IEC (Comisión Internacional de Electrónica)

- ✓ Normativa IEC 60870-5-101
- ✓ Normativa IEC 60870-5-104
- ✓ Normativa IEC 61850

Normativa IEC 60870-5-101: Es la más antigua, se utiliza para las operaciones básicas de telecontrol. Su arquitectura de comunicaciones tiene tres niveles y permite las comunicaciones locales con las RTUs. Este protocolo precisa de una Red determinista, es decir, conexiones físicas directas (RS232, 485, Fibra).

Normativa IEC 60870-5-104:

Con el uso masivo de las comunicaciones basadas en el TCP/IP y para permitir el acceso a través de redes TCP/IP para el protocolo IEC 60870-5-101, el IEC desarrollo el estándar 60870-5-104. Es decir, el nivel físico del 60870-5-101 se elimina y se pasa totalmente el TCP/IP.

Normativa IEC 61850

Este protocolo se utiliza para la automatización de subestaciones, permitiendo monitorizar y controlar los distintos sistemas de protección, medida y control. Desarrollado para sistemas de potencia eléctrica, permite extender los nuevos modelos de información a otros entornos (gas, agua). Proporciona un lenguaje de descripción de configuración (SCL) Utiliza Ethernet y TCP/IP.

En resumen, los protocolos IEC60870-101 se utilizan para comunicaciones locales con medios físicos serie tipo RS-485 y el IEC60870-104 para las remotas desde el SCADA del operador eléctrico sobre comunicaciones TCP/IP. El estándar IEC61850, más moderno, define los protocolos de comunicación para dispositivos electrónicos inteligentes en

subestaciones eléctricas, que permite la interoperabilidad de equipos de múltiples proveedores.

Capítulo 3. CRITERIOS DE CIBERSEGURIDAD

3.1 INTRODUCCIÓN

Existen muchas definiciones de lo que significa y representa la palabra ciberseguridad. Por ejemplo, ISACA (Information Systems Audit and Control Association) define Ciberseguridad como la "Protección de todos los activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados".

Si consultamos en la RAE (Real Academia Española), vemos que ciberseguridad no aparece como palabra, pero si el prefijo ciber y la palabra seguridad. Ciber "indica relación con redes informáticas" y seguridad se define como "cualidad de seguro", es decir hacer seguro todo lo que tenga relación con las redes informáticas.

Las empresas del sector eléctrico se enfrentan a un riesgo creciente de ver interrumpidos sus servicios o de perder datos a causa de ciberataques. La amenaza para las empresas energéticas en los próximos años está aumentando a medida que los nuevos desarrollos en las extensiones de las redes y la medición inteligente exponen más infraestructuras a Internet. De cualquier manera, hay que tener en cuenta que los equipos que no está conectados a Internet tampoco son inmunes a las amenazas. De hecho, ya se han producido varios ataques con éxito contra sistemas aislados. Los operadores de infraestructuras críticas, así como las empresas de servicios energéticos, deben ser conscientes de estas amenazas y prepararse en consecuencia.

Las amenazas para las empresas energéticas pueden proceder de varios frentes. En algunos casos, el espionaje de los competidores es el motivo principal, se buscan datos sobre nuevos proyectos, exploración y finanzas. Otros ataques tienen como objetivo la interrupción y la destrucción. Algunos casos parecen estar patrocinados por el Estado, como la interrupción del programa nuclear iraní por el virus Stuxnet en 2010 supuestamente creado por los

servicios de inteligencia de Estados Unidos e Israel. Otros ataques parecen ser obra de hacktivistas con agendas políticas o medioambientales. Por último, existen también los atacantes internos, como los empleados descontentos, una fuente importante de ataques que a menudo conducen a la interrupción del servicio.

3.2 OT (OPERATIONAL TECHNOLOGY) VS IT (INFORMATION TECHNOLOGY)

En el entorno de la ciberseguridad de una planta solar es muy importante comprender las diferencias que existen entre los Sistemas de Control Industrial (OT) y las Tecnologías de Información (IT).

Como se ha comentado previamente, muchas de las tecnologías de Información y de Comunicaciones (TICs) que se han desarrollado en las últimas décadas para IT, se están aplicando en entornos de control industrial.

El termino IT se refiere a la tecnología que se centra en el procesamiento de datos e información. Las Tecnologías de Información han evolucionado a lo largo del tiempo para manipular, almacenar, comunicar y proteger los datos de diferentes formas. Con el objetivo de llevar a cabo las operaciones comerciales habituales (uso de bases de datos, aplicaciones ofimáticas, corporativas, email, servidores web, etc.). Todo ello mediante el uso de redes locales, redes TCP/IP privadas o mediante comunicaciones a través de Internet.

Sin embargo, los sistemas de control industrial (ICS) incluyen, además de ordenadores y aplicaciones de control y gestión muy específicas, PLCs, sondas, controladores, robots, DPC (Discrete Process Control Systems), etc. En todos estos entornos industriales se tienen unos requerimientos y necesidades muy diferentes a los de los equipos informáticos, aplicaciones y de comunicaciones IT. Por ello, en los sistemas de control industrial, nos referimos a la tecnología de las operaciones OT (Operational Technology).

La OT podemos definirla como el conjunto de hardware y software que detecta o provoca un cambio en procesos y sistemas industriales. Estos cambios se producen gracias a la supervisión local o remota de los equipos industriales.

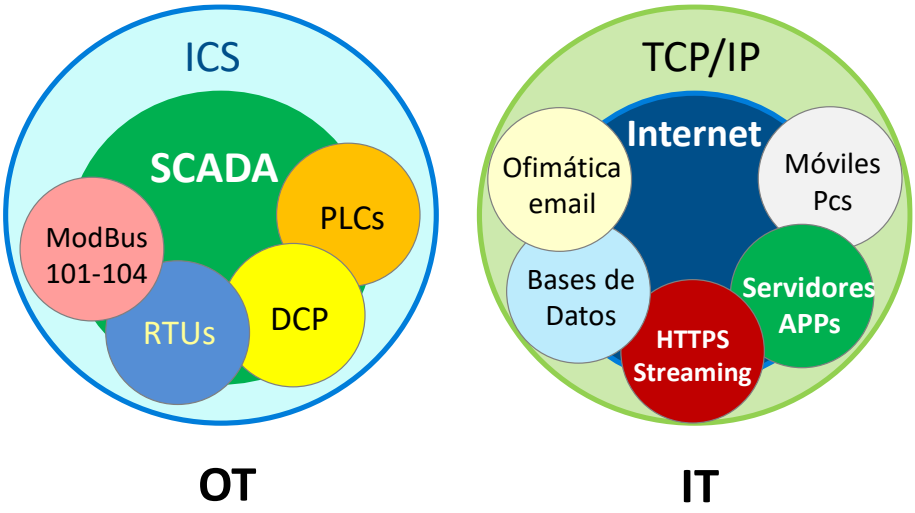


Figura 19: Comparativa entre OT e IT

En esta figura 19 se observa una comparativa entre elementos que forman parte del mundo OT y del mundo IT.

Por otra parte, en la tabla siguiente se resumen los requerimientos en ambientes OT e IT en cuanto a disponibilidad, necesidad de tráfico en tiempo real, vida media de los equipos, etc.

Requerimientos	OT	IT
Disponibilidad	Muy alta	Alta
Vida media equipos	>20 años	5 años
Tráfico en Tiempo real	Muy alto	Retardos tolerables
Auditorias de ciberseguridad	Infrecuentes	Programadas
Parcheo de vulnerabilidades	Infrecuentes	Muy Frecuentes

Tabla 2: Requerimientos OT vs IT

En el pasado, los sistemas OT han estado aislados en su gran mayoría, ya que dependían fundamentalmente de protocolos propietarios cerrados y de software, operado manualmente, para llevar a cabo sus funciones esenciales. Este aislamiento y su falta de interconexión con sistemas y comunicaciones IT los han protegido, evitando y disminuyendo la probabilidad de sufrir ciberataques. Sin embargo, a medida que la OT está adoptando cada vez más soluciones del mundo IT, ya que esto supone ventajas tanto técnicas y económicas, se expone a nuevas y peligrosas amenazas similares a las que se afrontan en entornos IT.

La aplicación de herramientas y soluciones de seguridad orientadas a IT en las redes OT no protege necesariamente de ataques específicos a estos sistemas. Utilizar herramientas de seguridad IT en OT podría ser incluso tan peligroso como no tener seguridad, ya que pueden proporcionan una falsa sensación de seguridad.

Las redes, los equipos y los protocolos utilizados en OT son diferentes a sus homólogos en IT, por lo que requieren de una mentalidad distinta. Por ejemplo, un firewall en IT normalmente inspecciona tráficos muy intensos (streams de vídeos, descargas de ficheros, etc.) donde los retardos o las variaciones de retardos no son críticos. En OT el tráfico es muy ligero, pero un retardo en un comando de control crítico puede hacer que una planta de energía se desconecte de la red. Por eso se necesitan redes OT que soporten tráfico en tiempo real, o lo que es lo mismo, retardos y variaciones del retardo muy bajas (del orden de milisegundos).

Los hechos nos dicen que a partir de la guerra en Ucrania han aumentado de manera muy significativa, tanto en número como en diversidad, los ciberataques a infraestructuras críticas y organismos gubernamentales. En un informe publicado por Microsoft el 27 de abril de 2022 se resume muy bien este crecimiento de amenazas, vulnerabilidades y ciberataques [1].

3.3 SOLUCIONES APLICADAS EN EL ENTORNO IT

Si resumimos, muy esquemáticamente, las soluciones aplicadas comúnmente en ambientes IT están basadas en:

1. **Protección perimetral:** mediante sistemas de firewalls, proxies, detectores de intrusos, gestión de los logs y alarmas que producen estos equipos.
2. **Control de acceso:** redes Privadas Virtuales (VPNs), utilización de sistemas de autenticación de usuarios y equipos mediante certificados digitales, control de passwords, uso de múltiple factor de autenticación y otros sistemas criptográficos.
3. **Segmentación de redes:** evitando que el tráfico de un grupo de usuarios y equipos se mezcle con otros. En la práctica esto se utiliza de forma intensiva en las redes de área local (LANS) mediante la técnica denominada VLANs (Redes Locales Virtuales). También es muy común separar distintas redes IP mediante routers con reglas de filtrados, lo que permite diferenciar tráficos, por ejemplo, la voz sobre IP de los datos.
4. **Gestión de vulnerabilidades y parcheo de las mismas:** esta medida se utiliza en grandes organizaciones que disponen de herramientas automáticas. También es posible usar servicios en la nube de empresas que ofrecen este tipo de soluciones. En empresas más pequeñas este punto suele realizarse manualmente o en el peor de los casos no se hace.
5. **Protección de los equipos de usuario final:** los usuarios finales son el eslabón más débil de la cadena de seguridad. La posibilidad de que, por desconocimiento, falta de atención o malas práctica se produzca un error de ciberseguridad es muy alto. Un usuario que esté operando un PC interconectado a la LAN empresarial, o acceda desde su casa a través de una VPN, puede favorecer la entrada de malware en otros equipos de la red interna. Por ello, normalmente se habilitan en los equipos de los usuarios limitaciones, políticas de seguridad, antivirus, antimalware, etc. Entre estas limitaciones destaca el uso de Wifi cifrada, la imposición de utilizar VPNs desde accesos públicos, negar al usuario la posibilidad de instalar aplicaciones, deshabilitar los puertos USB para que no se puedan conectar dispositivos de memoria, etc.

Desde el punto de vista de la protección de las redes y comunicaciones en IT, existe una guía de la NSA (National Security Agency), publicada en marzo de 2022 que ofrece un montón de consejos y soluciones para mejorar la ciberseguridad en las infraestructuras IT de red. [2]

3.4 SOLUCIONES APLICADAS EN EL ENTORNO OT

Para hacer un resumen equivalente en ambientes OT, en nuestro caso una planta de generación de energía solar fotovoltaica, lo primero que tenemos que saber es qué dispositivos son los que pueden ser objetivo de un ataque de ciberseguridad y su grado de criticidad.

Para ayudarnos en toda esta labor, existe un modelo de ciberseguridad desarrollado por la universidad de Purdue, así como las posteriores modificaciones y mejoras del mismo. Este modelo se basa en la clasificación de los diferentes elementos que conforman un entorno OT, posicionándolos en diferentes niveles de ciberseguridad. También incluye su integración con IT (convergencia de OT con IT).

3.4.1 MODELO DE PURDUE: ENTERPRISE REFERENCE ARCHITECTURE (PERA)

El modelo de Purdue, denominado PERA (Purdue Enterprise Reference Architecture), es un modelo de referencia estructural para la seguridad de los sistemas de control industrial (ICS). Incluye todo lo relativo a los procesos físicos, los sensores, los controles, la supervisión, las operaciones y la logística.

Fue desarrollado a primeros de los noventa para un entorno de fabricación integrada por ordenador. Ha servido de base para el desarrollo de varios estándares posteriores de seguridad, por ejemplo, el estándar de ciberseguridad ANSI/ISA-95/99 (International Society of Automation) y la normativa IEC 62443. En la actualidad sigue utilizándose de forma extensiva para el desarrollo de metodologías y herramientas de ciberseguridad, con nuevos aportes y modificaciones como por ejemplo la inclusión de la IoT.

Este modelo definió inicialmente los diferentes niveles de infraestructura crítica utilizados en las líneas de producción. De esta manera podemos focalizar en cómo asegurar cada nivel de manera individual. En el fondo lo que el modelo define, es una segmentación de redes y sistemas, en función de los diferentes tipos de dispositivos que se emplean en ICS. Al dividir

la red en varias redes lógicas y sobre todo restringir el acceso entre ellas, limitamos la superficie de ataque a los dispositivos más críticos.

Una arquitectura en la que todos los equipos se conecten a una red "plana" sería muy difícil, por no decir imposible, de asegurar, compleja de actualizar y además causaría muchos problemas de ciberseguridad a la hora de interconectarla con equipos y redes IT. En cambio, una arquitectura estratificada en capas, con zonas de seguridad bien definidas y niveles gestionados es fundamental para construir un buena la defensa en profundidad. También es importante para que la planta se pueda actualizar o sustituir cualquiera de sus sistemas en el futuro. Y es esencial para la colaboración, sin fricciones, entre los grupos de IT y OT, definiendo muy claramente los entornos de operación de cada uno, sin solapamiento de competencias.

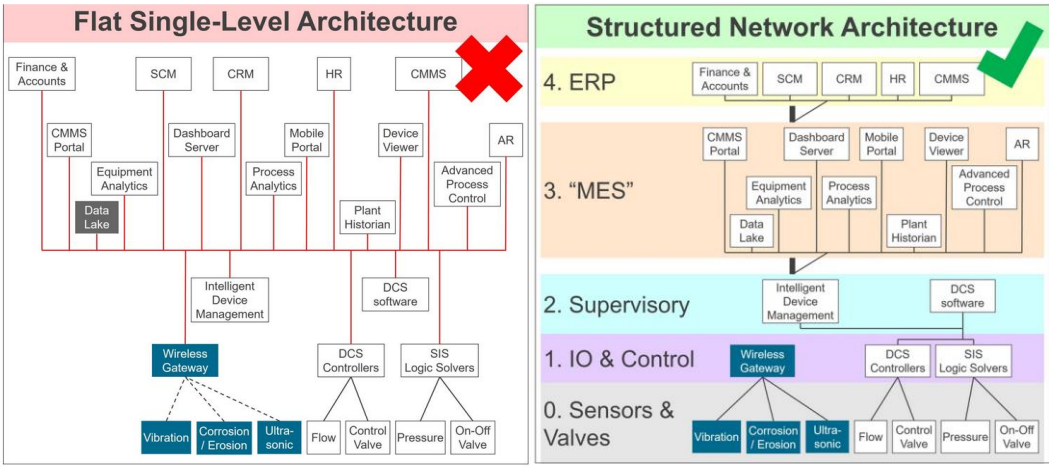


Figura 20: Arquitectura Plana vs Modelo Purdue (www.linkedin.com)

En esta figura se observan las diferencias entre una arquitectura plana y otra que sigue el modelo Purdue. La figura corresponde a una planta industrial no a una solar, pero lo importante es comprender las diferencias estructurales de forma general, para luego aplicar este modelo a cada instalación en particular.

Vamos a hacer un resumen del modelo clásico de Purdue, viendo los diferentes niveles definidos en el mismo. Para ello usaremos como referencia la figura 21, sacada de un

documento de ciberseguridad en OT del fabricante cisco, donde se observan muy claramente cada nivel y sus funciones.

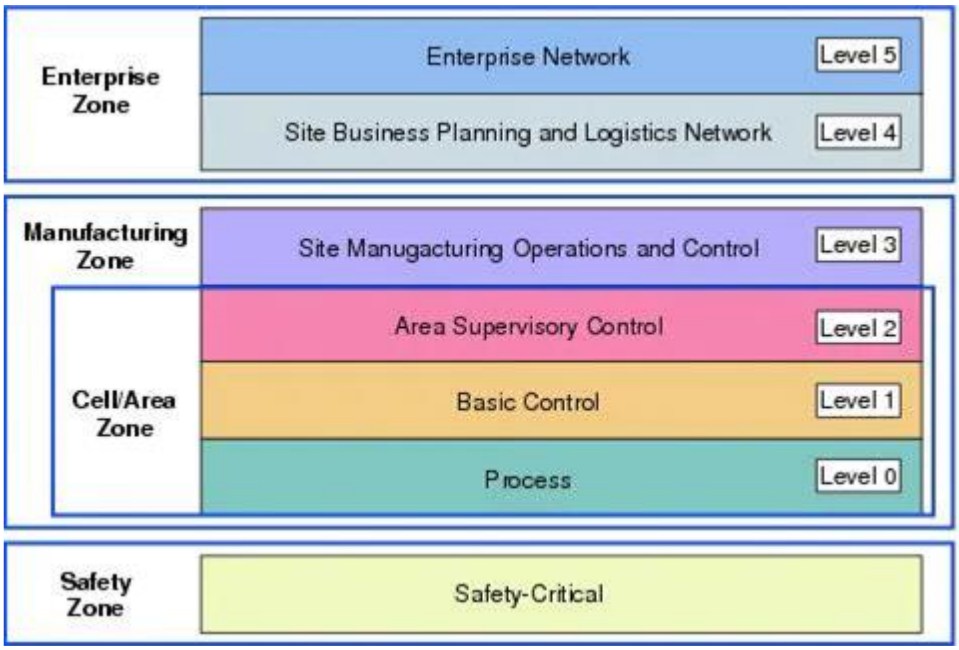


Figura 21: Arquitectura clásica del modelo de Purdue (www.cisco.com)

El modelo PERA define los siguientes niveles:

Niveles OT:

Nivel 0 - Proceso físico: Define los procesos físicos reales. Estos varían en función del tipo de planta industrial. En este nivel encontramos tantos sensores cómo actuadores.

Nivel 1 - Dispositivos inteligentes: La detección y manipulación de los procesos físicos se produce en este nivel, con sensores, analizadores, actuadores e instrumentación relacionada. Para impulsar la eficiencia, los sensores se comunican cada vez más directamente con el software de supervisión de su proveedor en la nube a través de redes celulares.

Nivel 2 - Sistemas de control: Se basa en el software de control y SCADA. Como ya sabemos, SCADA puede gestionar sistemas de manera remota, mientras que el sistema de control distribuido (DCS) y los controladores lógicos programables (PLC) suelen desplegarse dentro de la planta.

Nivel 3 - Sistemas de operaciones industriales: Aquí es donde se gestiona el flujo de trabajo de producción en la planta industrial. Se utilizan sistemas personalizados basados en sistemas operativos tipo Windows, para realizar la gestión, registrar datos y gestionar las operaciones y el rendimiento de la planta. Este nivel también consta de bases de datos o historiales para registrar los datos de las operaciones.

Niveles IT:

Nivel 4/5 - Empresa: Corresponde a los sistemas y redes IT tal y como la conocemos hoy en día, donde se producen las funciones empresariales principales. Este es el nivel que proporciona la dirección del negocio y orquesta las operaciones de fabricación. Los sistemas de planificación de recursos empresariales (ERP) dirigen los programas de producción de la planta, el uso de materiales, los envíos y los niveles de inventario. Cualquier interrupción en este nivel puede llevar a días o incluso semanas de inactividad, creando pérdidas de ingresos con los procesos posteriores retrasados o detenidos.

Posteriores mejoras añadieron el denominado nivel 3.5 o DMZ

Nivel 3.5 - Zona desmilitarizada (DMZ): Este nivel incluye sistemas de seguridad, como cortafuegos y proxies, que se utilizan para separar los entornos IT de OT. Aquí es donde los mundos IT y OT "convergen", aumentando enormemente la superficie de ataque para los sistemas OT. Muchas plantas no tienen esta capa o tienen capacidades muy limitadas. El aumento de la automatización ha creado una mayor necesidad de flujos de datos bidireccionales entre los sistemas OT e IT.

Incluso con una arquitectura estructurada en distintos niveles, cualquier sistema puede obtener datos de cualquier otro lugar de la planta. Aun así, los sistemas no necesitan los datos de todos los demás niveles. Por ejemplo, no se necesitan los datos de los sensores directamente en el sistema ERP. Será necesario estudiar qué sistemas necesitan realmente intercambiar datos y cuáles no, para establecer un aislamiento entre ellos.

En la figura 22 se ven los niveles, áreas (zonas grises) y conductos (zonas azules) que posibilitan la interconexión entre las distintas áreas y niveles. Obsérvese la presencia de firewalls en los conductos como elemento de ciberseguridad entre OT e IT.

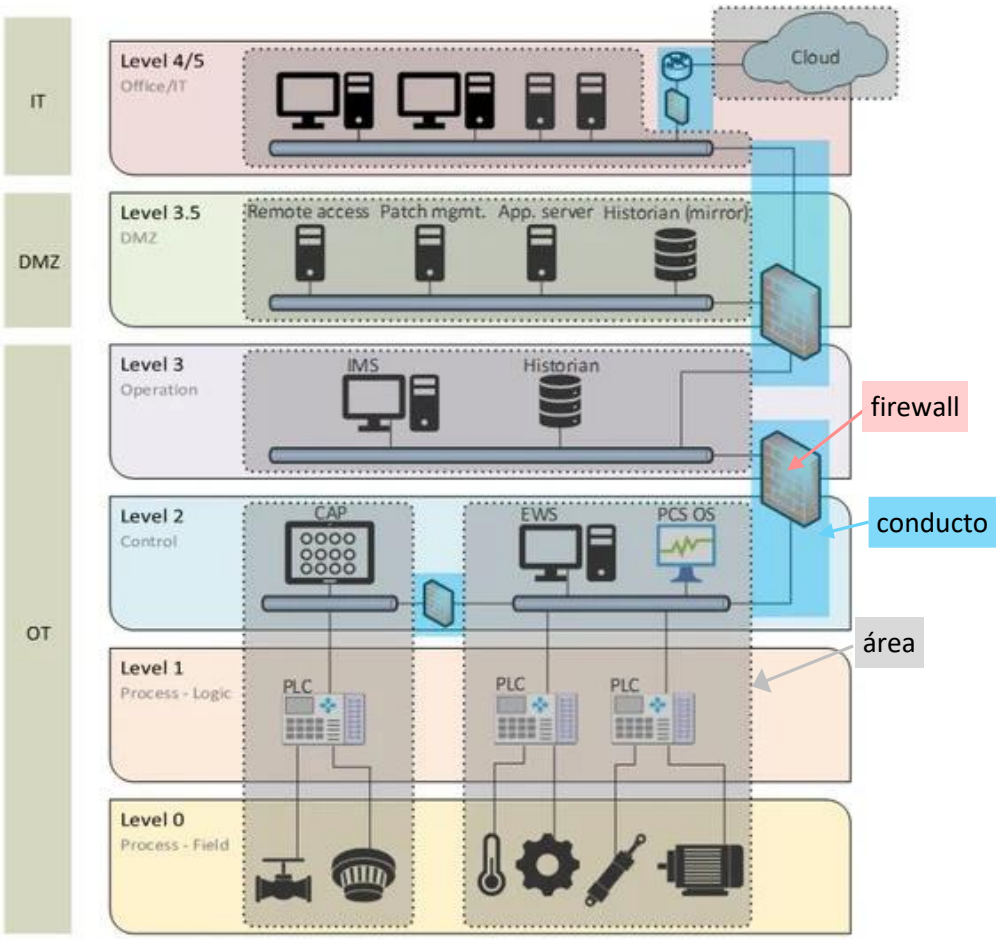


Figura 22: Arquitectura mejorada del modelo Purdue (www.mdpi.com)

Con la comprensión de este modelo, vamos a dar otro paso importante estudiando los equipos y dispositivos que pueden ser atacados en una planta solar fotovoltaica de generación de energía eléctrica.

3.5 ELEMENTOS Y DISPOSITIVOS SUSCEPTIBLES DE RECIBIR UN CIBERATAQUE EN OT

En principio cualquier dispositivo que tenga un sistema operativo embebido y ejecute alguna aplicación podría recibir un ciberataque. Sin embargo, nos vamos a centrar en equipos que están conectados a la red de comunicaciones local de la planta solar. Ya que por los procesos

que realizan, los efectos de una brecha de seguridad pueden ser más dañinos para la operación de la instalación.

En el Capítulo 2. analizamos los elementos de la red de comunicaciones, los protocolos utilizados y los dispositivos y sistemas que se interconectaban a la red. Fruto de este análisis podemos elaborar una lista de equipos que pueden ser atacados:

1. **Conmutadores LAN:** Elementos clave para construir una infraestructura de comunicaciones LAN.
2. **Inversores (nivel 1 PERA):** Elementos clave para la generación de energía en una planta solar fotovoltaica.
3. **PLCs (nivel 1 PERA):** Elementos clave para la automatización y control de estado de los dispositivos no inteligentes de la planta (sondas, sensores, protecciones, etc.).
4. **Power Plant Controller PPC (nivel 1 PERA):** Elemento clave para la regulación de la potencia de la planta.
5. **Servidores SCADA (nivel 2 PERA):** Elementos críticos del centro de control y operaciones locales y remotas.
6. **Operadores del sistema SCADA (nivel 1 PERA):** Factor humano, es el eslabón más débil de la cadena de seguridad.
7. **String box (nivel 0 PERA):** Pueden comunicarse vía Wifi para evitar los más costosos sistemas de cableado
8. **Router VPN (nivel 4/5 PERA):** Elemento clave para la interconexión con la supervisión externa.
9. **Otros equipos de ciberseguridad instalados (nivel 3,5 PERA):** Todos los dispositivos de ciberseguridad tienen un sistema operativo instalado, que puede tener vulnerabilidades no conocidas, o las propias aplicaciones de seguridad son susceptibles de recibir ciberataques. Sin embargo, su uso es de vital importancia para asegurar una red OT.

3.5.1 CONMUTADORES LAN

Los conmutadores LAN que se utilizan en OT, son funcionalmente equivalentes a los que se instalan en el mundo IT, aunque con algunas capacidades y características especiales del mundo industrial. Los diferentes ciberataques que se realizan en entornos IT, por lo tanto, pueden replicarse en OT.

Adicionalmente existen ataques específicos dirigidos a los protocolos de comunicaciones propios del mundo ICS (Modbus, Modbus TCP, IEC 104, IEC 61850). [3]

Cabe destacar, que los efectos en conmutadores LAN industriales pueden ser más dañinos en ambientes OT que en IT, esto es debido a que los requerimientos de fiabilidad y retardo son mucho más exigentes en los procesos de control industrial que en las instalaciones IT.

Para ver qué posibilidades de ciberseguridad ofrece un conmutador LAN, se ha seleccionado un fabricante de gama alta, como es cisco, y elegido uno de sus conmutadores industriales que tiene en su cartera de productos. Por ejemplo, el switch Industrial IE 4000 LAN Base.

Figura 23: Conmutador LAN de cisco IE 4000 (www.cisco,com)

En la tabla siguiente se visualizan las características, agrupadas por funcionalidades, más importantes de dicho equipo. Se han eliminado algunas no relevantes para este TFG, por motivos de espacio en la tabla.

Security	SCP, SSH, SNMPv3, TACACS+, RADIUS Server/Client, MAC Address Notification, BPDU Guard, Port-Security, Private VLAN, DHCP Snooping, Dynamic ARP Inspection, IP Source Guard, 802.1x, Guest VLAN, MAC Authentication Bypass, 802.1x Multi-Domain Authentication, Storm Control, Trust Boundary, FIPS 140-2, ACT2, Secure boot, Full flexible Netflow1
Management	Fast Boot, Express setup, Web Device Manager, Industrial Network Director (IND), MIB, Smartport, SNMP, syslog, storm control, unicast, multicast, broadcast, SPAN sessions, RSPAN, DHCP server, customized DOM (digital optical management), Embedded Event Manager (EEM), Plug-n-Play Agent, Port-based DHCP
Industrial Ethernet	CIP Ethernet/IP, Profinetv2, IEEE 1588 PTPv2, NTP to PTP translation, CIP Time Sync
Quality of service	Ingress Policing, Rate-Limit, Egress Queueing/shaping, AutoQoS, QoS, PROFINET QoS
Redundancy	Redundancy Ethernet Protocol ring (REP) Parallel Redundancy Protocol (PRP) Media Redundancy Protocol (MRP) ring, MRP Auto Manager (MAM) High Availability Seamless Redundancy (HSR), PTP over HSR HSR-PRP (Dual RedBox mode) HSR-HSR (Quadbox)
Utility	Power Profile 2011 and 2017, dying gasp, GOOSE messaging, SCADA protocol classification, MODBUS TCP/IP, utility SmartPort macro, BFD, Ethernet OAM, IEEE 802.3ah, CFM (IEEE 802.1ag)

Tabla 3: Funciones básicas del Conmutador LAN IE 4000 (www.cisco.com)

Los conmutadores LAN han sido y siguen siendo dispositivos de comunicaciones que se pueden atacar fácilmente, en el caso de que no se hayan habilitado correctamente las opciones de ciberseguridad, que la mayoría de los equipos de gama media/alta implementan.

En nuestro ejemplo, vemos que cisco tiene toda una gama de soluciones para fortificar su conmutador. De hecho, en la web del fabricante están disponibles varios documentos y artículos donde se explican detalladamente los diferentes tipos de ciberataques a los conmutadores, así como las soluciones disponibles. [4]

Lo más importante, además de que el equipo disponga de contramedidas para ataques ya conocidos, es su correcta configuración. Para ello es imprescindible conocer en detalle qué

tipo de ciberataque evita cada una de las alternativas de las que dispone el conmutador. No es viable activarlas todas, primero por lo complejo que sería el mantenimiento y gestión del equipo, segundo por el consumo de recursos hardware y software que ello implica.

En el caso del conmutador IE 4000 LAN Base, podemos contar hasta 21 contramedidas de seguridad posibles. Es decir, deberíamos conocer en profundidad que hace cada una, como se configura correctamente, etc. En la práctica, según varios estudios sobre este aspecto, lo normal es no hacer nada o casi nada, o peor aún, configurar mal el conmutador. [5]

Como ya vimos en el Modelo de Purdue: Enterprise Reference Architecture (PERA), es importante la segmentación de redes. En nuestro caso, separar los diferentes tipos de tráficos que circulan por la LAN de fibra, para formar diferentes áreas. Esta segregación de tráficos se puede hacer de dos maneras:

1. **Aislamiento físico de los diferentes tráficos:** Para ello desplegaremos múltiples anillos de fibra, y por cada anillo físico enviaremos el tráfico que corresponda a cada grupo de dispositivos. Por ejemplo, un anillo para el tráfico SCADA (área scada), otro para el tráfico de los seguidores solares (área trackers), el tercero para el envío de cámaras de seguridad (área camrec).

2. **Mediante el uso de VLANs (Redes Locales Virtuales):** Como ya se explicó en el Arquitectura y elementos de una planta solar fotovoltaica, la VLAN es una capacidad de la que disponen los conmutadores LAN que permite generar diferentes LANs virtuales sobre la misma infraestructura física. La seguridad en este caso es menor que el aislamiento físico, ya que existen ataques conocidos a las diferentes técnicas de implementación de VLANs, e incluso herramientas que permiten lanzar diferentes ciberataques específicos contra las VLANs [6]

En conclusión, es factible proteger los equipos industriales de comunicaciones de ataques internos, mediante la creación de distintas áreas. Los ataques internos se producen cuando

el hacker se puede interconectar a la red de comunicaciones de la planta, ya sea físicamente (atacante interno) o mediante el uso de un troyano (atacante externo). Para minimizar los riesgos y evitar este peligroso tipo de ciberataques, deberemos conocer y analizar las capacidades de ciberseguridad de los equipos utilizados y configurarlos adecuadamente.

También deberíamos deshabilitar los servicios no usados, por ejemplo, el servidor web embebido que suelen llevar este tipo de equipos, ya que el nivel de seguridad de este tipo de servicio suele ser bajo.

3.5.2 INVERSORES

Si buscamos en Google la siguiente frase "photovoltaic solar inverters ciberattaks" nos aparecen más de 1.5 millones de resultados. Es verdad que de las entradas que yo he podido ver, la mayoría de los documentos, informes y artículos se refieren a inversores utilizados en instalaciones de autoconsumo conectadas a Internet. No obstante, existen muchos documentos que expresan su preocupación por los posibles ataques a grandes plantas de generación de energía, de hecho, las primeras entradas de Google se refieren a estos ciberataques **[7]**.

Los inversores son los equipos clave para la generación de energía en una planta solar fotovoltaica. A nivel de su ciberseguridad, solo pueden ser atacados a través de los protocolos de comunicaciones que utilizan, normalmente el Modbus o el Modbus TCP, probablemente realizando un ataque de denegación de servicio (DoS), lo que nos produciría pérdidas económicas mientras se logre solventar dicho ataque.

De hecho, en 2017, en una presentación en la conferencia de seguridad SHA2017, Willem Westerhof, experto en ciberseguridad industrial, presento un escenario de un apagón en toda Europa, el origen se basaba en un análisis de vulnerabilidades de inversores fotovoltaicos del fabricante SMA, uno de los más conocidos del sector. Debido al revuelo que esto causo en Internet, el propio SMA tuvo que publicar varios documentos donde explicaba que esto se refería a inversores desarrollados ochos años atrás. En el siguiente enlace se puede acceder a un informe de SMA acerca de este incidente, con las respuestas de SMA a las citadas

vulnerabilidades [8]. Este caso, relativamente reciente, además de mediático, marca una línea de estudios y análisis de posibles ataques a inversores de gran tamaño mediante varias técnicas de ciberataques que utilizan medios indirectos (movimientos laterales) para conseguir su objetivo.

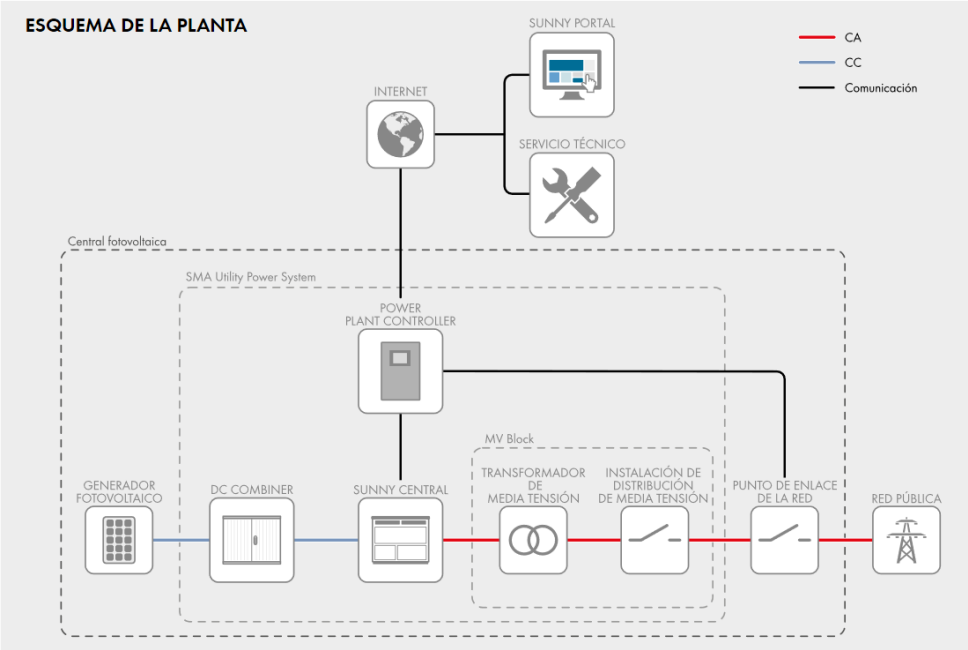


Figura 24: Esquema de planta y equipos relacionados (www.sma.de)

En la figura 24 observamos que el inversor recibe órdenes del PPC, y si este estuviese comprometido, por ejemplo, a través de un troyano que haya entrado en un PC conectado a la red interna de comunicaciones, se podría hacer que el inversor no trabajase a máximo rendimiento, lo que implica una perdida en la producción de energía de la planta.

3.5.3 PLCs – PACs

PLC es el acrónimo de Programmable Logic Controller, mientras que PAC significa Programmable Automation Controller. La mayor diferencia entre los PLC y los PAC reside en la forma en que se programan. Los PAC se programan usando lenguajes gráficos como diagramas de flujo, los cuales son muy intuitivos y de fácil comprensión, además de lenguajes orientados a objetos como C y C++, lo que hace que sean más adaptables y eficientes

Un controlador programable (PLC - PAC), es un dispositivo hardware que controla a otros equipos o procesos, en función de una lógica de circuito cerrado preprogramada. La lógica, o el programa, se almacena dentro del hardware utilizando una memoria "flash" no volátil, una memoria RAM respaldada por batería o un chip especial. Es decir, el dispositivo puede ejecutar la lógica integrada por sí mismo, sin la necesidad de un ordenador externo y un sistema operativo como Windows o Linux.

Los procesos que los controladores programables realizan en una planta fotovoltaica son:

- **Recepción de datos de instrumentación de campo:** Como sondas de temperatura, posicionamiento del colector, confirmaciones de marcha, etc.
- **Cálculo de la posición solar según algoritmos de alta resolución.**
- **Gestión del movimiento del colector:** Mediante el accionamiento, que puede ser de tipo hidráulico o con motores eléctricos, que permite rotar el sistema.
- **Control del ventilador instalado en el armario para refrigerarlo cuando sea necesario.**
- **Comunicaciones Ethernet:** Para comunicación con el sistema de control aceptando configuraciones y órdenes de éste y enviándole toda la información de estado del sistema.
- **Comunicaciones con un panel de operador:** Para el control y configuración de cada PLC de manera local.
- **Gestión del proceso:** Todas las CPUs de la instalación solar tienen exactamente el mismo programa, el cual contendrá toda la lógica necesaria para el proceso.

Para el estudio de la ciberseguridad de estos elementos vamos a utilizar un PAC de le compañía Emerson, en concreto el modelo RX3i CPE330 Controller.

Figura 25: Emerson RX3i CPE330 Controller (www.emerson.com)

A continuación, se adjunta su tabla de especificaciones.

• **Memoria**	64 MB
I/O	32k Bits Discrete I/O, 32k Words for Analog I/O
Redundancy Support	Media Redundancy (MRP), PROFINET System Redundancy (PNSR)
Ethernet Ports	3x 10/100/1000 (2 puertos)
Redundancia	REP (Redundancy Ethernet Protocol ring) PRP (Parallel Redundancy Protocol) MRP (Media Redundancy Protocol ring), MRP Auto Manager (MAM) HSR (High Availability Seamless Redundancy), PTP over HSR HSR-PRP (Dual RedBox mode) HSR-HSR (Quadbox)
Protocolos	Cliente/servidor SRTP, Modbus TCP/IP, Servidor OPC-UA, EGD, PROFINET, estación remota DNP3, cliente IEC-61850, servidor IEC-104, HART passthrough

Tabla 4: Especificaciones del Emerson RX3i CPE330 Controller. (www.emerson.com)

De dicha tabla vemos que este tipo de dispositivos permiten un gran número de posibilidades en lo que se refiere a sus comunicaciones, así como la redundancia a nivel de interconexión física (REP, PRP, etc.).

Aunque nos pudiera parecer, debido a sus características hardware (no es necesario un sistema operativo, no es un ordenador como lo es un PC, etc.), que un ciberataque es prácticamente imposible, el propio fabricante Emerson dispone de un documento de ciberseguridad en el que me llamo poderosamente la atención la siguiente frase: ***"No importa lo preparado que estes, ya que pueden ocurrir ataques o brechas de seguridad. Por lo tanto, es importante no solo tratar de evitar que ocurran, sino también asegurarse de que, si ocurren, el daño sea el mínimo posible."*** [9]

Para comprobar que la afirmación de Emerson era toda una profecía, a primeros del 2022, la empresa Mandiant junto con Schneider Electric, analizando una familia de herramientas de ciberataques a sistemas industriales, que llamaron INCONTROLLER, descubrieron nuevas posibilidades de amenazas. [10]

Estos raros y muy dañinos ciberataques, según define la propia Mandiant, se materializan mediante el uso combinado de tres distintos softwares. En la siguiente tabla se describen las diferentes funcionalidades de cada familia de programas.

Tool	Description
TAGRUN	A tool that scans for OPC servers, enumerates OPC structure/tags, brute forces credentials, and reads/writes OPC tag values.
CODECALL	A framework that communicates using Modbus—one of the most common industrial protocols—and Codesys. CODECALL contains modules to interact with, scan, and attack at least three Schneider Electric programmable logic controllers (PLCs).
OMSHELL	A framework with capabilities to interact with and scan some types of Omron PLCs via HTTP, Telnet, and Omron FINS protocol. The tool can also interact with Omron's servo drives, which use feedback control to deliver energy to motors for precision motion control.

Tabla 5: Herramientas de ciberataques a PLCs, INCONTROLLER (www.mandiant.com)

INCONTROLLER utiliza comunicaciones Modbus TCP, HTTP o telnet para introducir malware en varios tipos de PLCs de diferentes fabricantes.

En la figura siguiente, obtenida también de Mandiant se muestra, en el modelo de niveles de Purdue, el esquema completo de dicha amenaza y desde donde ataca. En este caso el ataque se produce desde el nivel de supervisión y control, es decir SCADA (servidores y equipos de los operadores). De nuevo nos puede parecer que esto resulta muy complejo y casi imposible en instalaciones bien protegidas. Cuando veamos más en detalle la ciberseguridad de los sistemas SCADA, veremos que este tipo de ciberataques son posibles y que pueden ser más sencillos de lo que parece.

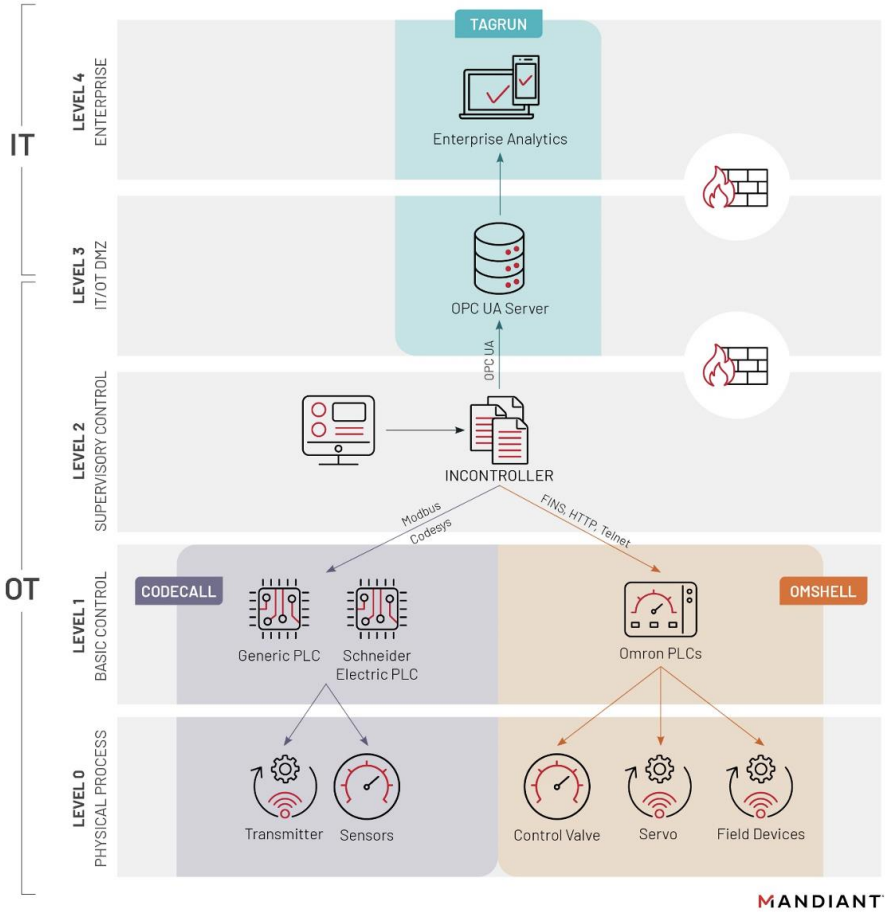


Figura 26: INCONTROLLER y sus ciberamenazas en OT aplicando el modelo PERA (www.mandiant.com)

Esto nos enseña que la ciberseguridad es una cadena en la entran demasiados actores, que es imposible controlar. Una intrusión o vulnerabilidad en un eslabón de la cadena de ciberseguridad, nos puede afectar sin tener ninguna capacidad de detectarla y evitar la ciber-amenaza.

3.5.4 POWER PLANT CONTROLLER (PPC)

El PPC es el corazón de la planta solar fotovoltaica desde el punto de vista eléctrico. A partir de la consigna recibida bien por parte del operador o del centro de control (MW, MVA, o lo que se quiera regular) fija las condiciones de funcionamiento para cada uno de los inversores. El PPC lee en tiempo real los parámetros eléctricos del POI (Point Of Interconnection).

Normalmente el PPC se construye en un PLC ó en un ordenador embebido/PC industrial.

En la siguiente tabla tenemos las especificaciones de un PPC de Gamesa que hace además funciones de control de los sistemas de baterías de la planta BESS (Battery energy storage system).

Para estudiar la ciberseguridad de un PPC vamos a utilizar uno de la empresa Gamesa que hace además funciones de control de los sistemas de baterías de la planta BESS (Battery energy storage system).

Figura 27: Gamesa Electric Orchestra Power Plant Controller para PV y BESS (www.gamesa.com)

A continuación, se adjunta la tabla de especificaciones del PPC elegido.

Inverter Compatibility	Gamesa Electric Proteus Series
Plant Configuration	Photovoltaic / BESS Standalone / Hybrid PV + BESS
Communications:	
Power Converters	Modbus TCP
SCADA	Modbus TCP
Grid Operator	Modbus TCP
Webserver	Included
Gir metering	Integrated Direct Analog Readings: 3 x CTs and 3 x VTs Optional: Grid Analyzer

Tabla 6: Especificaciones PPC Gamesa Electric Orchestra (www.gamesa.com)

Desde el punto de vista de comunicaciones, su intercambio de información tanto con los sistemas SCADA como con los inversores hace que el PPC necesite estar muy bien protegido.

Para ello y siguiendo el modelo PERA, deberá estar en la misma área que los SCADA locales de donde reciba información área y aislado mediante un firewall, junto con los equipos SCADA y auxiliares. También es necesario comprobar, mediante un analizador de vulnerabilidades, si tiene alguna sin parchear, sobre todo en los PPC basados en un ordenador embebido/PC industrial.

En la de especificaciones vemos que tiene un webserver incluido, es muy aconsejable deshabilitar este tipo de servicios, que resultan muy cómodos de usar a los operadores de planta y también a los potenciales hackers.

3.5.5 SERVIDORES SCADA

SCADA es un elemento clave de la infraestructura de una planta solar y por ello es un punto crítico y muy sensible de recibir ciberataques.

Históricamente, la mayoría de los sistemas de control industrial, incluido SCADA, estaban en redes separadas, no conectadas a Internet ni a ninguna otra red. Por desgracia, esta seguridad a través de la segmentación no protege completamente contra los ciberataques. En realidad, las redes rara vez están completamente aisladas. A menudo se instalan algunas actualizaciones software o se transfieren archivos de registro a estos sistemas de control. Si los sistemas no están conectados directamente a la red, el método elegido para este tipo de interacciones suele ser a través de una memoria USB o una conexión 3G no permanente, que proporciona una vía de acceso a las redes restringidas. Esto permite que el malware se propague en esas redes aisladas. Un ejemplo de este tipo de ciberamenzas fue el programa malicioso Stuxnet, del cual ya hemos hablado anteriormente, que se infiltró en gran variedad de sistemas SCADA en 2010. [11]

Además, si las redes están realmente segmentadas, esto significaría que no se instalarían actualizaciones de software, dejando las antiguas vulnerabilidades, a no ser que instalemos un sistema de actualizaciones en la propia planta. También hay problemas en torno a los procesos. Por ejemplo, las listas de revocación de los certificados digitales rara vez se actualizan y, por lo tanto, los certificados que ya no son válidos no se pueden comprobar adecuadamente y seguirían siendo aceptados. Por ello, aunque se crea que SCADA está aislado de la red y de Internet y por ello está a salvo, es una sensación de seguridad que nada tiene que ver con la realidad.

La mayoría de los protocolos SCADA nunca fueron concebidos para su uso en redes de acceso público y, en algunos casos, ni siquiera en redes IP. Mobus y Modbus TCP, protocolos típicos para SCADA. Estos protocolos se diseñaron sin tener en cuenta la ciberseguridad y para un uso en redes sencillas de control de procesos entre clientes y servidores. No se ha añadido ninguna protección adicional para asegurar las comunicaciones enviadas mediante estos protocolos. Para eliminar este problema tendríamos que cifrar y autenticar estos protocolos, lo que puede o no puede ser posible, en función de los diferentes productos de fabricantes que estemos utilizando.

Por otro lado, el problema de SCADA es una de sus mayores virtudes: su gran capacidad es conexión con distintos dispositivos. Puede llegar a ser difícil saber cómo están configurados todos los equipos que están controlados por SCADA.

Hay componentes equipados con funciones y servicios que permiten a los proveedores y operadores el acceso remoto a ellos. Estas interfaces aportan grandes ventajas a la hora de controlar y monitorizar los dispositivos ya que permiten al personal actualizar y configurar remotamente el software de estos elementos a través de Internet o de una conexión 3G. Estas conexiones externas suelen ser consideradas seguras, pero puede no ser así. Las contraseñas por defecto son un fenómeno común en los dispositivos de campo. Algunas políticas corporativas exigen que las contraseñas se cambien con una periodicidad mensual. Sin embargo, esta medida de seguridad rara vez se aplica a los sistemas SCADA, debido a los recursos necesarios para cambiar manualmente las contraseñas en cientos de dispositivos, y el riesgo para la empresa si estos dispositivos se vuelvan inaccesibles. Además, no es infrecuente que las que las interfaces supuestamente desconectadas estén en realidad conectadas y accesibles de forma constante. Dado que estas interfaces suelen estar destinadas al personal de soporte, el acceso a las mismas suele proporcionar privilegios que pueden utilizarse para reconfigurar dispositivos, borrar configuraciones o eliminar la funcionalidad de los equipos de protección. Por lo tanto, las personas no autorizadas podrían comprometer gravemente la funcionalidad de los dispositivos de campo y también influir en el comportamiento de otras partes del sistema SCADA.

La gestión de los firewalls en SCADA es más compleja de lo que parece. Como muchas veces se aplican tecnologías prefabricada para plantas solares dentro del dominio del sistema de control, el número de protocolos, puertos y servicios utilizados aumenta y a menudo dificulta su seguimiento. Por lo tanto, del mismo modo que puede haber una falta de información sobre qué servicios deben estar activados para que los ordenadores funcionen, suele faltar información sobre los parámetros necesarios para configurar los firewalls restrictivamente sin poner en peligro las operaciones

Hay varios pasos importantes que deben tomarse para asegurar las redes SCADA:

- ✓ Parchear los sistemas operativos del host, las aplicaciones y los componentes SCADA.
- ✓ Controlar las comunicaciones de las aplicaciones entre las redes SCADA y otras redes.
- ✓ Controlar las comunicaciones de las aplicaciones dentro de las redes SCADA.
- ✓ Controlar qué y quién puede interactuar con las redes y sistemas SCADA.
- ✓ Supervisar todas las redes y reaccionar rápidamente ante los virus y ataques.

Lamentablemente, debido a su criticidad, no siempre es posible aplicar parches a los sistemas SCADA en los plazos necesarios para evitar un ataque. La siguiente mejor solución es utilizar una estrategia de defensa en profundidad aplicando la seguridad de la capa de aplicación tanto en el host RTU como a nivel de red. Lo que se necesita es un sistema de seguridad consolidado que ofrezca múltiples mecanismos de detección, incluyendo:

- ✓ Firewalls con conocimiento del estado de las aplicaciones.
- ✓ Detección de antivirus.
- ✓ Control de aplicaciones.
- ✓ VPNs.
- ✓ Actualizaciones automáticas de las bases de datos de firmas de antivirus e IPS.
- ✓ Vulnerabilidade SCADA conocidas que estén incluidas en las bases de datos de antivirus y detectores de intrusos IPS.
- ✓ Prevención de anomalías en la red y de DoS.
- ✓ Protección de las bases de datos.

3.5.6 OPERADORES DEL SISTEMA SCADA

Es el eslabón más débil de la cadena de ciberseguridad, susceptible de sufrir ataques de ingeniería social, cometer errores por desconocimiento, malas prácticas, presión en momentos de aparición de problemas técnicos, etc.

Además, a primeros del 2022 ha aparecido un nuevo método de ataques a dispositivos industriales que evitan incluso la protección de firma digital en módulos software que se instalan en este tipo de equipos. En concreto el ataque se realizó robando la clave de firma de código de un conocido fabricante de drivers industriales (ASROCK), introduciendo un

malware en el mismo y firmando este driver con la firma de ASROCK. Esto permitió la introducción de dicho malware evitando los sistemas más seguros que comprueban la firma digital en el proceso del arranque del equipo.

En 2022 se ha emitido un aviso en Estados Unidos por el Departamento de Energía (DOE), CISA (Cybersecurity and Infrastructure Security Agency), la NSA (National Security Agency) y el FBI (Federal Bureau of Investigation), anunciando el peligro que corren los sistemas SCADA ante ciberamenzas [12]. En el documento se trata un ataque de amenaza persistente o ATP (Advanced Persistent Threat). Es un tipo de malware diseñado para atacar a una empresa o institución con el fin de robar información y mantenerse oculto en el sistema todo el tiempo que le sea posible, sin ser detectado.

3.5.7 STRING BOX O CAJAS DE CORRIENTE CONTINUA

Las cajas de corriente continua pueden comunicarse vía Wifi para evitar los más costosos sistemas de cableado. El problema de Wifi es la utilización del espectro electromagnético para transmitir los datos, para asegurar estas comunicaciones, los equipos Wifi pueden cifrar los datos y autenticar las conexiones de los clientes que intentan conectarse al punto de acceso Wifi.

Esta tecnología IT es una de las más utilizadas y una de las que más ataques recibe. Existen miles de enlaces en Internet donde se muestra como atacar a sistemas Wifi, sobre todo en instalaciones particulares. En las redes empresariales de IT se utiliza Wifi con soluciones más robustas y a la vez más complejas, que usan técnicas criptográficas avanzadas y servidores adicionales para autentificar a los usuarios. Para complicar aún más esto, existen diferentes estándares de cómo se implementan estás medidas de ciberseguridad. La inicial y obsoleta WEP (rota hace ya mucho tiempo), su sucesora WPA2 con muchas vulnerabilidades conocidas y el actual WPA3 que supuestamente arregla todos los problemas conocidos en su antecesor WPA2.

En entornos IT empresariales se aconseja no utilizar la posibilidad de usar ni el WPA2 ni el WPA3 con password precompartida. En un ambiente OT es más que aconsejable utilizar

solo WPA3 y hacer un análisis riesgo/beneficio de utilizar un servidor de autenticación. Otra posibilidad es utilizar una VPN sobre Wifi para asegurar doblemente las comunicaciones inalámbricas. Si un hacker rompe la seguridad Wifi se encontraría con una VPN cifrada y autenticada que tendría que volver a atacar.

3.5.8 ROUTER DE RED PRIVADA VIRTUAL (VPN)

El conducto de comunicaciones esencial que se utiliza para acceder de forma remota a los sistemas de control es una red privada virtual. Una VPN agrega una capa de seguridad (cifrado, autenticación, privacidad) sobre un acceso a través de una red pública (Internet, 3G, Wifi, etc.) para protegerla del acceso público.

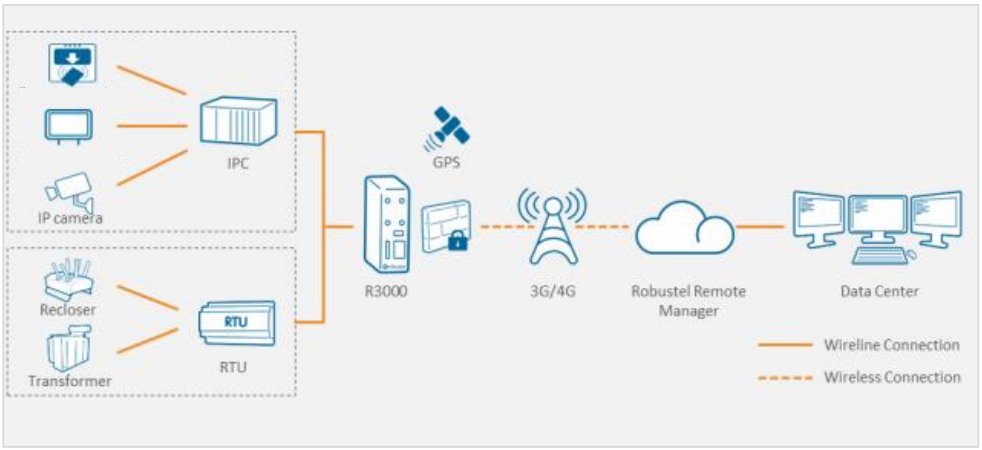


Figura 28: Ejemplo de aplicación de una VPN (www. xacom.com)

Cuando se configura una VPN, se dice que se crea un túnel entre un equipo externo y un equipo final de la VPN interno. Una VPN puede proporcionar autenticación, cifrado e integridad a los mensajes de información. Para crear una VPN se pueden utilizar diferentes técnicas criptográficas para intercambiar las distintas claves que usarán los equipos. En entornos IT es muy común utilizar VPNs basadas en SSL (Secure Sockets Layer). El SSL también se utiliza para accesos remotos y en Internet para el envío seguro de páginas web de los servidores. En SSL se cifra toda la información que va sobre el TCP.

Algunos fabricantes ofrecen soluciones que incluye la conectividad a través de un servicio de doble VPN en la nube consiguiente aumentar la seguridad. En la figura siguiente se ve la arquitectura de este tipo de soluciones.

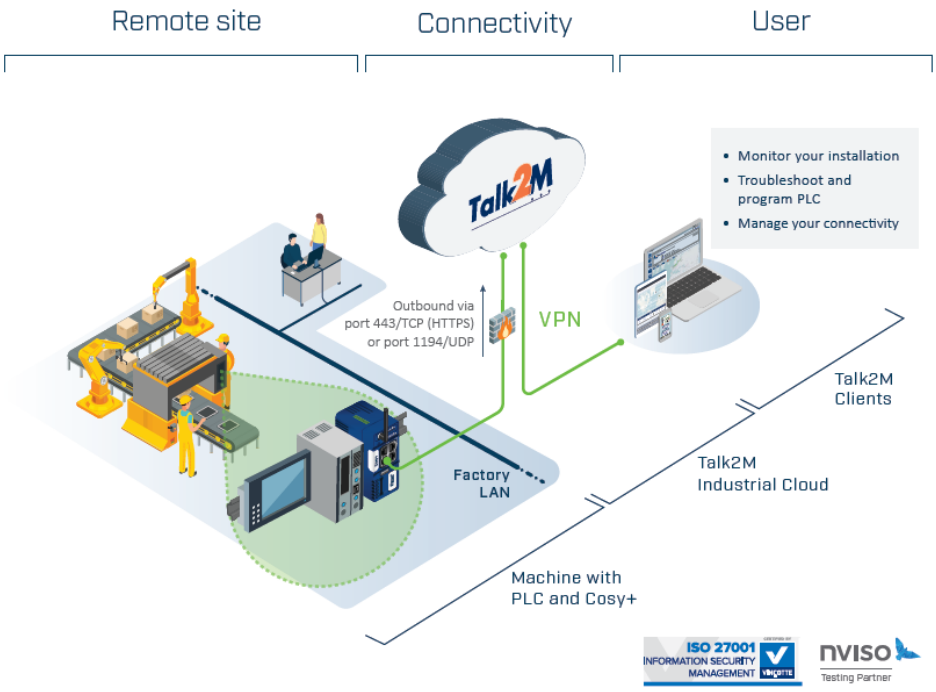


Figura 29: Solución de router industrial de Ewon Cosy con conectividad "Talk2M" (www.ewon.biz)

Obsérvese que se establecen dos VPNs, una entre el equipo externo con los servidores VPN alojados en la nube y desde allí la VPN que acaba en la instalación industrial destino. Esta arquitectura, permite un mayor control en el acceso y por lo tanto mejora la ciberseguridad.

Por otra parte, si analizamos las características técnicas de un router VPN de OT, podremos ver qué tipo de VPN ofrece, así como el acceso al router para su mantenimiento y configuración. En este caso hemos elegido un router 3G/4G modelo SCALANCE M de la empresa Siemens, con soporte VPN.

Figura 30: Siemens SCALANCE M (www.siemens.com)

En la tabla siguiente se ven las características de las tres gamas de este router VPN OT.

Model	**SCALANCE M876-4**	**SCALANCE M876-3**	**SCALANCE M874-3**
Standard	4G (LTE)	3G (UMTS, CDMA2000)	3G (UMTS)
Data rate	Downlink: up to 100 Mbps; Uplink: up to 50 Mbps	Downlink: 14.4 Mbps; Uplink: 5.76 Mbps (HSPA+); Forward link: 3.1 Mbps; Reverse link: 1.8 Mbps (EV-DO)	Downlink: 14.4 Mbps; Uplink: 5.76 Mbps (HSPA+)
Antenna connectors	2 x SMA	2 x SMA	1 x SMA
Degree of protection	IP20		
Security	VPN (IPsec / OpenVPN*) / Firewall		
Engineering	Command Line Interface (CLI), Web-based Management (WBM), MIB support, TRAPs via e-mail		
Special characteristics	Redundant power supply; Network management via SNMP; SMS alarming; Connection to SINEMA Remote Connect; NAT		

Tabla 7: Tabla características gama Siemens SCALANCE M (www.siemens.com)

Se puede ver el soporte de VPN tipo IPsec o OpenVPN en esta gama de productos. IPsec es un estándar IETF de Internet muy robusto y complejo, mientras que OpenVPN es una herramienta basada en software libre que utiliza SSL. También podemos comprobar que el router lleva incluidas las funcionalidades de un firewall.

De nuevo vemos que el acceso a un servidor embebido en el equipo es una opción que suelen incorporar la mayoría de los fabricantes, con independencia del tipo de equipo de comunicaciones (conmutador, Wifi, router, etc.). Como ya se ha comentado varias veces en este TFG, todos los organismos, agencias gubernamentales y empresas de ciberseguridad recomiendan que se deshabiliten este tipo se servicios. La razón es sencilla, suelen encontrarse constantemente vulnerabilidades de seguridad en estos servidores embebidos, que si no se parchean puede suponer una seria amenaza para toda la planta.

Las plantas solares fotovoltaicas están situadas en el campo, a menudo alejadas de la posibilidad de tener accesos mediante fibras ópticas u otros servicios de los proveedores de acceso (Movistar, Orange, Vodafone, etc.). Se suelen utilizar conexiones 3G o conexiones satelitales para interconectar la VPN con las instalaciones remotas del operador eléctrico que quiere telecontrolar la planta solar. Este tipo de conexiones pueden ser atacadas mediante un dron equipado con un equipamiento denominado “ISMI catcher” [13] que realiza lo que se denomina un ataque de “hombre en medio”. En resumen, el ISMI se comporta como una estación base de telefonía 3G frente al router VPN y como un cliente frente a la estación base del operador de telefonía móvil.

En la figura siguiente se ve el funcionamiento lógico de un sistema de “hombre en medio” para interceptar conexiones 3G, en este caso es un dron de Skycam technologies equipado con un ISMI catcher, cámara, etc.

Figura 31: Aerial ISMI Catcher (Google imágenes)

En este caso se realiza un "down gradding" al router 3G para que utilice las antiguas comunicaciones GPRS, de menor velocidad y cuya seguridad a nivel de cifrado ya está rota. Esta misma técnica se puede usar para atacar las comunicaciones Wifi, en este caso el equipo que lleva el dron es un punto de acceso Wifi.

Por último, quiero indicar que el uso de VPNs en este tipo de instalaciones es absolutamente imprescindible, aunque ello no conlleva que las propias VPNs estén libres de amenazas y vulnerabilidades.

3.5.9 EQUIPOS DE CIBERSEGURIDAD INSTALADOS

En este caso nos referimos a los equipos de seguridad instalados en la red de comunicaciones de la planta fotovoltaica, como son los firewalls, diodos de datos y sistemas de detección de anomalías y amenazas.

Estos dispositivos, nos van a proporcionar una mejora muy importante en la ciberseguridad de nuestra planta. Sin embargo, no debemos olvidar que siguen siendo equipos hard/soft y por lo tanto pueden recibir ciberataques de múltiple naturaleza. También los errores humanos

en su configuración, olvidos y malas prácticas pueden abrir brechas de ciberseguridad, si no disponemos de una buena metodología y guías de uso adecuadas.

Lo normal es encontrarnos con un firewall que protege el punto de entrada de las comunicaciones externas y otros firewalls dentro de la red protegiendo a equipos críticos e impidiendo las comunicaciones que queramos prohibir (recuérdese el concepto de las áreas del modelo PERA).

En términos simples, los firewalls son un medio para bloquear o permitir la transmisión de datos entre ordenadores y dispositivos inteligentes en una red de manera condicional. En la siguiente figura se ve el uso de firewalls para filtrar y proteger las redes y sistemas OT de las redes y sistemas IT.

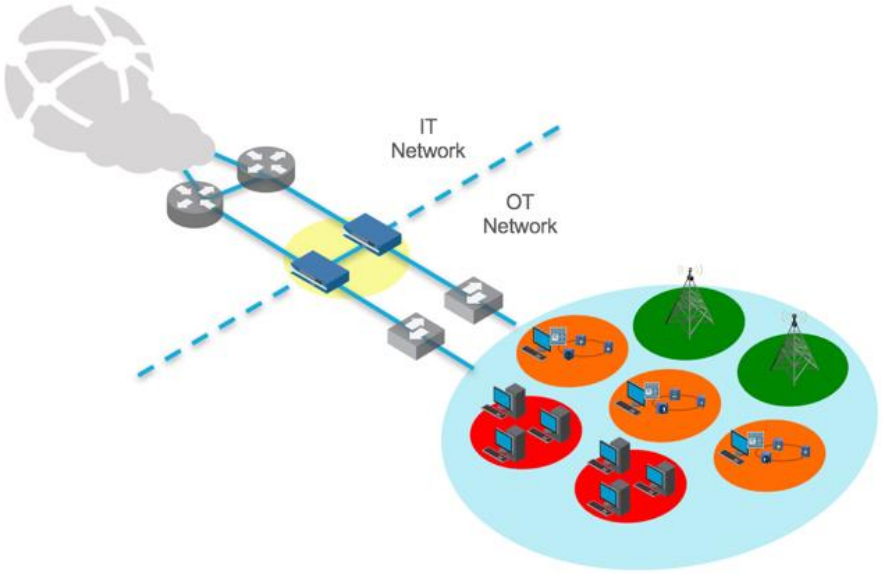


Figura 32: Firewalling IT-OT (www.knowledgebase.paloaltonetworks.com)¡

El filtrado de los mensajes de un firewall se puede realizar por:

- Dirección IP.
- Protocolo.
- Dirección del flujo de datos (entrada o salida).

- Estado del canal de comunicaciones (por ejemplo, quién inició las comunicaciones).

Los firewalls modernos pueden ser muy sofisticados y pueden incluir numerosas características adicionales más allá de la capacidad básica de filtrar mensajes. En el mundo IT, además existen diferentes tipos de firewall, en función de sus capacidades, características avanzadas, donde se realiza el filtrado, si los procesos los realizan por software o por hardware, etc.

En OT, además de servir de primer nivel de "corta fuegos" entre IT e OT, también se utilizan internamente, dentro de la red OT, para realizar dos tipos de funciones:

- **Realizar filtrados internos**. Utilizando reglas específicas entre las diferentes áreas existentes, muy distintas a las que se usan en el firewall de entrada.
- **Crear zonas desmilitarizadas (DMZ)**. Una DMZ es una red separada que actúa como una zona de amortiguamiento entre dos redes físicas que no confían entre sí, pero necesitan intercambiar cantidades limitadas de datos. La DMZ se crea mediante el uso de un firewall entre cada una de las redes y la DMZ.

En la figura 33 se ve una instalación OT donde se ve un firewall de entrada (del fabricante Palo Alto) que a su vez crea tres (3) DMZs (DMZ 1, DMZ 2 y DMZ 3), en color naranja. En cada DMZ están situados servidores diferentes, por ejemplo, en la DMZ 2 se encuentra un servidor web y otro servidor que realiza las tareas de parcheo de vulnerabilidades.

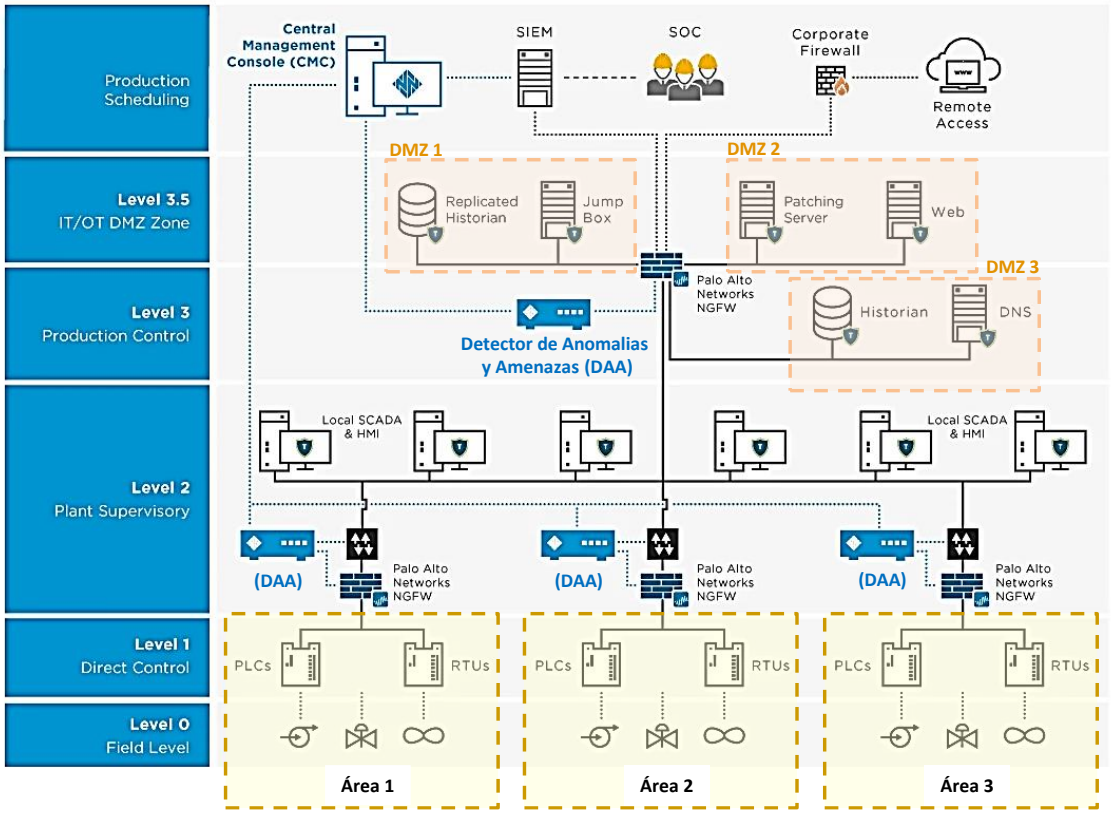


Figura 33: Instalación OT con tres DMZs, tres áreas y un sistema de detección de anomalías y amenazas (https://www.nozominetworks.com)

También podemos comprobar cómo se han separado los diferentes PLCs existentes en tres áreas (color amarillo) mediante la utilización de tres firewalls. Por último, se está utilizando un sistema para detectar anomalías y amenazas (DAA).

Los Detectores de Anomalías y Amenazas son equipos que monitorizan constantemente la parte del tráfico de la red donde están conectados e identifican amenazas de ciberseguridad y otros riesgos mediante reglas complejas, firmas de vulnerabilidades conocidas e incluso el uso de inteligencia artificial.

Otra medida de ciberseguridad son los diodos de datos que ofrecen una solución reforzada por hardware para defender las redes OT y los sistemas de seguridad. Para ello su utiliza un flujo de datos unidireccional sin permitir que regresen las amenazas.

En la siguiente figura se ve el funcionamiento de los diodos de datos.

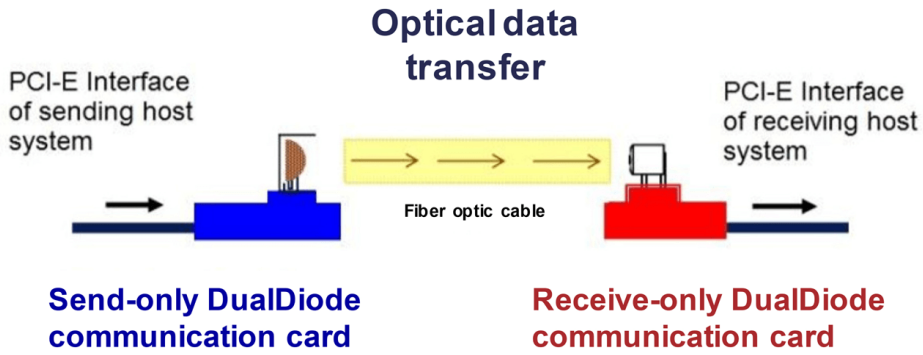


Figura 34: Diodo de datos en una fibra óptica (https://iebmedia.com/)

El flujo de datos unidireccional en los diodos de datos está diseñado para proteger las redes OT de las amenazas externas. Para ello elimina el flujo de datos entrantes y, en última instancia, las amenazas externas de un posible hacker a los segmentos de la red OT, al tiempo que proporciona el flujo de datos necesario para monitorizar la instalación.

3.6 FASES DE UN CIBERATAQUE (DESDE LA PERSPECTIVA DE UN HACKER)

Un ejercicio útil para pensar en la ciberseguridad de IT y OT es ver las diferentes acciones que un atacante realizaría o podría realizar para comprometer un sistema OT.

La compañía Lockheed Martin, ha creado un marco de acción denominada “Cyber Kill Chain” para describir estos pasos que podría dar un hacker. La figura 35 resume las diferentes fases de un ciberataque.

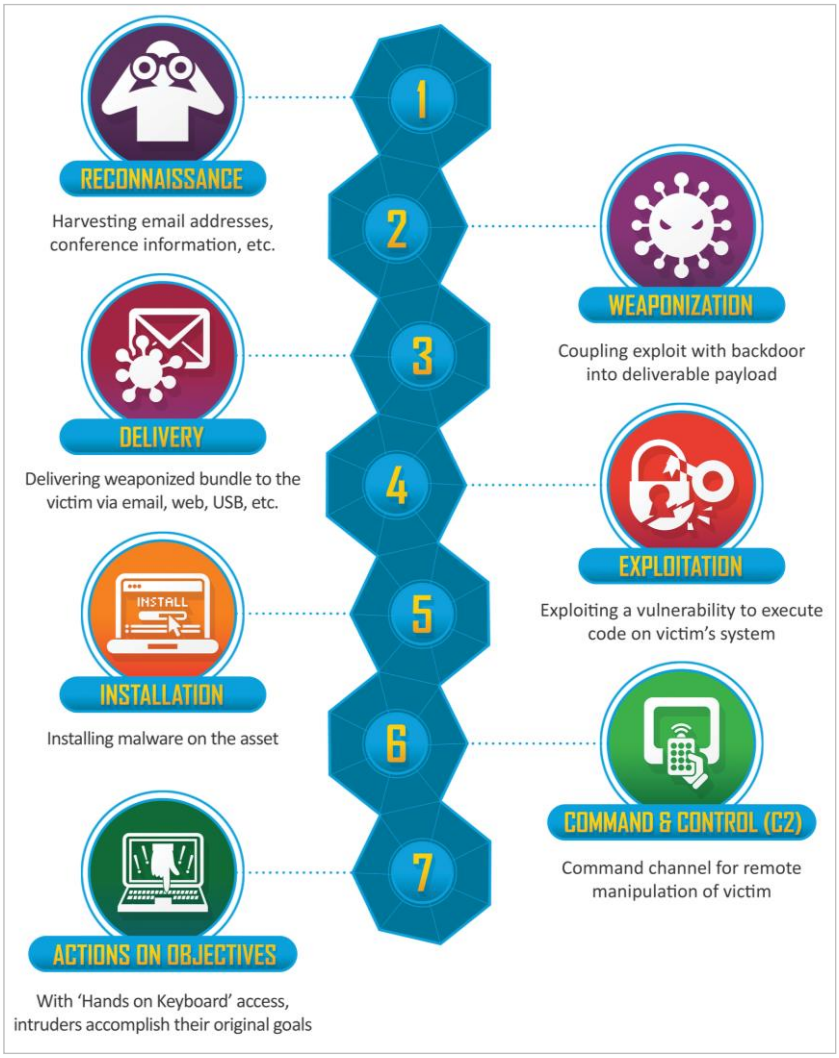


Figura 35: Las 7 fases de un ciberataque -The Lockheed Martin Cyber Kill Chain Framework (https://www.lockheedmartin.com)

Evidentemente este modelo genérico no siempre se va a dar, no todos los ciberataques requieren cada fase descrita en Ciber Kill Chain. Las fases generales de un ataque, como se describe en el marco "Ciber Kill Chain" de Lockheed Martin son:

1. **Reconocimiento:** Investigación, identificación y selección de objetivos e intentos de descubrir vulnerabilidades en la red, equipos y sistemas objetivos de un ciberataque.
2. **Armamento:** Creación de malware de acceso remoto diseñado para explotar el sistema basado en las vulnerabilidades identificadas.

3. **Entrega:** Transmisión del malware al objetivo, mediante un archivo adjunto de correo electrónico, USB, ftp, etc.
4. **Explotación:** El código del malware se activa para explotar la vulnerabilidad detectada.
5. **Instalación:** El malware instala un troyano de acceso remoto o una puerta trasera que puede utilizar el hacker.
6. **Comando y control:** El malware generalmente necesita configurar un canal de comunicaciones para comando y control, a través del cual puede comunicarse con el atacante.
7. **Acciones sobre el objetivo:** El atacante está ahora en posición de realizar acciones maliciosas, como robar, destruir, o corromper información, etc.

Para ver estos procesos, vamos a realizar tres prácticas sencillas. El objetivo es comprobar varios aspectos. Primero investigar, usando el buscador Google, el nivel de herramientas de ataque (pentesting, hacking ético, analizadores de vulnerabilidades, centros de información de vulnerabilidades, etc.) que se encuentran disponibles en Internet. Segundo, comprobar el grado de dificultad en el uso de las herramientas que vamos a utilizar y tercero ver su eficiencia desde el punto de vista de los ciberataques.

Debido a las limitaciones evidentes de este TFG y de los medios limitados que dispongo, he creído conveniente hacer las siguientes 3 prácticas. Además de la documentación escrita de las mismas, he añadido un vídeo de cada una de ellas para complementar la información obtenida durante su ejecución.

Las prácticas desarrolladas son las siguientes:

- **Practica 1**: Fase de reconocimiento básico y descubrimiento de vulnerabilidades de un inversor solar fotovoltaico en una instalación de autoconsumo. Para ello utilizaremos la herramienta NMAP de nmap.org
- **Practica 2**: Fase de reconocimiento avanzado “sigiloso”, identificación y análisis de vulnerabilidades encontradas a través de centros de información on-line. Para ello

utilizaremos el servicio web que ofrece Shodan y analizaremos las vulnerabilidades en varios centros de información on-line.

- **Practica 3**: Corresponde a las Fases 2,3,4,5 y 6. Para ello, y una vez detectada una vulnerabilidad en el equipo atacado, utilizaremos una herramienta denominada metaesploit que se caracteriza por su sencillez de uso y automatización de dichas fases, es decir armamento, entrega, explotación, instalación y comando y control.

3.6.1 PRACTICA 1: RECONOCIMIENTO (ESCANEO) DE UN INVERSOR FOTOVOLTAICO EN UNA INSTALACIÓN DE AUTOCONSUMO CASERO.

Se adjunta el link del vídeo de la práctica: https://youtu.be/bxxOOXj0V84

Esta práctica tiene como objetivo la realización de un análisis preliminar para ver las vulnerabilidades de un dispositivo inteligente y conectado a la red. En nuestro caso es un inversor de la instalación solar fotovoltaica de mi vecino, una vez que he obtenido su permiso para la realización de esta práctica.

El objetivo es familiarizarse y ver el funcionamiento de una herramienta freeware, muy utilizada, que permite conocer los servicios (aplicaciones) que tiene abiertos un equipo informático, así mismo podemos conocer el tipo y versión del su sistema operativo. En concreto utilizaremos el nmap (www.nmap.org) en su versión para Windows con un interface gráfica que es más sencillo de usar que el uso de comandos.

Aunque este TFG está enfocado a Plantas de generación de energía eléctrica, vamos a realizarla en un entorno de autoconsumo casero, más asequible y evidentemente mucho menos protegido a nivel de ciberseguridad. Esto nos permite entender los procesos básicos de la fase de reconocimiento que hacen los hackers previos al posible ataque o intrusión.

Ya se vio en el capítulo de descripción de la infraestructura de comunicaciones, que es habitual que los inversores de gran tamaño, disponga de alternativas Wifi para comunicarse con otros dispositivos.

Lo primero que tenemos que averiguar es si el inversor que estamos reconociendo tiene Wifi, y en caso de que así sea, cual es la identificación de la red. Para ello solo hace falta ver las redes Wifi que nuestro ordenador ve. Observamos, según se aprecia en la figura siguiente, que nos aparece una red con el candado (está cifrada) cuya identificación es SUN200, lo que nos indica, por su nombre, que puede ser la del inversor y además no tiene conectividad con Internet.

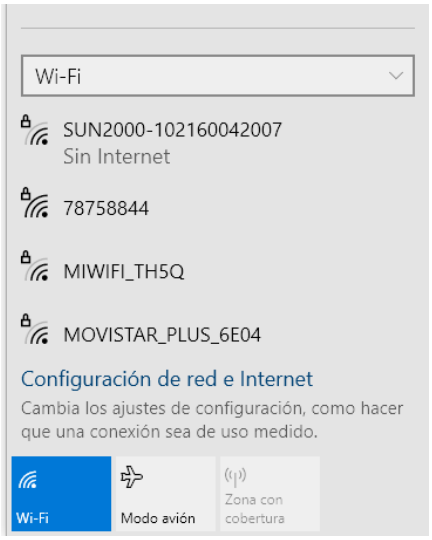


Figura 36: Redes Wifi Disponibles

El siguiente paso es acceder a Google y buscar la palabra SUN200, esto nos permitirá saber si estamos en lo cierto.

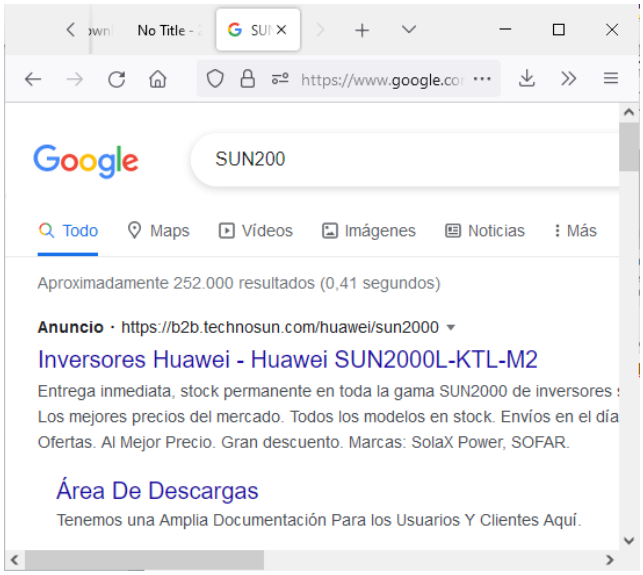
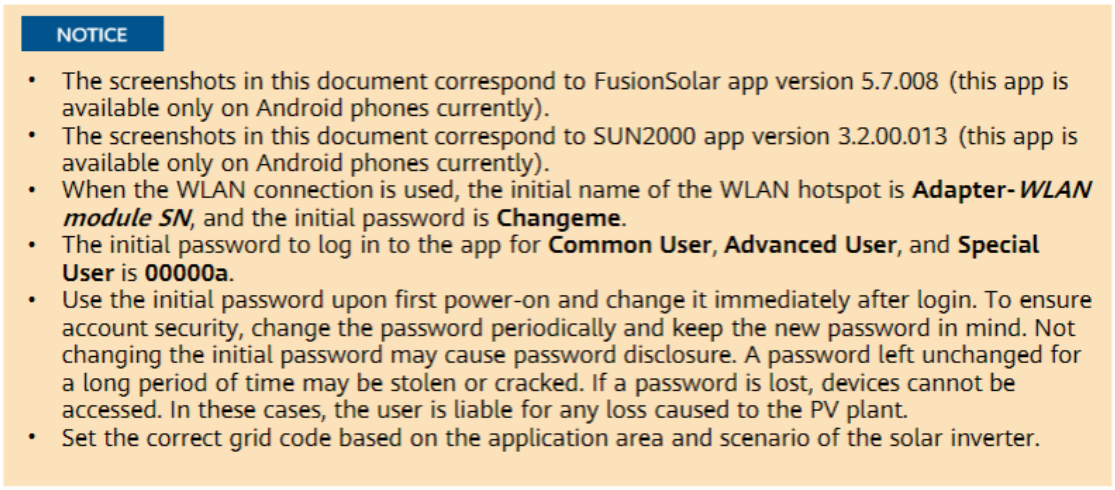


Figura 37: Resultados de la búsqueda en Google

El primer resultado cuadra al 100% y nos dice que pudiera ser un inversor del fabricante Huawei. El siguiente paso es descargar su manual de instrucciones y toda la información que encontremos de su instalación. El objetivo es ver las características de comunicaciones de este y cuáles son los usuarios y passwords por defecto, ya que lo normal es que esta información, altamente sensible, no se modifique.


NOTICE

- The screenshots in this document correspond to FusionSolar app version 5.7.008 (this app is available only on Android phones currently).
- The screenshots in this document correspond to SUN2000 app version 3.2.00.013 (this app is available only on Android phones currently).
- When the WLAN connection is used, the initial name of the WLAN hotspot is **Adapter-*WLAN module SN***, and the initial password is **Changeme**.
- The initial password to log in to the app for **Common User**, **Advanced User**, and **Special User** is **00000a**.
- Use the initial password upon first power-on and change it immediately after login. To ensure account security, change the password periodically and keep the new password in mind. Not changing the initial password may cause password disclosure. A password left unchanged for a long period of time may be stolen or cracked. If a password is lost, devices cannot be accessed. In these cases, the user is liable for any loss caused to the PV plant.
- Set the correct grid code based on the application area and scenario of the solar inverter.

Figura 38: Búsqueda de usuarios y passwords por defecto en el manual de instalación

Ahora toca probar si podemos acceder usando la password por defecto, que es **Changeme**. Pero antes de intentarlo, estudiaremos el esquema de instalación de estos inversores desde el punto de vista de sus comunicaciones. En la figura siguiente, sacada del manual, se aprecian las diferentes alternativas de interconexión que ofrece el fabricante.

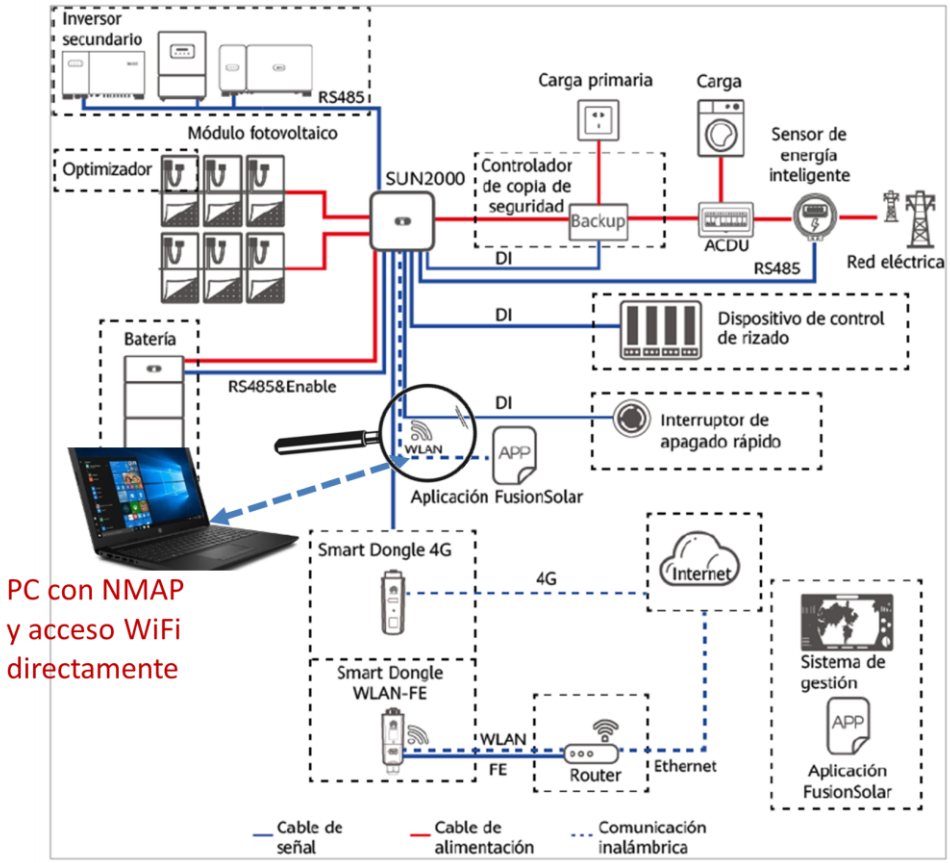


Figura 39: Esquema de instalación inversor SUN 200 (manual de instalación)

Para el envío de información al sistema de gestión externo se puede utilizar un "Smart dongle WLAN-FE" para que el inversor se conecte a la red Wifi del propietario de la instalación o mediante una red 4G.

Por otra parte, el inversor dispone de una red Wifi para que el instalador o el técnico de mantenimiento pueda configurar los parámetros o realizar mantenimiento. Parece obvio que el fabricante pretende que en caso de problemas o averías los técnicos no tengan que solicitar permiso y claves al propietario, pudiendo acceder al inversor mediante una aplicación que

está disponible en su web, para modificar, configurar y mantener el equipo. Esto va a generar una brecha de seguridad, como veremos más adelante.

Si no se ha cambiado las passwords, estaríamos en disposición de realizar un ataque de reconocimiento sin tener que acceder a la red Wifi del propietario de la instalación. Como era de esperar, al introducir la password por defecto entramos en la red Wifi del inversor. ¡No se había cambiado la misma!

Para saber nuestra IP en esta red y la del inversor solo tenemos que ir al símbolo del sistema (CMD) y teclear ipconfig, es decir ver la configuración que hemos obtenido al entrar en la red WiFi del inversor (figura siguiente).

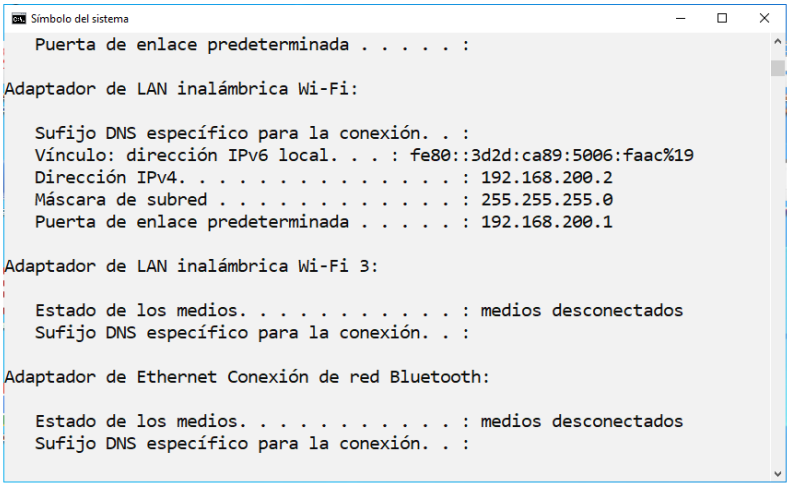


Figura 40: Captura de pantalla de la cmd de mi ordenador

Comprobamos que nuestra IP es la 192.168.200.2 y la del inversor tendrá que ser la 192.168.200.1 ya que es la puerta de enlace (router de salida) en el caso de que tuviera acceso a Internet, ya vimos que no lo tenía.

Por último, echaremos un vistazo a las propiedades de nuestra conexión Wifi con el inversor.

Figura 41: Propiedades de la conexión Wifi con el inversor

Vemos que la seguridad que se está utilizando es WPA2 Personal, que tiene varias debilidades. La primera es el uso de una única clave para acceder a la red, es decir no existe una clave diferente para cada usuario. La segunda radica en que WPA2 es un estándar de cifrado y autenticación bastante antigua, y ya se han reportado varios problemas de ciberseguridad por lo que actualmente se recomienda utilizar su sustituto WPA3.

Ahora ya estamos en disposición de ejecutar la aplicación NMAP para analizar en profundidad el equipo. Para ello ejecutaremos un escaneo intenso a todas las puertas TCP (de la 1 a la 65535), lo que nos llevara algún tiempo y generará tráfico que podría ser detectado si el equipo dispusiese de un detector de intrusión, lo cual es prácticamente imposible en una instalación de autoconsumo, y habría que ver si lo tienen los grandes inversores, yo no lo he podido encontrar en ninguno.

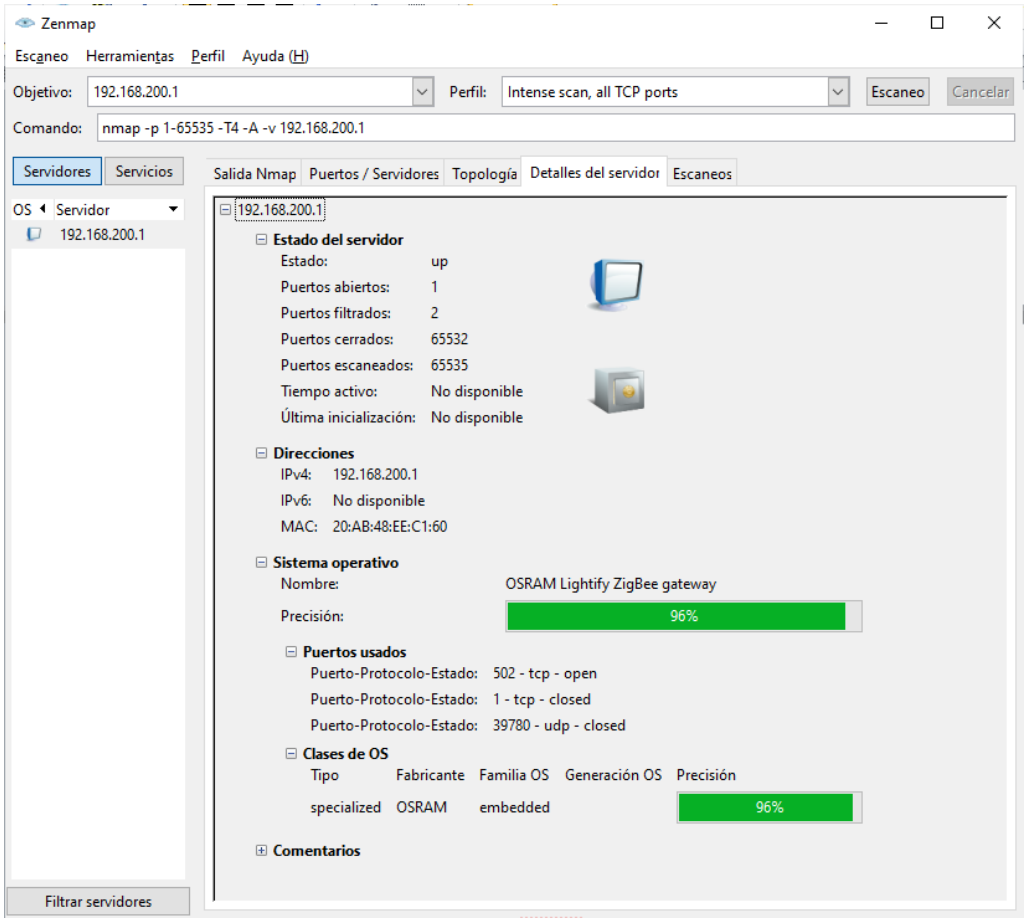


Figura 42: Datos obtenidos tras el análisis con namp

3.6.1.1 Conclusiones más importantes que sacamos de la realización de esta práctica:

El factor humano es uno de los escalones más débiles de la cadena de seguridad, en este caso probablemente por desconocimiento del instalador del equipo se ha dejado la password por defecto sin cambiar. Esto hace posible tener acceso al equipo y mediante la aplicación disponible en Internet para su configuración cambiar los parámetros de ajuste del mismo, ponerlo fuera de servicio o simplemente obtener datos de consumo y generación de la red de autoconsumo.

El resultado del análisis con NMAP nos indica que esta accesible la comunicación mediante el protocolo Modbus/TCP, que probablemente es el que utilice la aplicación de mantenimiento anteriormente comentada.

Por otra parte, el sistema operativo es una variante de un sistema UNIX, aunque el NMAP no nos lo confirma al 100% y seguramente será alguna modificación y adaptación del sistema operativo androide, ya que este fabricante (Huawei) es el que utilizaba en sus móviles. Un análisis más detallado con otro tipo de herramientas de reconocimiento de vulnerabilidades nos podría indicar que brechas de ciberseguridad podrían existir.

Lo más importante es lo fácil que ha resultado acceder al equipo, gracias a la nula protección del acceso Wifi. De esto se deduce que si utilizamos comunicaciones inalámbricas, como es el caso de Wifi deberemos auditar su seguridad correctamente, configurando bien los equipos desde el punto de vista de la ciberseguridad, y pasando herramientas de reconocimiento de vulnerabilidades cada cierto tiempo para detectar posibles brechas que pudieran usar los potenciales hackers para tener acceso a nuestra instalación.

Por último, la idea de dejar un acceso abierto para la instalación y mantenimiento del equipo es una mala práctica, ya que nadie cambia la password por razones obvias de cómo se gestionan, es más fácil dejar la de por defecto, lo cual es un agujero de entrada al equipo enorme.

3.6.2 PRÁCTICA 2: RECONOCIMIENTO AVANZADO (INVISIBLE) A TRAVÉS DE INTERNET PARA LOCALIZAR EQUIPOS DE SISTEMAS INDUSTRIALES Y VULNERABILIDADES CONOCIDAS

Se adjunta el link del vídeo de la práctica: https://youtu.be/u8L5aHrAFzo

Esta práctica tiene como objetivo la utilización de un buscador, no de enlaces a páginas web o documentos como Google, si no de equipos que están conectados a Internet.

Este buscador se llama Shodan y nos permite buscar y ver qué servicios están abiertos en dichos dispositivos, incluso las vulnerabilidades que están presentes. Lo más importante es

qué los usuarios que utilizan este buscador no necesitan realizar la conexión a dichos equipos, solo buscan en la gran base de información que tiene Shodan, al igual que hacemos en Google.

En la figura siguiente vemos la página de navegación de Shodan. Podemos comprobar que además de una entrada de búsqueda, según una serie de filtros y palabras que le indiquemos, dispone de cuatro categorías principales: Sistemas de Control Industrial, Bases de Datos, Infraestructuras de Red y Video Juegos. También nos muestra las etiquetas de búsqueda más utilizadas: cámaras web, cámaras, IPs, ftp, routers, etc.

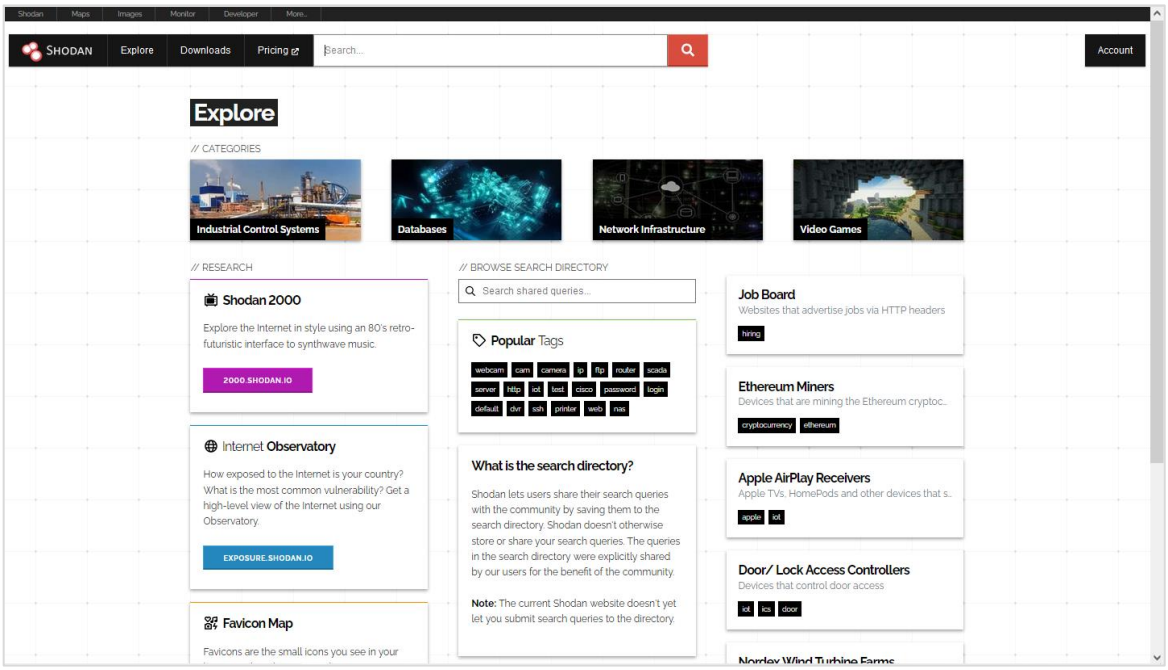


Figura 43: Página de búsqueda de Shodan

A Shodan tiene acceso cualquier persona, pero en su modalidad freeware, que tiene limitaciones muy importantes, existen otros tipos de subscripciones a este servicio mediante pagos mensuales que van desde 69 $ a 1099 $ al mes, todas ellas con diferentes capacidades y limitaciones.

En nuestro caso vamos a acceder a la página de entrada de Sistemas de Control Industrial, páginas que podemos ver en la imagen siguiente.

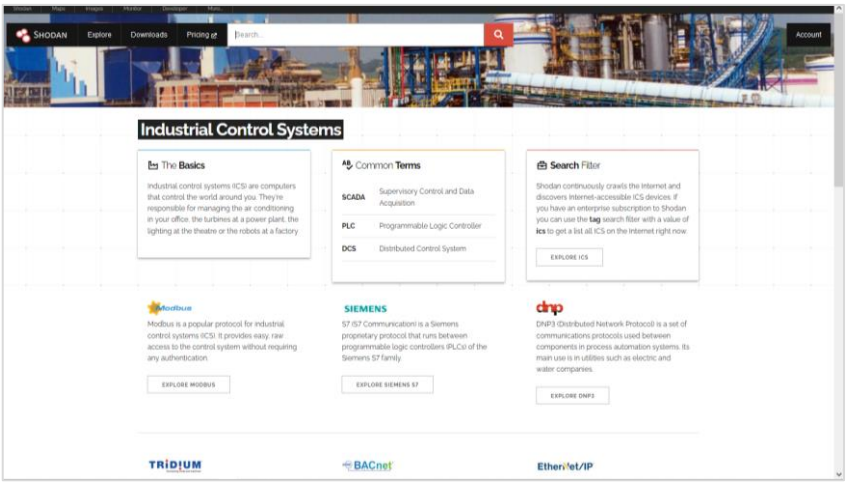


Figura 44: Página de búsqueda de sistemas de control industrial

Vemos que podemos buscar sistemas SCADA, PLCs, DCSs y fabricantes y protocolos utilizados comúnmente en este entorno: Modbus TCP, IEC 104 y un largo etc. Para ver que nos ofrece Shodan pinchamos en el protocolo IEC 104, del cual se ha hablado en este TGF. Los resultados se pueden ver en la imagen siguiente.

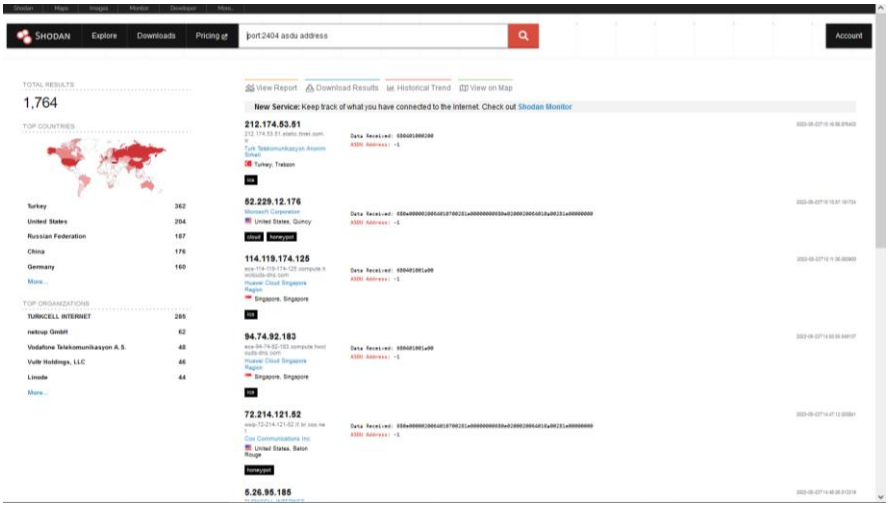


Figura 45: Resultados de la búsqueda del protocolo IEC 104

Casi dos mil dispositivos que a fecha de la realización de este documento aparecen en la base de datos de Shodan, este número varia día a día en función de lo que el motor de búsqueda de Shodan van encontrando.

Observamos que los resultados se ordenan por países, organizaciones y otros criterios que dependerán de cada tipo de equipo que estamos buscando. Si pinchamos en cualquiera de ellos, vemos los datos que nos resultan interesantes: Puertos abiertos (servicios), que han respondido a las consultas que ha hecho Shodan. En este ejemplo el puerto 443 TCP (que corresponde al servicio https), el 500 UDP (que corresponde al intercambio de claves IKE de una VPN, concretamente basada en IPsec) y la 2404 TCP (que corresponde al tráfico IEC 104).

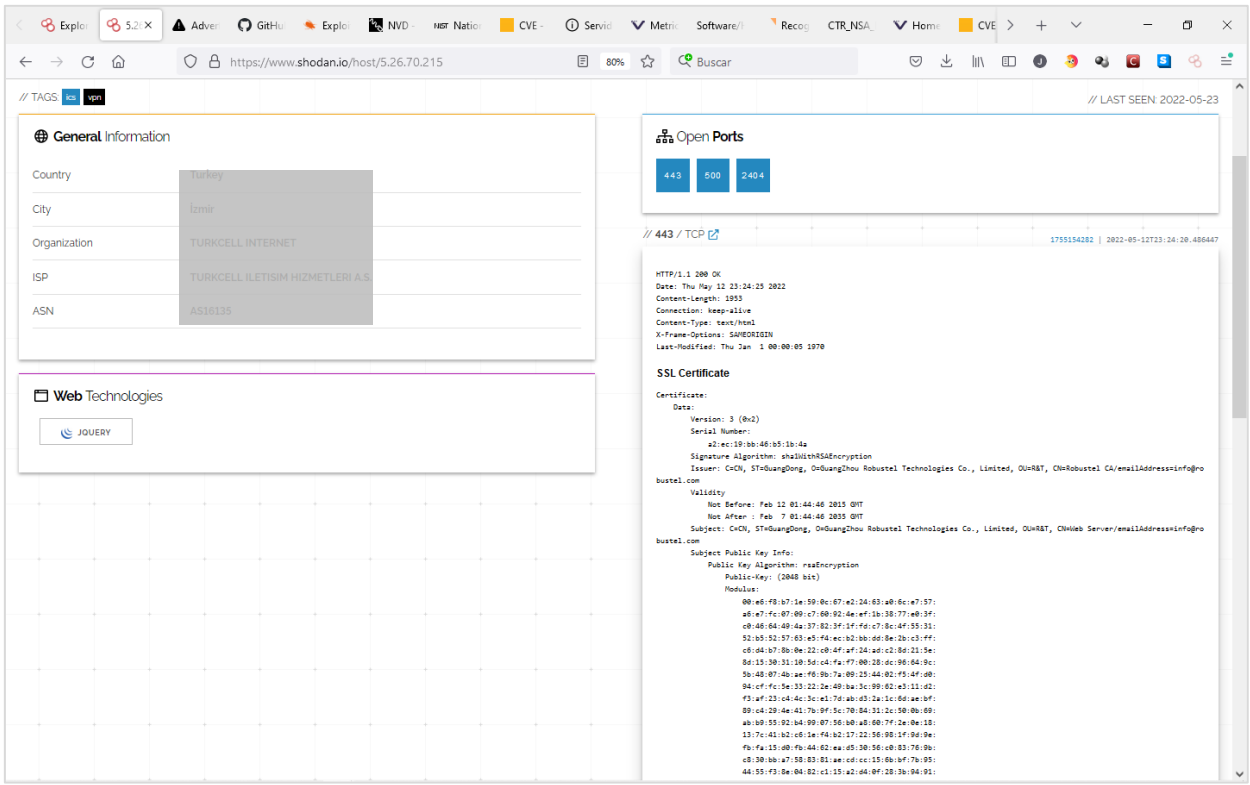


Figura 46: Detalles de un equipo buscado por el protocolo IEC 104

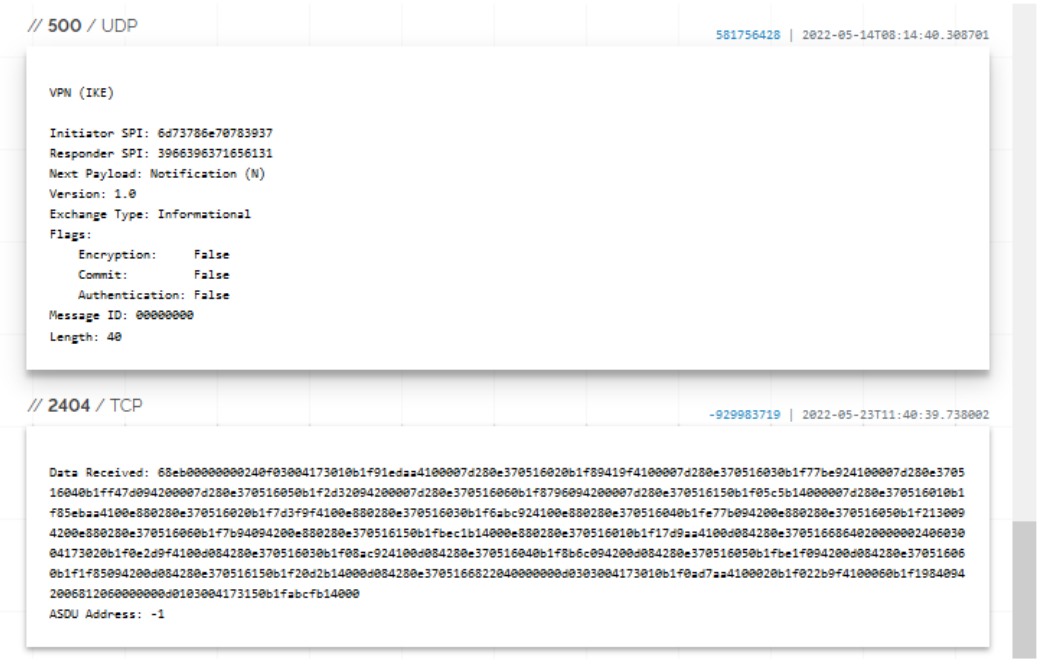


Figura 47: Detalles de la VPN y datos IEC 104 respondidos por el equipo

Lo más increíble es que no hemos tenido que hacer nada, ya sabemos dónde está localizado dicho equipo, que servicios están abiertos y disponibles y de qué tipo de comunicaciones dispone este equipo, del cual naturalmente nos da su IP, proveedor de Internet al que se conecta, etc.

En decir, la fase de reconocimiento, que en la primera práctica teníamos que hacer accediendo físicamente al equipo (inversor de una instalación de autoconsumo), está casi hecha sin que el propietario de dicho equipo haya detectado nuestra presencia.

Si buscamos por una palabra, por ejemplo, SCADA, nos aparece una primera página de resultados y si analizamos el tipo de productos (TOP PRODUCTS) vemos que existen 72 equipos que tienen la posibilidad de utilizar RDP (Remote Desktop Protocol).

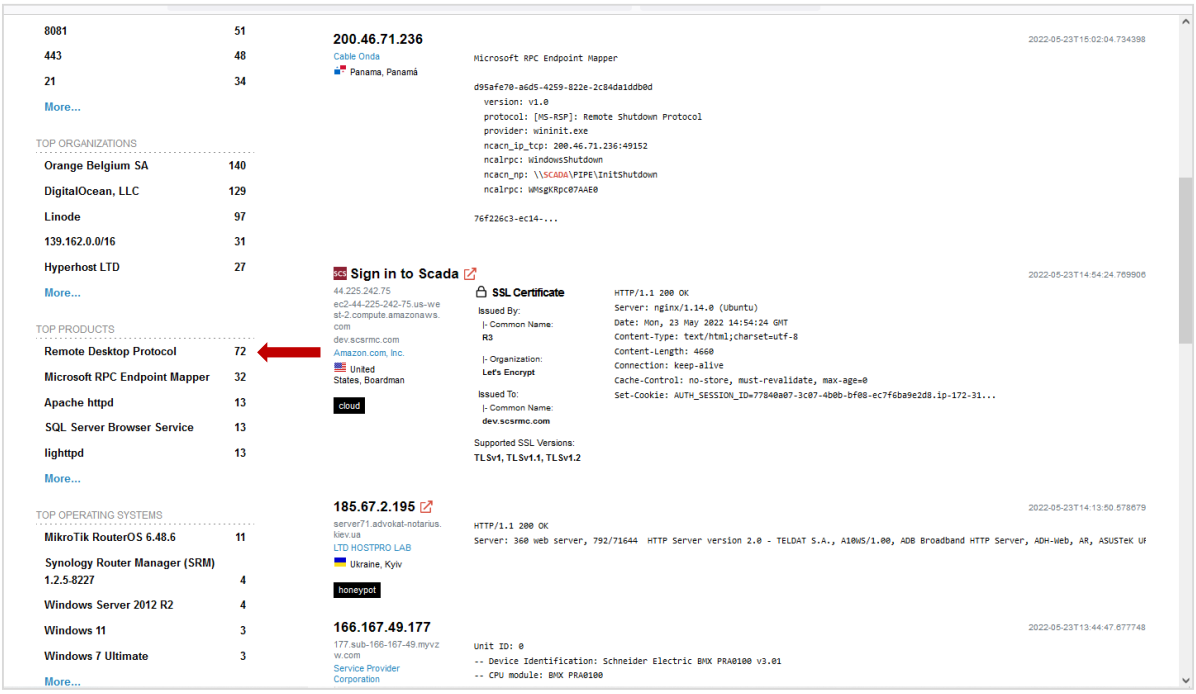


Figura 48: Resultados de búsqueda por la palabra SCADA

Por si esto fuera poco, Shodan nos facilita mucha más información de lo que encuentra, por ejemplo, la ventana de entrada al servicio si esta existiera, en dicha ventana puede aparecer información del sistema operativo, otros usuarios configurados, etc. Todo ello en función del servicio encontrado. En nuestro ejemplo, veríamos lo siguiente:

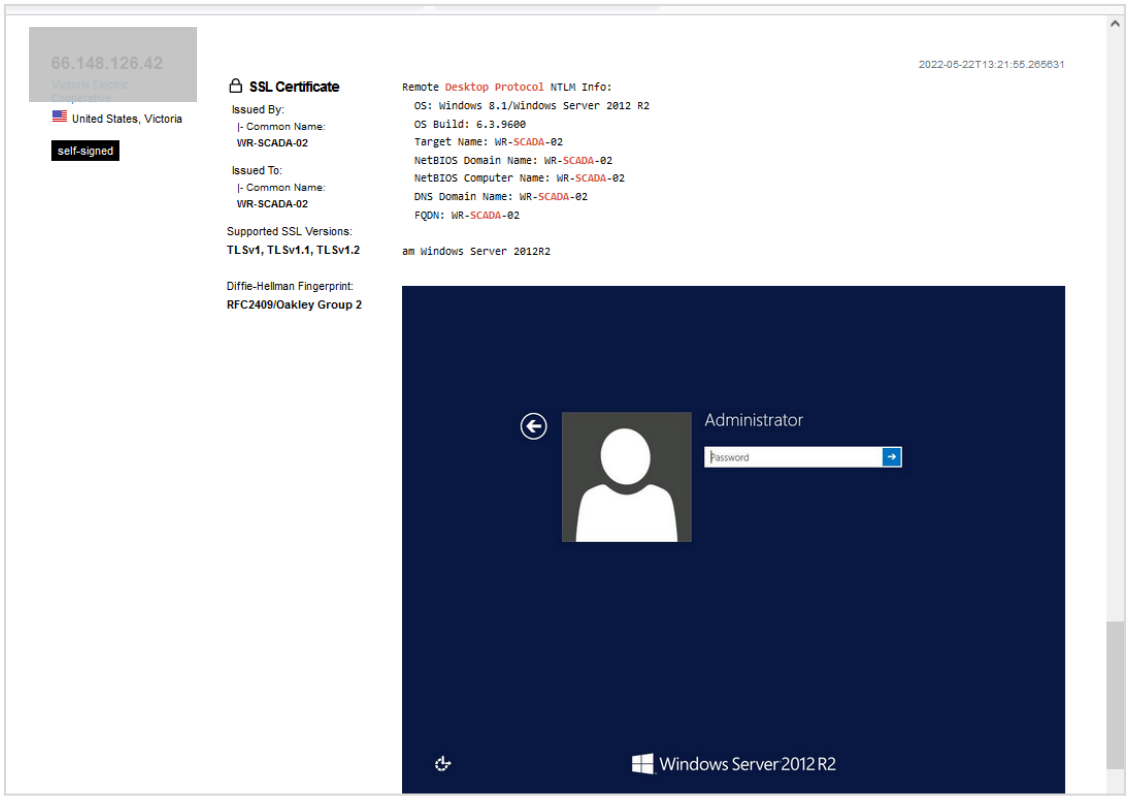


Figura 49: Detalles de un equipo con SCADA

Este equipo es un servidor Windows Server 2012R2, solo tiene configurado un usuario cuyo nombre es Administrator, soporta las versiones SSL 1, 1.1 y 1.2 para el acceso cifrado y utiliza el mecanismo criptográfico de Diffie-Hellman Grupo 2. Un usuario sin formación avanzada no dispone de conocimientos necesarios para comprender totalmente estos conceptos, pero ha resultado muy fácil obtenerlos. Sin embargo, a un hacker profesional le pueden resultar de gran utilidad.

Para acabar con esta búsqueda, me llamo poderosamente la atención en la Figura 48 encontrar tres equipos que estaban utilizando el sistema Windows 7 Ultimate. Sistema operativo fuera de servicio desde hace varios años, que seguramente tenga muchas vulnerabilidades y pueda ser atacado, sin mucha dificultad. Para corroborar mis suposiciones, veamos qué ocurre si analizamos este punto.

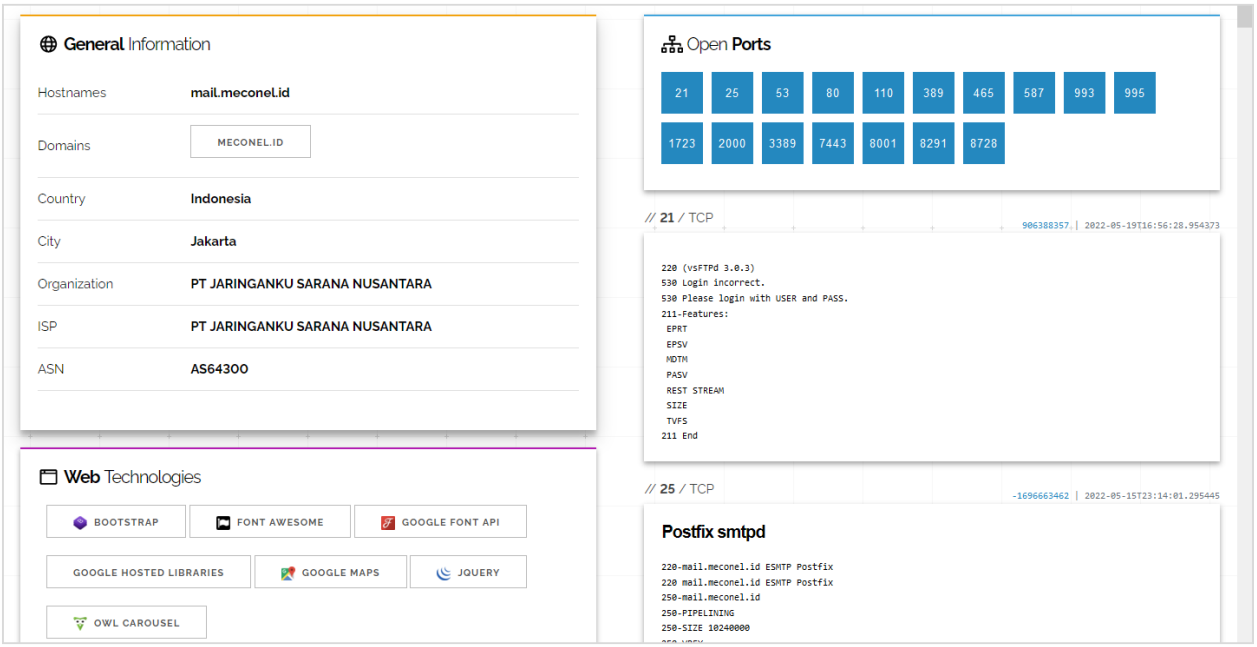
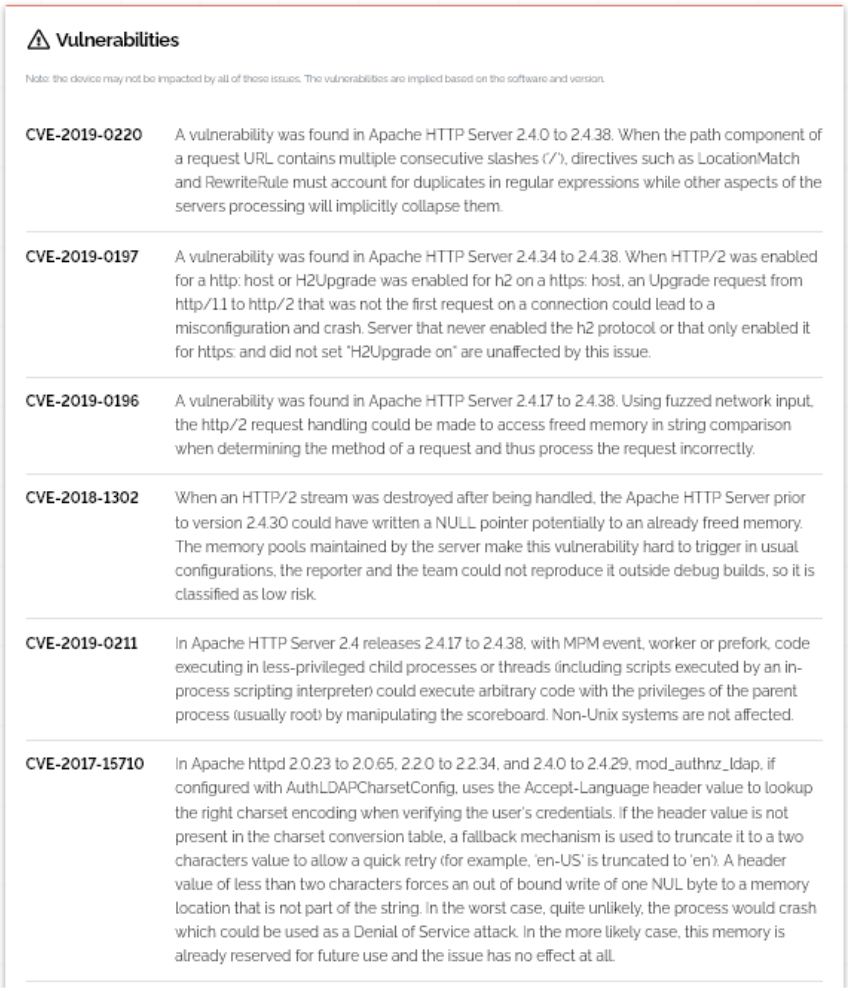


Figura 50: Detalles de un equipo SCADA con Windows 7 Ultimate

En este equipo, además de tener un elevado número de puertos abiertos, Shodan nos indica las vulnerabilidades conocidas para esta versión del sistema operativo. Como vemos, la lista es enorme, lo cual no quiere decir que todas las que aparecen necesariamente estén en el equipo, todo dependerá del nivel de parcheo que tenga instalado el ordenador.

Vemos que todas las vulnerabilidades tienen un código tipo CVE que significa “Common Vulnerability Exposure”, a continuación, el año en que se publicó dicha vulnerabilidad y por último un número serializado que todos los años se pone a cero.



Vulnerabilities

Note: the device may not be impacted by all of these issues. The vulnerabilities are implied based on the software and version.

CVE-2019-0220	A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.
CVE-2019-0197	A vulnerability was found in Apache HTTP Server 2.4.34 to 2.4.38. When HTTP/2 was enabled for a http: host or H2Upgrade was enabled for h2 on a https: host, an Upgrade request from http/1.1 to http/2 that was not the first request on a connection could lead to a misconfiguration and crash. Server that never enabled the h2 protocol or that only enabled it for https: and did not set "H2Upgrade on" are unaffected by this issue.
CVE-2019-0196	A vulnerability was found in Apache HTTP Server 2.4.17 to 2.4.38. Using fuzzed network input, the http/2 request handling could be made to access freed memory in string comparison when determining the method of a request and thus process the request incorrectly.
CVE-2018-1302	When an HTTP/2 stream was destroyed after being handled, the Apache HTTP Server prior to version 2.4.30 could have written a NULL pointer potentially to an already freed memory. The memory pools maintained by the server make this vulnerability hard to trigger in usual configurations, the reporter and the team could not reproduce it outside debug builds, so it is classified as low risk.
CVE-2019-0211	In Apache HTTP Server 2.4 releases 2.4.17 to 2.4.38, with MPM event, worker or prefork, code executing in less-privileged child processes or threads (including scripts executed by an in-process scripting interpreter) could execute arbitrary code with the privileges of the parent process (usually root) by manipulating the scoreboard. Non-Unix systems are not affected.
CVE-2017-15710	In Apache httpd 2.0.23 to 2.0.65, 2.2.0 to 2.2.34, and 2.4.0 to 2.4.29, mod_authnz_ldap, if configured with AuthLDAPCharsetConfig, uses the Accept-Language header value to lookup the right charset encoding when verifying the user's credentials. If the header value is not present in the charset conversion table, a fallback mechanism is used to truncate it to a two characters value to allow a quick retry (for example, 'en-US' is truncated to 'en'). A header value of less than two characters forces an out of bound write of one NUL byte to a memory location that is not part of the string. In the worst case, quite unlikely, the process would crash which could be used as a Denial of Service attack. In the more likely case, this memory is already reserved for future use and the issue has no effect at all.

Figura 51: Vulnerabilidades de un equipo SCADA con Windows 7 Ultimate

Las CVEs se encuentran disponibles, con acceso gratuito, en Internet. La organización que empezó esto fue Mitre, actualmente la base de datos de CVEs se mantiene en esta dirección web: https://www.cve.org/.

Las vulnerabilidades conocidas son actualmente más de 176.000, y el número no para de crecer. Cada vulnerabilidad contiene información detallada de la misma, así como enlaces a otros centros de información. Si buscamos más información de la primera vulnerabilidad (CVE-2019-0220) que nos aparecía en el SCADA con Windows 7 Ultimate en la web de mitre, obtendremos una lista de enlace donde existe datos adicionales, descripción de la amenaza, etc.

CVE-ID

CVE-2019-0220 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

A vulnerability was found in Apache HTTP Server 2.4.0 to 2.4.38. When the path component of a request URL contains multiple consecutive slashes ('/'), directives such as LocationMatch and RewriteRule must account for duplicates in regular expressions while other aspects of the servers processing will implicitly collapse them.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:107670
- URL:http://www.securityfocus.com/bid/107670
- BUGTRAQ:20190403 [SECURITY] [DSA 4422-1] apache2 security update
- URL:https://seclists.org/bugtraq/2019/Apr/5
- CONFIRM:https://httpd.apache.org/security/vulnerabilities_24.html
- URL:https://httpd.apache.org/security/vulnerabilities_24.html
- CONFIRM:https://security.netapp.com/advisory/ntap-20190625-0007/
- URL:https://security.netapp.com/advisory/ntap-20190625-0007/
- CONFIRM:https://support.f5.com/csp/article/K44591505
- URL:https://support.f5.com/csp/article/K44591505
- CONFIRM:https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03950en_us
- URL:https://support.hpe.com/hpsc/doc/public/display?docLocale=en_US&docId=emr_na-hpesbux03950en_us
- DEBIAN:DSA-4422
- URL:https://www.debian.org/security/2019/dsa-4422
- FEDORA:FEDORA-2019-119b14075a
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/EZRMTEIGZKYFNGIDOTXN3GNEJTLVCYU7/
- FEDORA:FEDORA-2019-a4ed7400f4
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/ALIRSS3O7NRHEGFMIDMUSYQIZOE4TJJN/
- FEDORA:FEDORA-2019-cf7695b470
- URL:https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/WETXNQWNQLWHV6XNW6YTO5UGDTIWAQGT/
- MISC:https://www.oracle.com/security-alerts/cpuapr2020.html
- URL:https://www.oracle.com/security-alerts/cpuapr2020.html
- MISC:https://www.oracle.com/security-alerts/cpujul2020.html
- URL:https://www.oracle.com/security-alerts/cpujul2020.html
- MISC:https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
- URL:https://www.oracle.com/technetwork/security-advisory/cpujul2019-5072835.html
- MISC:https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
- URL:https://www.oracle.com/technetwork/security-advisory/cpuoct2019-5072832.html
- MLIST:[debian-lts-announce] 20190403 [SECURITY] [DLA 1748-1] apache2 security update
- URL:https://lists.debian.org/debian-lts-announce/2019/04/msg00008.html
- MLIST:[httpd-bugs] 20200325 [Bug 63437] MergeSlashes option breaks protocol specifier in URIs
- URL:https://lists.apache.org/thread.html/r31f46d1f16ffcafa68058596b21f6eaf6d352290e522690a1cdccdd7@%3Cbugs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20190815 svn commit: r1048742 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
- URL:https://lists.apache.org/thread.html/84a3714f0878781f6ed84473d1a503d2cc382277e10045020923183O@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20190815 svn commit: r1048743 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
- URL:https://lists.apache.org/thread.html/56c2e7cc9deb1c12a843d0dc251ea7fd3e7e80293cde02fcd65286ba@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20200401 svn commit: r1058586 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
- URL:https://lists.apache.org/thread.html/rd18c3c43602e66f9cdcf09f1de233804975b9572b0456cc582390b6f@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20200401 svn commit: r1058587 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/vulnerabilities-httpd.xml security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
- URL:https://lists.apache.org/thread.html/re3d27b6250aa8548b8845d314bb8a350b3df326cacbbfdfe4d455234@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210330 svn commit: r1073139 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
- URL:https://lists.apache.org/thread.html/rf6449464fd8b7437704c55f88361b66f12d5b5f90bcce66af4be4ba9@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210330 svn commit: r1073139 [12/13] - in /websites/staging/httpd/trunk/content: ./ security/json/
- URL:https://lists.apache.org/thread.html/r03ee478b3dda3e381fd6189366fa7af97c980d2f602846eef935277d@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210330 svn commit: r1073140 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/cvejsontohtml.py security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
- URL:https://lists.apache.org/thread.html/rc998b18880df98bafaade071346690c2bc1444adaa1a1ea464b93f0a@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210330 svn commit: r1073143 [3/3] - in /websites/staging/httpd/trunk/content: ./ security/
- URL:https://lists.apache.org/thread.html/r06f0d87ebb6d59ed8379633f36f72f5b1f79cadfda72ede0830b42cf@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210330 svn commit: r1073149 [1/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/
- URL:https://lists.apache.org/thread.html/r9f93cf6dde308d42a9c807784e8102600d0397f5f834890708bf6920@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210330 svn commit: r1073149 [12/13] - in /websites/staging/httpd/trunk/content: ./ security/ security/json/
- URL:https://lists.apache.org/thread.html/re473305a65b4db888e3556e4dae10c2a04ee89dcff2e26ecdbd860a9@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210330 svn commit: r1888194 [12/13] - /httpd/site/trunk/content/security/json/
- URL:https://lists.apache.org/thread.html/rd2fb621142e7fa187cfe12d7137bf66e7234abcbbcd800074c84a538@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210603 svn commit: r1075360 [3/3] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2021-31618.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
- URL:https://lists.apache.org/thread.html/rd336919f655b7ff309385e34a143e41c503e133da80414485b3abcc9@%3Ccvs.httpd.apache.org%3E
- MLIST:[httpd-cvs] 20210606 svn commit: r1075470 [4/4] - in /websites/staging/httpd/trunk/content: ./ security/json/CVE-2020-13938.json security/vulnerabilities_13.html security/vulnerabilities_20.html security/vulnerabilities_22.html security/vulnerabilities_24.html
- URL:https://lists.apache.org/thread.html/r76142b8c5119df2178be7c2dba88fde552eedeec37ea993dfce68d1d@%3Ccvs.httpd.apache.org%3E
- MLIST:[oss-security] 20190401 CVE-2019-0220: URL normalization inconsistencies
- URL:http://www.openwall.com/lists/oss-security/2019/04/02/6
- REDHAT:RHSA-2019:2343
- URL:https://access.redhat.com/errata/RHSA-2019:2343
- REDHAT:RHSA-2019:3436
- URL:https://access.redhat.com/errata/RHSA-2019:3436
- REDHAT:RHSA-2019:4126
- URL:https://access.redhat.com/errata/RHSA-2019:4126
- REDHAT:RHSA-2020:0250
- URL:https://access.redhat.com/errata/RHSA-2020:0250
- REDHAT:RHSA-2020:0251
- URL:https://access.redhat.com/errata/RHSA-2020:0251
- SUSE:openSUSE-SU-2019:1190
- URL:http://lists.opensuse.org/opensuse-security-announce/2019-04/msg00051.html
- SUSE:openSUSE-SU-2019:1209
- URL:http://lists.opensuse.org/opensuse-security-announce/2019-04/msg00061.html
- SUSE:openSUSE-SU-2019:1258
- URL:http://lists.opensuse.org/opensuse-security-announce/2019-04/msg00084.html
- UBUNTU:USN-3937-1
- URL:https://usn.ubuntu.com/3937-1/

Figura 52: Enlaces con información de la vulnerabilidad CVE-2019-0220 (www. https://www.cve.org)

Para encontrar realizar búsquedas selectivas, existen otras webs que utilizan esta información, para buscar vulnerabilidades por fabricantes, tipos de productos y otras muchas características. Por ejemplo, la web de cvedetails: https://www.cvedetails.com/

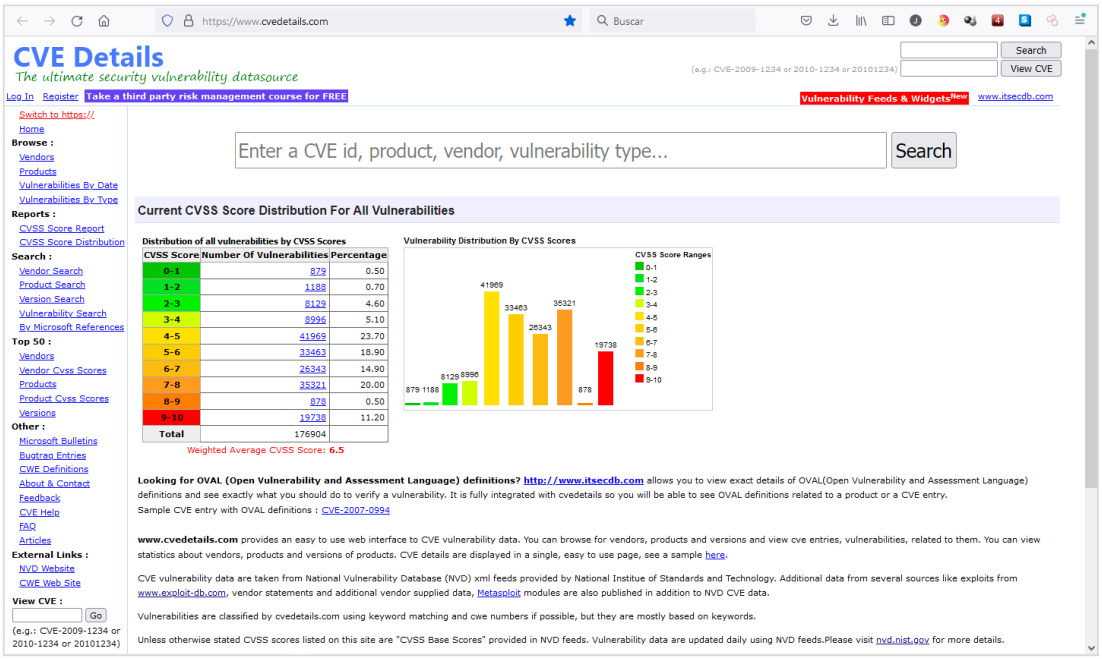


Figura 53: Web de cvedetalils

Otra web muy interesante en este aspecto es la del NIST (National Institute of Standards and Technology): https://nvd.nist.gov/

El NIST es una agencia nacional de EE. UU. cuya misión fundamental es promover la innovación, ciencia, estándares y tecnologías de ciberseguridad. En este caso las CVEs están clasificadas por diferentes tipos y características de las posibles amenazas. Con ello, el NIST tiene unas curvas de la evolución de cada tipo de amenazas, lo que nos permite analizar qué tipo de vulnerabilidades, según dicha clasificación, se atacan más, esto nos puede ayudar a saber dónde tendremos que priorizar los recursos de los que disponemos para asegurar nuestra instalación. En este caso las plantas de generación de energía solar fotovoltaica.

En la figura siguiente vemos las diferentes curvas clasificadas por tipos de amenazas que ha definido el NIST, así como su evolución a lo largo de los años. Podemos apreciar, por

ejemplo, como el tipo CWE-79 definido como: *"neutralización incorrecta de la entrada durante la generación de la página web"*, sufre un fuerte incremento a partir del año 2016, estando actualmente en unas 2.200 amenazas nuevas de este tipo por año.

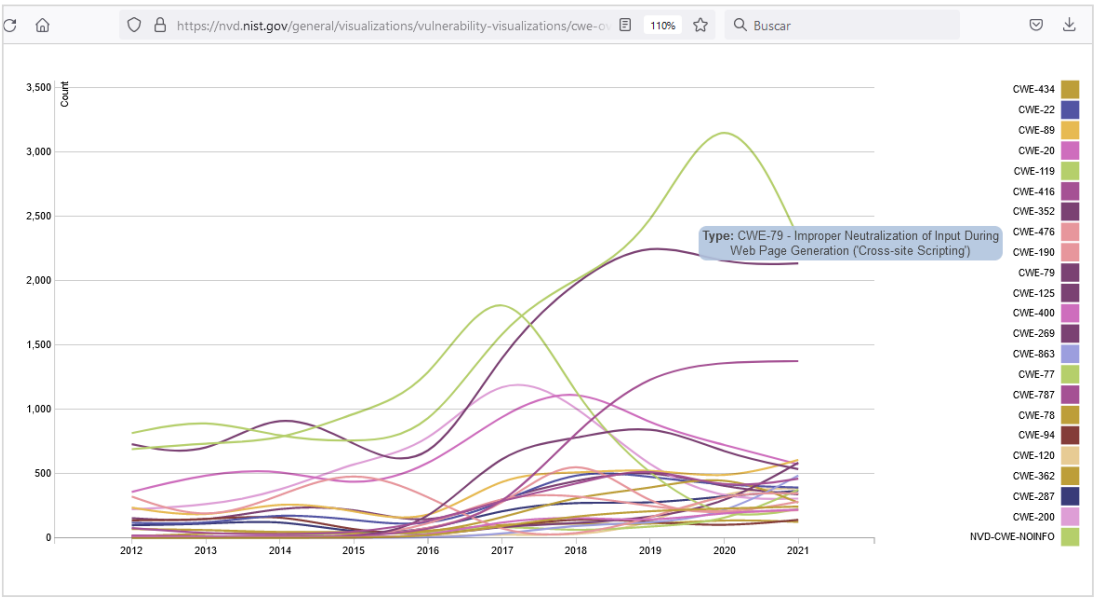


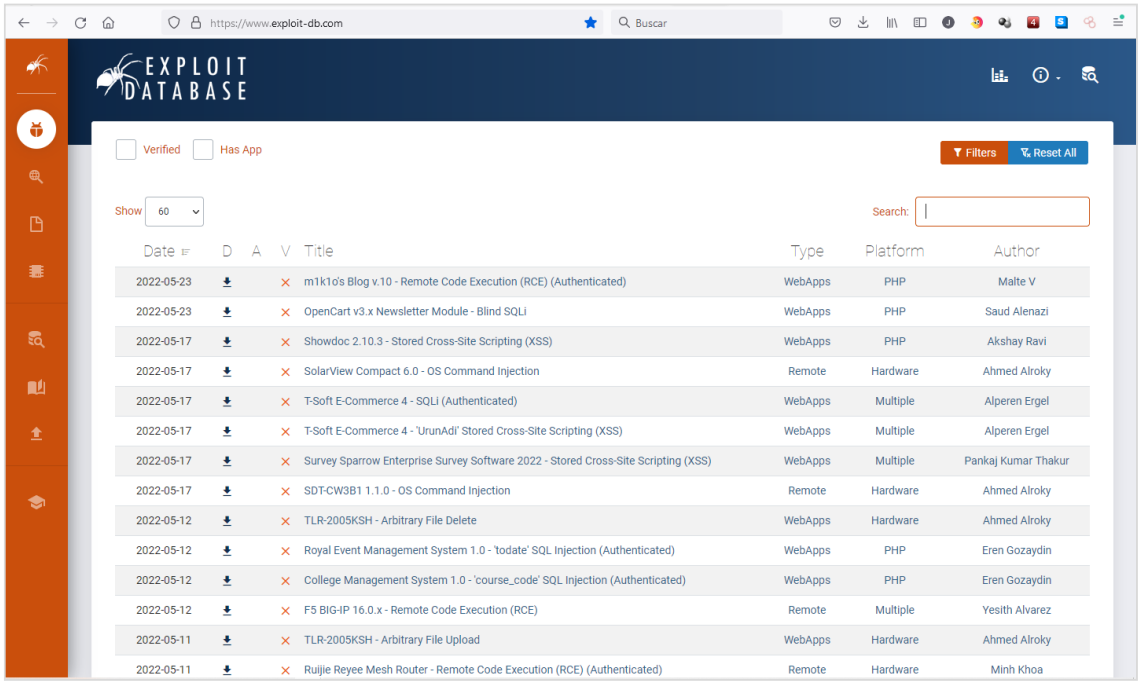
Figura 54: Tipos de amenazas y número de vulnerabilidades nuevas por tipo y año

(www. https://nvd.nist.gov)

Por último y como enlace con la práctica número 3, vamos a introducir la web donde se encuentra una base de datos de exploits mantenida por la empresa Offensive Security, una empresa de formación en ciberseguridad IT, así como de servicios de pruebas de penetración de alto nivel: https://www.exploit-db.com

Esta base de datos es compatible con las CVEs, es decir cada exploit tiene el mismo número CVE que la vulnerabilidad que vamos a atacar. La idea es que esto permita mejorar la capacitación de las personas que trabajan en ciberseguridad, pero como cualquier herramienta también tiene su lado oscuro ya que, como veremos en la practica 3, cualquier persona con unos pocos conocimientos puede utilizar esta información para lanzar ciberataques.

En la figura siguiente se ve una página de algunos de los exploits que mantiene la web de Offensive Security. A continuación, se observan detalles de uno de los exploits seleccionados (showdoc 2.10.3 – Stored Cross-Site Scripting) y las instrucciones detalladas para realizar este ciberataque. En concreto el cross-site scripting es un tipo de vulnerabilidad típico de las aplicaciones Web, puede permitir a una tercera persona inyectar en páginas web visitadas por el usuario código JavaScript o en otro lenguaje similar, el objetivo es el robo de información, el secuestro de sesiones de usuario comprometiendo la seguridad del navegador utilizado.



Date	D	A	V	Title	Type	Platform	Author
2022-05-23				m1k1o's Blog v.10 - Remote Code Execution (RCE) (Authenticated)	WebApps	PHP	Malte V
2022-05-23				OpenCart v3.x Newsletter Module - Blind SQLi	WebApps	PHP	Saud Alenazi
2022-05-17				Showdoc 2.10.3 - Stored Cross-Site Scripting (XSS)	WebApps	PHP	Akshay Ravi
2022-05-17				SolarView Compact 6.0 - OS Command Injection	Remote	Hardware	Ahmed Alroky
2022-05-17				T-Soft E-Commerce 4 - SQLi (Authenticated)	WebApps	Multiple	Alperen Ergel
2022-05-17				T-Soft E-Commerce 4 - 'UrunAdi' Stored Cross-Site Scripting (XSS)	WebApps	Multiple	Alperen Ergel
2022-05-17				Survey Sparrow Enterprise Survey Software 2022 - Stored Cross-Site Scripting (XSS)	WebApps	Multiple	Pankaj Kumar Thakur
2022-05-17				SDT-CW3B1 1.1.0 - OS Command Injection	Remote	Hardware	Ahmed Alroky
2022-05-12				TLR-2005KSH - Arbitrary File Delete	WebApps	Hardware	Ahmed Alroky
2022-05-12				Royal Event Management System 1.0 - 'todate' SQL Injection (Authenticated)	WebApps	PHP	Eren Gozaydin
2022-05-12				College Management System 1.0 - 'course_code' SQL Injection (Authenticated)	WebApps	PHP	Eren Gozaydin
2022-05-12				F5 BIG-IP 16.0.x - Remote Code Execution (RCE)	Remote	Multiple	Yesith Alvarez
2022-05-11				TLR-2005KSH - Arbitrary File Upload	WebApps	Hardware	Ahmed Alroky
2022-05-11				Ruijie Reyee Mesh Router - Remote Code Execution (RCE) (Authenticated)	Remote	Hardware	Minh Khoa

Figura 55: Lista de exploits mantenidos en la web (https://www.exploit-db.com)

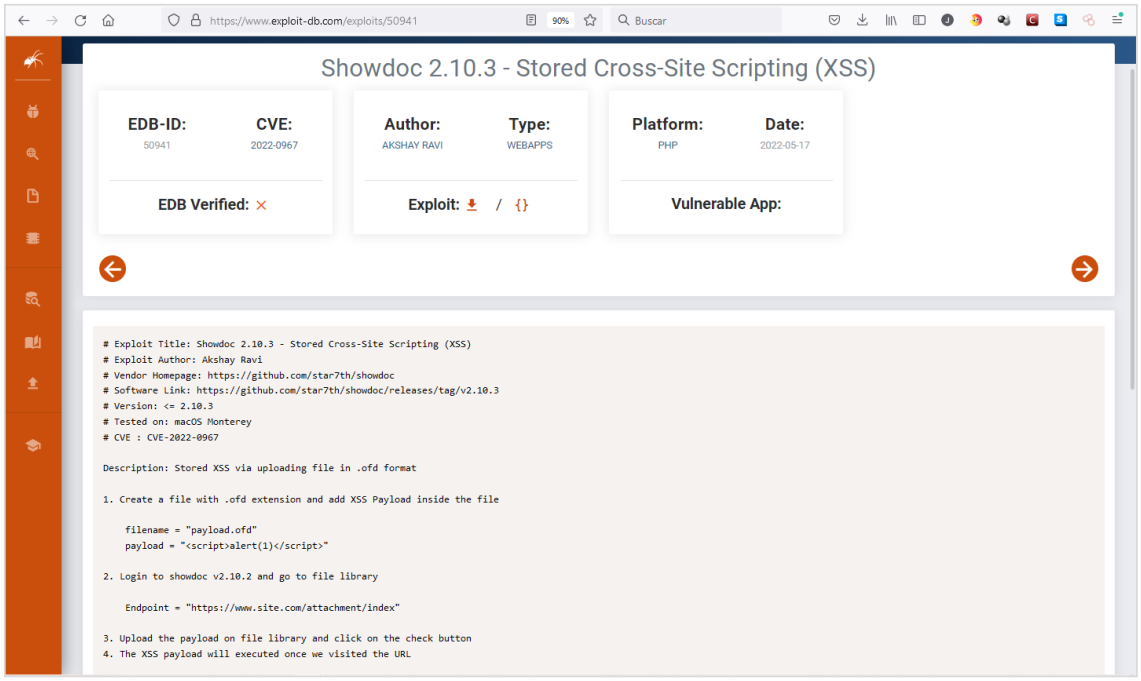


Figura 56: Detalle de uno de los exploits (https://www.exploit-db.com)

3.6.2.1 Conclusiones más importantes que sacamos de la realización de esta práctica:

Realizar análisis de reconocimiento es una de las primeras fases de un ciberataque. Los sistemas de escaneo de vulnerabilidades, como NMAP, son herramientas sencillas y muy útiles. Pero solo sirven para hacer un escaneo antes de que lo haga un hacker (con herramientas mucho mejores y sofisticadas) y así podamos intentar tapar los agujeros de ciberseguridad que encontremos. Existen herramientas y servicios comerciales que hacen esto de manera regular (análisis de vulnerabilidades), sobre todo en el mundo IT.

La cantidad de herramientas, centros de información, documentación sobre ciberamenazas y vídeos en YouTube que enseñan cómo realizar ciberataques, pueden ser una ayuda o un problema más. Precisamente en la práctica 3 vamos a ver cómo es posible utilizar herramientas que explotan, de forma automática miles de vulnerabilidades conocidas.

En esta práctica hemos comprobado lo sencillo que es hacer reconocimientos invisibles y sigilosos, que no alerten al posible atacado, lo que facilita la no detección o la detección

tardía de un ciberataque. Todo esto implica la necesidad de disponer de algún tipo de metodología o guía de buenas prácticas con puntos claros y sencillos que podamos incorporar en nuestra organización para mantener un buen nivel de ciberseguridad.

3.6.3 PRACTICA 3: ATAQUE CON LA HERRAMIENTA METASPLOIT A UN EQUIPO CON VULNERABILIDADES CONOCIDAS.

Se adjunta el link de la práctica: https://youtu.be/bacEb_dHgmI

La herramienta Metasploit es una de las más usadas en análisis de pentesting e intrusiones. Dispone de una versión gratuita, mantenida por la comunidad, con limitaciones en cuanto al número de "exploits" disponibles. Mientras que la versión comercial dispone de más de 44.000, la versión reducida nos permite aprender y conocer el uso de esta, con unos 2.200 "exploits".

Vamos a suponer que hemos realizado un reconocimiento de la instalación que queremos atacar y nos damos cuenta de que uno de los servidores, cuya dirección IP es 192.168.30.133, tiene "abierto" un servicio FTP (File Transfer Protocol), un protocolo de transferencia de ficheros.

En la figura siguiente se observa un intento de conexión fallida al servidor ftp, ya que se desconocenc el nombre de usuario y la password. Se ha probado la combinación root/root pero evidentemente no se ha conseguido acceder de forma efectiva.

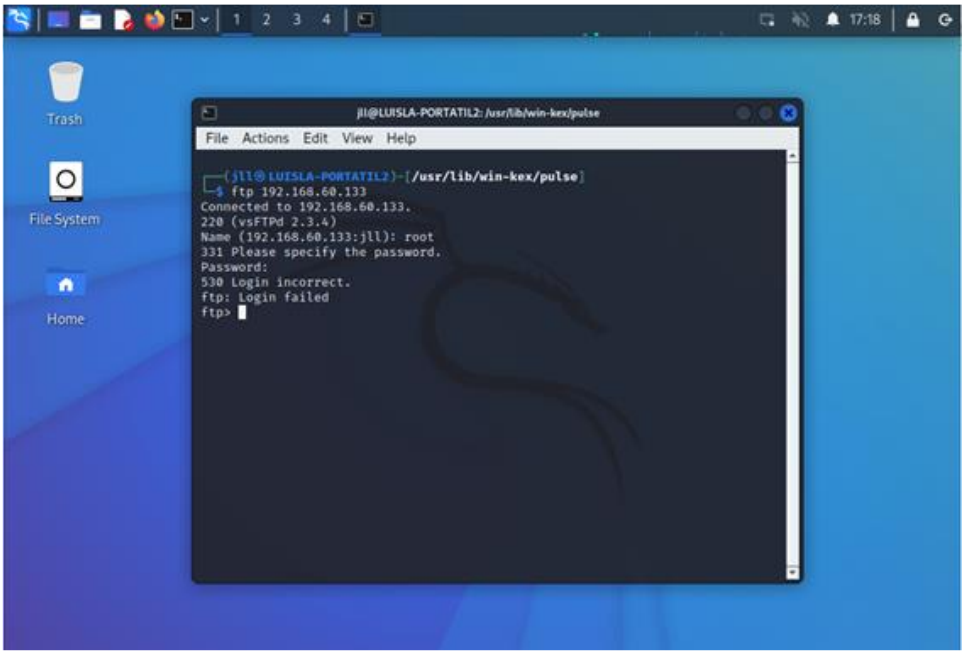


Figura 57: Intento de login fallido al servidor ftp

De primeras, llama la atención que el servidor envía en el proceso de bienvenida su banner (vsFTPd 2.3.4). Esto facilita un punto de ataque y es una brecha de ciberseguridad. Utilizando uno de los centros de información de vulnerabilidades, por ejemplo cvedetails, se buscará si existe alguna vulnerabilidad conocida de este servidor ftp.

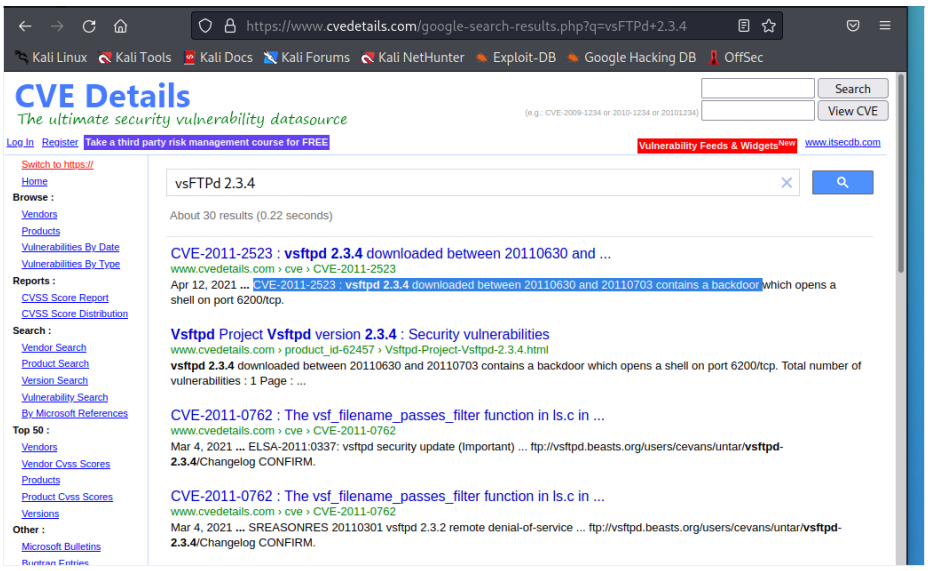


Figura 58: Vulnerabilidades relacionadas con el servidor FTP

Se detecta una vulnerabilidad muy peligrosa, ya que alguien programó en el servidor una puerta trasera que nos puede permitir el acceso al mismo, sin necesidad de autenticarnos. Pulsando en ese mismo enlace, cve details ofrece mucha más información sobre esta vulnerabilidad.

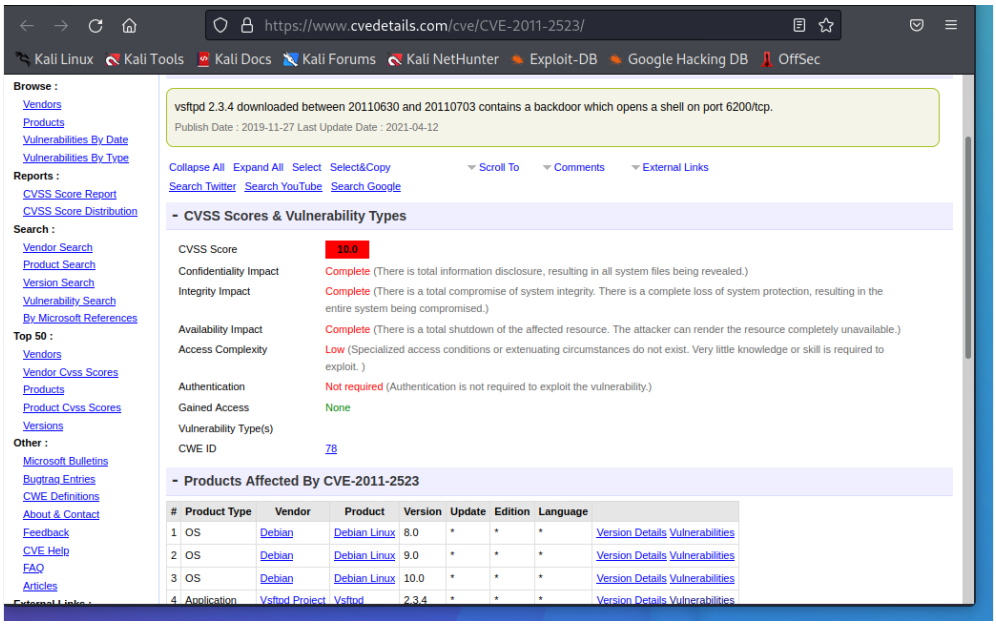


Figura 59: Información detallada de la vulnerabilidad

Se ha encontrado una vulnerabilidad severa (nota =10), que precisa bajos conocimientos para su explotación y su ejecución permitiría tomar el control total y absoluto del equipo donde reside el servidor (192.168.60.133).

Ahora tenemos que comprobar si existe un exploit ya programado para lanzar un ataque contra el servidor, o en su caso recopilar más información técnica que permita programar el exploit. Para ello, se utilizará una web que ofrece una base de datos de distintos exploits www.exploit-db.com.

Se busca por el nombre de la vulnerabilidad encontrada y como se ve en la siguiente imagen existen dos disponibles. Nos interesa el que se puede utilizar en Metasploit.

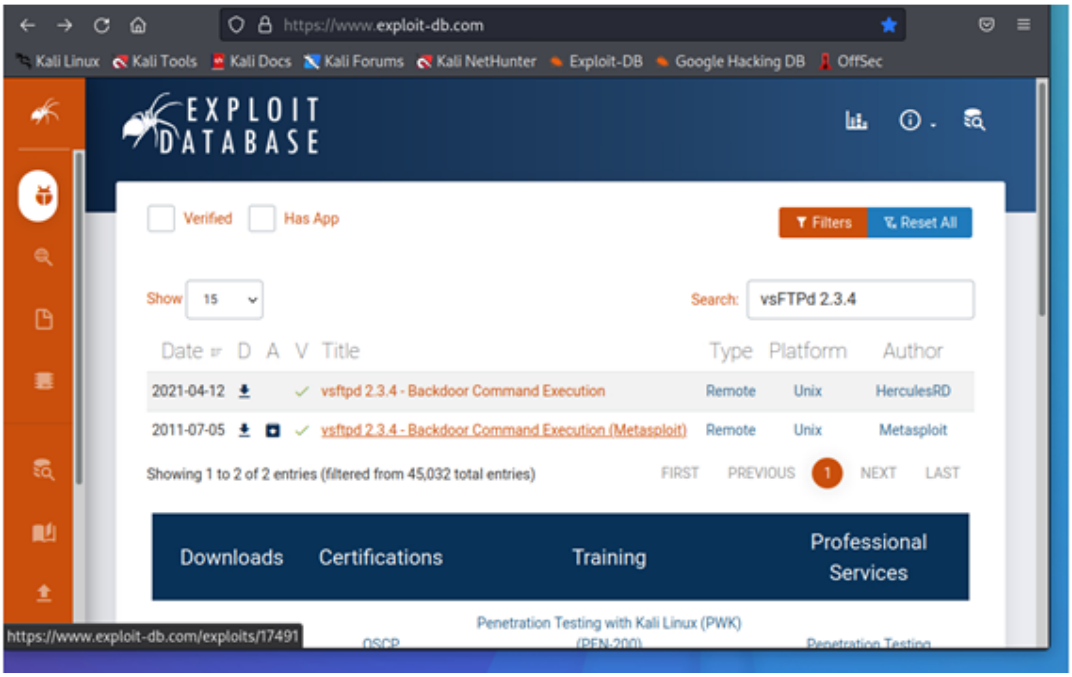


Figura 60: Distintos exploits de la vulnerabilidad que nos ofrece la web

Pulsando en la vulnerabilidad, se obtiene el código del programa que va a permitir entrar en el servidor, ver imagen siguiente.

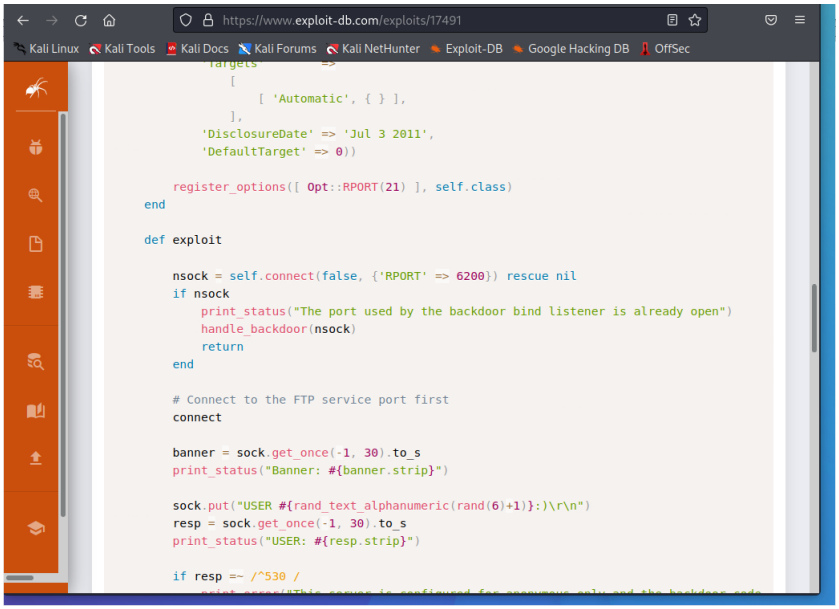


Figura 61: Código de programación del exploit a utilizar

Ya solo queda lanzar la aplicación Metasploit, buscar el exploit y ejecutarlo contra la maquina objetivo. Para ello vamos a utilizar Kali, que además de Metasploit dispone de centenares de aplicaciones de hacking. Kali es una distribución basada en Unix que compila las mejores herramientas de análisis, reconocimiento, testing, etc.

En la siguiente imagen se muestra como ejecutar Metasploit desde Kali.

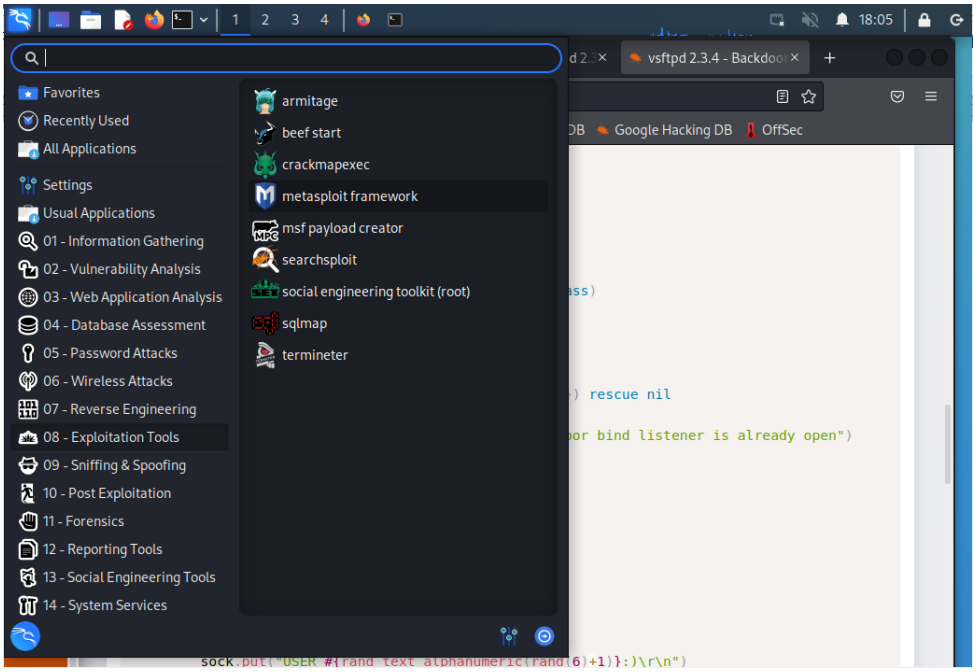


Figura 62: Pantalla de ejecución de Metaesploit desde Kali Linux

Una vez abierto Metasploit, se busca la vulnerabilidad de vsFTPd 2.3.4, utilizando el comando “search”.

A continuación, aparece la información del exploit y cómo se debe utilizar. En nuestro caso el exploit está localizado en la siguiente ruta de directorios: exploit/unix/ftp/vsftpd_234_backdoor y para lanzarlo hay que usar el comando “use” y a continuación su localización en el equipo que está ejecutando Metasploit.

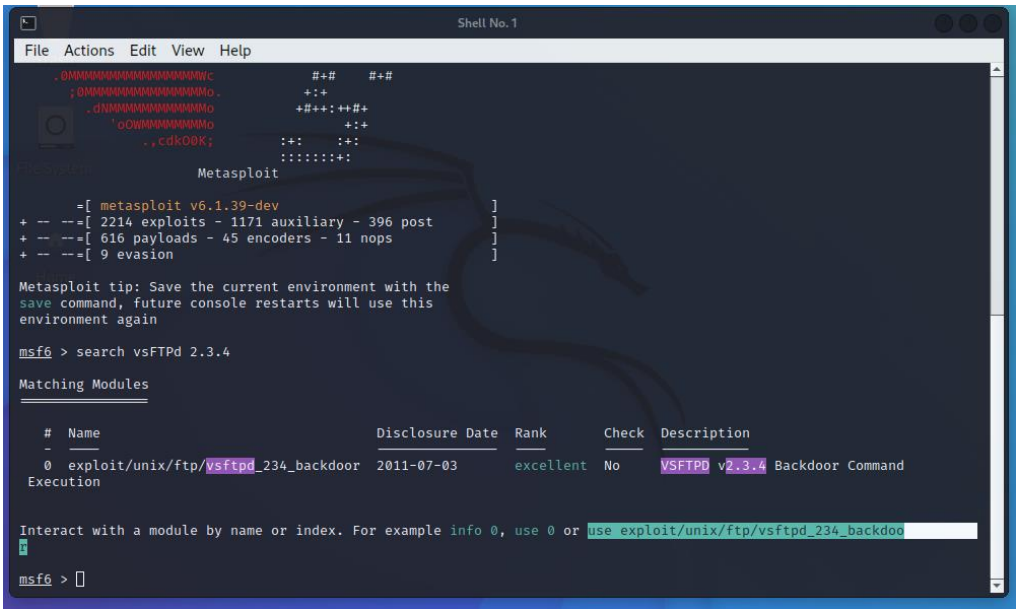


Figura 63: Información del exploit que se va a utilizar

Lo lanzamos y vemos las posibles opciones de ejecución. Como se ve en la siguiente imagen, Metasploit ofrece dos posibilidades, a través del RHOSTS o del RPORT puerto 21

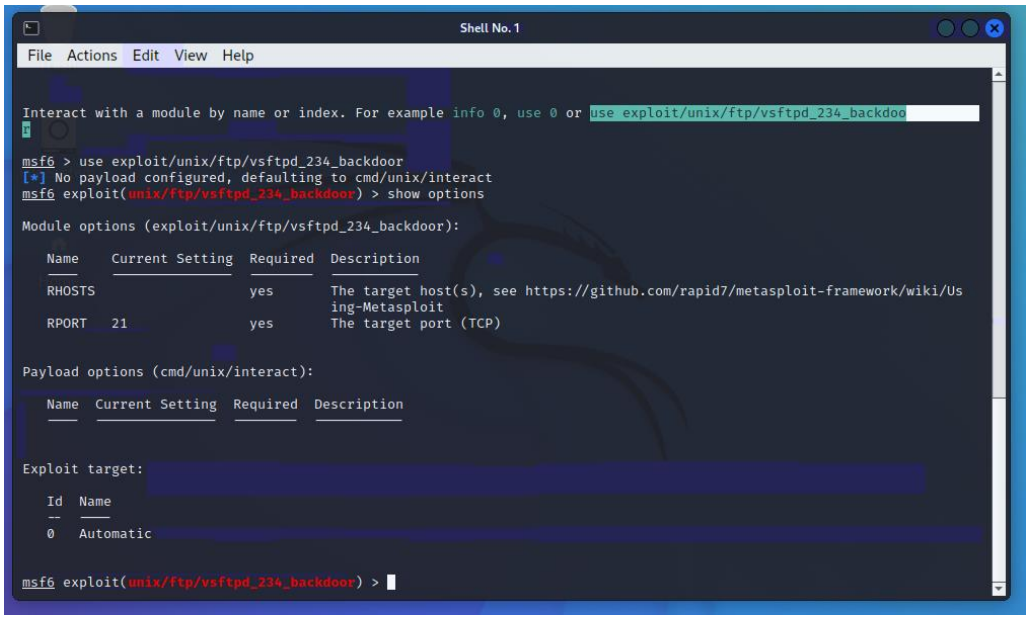


Figura 64: Posibilidades de ejecución del exploit que ofrece Metaesploit

Ejecutamos el comando "set RHOSTS" con la dirección IP de la víctima y ya estamos dentro. Hemos accedido a través de la puerta trasera. Por último, comprobamos que tenemos acceso a todos los directorios del equipo y que hemos entrado con el usuario root, usuario que es administrador del equipo.

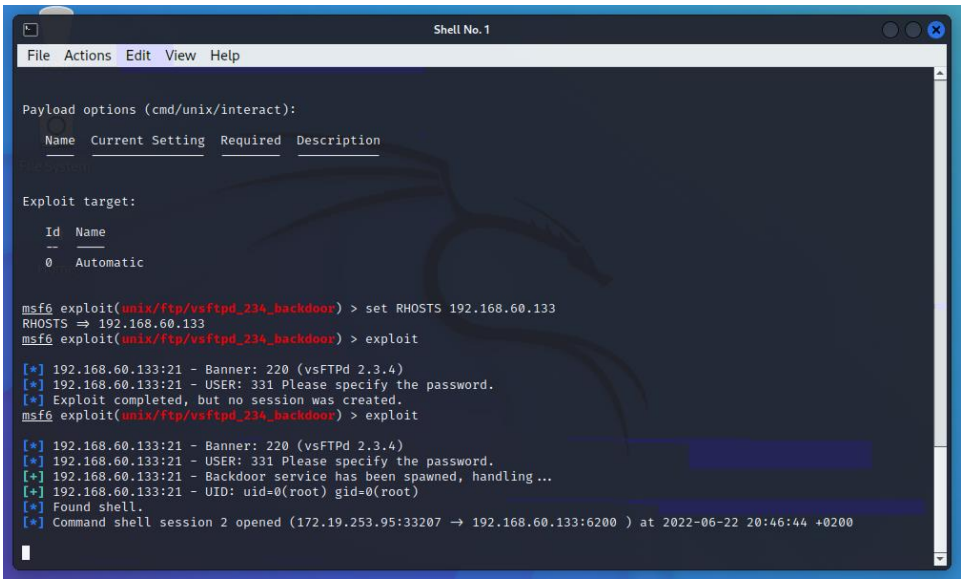


Figura 65: Ejecución del exploit y acceso al servidor

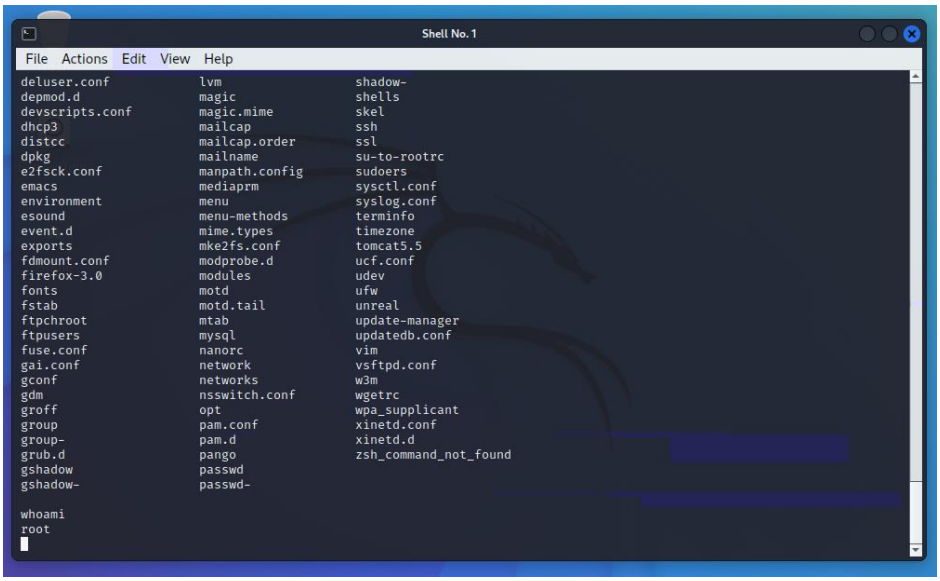


Figura 66: Comprobación que tenemos acceso cómo usuario root

3.6.3.1 Conclusiones más importantes que sacamos de la realización de esta práctica.

En esta práctica, se ha demostrado que dejar servicios abiertos, si no se utilizan, puede ser muy peligroso. Otro procedimiento muy importante en la ciberseguridad es comprobar las vulnerabilidades conocidas que pueden tener los equipos y en su caso parchearlas, Si un parche no fuera posible y la vulnerabilidad fuese crítica abría que sustituir el equipo, la aplicación o el sistema operativo.

Por último, se ha podido ver en acción una pequeña demostración de cómo opera Metaesploit, lo potente y fácil que resulta de utilizar y los graves daños que puede provocar no realizar un escaneo de vulnerabilidades antes de que lo haga un hacker.

Capítulo 4. ESTADO DE LA CUESTIÓN

4.1 MARCO DE TRABAJO DE CIBERSEGURIDAD DEL NIST (NIST CYBERSECURITY FRAMEWORK)

La ciberseguridad afecta de manera capital a las infraestructuras críticas de todos los países. Por ello, para poder mejorar todos los aspectos relativos a la ciberseguridad es necesario disponer de unas guías y de una metodología a seguir.

Si analizamos el estado del arte en este tema, no cabe duda de que una de las iniciativas para lograr esto la lidera el NIST (National Institute of Standards and Technology) de Estados Unidos, que desde el año 2013 impulsa un proyecto colaborativo para desarrollar un marco de trabajo de ciberseguridad que va evolucionando y está orientado a la reducción de riesgos. [14]

Este proyecto ha dado como resultado de unas guías de implementación, control y gestión de la ciberseguridad que contienen las mejores prácticas y estándares de la industria.

Los objetivos principales del marco de trabajo de ciberseguridad del NIST son:

- ✓ Identificar estándares de seguridad aplicables a las diferentes infraestructuras críticas
- ✓ No introducir nuevos estándares cuando ya existan otros que cubran los objetivos planteados
- ✓ Desarrollar guías para aplicar correctamente medidas de ciberseguridad
- ✓ Ayudar a los responsables y operadores de infraestructuras críticas a identificar, inventariar y gestionar riesgos informáticos
- ✓ Establecer criterios para la definición de métricas que permitan el control de la ciberseguridad en su implementación
- ✓ Establecer un lenguaje común para gestionar riesgos de ciberseguridad
- ✓ Identificar áreas de mejora que permitan ser gestionadas a través de colaboraciones futuras con sectores particulares y organizaciones para el desarrollo de estándares

El marco de trabajo, denominado CFS (Cibersecurity Framework Standard) [15], está dividido en tres áreas:

- ✓ Marco básico (Framework Core)
- ✓ Niveles de implementación del marco (Framework Implementation Tiers)
- ✓ Perfiles del marco básico (Framework Profiles)

4.1.1 MARCO BÁSICO

Está formado por el conjunto de actividades en favor de la ciberseguridad, los resultados esperados y las referencias aplicables que son comunes a las diferentes infraestructuras, mediante estándares, directrices y buenas prácticas.

Todo ello con el objetivo de permitir la comunicación de actividades de ciberseguridad y sus resultados a todos los niveles de la organización, es decir, desde el nivel ejecutivo hasta el nivel técnico de implementación y operaciones. Para ello, emplea cinco funciones fundamentales de ciberseguridad:

1. **Identificar**: Permite comprender de forma general en una infraestructura la gestión y el riesgo de ciberseguridad de los sistemas, las personas, los activos, los datos y sus capacidades.
   Por ejemplo:
   - Identificar los equipos físicos y el software para establecer un programa de gestión de activos.
   - Identificar políticas de ciberseguridad para definir un programa de gobernanza en la organización.
   - Identificación de una estrategia de gestión de riesgos para la organización

2. **Proteger:** Permite desarrollar e introducir las soluciones necesarias para limitar o la repercusión de una brecha de ciberseguridad que puede llegar a ocurrir en la infraestructura.
   Por ejemplo:
   - Formación del personal de la organización soba las bases de ciberseguridad.
   - Administrar la tecnología de defensa para aumentar la robustez de los sistemas.

- Establecer una seguridad de los datos que maneja la infraestructura para proteger su confidencialidad, integridad y disponibilidad.

3. **Detectar**: La función de detección define las actividades apropiadas para identificar una brecha de ciberseguridad de forma eficaz.
   Por ejemplo:
   - Implementar elementos de monitorización continua de la seguridad para identificar posibles fisuras + de ciberseguridad.
   - Verificar el correcto funcionamiento de las medidas de protección.

4. **Responder:** Permite reaccionar ante una brecha de ciberseguridad que ha sido previamente identificada logrando así solventar el problema o mitigar su impacto.
   Por ejemplo:
   - Garantizar que las soluciones preestablecidas de respuesta actúen durante y después de un incidente.
   - Analizar de la eficacia de las soluciones de respuesta.

5. **Recuperar**: Permite identificar las actividades apropiadas para mantener los planes de resiliencia y restaurar los servicios dañados durante los incidentes de ciberseguridad.
   Por ejemplo:
   - Garantizar que el sistema implemente los procesos y procedimientos de planificación de la recuperación.
   - Implementar mejoras basadas en soluciones aprendidas durante ataques anteriores.
   - Coordinar las comunicaciones durante las actividades de recuperación.

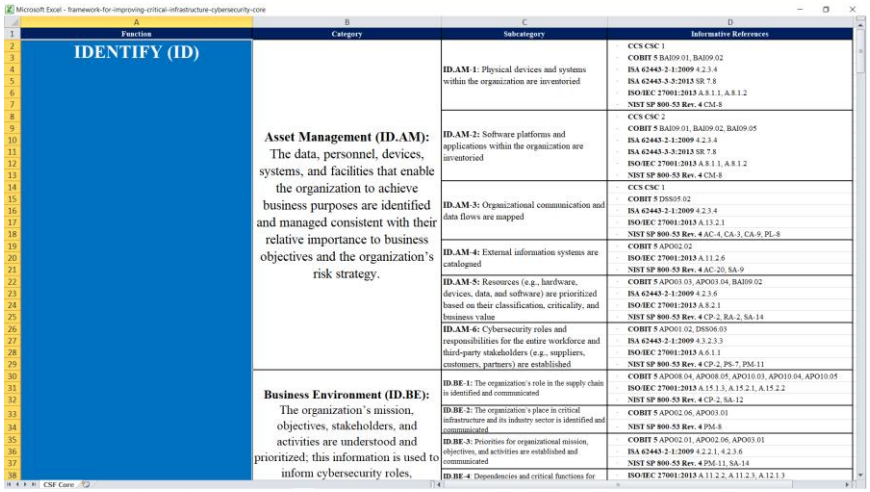
A su vez, cada una de estas funciones cuenta con categorías y sub-categorías con sus referencias informativas relacionadas (estándares, directrices y prácticas), como puede apreciarse en la siguiente figura.

ID Función	Función	ID Categoría	Categoría	Subcat.	Referencias Informativas
ID	Identificar	ID.AM	Gestión de Recursos	ID.AM1 ID.AM2 ……	CCS CSC 1, COBIT 5 , ……
		ID.BE	Entorno de Negocio	……	
		ID.GV	Gobernanza	……	
		ID.RA	Evaluación del Riesgo	……	
		ID.RM	Estrategia de gestión del Riesgo	……	
		ID.SC	Gestión Riesgo Cadena Suministro	……	
PR	Proteger	PR.AC …… ……	Gestión Acceso e Identificación …… ……		
DE	Detectar	DE.AE ……	Entorno de Negocio ……		
RS	Responder	……	……		
RC	Recuperar	……	……		

Figura 67: Estructura del marco básico del CFS

En la Figura 67: Estructura del marco básico del CFSvemos un ejemplo parcial de la estructura del marco básico en la función de "Identificar", donde se ve la categoría de gestión de recursos ("assets management") con sus correspondientes subcategorías (dispositivos físicos, plataformas software, comunicaciones corporativas, etc..) así como sus referencias informativas (estándares, documentos, guías, etc..).

La Figura 68: Ejemplo parcial de la Estructura del marco básico (excell descargable del NIST) esta sacada de la herramienta en Excel que el propio NIST tiene disponible para su descarga.



Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CCS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CCS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8
		ID.AM-3: Organizational communication and data flows are mapped	**CCS CSC** 1 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**COBIT 5** APO02.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	**COBIT 5** APO03.03, APO03.04, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	**COBIT 5** APO01.02, DSS06.03 **ISA 62443-2-1:2009** 4.3.2.3.3 **ISO/IEC 27001:2013** A.6.1.1 **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles,	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	**COBIT 5** APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 **ISO/IEC 27001:2013** A.15.1.3, A.15.2.1, A.15.2.2 **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	**COBIT 5** APO02.06, APO03.01 **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	**COBIT 5** APO02.01, APO02.06, APO03.01 **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for	**ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3

Figura 68: Ejemplo parcial de la Estructura del marco básico (excell descargable del NIST)

4.1.2 NIVELES DE IMPLEMENTACIÓN DEL MARCO (FRAMEWORK IMPLEMENTATION TIERS)

Los niveles de implementación permiten que cada empresa puede identificar en que nivel se encuentra respecto a sus prácticas actuales de la gestión de riesgo, el entorno de amenazas, los requerimientos legales, sus objetivos de negocio y las restricciones de la propia empresa.

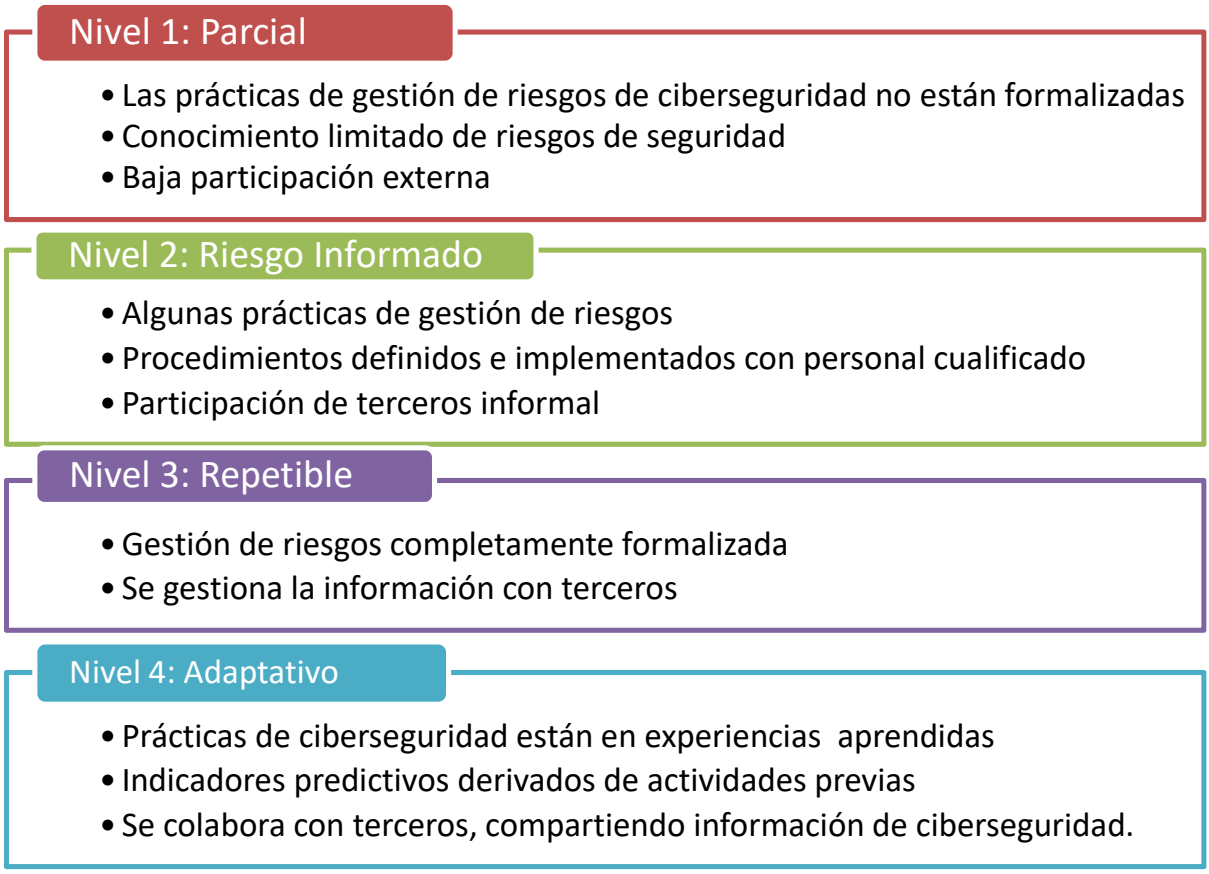


Figura 69: Niveles de implantación del CFS

4.1.3 PERFILES DEL MARCO BÁSICO (FRAMEWORK PROFILES)

Los perfiles se emplean para describir el estado actual y el estado objetivo de determinadas actividades de ciberseguridad. El análisis diferencial entre perfiles permite la identificación de brechas de seguridad que deberían ser gestionadas para cumplir con los objetivos de gestión de riesgos.

Para ello, se requiere la definición de un plan de acción que incluya una priorización de actividades dependiendo de los procesos de gestión de riesgos de la organización. Este enfoque permite a la organización estimar los recursos necesarios (personal, inversión, etc.) para lograr las metas de ciberseguridad establecidas.

De acuerdo con las descripciones anteriores, la arquitectura global del marco de trabajo de ciberseguridad según el NIST quedaría de la siguiente manera:

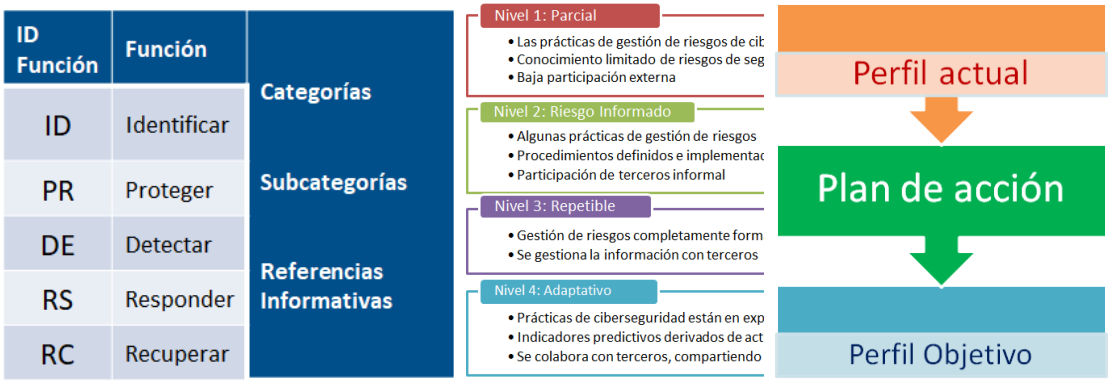


Figura 70: Marco global de trabajo del NIST

4.2 APLICACIÓN DE MEDIDAS CONCRETAS DE CIBERSEGURIDAD A UN ENTORNO INDUSTRIAL

Una vez analizadas de forma general las directrices que el NIST indica para mejorar la ciberseguridad de cualquier tipo de empresa, vamos a intentar estudiar las medidas que se pueden aplicar en un entorno industrial con tecnología OT, más en concreto una planta solar fotovoltaica.

Hay gran variedad de empresas que han realizado estudios y análisis para desarrollar modelos de ciberseguridad que se puedan aplicar a entornos OT. Vamos a basarnos en los informes de tres organizaciones punteras en este tema cómo son: Gartner, CISA y NREL.

La reflexión más importante cuando uno trabaja en ciberseguridad es tener presente que la seguridad total en un entorno industrial es imposible.

4.2.1 MEDIDAS Y SOLUCIONES DE IMPLEMENTACIÓN RÁPIDA

CISA al ser una agencia federal del gobierno de Estados Unidos propone unas medidas de fácil aplicación a los entornos industriales que pueden solventar problemas. Me gusta

destacarlas porque hay veces que el ser humano va de lo particular a lo general y en ciberseguridad es importante no descuidar las bases. Ciertas medidas pueden parecer obvias pero la importancia de su aplicación es capital y no han de ser olvidadas. Entre ellas destacan las siguientes:

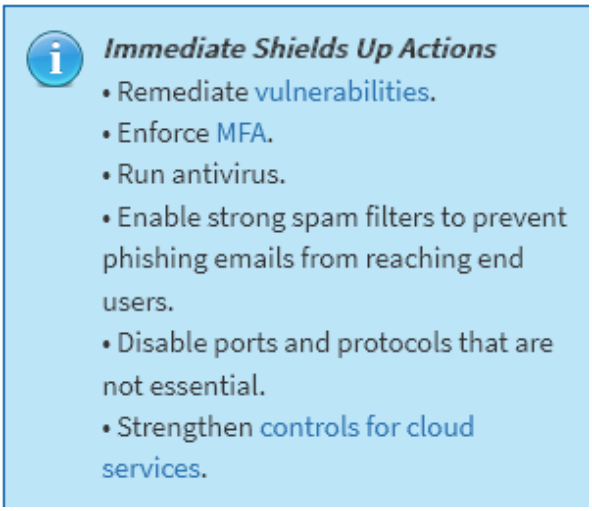


Figura 71: Medidas (1) CISA (www.cisa.gov)

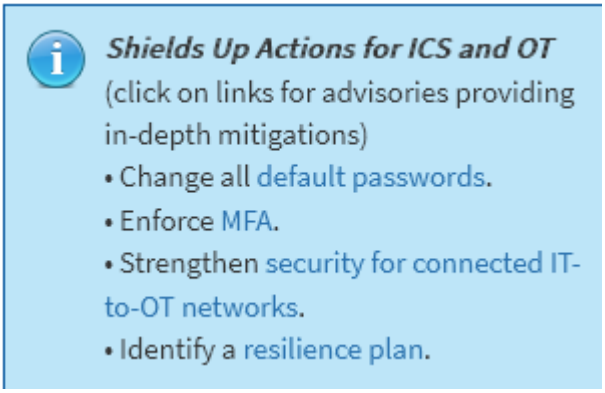


Figura 72: Medidas (2) CISA (www.cisa.gov)

Por otro lado, el grupo Gartner recomienda establecer toda una serie de controles en las empresas que tienen una infraestructura OT para mejorar su ciberseguridad y prevenir posibles incidentes que afecten a su infraestructura industrial. En la siguiente figura se plasman los 10 aspectos a tener en cuenta.

Figura 73: Los 10 Controles de Seguridad en OT (https://www.gartner.com)

A continuación, se van a ofrecer una recopilación de ciertas medidas que pueden ser aplicadas en nuestra planta solar. Estas proceden de las fuentes mencionadas anteriormente.

Lo primero, es importante actualizar el software, incluidos los sistemas operativos, las aplicaciones y el firmware de forma periódica. Hay que dar prioridad a la aplicación de parches a los sistemas que contienen vulnerabilidades conocidas que ya han sido explotadas y a las vulnerabilidades críticas que permitan la ejecución remota de código o la denegación de servicio en los equipos orientados a Internet. Se puede considerar la posibilidad de utilizar un sistema centralizado de gestión de parches. En concreto, en las redes OT, conviene utilizar una estrategia de evaluación basada en el riesgo para determinar los dispositivos y zonas de la red OT que deben participar en el programa de gestión de parches.

Por otro lado, hay que aplicar el MFA (Autenticación Multi-Factor) en la mayor medida posible. En cuanto a los inicios de sesión es necesario cambiar de forma rutinaria tanto las contraseñas cómo los usuarios. No se han de permitir contraseñas que se utilicen en varias cuentas. Últimamente el Estado ruso han demostrado la capacidad de explotar los protocolos MFA por defecto y las vulnerabilidades conocidas, las organizaciones deben revisar las políticas de configuración para protegerse contra los escenarios de "fail open" y reinscripción. [16]

Si se utiliza RDP (Remote Desktop Protocol) u otros servicios potencialmente peligrosos, estos han de ser asegurados y vigilados. La explotación de RDP es uno de los principales focos de infección inicial del ransomware. Los servicios de alto riesgo, incluido RDP, pueden permitir el acceso no autorizado a sesiones dentro de la propia infraestructura OT. Después de evaluar los riesgos, si se considera que el RDP es necesario, hay que limitar desde donde se puede acceder e implementar el MFA para mitigar el robo y la reutilización de credenciales. Si el RDP debe estar disponible externamente, es necesario implementar una red privada virtual (VPN) u otros medios para autenticar y asegurar la conexión.

Por otro lado, hay que comprobar la correcta configuración de los dispositivos, asegurando que las funciones de ciberseguridad están activadas y operativas. Desactivar los puertos y protocolos que no se utilicen con fines empresariales (por ejemplo, el puerto 3389 que corresponde al Protocolo de Control de Transmisión del RDP).

La labor de concienciación y formación de los usuarios finales es muy importante para ayudar a prevenir el éxito de las campañas de ingeniería social y phishing. El phishing es uno de los principales vectores de infección del ransomware. Los empleados han de ser conscientes de las posibles ciberamenazas y deben saber que hacer y con quién ponerse en contacto cuando reciban un correo electrónico sospechoso de phishing o sospechen de un incidente cibernético.

Como parte de un esfuerzo a más largo plazo, es importante la segmentación de la red. Esta segmentación puede ayudar a prevenir la propagación del ransomware y el movimiento lateral de los actores de la amenaza mediante el control de los flujos de tráfico y el acceso a varias subredes. Además, hay que implementar adecuadamente la segmentación entre las redes de IT y OT. Esto limita la capacidad de los adversarios de pasar a la red de OT incluso si la red de IT se ve comprometida. Hay por ello que definir una zona desmilitarizada que elimine la comunicación no controlada entre las redes de IT y OT.

Los recursos y dispositivos OT no han de ser accesibles desde el exterior. Si necesariamente estos deban ser accesibles desde el exterior en algún momento puntual, hace falta garantizar una sólida gestión de identidades y accesos.

Organizar los activos OT en zonas lógicas teniendo en cuenta su criticidad, las consecuencias de sufrir un ciberataque y la necesidad de que se mantengan operativos. Para ello el modelo de Purdue es sumamente útil. También es necesario definir los conductos de comunicación aceptables entre las distintas zonas y desplegar controles de seguridad para filtrar el tráfico de red y supervisar las comunicaciones entre zonas. Prohibir que los protocolos ICS atraviesen la red IT.

Capítulo 5. CONCLUSIONES FINALES Y FUTUROS TRABAJOS

En esta memoria se han analizado los componentes sensibles de ciberataques de una planta solar fotovoltaica y se han aportado algunas soluciones para mejorar la robustez del sistema. Además, se ha tratado de mostrar desde el punto de vista del hacker lo sencillo que puede llegar a ser conocer información crítica sobre un sistema utilizando herramientas gratuitas online.

Tras la realización de este trabajo de investigación se llega a una conclusión clara y determinante, la ciberseguridad total en cualquier entorno es inalcanzable. Muchas empresas y sistemas pueden tener una falsa sensación de seguridad que se aleja de la realidad y que supone un gran peligro. Se puede pensar que una planta es completamente ciber segura y no prestar la suficiente atención a la detección y prevención de futuros ataques, facilitando así el trabajo a los atacantes. Sabiendo pues que la ciberseguridad total es una utopía, es de primordial importancia asegurar lo máximo posible una planta de generación de energía y realizar una labor de prevención sistemática y eficaz.

Por otro lado, en los próximos años, con la inclusión de nuevos equipos inteligentes conectados a internet y el aumento de la interacción entre el mundo IT y OT, las brechas de seguridad no harán más que crecer. La tendencia es clara e imparable, Los ciberataques a sistemas OT están creciendo de forma significativa. Según el informe X-Force de IBM, durante el año 2021 los ataques a empresas industriales ocuparon el primer puesto (23,2% de los ataques), superando por primera vez a los ciberataques a servicios financieros [17]. El mismo informe indica que durante 2021 se produjo un aumento del dos mil doscientos cuatro por ciento (2.204%) de casos de reconocimiento contra OT. Fundamentalmente contra dispositivos SCADA Modbus OT que resultaban accesibles a través de internet.

La dependencia de los países de las energías renovables para proporcionar un futuro próspero a las nuevas generaciones solo aumentará. Por ello, se concluye que la importancia de construir plantas renovables ciberseguras es crucial y debería ser una prioridad.

Respecto a los posibles trabajos futuros. Sería interesante elaborar un estudio de las pérdidas económicas que puede suponer un ciberataque a la red eléctrica. Analizar las diferencias entre los distintos ataques que se realizan y el impacto que tendría en un país como España un ataque a una planta de generación de energía solar fotovoltaica o a una planta eólica.

Capítulo 6. BIBLIOGRAFÍA

[1] Microsoft. "An overview of Russia's cyberattack activity in Ukraine",2022. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd.

[2] N.S.A. "Network Infrastructure Security Guidance", 2022. https://www.cisa.gov/uscert/ncas/current-activity/2022/03/03/nsa-releases-network-infrastructure-security-guidance.

[3] Nozomi Networks Labs. "Nozomi Networks Labs Analyzes the IEC 104 payload", Abril 2022. https://www.nozominetworks.com/blog/industroyer2-nozomi-networks-labs-analyzes-the-iec-104-payload/

[4] Hany EL Mokadem. "Switch Attacks and Countermeasures", Cisco, 2022. https://www.cisco.com/c/dam/en_us/training-events/le31/le46/cln/promo/share_the_wealth_contest/finalists/Hany_EL_Mokadem_Switch_Attacks_and_Countermeasures.pdf

[5] Cibersecurity & Infrastructure Security Agency. "Securing Network Infrastructure Devices", 2018. https://www.cisa.gov/uscert/ncas/tips/ST18-001

[6] Louis Senecal. "Layer 2 Attacks and Their Mitigation", Cisco, 2021. https://www.cs.dartmouth.edu/~sergey/netreads/L2-security-Bootcamp.pdf

[7] S. E. T. Office. "Solar Cybersecurity Basics", 2020. https://www.energy.gov/eere/solar/solar-cybersecurity-basics

[8] SMA. "STATEMENT BY SMA SOLAR TECHNOLOGY AG ON THE CYBER SECURITY OF PV INVERTERS (HORUS SCENARIO)", 2017 https://www.sma.de/fileadmin/content/global/specials/documents/cyber-security/Whitepaper-Cyber-Security-AEN1732_07.pdf

[9] Emerson. "How To Protect Your PLC Control Systems From Security Threats", 2019. https://www.emerson.com/documents/automation/case-study-how-to-protect-your-plc-control-systems-from-security-threats-emerson-en-6325986.pdf

[10] Mandiant. "INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems", Abril 2022. https://www.mandiant.com/resources/incontroller-state-sponsored-ics-tool

[11] Danielle Veluz. "STUXNET Malware Targets SCADA Systems", Octubre 2011. https://www.trendmicro.com/vinfo/us/threat-encyclopedia/web-attack/54/stuxnet-malware-targets-scada-systems

[12] Cibersecurity & Infrastructure Security Agency. "APT cyber tools targeting ICS/SCADA devices", Abril 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-103a

[13] Revector. " Revector Detector IMSI Catcher UAV Payload". https://www.unmannedsystemstechnology.com/company/revector/revector-detector-imsi-catcher-uav-payload/

[14] NIST. "Cybersecurity Framework Version 1.1", Abril 2018. https://www.nist.gov/cyberframework/framework

[15] NIST. "Framework for Improving Critical Infrastructure Cybersecurity", Abril 2018. https://nvlpubs.nist.gov/nistpubs/cswp/nist.cswp.04162018.pdf

[16] CISA. "Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and "PrintNightmare" Vulnerability", Mayo 2022. https://www.cisa.gov/uscert/ncas/alerts/aa22-074a

[17] IBM. "X-Force Threat Intelligence Index 2022", 2022. https://www.ibm.com/downloads/cas/ADLMYLAZ