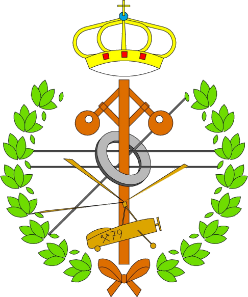
****

**Escuela de Ingenierías**

**Industrial, Informática y Aeroespacial**

**GRADO EN INGENIERÍA INFORMÁTICA**

Trabajo de Fin de Grado

ANÁLISIS DE CIBERSEGURIDAD EN SUSESTACIONES CON EL ESTÁNDAR 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:** Julio, 2022 | |
| **RESUMEN:** En este proyecto de fin de grado el objetivo principal es descubrir que herramientas se pueden implementar para poder defender todos los sistemas y elementos que forman una subestación eléctrica que tenga implementado el estándar IEC 61850, así como configurarlas de manera más óptima según las necesidades. Para ello, se debe comprender primero los principios básicos de la ciberseguridad, así como la estructuración y normas del estándar IEC 61850. Después haremos uso de la herramienta IEDScout para la simulación y virtualización de una comunicación entre IEDs (**I**ntelligent **E**lectronic **D**evice), creando una red exclusiva para la virtualización de esos IEDs. Dentro de esa red implementaremos la herramienta Nozomi Guardian, la cual estudiará cual es el tráfico “normal” entre esos IEDs y si detecta alguna anomalía de paquetes en la red nos saltara la alerta correspondiente. Por lo que conseguimos crear una simulación entre IEDs como si fueran de una subestación eléctrica y tenemos la herramienta controlando que todo el tráfico que está detectando es normal. | |
| **ABSTRACT: In this final degree project, the main objective is to discover what tools can be implemented to be able to defend all the systems and elements that make up an electrical substation that has the IEC 61850 standard implemented, as well as to configure them in the most optimal way according to the needs. To do this, we must first understand the basic principles of cybersecurity as well as the structure and standards of the IEC 61850 protocol. Then we will use the IEDScout tool to simulate and virtualize communication between IEDs, creating an exclusive network for the virtualization of those FDIs. Within that network we will implement the Nozomi Guardian tool, which will study what is the "normal" traffic between those IEDs and if it detects any anomaly of packets in the network, it will trigger the corresponding alert. So we managed to create a simulation between IEDs as if they were from an electrical substation and we have the tool checking that all the traffic it is detecting is normal.** | |
| **Palabras clave:** Ciberseguridad, subestación eléctrica, IEC 61850, IED, IEDScout, Nozomi Guardian. | |
| **Firma del alumno:** | **VºBº Tutor/es:** |

**Índice de contenidos**

[1 Introducción 9](#_Toc107305406)

[1.1 ESTRUCTURA DEL PROYECTO 10](#_Toc107305407)

[2 Justificación y objetivos 11](#_Toc107305408)

[2.1 JUSTIFICACIÓN DEL PROYECTO 11](#_Toc107305409)

[2.2 OBJETIVOS DEL PROYECTO 11](#_Toc107305410)

[3 Metodología y planificación 12](#_Toc107305411)

[3.1 METODOLOGÍA 12](#_Toc107305412)

[3.2 PLANIFICACIÓN 12](#_Toc107305413)

[4 Tecnologías usadas 14](#_Toc107305414)

[4.1 VMWARE WORKSTATION PRO 14](#_Toc107305415)

[4.2 NOZOMI NETWORKS 15](#_Toc107305416)

[4.3 WIRESHARK 17](#_Toc107305417)

[4.4 TCPDUMP 19](#_Toc107305418)

[4.5 IED SCOUT 21](#_Toc107305419)

[4.6 ADVANCED IP SCANNER 22](#_Toc107305420)

[5 Núcleo del trabajo 24](#_Toc107305421)

[5.1 CIBERSEGURIDAD 24](#_Toc107305422)

[5.1.1 PRINCIPALES ATAQUES CIBERNETICOS EN EL MUNDO INDUSTRIAL 27](#_Toc107305423)

[5.1.2 AMBITOS DE LA CIBERSEGURIDAD 32](#_Toc107305424)

[5.1.3 CIBERSEGURIDAD EN LA ACTUALIDAD 33](#_Toc107305425)

[5.1.4 CIBERSEGURIDAD APLICADA AL MUNDO INDUSTRIAL 36](#_Toc107305426)

[5.2 ESTÁNDAR IEC 61850 38](#_Toc107305427)

[5.2.1 INTRODUCCION AL IEC 61850. ¿QUÉ ES? 38](#_Toc107305428)

[5.2.1.1 SUBESTACIÓN ELECTRICA 39](#_Toc107305429)

[5.2.2 ORÍGENES DEL ESTÁNDAR IEC 61850 40](#_Toc107305430)

[5.2.3 ESTRUCTURA DEL ESTÁNDAR IEC 61850 41](#_Toc107305431)

[5.2.4 PRINCIPALES CARACTERISTICAS Y BENEFICIOS DEL ESTÁNDAR IEC 61850 42](#_Toc107305432)

[5.2.5 ARQUITECTURA DEL ESTÁNDAR IEC 6850 43](#_Toc107305433)

[5.2.6 MODELOS DE COMUNICACIÓN DEL ESTÁNDAR IEC 61850 45](#_Toc107305434)

[5.2.7 MODELADO DE DATOS DEL ESTÁNDAR IEC 61850 50](#_Toc107305435)

[5.2.8 LENGUAJE DE CONFIGURACIÓN DE UNA SUBESTACION 53](#_Toc107305436)

[5.3 VIRTUALIZACIÓN DE INTELLIGENT ELECTRONIC DEVICE CON IED SCOUT 58](#_Toc107305437)

[5.4 IMPLEMENTACIÓN DE NOZOMI GUARDIAN PARA MONITORIZACIÓN DE IEDs 64](#_Toc107305438)

[5.4.1 DESCRIPCIÓN DE LOS SERVICIOS BASICO DE NOZOMI GUARDIAN 65](#_Toc107305439)

[5.4.2 PANEL DE CONTROL DE SEGURIDAD DE NOZOMI GUARDIAN 70](#_Toc107305440)

[6 Resultados 74](#_Toc107305441)

[6.1 RED LOCAL MONITORIZADA POR NOZOMI GUARDIAN 74](#_Toc107305442)

[6.2 REPOSITORIO GIT HUB 74](#_Toc107305443)

[7 Conclusiones 75](#_Toc107305444)

[8 Presupuesto 76](#_Toc107305445)

[9 Agradecimientos 78](#_Toc107305446)

[10 Bibliografía 79](#_Toc107305447)

[11 Anexos 80](#_Toc107305448)

[11.1 INSTALACIÓN Y CONFIGURACION VMWARE WORKSTATION PRO 80](#_Toc107305449)

[11.2 DISEÑO Y CONFIGURACION DE UNA RED LOCAL PARA PRUEBAS 83](#_Toc107305450)

[11.3 INSTALACIÓN Y CONFIGURACIÓN IED SCOUT 84](#_Toc107305451)

[11.4 INSTALACIÓN Y CONFIGUACIÓN DE NOZOMI GUARDIAN 86](#_Toc107305452)

**Índice de Ilustraciones**

[Ilustración 3.1. Diagrama de planificación Gantt (Fuente: propia) 13](#_Toc107305453)

[Ilustración 4.1. Logotipo VMware Workstation Pro (Fuente: https://www.Vmware.com/es/products) 14](#_Toc107305454)

[Ilustración 4.2. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia) 15](#_Toc107305455)

[Ilustración 4.3. Logo de la herramienta Nozomi Networks (Fuente: https://www.nozominetworks.com) 16](#_Toc107305456)

[Ilustración 4.4. Panel principal Nozomi Guardian (Fuente: Elaboración propia) 17](#_Toc107305457)

[Ilustración 4.5. Logo de la herramienta Wireshark (Fuente: https://www.wireshark.org ) 17](#_Toc107305458)

[Ilustración 4.6. Logotipo TCPDUMP (Fuente: https://www.tcpdump.org ) 19](#_Toc107305459)

[Ilustración 4.7. Resumen opciones de filtros TCPDUMP (Fuente: propia) 21](#_Toc107305460)

[Ilustración 4.8. Captura pantalla programa IED Scout (Fuente: propia) 22](#_Toc107305461)

[Ilustración 4.9. Captura pantalla de Advanced IP scanner de la red de SICA (Fuente: propia) 23](#_Toc107305462)

[Ilustración 5.1. Logotipo representativo al virus Stuxnet. (Fuente: https://www.lapatilla.com/wp-content/uploads/2019/09/Stuxnet-virus.jpg?resize=640%2C345) 27](#_Toc107305463)

[Ilustración 5.2.Pantalla activación de macros BlackEnergy. (Fuente: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/) 28](#_Toc107305464)

[Ilustración 5.3. Línea temporal del troyano BlackEnergy. (Fuente: https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos) 29](#_Toc107305465)

[Ilustración 5.4.Grafico evolución ciberataques años 1980-85. (Fuente: curso CyberOps) 30](#_Toc107305466)

[Ilustración 5.5. Gráfico evolución ciberataques año 2000. (Fuente: curso CyberOps) 31](#_Toc107305467)

[Ilustración 5.6.Grafico evolución ciberataques año 2015-17. (Fuente: curso CyberOps) 31](#_Toc107305468)

[Ilustración 5.7. Agencias estatales de ciberseguridad. (Fuente: https://javierdisan.com/2018/09/25/) 33](#_Toc107305469)

[Ilustración 5.8. Gráfico uso de Internet por la población española. (Fuente: https://wearesocial.com/es/blog/2022/02 ) 34](#_Toc107305470)

[Ilustración 5.9. Portada Decálogo ciberseguridad para empresas elaborado por el INCIBE. (Fuente: https://www.incibe.es/sites/default/files/contenidos/guias/doc/sta\_decalogo\_ciberseguridad\_metad.pdf) 35](#_Toc107305471)

[Ilustración 5.10. Logotipo IEC. (Fuente: http://www.seguridadepm.com/iec ) 37](#_Toc107305472)

[Ilustración 5.11. Logotipo IEC. (Fuente: http://www.seguridadepm.com/iec ) 38](#_Toc107305473)

[Ilustración 5.12. Resumen IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 39](#_Toc107305474)

[Ilustración 5.13. Imagen subestación eléctrica (Fuente: https://www.tecsaqro.com.mx/wp-content/uploads/2021/05/seguridad\_subestacion\_electrica.jpg) 40](#_Toc107305475)

[Ilustración 5.14. Capítulos IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 42](#_Toc107305476)

[Ilustración 5.15. Arquitectura ESTÁNDAR IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 45](#_Toc107305477)

[Ilustración 5.16. Capas modelo TCP/IP (Fuente: https://elprofealegria.com/redes/modelo-tcp-ip/) 46](#_Toc107305478)

[Ilustración 5.17. Two-Party-Application-Association (Fuente: propia) 47](#_Toc107305479)

[Ilustración 5.18. MultiCast-Application-Association (Fuente: propia) 48](#_Toc107305480)

[Ilustración 5.19. Estructura de datos del ESTÁNDAR IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 50](#_Toc107305481)

[Ilustración 5.20. Nomenclatura de un Logical Node (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 51](#_Toc107305482)

[Ilustración 5.21. Nomenclatura de un objeto (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 52](#_Toc107305483)

[Ilustración 5.22. Jerarquía datos de un dispositivo lógico en el protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 53](#_Toc107305484)

[Ilustración 5.23. Ejemplo de un diagrama de una sola línea (single-line diagram) (Fuente: https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation ) 54](#_Toc107305485)

[Ilustración 5.24. Header de un archivo .SCD (Fuente: propia ) 55](#_Toc107305486)

[Ilustración 5.25. Communication de un archivo .SCD (Fuente: propia ) 55](#_Toc107305487)

[Ilustración 5.26. IED name de un archivo .SCD (Fuente: propia ) 56](#_Toc107305488)

[Ilustración 5.27. DataTypeTemplate de un archivo .SCD (Fuente: propia) 56](#_Toc107305489)

[Ilustración 5.28. DataTypeTemplate de un archivo .SCD (Fuente: propia) 57](#_Toc107305490)

[Ilustración 5.29. DataTypeTemplate de un archivo .SCD (Fuente: propia) 57](#_Toc107305491)

[Ilustración 5.30. Resumen archivos de configuración del estándar IEC 61850 (Fuente: Propia ) 57](#_Toc107305492)

[Ilustración 5.31. Parte del archivo .CID donde se cambia la IP (Fuente: Propia ) 58](#_Toc107305493)

[Ilustración 5.32. Opción “Simulator” de la herramienta IED Scout (Fuente: Propia ) 59](#_Toc107305494)

[Ilustración 5.33. Selección de archivo para su virtualización en IED Scout (Fuente: Propia ) 59](#_Toc107305495)

[Ilustración 5.34. Estructura de los datos del IED “E22\_LINEA2\_7SJ85” en IED Scout (Fuente: Propia ) 60](#_Toc107305496)

[Ilustración 5.35. Pestaña para comenzar la simulación del IED “E22\_LINEA2\_7SJ85” (Fuente: Propia ) 60](#_Toc107305497)

[Ilustración 5.36. Interfaz de la opción “Browser” dentro de IED Scout (Fuente: Propia ) 61](#_Toc107305498)

[Ilustración 5.37. Pestaña “Discover” para buscar el IED previamente virtualizado (Fuente: Propia ) 62](#_Toc107305499)

[Ilustración 5.38. Resultados de filtrado de paquetes en Wireshark con “ip.addr == 192.168.2.140” (Fuente: Propia ) 63](#_Toc107305500)

[Ilustración 5.39. Paquetes capturados por el Sniffer de IED Scout (Fuente: Propia ) 64](#_Toc107305501)

[Ilustración 5.40. (Fuente: Propia ) 65](#_Toc107305502)

[Ilustración 5.41. Pestaña de un activo en Nozomi Guardian (Fuente: Propia ) 66](#_Toc107305503)

[Ilustración 5.42. Pestaña de un activo en Nozomi Guardian (Fuente: Propia ) 67](#_Toc107305504)

[Ilustración 5.43. Pestaña de un activo en Nozomi Guardian (Fuente: Propia ) 67](#_Toc107305505)

[Ilustración 5.44. (Fuente: Propia ) 68](#_Toc107305506)

[Ilustración 5.45. Vista de proceso donde se muestran las variables monitoreadas en Nozomi Guardian(Fuente: Propia ) 68](#_Toc107305507)

[Ilustración 5.46.(Fuente: Propia ) 69](#_Toc107305508)

[Ilustración 5.47.(Fuente: Propia ) 71](#_Toc107305509)

[Ilustración 11.1. Paso 1 instalacion de Vmware Workstation Pro (Fuente: propia ) 80](#_Toc107305510)

[Ilustración 11.2. Paso 2 de la instalación de VMware Workstation Pro (Fuente: propia ) 81](#_Toc107305511)

[Ilustración 11.3. Paso 3 de la instalación de VMware Workstation Pro (Fuente: propia ) 82](#_Toc107305512)

[Ilustración 11.4. Pestaña de finalización de la instalación de VMware Workstation Pro (Fuente: propia ) 82](#_Toc107305513)

[Ilustración 11.5. Pantalla principal de VMware Workstation Pro (Fuente: propia ) 83](#_Toc107305514)

[Ilustración 11.6. Esquema básico de la red local creada para realizar las pruebas con Nozomi Guardian (Fuente: propia ) 84](#_Toc107305515)

[Ilustración 11.7. Esquema básico de la red local creada para realizar las pruebas con Nozomi Guardian (Fuente: propia ) 84](#_Toc107305516)

[Ilustración 11.8. Ventana de instalación de IED Scout. Elección del PATH (Fuente: propia ) 85](#_Toc107305517)

[Ilustración 11.9. Pestaña instalación adicional herramienta WinPcap (Fuente: propia ) 86](#_Toc107305518)

**Índice de tablas**

**Glosario de términos**

**Sniffer:** herramienta que permite al usuario capturar tramas de una red de computadoras

**Nicho de mercado:** porción especifica de una parte de mercado compuesta por individuos con características y necesidades homogéneas.

**Subestación eléctrica:** instalación cuyo objetivo es la distribución y transmisión de la energía eléctrica estableciendo unos niveles de tensión adecuados para su distribucion.

**Interruptor de potencia:** equipos mecánicos que abren y cierran los circuitos eléctricos con el fin de proteger los sistemas en caso de fallo eléctrico

**Transformador de corriente:** máquina de corriente alterna cuyo objetivo es modificar alguna característica de la corriente, como la intensidad o voltaje

**Fusible de protecciones:**

**Celdas de protección:**

**Reconectadores:**

**IEEE:**

**Ataques DoS:**

**Ataques DDoS:**

**ICS:** Industrial Control System

**Request:**

**Response:**

**Data-set:**

**Merge unit:**

**Single line diagram:**

**PATH:**

**Tools:**

**Port-mirroring:**

# Introducción

## 

La realidad en la que se vive es que la ciberseguridad es una pieza fundamental en el ámbito de infraestructuras críticas relacionadas con la energía. La protección de los sistemas tanto eléctricos como informáticos es estrictamente necesaria. Sabiendo que cualquier falla de seguridad en una subestación eléctrica, puede dejar sin electricidad a una gran parte de ciudadanos de un país, así como toda la industria situada en esa zona. Y todo ello, desemboca en una única situación, caos en la población y pérdidas dinerarias irreparables para las empresas.

A medida que la tecnología va evolucionando, aparecen nuevos elementos importantes. Ya sean, nuevas amenazas que pueden comprometer el sistema de una empresa, nuevos posibles ataques a infraestructuras críticas, nuevos protocolos y estándares, los cuales se empiezan a aplicar en distintas situaciones o nuevas plataformas y aplicaciones usadas en este ámbito.

Es el caso del estándar IEC 61850, que está implementándose en las subestaciones eléctricas con el objetivo de proporcionar una interoperabilidad entre los Intelligent Electronic Device (IED). Este es el nuevo nombre dado por el estándar IEC 61850, y en el cual se encuentras dispositivos como relés, interruptores y transformadores.

La elaboración del siguiente proyecto tiene como objetivo exponer en que consiste ese estándar IEC 61850 así como la configuración y el uso de la herramienta Nozomi Guardian. Esta herramienta de monitorización es usada para la defensa y supervisión de los elementos que forman una subestación eléctrica que tiene implementado el estándar IEC 61850, ya sean IEDs, SCADAS o cualquier otro elemento de una subestación.

La elaboración de este proyecto ha sido posible gracias a la colaboración con la empresa SICA S.A., la cual ha proporcionado las herramientas necesarias para el desarrollo de la misma.

## ESTRUCTURA DEL PROYECTO

El proyecto se encuentra dividido en diez capítulos bien diferenciados. Todos ellos siguiendo el estándar básico aportado por la Universidad de León. El proyecto comenzará con una pequeña descripción de los objetivos a conseguir y del por qué se ha realizado este proyecto. Seguido de él, se explicará la planificación llevada a cabo, con la inserción de un diagrama Gantt, así como los métodos de aprendizaje que han sido usados para el desarrollo del proyecto. En tercer lugar, se dedicará un apartado a cada una de las tecnologías que se han necesitado para la elaboración del proyecto, desde herramientas básicas como tcpdump, hasta herramientas de monitorización como Nozomi Guardian.

Una vez dentro del capítulo 5, denominado Núcleo del trabajo, se desarrollará técnicamente todo lo relacionado con la ciberseguridad, el estándar IEC 61850 y las pruebas realizadas para la finalización del proyecto. Este capítulo se encuentra dividido en 4 subapartados. En el primero de ellos, aparecerá toda la información relacionada con la ciberseguridad como termino genérico, introduciendo de forma global el tema a los lectores, incluyendo una breve descripción de la ciberseguridad en el mundo industrial y eléctrico.

Toda la información recopilada sobre el estándar IEC 61850, aparecerá en el segundo subapartado. Desde una breve introducción hasta el tipo de modelado de datos serán los campos introducidos en el proyecto, mencionando también como está dividido el estándar, cuál fue su origen, que protocolos de comunicación dispone para las comunicaciones y cuál debe ser el lenguaje de los archivos para la configuración de los sistemas de una subestación eléctrica. Los dos subapartados restantes, se focalizarán en la explicación y descripción del funcionamiento de las herramientas IED Scout y Nozomi Guardian, incluyendo las pruebas realizadas con las mismas herramientas.

Finalmente se dedicará un capítulo para cada uno de los siguientes conceptos: resultados obtenidos, conclusiones de la finalización del proyecto, presupuesto necesario para llevar a cabo el proyecto, agradecimientos a las personas que han ayudado a la realización del proyecto, la bibliografía con todas las referencias necesarias y los anexos donde se explica la instalación y diseño de las herramientas usadas durante el proyecto.

# Justificación y objetivos

## JUSTIFICACIÓN DEL PROYECTO

Uno de las infraestructuras más críticas e importantes en la actualidad son las subestaciones eléctricas. Son un pilar fundamental en la distribución de la electricidad a toda la población incluyendo todo tipo de empresas. Cualquier falla o problema surgido en cualquiera de ellas, puede suponer unas pérdidas dinerarias irreparables para las grandes empresas, así como un parón en la vida cotidiana de la población. Por lo que, un aspecto importante es la protección de los elementos que forman una subestación eléctrica, añadiendo además el estándar implementado en la subestación, en este caso el IEC 61850. Este estándar, indica que protocolos de comunican han de usar los elementos de la subestación, así como que modelo de datos tiene que implementarse entre otros. De ahí es sacado el nombre del proyecto, “Ciberseguridad en subestaciones eléctricas con el estándar IEC 61850”.

## OBJETIVOS DEL PROYECTO

En este apartado se describirán cuáles son los propósitos de la elaboración y desarrollo de este proyecto.

* Iniciación en el mundo de subestaciones eléctricas
* Comprensión de la jerarquía de una subestación eléctrica
* Comprensión del estándar IEC 61850
  + Conocimiento de los beneficios que aporta el estándar
  + Comprensión de los protocolos de comunicación descritos en el estándar IEC 61850
  + Comprensión el modelado de datos del estándar IEC 61850
  + Conocimiento del lenguaje usado para la configuración de una subestación
* Búsqueda de herramientas para la mejora de la seguridad de los elementos que forman una subestación eléctrica
* Mejorar la seguridad de los elementos de una subestación eléctrica mediante Nozomi Guardian.
* Uso y manejo de la herramienta de monitorización Nozomi Guardian.

# Metodología y planificación

## 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 incluyendo la elaboración de apuntes y esquemas que resumían los capítulos. Una vez conseguido estos conocimientos, IED SCOUT fue la herramienta usada para ver una simulación de comunicación entre un suscriptor y un publicador que emulaba el manejo de un IED real. Una vez conseguida esa comunicación entre un publicador y un suscriptor, la herramienta Nozomi Guardian entra a escena. La herramienta de monitorización de Nozomi Guardian aportaba información muy importante, como que dispositivos están conectado al publicador, que datos están siendo transmitidos o han sido transmitidos o la posibilidad de creación de alertas a gusto del usuario.

## PLANIFICACIÓN

Uno de los apartados fundamentales para un desarrollo correcto de la realización de este proyecto, es la planificación. El desarrollo de este se dividió en 7 tareas principales:

1. **Introducción al estándar IEC 61850**

En esta primera parte del proyecto, se realizaron varias charlas con el tutor de la empresa SICA S.A., con el objetivo de introducción de la temática de una manera más intuitiva, aportando una presentación introductoria al estándar IEC 61850.

1. **Lectura y documentación de todas las partes importantes del estándar IEC 61850**

Se llevó a cabo una lectura profunda de los diferentes capítulos que componen el estándar. Una vez leídos, se elaboraron resúmenes que ayudarían en el futuro a la elaboración del documento del proyecto

1. **Instalación y configuración de la herramienta de virtualización IED Scout.**
2. **Instalación y configuración de la herramienta de virtualización VMware Workstation Pro.**
3. **Diseño y configuración de una red local para pruebas**
4. **Instalación y configuración de la herramienta de monitorización Nozomi Guardian.**
5. **Realización de pruebas con Nozomi Guardian e IED Scout.**

En este último apartado, se realizó la parte más práctica del proyecto. Incluye todas las pruebas realizadas con IED Scout, así como los diferentes modos de defensa que posee Nozomi Guardian.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Ilustración 3.1. Diagrama de planificación Gantt (Fuente: propia)

# Tecnologías usadas

## VMWARE WORKSTATION PRO

VMware Workstation Pro es una herramienta de virtualización en la que se pueden desplegar máquinas virtuales. Una máquina virtual es igual que un ordenador físico, tiene su propia memoria, su CPU, su disco para almacenar información y su interfaz de red disponible para concretarse a internet. La única diferencia es que no es un ordenador físico, sino que es un ordenador virtual e intangible compuesto únicamente por líneas de código. Para poder “utilizar” estas máquinas virtuales, se necesita lo que se denomina una herramienta de virtualización. Por lo que VMware Workstation Pro es la herramienta de virtualización implementada para correr la máquina virtual de Nozomi Guardian.

VMware Workstation Pro es un servicio ofrecido por la empresa filiar VMWARE, la cual se dedica al mundo del software y virtualización, y ofrece herramientas como VMware Blockchain, CloudHealth Secure State, VMware Secure Access, VMware Cloud Foundation o VMware Workstation Pro.



Ilustración 4.1. Logotipo VMware Workstation Pro (Fuente: <https://www>.Vmware.com/es/products)

.

)

Ilustración 4.2. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia)

## 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. Nozomi Central Management Console
4. Nozomi Cyber Threat Intelligence
5. Nozomi OT y IoT Asset Intelligence



Ilustración 4.3. Logo de la herramienta Nozomi Networks (Fuente: <https://www>.nozominetworks.com)

Para la implementación de este 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 define como una **herramienta de supervisión y monitorización** de tráfico de red. 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 características que posee la herramienta Nozomi Guardian. Entre las cuales se pueden señalar las siguientes:

* Información de entorno
* Descripción 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 identificar 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 activos situados dentro de dicha red.

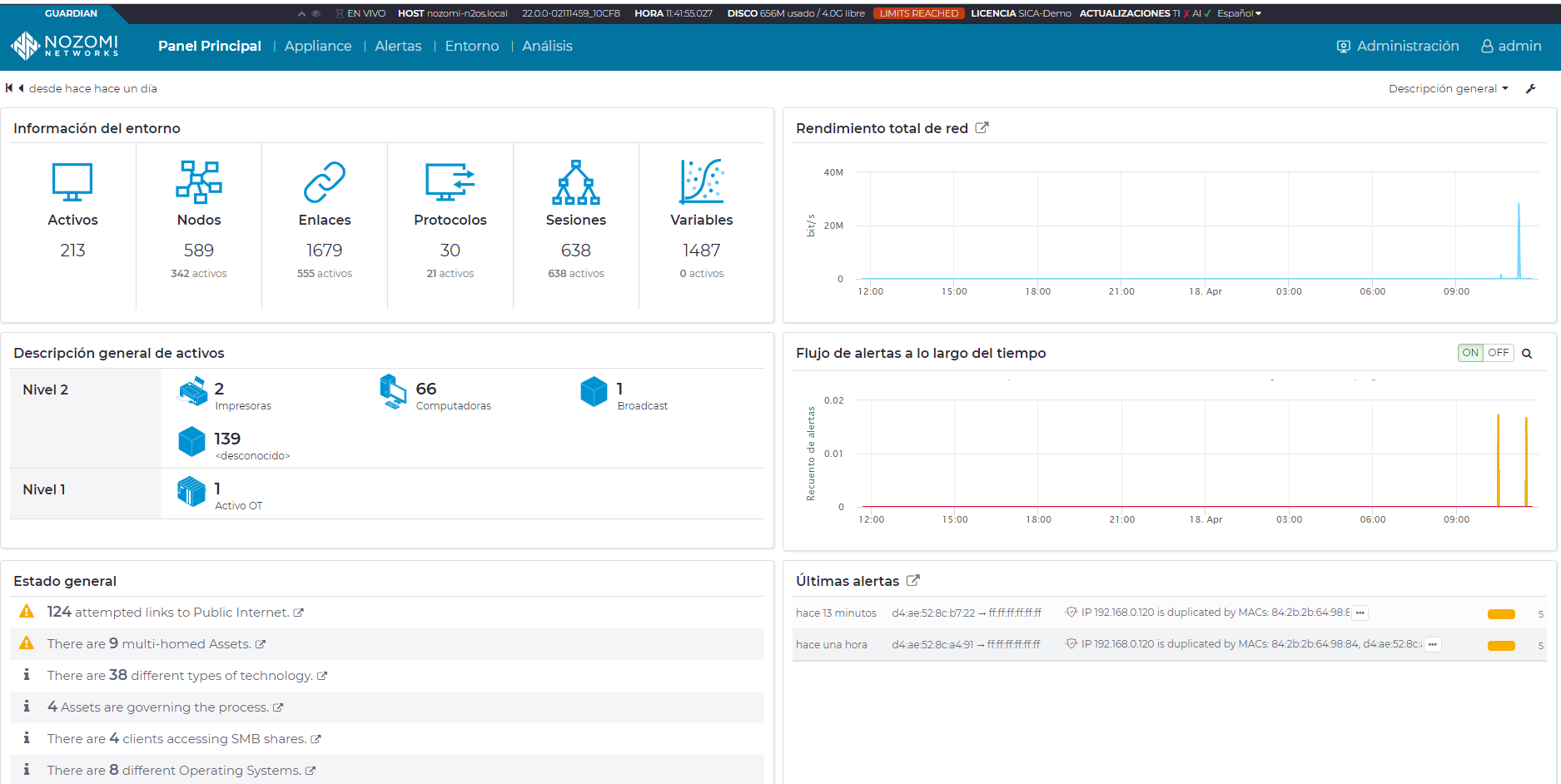


Ilustración 4.4. Panel principal Nozomi Guardian (Fuente: Elaboración propia)

## 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.

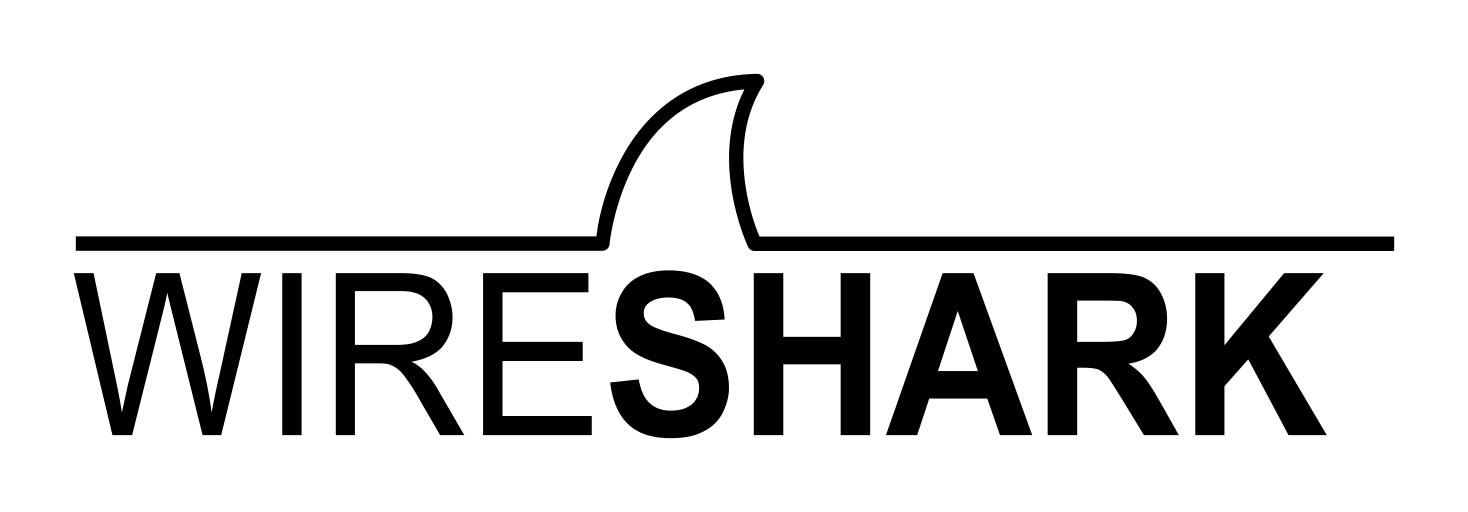


Ilustración 4.5. Logo de la herramienta Wireshark (Fuente: <https://www.wireshark.org> )

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 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.

Un aspecto positivo a destacar es la compatibilidad de Wireshark, con las tramas obtenidas desde Nozomi Guardian. Nozomi Guardian, posee la capacidad de poder guardar y descargar tramas de paquetes, y poder cargarlas en Wireshark para poder ver con detalle esos paquetes. Esta compatibilidad es un recurso importante, ya que si Nozomi detecta tráfico irregular y guarda esas tramas, el usuario puede ser capaz de identificar qué tipo de trama se trata y de si puede estar siendo algún tipo de ataque o no. La función inversa también se encuentra disponible. El usuario es capaz de poder cargar tramas Wireshark en el entorno de Nozomi Guardian y poder simular y ver como el propio Nozomi reaccionaria.

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.

## 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 4.6. 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.
* **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.

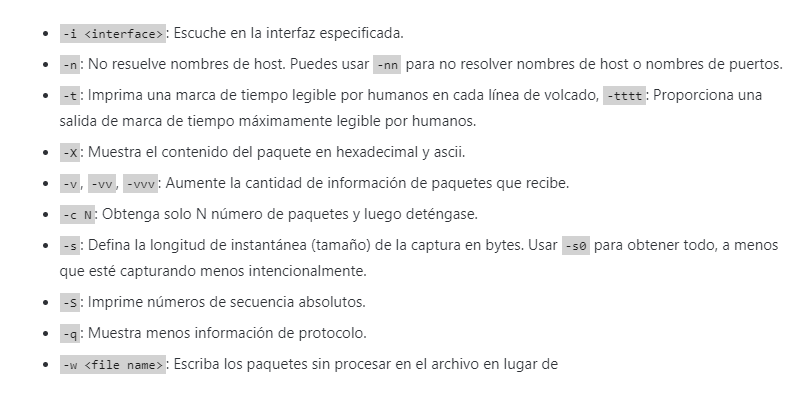


Ilustración 4.7. Resumen opciones de filtros TCPDUMP (Fuente: propia)

## 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.

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 de la 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.

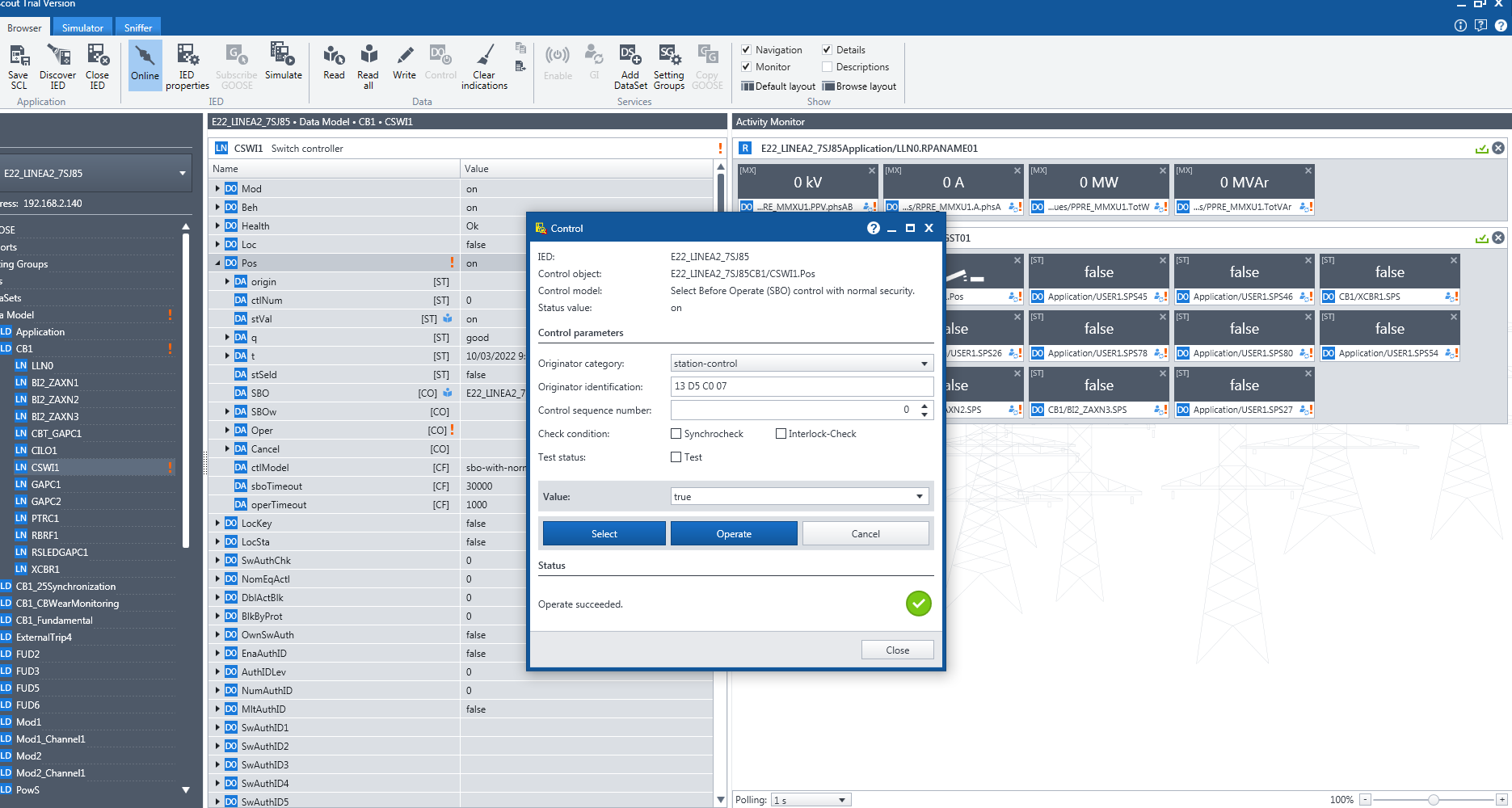


Ilustración 4.8. Captura pantalla programa IED Scout (Fuente: propia)

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

## ADVANCED IP SCANNER

Advanced IP scanner es una herramienta que se encarga de realizar un escáner de la red, obteniendo así toda la información requerida sobre los equipos que están conectados a dicha red escaneada. Es una herramienta gratuita y simple, pero muy útil. Durante el proyecto, ha sido usada continuamente, para poder ver que host estaban dentro de la red creada para ello, así como poder ver en qué IP está, su MAC, y si el host esta encendido o apagado.

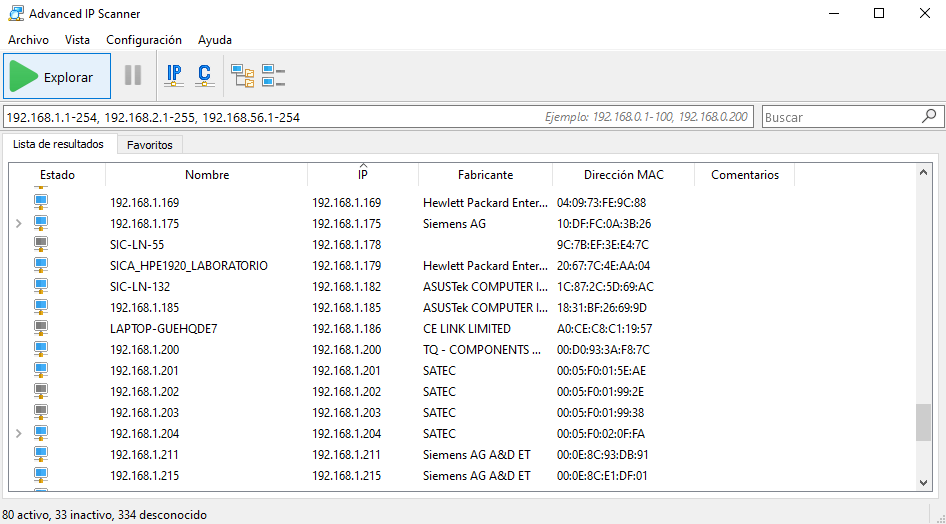


Ilustración 4.9. Captura pantalla de Advanced IP scanner de la red de SICA (Fuente: propia)

# 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, corporativo, activa, pasiva, nacional, lógica y física son los ámbitos más importantes. En el siguiente párrafo se definirá y delimitará cada uno de los distintos contextos.

* **Ciberseguridad de software.** Debemos saber primero, que significa software antes de poder definirlo claramente. Software se encuentra definido en la RAE como “Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora”. Por lo que la ciberseguridad en la modalidad del software, busca proteger la integridad de los programas, instrucciones y reglas de un sistema o sistemas informáticos.
* **Ciberseguridad de hardware.** Si el termino de software acuñaba todo lo relacionado con los programas, instrucciones y reglas informáticas, el termino hardware recopila todo lo contrario. Definido en la RAE como “Conjunto de aparatos de una computadora”, por lo que ya nos podemos hacer una idea de por dónde se encaminará. Se centra en la búsqueda de proteger la integridad del conjunto de aparatos de una computadora.
* **Ciberseguridad en redes.** Este es uno de los contextos más importantes y a su vez peligrosos de la ciberseguridad. Es uno de los pilares críticos de la informática. En este contexto, lo que se busca es proteger la integridad de los datos durante la comunicación entre distintos sistemas informáticos, asegurándonos de que durante esa comunicación nadie está accediendo a esos datos. La mayoría de los grandes ataques informáticos provienen de este contexto.
* **Ciberseguridad personal.** Consiste en mantener la integridad de los datos personales de un usuario determinado en su dispositivo particular. Información personal, contraseñas, fotos, cualquier dato que puede guardar un usuario en su dispositivo particular.
* **Ciberseguridad corporativa.** Una vez definida la ciberseguridad personal, la corporativa se asemeja a ella. Consiste en mantener la integridad de la información que una sociedad corporativa puede tener almacenada en sus sistemas informáticos.
* **Ciberseguridad activa.** Este contexto, se centra en la actuación de las estrategias de protección llevadas a cabo por el usuario o responsable de configuración de la red, cuando algún sistema informático ha sido atacado. En resumen, que estrategias lleva a cabo el administrador de la red/ (usuario cuando alguno de sus sistemas informáticos han sido hackeados para buscar la forma de recuperar y reparar los datos perdidos y los sistemas dañados.
* **Ciberseguridad pasiva.** Una vez aclarado que conceptos ocupa la ciberseguridad activa, sabremos delimitar con facilidad la ciberseguridad pasiva. Son aquellas herramientas y reglas configuradas por el administrador de red para intentar construir una barrera y evitar posibles ataques a la red. El firewall podría ser un ejemplo claro dentro del contexto de ciberseguridad pasiva.
* **Ciberseguridad nacional.** Como el mismo nombre indica, este engloba todas las medidas aplicadas sobre sistemas informáticos que pertenecen a la red nacional de un país en concreto. Por lo que ataques a este tipo de ámbitos es muy común, ya que un país tiene almacenado millones y millones de datos muy valiosos para los atacantes que incluso suelen ser otros países para obtener un beneficio político o económico.
* **Ciberseguridad física.** Agruparemos en este grupo todos aquellos métodos rudimentarios y tradicionales de ciberseguridad, todos ellos relacionados con el medio físico y el hardware. En resumen, este tipo de seguridad busca la protección analógica de los sistemas informáticos.

### PRINCIPALES ATAQUES CIBERNETICOS EN EL MUNDO INDUSTRIAL

Para poder conocer la actualidad de la ciberseguridad con respecto al mundo industrial, es necesario hacer un repaso de cuáles han sido los mayores ataques cibernéticos que han sufrido estructuras industriales y eléctricas de la historia, y con ello podremos entender el por qué se han tomado ciertas decisiones en determinados aspectos. A continuación, se enumerarán y describirán los ataques más conocidos:

* **Stuxnet.**

Uno de los softwares más conocido y complejos de la historia es el Stuxnet. Desarrollado en Bielorrusia en el año 2010, creado para captar información y manejar el funcionamiento de equipos industriales. El principal objetivo de este ataque con Stuxnet era la planta nuclear de Natanz, situada en el país de Irán. Todo empezó con la visita de unos inspectores rutinarios de la Agencia Internacional de Energía Atómica a la planta nuclear iraní.



Ilustración 5.1. Logotipo representativo al virus Stuxnet. (Fuente: <https://www>.lapatilla.com/wp-content/uploads/2019/09/Stuxnet-virus.jpg?resize=640%2C345)

Empezaron a sospechar del comportamiento de unas centrifugadoras que se usaban para enriquecer el uranio. Este comportamiento se repitió unos meses después, y tras una investigación, detectaron la infección de sus equipos, por culpa de un gusano informático. Se descubrió que este virus afectaba a los sistemas informáticos, SCADAs, e incluso PLCs, por lo que se consideró como la primera arma cibernética a nivel mundial. La forma de infección de este gusano es una de las más fáciles que existen, el USB. Se comenta que este virus entro en esta panta nuclear debido a que alguien perteneciente a la planta, se encontró un USB en el suelo y lo primero que hizo fue conectarlo a su ordenador de la central. El resultado fue el que el mundo conoce, la infección de la planta entera, y la autodestrucción de las maquinas industriales que alimentaban al uranio, suponiendo una pérdida de millones de euros para el país iraní, así como una demostración de que la ciberseguridad plena no existe.

* **BlackEnergy.**

Se puede definir como un troyano surgido a principios del año 2007 cuyo objetivo es lanzar constantes ataques de DDoS, campañas de espionaje cibernético o ataques con el fin de destrucción de información privilegiada. Este programa malicioso es capaz de expandirse mediante componentes o plugins, las cuales son capaces de atacar a otras plataformas. Con el tiempo se ha ido desarrollando y modificándose a sí mismo. La infección se realizaba mediante correo electrónico. Los atacantes de BlackEnergy usaban correos corporativos falsos y adjuntaban en los correos que enviaban, documentos Office con macros maliciosas.

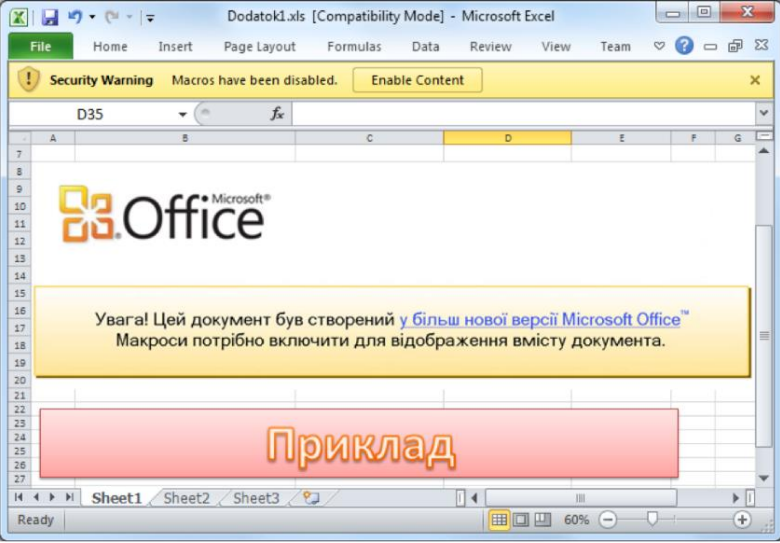


Ilustración 5.2.Pantalla activación de macros BlackEnergy. (Fuente: <https://www>.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/)

Una vez que se descargaba ese documento y se abría, al usuario le aparecía una pantalla que recomendaba habilitar las macros para poder ver el contenido del archivo. Aceptando esas macros, era como se activaba la infección del malware BlackEnergy.

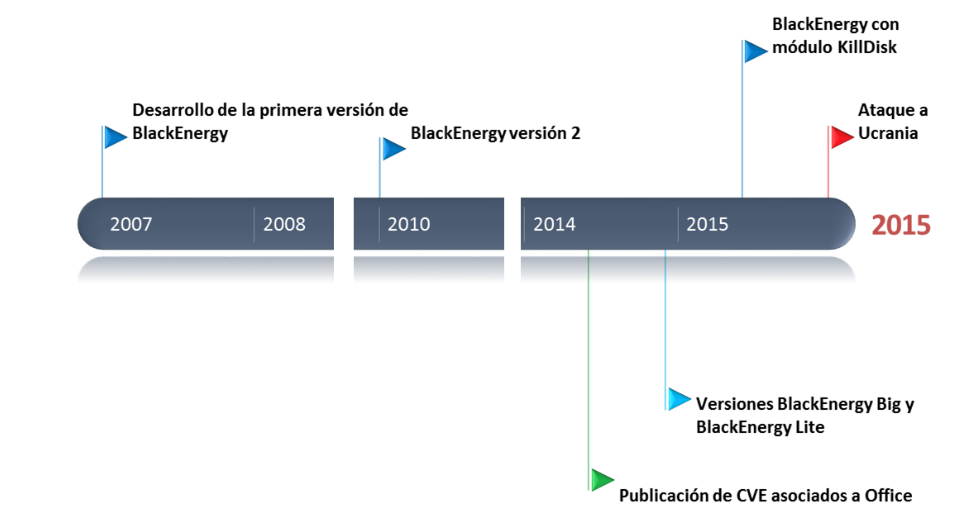


Ilustración 5.3. Línea temporal del troyano BlackEnergy. (Fuente: <https://www>.incibe-cert.es/blog/blackenergy-sistemas-criticos)

Los objetivos principales de este troyano han sido principalmente tres grupos bien identificados:

* Empresas energéticas mundiales
* Empresas SCADA y SCI de todo el mundo
* Ámbito energético, SCI, político y de comunicación ucraniano

Uno de los ataques BlackEnergy más conocidos se produjo en el año 2015 a la red eléctrica de Ucrania. El ataque cibernético BlackEnergy, consiguió sabotear los sistemas de control de las infraestructuras públicas eléctricas, dejando de esta forma a más de 1 millón y medio de habitantes ucranianos sin electricidad durante el 23 de diciembre de ese año 2015. Sumándole a este ataque, atraques al aeropuerto ucraniano de Kiev, st como a cadenas de televisión y medios de comunicación con un ataque similar al de la red eléctrica.

Anteriormente se ha podido ver cómo ha sido la evolución de las herramientas de ataque y el conocimiento técnico de los atacantes. Estos tres gráficos extraídos del curso de Cisco CyberOps realizado por el propio autor, reflejan a la perfección esa evolución.

Durante los primeros años de la implementación de los sistemas informáticos, las herramientas y opciones de ataque no eran sofisticadas, por no decir que eran técnicas “arcaicas”, muy simples y sin apenas complejidad. Por el contrario la habilidad y conocimientos de los atacantes era bastante complejo y superior.

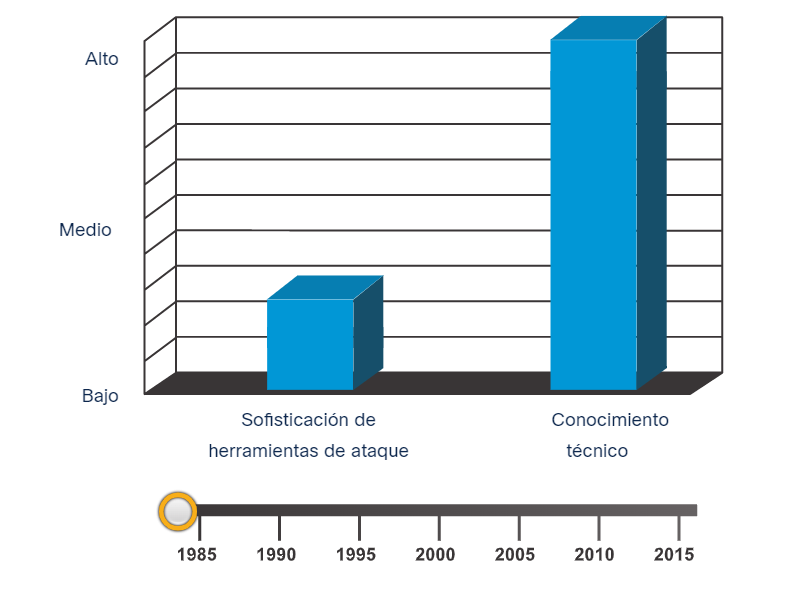


Ilustración 5.4.Grafico evolución ciberataques años 1980-85. (Fuente: curso CyberOps)

Según van transcurriendo años y nos vamos acercando a la entrada del siglo XXI, vemos como en las barras del gráfico, la diferencia entre ellas es mínima. Esto quiere decir que al haber mejorado las herramientas para realizar ataques, el atacante no necesita tener tanto conocimiento técnico como anteriormente, ya que las propias herramientas son bastante intuitivas y te van guiando. Pero el propio atacante necesitará también tener un nivel medio de conocimientos para poder desarrollar con efectividad.

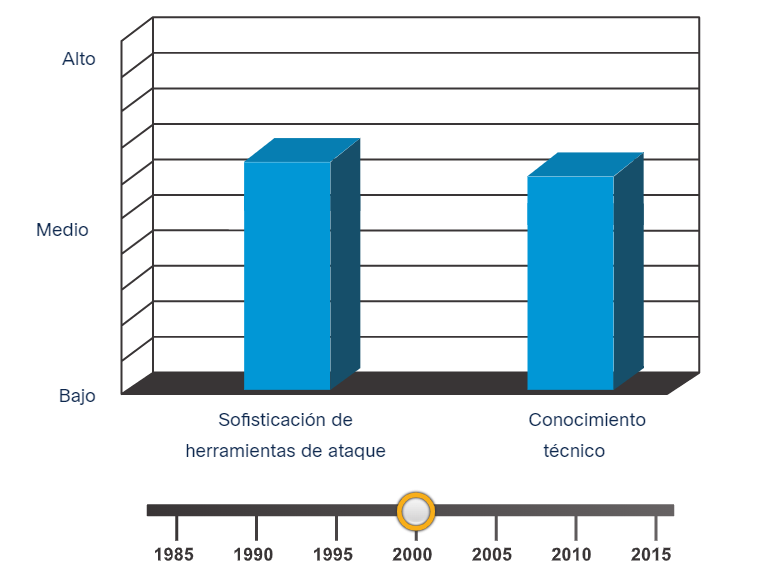


Ilustración 5.5. Gráfico evolución ciberataques año 2000. (Fuente: curso CyberOps)

Acercándonos a la actualidad, vemos como las barras del grafico han cambiado al viceversa. Ahora apenas es necesario que el atacante tenga conocimientos a alto nivel, ya que la sofisticación de las herramientas de ataque es tal alta, que prácticamente el atacante solo tiene que configurar de manera simple esa herramienta para poder realizar el ataque. Esto se ve influido por el rápido desarrollo de sistemas informáticos y de la búsqueda de nuevas tecnologías que hacen cada vez más compleja la ingeniera informática. Mucho que ver tienen las empresas, que buscan sacar nuevos productos, más complejos, para poder obtener así una rentabilidad económica alta y ser los líderes de su nicho de mercado

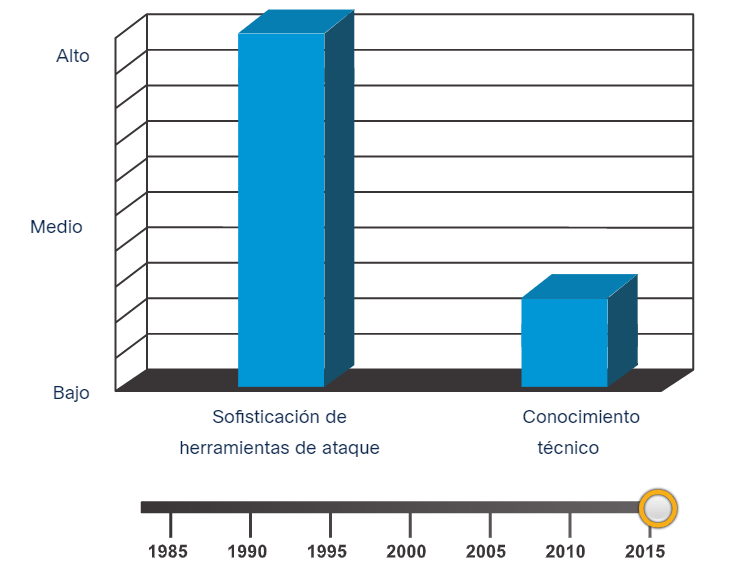


Ilustración 5.6.Grafico evolución ciberataques año 2015-17. (Fuente: curso CyberOps)

En resumen, juntando las tres gráficas, se puede sacar en conclusión una seria de características. Hoy en día, cualquier usuario que tenga un conocimiento muy básico sobre informática y redes puede llegar a ser capaz de realizar un ataque de cierto potencial. ¿Por qué? La respuesta es simple. La alta sofisticación de las herramientas de ataque. Con descargarse la herramienta necesaria y configurar sus parámetros es más que suficiente. No es necesario desarrollar ningún código ni script, ni tener que encontrar las vulnerabilidades de un OS para poder después atacarlo. Cosa que a principios de los 80, como vimos en el gráfico, apenas existían esas herramientas de tan fácil uso, por lo que el ataque y la forma de ataque dependían al 90% del conocimiento del usuario. Con el paso del tiempo, la tendencia evolutiva desembocará en herramientas muy sofisticadas, habrá cada vez más herramientas de ataque, y al ser tan sofisticadas, el usuario apenas necesitará conocimiento para poder realizar un ataque.

### AMBITOS DE LA CIBERSEGURIDAD

En la actualidad, los sistemas informáticos y electrónicos están a la orden del día. Ya sea desde el ámbito particular, como ciudadanos con sus computadoras y dispositivos electrónicos, hasta las organizaciones y negocios y empresas.

En el ámbito individual, la población cotidiana ha normalizado el uso de los dispositivos y de las redes informáticas. Gestión de banca electrónica, seguimiento de actualidad mediante periódico online, entretenimiento con las redes sociales, gestión y mantenimiento de los recursos de una vivienda (domótica), hacer compras online… y así una larga lista de eventos. El abanico de eventos informáticos realizados es interminable y según pase el tiempo y se continúe con el crecimiento de lo que se denomina **IoT** (Internet of Things, Internet de las cosas), más seguirá creciendo ese abanico.

Por otra parte, tenemos el ámbito empresarial, donde la evolución y el desarrollo de los sistemas ha sido exponencial. Hace dos décadas, era impensable que todas las empresas que forman el abanico empresarial implementaran para su desarrollo diario sistemas y el uso de las redes e Internet. Hoy en día, el Internet y los sistemas es la herramienta de trabajo por excelencia para la gran mayoría del abanico de empresas. Esto está influenciado también por la evolución de la sociedad en estos años. Cada vez la sociedad está más acostumbrada al uso de sistemas informáticos y por lo tanto tienen más conocimientos y capacidades prácticas para poder implementar esta herramienta en sus respectivos trabajos.

Y finalmente, se encuentra el ámbito estatal. Nuestros sistemas informáticos estatales, tienen la prioridad de protección e integridad de las infraestructuras y de los datos que se poseen. Administrar el control del padrón municipal o la supervisión de las infraestructuras críticas, es responsabilidad de la administración, la cual se divide en distintos escalones, ya sea local, autonómico/regional o estatal. El siguiente gráfico, muestra gráficamente como está estructurado el sistema estatal con los distintos órganos de cada escalafón de la administración.

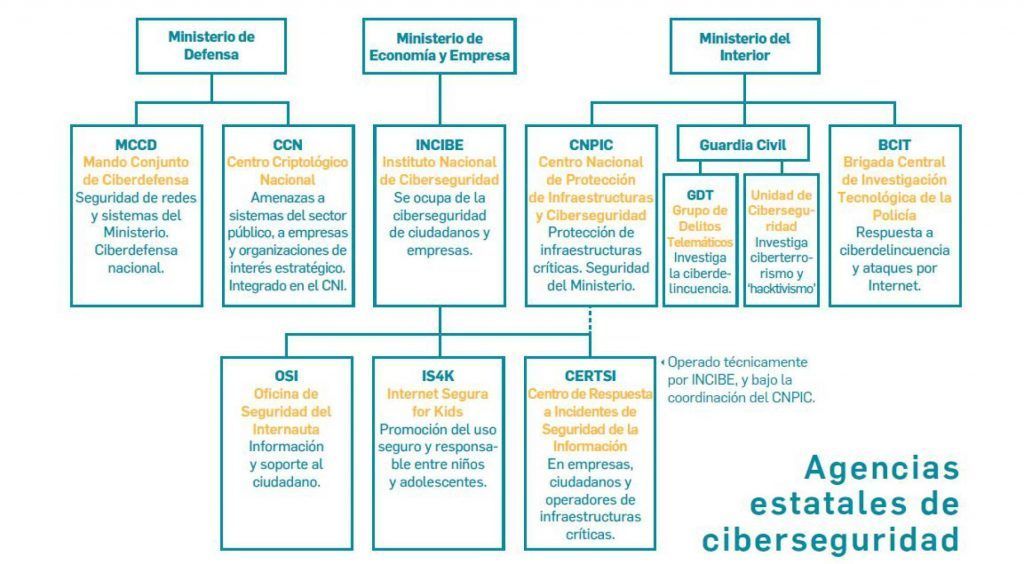


Ilustración 5.7. Agencias estatales de ciberseguridad. (Fuente: <https://javierdisan>.com/2018/09/25/)

### CIBERSEGURIDAD EN LA ACTUALIDAD

Como vimos anteriormente, en la actualidad cualquier usuario con unos conocimientos mínimos en informática y redes puede ser un potencial atacante. Esto quiere decir que la ciberseguridad tiene la obligación de estar cien por cien presente en todos los ámbitos informáticos para la defensa de todos aquellos sistemas ya sean empresariales, particulares o estatales.

En febrero del año 2022, el número total de usuarios de Internet fue de 43.93 millones. La población de España consta de 47.435.597 personas, de las cuales más del 94% usan Internet y/o redes sociales. Esto significa que hay una cantidad de datos masiva y cualquier ataque en los sistemas informáticos puede ser una gran brecha de robo de datos súper valiosos para el atacante o atacantes. Además, podemos ver en el grafico como de un año a otro sigue incrementándose el número de usuarios de Internet.

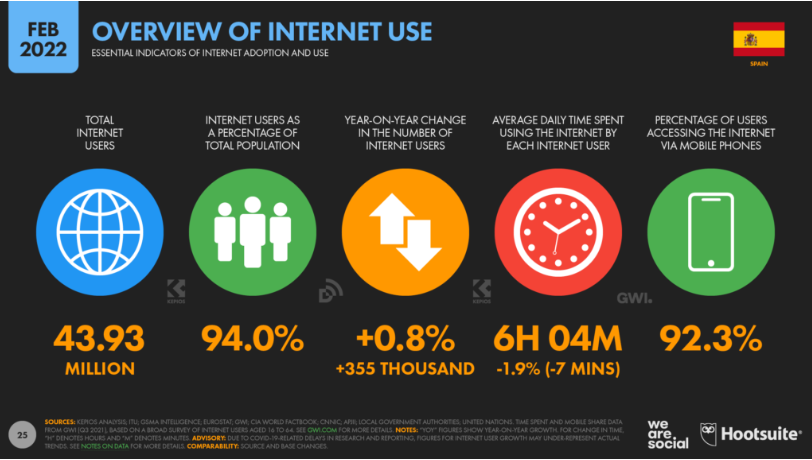


Ilustración 5.8. Gráfico uso de Internet por la población española. (Fuente: <https://wearesocial.com/es/blog/2022/02> )

Viendo el grafico anterior, se puede sacar en claro que el Internet es una pieza fundamental en la vida social y economía, pero por contraposición se ha podido ver como de vulnerable es debido a una multitud de ataques e incidentes cibernéticos.

En resumen, al incrementarse cada vez más el uso de Internet por parte de las personas, más importante es la forma en la que se tienen que defender esos sistemas, ya que nuestra privacidad se encuentra involucrada en ello mismo.

Con respecto al tema empresarial, se está viendo como las empresas se van mentalizando de loa importancia de este ámbito dentro de su jerarquía y su estructura. Están empezando a implementar equipos de ingenieros especializados en ciberseguridad para mantener sus sistemas fuera del alcance de cualquier tipo de ataque cibernético.

Como muchos ya conoceréis, el **INCIBE** que es el **I**nstituto **N**acional de **C**iberseguridad, se dedica en parte a guiar tanto a empresas como a particular a cómo reaccionar a cualquier tipo de incidencia cibernética. Este instituto, elaboró un decálogo de ciberseguridad para empresas. Cualquiera usuario de Internet puede acceder a este contenido que hace de guía de aproximación para cualquier tipo de empresario. Este tipo de iniciativas ayudan y fomentan que los empresarios tomen las medidas necesarias en el ámbito de ciberseguridad y sirva de apoyo para iniciar una implementación de sistemas contra la ciberdelincuencia.



Ilustración 5.9. Portada Decálogo ciberseguridad para empresas elaborado por el INCIBE. (Fuente: <https://www>.incibe.es/sites/default/files/contenidos/guias/doc/sta\_decalogo\_ciberseguridad\_metad.pdf)

En esta guía para los empresarios, que consta de 29 páginas, se encuentras aspectos como normativa legal, controles de acceso, como hacer copias de seguridad, actualizaciones de los sistemas, configuración de redes de forma óptica, registro y monitorización de actividades entre otras.

La importancia de la ciberseguridad en el ámbito empresarial es doble. Por un lado, tienen que implementar los sistemas necesarios para evitar interrupciones o caídas en sus sistemas informáticos debido, por ejemplo, a cualquier ataque DoS. Y, por otro lado, intentar mantener todos sus datos a salvo, manteniendo su integridad, confidencialidad y disponibilidad de estos. Para ambos casos, la cantidad monetaria que hay en juego es muy importante, además de las posibles acciones legales que pueden tener como repercusión.

### CIBERSEGURIDAD APLICADA AL MUNDO INDUSTRIAL

El mundo industrial y eléctrico tiene varios pilares críticos fundamentales, y la ciberseguridad es uno de ellos. Con la ciberseguridad, fiabilidad y reducción de tiempo de inactividad en caso de fallo en los sistemas. En un principio, la idea principal de las empresas era la búsqueda de la manejabilidad y efectividad de los sistemas, dejando de lado el tema de la seguridad. Con el paso del tiempo, las empresas cambiaron su enfoque, evolucionando a una visión más defensiva de estos sistemas. Debido a la globalización y evolución de los sistemas, las empresas fijaron unos estándares de seguridad con el fin de proteger de mejor manera sus sistemas industriales. La protección se basa en los siguientes objetivos mediante lo que se conoce como triada CID:

* **Confidencialidad**. Sinónimo de privacidad. Esta consiste en la protección de la información frente a personas no autorizadas para su obtención y visualización. Es decir, evitar que personas no autorizadas a ver esa información, puedan llegar a obtenerla sin el acceso requerido. Para obtener confidencialidad, se aplican varios métodos, que son los siguientes:
  + **Cifrado de datos**
  + **Tokens de seguridad**
  + **Doble autenticación**
* **Integridad.** Búsqueda de la precisión, exactitud y validez de la información. Esto quiere decir que personas ajenas puedan llegar a modificar la información a la que no deberían ser capaces de acceder provocando así alteraciones en los datos para su beneficio. Para ello, se puede usar el control de versiones de la información.
* **Disponibilidad.** Garantizar el acceso a ese sistema/sistemas a cualquier hora y día. Es decir, prevenir ataques de denegación de servicio que puedan impedir el normal funcionamiento de los sistemas. Para su prevención, es vital el mantenimiento habitual del sistema, así como tenerlo actualizado a las últimas versiones.

En el ámbito industrial y eléctrico, los tres pilares son importantes, pero al que más importancia se le da es a la disponibilidad de los sistemas. Algunas empresas eléctricas, han implantado un tipo de modelo de defensa para sus sistemas. Se conoce como “Defensa en profundidad”. Este modelo consta de la implementación de una pirámide con diferentes capas de seguridad, asegurando que si aluna capa no detecta cualquier tipo de anomalía, la siguiente lo haga. Encubriendo así la información en lo más alto de la pirámide para que sea más difícil poder acceder a la misma, teniendo que saltarse 6 capas previas para acceder a los datos.

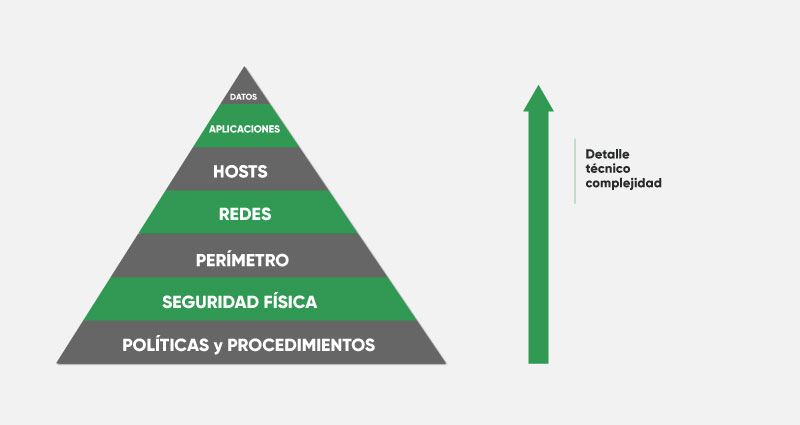


Ilustración 5.10. Logotipo IEC. (Fuente: <http://www.seguridadepm.com/iec> )

## ESTÁNDAR IEC 61850

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

**I**nternational **E**lectrotechnical **C**omission, es el significado de las siglas correspondientes a **IEC**, la cual se define como una organización de normalización de los campos electrónicos, eléctricos y tecnologías relacionadas. Esta organización de estándares se fundó en el año 1906 en la ciudad británica de Londres a raíz de la primera reunión del Congreso Eléctrico Internacional surgido en el año 1881 en la que se acordó desarrollar un sistema internacional de unidades de medidas eléctricas y magnéticas. Hoy en día, la sede actual está ubicada en la ciudad suiza de Ginebra.



Ilustración 5.11. Logotipo IEC. (Fuente: <http://www.seguridadepm.com/iec> )

Este organismo se encarga de promover entre sus miembros la cooperación internacional en todas las áreas de la normalización electrotécnica. En la actualidad, este organismo cuenta con 88 miembros en total, 62 de ellos miembros plenos, y los 26 restantes son miembros asociados. Con el objetivo prioritario de normalizar todos los campos de la electrotécnica, desde el área de potencia eléctrica, hasta áreas de comunicaciones, electrónica, nuclear, solar o eólica.

Podemos definir el IEC 61850 como el estándar que se encarga de definir los protocolos de comunicación entre diferentes equipos ubicados en las subestaciones eléctricas. Define la comunicación entre equipos de 3 distintos tipos:

* Equipos de protección
* Equipos de control
* Equipos de medición

Los equipos de protección abarcan un gran número de dispositivos que van desde disyuntores hasta transformadores de corriente, fusibles de protecciones o celdas de protección. Con respecto a los equipos de control, el más importante y conocido es el SCADA o HMI (**H**uman **M**achina **I**nterface), que será la parte principal de control de los elementos de la subestación. Y por último tenemos los equipos de medición, donde se agruparan e mayor parte lo que se conoce como IED (Intelligent Electronic Device).

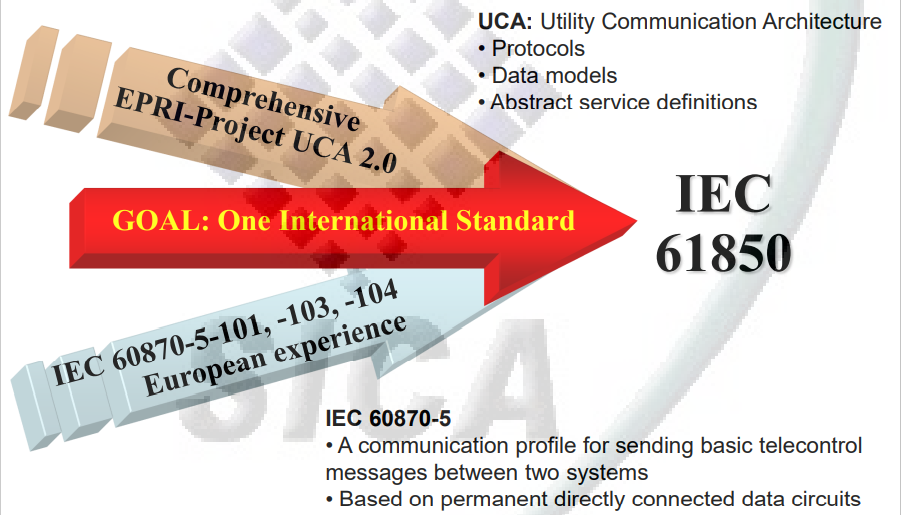


Ilustración 5.12. Resumen IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

#### SUBESTACIÓN ELECTRICA

Para poder comprender correctamente el estándar IEC 61850, es necesario saber que es una subestación eléctrica, así como cuál es su finalidad. Se podría definir subestación eléctrica como aquella instalación cuyo objetivo es la distribución de electricidad modificando los niveles de tensión necesarios para su distribución. Una subestación está compuesta de distintos sistemas, como transformadores, interruptores o protecciones, los cuales desarrollan un papel importante en el mantenimiento y operación de una subestación.



Ilustración 5.13. Imagen subestación eléctrica (Fuente: https://www.tecsaqro.com.mx/wp-content/uploads/2021/05/seguridad\_subestacion\_electrica.jpg)

### ORÍGENES DEL ESTÁNDAR IEC 61850

A finales del año 1994, un grupo de ingenieros de IEEE y del IEC, diseñó lo que hoy conocemos como IEC 61850. Esto fue como respuesta a la creación y desarrollo de la Generación de Energía Distribuida (DER) y de las microgrid. La necesidad de la creación de un canal de datos bidireccional y de una automatización casi total por parte de la estandarización, fueron los principales motivos, además de la necesidad de conseguir interoperabilidad entre dispositivos de distintos fabricantes, así como la búsqueda de la seguridad de las infraestructuras correspondientes. Pero hasta finales del año 2005 no se pudo publicar oficialmente debido a que faltaba la aprobación de alguna de ellas.

Con anterioridad al estándar IEC 61850, se encontraban otros como IEC60870, Profibus o DNP3 que satisfacían la necesidad de adecuada en el tiempo pasado. El problema vino con el paso del tiempo y la evolución y mejora del modelo eléctrico, además de numerosos cambios legislativos, los cuales exigían una posible interoperabilidad entre los distintos elementos eléctricos.

Con la puesta en marcha del IEC 61850, se consiguió una flexibilidad nunca vista en un ESTÁNDAR eléctrico. El IEC 61850 usa por defecto Ethernet, TCP/IP, y Manufacturing Message Specification (MMS) pero la ventaja de este mismo es que todos ellos se pueden sustituir por el que sea adapte mejor a las necesidades exigidas. Como ya se comentó anteriormente, el estándar IEC 6850 resolvió todos los problemas de interoperabilidad de sistemas/maquinaria de distintos fabricantes, aglutinando todos estos estándares para que puedan ser usados a gusto de cliente. Antes de esto, cada fabricante tenía su protocolo propietario y solo era válido para aquellos equipos que fueran pertenecientes a esa misma empresa.

### ESTRUCTURA DEL ESTÁNDAR IEC 61850

El estándar IEC 61850 se divide en 10 capítulos, alguno de ellos con varios subcapítulos en su interior. Los 10 capítulos, son los siguientes:

1. Introducción y visión general.
2. Glosario.
3. Requerimientos generales.
4. Sistema y administración del proyecto.
5. Requisitos de comunicación para funciones y modelos de dispositivos.
6. Lenguaje de descripción de configuraciones para comunicaciones en subestaciones eléctricas relacionadas con IEDs.
7. Estructura básica de comunicación.
   1. Estructura básica de comunicación para equipos de subestaciones y equipos de alimentación- Principios y modelos.
   2. Estructura básica de comunicación para equipos de subestaciones y equipos de alimentación- Interfaz de servicio de comunicación (ACSI).
   3. Estructura básica de comunicación para equipos de subestaciones y equipos de alimentación- Clases de datos comunes.
   4. Estructura básica de comunicación para equipos de subestaciones y equipos de alimentación- Clases de nodos lógicos y clases de nodos compatibles.
8. Mapeo de servicios de comunicación específicos (SCSM) – Asignaciones a MMS.
9. Servicios específicos de comunicación.
   1. Servicio específico de comunicación (SCSM) -Valores muestreados a través de un enlace “point to point” multipunto unidireccional y en serie.
   2. Servicio específico de comunicación (SCSM)- Valores muestreados sobre ISO/IEC 8802-3.
10. Pruebas de conformidad.

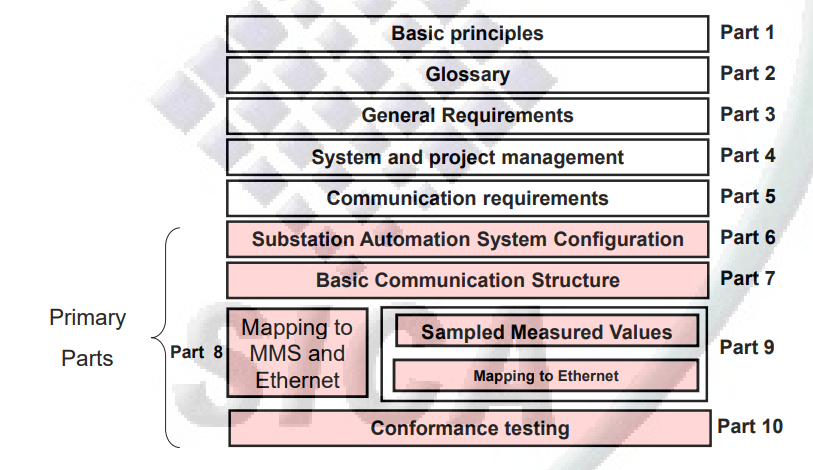


Ilustración 5.14. Capítulos IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

### PRINCIPALES CARACTERISTICAS Y BENEFICIOS DEL ESTÁNDAR IEC 61850

Como ya sabemos, la elaboración de este ESTÁNDAR es un gran avance en el ámbito eléctrico para todos. El objetivo es mejorar la automatización de las subestaciones eléctricas y para ello la Comisión Electrotécnica Internacional, diseñó este ESTÁNDAR con las siguientes características que se adecuan con el fin de conseguir el principal objetivo:

* Estandarización de nombres y estructura de datos.
* Definición de un protocolo de comunicaciones unificado. Considera todas las necesidades de comunicación de una subestación.
* Mapeo de datos de IEDs único y universal excluyendo la procedencia del mismo.
* Estandarización de formatos de ficheros de configuración, basado en el lenguaje XML.
* Definición de un bus de procesos
* Fácil configuración, diseño óptimo y rápida y fácil puesta en marcha del mismo.
* Comunicaciones horizontales
* Reducción de costes a largo plazo.
* Implementación como un sistema distribuido, esto significa más eficacia contra los fallos.
* Implementación de una comunicación que se basa en mensajes digitales fiables y rápidos
* Unificación de ficheros de configuración, SCL.
* Comunicación posible entre equipos de distintos fabricantes
* Eficiencia económica y mayor rentabilidad económica
* Representación de los datos orientada a objetos
* Jerarquía y arquitectura fácil de entender y visualizar

### ARQUITECTURA DEL ESTÁNDAR IEC 6850

La comisión IEC, decidió establecer tres niveles distintos, **Nivel de proceso** (Process Level), **nivel de bahía** (Bay Level) y **nivel de estación** (Station Level).

* **Nivel de proceso (“*Process Level*”).** Este es el nivel más inferior de una subestación eléctrica que use el ESTÁNDAR IEC 61850. En él, se encuentras los equipos eléctricos de maniobras. Los cuales pueden ser **dispositivos de computación**, como interruptores, o **dispositivos de instrumentos**, como son los transformadores o los **transformadores de voltaje**.
* **Nivel de Bahía (“*Bay Level*”).** En este nivel de la arquitectura, conocido como el nivel intermedio, se encontrarán lo que se conoce en la actualidad como **IED** (Intelligent Electronic Device) o en español, dispositivo electrónico inteligente. Los IEDs es el nuevo nombre que se le ha dado a todo aquel dispositivo que contiene uno o varios procesadores y es capaz de reflejar las capacidades que posee para la toma de decisiones basadas en la lógica y en la información recopilada de los dispositivos de nivel de proceso. Un IED es capaz de ejecutar el comportamiento de uno o varios nodos lógicos, y suele tener un reloj interno que proporciona sincronización horaria. Ejemplos de IEDs, serian contadores electrónicos o relés.
* **Nivel de estación (“*Station Level*”).** El nivel más alto de la arquitectura de una subestación eléctrica que use el IEC 61850, se le conoce como nivel de estación o “Station Level”. En este nivel podemos encontrar dos elementos básicos: un SCADA y un HMI. **SCADA** cuyas siglas significan **S**upervisory **C**ontrol **A**nd **D**ata **A**cquisition y **HMI** **H**uman **M**achine **I**nterface, son usados para el control y monitorización de una subestación.

La comunicación entre los elementos de los distintos niveles se realiza mediante la implementación de buses. Tenemos dos tipos de buses, bus de procesos y bus de estación.

* El bus de procesos se encarga de comunicar a los equipos pertenecientes al nivel de proceso con los IEDs del nivel de bahía (“**Process Bus**”). El bus de procesos implementado por el estándar IEC 61850 permite la comunicación entre los IEDs y los interruptores y transformadores.
* Por el otro lado, nos encontramos con el bus de estación. Las comunicaciones entre en nivel de bahía y el nivel de estación se realizan a través del bus de estación (”**Station Bus**”).

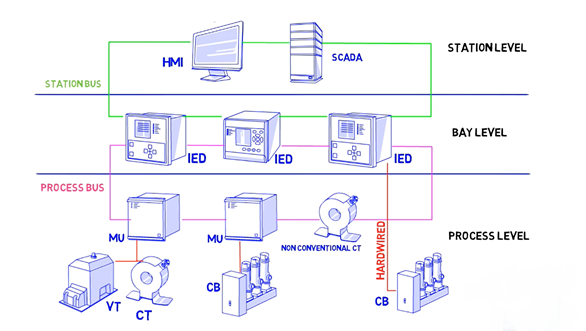


Ilustración 5.15. Arquitectura ESTÁNDAR IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

### MODELOS DE COMUNICACIÓN DEL ESTÁNDAR IEC 61850

Antes de empezar a describir los protocolos de comunicación del estándar IEC 61850, es necesario hacer un breve resumen sobre la estructura del protocolo de Internet. Esto ayudará a comprender mejor los protocolos de comunicación usados por el IEC 61850.

Internet está basado en 4 capas fundamentales (denominado modelo TCP/IP), lo que quiere decir que hay 4 niveles de servicios independientes para entregar la información. Las capas son las siguientes:

* **Capa de aplicación (“Application Layer”).**

La capa superior es la conocida como capa de aplicación. Usa un simple comando para transferir datos de un punto a otro. Por ejemplo, la aplicación World Wide Web (**www**), es usado por todos los navegadores de internet para acceder al contenido de las páginas web.

* **Capa de transporte** (“Transport Layer”).

Justo debajo de la capa de aplicación, se encuentra la capa de transporte. Cuyo objetivo es chequear que la información ha sido entregada satisfactoriamente.

* **Capa de red** (“Network Layer”).

La segunda capa en discordia es la capa de red. Es la encargada de permitir que los datos satén a una red local distinta a través del router.

* **Capa de enlace** (“Link Layer”).

La capa inferior, se conoce como capa de enlace. Es la encargada de transferir la información local a través de los distintos switches.

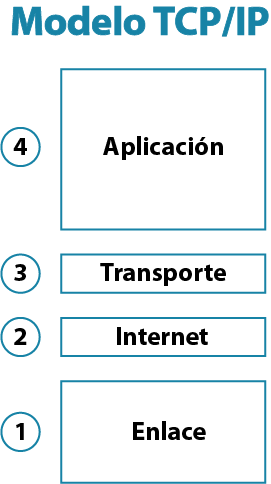


Ilustración 5.16. Capas modelo TCP/IP (Fuente: <https://elprofealegria>.com/redes/modelo-tcp-ip/)

El estándar IEC 61850, desarrolló dos modelos básicos de comunicaciones en los que se basan los protocolos de comunicación desarrollados en el estándar IEC 61850. Estos son los siguientes:

* **Two-Party-Application-Association** (TPAA).

Es un modelo de comunicación basado en cliente-servidor. Para iniciar una comunicación, el cliente envía un paquete de asociación, al cual el servidor responde si autoriza esa nueva comunicación. Una vez establecida esa comunicación, se comienza con el flujo de envío de datos. El cliente solicita unos determinados datos al servidor, y este se los envía. Estos paquetes llevan un campo de confirmación para saber que lo ha recibido. Para finalizar la comunicación, el cliente envía la solicitud al servidor y este se la devuelve y cierra la comunicación establecida previamente.

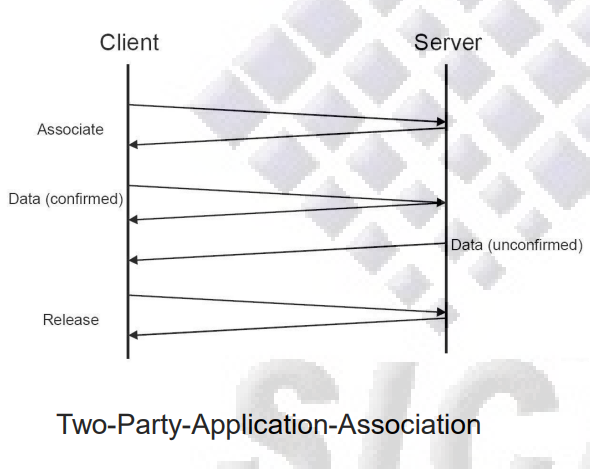


Ilustración 5.17. Two-Party-Application-Association (Fuente: propia)

* **MULTICAST-Application-Association** (MCAA)

Este modelo de comunicación está basado en la arquitectura publicador-suscriptor. Como podemos ver en la figura 5.18**,** puede haber uno o varios suscriptores suscritos a un mismo publicador. Cada suscriptor/cliente se puede suscribir a tantos publicadores como desee. Cuando el publicador tenga que notificar algún cambio, enviará ese paquete con el cambio a todos los elementos que se encuentran en esa red, pero solo lo procesaran aquellos clientes que estén suscritos a ese publicador. Ese es un método rápido de comunicación, usado para mensajes urgentes y de prioridad máxima. Los datos viajan sin confirmación de recepción alguna. El publicador publica el mensaje en la red, y aquellos suscriptores que este escuchando lo recibirán y procesarán.

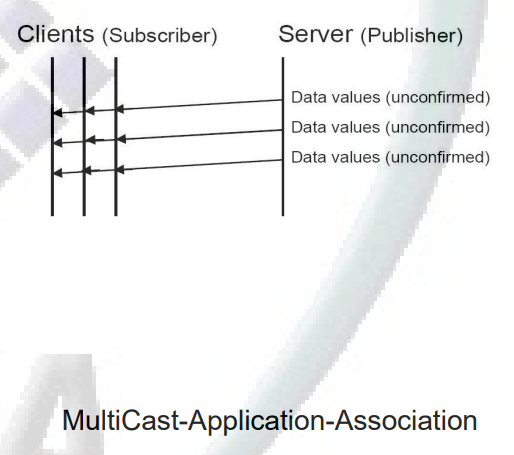


Ilustración 5.18. MultiCast-Application-Association (Fuente: propia)

El estándar IEC 61850, ha definido tres protocolos distintos de comunicación para tres aplicaciones distintas. Son las siguientes:

* **Manufacturing Message Specification** (MMS).

El primero y más usado es el MMS. Definido en la ISO 9506. Es un protocolo de comunicación cliente-servidor. Se caracteriza por establecer una comunicación privada y segura a tiempo real. El proceso de establecimiento de comunicación es bastante sencillo. El cliente envía una “request” al servidor. Una vez recibida, el servidor le envía de vuelta una “response” y ya se habría establecido la comunicación entre ambos.

Usado para establecer comunicación entre IEDs y sistemas SCADA, para hacer reportes o enviar instrucciones de control.

* **GOOSE (Generic Object-Oriented Substation Event).**

GOOSE se encuentra dentro del protocolo de comunicación Generic Substation Event (GSE). GSE posee dos tipos de mensajes: Mensajes Generic Substation State Event (**GSSE**) y los mensajes GOOSE.

Por un lado, tenemos los mensajes GSSE, que proporcionan la capacidad de transmitir los cambios de estado de información (en pares de bits). Estos han quedado anticuados y apenas se usan hoy en día.

Y por el otro, tenemos los mensajes GOOSE. Estos mensajes son usados para enviar mensajes urgentes entre IEDs. Permiten llevar una gran cantidad de datos organizados en lo que se conoce como data-set. GOOSE, está directamente conectado con la capa de enlace, lo que permite entregar de forma rápida la información en unos 3 milisegundos. A esto se le denomina un protocolo de tiempo real.

El mecanismo de comunicación es bastante intuitivo. Es un mecanismo basado en la comunicación entre publicador-suscriptor. El publicador se identifica como el que genera y publica el mensaje en la red, y suscriptor, el que quiere ver todos los mensajes de un determinado publicador.

El publicador transmite el mensaje a toda la red local. Y los dispositivos que estén suscritos (que estén escuchando), recibirán el mensaje GOOSE.

* **Sampled Measured Value** (SMV).

SMV está directamente conectado con la capa de enlace y usa también mecanismos de publicador-suscriptor. Este protocolo permite enviar corriente y voltaje de forma digital a través del bus de procesos a través de un instrumento digital o una “merge unit”. Esta “merge unit” se encarga de transponer la señal analógica a una señal digital, un valor discreto etiquetado con tiempo sincronizado.

Ese voltaje y medida de corriente pueden ser usados por cualquier IED el cual requiera esa información. Todo ello sin cableado adicional, solo con el uso del bus de procesos, el cual necesita el suficiente ancho de banda para poder soportar ese gran flujo de información. SMV soporta 2 métodos distintos de transmisiones, que son las siguientes:

* + “*Multicast service over Ethernet*” (MSVC).

Hace uso del modelo de comunicación Multicast-Association-Application. El cual el valor del voltaje medido es enviado a todos los elementos, siendo procesado únicamente por aquellos que estén suscritos.

* + “*Unicast service over serial links”* (USVC).

Como el propio nombre indica, está basado en el modelo de comunicación Unicast-associaton-application. Se establece una conexión peer to peer entre cliente y servidor. Los datos son confirmados a su recepción y es un modelo de transmisión más lento que el anterior.

### MODELADO DE DATOS DEL ESTÁNDAR IEC 61850

El estándar IEC 61850 elaboró un modelado de datos orientado a objetos. Simplificando el modelaje y la interoperabilidad entre los distintos elementos de una subestación. Como podemos en la figura inferior, el modelado de datos se establece en torno a un “*Physical Device*” (Dispositivo Físico). Esto lo que quiere decir es que cada dispositivo físico presentara la misma estructura de datos, cambiando sus valores y especificaciones.

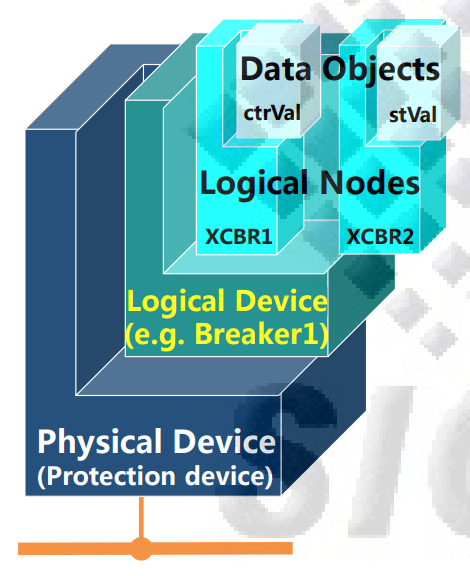


Ilustración 5.19. Estructura de datos del ESTÁNDAR IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

Los tipos de datos que se encuentran dentro de un dispositivo físico, son los siguientes:

1. **Dispositivo Lógico** (“Logical Device”, LD). Está formado por un conjunto de nodos lógicos que están implementados en un IED, es decir de forma no distribuida. Un dispositivo físico puede estar formado por uno o más dispositivos lógicos, por lo que pueden estar formados por un número elevado de nodos lógicos.
2. **Nodos Lógicos** (“Logical Node”, LN). Cada nodo lógico se puede definir como una pequeña parte de una función que intercambia datos. Un nodo lógico es un objeto definido por sus datos y métodos. Como ejemplo de nodos lógicos podemos incluir en la lista los interruptores, protecciones o sensores.

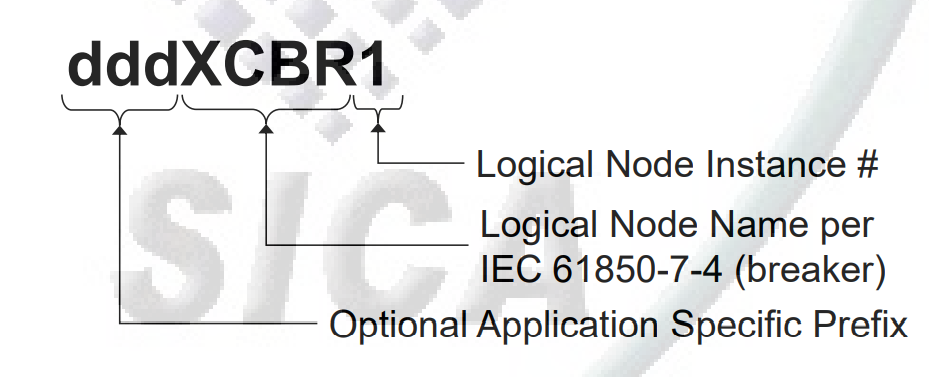


Ilustración 5.20. Nomenclatura de un Logical Node (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

A la hora de representar todos los nodos lógicos, la estructura es siempre la misma ya que está todo unificado. Como podemos ver en la figura 5.20**,** un ejemplo de nomenclatura de un nodo lógico puede ser la siguiente: dddXCBR1. Las tres primeras letras, representan el prefijo específico de aplicación opcional. En segundo lugar, tenemos XCBR, que se corresponde con el nombre del nodo lógico dado por el estándar IEC 61850. En este caso XCBR significa que es un interruptor. Y por último encontraremos un número, en este caso es el 1, este se corresponderá con el número de instancia del nodo lógico.

1. **Objetos de datos** (“Data Objects”). En este nivel de la pirámide, se encuentran todas las propiedades de los nodos lógicos. Como por ejemplo la posición de un dispositivo.
2. **Atributo de los datos** (“Data Attribute”, DA). Lo componen los atributos y especificaciones que se encuentran en los objetos de datos. Las características de los datos y sus atributos son las siguientes:

* Estructura y semántica bien definida
* Configuración: asignación de valores seleccionados y mecanismos de intercambio

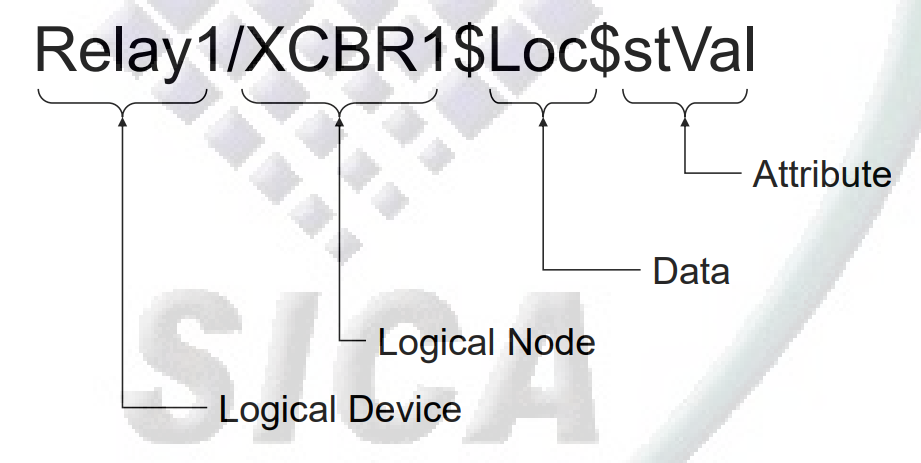


Ilustración 5.21. Nomenclatura de un objeto (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

Por otro lado, tenemos la estructura de instanciación de un objeto en el estándar IEC 61850. Como se puede apreciar en la figura 5.21**,** la estructura es idéntica a la de los nodos lógicos. En primer lugar, aparecerá en nombre del dispositivo lógico, en este caso Relay1 (que significa relé 1).Seguido de un “/”, podremos encontrar el nombre que identificará al nodo lógico. En este caso, como en la figura anterior, es XCBR1. Seguido del símbolo “$”, encontraremos el nombre del dato y seguido de este el atributo, en este caso stVal, que significa “Status Value” que traducido al español nos queda valor de estado.

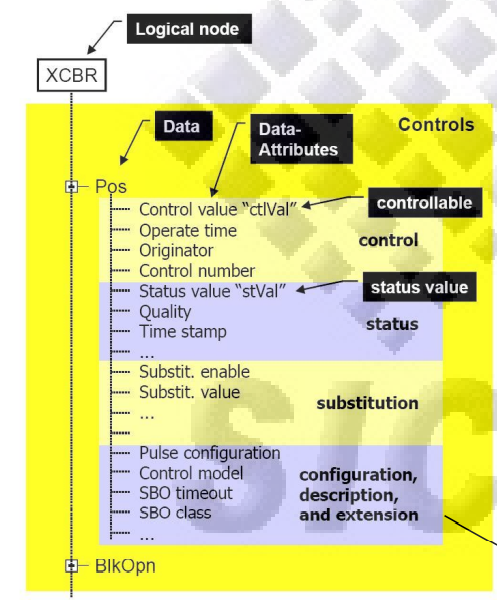


Ilustración 5.22. Jerarquía datos de un dispositivo lógico en el protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

### LENGUAJE DE CONFIGURACIÓN DE UNA SUBESTACION

Este lenguaje de configuración, también conocido como Substation Configuration Language (SCL), permite crear archivos de descripción y configuración de dispositivos de subestaciones. Está basado en el lenguaje de programación XML y permite el intercambio de información entre los distintos dispositivos de una subestación. En ellos, se incluyen descripciones de los modelos de los dispositivos, la infraestructura de comunicación y la relación con el sistema de energía.

Este lenguaje permite la creación de cuatro archivos SCL distintos, necesarios para poder definir una subestación con el estándar IEC 61850. Son los siguientes:

* **Substation Description** (.SSD)

El primer paso para comenzar a implementar este lenguaje en las subestaciones es la creación del archivo .SSD. Estos archivos contienen la “traducción” de un diagrama de una sola línea (single line diagram) a un archivo .SSD.

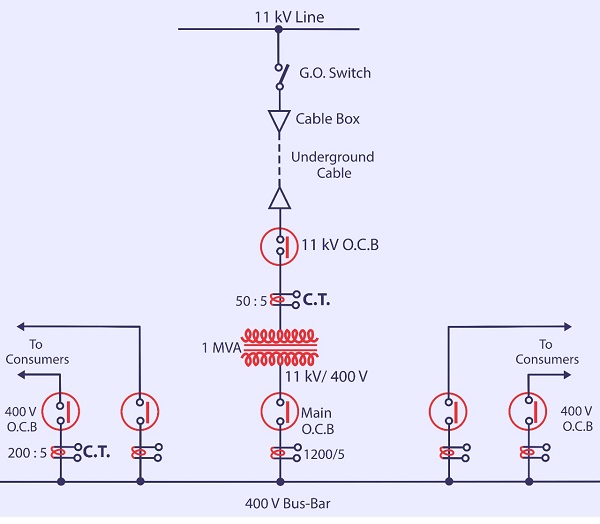


Ilustración 5.23. Ejemplo de un diagrama de una sola línea (single-line diagram) (Fuente: <https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation> )

* **IED Capability Description** (.ICD)

El segundo paso es la creación de los archivos .ICD. En cada uno de ellos se recoge una autodescripción de las capacidades de cada IED. Para aquellos IEDs que poseen el mismo conjunto de funciones, usaran el mismo archivo .ICD. Pero no compartirán en ningún caso el archivo .CID. Cada IED tendrá su propio archivo .CID independientemente de sus características y funciones.

* **Substation Configured Description** (.SCD).

El tercer paso en discordia es la elaboración del archivo .SCD. Para la elaboración de este, se usan los dos archivos previamente nombrados, el .ICD y el .SSD.

* **Configured IED Description** (.CID).

La creación de un .CID, viene dada a través de un archivo .SCD. Consiste en extraer de un archivo .SCD, la configuración de un IED, obteniendo así un archivo individual para cada IED con la configuración de cada uno. Este archivo es cargado en cada IED respectivo para establecer automáticamente su configuración previamente configurada en el archivo .CID.

Tanto los archivos .SCD como los .CID poseen una estructura bien marcada, compuesta por 4 partes delimitadas en las que se recoge toda la información y configuración. Recordando siempre que estos archivos están programados en el lenguaje XML. Esas 4 partes son las siguientes:

* “**Header**”.

En este apartado, se introducen los datos sobre la fuente del documento. Versión usada, ID de la herramienta y estructura del nombre son los datos básicos de este apartado.



Ilustración 5.24. Header de un archivo .SCD (Fuente: propia )

* “**Comunicación**”.

Se encuentra toda la información relacionada con redes de comunicación. Se define la subred y los puntos de acceso. Se establece la IP que el IED tendrá una vez funcionando en una red. Y se establece el puerto que el cliente quiera para el servicio del protocolo de comunicación MMS.

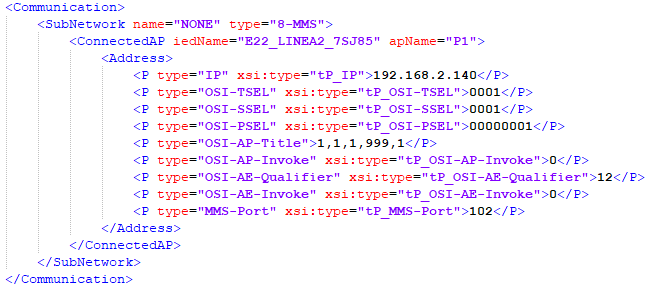


Ilustración 5.25. Communication de un archivo .SCD (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

* “**IED name**”.

Además de establecer el nombre del IED, se define los servicios de comunicaciones, así como los Logical Devices y Logical Nodes del propio IED.



Ilustración 5.26. IED name de un archivo .SCD (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

* “**DataTypeTemplates**”

En este último apartado, se describen definiciones completas de los Logical Nodes, Data Objects y Data Types.

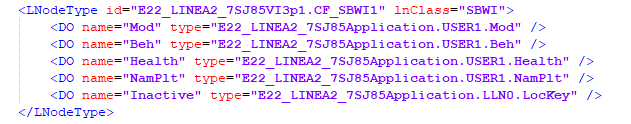


Ilustración 5.27. DataTypeTemplate de un archivo .SCD (Fuente: propia)

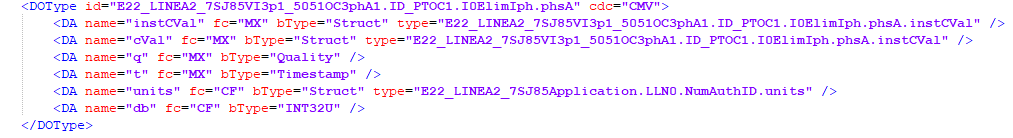


Ilustración 5.28. DataTypeTemplate de un archivo .SCD (Fuente: propia)

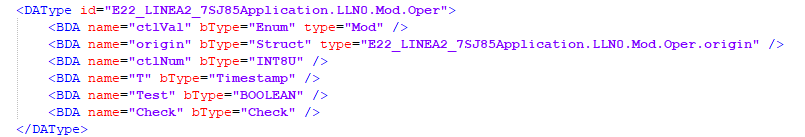


Ilustración 5.29. DataTypeTemplate de un archivo .SCD (Fuente: propia)

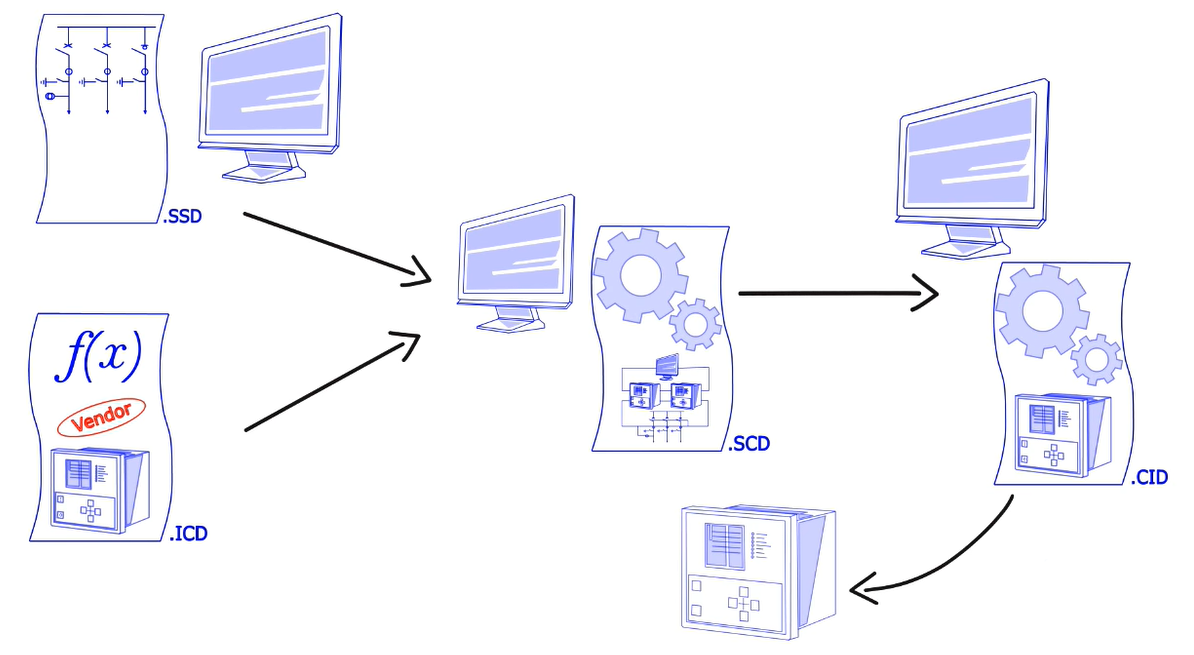


Ilustración 5.30. Resumen archivos de configuración del estándar IEC 61850 (Fuente: Propia )

## VIRTUALIZACIÓN DE INTELLIGENT ELECTRONIC DEVICE CON IED SCOUT

Como ya se describió anteriormente en el capítulo de “Tecnologías Usadas”, la herramienta IED Scout nos permite virtualizar el funcionamiento y comunicación de IEDs. Para poder hacerlo, es necesario disponer de un archivo .CID o .SCD que aglutine toda la información necesaria de un IED. Para la realización de este proyecto, fueron usados dos archivos diferentes, uno denominado “E15\_BARRAS\_INGEPAC” de tipo .SCD y otro “E22\_LINEA2\_7SJ85” de tipo .CID. El archivo “E15\_BARRAS\_INGEPAC.scd” tiene asignada de manera manual la IP 192.168.2.141 y el archivo E22\_LINEA2\_7SJ85.cid la 192.168.2.140. Para cambiar la IP que se quiera asignar a determinado IED, solamente es necesario abrir el archivo con el Notepad o cualquier aplicación de edición de textos, y cambiar la IP por la que el usuario quiera.

Texto, Carta

Descripción generada automáticamente

Ilustración 5.31. Parte del archivo .CID donde se cambia la IP (Fuente: Propia )

La idea principal era, una vez instalada y configurada la herramienta IED Scout, cargar uno de los dos archivos mencionados anteriormente (a elegir, es indiferente uno u otro) e iniciar la simulación del IED. Es decir, simular que en nuestra red hay un IED (real), con su nombre y su IP. Una vez que se tiene corriendo de forma virtualizada ese IED, se hace uso de la herramienta Advanced IP Scanner para poder observar que en esa IP tenemos ese IED corriendo. Finalmente, se establecerá mediante otro host que tenga la herramienta IED Scout instalada y configurada una comunicación entre cliente y servidor, estableciendo una comunicación mediante el protocolo MMS.

Se describirán en primer lugar los pasos a seguir en el PC-Publicador y posteriormente en el PC-Suscriptor.

La configuración de IED Scout en el PC-Publicador es sencilla. El primer paso será iniciar la aplicación. Una vez que aparezca la pantalla principal, se clicará sobre la **opción “Simulator”.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 5.32. Opción “Simulator” de la herramienta IED Scout (Fuente: Propia )

El siguiente paso es **cargar el archivo .SCD o .CID** en la herramienta. Para ello, se hará clic sobre la opción “Open SCL” y se seleccionará el archivo deseado. Para el desarrollo de la práctica se eligió el “E22\_LINEA2\_7SJ85” el cual tiene asignada la IP 192.168.2.140.

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Ilustración 5.33. Selección de archivo para su virtualización en IED Scout (Fuente: Propia )

Tras unos segundos, aparecerá toda la **arquitectura de datos** de ese IED en la pantalla, y habrá que comenzar a virtualizarlo.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 5.34. Estructura de los datos del IED “E22\_LINEA2\_7SJ85” en IED Scout (Fuente: Propia )

Para comenzar a virtualizarlo, se **seleccionará** la opción **“Start”.** El comienzo de la virtualización tardará unos segundos, una vez finalizado el inicio de la virtualización, ya se tendrá el IED virtual corriendo en la red determinada y con la IP asignada previamente.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 5.35. Pestaña para comenzar la simulación del IED “E22\_LINEA2\_7SJ85” (Fuente: Propia )

Puesto que ya se tiene configurado y corriendo el IED “E22\_LINEA2\_7SJ85” en el PC-Publicador, ahora solo queda el PC-Suscriptor. Para poder establecer una comunicación con el PC-Publicador, se realizarán 3 pasos en el PC-Suscriptor:

* **Iniciar la herramienta IED Scout**.

Consiste únicamente en ejecutar la aplicación previamente instalada e esperar hasta que se inicie automáticamente.

* **Seleccionar la opción de “Browser”.**

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 5.36. Interfaz de la opción “Browser” dentro de IED Scout (Fuente: Propia )

* **Seleccionar la IP del IED virtualizado en el PC-Publicador para establecer una conexión**.

Únicamente se necesitará saber la IP que se estableció en el IED para poder conectarnos a él desde cualquier parte de la red. Esto permite que cualquier usuario de la red que conozca esa IP, tenga acceso total a establecer una conexión con el IED.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ilustración 5.37. Pestaña “Discover” para buscar el IED previamente virtualizado (Fuente: Propia )

Una vez establecida la conexión, existen varias formas de captar ese tráfico entre ambos PC. Wireshark y IEDScout son las principales.

* **Wireshark.**

Como se describió en el capítulo de “Tecnologías Usadas”, Wireshark es un sniffer de paquetes de red el cual permite ver lo que esta pasando en la red. Como se sabe, el estándar IEC 61850 usa el protocolo MMS, entre otros.

Para poder el trafico entre el PC-Suscriptor y el PC-Publicador, valdrá únicamente con que se introduzca en los filtros de Wireshark la IP del IED. En este caso, el filtro sería el siguiente: “**ip.addr == 192.168.2.140**”.

Wireshark captará únicamente aquellos paquetes de red los cuales contengan ya sea la IP origen o la de destino igual a 192.168.2.140. Como se puede observar, se detectan 3 tipos de protocolos. TCP y COTP, por el lado de capa de transporte, y MMS por el lado de la comunicación. Esto quiere decir que el IED esta enviando al PC-Suscriptor toda la información del IED, para poder cargarla en su sistema y trabajar posteriormente con ese IED.

Captura de pantalla de computadora

Descripción generada automáticamente

Ilustración 5.38. Resultados de filtrado de paquetes en Wireshark con “ip.addr == 192.168.2.140” (Fuente: Propia )

* **“Sniffer”** **de** **IED Scout.**

Por otro lado, se tiene el sniffer de IED Scout. La herramienta IED Scout además de virtualizar IEDs, también permite la captación del tráfico de la comunicación entre los IEDs que está virtualizando. Para ello tiene la opción de “Sniffer”. Esta opción es preferible a la de Wireshark, ya que muestra con una descripción el contenido de cada paquete. Esto facilita al usuario entender el proceso de comunicación y ver en que estado esta la comunicación entre ambos.

Como se puede ver en la figura 5.39, el “sniffer” se centra únicamente en mostrar la IP origen y destino, la hora del envío del paquete y el contenido de cada paquete, por lo que es mas manejable que Wireshark. El primer paquete mostrado en el sniffer, es la petición de asociación hecha por el PC-Suscriptor al PC-Publicador. A partir de ahí, el PC-Publicador comenzará a transmitir los datos y valores al PC-Suscriptor.

Interfaz de usuario gráfica, Aplicación, Word

Descripción generada automáticamente

Ilustración 5.39. Paquetes capturados por el Sniffer de IED Scout (Fuente: Propia )

## IMPLEMENTACIÓN DE NOZOMI GUARDIAN PARA MONITORIZACIÓN DE IEDs

Una vez establecida la comunicación entre PC-Publicador y PC-Suscriptor desarrollada en el apartado previo, el siguiente y último paso sería la introducción de una herramienta de monitorización que controle todo el tráfico de la red local en cuestión, en este caso será Nozomi Guardian.

Nozomi Guardian es una herramienta de monitorización de pago, es decir se necesita una licencia la cual se obtiene pagando una determinada cantidad monetaria o registrándose en su página web y obteniendo una versión gratuita de prueba de 30 días. Gracias a SICA S.A., se pudo obtener una licencia gratuita por un periodo limitado de un año y sin ninguna restricción de servicios.

### DESCRIPCIÓN DE LOS SERVICIOS BASICO DE NOZOMI GUARDIAN

La pantalla principal de Nozomi viene configurada por defecto con un diseño el cual aparece demasiada información. Nozomi da la oportunidad de diseñar tu propio diseño de panel principal con el fin de adaptarlo a las necesidades del usuario. Los aspectos importantes que se recogen en el panel principal son los siguientes: “Información del entorno”, “Rendimiento total de red”, “Últimas alertas” y “Flujo de alertas a lo largo del tiempo”. En el siguiente párrafo se describirá punto a punto lo que engloba cada una y por qué esa información si es relevante para el desarrollo del proyecto.

* **Información del entorno.**
  + **Activos.**

En la sección de activos, se mostrarán todos los dispositivos activos en la red en la que está colocada Nozomi. En esta sección es fácil visualizar, encontrar y desglosar la información de cada activo, así como las versiones de hardware y software.

Si se hace clic encima del recuadro, aparecerá la vista de activos. En esta página se enumeran todos los activos en formato de tabla. Si se vuelve a hacer clic sobre cualquier activo, una pestaña nueva aparecerá con información adicional sobre el activo seleccionado (ver ilustración 5.40).

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 5.40. Ventana con información adicional de un activo (Fuente: Propia )

En esta pestaña, las opciones de sesiones y alertas son las importantes. En la opción de sesiones, se puede ver todas las sesiones que ese activo tiene o ha tenido históricamente. Existen dos tipos de estado de sesiones: “Active” y “Closed”. Este estado indica si la sesión está activa en ese momento o si no lo está. Además, indica la IP origen y la IP de destino, que protocolo se está usando en esa sesión, el puerto de destino e información sobre bytes transferidos y detalles de fecha y hora de la primera y la última actividad.



Ilustración 5.41. Pestaña de sesiones de un activo en Nozomi Guardian (Fuente: Propia )

* + **Nodos**

Cada nodo representa lo que se puede denominar como un “actor” en la comunicación de la red. Dependiendo de la comunicación establecida y de los protocolos usados, un nodo puede representar desde a un ordenador personal hasta a un Programmable Logic Controller (PLC) o Remote Terminal Unit (RTU).

Captura de pantalla de computadora

Descripción generada automáticamente

Ilustración 5.42. Pestaña de un activo en Nozomi Guardian (Fuente: Propia )

* + **Enlaces**

Cada enlace representa la comunicación entre dos nodos usando un protocolo específico. En el caso de la figura 5.43, los dos enlaces disponibles son entre comunicaciones entre mismos dispositivos, pero una de ellas usa el protocolo MMS y la otra el COTP. Por lo que descrito anteriormente, se puede deducir que tanto la IP 192.168.1.121 como IP 192.168.2.140 pertenecen a un IED.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ilustración 5.43. Pestaña de un activo en Nozomi Guardian (Fuente: Propia )

* + **Protocolos.**

En el apartado de protocolos, Nozomi Guardian elabora un resumen de todos los protocolos usados en las comunicaciones de la red, y lo muestra en la ventana principal.

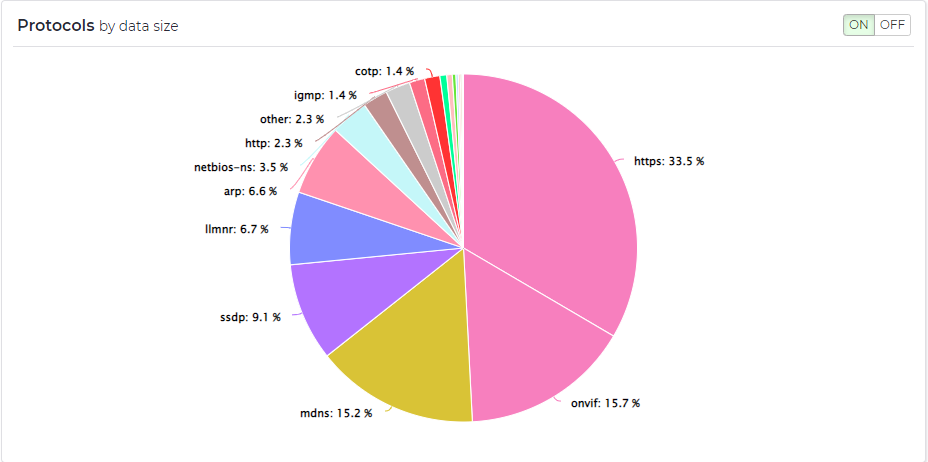


Ilustración 5.44. (Fuente: Propia )

* + **Sesiones**

Una sesión es un intercambio de información semipermanente entre dos o mas nodos. Cada sesión establecida puede llegar a involucrar más de un mensaje en ambas direcciones. Como se describió anteriormente en el apartado de ”Activos”, se destacan los dos tipos de sesiones. “ACTIVE” y “CLOSED” son los dos estados posibles de una sesión.

Una captura de pantalla de una red social

Descripción generada automáticamente

Ilustración 5.45. (Fuente: Propia )

* + **Variables**

Nozomi Guardian introduce una variable para cada comando usado, medida monitoreada o para cualquier información a la que un sistema SCADA accede o modifica.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Ilustración 5.46. Vista de proceso donde se muestran las variables monitoreadas en Nozomi Guardian(Fuente: Propia )

* **Rendimiento total de red.**

Mediante la elaboración de un gráfico que representa por un lado la cantidad de datos transferidos en la red y por otro la hora, Nozomi Guardian crea un resumen rápido y visual de la cantidad de datos que se están transmitiendo a través de la red estableciendo la variable de referencia de la hora. Gracias a ello se pude visualizar la evolución de los datos transmitidos con respecto a la hora.

Texto

Descripción generada automáticamente con confianza baja

Ilustración 5.47.(Fuente: Propia )

* **Últimas alertas.**

Todas aquellas alertas monitorizadas por Nozomi aparecerán en este apartado. Todas ellas vendrán ordenadas en una tabla, en la que se incluye el riesgo de la alerta, así como el nombre de la alerta, una descripción de la misma y la fecha y hora.

El riesgo de una alerta va desde 1 hasta 10. Relacionando 1 con una alerta de seguridad poco importante y 10 con una alerta muy importante.

* **Flujo de alertas a lo largo del tiempo.**

Al igual que anteriormente, Nozomi Guardian elaboraba un gráfico del rendimiento de red, con las alertas elabora el mismo gráfico. Para representar gráficamente la evolución de las alertas, establece por un lado la hora de la alerta, y por el otro el riego de cada alerta. A mayor riesgo de la alerta, la representación será con un pico más alto que una de riego menor.

### PANEL DE CONTROL DE SEGURIDAD DE NOZOMI GUARDIAN

Nozomi Guardian cuenta con sistema muy desarrollado de seguridad, el cual puede ser adaptado por el usuario como mejor le venga según sus necesidades. Para ello, en las opciones de configuración, aparece la opción de “**Panel de control de seguridad**”. Desde aquí, se realiza cualquier ajuste y configuración de las características que administran el “Aprendizaje”, “Perfil de seguridad”, “configuración de zonas”, “Ajustes de alertas” y “Opciones de cierre de alertas”, siendo importantes las dos primeras.

* **Aprendizaje.**

Nozomi Guardian proporciona dos tipos de métodos de detección: “Aprendizaje adaptativo” y “Aprendizaje estricto”.

Por otro lado, se tiene el “Cambio de fase”. Posee dos opciones: “Dinámico” o “Dos fases”. El dinámico funciona en torno a un rango de fechas en las que actuará Nozomi. Por el contrario, la opción de dos fases se divide en otras dos opciones:

* + **“Aprender”.**

Nozomi Guardian va incorporando nuevos comportamientos a medida que va aprendiendo. Si un usuario se conecta por primera vez con su ordenador a la red, Nozomi incorporará ese dispositivo a la jerarquía de la red y aprenderá de las comunicaciones establecidas por ese dispositivo.

* + **“Proteger”.**

Cada vez que el sistema de Nozomi Guardian detecte alguna anomalía sobre lo aprendido anteriormente, generará automáticamente una alerta sobre ello.

* **Perfil de seguridad.**

El perfil de seguridad permite cambiar la visibilidad de las alertas en función de su tipo. Existen cuatro tipos de perfiles distintos: “Bajo”, “Medio”, “Alto” y “Paranoico”.

Con el perfil bajo activado, solo aquellas alertas de nivel alto, serán generadas y notificadas por el sistema de Nozomi. Según aumentemos el tipo de perfil, Nozomi ira mostrando además de las alertas más altas, las de nivel medio. Y en modo paranoico todo tipo de alerta es mostrada por el sistema de Nozomi. Es recomendable el uso del perfil paranoico para la monitorización de sistemas críticos como puede ser cualquier IED.

### ANÁLISIS DE NOZOMI GUARDIAN

Dentro de la pestaña de “Análisis”, Nozomi Guardian ofrece cuatro servicios útiles para el usuario. “Consultas”, “Informes”, “Máquina del tiempo” y “Vulnerabilidades”

* **Consultas**

Nozomi Guardian permite realizar consultas usando N2QL(Nozomi Networks Query Language).

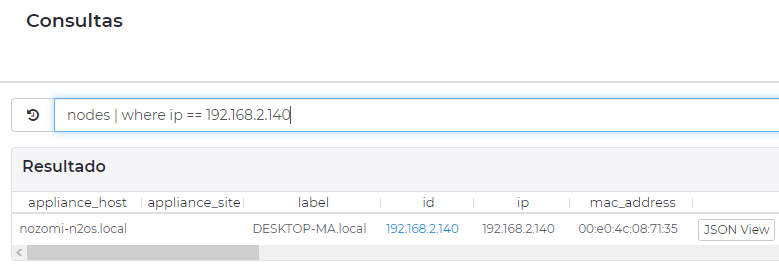


Ilustración 5.48. Consulta realizada en Nozomi Guardian (Fuente: Propia )

* **Informes**

En el apartado de informes, el usuario puede generar informes personalizados. Estos informes personalizados están basados en consultas y diseños personalizados.



Ilustración 5.49. Consulta realizada en Nozomi Guardian (Fuente: Propia)

* **Máquina del tiempo**

Otro de los servicios que nos incluyen la herramienta Nozomi Guardian, es “La máquina del tiempo”. Gracias a esta función, el usuario puede cargar un estado previamente guardado, el cual se denomina instancia y retroceder en el tiempo. Esto significa que Nozomi mostrará todos los datos que se guardaron en ese mismo instante pasado, y el usuario podrá analizar la situación desde otra perspectiva. Nozomi da la posibilidad de poder cargar una instancia, o cargar dos instancias a la vez para hacer una comparación y destacar lo que ha cambiado.

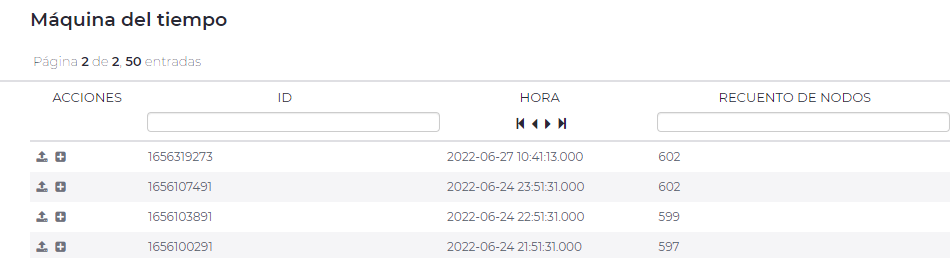


Ilustración 5.50. Consulta realizada en Nozomi Guardian (Fuente: Propia)

* **Vulnerabilidades**

Nozomi genera automáticamente una tabla con todas las vulnerabilidades de todos los activos situados en la red actual. Para ver todas las vulnerabilidades, Nozomi da la opción al usuario de hacerlo de tres maneras distintas:

* + **Mediantes activos.**

Enumera todas las vulnerabilidades por activo. Es decir en el aparatado de cada activo, aparecerán todas las vulnerabilidades únicamente de ese activo seleccionado.

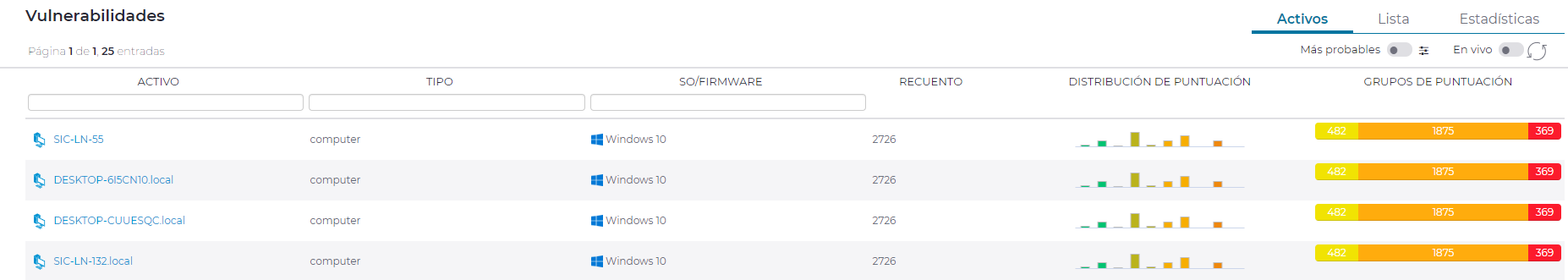


Ilustración 5.51. Consulta realizada en Nozomi Guardian (Fuente: Propia)

* + **En forma de lista.**

Nozomi Guardian enumera en forma de lista todas las vulnerabilidades.



Ilustración 5.52. Consulta realizada en Nozomi Guardian (Fuente: Propia)

* + **Mediante estadísticas.**

Enumera las estadísticas de las vulnerabilidades a nivel global.

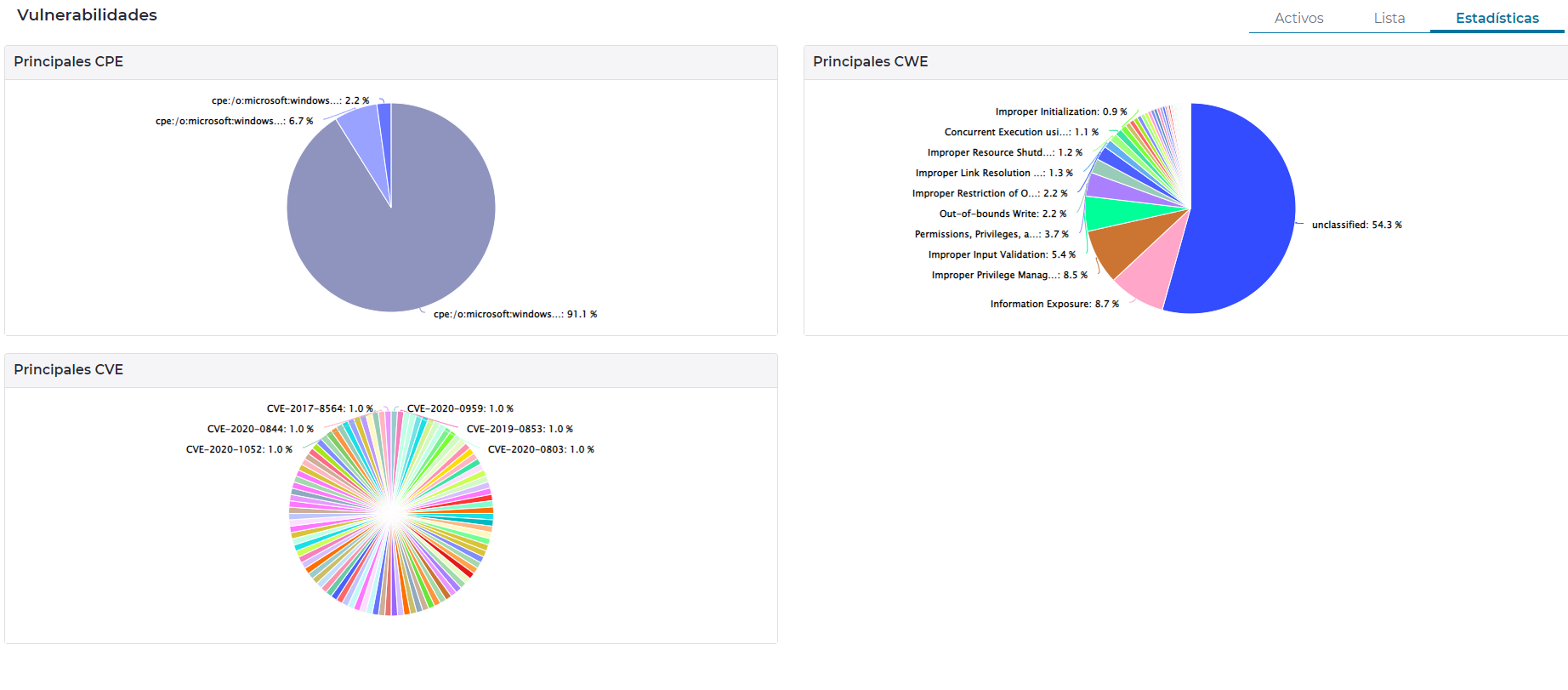


Ilustración 5.53. Consulta realizada en Nozomi Guardian (Fuente: Propia)

### CONFIGURACIÓN DE SEGURIDAD DE NOZOMI GUARDIAN

Una vez descritas las funciones y servicios que Nozomi Guardian aporta como herramienta de monitorización, toca describir cuales fueron los pasos para obtener protección de los IEDs virtualizadas en el paso anterior.

En primer lugar, cabe recordar que en la red local previamente configurada (ver Anexo 11.2), se tiene únicamente dos PCs. PC-Publicador y PC-Suscriptor, conectados ambos a un Switch. Una vez que se ha iniciado la virtualización del IED en el PC-Publicador y el PC-Suscriptor ha establecido una comunicación con el PC-Publicador mediante IED Scout, se iniciaría la herramienta de Nozomi Guardian.

El primer paso a realizar, es establecer el modo de fase en “Aprendizaje”. Para ello, se hará clic en la opción de “Administración”, después en “Panel de control de seguridad” y por último en la opción de “Aprendizaje”. En el apartado de “Dos fases”, se establecerá en modo Aprendizaje. Esto quiere decir que Nozomi aprenderá de todo el tráfico que haya en ese momento en la red, y guardara información de los activos, sesiones, nodos y demás características descritas en el apartado 5.4.1.



Ilustración 5.54. Consulta realizada en Nozomi Guardian (Fuente: Propia)

Se dejará ese modo durante un espacio de tiempo suficiente para que Nozomi aprenda de todo el tráfico generado por la comunicación de los PC-Suscriptor y PC-Publicador mediante IED Scout. El tiempo recomendable se establece entre uno y dos días aproximadamente para el caso de una red sencilla en la que únicamente existe un IED virtualizado y una comunicación entre PCs.

El siguiente paso será establecer el modo de fase en “Protección”. Anteriormente se estableció en modo de “Aprendizaje” para que aprendiera de la situación actual en la red, pues una vez aprendido se establece en el modo de “Protección”.



Ilustración 5.55. Consulta realizada en Nozomi Guardian (Fuente: Propia)

Esto quiere decir que ahora Nozomi, detectará cualquier anomalía en la red y generará una alerta al usuario por cada anomalía que detecte. Para ello es necesario establecer el “Perfil de seguridad” en nivel de “Paranoico”. Para ello, se hará clic en “Administración”, después en “Panel de control de seguridad” y finalmente en “Perfil de seguridad”.



Ilustración 5.56. Consulta realizada en Nozomi Guardian (Fuente: Propia)

Por lo tanto en esta fase Nozomi Guardian detectará cualquier tipo de tráfico que no sea correspondiente a los PCs PC-Publicador y PC-Suscriptor. Para comprobar que Nozomi detectaría cualquier anomalía en la red en base a lo aprendido anteriormente, se decide incluir otro PC en la red, denominado PC-Atacante.

Para ello, se conectaría el PC-Atacante al Switch, simulando que cualquier atacante se ha conseguido introducir en la red del IED. Y mediante IED Scout, se establecería una nueva conexión con el IED que está siendo virtualizado en el PC-Publicador. Por lo que ahora mismo, la red estaría formada por tres PCs, y un Switch. Y habría dos comunicaciones mediante el protocolo MMS mencionado anteriormente. Una de ellas sería la conexión fiable y original de la cual Nozomi Guardian ha aprendido, que sería entre el PC-Publicador y el PC-Suscriptor y la otra seria la establecida entre el PC-Atacante y el PC-Publicador.

Gracias a la fase de “Protección”, Nozomi generará una nueva alerta al detectar, en primer lugar un nuevo dispositivo (PC-Atacante) y en segundo lugar una nueva comunicación MMS del PC-Atacante con el PC-Publicador.

De esta forma se ha conseguido implementar una herramienta de seguridad que cada vez que detecte una anomalía en la red, sea capaz de avisar a usuario mediante la generación automática de alertas.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ilustración 5.48.(Fuente: Propia )

# Resultados

## RED LOCAL MONITORIZADA POR NOZOMI GUARDIAN

## REPOSITORIO GIT HUB

# Conclusiones

# Presupuesto

En este capítulo, se describirá cual sería el coste desglosado de la elaboración del proyecto, incluyendo mano de obra, recursos de hardware y herramientas de software necesarias para la elaboración del mismo.

* **Costes de mano de obra.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Concepto** | **Cantidad** | **Coste por hora** | **Numero total de horas** | **Coste final** |
| **Ingeniero Informático** | **1** | **11,50€** | **425** | **4887,5 €** |

* **Costes de hardware.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Concepto** | **Cantidad** | **Precio por unidad** | **Coste final del producto** |
| **Ordenador de sobremesa** | **1** | **900€** | **900€** |
| **Pantalla periférica** | **2** | **250€** | **500€** |
| **Ratón periférico** | **1** | **25€** | **25€** |
| **Teclado periférico** | **1** | **40€** | **40€** |
| **Switch** | **1** | **380€** | **380€** |
| **Coste final del equipamiento hardware:** | | | **1845€** |

* **Costes de software.**

|  |  |  |  |
| --- | --- | --- | --- |
| **Concepto** | **Cantidad** | **Precio por unidad** | **Coste final del producto** |
| **Licencia Nozomi Guardian Appliance V-100** | **1** | **2390€** | **2390€** |
| **Licencia Threat Intelligence** | **1** | **370€** | **370€** |
| **Licencia Asset Intelligence** | **1** | **370€** | **370€** |
| **Licencia IED Scout** | **1** | **€** | **€** |
| **Coste final del equipamiento software:** | | | **1465€** |

* **Resto de costes**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Concepto** | **Cantidad** | **Precio por unidad** | **Tiempo de uso** | **Coste final del producto** |
| **Luz** | **1** | **900€** |  | **900€** |
| **Internet** | **2** | **250€** |  | **500€** |
|  | **1** | **25€** |  | **25€** |
|  | **1** | **40€** |  | **40€** |
| **Coste final de los restos de costes:** | | |  | **€** |

* **Coste total del proyecto**

|  |  |
| --- | --- |
| **Concepto** | **Coste final del producto** |
| **Costes de mano de obra** | **4887,5 €** |
| **Costes de hardware** | **1845€** |
| **Costes de software** | **1465€** |
| **Resto de costes** | **€** |
| **COSTE TOTAL** | **€** |

# Agradecimientos

# Bibliografía

# Anexos

## INSTALACIÓN Y CONFIGURACION VMWARE WORKSTATION PRO

El primer paso para la instalación es realizar la descarga de la aplicación Workstation 16 Pro para Windows. Una vez descargado el archivo de instalación .exe, se procederá a su ejecución. Se esperará a que nos salga un cuadro de dialogo con las instrucciones para su instalación.

La primera pestaña que aparecerá se corresponderá con introducción y bienvenida de la aplicación, se presionará la opción “next” para seguir.

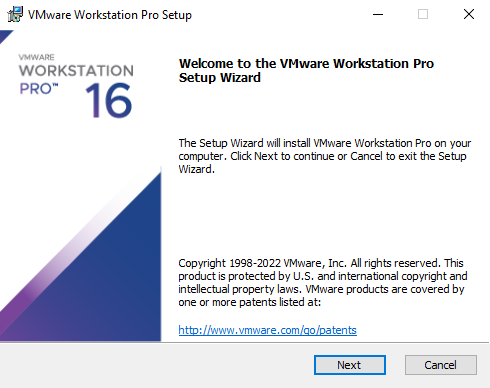


Ilustración 11.1. Paso 1 instalacion de Vmware Workstation Pro (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

El segundo paso por realizar es aceptar el acuerdo de licencia, como en toda aplicación es requerida para su instalación. Una vez se ha aceptado el acuerdo, se tendrá que marcar que tipo de instalación se requiere. Se marcará únicamente la pestaña inferior, en la que se está aceptando que las “tools” de la herramienta VMware Workstation Pro sean añadidas al PATH del sistema.

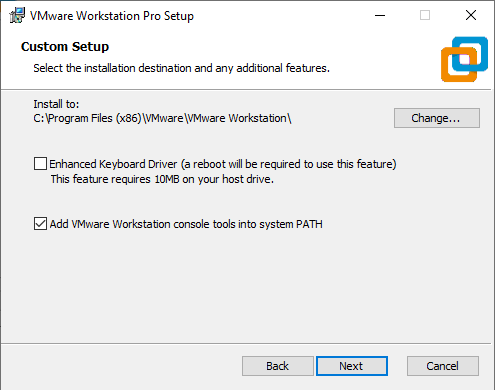


Ilustración 11.2. Paso 2 de la instalación de VMware Workstation Pro (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

La siguiente pestaña en aparecer, corresponderá con la configuración que el usuario quiera tener en relación con las alertas, avisos y actualizaciones de la herramienta. Por defecto, vienen marcadas ambas pestañas, para que si aparece una nueva versión o cualquier alerta del estilo, la propia aplicación avise al usuario.

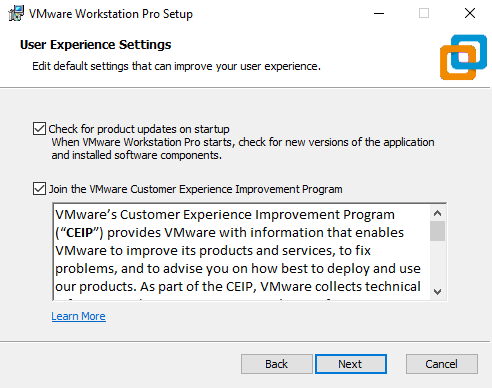


Ilustración 11.3. Paso 3 de la instalación de VMware Workstation Pro (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

La siguiente pestaña en cuestión, corresponderá únicamente a si se quiere crear en el escritorio principal y en la carpeta del programa del menú de inicio, un acceso directo a la aplicación. Ambos “checkboxs” vienen marcados previamente.

Finalmente comenzará el proceso de instalación, teniendo una duración en torno a 1 minuto aproximadamente.

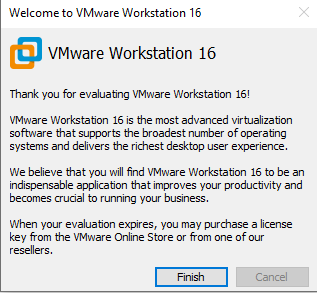


Ilustración 11.4. Pestaña de finalización de la instalación de VMware Workstation Pro (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

Una vez finalizada la instalación, la herramienta de virtualización ya está lista para ser usada. Se podrá importar cualquier máquina virtual para su uso. En nuestro caso, la que será instalada es Nozomi Guardian. La explicación detallada de los pasos de instalación a seguir viene dada en el Anexo 11.4.

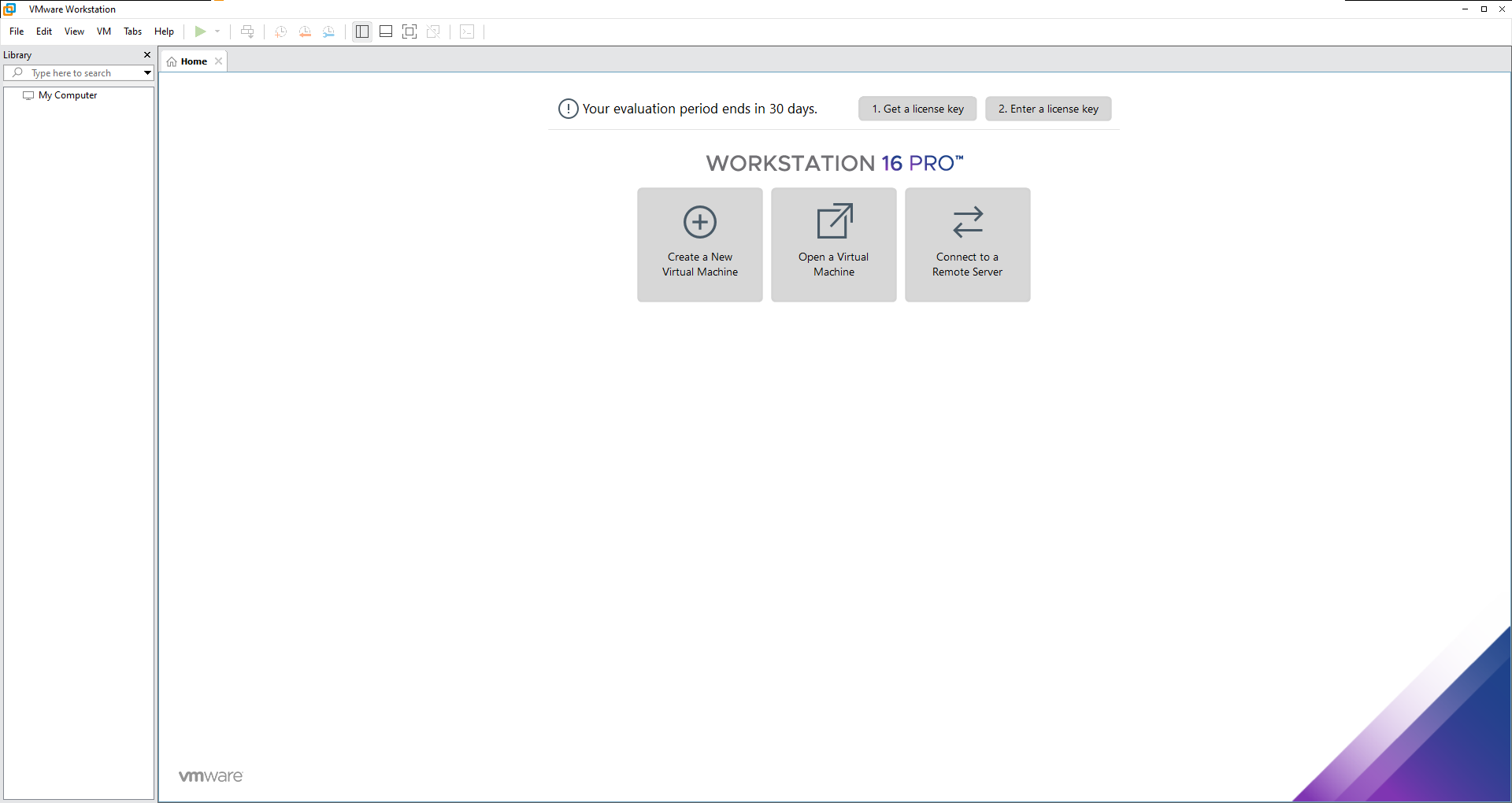


Ilustración 11.5. Pantalla principal de VMware Workstation Pro (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

## DISEÑO Y CONFIGURACION DE UNA RED LOCAL PARA PRUEBAS

Con el fin de evitar cualquier tipo de inconveniente en la red de la empresa, se decidió crear una propia red local, formada únicamente por tres ordenadores y un switch. La configuración del switch, es sencilla. Se habilito uno de los puertos del switch como “port-mirroring”. Ese puerto se encuentra conectado con la interfaz de red 2 del PC-Suscriptor, la cual está configurada por Nozomi para que capte todo el tráfico de esa red local.

Como se puede observar en la figura 11.6,por un lado, se encuentra el PC-Publicador, el cual estará virtualizando un IED con la herramienta IED Scout. Por el otro lado, se encontrará el PC-Suscriptor, el cual habrá iniciado una comunicación con el PC-Publicador a través de IED Scout, sabiendo en todo momento la IP del IED que está siendo virtualizado en el PC-Publicador.

Diagrama

Descripción generada automáticamente

Ilustración 11.6. Esquema básico de la red local creada para realizar las pruebas con Nozomi Guardian (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

Finalmente, solo quedaría introducir el Laptop-Atacante a la red. Conectaríamos ese ordenador al Switch, ya que es la única forma de simular una conexión de un atacante a un IED. Este Laptop-Atacante se conectará al PC-Publicador mediante IED Scout, y en esa conexión es donde entra en juego la herramienta de Nozomi Guardian.

Diagrama

Descripción generada automáticamente

Ilustración 11.7. Esquema básico de la red local creada para realizar las pruebas con Nozomi Guardian (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

## INSTALACIÓN Y CONFIGURACIÓN IED SCOUT

Para realizar la instalación y configuración de herramienta de virtualización IED Scout, es necesario seguir una serie de sencillos pasos:

* En primer lugar, descargar el archivo de instalación de la aplicación. Accediendo y registrándose en la página web[[1]](#footnote-1) es la forma de obtenerlo. La licencia y enlace a la aplicación fue dada por la empresa SICA S.A.
* El segundo paso será ejecutar el archivo previamente obtenido.
* En tercer lugar, se seleccionará el Path donde se desea instalar la aplicación. En este caso se dejó la que venía por defecto.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ilustración 11.8. Ventana de instalación de IED Scout. Elección del PATH (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

* Por último, será necesario tener instalado WinPcap. Es la herramienta que permite a ciertas aplicaciones captar los paquetes de la red, así como su transmisión. Sin esta herramienta adicional, IED Scout no podría ser ejecutado correctamente. Si no se tiene instalada, el propio proceso de instalación preguntara si se quiere instalar.

Una vez finalizados estos pasos, la herramienta IED Scout ya estará lista para ser usada.

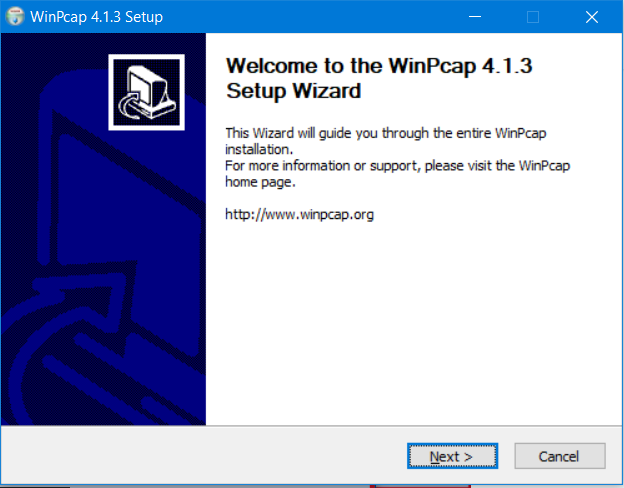


Ilustración 11.9. Pestaña instalación adicional herramienta WinPcap (Fuente: [propia](https://axis-india.com/2022/04/single-line-diagram-for-substation-detailed-explanation) )

## INSTALACIÓN Y CONFIGUACIÓN DE NOZOMI GUARDIAN

1. https://www.omicronenergy.com/es/productos/iedscout/# [↑](#footnote-ref-1)