****

**Escuela de Ingenierías**

**Industrial, Informática y Aeroespacial**

**GRADO EN INGENIERÍA INFORMÁTICA**

Trabajo de Fin de Grado

ANÁLISIS DE CIBERSEGURIDAD EN SUSESTACIONES CON EL ESTANDAR IEC 61850

CYBERSECURITY ANALYSIS IN SUBSTATIONS WITH IEC 61850 STANDARD

Autor: Marcos González Maestre

Tutor: Isaías García Rodríguez

(Julio, 2022)

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

**Índice**

[1 Introducción 6](#_Toc104460979)

[1.1 INTRODUCCIÓN 6](#_Toc104460980)

[1.2 JUSTIFICACIÓN DEL PROYECTO 7](#_Toc104460981)

[1.3 OBJETIVOS DEL PROYECTO 7](#_Toc104460982)

[1.4 ESTRUCTURA DEL PROYECTO 7](#_Toc104460983)

[1.5 METODOLOGÍA 7](#_Toc104460984)

[2 Planificación y gestión del proyecto 8](#_Toc104460985)

[2.1 ALCANCE DEL PROYECTO 8](#_Toc104460986)

[2.2 PLANIFICACIÓN 8](#_Toc104460987)

[3 Estado del arte 9](#_Toc104460988)

[3.1 ESTO ES UNA PRUEBA 9](#_Toc104460989)

[4 Tecnologías usadas 9](#_Toc104460990)

[4.1 VMWARE WORKSTATION PRO 9](#_Toc104460991)

[4.2 NOZOMI NETWORKS 10](#_Toc104460992)

[4.3 WIRESHARK 12](#_Toc104460993)

[4.3.1 PARA QUE SE USA WIRESHARK 13](#_Toc104460994)

[4.4 IED SCOUT 13](#_Toc104460995)

[4.5 ADVANCED IP SCANNER 15](#_Toc104460996)

[4.6 TCPDUMP 15](#_Toc104460997)

[4.7 IEDs 17](#_Toc104460998)

[5 Núcleo del trabajo 18](#_Toc104460999)

[5.1 CIBERSEGURIDAD 18](#_Toc104461000)

[5.1.1 HISTORIA DE LA CIBERSEGURIDAD 20](#_Toc104461001)

[5.1.2 PRINCIPALES ATAQUES CIBERNETICOS 25](#_Toc104461002)

[5.1.3 AMBITOS DE LA CIBERSEGURIDAD 28](#_Toc104461003)

[5.1.4 CIBERSEGURIDAD EN LA ACTUALIDAD 28](#_Toc104461004)

[5.1.5 CIBERSEGURIDAD APLICADA AL MUNDO INDUSTRIAL 28](#_Toc104461005)

[5.2 ESTÁNDAR IEC 61850 28](#_Toc104461006)

[5.2.1 INTRODUCCION AL IEC 61850. ¿QUÉ ES? 28](#_Toc104461007)

[5.2.2 ORÍGENES DEL ESTANDAR IEC 61850 28](#_Toc104461008)

[5.2.3 ESTRUCTURA DEL IEC 61850 28](#_Toc104461009)

[5.2.4 MODELOS DE COMUNICACIÓN 29](#_Toc104461010)

[5.3 Wireshark 29](#_Toc104461011)

[5.4 Nozomi 29](#_Toc104461012)

**Índice de Ilustraciones**

[Ilustración 1. Logotipo VMWare Workstation Pro (Fuente: https://www.vmware.com/es/products) 10](#_Toc104538361)

[Ilustración 2. Panel de configuración de NOZOMI mediante VMWARE (Fuente: propia) 11](#_Toc104538362)

[Ilustración 3. Logo de la herramienta Nozomi Networks(Fuente: https://www.nozominetworks.com) 12](#_Toc104538363)

[Ilustración 4. Panel principal Nozomi Guardian (Fuente: Elaboración propia) 13](#_Toc104538364)

[Ilustración 5. Logo de la herramienta Wireshark (Fuente: https://www.wireshark.org ) 13](#_Toc104538365)

[Ilustración 6. Logotipo Omicron Electronics (Fuente: https://www.acinel.com/omicron-es ) 15](#_Toc104538366)

[Ilustración 7. Logotipo Advanced IP Scanner (Fuente: https://www.advanced-ip-scanner.com/es ) 16](#_Toc104538367)

[Ilustración 7. Logotipo TCPDUMP (Fuente: https://www.tcpdump.org ) 17](#_Toc104538368)

[Ilustración 8. Resumen opciones de filtros TCPDUMP (Fuente: propia) 18](#_Toc104538369)

[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) 19](#_Toc104538370)

[Ilustración 10. Ordenador IBM PC-XT (Fuente: https://thedatacyclehub.com/wp-content/uploads/2019/12/TDCH-Ciberseguridad.jpg) 21](#_Toc104538371)

[Ilustración 10. Ordenador IBM PC-XT (Fuente: https://www.fdi.ucm.es/migs/catalogo/ibm\_pc\_xt/) 22](#_Toc104538372)

[Ilustración 11. Evolución ARPANET 1969-1982 (Fuente: https://pbs.twimg.com/media/FIBHzVqXwAMyNLR.jpg ) 23](#_Toc104538373)

[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) 23](#_Toc104538374)

[Ilustración 13. (Fuente: https://arc-anglerfish-arc2-prod-infobae.s3.amazonaws.com/public/EFPYZQ5RB5GLTMGKEOQJP4CZXI.jpg) 26](#_Toc104538375)

[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) 27](#_Toc104538376)

[Ilustración 14. Logotipo representativo al gusano Conficker. (Fuente: https://norfipc.com/img/articulos/virus-conficker.png) 27](#_Toc104538377)

[Ilustración 14. Logotipo representativo al virus Stuxnet. (Fuente: https://www.lapatilla.com/wp-content/uploads/2019/09/Stuxnet-virus.jpg?resize=640%2C345) 28](#_Toc104538378)

**Glosario de términos**

**Sniffer:**

**DSJKWDH**

**HEW:**

# Introducción

## INTRODUCCIÓN

## 

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

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

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

## JUSTIFICACIÓN DEL PROYECTO

## OBJETIVOS DEL PROYECTO

## ESTRUCTURA DEL PROYECTO

## METODOLOGÍA

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

# Planificación y gestión del proyecto

## ALCANCE DEL PROYECTO

## PLANIFICACIÓN

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

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

# Estado del arte

## ESTO ES UNA PRUEBA

# Tecnologías usadas

## VMWARE WORKSTATION PRO

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

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

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

)

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

Seguimps escribiendo

## NOZOMI NETWORKS

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

1. Nozomi Vantage
2. Nozomi Guardian
3. 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
* Descripcion general de activos
* Estado general
* Rendimiento total de red
* Flujo de alertas a lo largo del tiempo
* Ultimas alertas

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

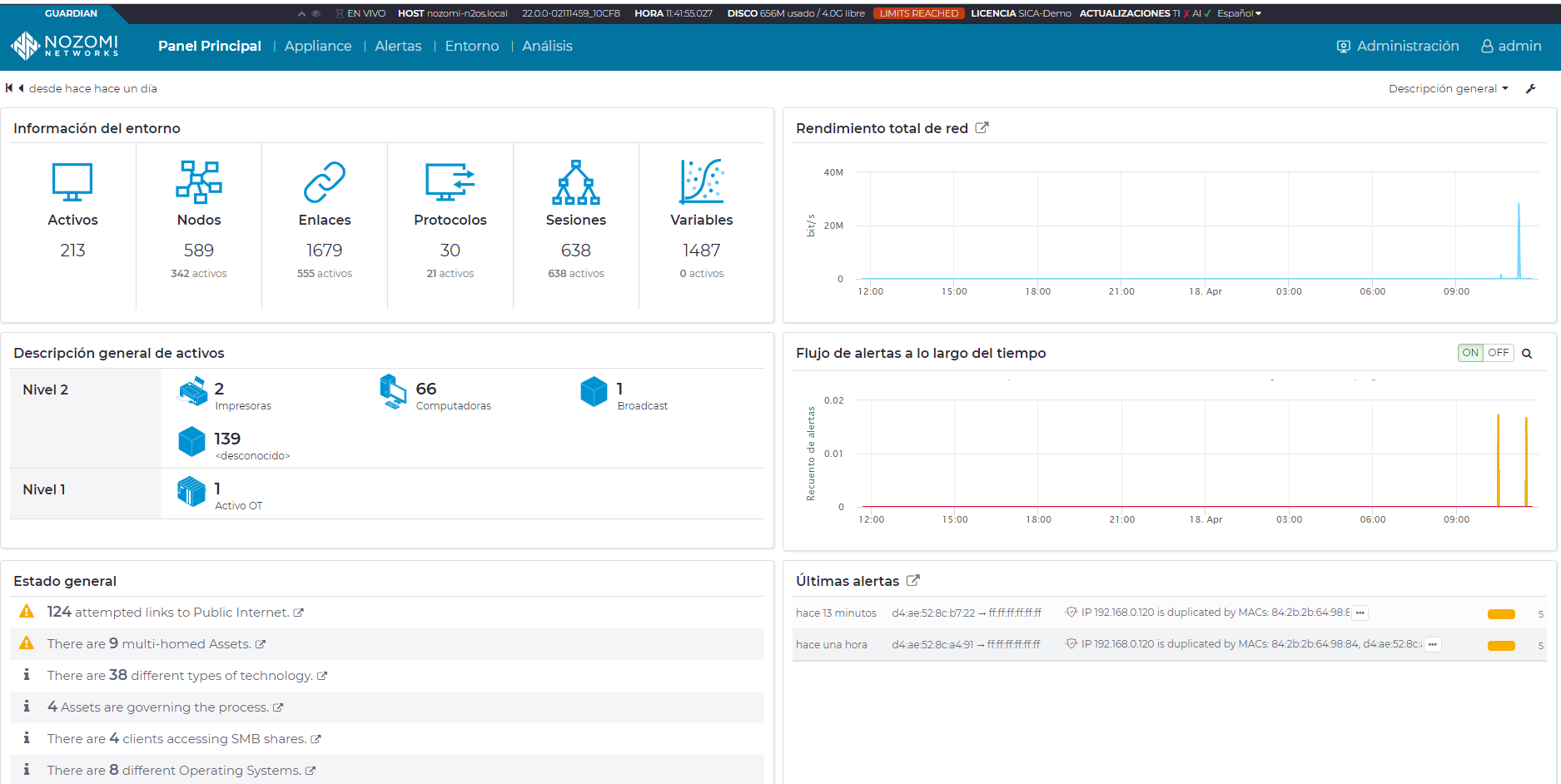


Ilustración 4. Panel principal Nozomi Guardian (Fuente: Elaboración propia)

## WIRESHARK

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

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

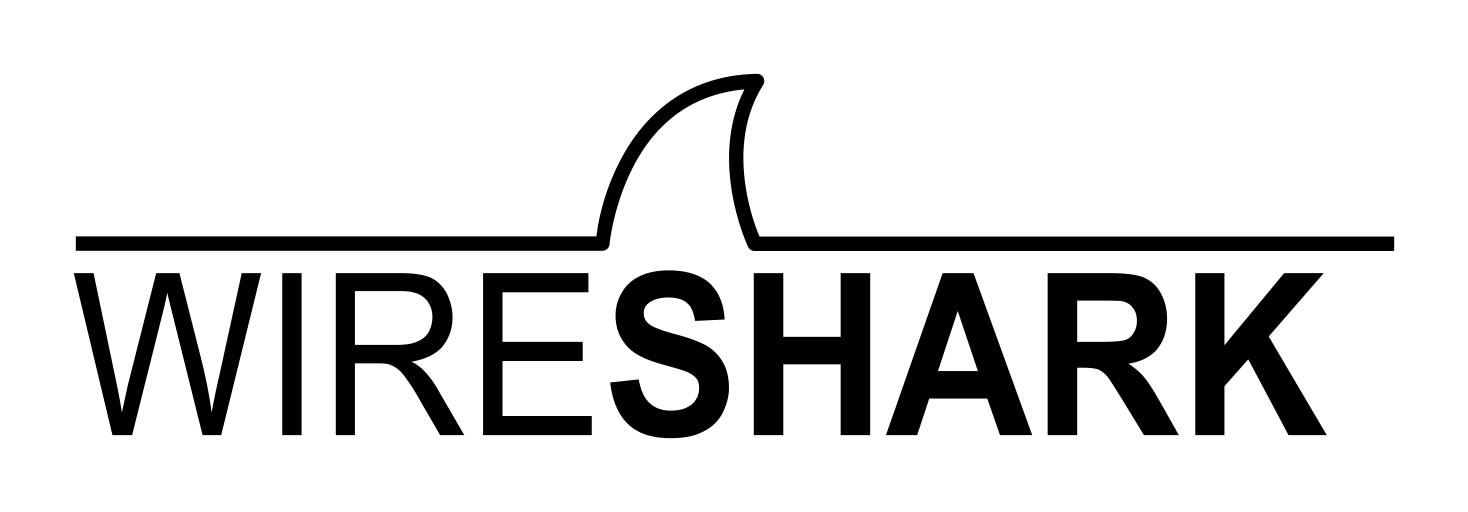


Ilustración 5. Logo de la herramienta Wireshark (Fuente: <https://www.wireshark.org> )

### PARA QUE SE USA WIRESHARK

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

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

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

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

## IED SCOUT

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



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

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

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

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

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

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

## ADVANCED IP SCANNER

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



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

## TCPDUMP

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



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

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

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

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

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

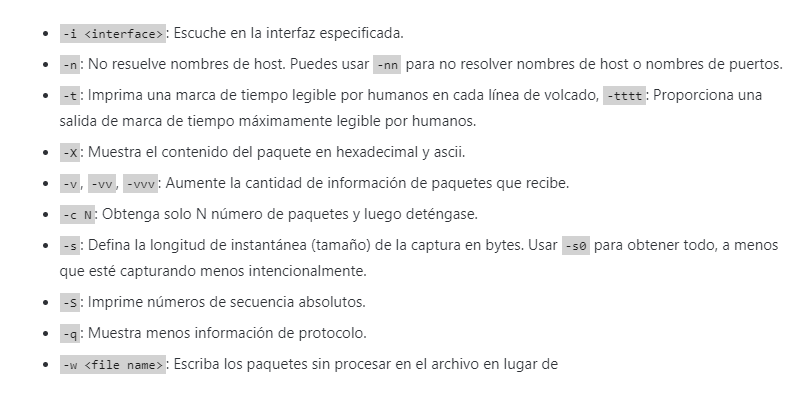


Ilustración 8. Resumen opciones de filtros TCPDUMP (Fuente: propia)

## IEDs

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

Tenemos varios tipos de IEDS. Que son los siguientes:

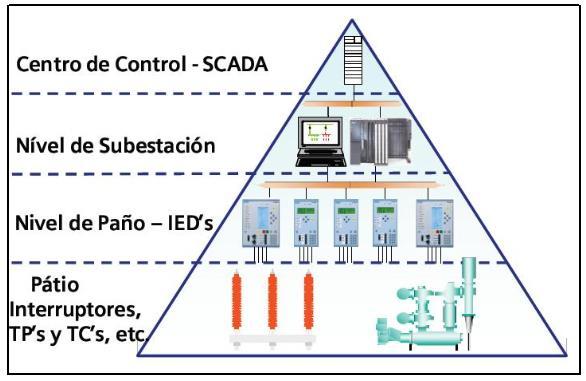


Ilustración 8. Niveles elementos subestaciones (Fuente: <https://www.google.com/search?q=tipos+ieds+electrica&client=opera&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiL3YT0huv2AhWsxYUKHffvDUQQ_AUoAXoECAEQAw&biw=1880&bih=939&dpr=1#imgrc=OJltEW2UdpVPiM>)

# Núcleo del trabajo

## CIBERSEGURIDAD

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

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

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

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

Ciberseguridad de software, de hardware, en redes, personal, 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. Ordenador IBM PC-XT (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.

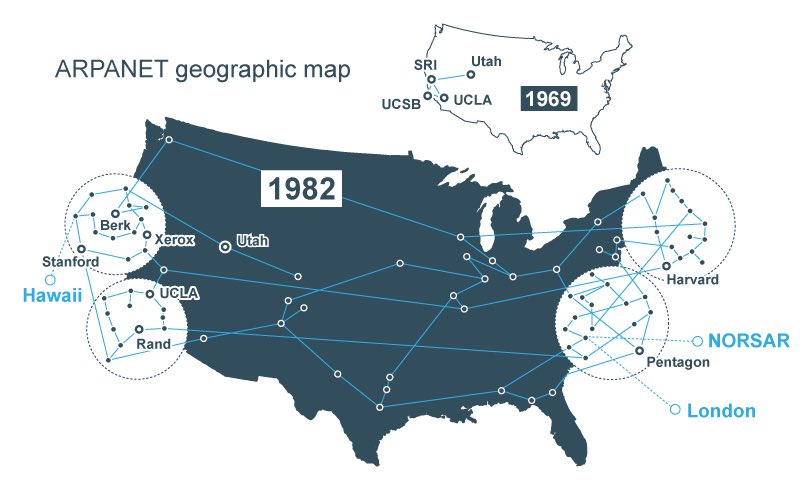


Ilustración 11. Evolución ARPANET 1969-1982 (Fuente: https://pbs.twimg.com/media/FIBHzVqXwAMyNLR.jpg )

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 fromato dela rchivo encontrado y lo transformaba a VBS.

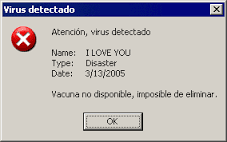


Ilustración 14. Alerta detección virus ILoveYou. (Fuente: https://sites.google.com/site/seguridadinformaticacmj/\_/rsrc/1433934964613/virus/i-love-you/i%20love%20you.png?height=250&width=400)

* **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.

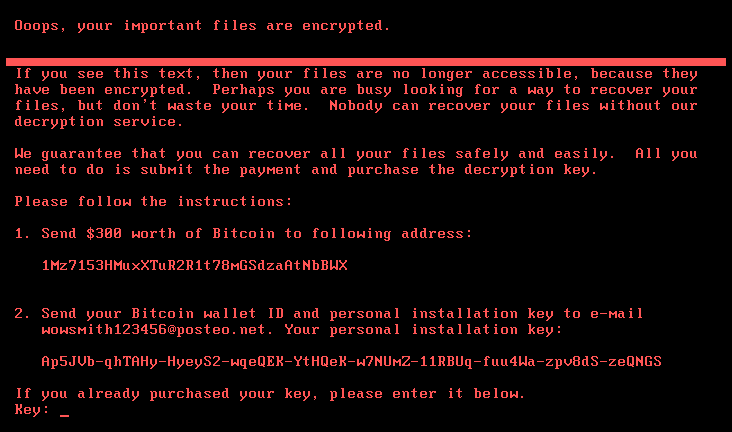


Ilustración 15. Pantalla rescate troyano Petya. (Fuente: <https://es.wikipedia.org/wiki/Petya_(malware)> )

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.

### 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.

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

Por su parte, en el ámbito empresarial no cabe duda de que Internet es la herramienta de trabajo por excelencia para la gran mayoría de las empresas, ya sea porque sus empleados son trabajadores del conocimiento (y ese conocimiento está vinculado a la Red) o bien porque muchas de sus operaciones industriales se realizan mediante herramientas conectadas a la Red.

En cuanto al ámbito de lo público, la segurización de las infraestructuras y de los datos que gestionan es una prioridad porque de ello depende nuestra confianza en el propio sistema. De hecho, a través de sus diferentes niveles de actuación (local, autonómico o nacional), la administración es responsable de cosas tan dispares como controlar el padrón municipal o la supervisión de infraestructuras críticas. Afortunadamente, tanto a nivel estatal como autonómico existen diversos organismos que velan por la ciberseguridad como puedes ver en la siguiente gráfica:

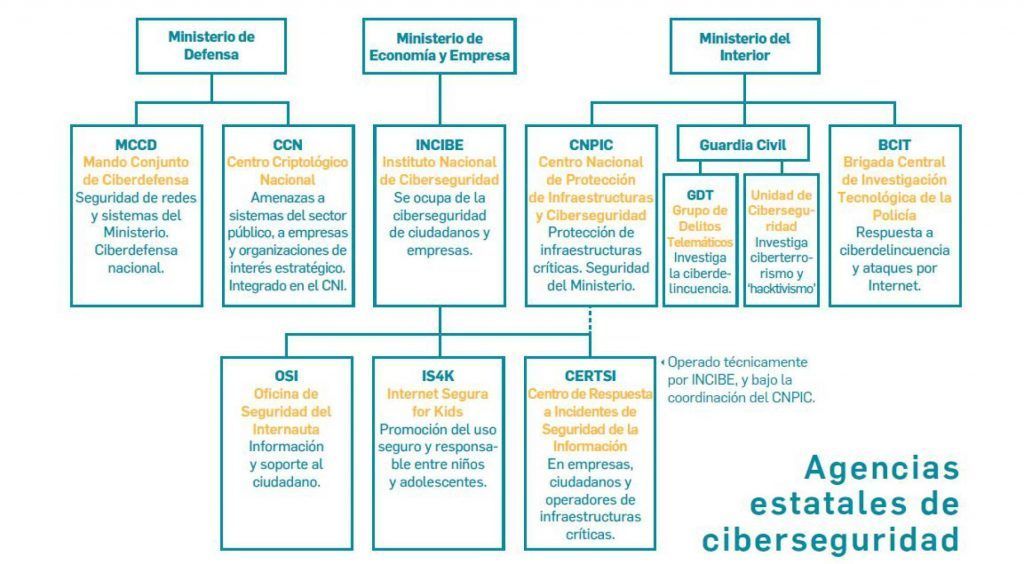
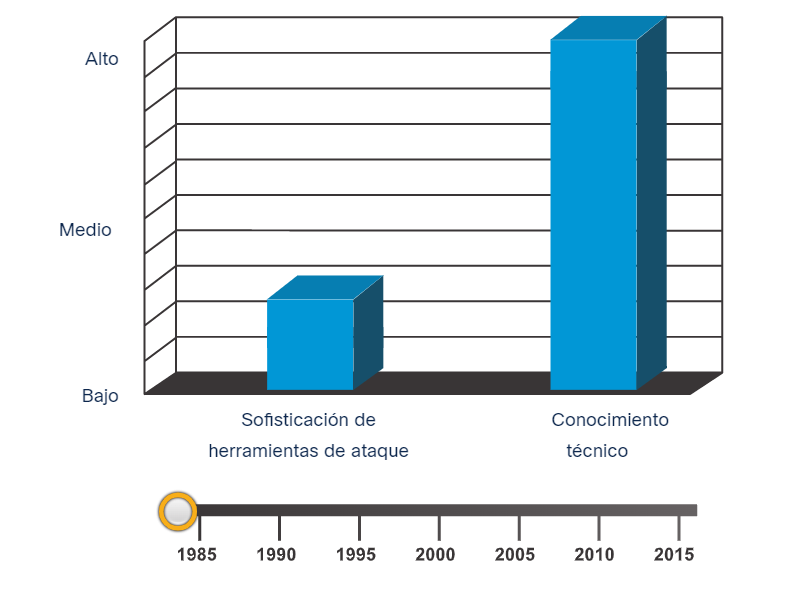
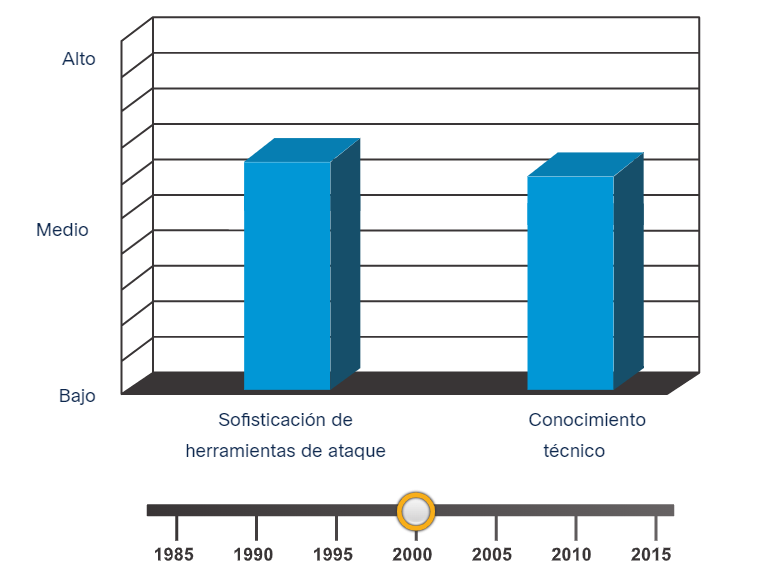
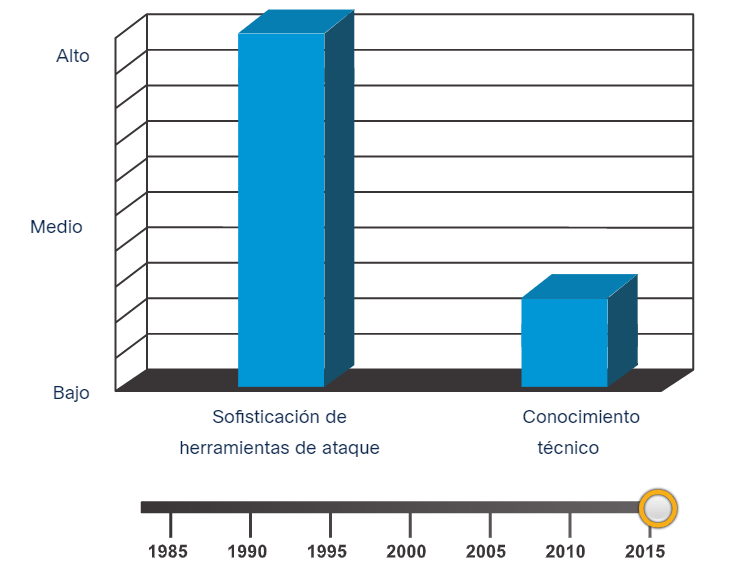


Ilustración 17. Agencias estatales de ciberseguridad. (Fuente: https://www.avast.com/es-es/c-wannacry )

### CIBERSEGURIDAD EN LA ACTUALIDAD







### CIBERSEGURIDAD APLICADA AL MUNDO INDUSTRIAL

## ESTÁNDAR IEC 61850

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

IEC 61850 es un estándar relacionado con

### ORÍGENES DEL ESTANDAR IEC 61850

### ESTRUCTURA DEL IEC 61850

### MODELOS DE COMUNICACIÓN

## Wireshark

## IED Scout

## Nozomi