****

**Escuela de Ingenierías**

**Industrial, Informática y Aeroespacial**

**GRADO EN INGENIERÍA INFORMÁTICA**

Trabajo de Fin de Grado

ANÁLISIS DE CIBERSEGURIDAD EN SUSESTACIONES CON EL ESTANDAR IEC 61850

CYBERSECURITY ANALYSIS IN SUBSTATIONS WITH IEC 61850 STANDARD

Autor: Marcos González Maestre

Tutor: Isaías García Rodríguez

(Julio, 2022)

|  |  |
| --- | --- |
| **UNIVERSIDAD DE LEÓN**  **Escuela de Ingenierías Industrial, Informática y Aeroespacial**  **GRADO EN INGENIERÍA INFORMÁTICA**  **Trabajo de Fin de Grado** | |
| **ALUMNO:** Marcos González Maestre | |
| **TUTOR:** Isaías García Rodríguez | |
| **TÍTULO:** Análisis de ciberseguridad en subestaciones con el estándar IEC 61850 | |
| **TITLE:** Cybersecurity analysis in substation with IEC 6150 STANDARD | |
| **CONVOCATORIA:** Mes, Año | |
| **RESUMEN:**  El resumen reflejará las ideas principales de cada una de las partes del trabajo, pudiendo incluir un avance de los resultados obtenidos. Constará de un único párrafo y se recomienda una longitud no superior a 300 palabras. En cualquier caso, no deberá superar una página de longitud. | |
| **ABSTRACT:** | |
| **Palabras clave:** Lorem, ipsum, dolor, sit, amet. | |
| **Firma del alumno:** | **VºBº Tutor/es:** |

**Índice**

[1 Introducción 6](#_Toc104193639)

[1.1 INTRODUCCIÓN 6](#_Toc104193640)

[1.2 JUSTIFICACIÓN DEL PROYECTO 7](#_Toc104193641)

[1.3 OBJETIVOS DEL PROYECTO 7](#_Toc104193642)

[1.4 ESTRUCTURA DEL PROYECTO 7](#_Toc104193643)

[1.5 METODOLOGÍA 7](#_Toc104193644)

[2 Planificación y gestión del proyecto 8](#_Toc104193645)

[2.1 ALCANCE DEL PROYECTO 8](#_Toc104193646)

[2.2 PLANIFICACIÓN 8](#_Toc104193647)

[3 Estado del arte 9](#_Toc104193648)

[3.1 ESTO ES UNA PRUEBA 9](#_Toc104193649)

[4 Tecnologías usadas 9](#_Toc104193650)

[4.1 VMWARE WORKSTATION PRO 9](#_Toc104193651)

[4.2 NOZOMI NETWORKS 10](#_Toc104193652)

[4.3 WIRESHARK 12](#_Toc104193653)

[4.3.1 PARA QUE SE USA WIRESHARK 13](#_Toc104193654)

[4.4 IED SCOUT 13](#_Toc104193655)

[4.5 ADVANCED IP SCANNER 15](#_Toc104193656)

[4.6 TCPDUMP 15](#_Toc104193657)

[4.7 IEDs 17](#_Toc104193658)

[5 Núcleo del trabajo 18](#_Toc104193659)

[5.1 CIBERSEGURIDAD 18](#_Toc104193660)

[5.1.1 HISTORIA DE LA CIBERSEGURIDAD 18](#_Toc104193661)

[5.1.2 PRINCIPALES ATAQUES CIBERNETICOS 18](#_Toc104193662)

[5.1.3 AMBITOS DE LA CIBERSEGURIDAD 18](#_Toc104193663)

[5.1.4 CIBERSEGURIDAD EN LA ACTUALIDAD 19](#_Toc104193664)

[5.1.5 CIBERSEGURIDAD APLICADA AL MUNDO INDUSTRIAL 19](#_Toc104193665)

[5.2 ESTÁNDAR IEC 61850 19](#_Toc104193666)

[5.2.1 INTRODUCCION AL IEC 61850. ¿QUÉ ES? 19](#_Toc104193667)

[5.2.2 ORÍGENES DEL ESTANDAR IEC 61850 19](#_Toc104193668)

[5.2.3 ESTRUCTURA DEL IEC 61850 19](#_Toc104193669)

[5.2.4 MODELOS DE COMUNICACIÓN 19](#_Toc104193670)

[5.3 Wireshark 19](#_Toc104193671)

[5.4 Nozomi 20](#_Toc104193672)

**Índice de Ilustraciones**

[Ilustración 1. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia) 8](#_Toc103848801)

[Ilustración 2. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia) 9](#_Toc103848802)

[Ilustración 3. Logo de la herramienta Nozomi Networks(Fuente: https://www.nozominetworks.com) 10](#_Toc103848803)

[Ilustración 4. Panel principal Nozomi Guardian (Fuente: Elaboración propia) 11](#_Toc103848804)

[Ilustración 5. Logo de la herramienta Wireshark (Fuente: https://www.wireshark.org ) 11](#_Toc103848805)

[Ilustración 6. Logotipo Omicron Electronics (Fuente: https://www.acinel.com/omicron-es ) 13](#_Toc103848806)

[Ilustración 7. Logotipo Advanced IP Scanner (Fuente: https://www.advanced-ip-scanner.com/es ) 14](#_Toc103848807)

[Ilustración 8. Niveles elementos subestaciones (Fuente: https://www.google.com/search?q=tipos+ieds+electrica&client=opera&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiL3YT0huv2AhWsxYUKHffvDUQQ\_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=OJltEW2UdpVPiM) 15](#_Toc103848808)

**Glosario de términos**

**Sniffer:**

**DSJKWDH**

**HEW:**

# Introducción

## INTRODUCCIÓN

## 

En la actualidad, vivimos en un mundo globalizado y en constante cambio y evolución. Por la parte de ingeniería informática que nos involucra, es muy importante estar alerta y en constante evolución y aprendizaje para seguir el ritmo evolutivo de nuestro planeta. Ya lo pudimos ver, como durante la pandemia del COVID, todas las empresas tuvieron que adoptar medidas para el teletrabajo, que sin la colaboración de ingenieros y de instituciones informáticas hubiera sido todo mucho más complicado.

Adentrándonos en el ámbito informático, veremos qué pasa lo mismo en la rama de la ciberseguridad informática. Cada día que pasa, sale algo nuevo, algún nuevo gusano que puede comprometer el sistema de una empresa, posibles ataques a infraestructuras criticas de todo tipo (como por ejemplo en el ámbito nuclear), nuevos protocolos y estándares, los cuales se empiezan a aplicar e distintas situaciones o nuevas plataformas y aplicaciones usadas en este ámbito.

Durante la realización de este trabajo, estamos viendo como de importante es la ciberseguridad en el ámbito de infraestructuras críticas relacionadas con la energía. Sabiendo que cualquier falla de seguridad en una central nuclear por ejemplo puede desencadenar en una catástrofe humanitaria grandísima. O cualquier fallo o brecha en una subestación eléctrica, puede dejar sin electricidad a una gran parte de ciudadanos de un país incluido empresas situadas en esa zona. Y todo ello, desemboca en una única situación, caos en la población y pérdidas dinerarias irreparables para las empresas.

## JUSTIFICACIÓN DEL PROYECTO

## OBJETIVOS DEL PROYECTO

## ESTRUCTURA DEL PROYECTO

## METODOLOGÍA

Para poder tener los conocimientos necesarios y la base adecuada para la correcta realización del proyecto, fue necesario un periodo de tiempo de aprendizaje que consistió en la lectura y comprensión del estándar IEC 61850, lo cual englobaba la lectura de todos los capítulos del estándar y unas preguntas y ejercicios realizada por el tutor. Una vez conseguido estos conocimientos, IED SCOUT fue la plataforma usada para ver una simulación de comunicación entre un suscriptor y un publicador que emulaba el manejo de un IED real. Una vez entendido y visto cómo funciona la comunicación entre suscriptor y publicador, pasamos a usar la herramienta NOZOMI.

# Planificación y gestión del proyecto

## ALCANCE DEL PROYECTO

## PLANIFICACIÓN

Uno de los apartados fundamentales para un desarrollo correcto de la realización de este proyecto, es la planificación. El desarrollo del mismo, se dividió en 3 secciones:

1. **Introducción al estándar IEC 61850**
2. **Lectura y documentación de todas las partes del IEC 61850**
3. **Parte práctica del proyecto.**

# Estado del arte

## ESTO ES UNA PRUEBA

# Tecnologías usadas

## VMWARE WORKSTATION PRO

VMWARE es una empresa filial de EMC, dedicada al mundo del software y virtualización, la cual ofrece herramientas como VMWARE Blockchain, CloudHealth Secure State, VMware Secure Access, VMware Cloud Foundation o VMware Workstation Pro. Esta última, será la herramienta de virtualización de VMware que se usará para la implementación de otra herramienta básica en la implementación de este proyecto, denominada Nozomi.

Ilustración 1. Logotipo VMWare Workstation Pro (Fuente: https://www.vmware.com/es/products)

VMware Workstation Pro es una herramienta de virtualización que sirve para emular un elemento al que no estamos teniendo acceso. Es decir, físicamente no tenemos acceso directo a ese recurso, ya que solo lo estamos emulando. Esta herramienta ha sido usada para la implantación y configuración de la herramienta que más abajo explicaré, Nozomi Guardian.

)

Ilustración 2. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia)

Seguimps escribiendo

## NOZOMI NETWORKS

Nozomi es una compañía de software relacionado con el tratamiento de los datos y la ciberseguridad. Se definen así mismo como *“la mejor opción en soluciones de seguridad y visibilidad de la tecnología operativa y del internet de las cosas. Acelera la transformación digital protegiendo la infraestructura crítica así como a las organizaciones industriales y gubernamentales de las ciber-amenazas”*. Disponen de una serie de productos, entre los que se encuentran los siguientes:

1. Nozomi Vantage
2. Nozomi Guardian
3. Nozomu Central Management Console
4. Nozomi Cyber Threat Intelligence
5. Nozomi OT y IoT Asset Intelligence



Ilustración 3. Logo de la herramienta Nozomi Networks(Fuente: https://www.nozominetworks.com)

En nuestro proyecto, la herramienta necesaria para el análisis de todo el tráfico de red y la creación de alertas en los casos necesarios es Nozomi Guardian.

Nozomi Guardian se caracteriza por reducir los riesgos de OT para las mayores infraestructuras críticas, energía y fabricación, minería, transporte, automatización de edificios y otras instalaciones de OT en todo el mundo.

En la ilustración 3 se puede ver reflejado todas las aplicaciones y caracterisiticasque posee la herramienta Nozomi Guardian. Entre las cuales se pueden señalar las siguientes:

* Información de entorno
* Descripcion general de activos
* Estado general
* Rendimiento total de red
* Flujo de alertas a lo largo del tiempo
* Ultimas alertas

Como se puede apreciar, todas esas opciones están relacionadas con la seguridad y control de dicha red. Podemos identificare todo el tráfico de red, sabiendo que protocolos están siendo utilizados así como todas las sesiones activas y todos los nodos tanto activos como no situados dentro de dicha red.

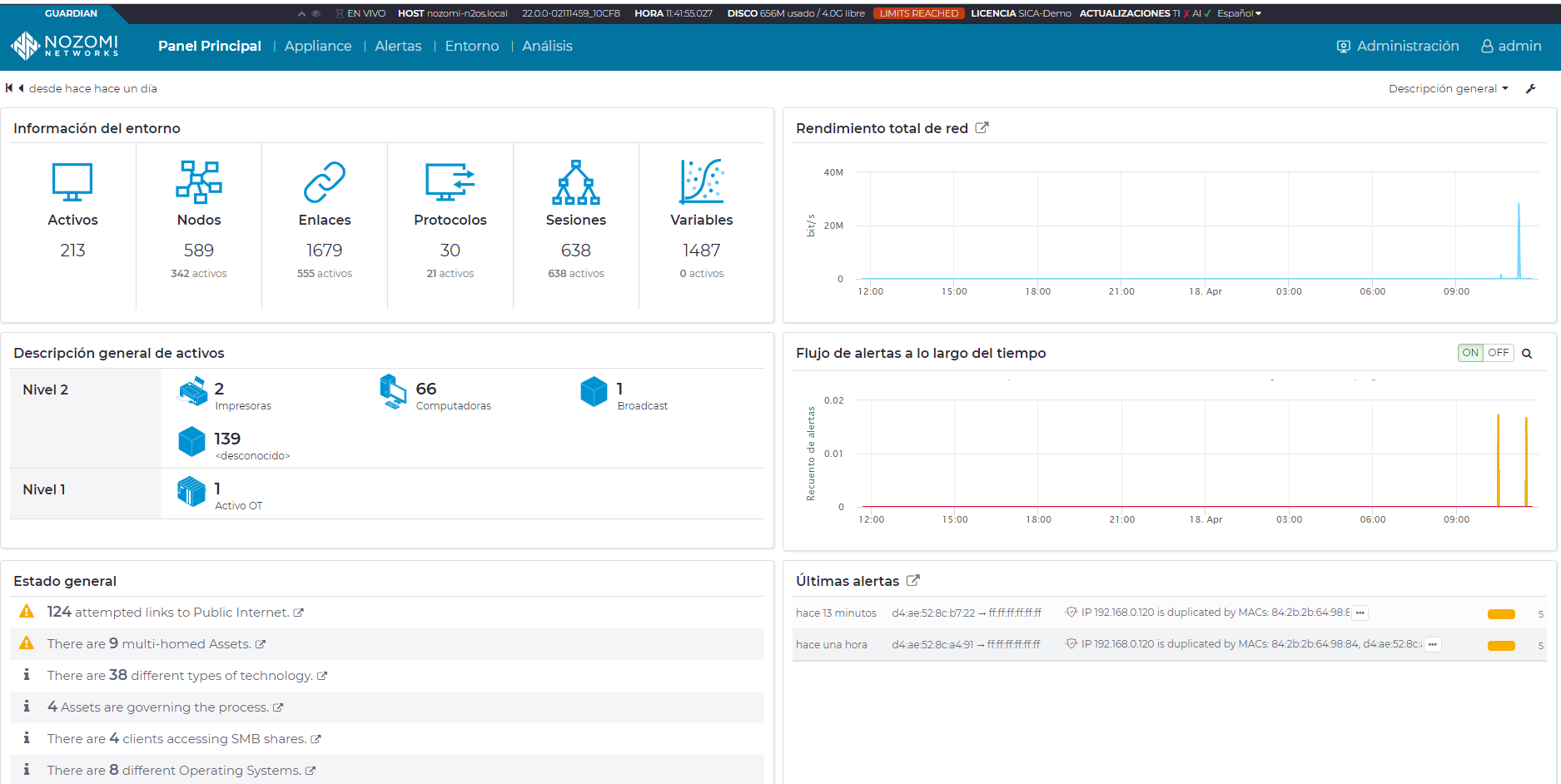


Ilustración 4. Panel principal Nozomi Guardian (Fuente: Elaboración propia)

## WIRESHARK

La herramienta Wireshark es una de las herramientas más antiguas, conocidas y usadas en el ámbito de redes y ciberseguridad. Wireshark se puede definir como un analizador de protocolos de código abierto cuyo principal objetivo es analizar el tráfico en la red. Está disponible tanto para plataformas Windows como para Linux. Wireshark posee una amplia gama de filtros de búsqueda de tramas para los más de 1000 protocolos soportados actualmente.

Originalmente Wireshark nació del proyecto de la herramienta llamada Ethereal, la cual haya personas que les suene el nombre y posiblemente la hayan usado. Ethereal se empezó a desarrollar en 1997 y la cual se dejó de implementar en el año 2006. A partir de ahí paso a llamarse como la conocemos hoy en día, Wireshark.

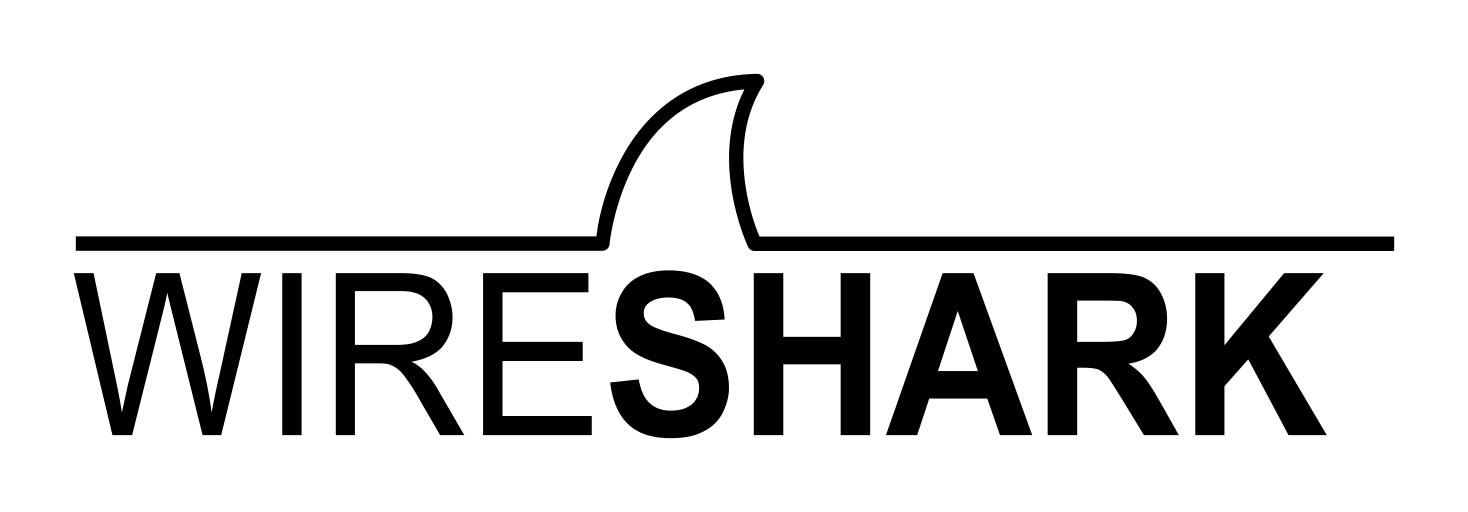


Ilustración 5. Logo de la herramienta Wireshark (Fuente: <https://www.wireshark.org> )

### PARA QUE SE USA WIRESHARK

La idea básica de esta herramienta es que el usuario pueda ver con detalle el tráfico de paquetes que se está generando en una determinada red. Se tiene que tener en cuenta que hasta en redes domésticas en las que un solo host está conectado, habrá movimiento de paquetes. En este tipo de redes pequeñas, se podrá ver con facilidad todos los tipos de paquetes y para qué sirven cada uno.

Si por el contrario, la red a la que se conecta el host, es una red mucho más extensa (esto quiere decir que hay un número alto de host conectados en la misma red, ejemplo: oficina de una empresa con 25 trabajadores conectados en la misma red), habrá mucho más paquetes y será más difícil captar los paquetes que interesen. Por lo que se tendrán que usar lo que se denomina como filtros. Esta herramienta posee infinidad de filtros para detectar los paquetes que contengan la característica indicada en ese filtro. Por ejemplo si se quiere ver únicamente los paquetes que contengas una IP de origen o de destino usaremos este filtro: ip.src\_host==192.1.168.1.128 || ip.dst==192.168.1.128, donde 192.168.1.128 sería la IP del host que queremos que aparezcan sus paquetes.

Adentrándose más en las características principales de Wireshark, se puede llegar a ver paquetes perdidos, actividad maliciosa en la red mediante la captura de paquetes http, así como problemas de latencia o problemas de conexiones. En apartados superiores, veremos varias implementaciones y usos de esta herramienta.

En resumen, con Wireshark podremos ver y analizar todos los paquetes de nuestra red como si estuviéramos en un laboratorio con un microscopio analizando todo lo que pasa en una determinada red.

## IED SCOUT

IED Scout es una herramienta que nos permite la automatización y virtualización de protección de subestaciones que disponen del estándar IEC 61850. Esta herramienta nos permite ver la comunicación entre un suscriptor y un publicador, así como todos los paquetes enviados por cada uno de los extremos y poder analizar su contenido y los diferentes valores que se transportan. Además, se puede observar los cambios realizados en cualquier de los dos extremos.



Ilustración 6. Logotipo Omicron Electronics (Fuente: <https://www.acinel.com/omicron-es> )

Definen su herramienta como “*un cliente universal de servidores IEC 61850 (como los IED de subestación) y editor/suscriptor de mensajes GOOSE. Proporciona numerosas funciones útiles que son necesarias en la subestación o el laboratorio”.*

Entre otras características de la herramienta IED Scout, se pueden destacar las siguientes:

* Como cliente IEC 61850, admite diversas funciones, desde la lectura/escritura genérica de atributos de datos hasta la utilización del auto descripción del IED y la generación de archivos SCL a partir de ella.
* Detecta mensajes GOOSE en la red y los supervisa.
* Puede utilizarse incluso con información de configuración incompleta o sin ella
* El IED Scout también simula mensajes GOOSE.
* Proporciona acceso a IED compatibles con IEC 61850 de cualquier proveedor

Esta herramienta es perfecta para empezar a manejar comunicaciones GOOSE y ver el intercambio de mensajes entre publicador y suscriptor, así como para ver dichas implementaciones virtualizadas. Todo ello sin poner en peligro ningún IED ni ninguna protección. Además, se pueden crear archivos SCL totalmente idénticos a cualquier IED real. Por lo que es una de las mejores herramientas de virtualización dentro del mundo de la ingeniería y de las comunicaciones.

En resumen, IED Scout nos permite virtualizar IEDs y simular posibles comunicaciones como si de un entrono real se tratase.

## ADVANCED IP SCANNER

Escáner de la red fiable y gratuitduo para analizar LAN. El programa escanea todos los dispositivos de red, le da acceso a las carpetas compartidas y a los servidores FTP, le proporciona control remoto de las computadoras (mediante RDP y Ranedmin) e incluso puede apagar las computadoras de manera remota. Es fácil de usar y se ejecuta como una edición portable. Debe ser la primera opción para cada administrador de red.



Ilustración 7. Logotipo Advanced IP Scanner (Fuente: https://www.advanced-ip-scanner.com/es )

## TCPDUMP

TCPDUMP es una de las herramientas más conocidas a nivel global la cual se enfocada en el análisis de la red. Esto se debe a que esta herramienta es open source y se puede implementar tanto en Windows como en Linux. Con este sniffer lo que el usuario consigue es poder capturar en tiempo real los paquetes recibidos y enviados de la interfaz de red seleccionada. Algunos se preguntarán por que usar TCPDUMP en vez de Wireshark, y la respuesta es súper sencilla. TCPDUMP no tiene interfaz gráfica ya que se ejecuta e implementa sobre un terminal, y Wireshark necesita más recursos para funcionar y para su interfaz gráfica. Por lo que, para comprobar que a mi Nozomi Guardian le estaban llegando todos los paquetes que circulaban por la red, se puede ejecutar TCPDUMP en la máquina virtual donde se está corriendo Nozomi, así podrá ver y detectar que trafico está llegando a la interfaz donde tienes configurado el Nozomi.



Ilustración 7. Logotipo TCPDUMP (Fuente: https://www.tcpdump.org )

Como ya dije antes, TCPDUMP tiene varios comandos configurados que hacen más complejo el uso de la misma. Estos son los siguientes:

* **Sudo tcpdump:** Con este comando, permite ver todo el tráfico de todas las interfaces activas en la maquina en la que se corra.
* **Sudo tcpdump –i em0**: El contenido es el mismo que el anterior, pero en vez de ver el tráfico de todas las interfaces, solo veremos el indicado en el comando, en este caso la interfaz em0.
* **Sudo tcpdump –i em0 –ttttnnvvS host 192.168.x.x:** Se consigue filtrar paquetes tanto por la interfaz introducida, en este caso em0 como por ip de host, en este caso 192.168.x.x. Se conseguirá ver todos los paquetes tanto enviados como recibidos por ese host dentro de esa interfaz de red.
* **Sudo tcpdump –i em0 –nn port 22:** Repetimos el segundo comando, añadiéndole la opción del puerto. Esto quiere decir que se filtrará tanto por interfaz primero, y después por puerto. Solo aparecerán los mensajes que entren y salgan por ese puerto, en este caso el 22, y que sean a través de la interfaz de red em0.
* **Sudo tcpdump –i em0 -nn mms:** Misma estructura que el segundo comando de la lista, añadiendo además un nuevo filtro por protocolo. En este caso, veremos todos los mensajes correspondientes al protocolo mms (Manufacturing Message Specification) dentro de la interfaz de red em0.

Otro de los comandos más importantes también se corresponde con la opción de poder guardar todo ese tráfico capturado en un único archivo pcap.

* **Sudo tcpdump –i em0 –w paquetes.pcap –s 0:** Se guardarán todos los paquetes que pasen por la interfaz de red em0 en el archivo pquetes.pcap. Con la opción –s 0, le estamos indicando que guarde todo el paquete sin excluir nada.

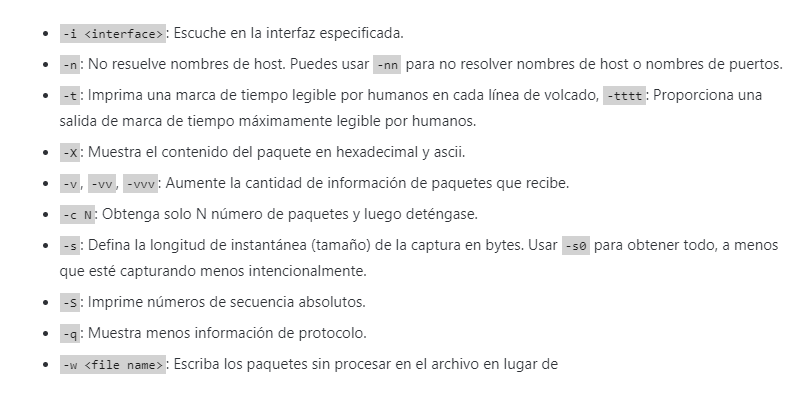


Ilustración 8. Resumen opciones de filtros TCPDUMP (Fuente: propia)

## IEDs

IED, es una de las siglas más utilizadas en el ámbito eléctrico, cuyas siglas significan Inteligent Electronic Device. Los IEDs, forman una parte importe de este proyecto, ya que son el pilar básico del mismo. El cual consiste en estudiar su comportamiento y evitar conexiones ajenas y maliciosas sobre ellos.

Tenemos varios tipos de IEDS. Que son los siguientes:

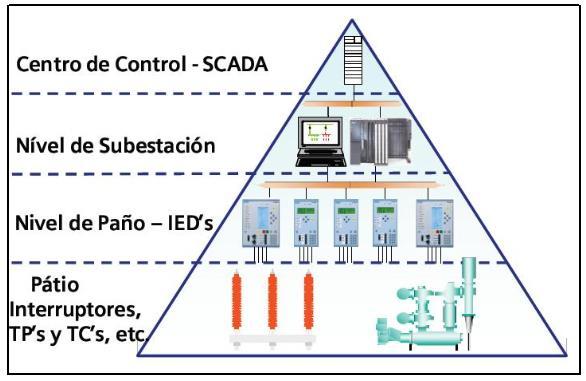


Ilustración 8. Niveles elementos subestaciones (Fuente: <https://www.google.com/search?q=tipos+ieds+electrica&client=opera&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiL3YT0huv2AhWsxYUKHffvDUQQ_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=OJltEW2UdpVPiM>)

# Núcleo del trabajo

## CIBERSEGURIDAD

Que mejor forma de definir un concepto, que acudiendo al diccionario de la Real Academia Española (RAE). La palabra “ciberseguridad” como tal no la podemos encontrar en el diccionario de la Real Academia Española, ya que esta proviene de la unión de las palabras ciber- y seguridad. Pero buscando por separado ciber- y seguridad, se puede obtener una idea del significado de la palabra aunque esta ya es muy conocida individualmente.

* Ciber-.
  + Indica relación con redes informáticas. *Ciberespacio, cibernauta.*
* Seguridad.
  + Cualidad de seguro.
  + Seguridad que proporciona un conjunto de mecanismos, características o prestaciones de un elemento cuya función es evitar o prevenir accidentes.

Una vez obtenidas ambas definiciones, se puede sacar la idea fundamental del concepto. Se puede definir como “ámbito de la informática que se centra en la protección de una entidad o de un espacio virtual mediante el uso de protecciones, equipos y reglas.”

Pero como se sabe, el ámbito de la informática es muy extenso, y por lo cual el de la ciberseguridad también. El término “ciberseguridad” se puede aplicar a diferentes contextos. Por lo que es importantes delimitar cuales son, y definirlos correctamente.

Ciberseguridad de software, de hardware, en redes, personal, coorporativa, activa, pasiva, nacional, lógica y física son los ámbitos mas importantes. En el siguiente párrafo se definirá y delimitará cada uno de los distinos contextos.

* Ciberseguridad de software
* Ciberseguridad de hardware
* Ciberseguridad en redes
* Ciberseguridad personal
* Ciberseguridad coorporativa
* Ciberseguridad activa
* Ciberseguridad pasiva
* Ciberseguridad nacional
* Ciberseguridad lógica
* Ciberseguridad física

### HISTORIA DE LA CIBERSEGURIDAD

### PRINCIPALES ATAQUES CIBERNETICOS

### AMBITOS DE LA CIBERSEGURIDAD

Cada día que pasa podemos ver como la palabra ciberseguridad, está siendo cada vez más familiar para las empresas. Desde inicio de los 60,

### CIBERSEGURIDAD EN LA ACTUALIDAD

### CIBERSEGURIDAD APLICADA AL MUNDO INDUSTRIAL

## ESTÁNDAR IEC 61850

### INTRODUCCION AL IEC 61850. ¿QUÉ ES?

IEC 61850 es un estándar relacionado con

### ORÍGENES DEL ESTANDAR IEC 61850

### ESTRUCTURA DEL IEC 61850

### MODELOS DE COMUNICACIÓN

## Wireshark

## Nozomi