****

**Escuela de Ingenierías**

**Industrial, Informática y Aeroespacial**

**GRADO EN INGENIERÍA INFORMÁTICA**

Trabajo de Fin de Grado

ANÁLISIS DE CIBERSEGURIDAD EN SUSESTACIONES CON EL ESTANDAR IEC 61850

CYBERSECURITY ANALYSIS IN SUBSTATIONS WITH IEC 61850 STANDARD

Autor: Marcos González Maestre

Tutor: Isaías García Rodríguez

(Julio, 2022)

|  |  |
| --- | --- |
| **UNIVERSIDAD DE LEÓN**  **Escuela de Ingenierías Industrial, Informática y Aeroespacial**  **GRADO EN INGENIERÍA INFORMÁTICA**  **Trabajo de Fin de Grado** | |
| **ALUMNO:** Marcos González Maestre | |
| **TUTOR:** Isaías García Rodríguez | |
| **TÍTULO:** Análisis de ciberseguridad en subestaciones con el estándar IEC 61850 | |
| **TITLE:** Cybersecurity analysis in substation with IEC 6150 STANDARD | |
| **CONVOCATORIA:** 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 con configurarlas de manera más óptima según las necesidades. Para ello, primero debemos comprender los principios básicos de la ciberseguridad así como la estructuración y normas del protocolo IEC 61850. Después haremos uso de la herramienta IEDScout para la simulación y virtualización de una comunicación entre IEDs, 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**

[1 Introducción 7](#_Toc104974574)

[1.1 INTRODUCCIÓN 7](#_Toc104974575)

[1.2 JUSTIFICACIÓN DEL PROYECTO 8](#_Toc104974576)

[1.3 OBJETIVOS DEL PROYECTO 8](#_Toc104974577)

[1.4 ESTRUCTURA DEL PROYECTO 8](#_Toc104974578)

[1.5 METODOLOGÍA 8](#_Toc104974579)

[2 Planificación y gestión del proyecto 9](#_Toc104974580)

[2.1 ALCANCE DEL PROYECTO 9](#_Toc104974581)

[2.2 PLANIFICACIÓN 9](#_Toc104974582)

[3 Estado del arte 9](#_Toc104974583)

[3.1 ESTO ES UNA PRUEBA 10](#_Toc104974584)

[4 Tecnologías usadas 10](#_Toc104974585)

[4.1 VMWARE WORKSTATION PRO 10](#_Toc104974586)

[4.2 NOZOMI NETWORKS 11](#_Toc104974587)

[4.3 WIRESHARK 13](#_Toc104974588)

[4.3.1 PARA QUE SE USA WIRESHARK 14](#_Toc104974589)

[4.4 IED SCOUT 14](#_Toc104974590)

[4.5 ADVANCED IP SCANNER 16](#_Toc104974591)

[4.6 TCPDUMP 16](#_Toc104974592)

[4.7 IEDs 18](#_Toc104974593)

[5 Núcleo del trabajo 19](#_Toc104974594)

[5.1 CIBERSEGURIDAD 19](#_Toc104974595)

[5.1.1 HISTORIA DE LA CIBERSEGURIDAD 21](#_Toc104974596)

[5.1.2 PRINCIPALES ATAQUES CIBERNETICOS 24](#_Toc104974597)

[5.1.3 AMBITOS DE LA CIBERSEGURIDAD 31](#_Toc104974598)

[5.1.4 CIBERSEGURIDAD EN LA ACTUALIDAD 33](#_Toc104974599)

[5.1.5 CIBERSEGURIDAD APLICADA AL MUNDO INDUSTRIAL 33](#_Toc104974600)

[5.2 ESTÁNDAR IEC 61850 34](#_Toc104974601)

[5.2.1 INTRODUCCION AL IEC 61850. ¿QUÉ ES? 34](#_Toc104974602)

[5.2.2 ORÍGENES DEL ESTANDAR IEC 61850 36](#_Toc104974603)

[5.2.3 ESTRUCTURA DEL ESTANDAR IEC 61850 36](#_Toc104974604)

[5.2.4 PRINCIPALES CARACTERISTICAS Y BENEFICIOS DEL PROTCOLO IEC 61850 37](#_Toc104974605)

[5.2.5 ARQUITECTURA DEL PROTOCOLO IEC 6850 37](#_Toc104974606)

[5.2.6 MODELADO DE LOS DATOS 37](#_Toc104974607)

[5.2.7 MODELOS DE COMUNICACIÓN 37](#_Toc104974608)

[5.3 Virtualización de IEDs con la herramienta IED Scout 38](#_Toc104974609)

[5.4 Uso de Nozomi Guardian para protección de IEDs 38](#_Toc104974610)

**Índice de Ilustraciones**

[Ilustración 1. Logotipo VMware Workstation Pro (Fuente: https://www.VMware.com/es/products) 12](#_Toc105663209)

[Ilustración 2. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia) 12](#_Toc105663210)

[Ilustración 3. Logo de la herramienta Nozomi Networks (Fuente: https://www.nozominetworks.com) 13](#_Toc105663211)

[Ilustración 4. Panel principal Nozomi Guardian (Fuente: Elaboración propia) 14](#_Toc105663212)

[Ilustración 5. Logo de la herramienta Wireshark (Fuente: https://www.wireshark.org ) 14](#_Toc105663213)

[Ilustración 6. Logotipo Omicron Electronics (Fuente: https://www.acinel.com/omicron-es ) 16](#_Toc105663214)

[Ilustración 7. Logotipo Advanced IP Scanner (Fuente: https://www.advanced-ip-scanner.com/es ) 17](#_Toc105663215)

[Ilustración 8. Logotipo TCPDUMP (Fuente: https://www.tcpdump.org ) 18](#_Toc105663216)

[Ilustración 8. Resumen opciones de filtros TCPDUMP (Fuente: propia) 19](#_Toc105663217)

[Ilustración 8. Niveles elementos subestaciones (Fuente: https://www.google.com/search?q=tipos+ieds+electrica&client=opera&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiL3YT0huv2AhWsxYUKHffvDUQQ\_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=OJltEW2UdpVPiM) 20](#_Toc105663218)

[Ilustración 10. Ciberseguridad (Fuente: https://thedatacyclehub.com/wp-content/uploads/2019/12/TDCH-Ciberseguridad.jpg) 22](#_Toc105663219)

[Ilustración 10. Ordenador IBM PC-XT (Fuente: https://www.fdi.ucm.es/migs/catalogo/ibm\_pc\_xt/) 23](#_Toc105663220)

[Ilustración 11. Evolución ARPANET 1969-1982 (Fuente: https://pbs.twimg.com/media/FIBHzVqXwAMyNLR.jpg) 24](#_Toc105663221)

[Ilustración 12. (Fuente: https://www.google.com/search?q=im+the+creeper&client=opera&hl=es&source=lnms&tbm=isch&sa=X&ved=2ahUKEwic0sXDtPr3AhXXgf0HHX4cCwcQ\_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=0rvDPPv74EQLOM) 24](#_Toc105663222)

[Ilustración 13. (Fuente: https://arc-anglerfish-arc2-prod-infobae.s3.amazonaws.com/public/EFPYZQ5RB5GLTMGKEOQJP4CZXI.jpg) 26](#_Toc105663223)

[Ilustración 14. Alerta detección virus ILoveYou. (Fuente: https://sites.google.com/site/seguridadinformaticacmj/\_/rsrc/1433934964613/virus/i-love-you/i%20love%20you.png?height=250&width=400) 26](#_Toc105663224)

[Ilustración 14. Logotipo representativo al gusano Conficker. (Fuente: https://norfipc.com/img/articulos/virus-conficker.png) 27](#_Toc105663225)

[Ilustración 14. Logotipo representativo al virus Stuxnet. (Fuente: https://www.lapatilla.com/wp-content/uploads/2019/09/Stuxnet-virus.jpg?resize=640%2C345) 27](#_Toc105663226)

[Ilustración 15. Pantalla rescate troyano Petya. (Fuente: https://es.wikipedia.org/wiki/Petya\_(malware) ) 28](#_Toc105663227)

[Ilustración 16. Pantalla rescate ransomware WannaCry. (Fuente: https://www.avast.com/es-es/c-wannacry) 29](#_Toc105663228)

[Ilustración 16.Pantalla activación de macros BlackEnergy. (Fuente: https://www.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/) 31](#_Toc105663229)

[Ilustración 16. Línea temporal del troyano BlackEnergy. (Fuente: https://www.incibe-cert.es/blog/blackenergy-sistemas-criticos) 31](#_Toc105663230)

[Ilustración 16.Grafico evolución ciberataques años 1980-85. (Fuente: curso CyberOps) 32](#_Toc105663231)

[Ilustración 16.Grafico evolución ciberataques año 2000. (Fuente: curso CyberOps) 33](#_Toc105663232)

[Ilustración 16.Grafico evolución ciberataques año 2015-17. (Fuente: curso CyberOps) 34](#_Toc105663233)

[Ilustración 17. Agencias estatales de ciberseguridad. (Fuente: https://javierdisan.com/2018/09/25/) 35](#_Toc105663234)

[Ilustración 17. Grafico uso de Internet por la población española. (Fuente: https://wearesocial.com/es/blog/2022/02 ) 36](#_Toc105663235)

[Ilustración 17. Portada Decálogo ciberseguridad para empresas elaborado por el INCIBE. (Fuente: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\_decalogo\_ciberseguridad\_metad.pdf) 37](#_Toc105663236)

[Ilustración 19. Logotipo IEC. (Fuente: http://www.seguridadepm.com/iec ) 39](#_Toc105663237)

[Ilustración 20. Resumen IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 40](#_Toc105663238)

[Ilustración 21. Capítulos IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 42](#_Toc105663239)

[Ilustración 22. Arquitectura protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 44](#_Toc105663240)

[Ilustración 2. Estructura de datos del protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 44](#_Toc105663241)

[Ilustración 22. Nomenclatura de un Logical Node (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 45](#_Toc105663242)

[Ilustración 23. Nomenclatura de un objeto (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 46](#_Toc105663243)

[Ilustración 22. Jerarquía datos de un dispositivo lógico en el protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA) 46](#_Toc105663244)

**Glosario de términos**

**Sniffer:**

**DSJKWDH**

**HEW:**

**Nicho de mercado:**

**Subestaciones:**

**Disyuntores**

**Transformadores de corriente**

**Fusibles de protecciones,**

**Celdas de protección**

**Reconectadores**

**IEEE**

**Ataques DoS:**

**Ataques DDoS:**

**Router:**

# Introducción

## INTRODUCCIÓN

## 

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

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

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

## JUSTIFICACIÓN DEL PROYECTO

## OBJETIVOS DEL PROYECTO

## ESTRUCTURA DEL PROYECTO

## METODOLOGÍA

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

# Planificación y gestión del proyecto

## ALCANCE DEL PROYECTO

## PLANIFICACIÓN

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

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

# Estado del arte

## ESTO ES UNA PRUEBA

# Tecnologías usadas

## VMWARE WORKSTATION PRO

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

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

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

)

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

Seguimps escribiendo

## NOZOMI NETWORKS

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

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



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

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

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

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

* Información de entorno
* 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 identificare todo el tráfico de red, sabiendo que protocolos están siendo utilizados así como todas las sesiones activas y todos los nodos tanto activos como no situados dentro de dicha red.

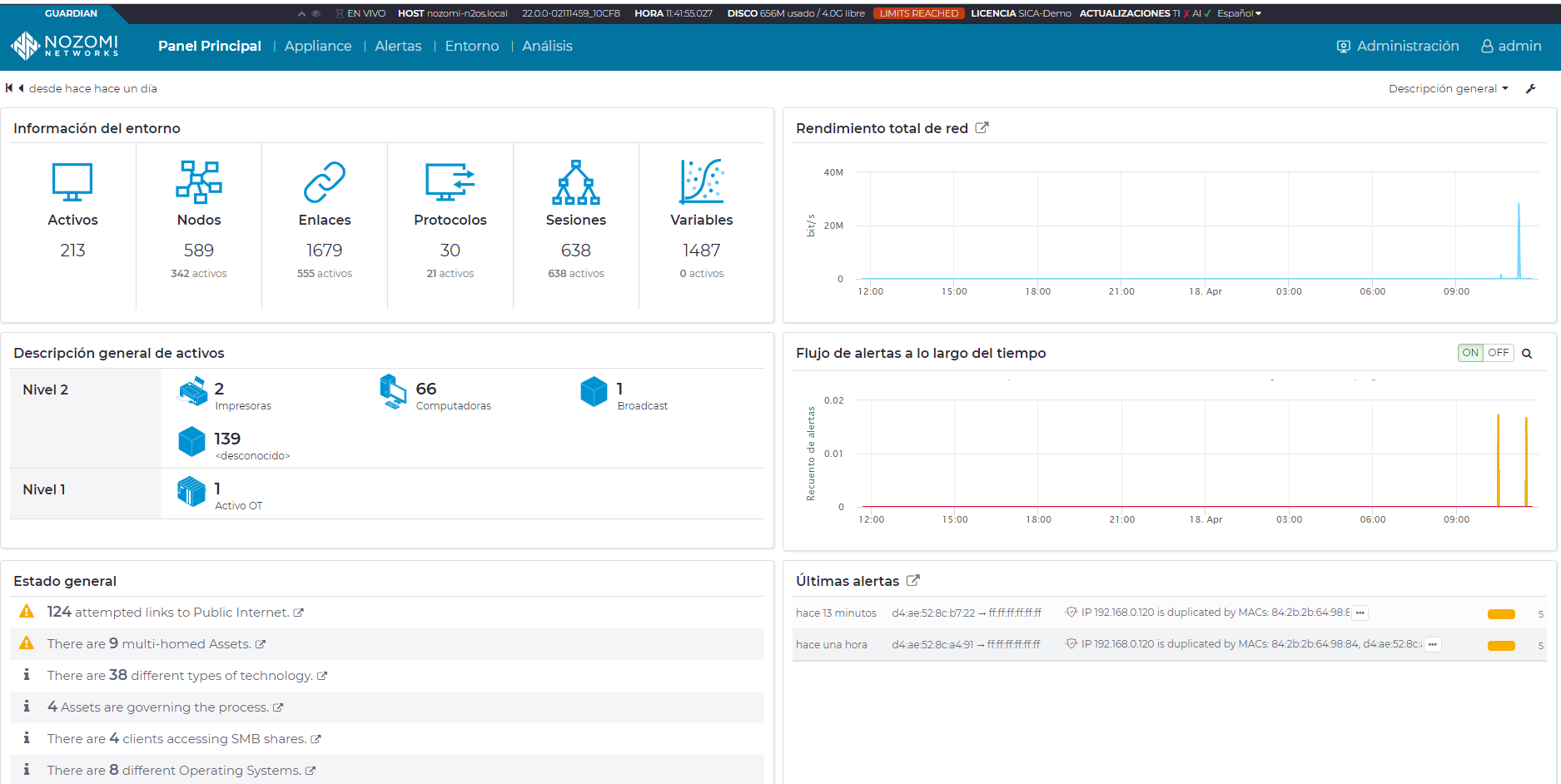


Ilustración 4. Panel principal Nozomi Guardian (Fuente: Elaboración propia)

## WIRESHARK

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

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

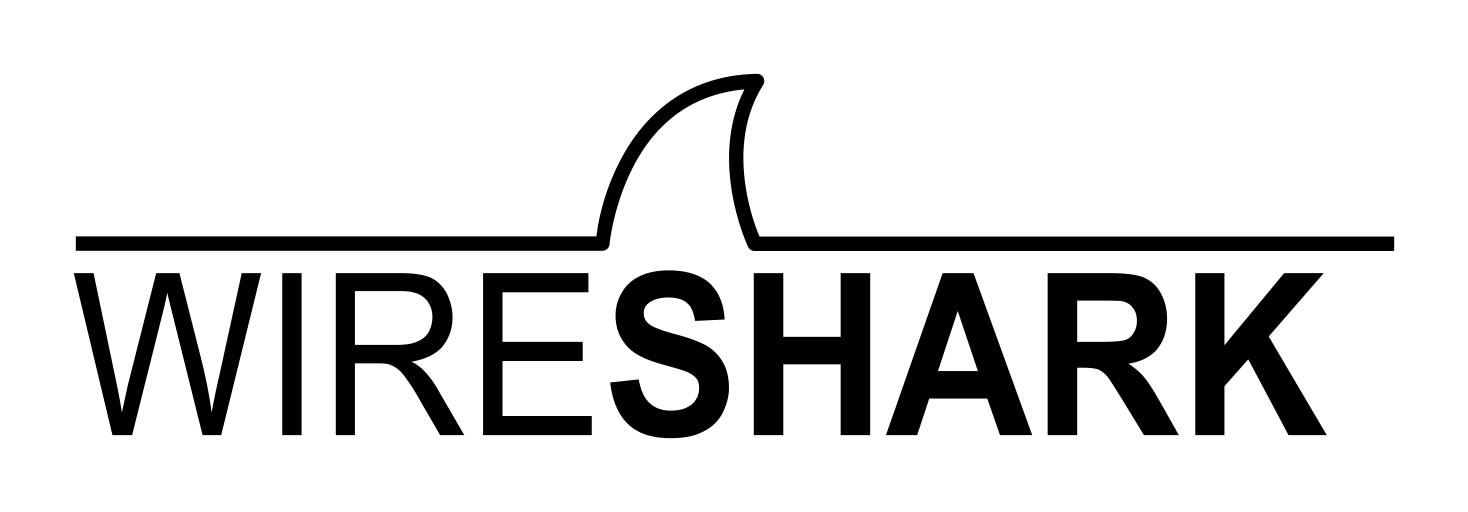


Ilustración 5. Logo de la herramienta Wireshark (Fuente: <https://www.wireshark.org> )

### PARA QUE SE USA WIRESHARK

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

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

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

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

## IED SCOUT

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



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

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

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

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

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

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

## ADVANCED IP SCANNER

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



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

## TCPDUMP

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



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

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

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

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

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

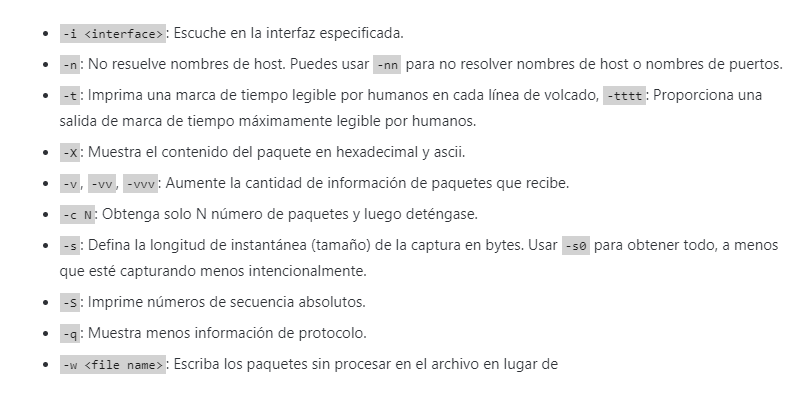


Ilustración 8. Resumen opciones de filtros TCPDUMP (Fuente: propia)

## IEDs

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

Tenemos varios tipos de IEDS. Que son los siguientes:

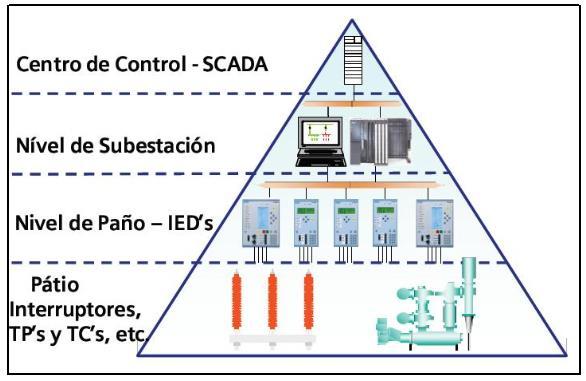


Ilustración 8. Niveles elementos subestaciones (Fuente: <https://www.google.com/search?q=tipos+ieds+electrica&client=opera&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiL3YT0huv2AhWsxYUKHffvDUQQ_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=OJltEW2UdpVPiM>)

# Núcleo del trabajo

## CIBERSEGURIDAD

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

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

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

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

Ciberseguridad de software, de hardware, en redes, personal, 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.



Ilustración 10. Ciberseguridad (Fuente: https://thedatacyclehub.com/wp-content/uploads/2019/12/TDCH-Ciberseguridad.jpg)

### HISTORIA DE LA CIBERSEGURIDAD

Como todo en la vida, la evolución y el desarrollo está a la orden del día, y la ciberseguridad no se encuentra al margen de esa evolución. Han pasado ya unas cuantas décadas desde que se empezó a usar y desarrollar sistemas informáticos en todos los ámbitos diarios, tanto en empresas del sector económico, como el de servicios…etc. Páginas web arcaicas y sin seguridad, redes poco confiables, escaso uso de sistemas informáticos en el día a día, por lo que la ciberseguridad tal y como la conocemos a día de hoy, ha sido un largo proceso de desarrollo y cambios, que comenzó en la década de los 70 y continua a día de hoy y seguirá desarrollándose con el paso del tiempo.



Ilustración 10. Ordenador IBM PC-XT (Fuente: https://www.fdi.ucm.es/migs/catalogo/ibm\_pc\_xt/)

Retrocedemos a finales de la década de los 70. Lo que hoy conocemos como ciberseguridad, en aquella época se denominaba “seguridad de los datos”. En aquella época la visión que se tenía sobre la seguridad de los datos era bastante mala, se percibía como un gasto de dinero, tiempo y recursos de la empresa y encima no aportaba nada visible a la misma. Por lo que se veía casi como un gasto innecesario en la empresa.

A finales de los 70, el especialista e ingeniero Bob Thomas, creó de forma inocente el primer virus informático. Bob, se encontraba programando un código para establecer un movimiento fácil entre todos los host que estaban conectados a la versión básica de lo que hoy conocemos como Internet, denominada *ARPANET.*

**ARPANET**, proveniente de las siglas **A**dvanced **R**esearch **P**rojects **A**gency **N**etwork, en castellano, Red de la Agencia de Proyectos de Investigación Avanzada, se puede definir como una red de computadoras establecida en 1969 por el Departamento de Defensa de los Estados Unidos como medio de comunicación para enviar datos militares y conectar grupos de investigación estatales en el país estadounidense.

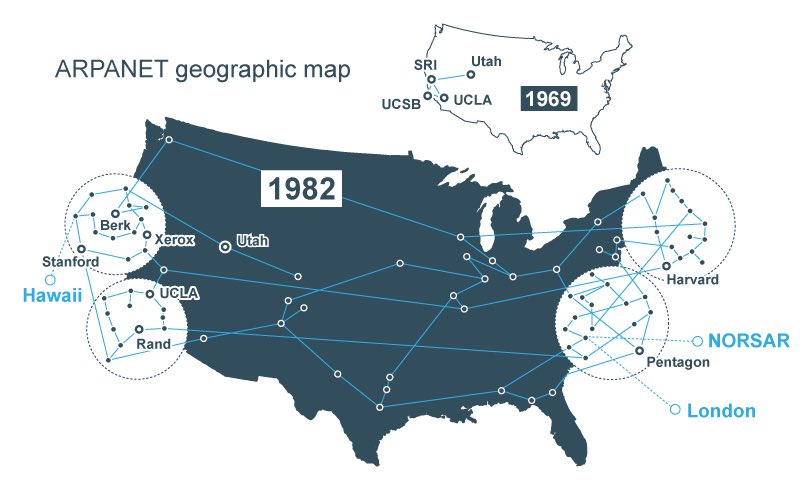


Ilustración 11. Evolución ARPANET 1969-1982 (Fuente: https://pbs.twimg.com/media/FIBHzVqXwAMyNLR.jpg)

Volviendo a Bob Thomas, creador del primer virus informático que es muy famoso primero por ser el primero y segundo por el mensaje que aparecía en el terminal. “I´M THE CREEPER, CATCH ME IF YOU CAN”, que en español significa “Soy el creeper, atrápame si puedes”, era el mensaje que aparecía al ejecutar el código creado por Bob. Un tiempo más tarde Ray Tomlinson, programó una nueva versión del programa, que permitía que el programa se duplicase en los sistemas informáticos conectados. Creeper y Reaper son los nombres con los que se les conoce a este programa, en honor a los dos creadores del mismo.



Ilustración 12. (Fuente: https://www.google.com/search?q=im+the+creeper&client=opera&hl=es&source=lnms&tbm=isch&sa=X&ved=2ahUKEwic0sXDtPr3AhXXgf0HHX4cCwcQ\_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=0rvDPPv74EQLOM)

Otro momento importante en la historia de la ciberseguridad o seguridad de los datos fue el desarrollo del primer ataque de virus denominado The Morris Worm, que consiguió llegar a infectar unas 6500 computadoras.

Entrando ya en finales de la década de los 80, apareció el primer ataque de ransomware. Es muy conocido debido a como se produjo. Consistía en la creación de unos CD protegidos con una caratula que ponía “Información Introductoria sobre el Sida”. Este CD, fue enviado a más de 90 países distintos. Se entregaron más de 20 mil CD por casi todas partes del mundo. Esto lo que hacía era que, cuando el usuario metiera ese CD en su computadora, este iba a conseguir cifrar en disco duro de su ordenador e iba a exigir un rescate de 189 dólares para recuperar su información a ingresar en una cuenta en Panamá, lugar donde había sido creada la empresa ficticia para ejecutar este ataque. “Gracias” a este ataque, comenzó a desarrollarse técnicas mejoradas de cifrado, que finalmente desembocaron en el RSA (cifrado Rivest-Shamir-Adleman).

### PRINCIPALES ATAQUES CIBERNETICOS

Para poder conocer la actualidad de la ciberseguridad, es necesario hacer un repaso de cuales han sido los mayores ataques cibernéticos de la historia, y con ello podremos entender el por qué se han tomado ciertas decisiones en determinados aspectos. Se puede entender como los mayores ciberataques como aquellos en lo que se ha conseguido una gran cantidad de datos de usuarios, información privilegiada sobre ciertas personas, conseguir parar los sistemas informáticos de una cierta empresa o estado...etc. A continuación, se enumeraran y describirán los ataques más conocidos:

* **ILoveYou.**

La expansión de este virus se realizó básicamente y principalmente vía correo electrónico a inicios del 2000, con un mensaje y un archivo adjunto como el que podemos ver en la Ilustración 13. En teoría, esto era una carta de amor que te enviaban por correo electrónico, solía nombrarse como LOVE-LETTER-HOR-YOU.TXT, aunque en realidad su extensión no era TXT, sino que era vbs. Con esto conseguían que aquellos sistemas operativos que tenían en “Oculto” mostrar la extensión del archivo, no les salía que en verdad no era un txt, sino que era un vbs. Esto sumado a que a principios de los 2000, la ciberseguridad no estaba nada avanzada y los usuarios no tenían ninguna noción sin concienciación sobre este tipo de ataque informático.



Ilustración 13. (Fuente: <https://arc-anglerfish-arc2-prod-infobae.s3.amazonaws.com/public/EFPYZQ5RB5GLTMGKEOQJP4CZXI.jpg>)

Una vez que el cliente de correo abría el archivo LOVE-LETTER-HOR-YOU.TXT.vbs, el propio virus de ILoveYou, accedía a todos los contactos de ese usuario en Outlook, y enviaba una copia del mensaje a todos ellos. Con lo que con esto, se conseguía poder replicar el mensaje y difundirlo a una rapidez abismal.

Una vez que se infectaba el equipo del usuario, el gusano se replicaba sobre todos los archivos que tuvieran una de estas extensiones: JPG, JPEG, MP3, MP2, JS, JSE, CSS, WSH, SCT, HTA, VBS y VBE. ILoveYou cambia el formato del archivo encontrado y lo transformaba a VBS.

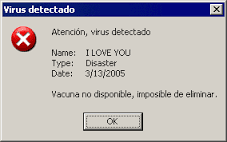


Ilustración 14. Alerta detección virus ILoveYou. (Fuente: https://sites.google.com/site/seguridadinformaticacmj/\_/rsrc/1433934964613/virus/i-love-you/i%20love%20you.png?height=250&width=400)

* **Conficker.**

Nos situamos en el mes de octubre de 2008, y se puede definir como un gusano informático que atacaba a los equipos que tenían implementado el sistema operativo Windows. También conocido como *Downup*, *Downandup* o *Kido*, se basaba en infectar al mayor número posible de computadoras que tenían implementado Windows como sistema operativo, para que estos empezaran a formar parte de un red de bots, la cual estaba administrada de forma remota por un nodo central. El objetivo era básicamente robar información de los sistemas infectados y realizar campañas de envío de correos basura masiva, también conocida como SPAM.



Ilustración 14. Logotipo representativo al gusano Conficker. (Fuente: https://norfipc.com/img/articulos/virus-conficker.png)

Para marzo de 2009, este gusano había sido capaz de infectar a más del 6% de todas las computadoras mundiales, a partir de 2009 el efecto de este gusano fue disminuyendo, aunque han salido nuevas versiones mejoradas del mismo.

* **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 14. 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 volvió a repetir 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 todos conocemos, la infección de la planta entera, y la autodestrucción de las maquinas industriales que alimentaban al urania, suponiendo una pérdida de millones de euros para el país iraní, así como una demostración de que nada en este mundo es 100% seguro.

* **Petya.**

Si hablamos de la plataforma de almacenamientos de archivos en la nube Dropbox, nos tiene que venir a la mente el malware Petya. Conocido como uno de los malware de tipo ransomware más sofisticados creados hasta nuestros días. Lanzado en el año 2016 por la empresa Heise Security, y el funcionamiento usaba técnicas de ingeniería social y de cifrado. El funcionamiento de infección y propagación del troyano era bastante entendible. Una vez que descargabas este archivo, este se auto extraía y se ejecutaba. Como cada vez que ejecutas algún archivo en Windows, nos aparece la ventana de alerta de Windows. Dándole a si, Petya se adentraba en el registro de arranque principal de la computadora, desactivaba el modo seguro de Windows y para que esto fuera efectivo, reiniciaba W2indows. Una vez reiniciado, aparecía una pestaña advirtiendo que habías sido hackeado y cuanta era la cantidad monetaria a ingresar para descifrar el disco y poder recuperar toda la información.

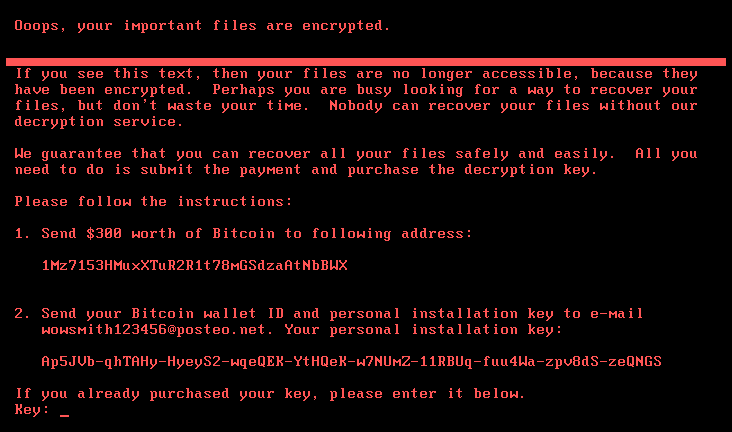


Ilustración 15. Pantalla rescate troyano Petya. (Fuente: <https://es.wikipedia.org/wiki/Petya_(malware)> )

Como se comentó antes, este troyano fue lanzado en 2016, pero hasta 2017 no se comenzaron a ver los primeros ataques importantes. En junio de ese mismo año comenzó un ciberataque mundial mediante una variante del troyano Petya. Más de 80 importantes empresas fueron infectadas, situándose en países como Polonia, Italia, Reino Unido, Estados Unidos, Alemania, Francia y Ucrania, la más perjudicada de todas. El Banco Nacional de Ucrania fue infectado también, dándose todavía más a conocer este troyano y aumentando el nivel de alerta en todos los estados y grandes empresas.

* **WannaCry.**

Posiblemente el troyano más conocido a nivel mundial en la actualidad. Desarrollado por el coreano Park Jin Hyok en el año 2017, y clasificado como uno de los ransomware más potentes a día de hoy. Conocido como WannaCry, WanaCrypt0r 2.0 o Wannadecryptor, aprovechaba una vulnerabilidad de los equipos que tenían implementado un sistemas operativo Windows no actualizado debidamente (es decir, desactualizado). EternalBlue, desarrollada por la Agencia de Seguridad Nacional estadounidense, fue la brecha encontrada en los sistemas operativos de Windows anticuados para poder cifrar archivos valiosos de una computadora y después solicitar una cuantía económica al usuario para poder recuperar los archivos cifrados.



Ilustración 16. Pantalla rescate ransomware WannaCry. (Fuente: https://www.avast.com/es-es/c-wannacry)

El “modus operandi” era bastante similar al del ransomware Petya, y el objetivo el mismo, chantajear al usuario para poder obtener un beneficio económico. Además de la vulnerabilidad encontrada en el servicio EternalBlue para poder propagar el ransomware, Wannacry instalaba en los ordenadores infectados lo que se conoce como una puerta trasera, denominada DoublePulsar, usada para poder ejecutar Wannacry.

Meses antes del ataque, Windows ya había detectado esta vulnerabilidad (EternalBlue) y había sacado un parche para la misma. El problema fue que muchos de los usuarios de computadoras, no mantenían su equipo actualizado y por lo tanto no tenían este parche implementado en su computadora. Por lo que todos estos equipos sin parche de actualización, eran posibles víctimas del ataque de WannaCry.

Este ataque de ransomware, afecto a más de 230.000 computadoras en todo el mundo. Lo que quiere decir que un cuarto de millón de computadoras estaban desactualizadas. Con respecto a nuestro país, Telefónica fue la gran perjudicada por el mismo. Paralizo miles de computadoras y genero un daño económico irreparable. WannaCry afecto a computadoras de más de 150 países distintos y provoco pérdida de más de 4 millones de dólares en todo el mundo.

En la actualidad este tipo de ataques siguen siendo peligrosos debido a que todavía hay miles de equipos desactualizados y que pueden ser críticos.

* **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.

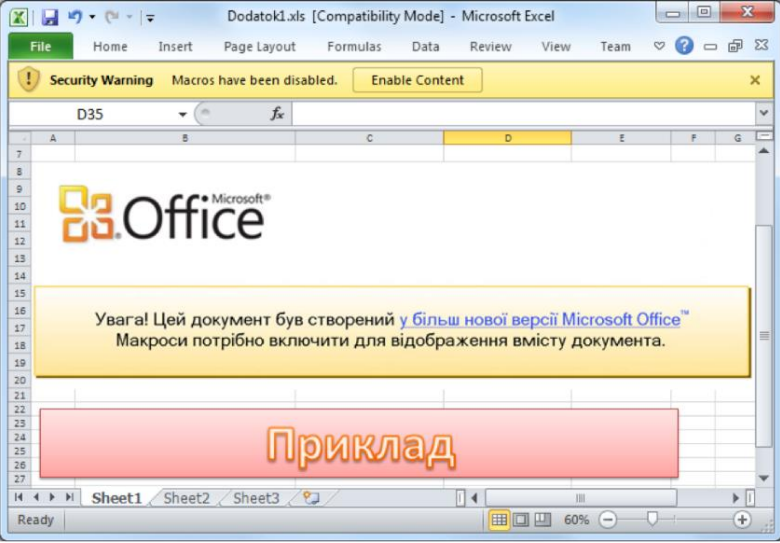


Ilustración 16.Pantalla activación de macros BlackEnergy. (Fuente: <https://www>.welivesecurity.com/la-es/2016/01/05/troyano-blackenergy-ataca-planta-energia-electrica-ucrania/)

Una vez que se descargaba ese docuemnto y se abria, al usuario le aparecia un pantalla que recomendaba habilitar las macros para poder ver el contenido del archvio. Aceptando esas macros, era como se activaba la infección del malware BlackEnergy.

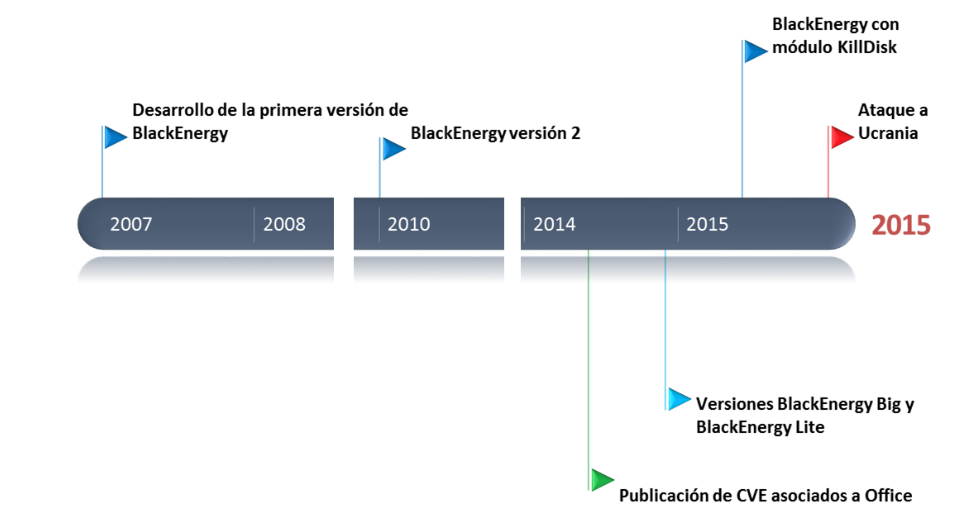


Ilustración 16. Línea temporal del troyano BlackEnergy. (Fuente: <https://www>.incibe-cert.es/blog/blackenergy-sistemas-criticos)

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, asi 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.

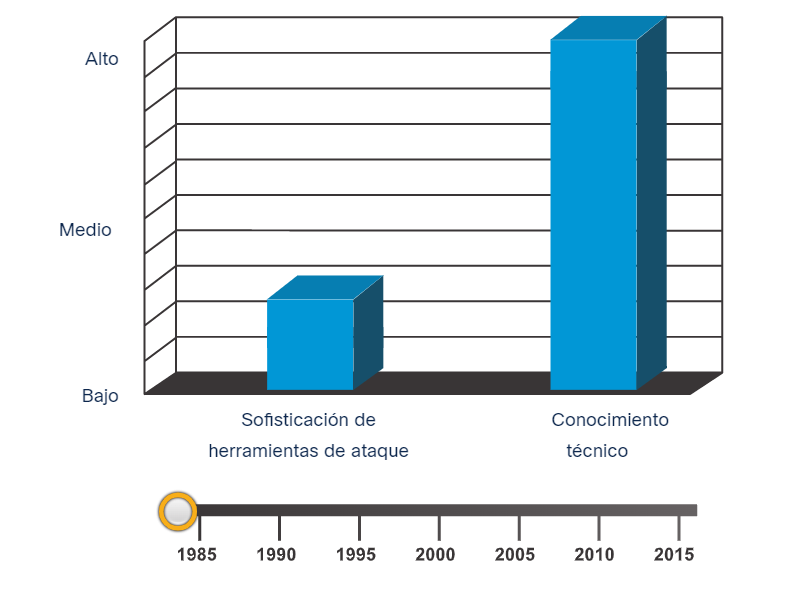


Ilustración 16.Grafico evolución ciberataques años 1980-85. (Fuente: curso CyberOps)

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.

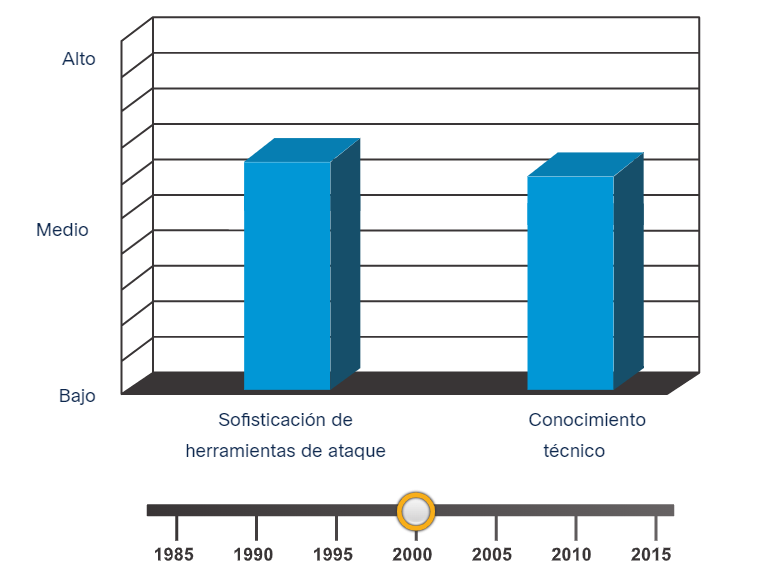


Ilustración 16.Grafico evolución ciberataques año 2000. (Fuente: curso CyberOps)

Acercándonos a la actualidad, vemos como las barras del grafico han cambiado a la 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 búsqueda der 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

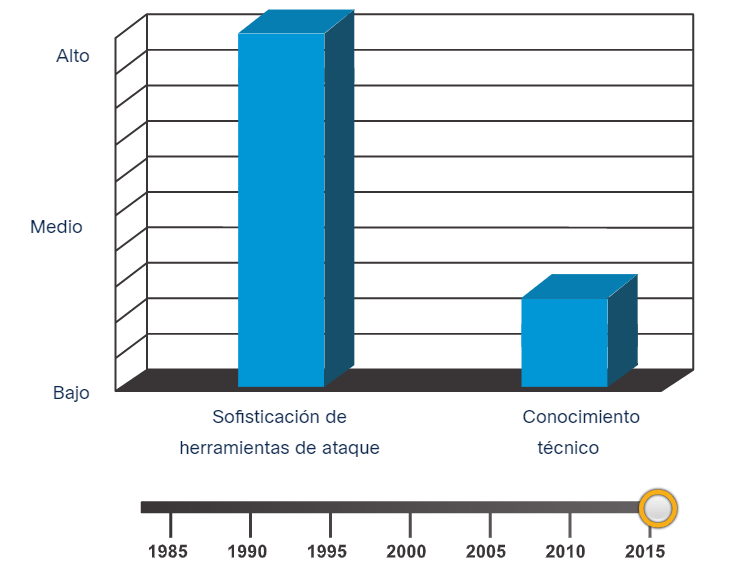


Ilustración 16.Grafico evolución ciberataques año 2015-17. (Fuente: curso CyberOps)

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, el ciudadano de calle 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.

En resumen, con el paso del tiempo más integrado todavía estarán los sistemas y el mundo IoT en el ámbito personal y por lo tanto este será un objetivo mayor para los ciberdelincuentes.

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 ca0pacidades 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.

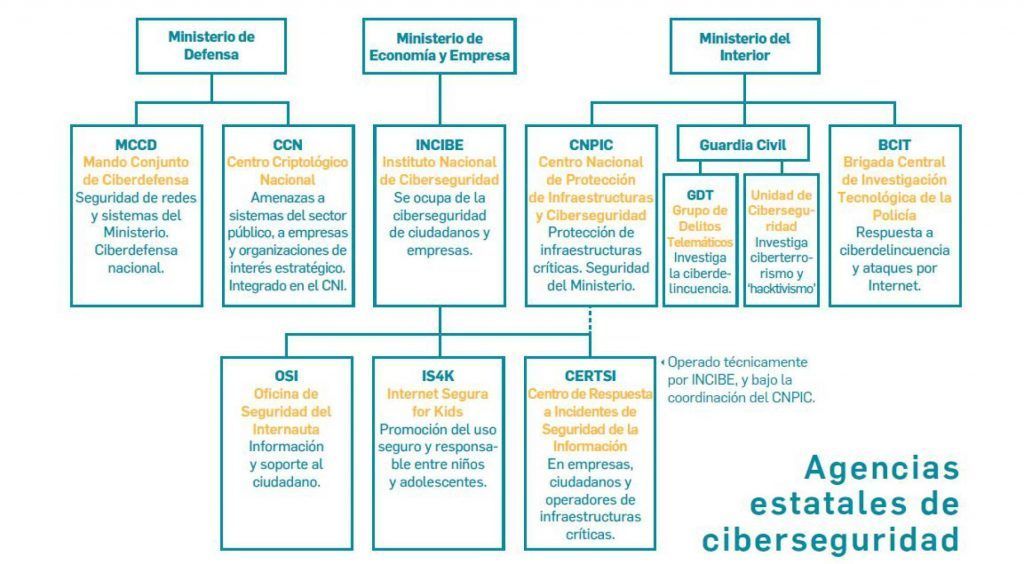


Ilustración 17. Agencias estatales de ciberseguridad. (Fuente: https://javierdisan.com/2018/09/25/)

### 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.

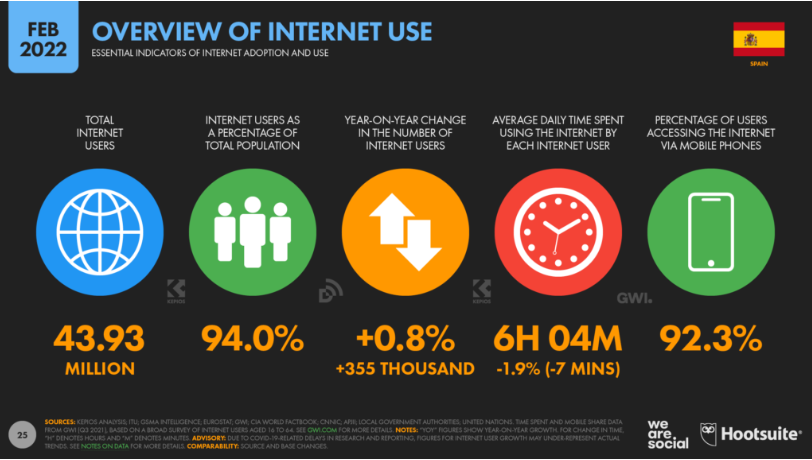


Ilustración 17. Grafico uso de Internet por la población española. (Fuente: <https://wearesocial.com/es/blog/2022/02> )

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 17. Portada Decálogo ciberseguridad para empresas elaborado por el INCIBE. (Fuente: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia\_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 ataques DoS. Y por otro lado, intentar mantener todos sus datos a salvo, manteniendo su integridad, confidencialidad y disponibilidad de los mismos. 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

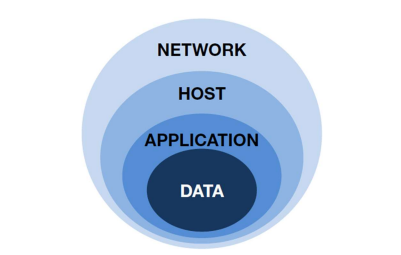
A principios del año 2020, las empresas industriales se empezaron a dar cuenta de que las infraestructuras eléctricas críticas necesitaban tener más seguridad de la que tenían, que en muchos casos era escasa y en otros inexistente.

Con la seguridad informática se trata de conseguir que las instalaciones eléctricas sean más fiables, y reducir el tiempo de inactividad en el caso de que surjan problemas. En un principio, cuando se diseñaban sistemas eléctricos, se buscaba sobre todo la eficacia y facilidad de uso, la seguridad no era una de las principales preocupaciones de los administradores de red o instaladores. Sin embargo, ese enfoque que se tenía ya no es válido ni suficiente. 4 Como se menciona en el punto anterior, en los últimos años la complejidad de las redes eléctricas se ha incrementado, así como su incursión en el mundo digital. Además, se han interconectado sistemas de diferentes países, lo cual ha hecho que aumente su alcance, aunque también su coste y la probabilidad de que haya errores y surjan problemas. Por ello, son necesarias las políticas de seguridad informática para prevenir o minimizar las amenazas, con los siguientes objetivos: • Confidencialidad: evitar accesos no autorizados. • Integridad: impedir modificaciones o robo de información. • Disponibilidad: prevenir las denegaciones de servicio para garantizar el acceso. Estos objetivos, adquieren mayor o menor prioridad en función de las redes analizadas; por ejemplo, en el caso de las redes TI se le da mucha importancia a la confidencialidad, en cambio, en las redes industriales, se le da mucha importancia a la disponibilidad. Hay que resaltar, que la seguridad informática es un proceso iterativo, no es estático. A medida que las condiciones del entorno o los orígenes de amenazas van cambiando, los sistemas y políticas de seguridad necesitan ir actualizándose para poder ser capaces de hacer frente a dichos cambios.

Las redes eléctricas son objetivos cada vez más fáciles para los hackers. Por ello es necesario desarrollar modelos de estrategia, para poder evitar los ataques. Un ejemplo de estrategia de seguridad es el modelo de “Defensa en profundidad”. Este modelo consiste en la superposición de diferentes capas se seguridad, que puedan detectar y responder a las diversas amenazas a las que están expuestas los sistemas eléctricos, para poder así proporcionar una mejor protección. Este modo de actuación asegura que si alguna de las capas pasa por alto ciertos agentes extraños, otra capa proporcionará la defensa.

Figura 1.3.CAPAS DE SEGURIDAD. «Cyber Security in Electrical Substations» [1]

El éxito de estos modelos, reside en el hecho de que los sistemas no pueden confiar por completo en un solo punto de la seguridad, por muy bueno que sea. [1]



## ESTÁNDAR IEC 61850

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

Para saber con seguridad lo que es IEC 61850, primero es necesario saber lo que las siglas IEC significan. **I**nternational **E**lectrotechnical **C**omission, es el significado de las siglas correspondientes a **IEC** traducido al castellano Comisión Electrotécnica Internacional, 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 19. 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 objetico 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, celdas de protección o reconectadores. Con respecto a los equipos de control, el más importante y conocido es el SCADA o HMI, 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).

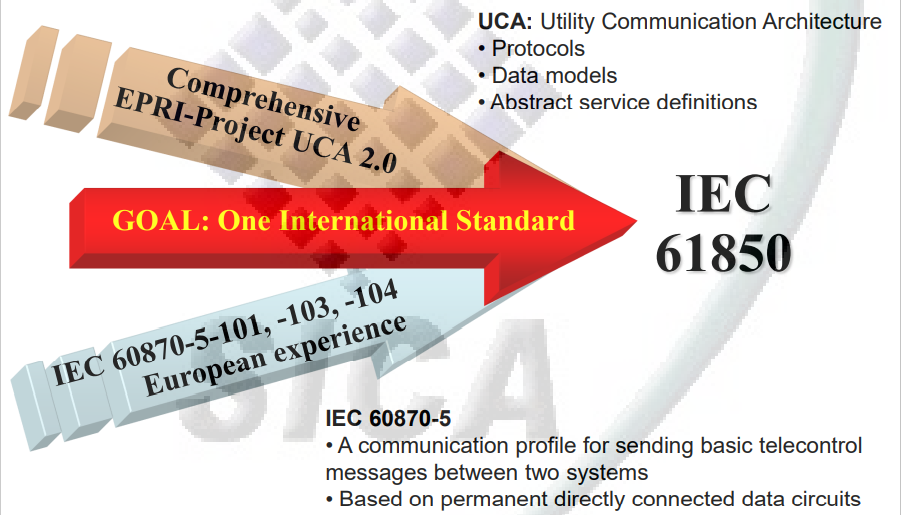


Ilustración 20. Resumen IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

### ORÍGENES DEL ESTANDAR 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.

Anteriormente al protocolo IEC 61850, se encontraban ostros 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 protocolo eléctrico. El IEC 61850 usa por defecto Ethernet, TCP/IP, y 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 protocolo IEC 61850 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 ESTANDAR IEC 61850

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

1. Principios básicos
2. Glosario
3. Requerimientos generales/principales
4. Sistema y administración del proyecto
5. Requerimientos de comunicación
6. Configuración del sistema de automatización de subestaciones
7. Estructura básica de comunicación
8. Mapeo de servicios de comunicación específicos (SCSM) - Asignaciones a MMS
9. Servicio específico de comunicación. Mapeo (SCSM) -Valores muestreados sobre unidireccional en serie enlace multidrop punto a punto y sobre ISO/IEC 8802-3
10. Pruebas de conformidad

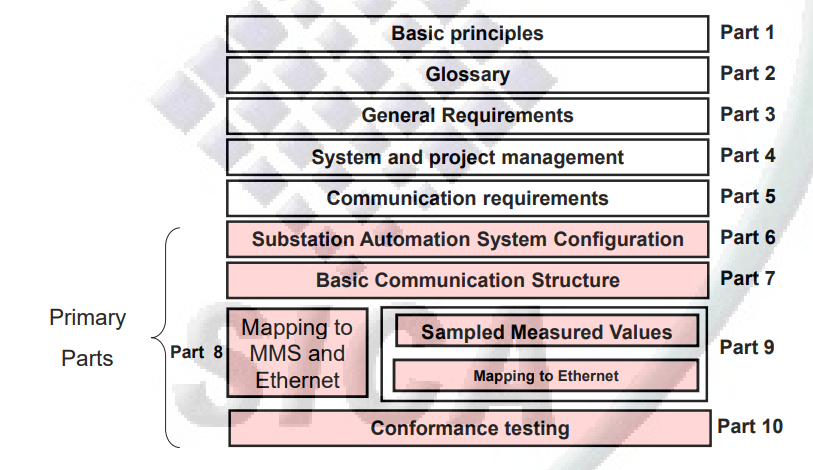


Ilustración 21. Capítulos IEC 61850(Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

### PRINCIPALES CARACTERISTICAS Y BENEFICIOS DEL PROTCOLO IEC 61850

Como ya sabemos, la elaboración de este protocolo 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, diseño este protocolo 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.
* Comunicación 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 PROTOCOLO IEC 6850

Arquitectura*. “Estructura lógica y física de los componentes de una parte de la informática”*. Así es como la Real Academia Española define arquitectura. Por lo que, toda la estructura lógica y física del protocolo IEC 61850 debe ir descrito en este apartado. La comisión IEC, decidió establecer tres niveles distintos, en los cuales se encontraran un tipo de maquinaria especifica.

**Nivel de proceso**, **nivel de bahía** y **nivel de estación**. **Process Level**, **Bay Level** y **Station Level** es como vienen definidos en la documentación del protocolo, en el idioma reconocido, que es inglés.

* **Nivel de proceso ("*Process Level*”).** Este es el nivel más inferior de un subestación eléctrica que use el protocolo 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, también conocido anteriormente como relés. Los IEDs es el nuevo nombre que se le ha dado a lo que se conocía como antes como relés para 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.
* **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**”).

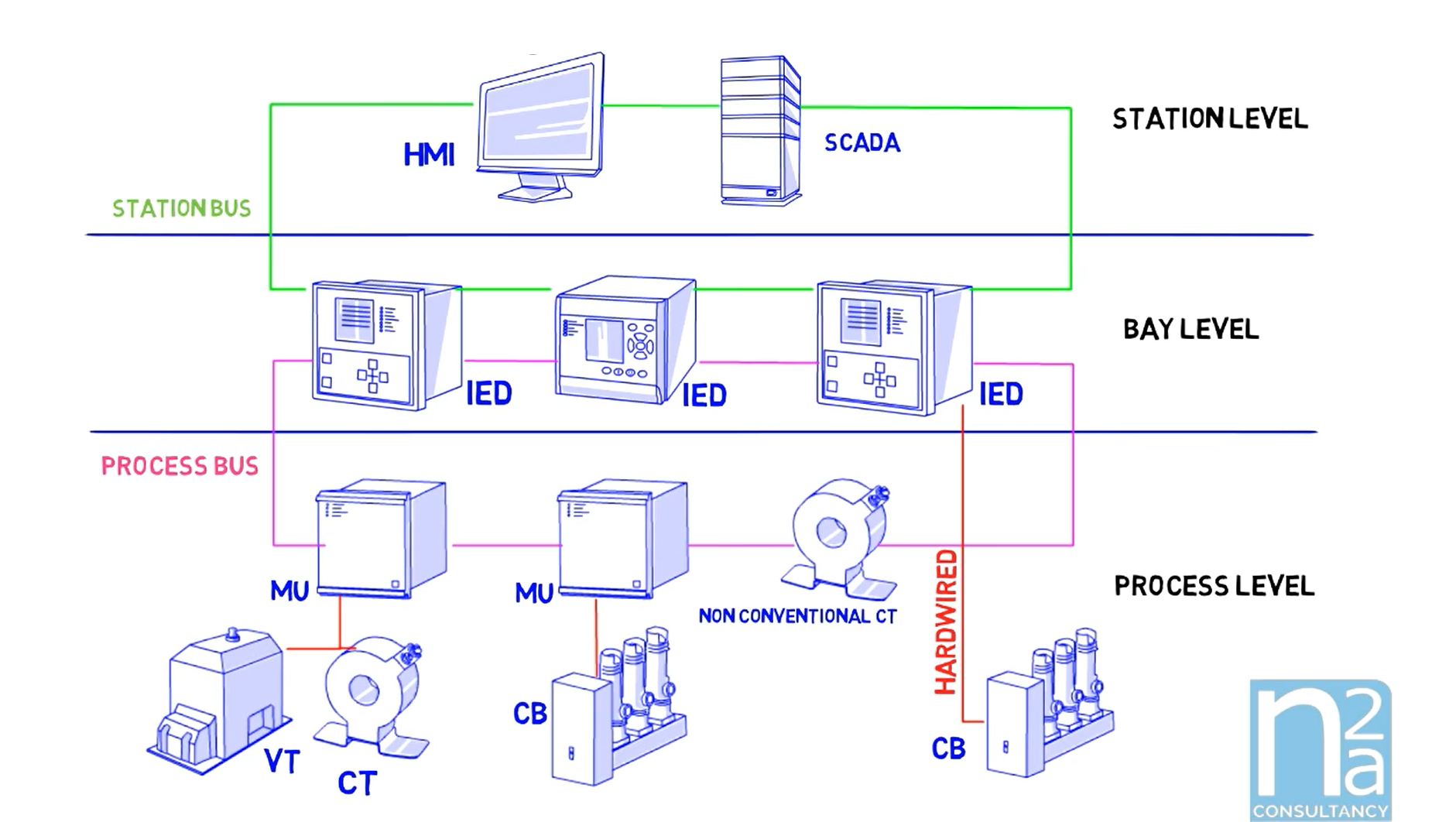


Ilustración 22. Arquitectura protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

### MODELADO DE DATOS IEC 61850

El protocolo 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*”, que traducido al español, significa **Dispositivo Físico**. Esto lo que quiere decir es que cada dispositivo físico presentara la misma estructura de datos, cambiando sus valores y especificaciones.

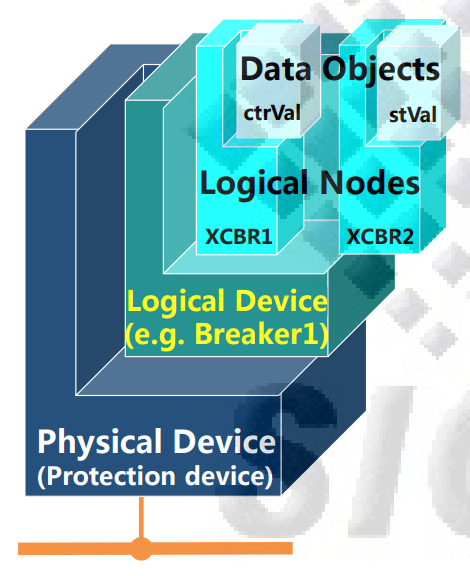


Ilustración 2. Estructura de datos del protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

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.

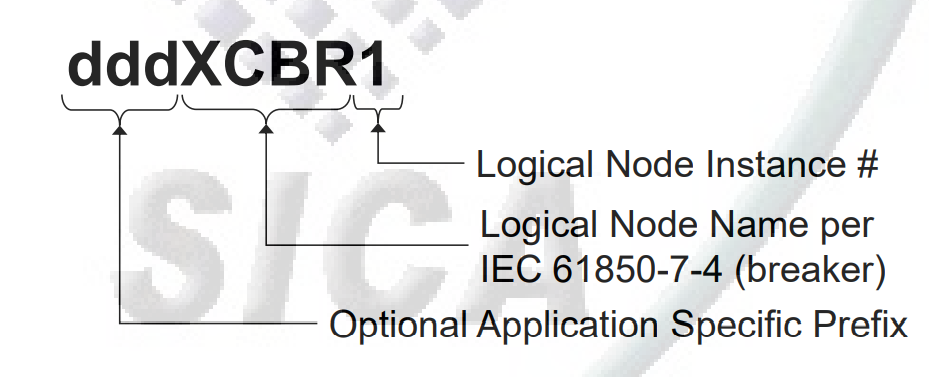


Ilustración 22. Nomenclatura de un Logical Node (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

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 22,** 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

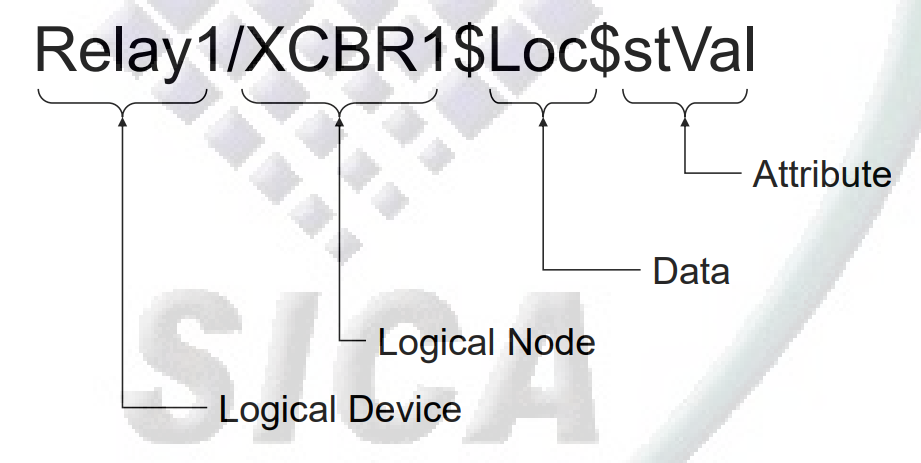


Ilustración 23. Nomenclatura de un objeto (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

Por otro lado tenemos la estructura de instanciación de un objeto en el estándar IEC 61850. Como se puede apreciar en la **figura 23,** 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.

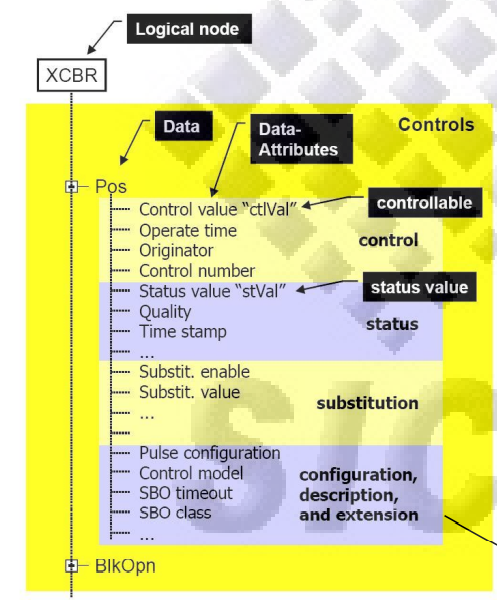


Ilustración 22. Jerarquía datos de un dispositivo lógico en el protocolo IEC 61850 (Fuente: extraído de MANUALES IEC61850 dados por SICA SA)

### MODELOS DE COMUNICACIÓN

Para conocer a fondo el estándar IEC 61850, es necesario saber la estructura y servicios que maneja el mismo. Tomando como base la arquitectura y estructura del modelo TCP/IP, seremos capaces de comprender que servicios de comunicación se usan en las distintas capas.

El Internet que todos conocemos está basado principalmente en 4 capas distinguidas (reflejadas en el modelo TCP/IP), lo que significa cuatro niveles independientes de servicios para entregar la información. A continuación, se describirá brevemente estas 4 capas:

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

Es la encargada de transferir los datos de un punto a otro mediante el uso de un simple comando. Como por ejemplo la aplicación World Wide Web (www) es usada por todos los navegadores de internet para acceder al contenido de una página web.

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

Esta capa se encuentra justo por debajo de la capa de transporte y la cual se encarga de chequear que la información ha sido entregada correctamente a su destinatario.

* **Capa de red (“Network Layer”).**

A través de esta capa de red, los datos son capaces de saltar a una red local distinta mediante el router.

* **Capa de enlace (“Link Layer”).**

Y la última capa, es la capa de enlace. La cual se encarga de transferir la información local a través de los switches. Internet nos da la opción de transmitir los datos de una forma segura de un punto a otro a través de los switches y routers, pero todos esos mecanismos son demasiado lentos para una aplicación en tiempo real.

Teniendo como base las cuatro capas básicas, será de fácil comprensión los protocolos creados por el estándar IEC 61850. Para poder activar el intercambio de datos entre todos los dispositivos vistos anteriormente, IEC 61850 ha definido 3 protocolos de comunicación para 3 aplicaciones distintas. MIN 3\*49

* MMS
* GOOSE
* SMV

# 

## VIRTUALIZACION DE IEDs CON LA HERRAMIENTA IED SCOUT

## USO DE NOZOMI GUARDIAN PARA PROTECCION DE IEDs