Erasmus Plus Programme – KA2 Strategic Partnerships for higher education

IO1: Industrial Cyber Security Training Course for Technicians in Industry 4.0

Spanish Version

Project № 2018-1-ES01-KA203-050493

This project has been funded with support from the European Commission. This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein

Co-funded by the
Erasmus+ Programme
of the European Union

MÓDULO 1

Sistemas Industriales - Componentes y Características

1.1 Componentes de un Sistema de Control Industrial

Description

1.1 Componentes de un Sistema de Control Industrial

Table of contents

El Sistema de control industrial (ICS) es un término general que abarca varios tipos de sistemas de control, redes e instrumentos asociados que se utilizan para controlar procesos industriales. Tal y como se muestra en la Figura 1.1, el control de procesos se implementa utilizando bucles en los que el valor de una variable de proceso (PV) medida se ajusta automáticamente para igualar al valor del punto de ajuste (SP) deseado. Incluye el sensor de proceso, la función de controlador y el elemento final de control (FCE) necesarios para el control automático..

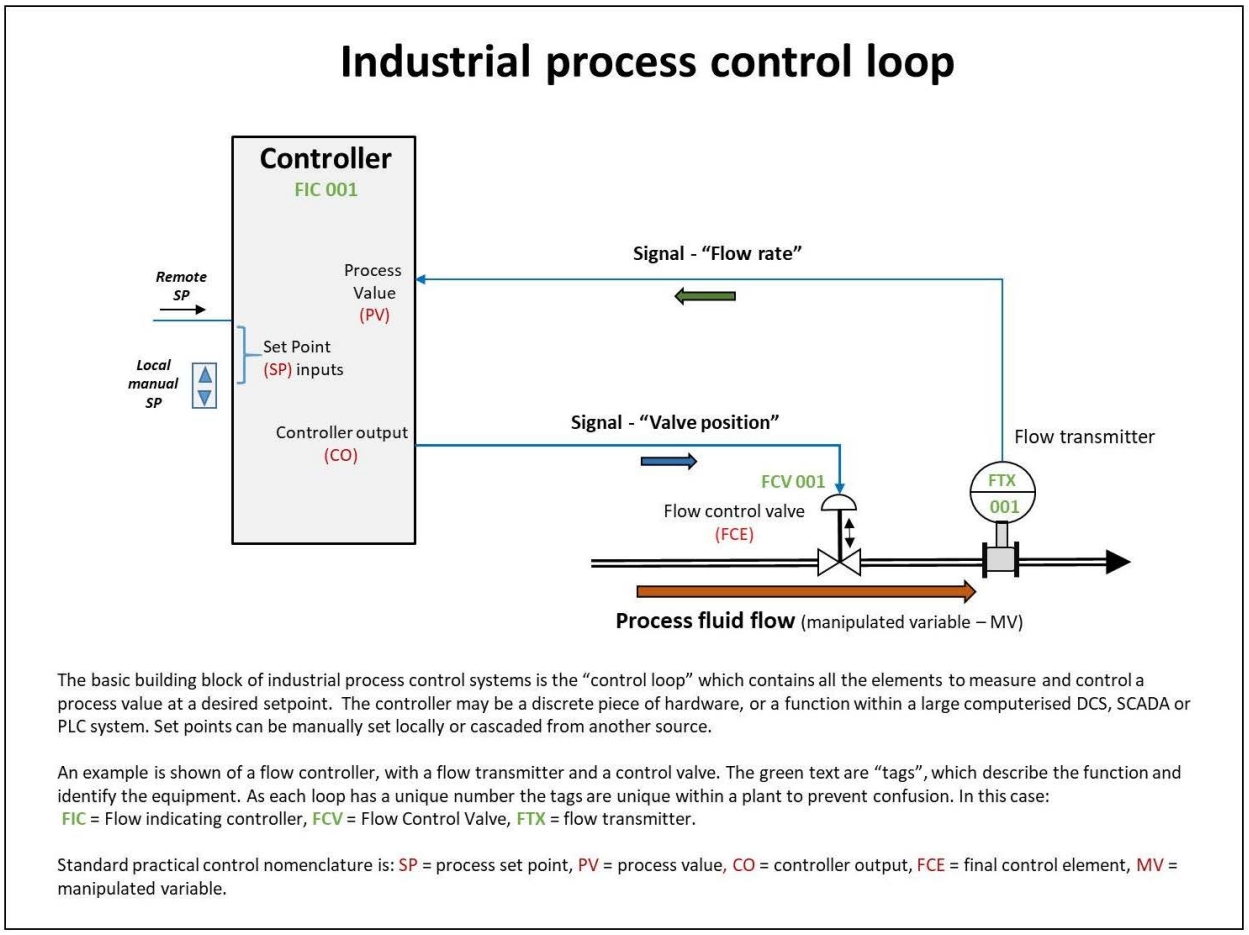


Figura 1.1 - Bucle de control del proceso industrial (fuente: Wikipedia)

Dichos sistemas pueden variar, pueden ser varios controladores modulares montados en un panel hasta grandes sistemas de control distribuidos interconectados e interactivos con miles de conexiones de campo. Todos los sistemas reciben datos procedentes de sensores remotos que miden las variables del proceso, las comparan con los puntos de ajuste deseados y obtienen funciones de comando que se utilizan para controlar un proceso a través de los elementos de control finales, como las válvulas de control.

Existen varios tipos de ICS, los más comunes son los sistemas de **sistemas de control y de adquisición de datos** (**SCADA**) y los **Sistemas de Control Distribuido (DCS)**. En la práctica, los grandes sistemas SCADA han aumentado tanto que hoy son muy similares a los sistemas de control distribuido en función, con la excepción de que emplean múltiples medios para interactuar con la planta.

Como se muestra en el diagrama de la Figura 1.2, los ICS están integrados en las empresas industriales. El personal de gestión utiliza los datos de la planta de fabricación y toma decisiones basadas en estos, lo que resulta en planes que se transfieren al nivel de producción y deben llevarse a cabo utilizando recursos controlados por el ICS.

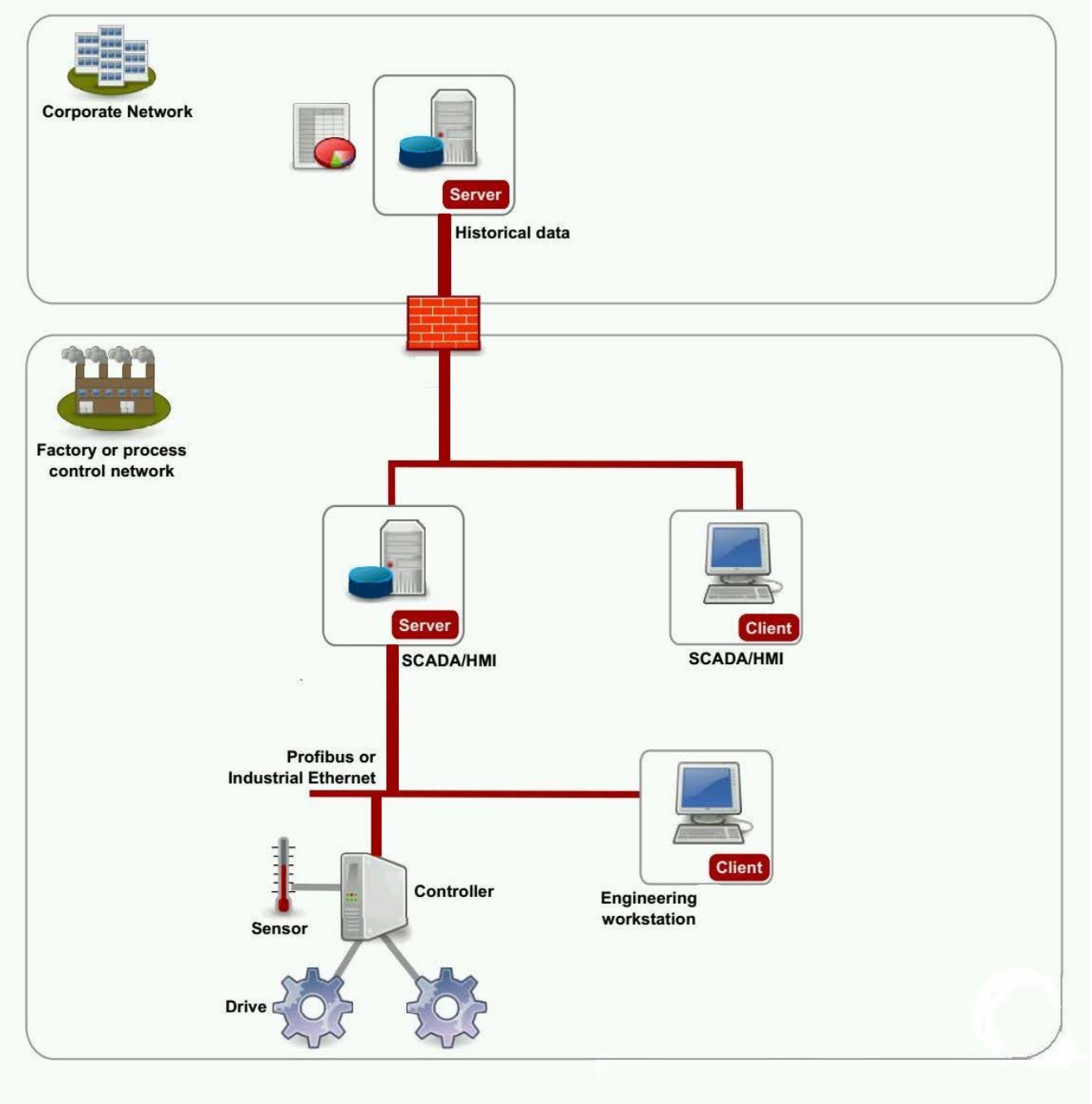


Figure 1.2 - Integration de un SCI en una empresa (fuente: Open Security Archive)

Un caso específico de ICS es el **sistema instrumentado de seguridad (SIS)** que consiste en un conjunto diseñado de controles de hardware y software que se utilizan especialmente en **sistemas de procesos críticos** como los que se utilizan en **refinerías, instalaciones químicas y nucleares** para proporcionar protección, como abrir/cerrar una válvula crítica para reducir el peligroso exceso de presión de gas o la alta temperatura del líquido.

Los sistemas instrumentados de seguridad están compuestos por los mismos tipos de elementos de control (incluyendo sensores, solucionadores lógicos, actuadores y otros equipos de control) que los sistemas de control de procesos básicos (BPCS). Sin embargo, todos los elementos de control de un SIS se dedican exclusivamente al correcto funcionamiento del SIS. Los **sistemas de apoyo**, como la energía, el aire de los instrumentos y las comunicaciones, son generalmente necesarios para el funcionamiento del SIS. Los sistemas de apoyo deben estar diseñados para proporcionar la **integridad y fiabilidad** requeridas por estos sistemas.

Como norma general, los SCI se clasifican en **5 niveles**, como se muestra en la Figura 1.3. Cada nivel tiene su propia funcionalidad y debe comunicarse con los otros niveles para poder llevar a cabo las acciones previstas.

La adquisición de datos comienza en el **Unidad de Terminal Remoto (RTU)** o **Controlador Lógico Programable (PLC)** de nivel 1 e incluye lecturas de instrumentación e informes de estado del equipo que se comunican al SCADA del nivel 2 según sea necesario. Luego, los datos se compilan y formatean de tal manera que un operario de sala de control que utiliza la HMI (Interfaz hombre-máquina) puede tomar decisiones de supervisión para ajustar los controles del RTU o PLC. También se le pueden remitir los datos a un historico, a menudo basado en un sistema de gestión de **bases de datos**, para permitir la realización de auditorías de analísis de tendencias y de otro tipo.

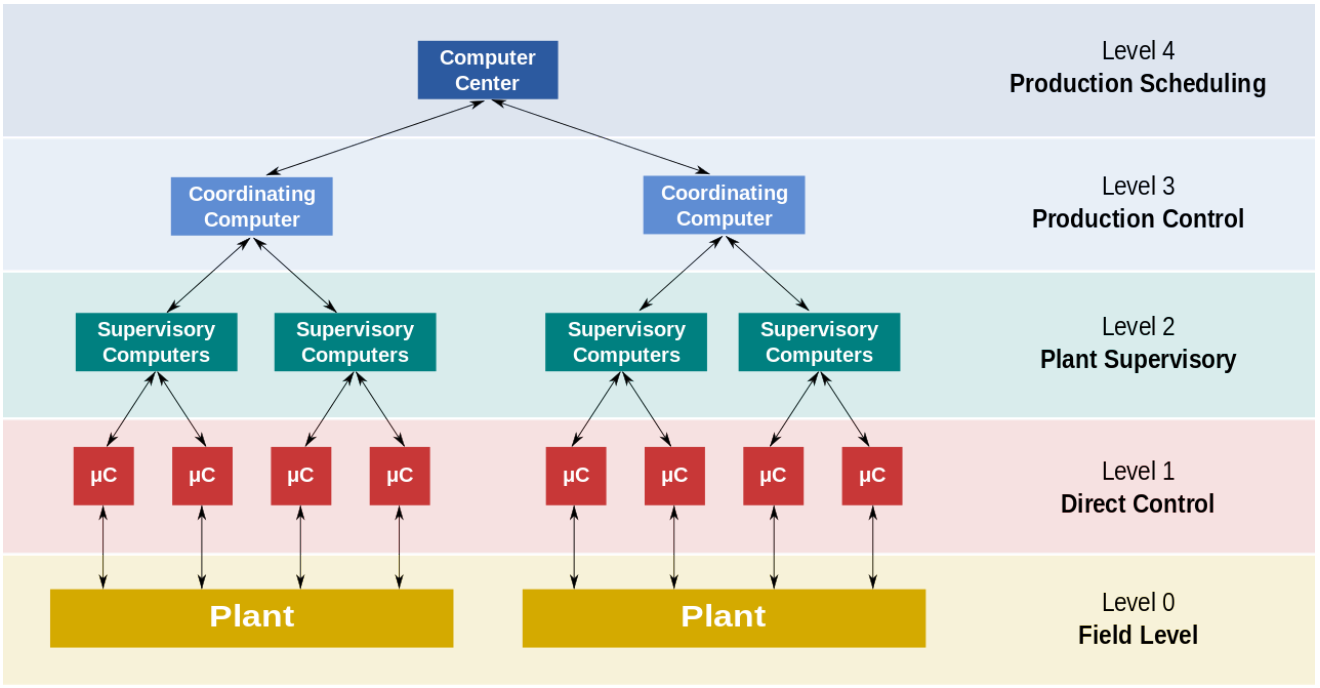


Figure 1.3 - Niveles SCI (fuente: Wikipedia)

Este nivel contiene los dispositivos de campo tales como **sensores** y elementos de control finales o **actuadores**.

En su definición más amplia, un sensor es un dispositivo, módulo o subsistema cuyo propósito es detectar eventos o cambios en su entorno y enviar la información a otra electrónica, frecuentemente un procesador de ordenador. Un sensor siempre se utiliza con otros componentes electrónicos.

Los sensores (la Figura 1.4 muestra un sensor IR) se utilizan en objetos cotidianos como botones sensibles al tacto (sensor táctil) y en procesos industriales para medir diferentes magnitudes (presión, posición, temperatura...).

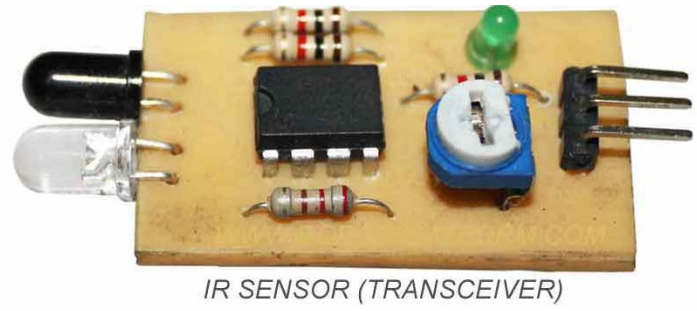


Figura 1.4- sensor IR (fuente: Wikipedia)

Un actuador (la Figura 1.5 muestra una válvula hidráulica) es un componente de una máquina, responsable de mover y controlar un mecanismo o sistema, por ejemplo, abriendo una válvula. En términos sencillos, es un "motor".

Un actuador requiere una señal de control y una fuente de energía. La señal de control es de energía relativamente baja y puede ser voltaje o corriente eléctrica, presión neumática o hidráulica, o incluso energía humana. Cuando recibe una señal de control, un actuador responde convirtiendo la energía de la señal en un movimiento mecánico.

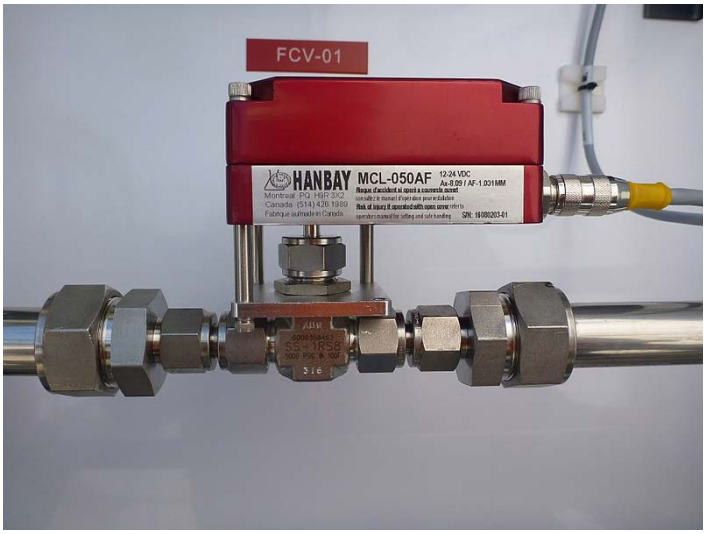


Figura 1.5- Válvula hidráulica (fuente: Wikipedia)

Este nivel contiene los módulos industrializados de entrada/salida (E/S) y sus procesadores electrónicos distribuidos asociados. Contiene controladores lógicos programables (PLC) o unidades terminales remotas (RTU).

Un **controlador lógico programable (PLC)** es un ordenador digital industrial reforzado y adaptado para el control de procesos de fabricación, tales como líneas de montaje, dispositivos robóticos, o cualquier actividad que requiera un control de alta fiabilidad y facilidad de programación y diagnóstico de fallos de proceso.

Un PLC (Figura 1.6) es un ejemplo de un **sistema en tiempo real**, ya que los señales de salida deben producirse en respuesta a las condiciones de entrada en un tiempo limitado, de lo contrario se puede producir una operación incorrecta.

Figura 1.6- controlador lógico programable (PLC) (fuente: Wikipedia)

La figura 1.7 muestra una **unidad terminal remota (RTU)**, un dispositivo electrónico controlado por microprocesador que conecta objetos en el mundo físico a un sistema de control distribuido o a un sistema SCADA (sistemas de control y de adquisición de datos) mediante la transmisión de datos de telemetría a un sistema maestro. Se emplean los mensajes del sistema maestro de supervisión para controlar objetos conectados. Otros términos que pueden usarse para hacer referencia al RTU son "unidad de telemetría remota" y "unidad de telecontrol remoto".

Figura 1.7- unidad terminal remota (RTU) (fuente: Wikipedia)

Este nivel contiene los **ordenadores de supervisión**, que cotejan la información de los nodos procesadores del sistema (PLC´s) y proporcionan las pantallas de control del operario.

El nivel 2 contiene el software **SCADA** y la plataforma de procesamiento del conjunto del sistema. El software SCADA sólo existe en este nivel de supervisión, ya que las acciones de control las realizan automáticamente las RTUs o PLCs de Nivel 1. Las funciones de control de SCADA están generalmente restringidas a la intervención básica de nivel superior o de supervisión. Por ejemplo, un PLC puede controlar el flujo de agua de enfriamiento a través de parte de un proceso industrial a un nivel de punto de referencia, pero el software del sistema SCADA permitirá a los operarios cambiar los puntos de referencia de dicho flujo.

El SCADA también permite que se muestren y registren las condiciones de **alarma**, tales como pérdida de flujo o alta temperatura. Un **lazo de control de retroalimentación** está controlado directamente por la RTU o PLC, pero el software SCADA hace un seguimiento el rendimiento general del bucle.

La **interfaz hombre-máquina (HMI)** (la figura 1.8 muestra un panel táctil HMI clásico) es la pantalla del responsable del sistema de supervisión. Presenta la información de la planta al personal de operación de manera gráfica y en forma de diagramas mímicos, que son una representación esquemática de la planta que se está controlando, y páginas de registro de alarmas y eventos. La HMI está conectada al ordenador de supervisión SCADA para proporcionar datos en tiempo real y poder controlar los diagramas, las pantallas de alarma y los gráficos de tendencias. En muchas instalaciones la HMI es la interfaz gráfica de usuario que emplea el operario, recoge todos los datos de dispositivos externos, crea informes, realiza alarmas, envía notificaciones, etc.

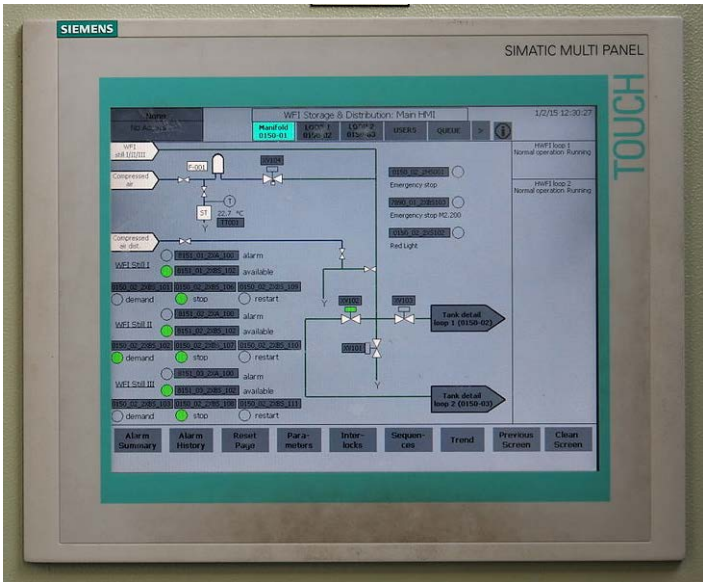


Figura 1.8- Panel tactil HMI (fuente: Wikimedia)

El núcleo del sistema SCADA es la **Estación de Trabajo de Supervisión**, que recopila datos sobre el proceso y envía comandos de control a los dispositivos conectados en campo. Se refiere al ordenador y al software responsable de la comunicación con los controladores de conexión de campo, que son RTUs y PLCs, e incluye el software HMI que se ejecuta en las estaciones de trabajo de los operarios.

En sistemas SCADA más pequeños, el ordenador de supervisión puede estar compuesto por un único PC. En dicho caso, la HMI formará parte de este ordenador. En sistemas SCADA más grandes, la estación maestra puede incluir varias HMI alojadas en computadoras cliente, múltiples servidores para la adquisición de datos, aplicaciones de software distribuidas y sitios de recuperación de desastres. Para aumentar la integridad del sistema, los múltiples servidores a menudo se configuran en una formación de doble redundancia o de espera en caliente, lo que proporciona un control y una supervisión continuos en caso de que se produzca un mal funcionamiento o una avería en el servidor.

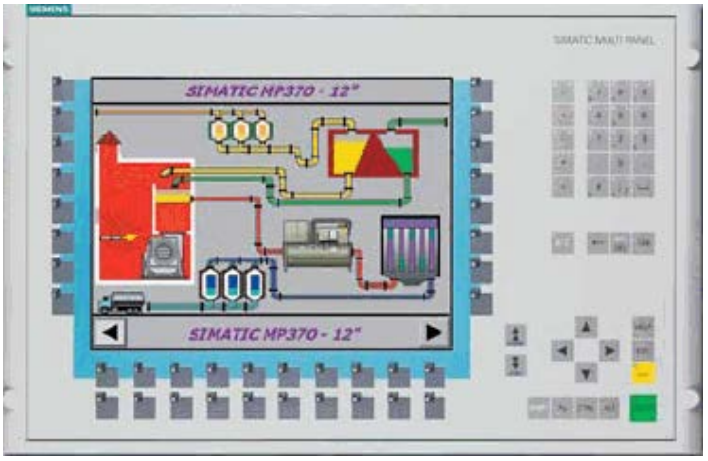


Figura 1.9- pantalla SCADA (fuente: Wikimedia)

Los niveles 3 y 4 no son estrictamente de control de proceso en el sentido tradicional, sino los niveles en los que se lleva a cabo el control de producción y la programación.

Este nivel no controla directamente el proceso, sino que se ocupa de **supervisar la producción**. Contiene sistemas MES, CMMS y WMS.

Los **sistemas de ejecución de la fabricación (MES)** son sistemas computarizados utilizados en la fabricación para rastrear y documentar la transformación de materias primas en productos terminados. MES proporciona información que ayuda a los responsables de la toma de decisiones de fabricación a comprender cómo se pueden optimizar las condiciones actuales en la planta de producción para mejorar el rendimiento de la producción. MES trabaja en tiempo real para permitir el control de múltiples elementos del proceso de producción. La Figura 1.10 muestra las diferentes partes de un sistema MES.

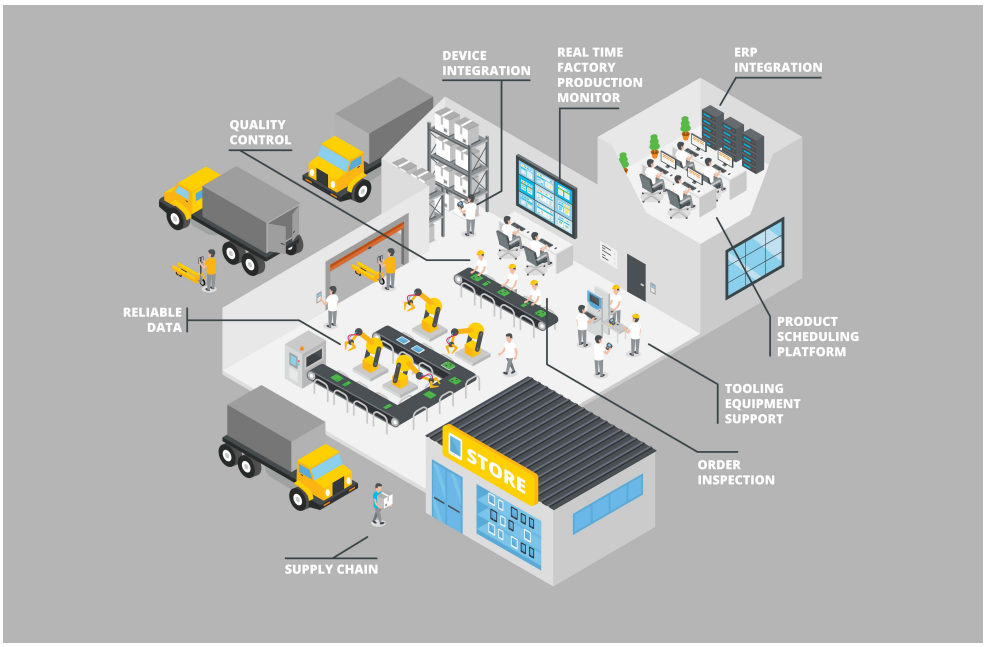


Figura 1.10- Organización para gestión MES (fuente: Wikimedia)

El **sistema de gestión de almacenes (WMS)** es una aplicación de software diseñada para soportar y optimizar la funcionalidad del almacén y la gestión del centro de distribución. Estos sistemas facilitan la gestión en su planificación diaria, organización, dotación de personal, dirección y control de la utilización de los recursos disponibles, para mover y almacenar materiales dentro, dentro y fuera de un almacén, al tiempo que apoyan al personal en el desempeño del movimiento y almacenamiento de materiales dentro y alrededor de un almacén.

El **sistema computerizado de gestión del mantenimiento (CMMS)** es un paquete de software que mantiene una base de datos informática de información sobre las operaciones de mantenimiento de una organización. Esta información tiene por objeto ayudar a los trabajadores de mantenimiento a realizar su trabajo de forma más eficaz (por ejemplo, determinar qué máquinas requieren mantenimiento y qué almacenes contienen las piezas de repuesto que necesitan) y ayudar a la dirección a tomar decisiones informadas (por ejemplo, calcular el coste de la reparación de averías de las máquinas en comparación con el mantenimiento preventivo de cada una de ellas, lo que puede dar lugar a una mejor asignación de recursos).

Este nivel contiene sistemas de planificación de los recursos institucionales y su principal función es proporcionar información y apoyo a la adopción de decisiones al personal directivo.

El **planificador de recursos empresariales (ERP)** suele denominarse una categoría de software de gestión empresarial, normalmente un conjunto de aplicaciones integradas, que una organización puede utilizar para recopilar, almacenar, gestionar e interpretar datos en tiempo real de estas numerosas actividades empresariales. Proporciona una visión integrada y continuamente actualizada de los procesos empresariales básicos utilizando bases de datos comunes las cuales mantiene un sistema de gestión de bases de datos.

Los sistemas ERP hacen un seguimiento de los recursos del negocio (efectivo, materias primas, capacidad de producción) y del estado de los compromisos del negocio: pedidos, órdenes de compra y nóminas. Las aplicaciones que componen el sistema comparten datos entre los distintos departamentos (fabricación, compras, ventas, contabilidad, etc.) que proporcionan los datos.

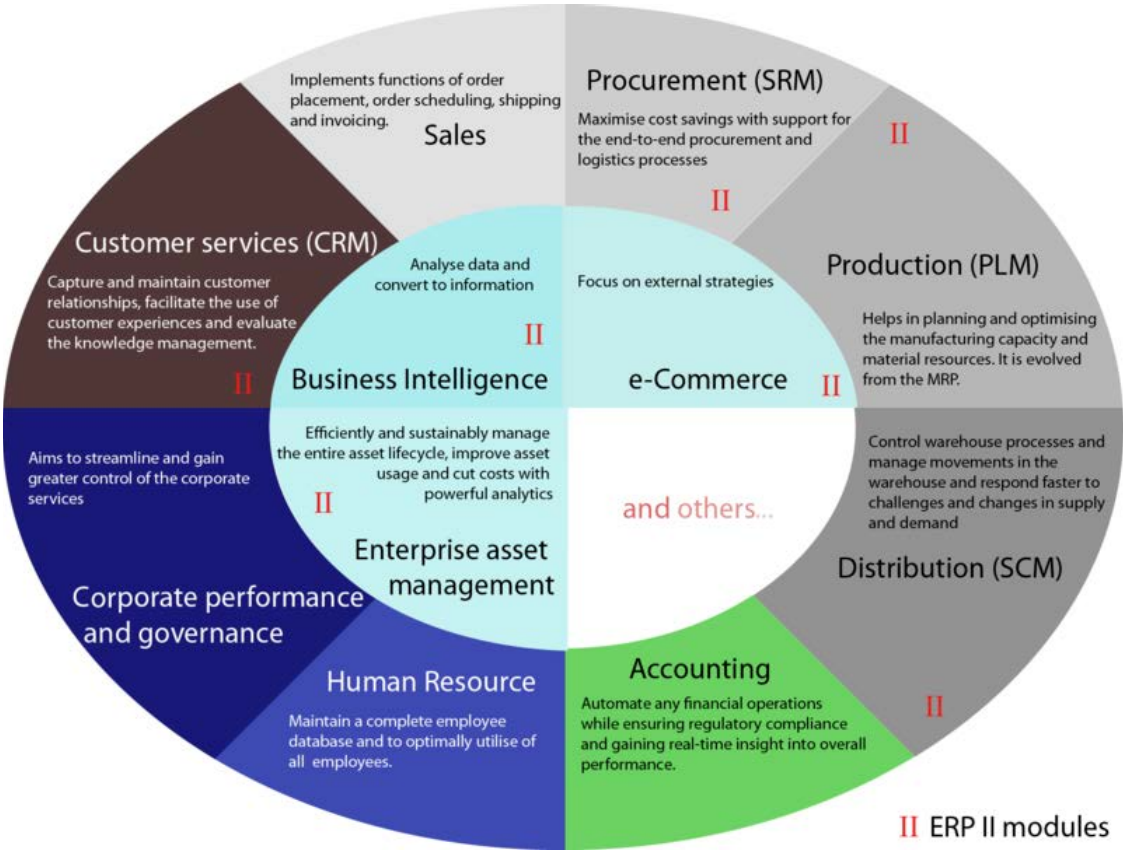


Figura 1.11- módulos ERP (fuente: Wikipedia)

1.2 Diseño y arquitectura de las redes informáticas

Description

1.2 Diseño y arquitectura de las redes informáticas

Table of contents

En el capítulo anterior se ha señalado que los Sistemas de Control Industrial (Figura 1.12) están compuestos por dispositivos interconectados que comparten y transfieren información entre sí. En este capítulo vamos a estudiar cuáles son las estructuras de red más comunes y cuáles son sus características.

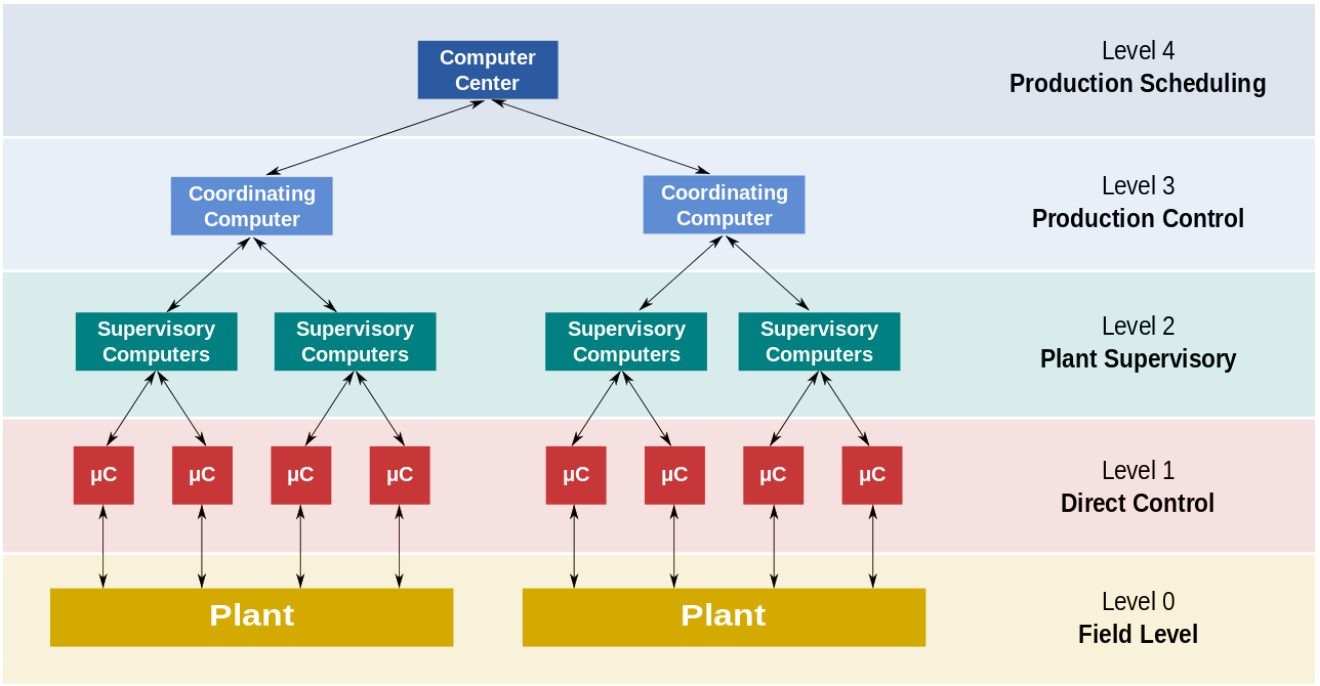


Figura 1.12- niveles SCI (fuente: Wikipedia)

Para ello, comenzaremos a estudiar el modelo de **Interconexión de Sistemas Abiertos** (**modelo OSI)**, que es un modelo conceptual que caracteriza y estandariza las funciones de comunicación de un sistema de telecomunicaciones o de computación sin tener en cuenta su estructura interna subyacente y su tecnología. Su objetivo es la interoperabilidad de diversos sistemas de comunicación con protocolos estándar. El modelo divide un sistema de comunicación en capas de abstracción. La versión original del modelo definía siete capas.

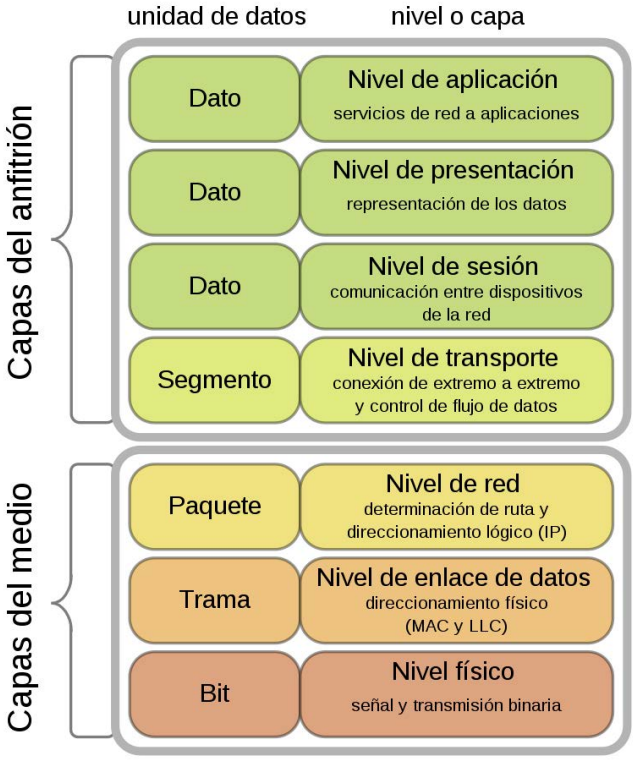


Figura 1.13- niveles OSI (fuente: Wikipedia)

La **capa física** es responsable de la transmisión y recepción de datos brutos no estructurados entre un dispositivo y un medio de transmisión físico.

Convierte los **bits** digitales en señales eléctricas, radioeléctricas u ópticas. Las especificaciones de las capas definen características como los niveles de tensión, el momento en el que se producen los cambios de tensión, las velocidades físicas de los datos, las distancias máximas de transmisión, el esquema de modulación, el método de acceso al canal y los conectores físicos.

La capa de **enlace de datos** proporciona transferencia de datos (**tramas**) de nodo a nodo. Se divide en dos subcapas:

- Capa de **control de acceso a medios (MAC)**: responsable de controlar cómo los dispositivos de una red obtienen acceso a un medio y permiso para transmitir los datos requeridos.
- Capa de **control de enlace lógico (LLC)**: responsable de identificar y encapsular los protocolos de la capa de red, y controla la comprobación de errores y la sincronización de tramas.

Los protocolos 802.3 **Ethernet** y 802.11 **Wi-Fi**, operan en la capa de enlace de datos.

La capa de **red** es la responsable de transferir secuencias de datos (llamadas **paquetes**) de un nodo a otro conectado en "redes diferentes". Estos nodos se identifican por una dirección de capa 3, que normalmente es la **dirección IP**.

Los **enrutadores** son responsables de transferir los paquetes a sus nodos de destino encontrando su camino a través de las diferentes redes.

La capa de **transporte** es responsable de transferir secuencias de datos (llamados **segmentos**) de una fuente a un host de destino, manteniendo al mismo tiempo la **calidad del servicio**. Los protocolos como **TCP y UDP** funcionan en este nivel. Los **puertos** definidos en este nivel son los puntos de entrada a los servicios públicos del servidor.

La capa de **sesión** controla los diálogos (también conocidos como conexiones o sesiones) entre ordenadores (entre aplicaciones locales y remotas).

La capa de **presentación** permite la comunicación entre sistemas con diferentes **sintaxis** y semántica (por ejemplo, códigos **ASCII** y EBCDIC, compresión de vídeo **MPEG** o estructura de datos **XML**).

La capa de **aplicación** interactúa con **aplicaciones de software** que implementan un componente de comunicación. Estos programas de aplicación (por ejemplo, servidores/clientes **FTP**, navegadores de Internet...) quedan fuera del ámbito del modelo OSI.

Los protocolos más conocidos de la Capa 7 son HTTP, Modbus.

En las redes de computadoras, el **encapsulamiento** es un método de diseño de protocolos de comunicación modulares en el que cada capa construye una unidad de datos de protocolo (**PDU**) agregando un **encabezado** que contiene información de control a la PDU desde la capa superior.

La capa física es responsable de la transmisión física de los datos,el posterior encapsulamiento de los bits en el nivel de enlace de datos (añadiendo la cabecera correspondiente a cada trama) permite la creación de **redes de área local**, el Protocolo de Internet **(IP)** proporciona direcciones globales de ordenadores individuales y el Protocolo de Control de Transmisión (**TCP**) selecciona el proceso o aplicación, es decir, el puerto que especifica el servicio, como un servidor Web o FTP.

Por ejemplo, en el conjunto de protocolos de Internet, el contenido de una página web se encapsula con una cabecera HTTP, luego con una cabecera TCP, una cabecera IP y, finalmente, se generan las tramas de nivel de enlace de datos. La trama se envía al nodo de destino como un flujo de bits, donde se desencapsula en las respectivas PDU y es interpretada en cada capa por el nodo receptor.

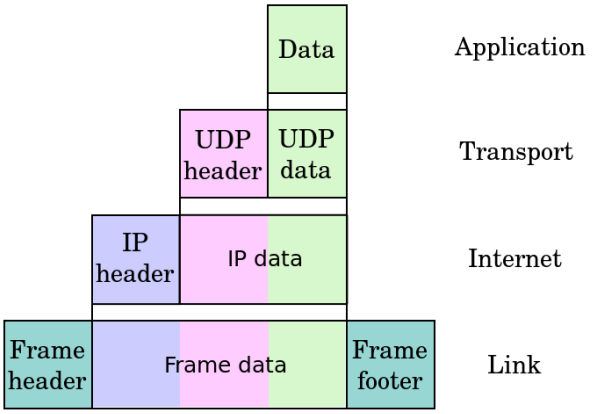


Figura 1.14- encapsulamiento de datos (fuente: Wikipedia)

La **topología** de red es la disposición de los elementos (enlaces, nodos, etc.) de una red de comunicaciones.

La **topología física** es la colocación de los diversos componentes de una red (por ejemplo, ubicación de dispositivos e instalación de cables), mientras que la **topología lógica** ilustra cómo fluyen los datos dentro de una red. Las distancias entre nodos, las interconexiones físicas, las velocidades de transmisión o los tipos de señal pueden diferir entre dos redes diferentes, aunque sus topologías pueden ser idénticas.

La topología física de una red es una preocupación particular de la capa física del modelo OSI.

En la topología en bus, las estaciones de trabajo se conectan directamente a un enlace común semidúplex lineal con algún medio como cable de par trenzado o cable coaxial, y reciben todo el tráfico generado por cada estación. Necesitan una resistencia de terminación al final de la línea, que elimina los rebotes de la señal.

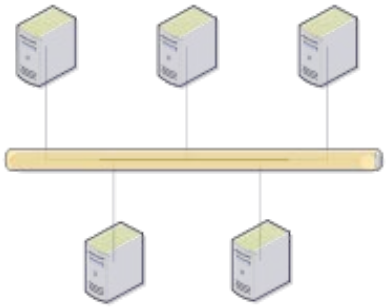


Figura 1.15- topología bus (fuente: Wikipedia)

En una red en estrella, cada host está conectado a un concentrador central (normalmente un conmutador), que retransmite los mensajes de las estaciones emisoras a las receptoras. Esta es una de las topologías de red de ordenadores más comunes.

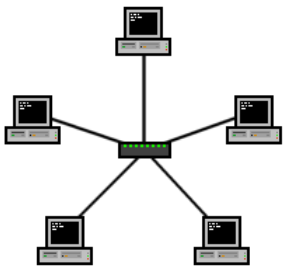


Figura 1.16- topología en estrella (fuente: Wikipedia)

Una red en anillo es una topología de red en la que cada nodo se conecta exactamente a otros dos nodos, formando una única ruta continua de señales a través de cada nodo. Los datos viajan de nodo en nodo, y cada nodo a lo largo del camino maneja cada paquete.

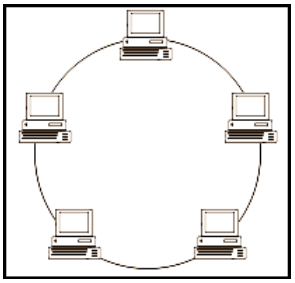


Figura 1.17- topología en anillo (fuente: Wikimedia)

Una red celular es una red de comunicación donde el último enlace es inalámbrico. La red está distribuida en áreas llamadas células, cada una servida por al menos un punto de acceso. Estos nodos proporcionan a la célula la cobertura de red que puede utilizarse para la transmisión de voz, datos y otros tipos de contenido.

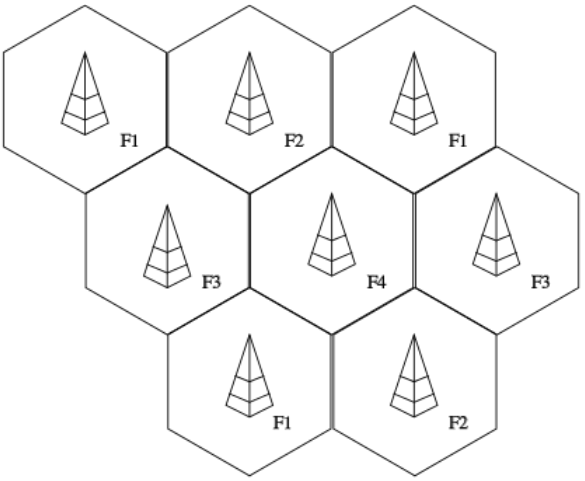


Figura 1.18- topología celular (fuente: Wikipedia)

El **ancho de banda y la latencia** (Figura 1.19) son dos de las características más relevantes en una red digital.

La latencia se expresa en una unidad de tiempo, generalmente milisegundos (ms). La latencia es la cantidad de tiempo que necesitan los datos para viajar de un punto a otro. Depende de la distancia física a la que deben viajar los datos a través de cables, redes y similares para llegar a su destino.

El ancho de banda se expresa en bits por segundo (**bps**). Se refiere a la cantidad de datos que se pueden transferir durante un segundo. Obviamente, cuanto más ancha es la tubería, más bits se pueden transferir por segundo. Y si su ancho de banda está congestionado, su latencia (retraso) aumenta.

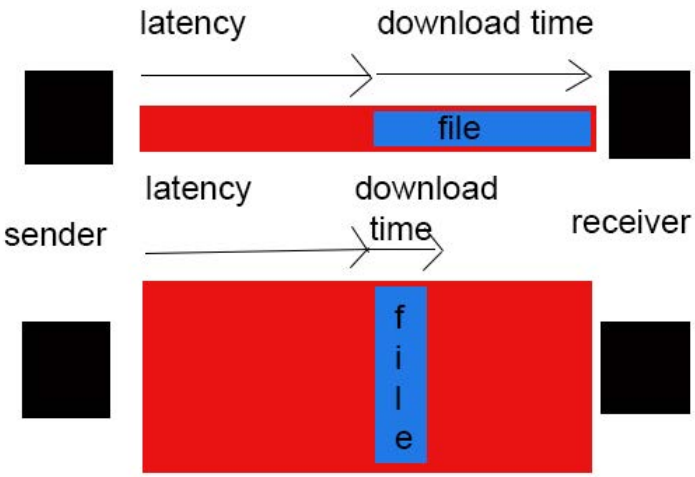


Figura 1.19- Latencia y ancho de banda en una transmisión (fuente: Wikipedia)

En la transmisión digital, la **tasa de error de bits (BER)** es el número de errores de bits por unidad de tiempo. La **proporción de bits erróneos (también BER)** es el número de errores de bits dividido por el número total de bits transferidos durante un intervalo de tiempo estudiado. La proporción de bits erróneos es una medida de rendimiento sin unidades, a menudo expresada como porcentaje.

Los bits recibidos de un flujo de datos a través de un canal de comunicación pueden alterarse debido a ruido, interferencia, distorsión o error de sincronización de bits. El parámetro relación **señal-ruido (SNR)** indica la proporción de la señal no deseada relacionada con la señal de transmisión de información. Como muestra la Figura 1.20, cuanto mayor es la SNR (mejor señal), menor es la BER (menos errores durante la transmisión).

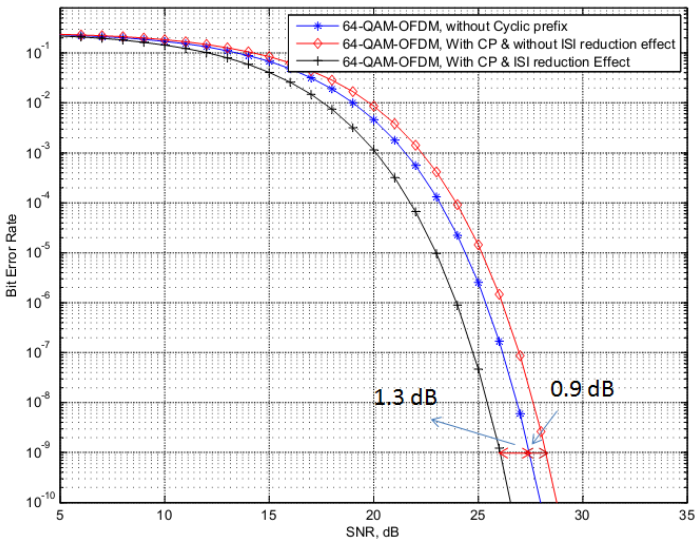


Figura 1.20- SNR vs BER (fuente: Wikipedia)

Una **red de área local (LAN)** es una red de computadoras que interconecta computadoras dentro de un área limitada, como una residencia, escuela, laboratorio, campus universitario o edificio de oficinas.

Ethernet y Wi-Fi son las dos tecnologías más comunes en uso para redes de área local.

1000BASE-T y el cableado estructurado son la base de la mayoría de las LAN comerciales actuales. Si bien el cable de fibra óptica es común para los enlaces entre los conmutadores de red, el uso de fibra en el ordenador de sobremesa es algo poco habitual

En una **LAN inalámbrica**, los usuarios tienen movimiento ilimitado dentro del área de cobertura.Las redes inalámbricas se han vuelto populares en residencias y pequeñas empresas, debido a su facilidad de instalación. La mayoría de las LAN inalámbricas utilizan Wi-Fi, ya que está integrado en teléfonos inteligentes, ordenadores de sobremesa y portátiles. A los huéspedes se les ofrece a menudo acceso a Internet a través de un servicio de hotspot.

Las LAN simples generalmente consisten en cableado y uno o más **conmutadores (switch)**. Un conmutador puede conectarse a un enrutador, módem de cable o módem ADSL para el acceso a Internet.

Una LAN puede incluir una amplia variedad de otros dispositivos de red, como **cortafuegos (firewall)**, balanceadores de carga y detección de intrusos en la red. Las LAN avanzadas se caracterizan por el uso de enlaces redundantes con conmutadores que utilizan el protocolo de árbol de expansión para evitar bucles, su capacidad para gestionar diferentes tipos de tráfico a través de la calidad de servicio (QoS) y su capacidad para segregar el tráfico con VLAN.

En las capas superiores de la red, los protocolos como NetBEUI, IPX/SPX, AppleTalk y otros eran comunes, pero el conjunto de protocolos de Internet **(TCP/IP)** ha prevalecido como estándar de elección.

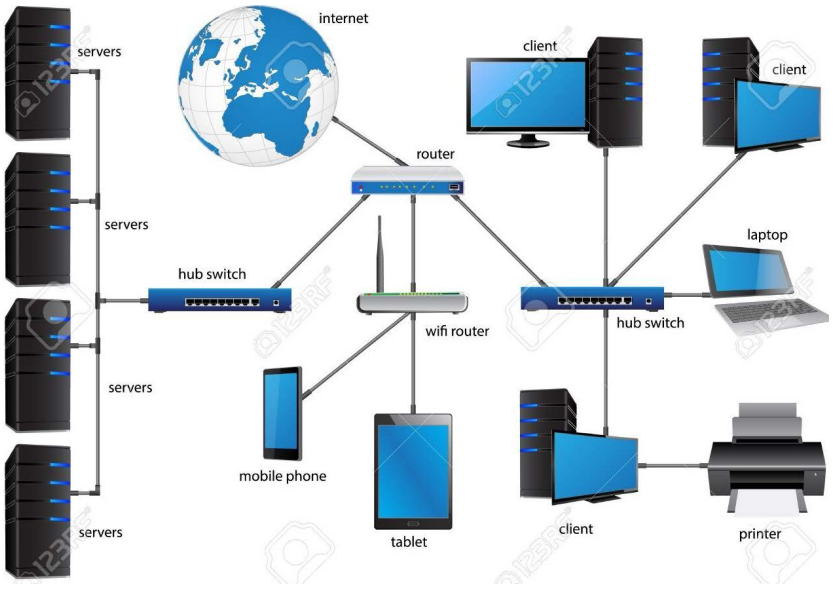


Figura 1.21- estructura de una red LAN (fuente: Wikimedia)

Las redes LAN pueden mantener conexiones con otras redes LAN a través de líneas alquiladas, servicios alquilados o a través de Internet utilizando tecnologías de **red privada virtual (VPN)**. Dependiendo de cómo se establezcan y aseguren las conexiones, y de la distancia implicada, estas redes LAN enlazadas también pueden clasificarse como una red de área metropolitana (MAN) o una **red de área extendida (WAN)**.

Una red de área extendida (WAN) es una red de telecomunicaciones que se extiende a lo largo de una gran distancia geográfica con el propósito principal de establecer redes informáticas. A menudo se establecen redes de área extendida con circuitos de telecomunicaciones alquilados.

Las empresas, la educación y las entidades gubernamentales utilizan redes de área amplia para transmitir datos al personal, los estudiantes, los clientes, los compradores y los proveedores de diversas ubicaciones en todo el mundo. En esencia, este modo de telecomunicación permite a una empresa llevar a cabo su función diaria de forma eficaz, independientemente de su ubicación. Internet puede considerarse una WAN.

Muchas WAN se construyen para una organización en particular y son privadas, por ejemplo, conectando las diferentes oficinas de una empresa con su sede central. Otros, construidos por proveedores de servicios de Internet, proporcionan conexiones desde la LAN de una organización a Internet.

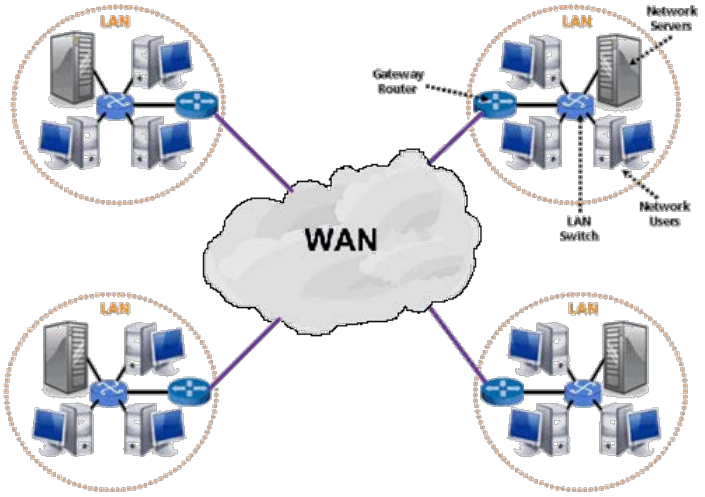


Figura 1.22 - red WAN (fuente: Wikimedia)

Existen muchas tecnologías disponibles para enlaces de red de área amplia, tales como líneas telefónicas con conmutación de circuitos, transmisión de ondas de radio y fibra óptica.

El método estandarizado mediante el cual se permite que los nodos transmitan información al bus o al cableado de red se denomina **protocolo**. El protocolo define las reglas, sintaxis, semántica y sincronización de la comunicación y los posibles métodos de recuperación de errores. Los protocolos pueden ser implementados por hardware, software o una combinación de ambos.

Los protocolos múltiples a menudo describen diferentes aspectos de una misma comunicación. Un grupo de protocolos diseñados para trabajar juntos se conoce como un conjunto de protocolos.

La figura 1.23 muestra los protocolos utilizados para la transmisión de información a través de internet.

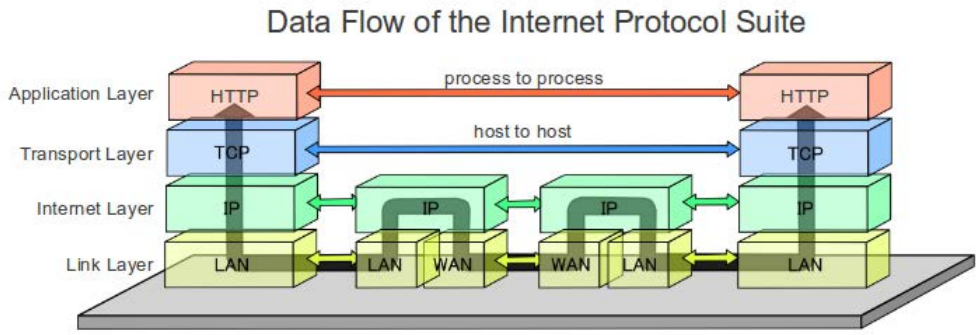


Figura 1.23- conjunto de protocolos de TCP/IP (fuente: Wikimedia)

En la transmisión de datos, la **comunicación en serie** es el proceso de enviar datos un bit a la vez, secuencialmente, a través de un canal de comunicación o bus de computadora. Son muy comunes en las redes industriales debido a su simplicidad, y **RS-232 y RS-485** son algunos de los protocolos de comunicación serie más extendidos. Estos protocolos corresponden a la capa física del modelo OSI.

RS-232 se refiere a un estándar para la transmisión de datos de comunicación en serie. Define formalmente las señales que se conectan entre un **DTE** (equipo terminal de datos), como un terminal de ordenador, y un **DCE**.(equipo de terminación del circuito de datos o equipo de comunicación de datos), como un módem. Por lo tanto, no puede considerarse un protocolo de red, sino un protocolo de **comunicación punto a punto**.

La norma define las características eléctricas y la temporización de las señales, el significado de las señales y el tamaño físico y el pinout de los conectores (figura 1.24). El estándar RS-232 se había utilizado comúnmente en los puertos serie de los ordenadores.

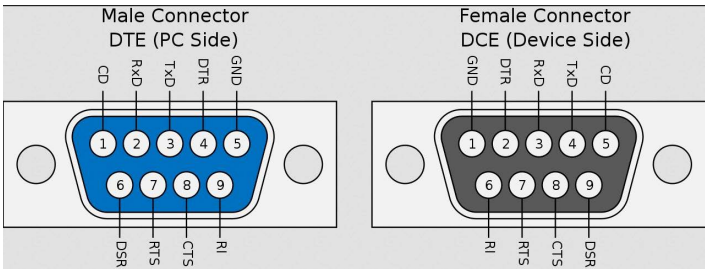


Figura 1.24- pinout RS-232 (fuente: Wikimedia)

RS-232, en comparación con interfaces posteriores como RS-485 y Ethernet, tiene menos características. En los ordenadores personales modernos, el USB ha desplazado a RS-232 de la mayoría de sus funciones de interfaz periférica. Pero gracias a su simplicidad, las interfaces RS-232 todavía se utilizan, especialmente en máquinas industriales donde una conexión de datos por cable de corto alcance, punto a punto y baja velocidad es totalmente adecuada.

RS-485 es un estándar que define las características eléctricas de los controladores y receptores para su uso en sistemas de comunicaciones en serie.

Las redes de comunicaciones digitales que implementan la norma pueden utilizarse eficazmente a grandes distancias y en entornos con ruido eléctrico.

Se pueden conectar varios receptores a dicha red en un **bus lineal multipunto**. Estas características hacen que RS-485 sea útil en sistemas de control industrial y aplicaciones similares.

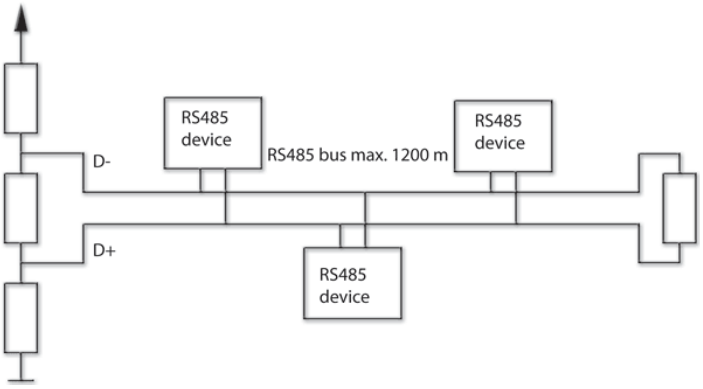


Figura 1.25- estructura de red RS-485 (fuente: Wikimedia)

Los ordenadores personales pueden necesitar convertidores de red (normalmente RS232 a RS485 o USB a RS485) para conectarse a una red RS485.

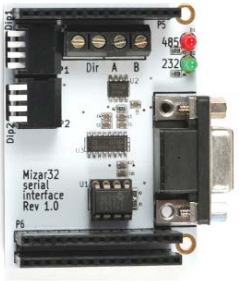


Figura 1.26- convertidor RS-485/RS-232 (fuente: Wikimedia)

Ethernet es una familia de tecnologías de redes informáticas de uso común en redes de área local (LAN). Las nuevas variantes de Ethernet utilizan par trenzado (**cables UTP y conectores RJ45)** y enlaces de cable de fibra óptica o par trenzado junto con los **conmutadores (switches)**. Los estándares Ethernet comprenden varias variantes de cableado y señalización de la capa física OSI utilizada con Ethernet.

Figura 1.28- cable Ethernet (UTP+RJ45) (fuente: Wikimedia)

La topología física más común para las redes Ethernet es la topología en estrella basada en switches.

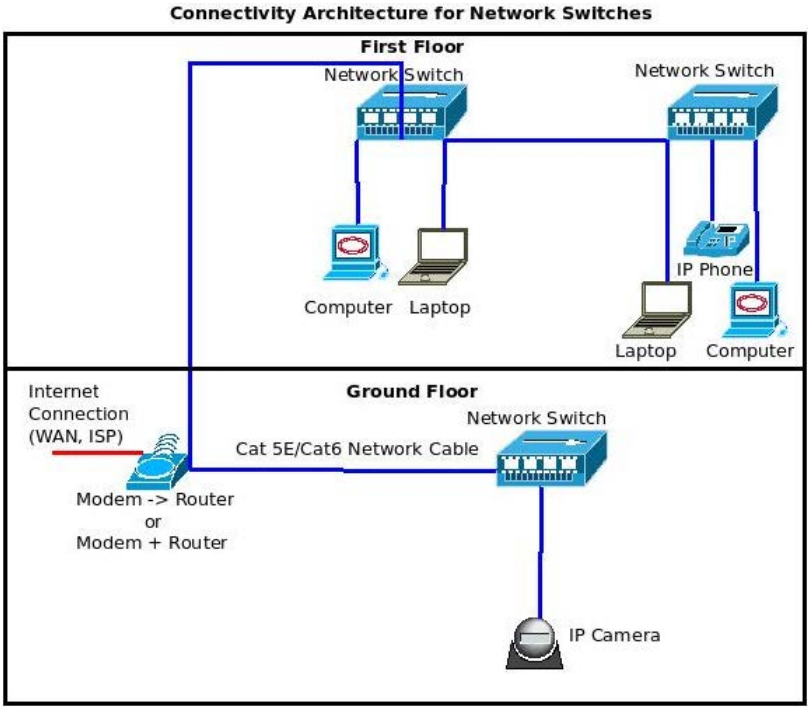


Figura 1.29- estructura en estrella de red Ethernet (fuente: Wikipedia)

Los sistemas de control industrial se basan a menudo en el protocolo Ethernet, que facilita el intercambio de información entre los **dispositivos OT** (automatización) y las **estaciones de trabajo IT** (tecnología informática). Los switches industriales se utilizan para conectar equipos OT como PLC's, HMI y monitores (Figura 1.30).

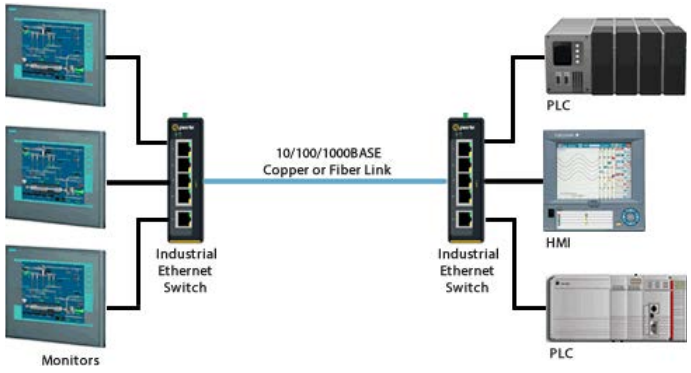


Figura 1.30- estructura de red Ethernet Industral (fuente: Wikipedia)

Cada uno de los nodos (ordenadores, PLC's...) conectados a una red Ethernet necesita una tarjeta especial (**Network Interface Controller, NIC**) que proporciona la interfaz física y el procedimiento lógico (**CSMA/CD**) necesarios para acceder e intercambiar información a través de esa red Ethernet.

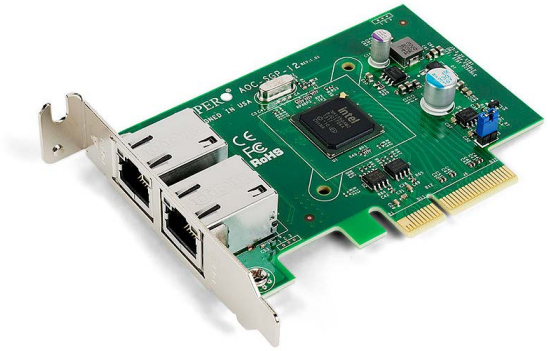


Figura 1.31- tarjeta de red Ethernet (fuente: Wikipedia)

Los sistemas que se comunican a través de Ethernet dividen un flujo de datos en trozos más cortos llamados **tramas** (frames). Cada trama contiene **direcciones de origen y destino (dirección MAC de 48 bits)**, y datos de **comprobación de errores** para que las tramas dañadas puedan ser detectadas y desechadas. Según el modelo OSI, Ethernet proporciona servicios incluidos en la capa de enlace de datos.

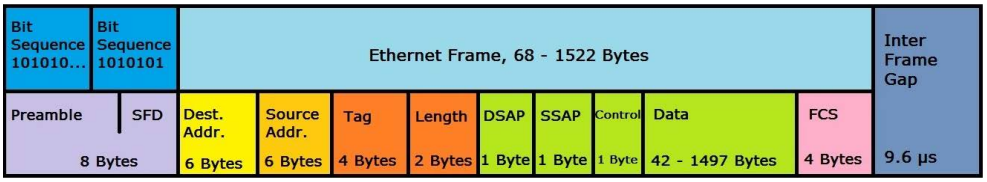


Figura 1.32- trama Ethernet (fuente: Wikipedia)

El Protocolo de Internet (IP) es comúnmente transportado a través de Ethernet, por lo que se considera una de las tecnologías clave que conforman Internet.

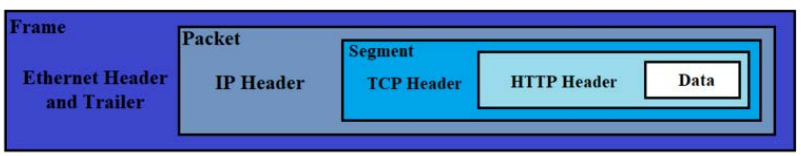


Figura 1.33- paquete IP encapsulado en una trama Ethernet (fuente: Wikimedia)

El **conjunto de protocolos de Internet** es el modelo conceptual y el conjunto de protocolos de comunicaciones utilizados en Internet y redes informáticas similares. Se conoce comúnmente como **TCP/IP** porque los protocolos fundamentales de la suite son el Protocolo de Control de Transmisión (TCP) y el Protocolo de Internet (IP). La figura 1.33 compara el modelo OSI con la implementación de TCP/IP, en la que los protocolos de capa de aplicación (FTP...) utilizan los servicios de transporte proporcionados por los protocolos TCP/IP.

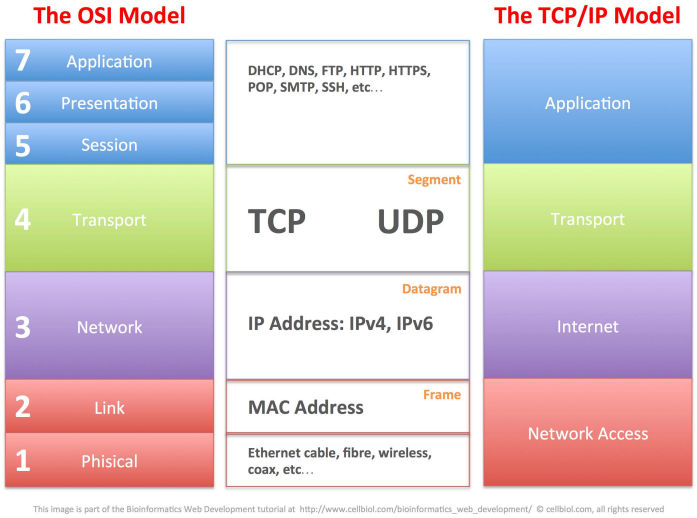


Figura 1.33- protocolos de comunicaciones (fuente: blog.pythian.com)

TCP/IP proporciona comunicación de datos de **extremo a extremo** especificando cómo se deben empaquetar, direccionar, transmitir, enrutar y recibir los datos. Esta funcionalidad está organizada en **cuatro capas de abstracción**. Desde el nivel más bajo hasta el más alto, las capas son la **capa de enlace** (normalmente basada en Ethernet), que contiene métodos de comunicación para los datos que permanecen dentro de un único segmento de red (enlace); la **capa de Internet** (basada en el protocolo IP), que proporciona conexión en red entre redes independientes; la **capa de transporte** (basada en el protocolo TCP), que gestiona la comunicación de host a host; y la **capa de aplicación** (protocolos como HTTP y FTP se definen en esta capa), que proporciona el intercambio de datos de proceso a proceso para aplicaciones.

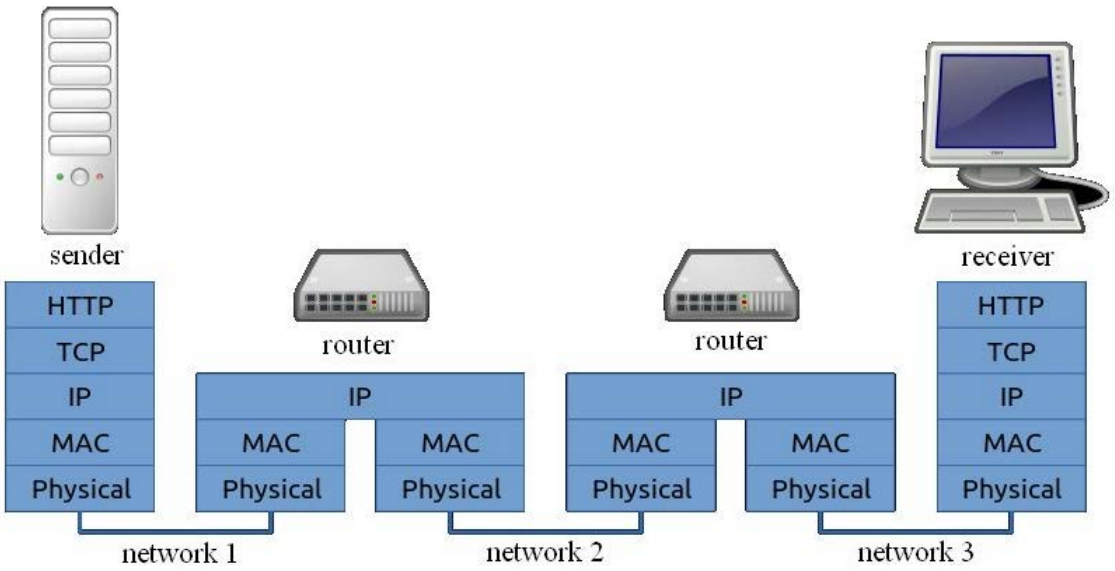


Figura 1.34- esquema conexión basada en TCP/IP (fuente: Wikimedia)

Un **enrutador (router)** es un dispositivo de red que reenvía paquetes de datos entre redes de ordenadores. Los datos enviados a través de Internet, como una página web o un correo electrónico, se presentan en forma de paquetes de datos. Un paquete es típicamente reenviado de un enrutador a otro enrutador a través de las redes que constituyen una red hasta que llega a su nodo de destino.

Figura 1.35- enrutamiento de paquetes IP (fuente: http://routinglab.blogspot.com)

El enrutamiento se basa en las **direcciones IP** asignadas a los nodos. Las direcciones IP (v4) pueden representarse en cualquier notación que exprese un valor entero de 32 bits. La mayoría de las veces se escriben en la notación decimal por puntos, que consiste en cuatro octetos de la dirección expresados individualmente en números decimales y separados por puntos.

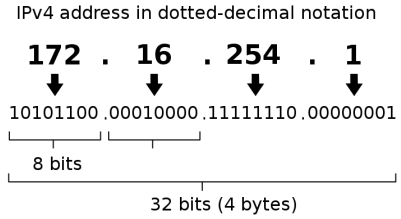


Figura 1.36- estructura de una dirección IP (fuente: Wikimedia)

La información se envía desde un nodo transmisor a uno receptor en forma de paquetes IP, que incluyen las direcciones IP de origen y destino.

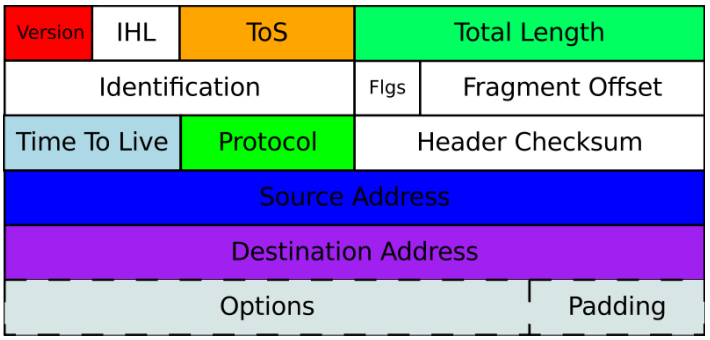


Figura 1.37- estructura de un paquete IP (fuente: Wikimedia)

La **segmentación** de redes en redes informáticas es el acto o la práctica de dividir una red informática en subredes, como se muestra en la Figura 1.38, siendo cada una de ellas un segmento de red. Las ventajas de esta división son principalmente para aumentar el rendimiento y mejorar la seguridad.

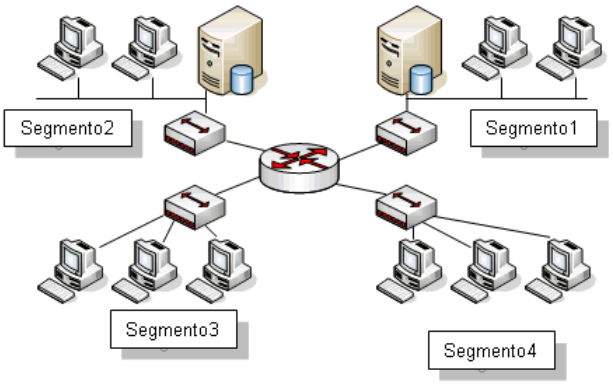


Figura 1.38- segmentación de redes (fuente: Wimex)

Se consigue un **mejor rendimiento**, ya que en una red segmentada hay menos hosts por subred, lo que minimiza el tráfico local y reduce la congestión.

La **mejora de la seguridad** se debe a las siguientes razones:

- Las transmisiones serán contenidas a la red local. La estructura interna de la red no será visible desde el exterior.
- Hay una superficie de ataque reducida disponible. Los vectores de ataque comunes pueden ser parcialmente aliviados mediante una adecuada segmentación de la red, ya que sólo funcionan en la red local. Al crear segmentos de red que contienen sólo los recursos específicos de los consumidores a los que autoriza el acceso, está creando un entorno de menor privilegio.

El **control de acceso de visitantes** se logra implementando VLANs para segregar la red.

Una **LAN virtual (VLAN)** es cualquier dominio de difusión que está particionado y aislado en una red informática en la capa de enlace de datos (capa 2 de OSI).

Para subdividir una red en VLANs, los equipos de red (normalmente conmutadores) deben ser configurados por software asignando un grupo de puertos a cada VLAN.

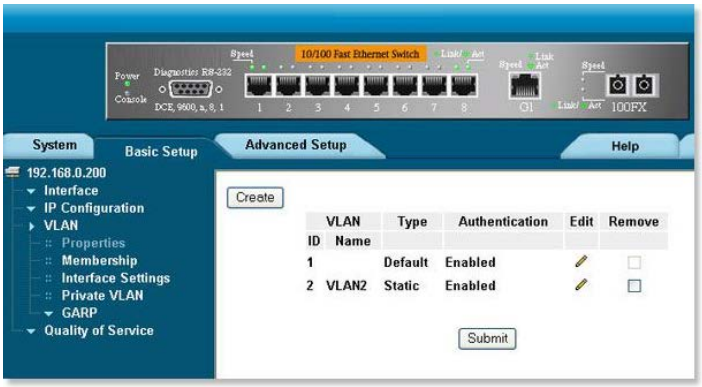


Figura 1.39- pantalla de configuración de un switch para generar

VLAN

Una vez asignados los puertos a cada VLAN, no se pueden intercambiar datos entre nodos (ordenadores, PLC...) conectados a diferentes puertos VLAN.

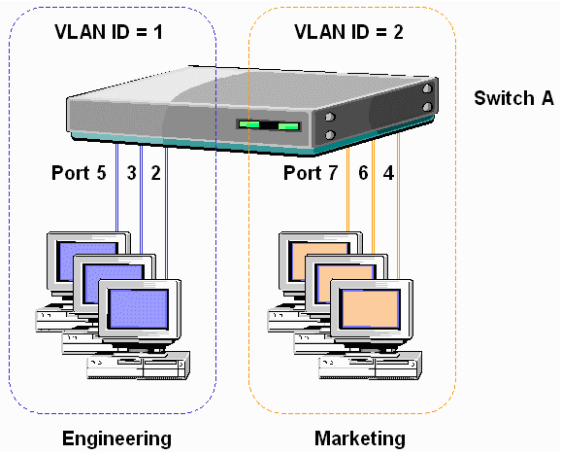


Figura 1.40- segmentación VLAN (fuente:http://photos1.blogger.com/blogger/6124/4181/320/vlan-fig1.png)

Las VLANs funcionan aplicando **etiquetas** (este método se desarrolla bajo el estándar 802.1Q) a tramas de capa 2, creando la apariencia y funcionalidad del tráfico de red que se encuentra físicamente en una sola red pero que actúa como si estuviera dividido entre redes separadas.

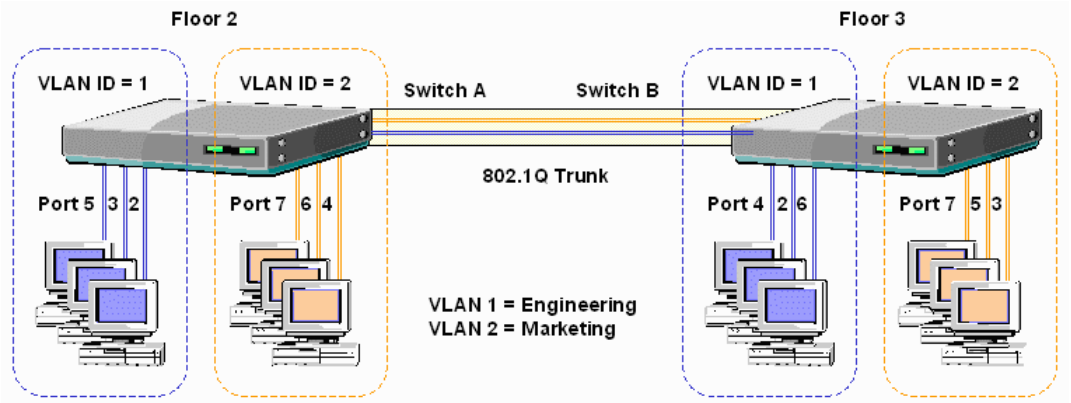


Figura 1.41- etiquetado VLAN (fuente: Wikimedia)

Las VLAN permiten a los administradores de red agrupar hosts, incluso si los hosts no están conectados directamente al mismo conmutador de red.

En términos técnicos, un enrutador es un dispositivo de puerta de enlace de red de Nivel 3, lo que significa que entra en contacto con dos o más redes y que el enrutador funciona en la capa de red del modelo OSI. La Figura 1.42 muestra cómo tres enrutadores interconectan diferentes redes LAN (se identifican por las direcciones de red 150.10.0.0, 160.10.0.0 y 170.10.0.0).

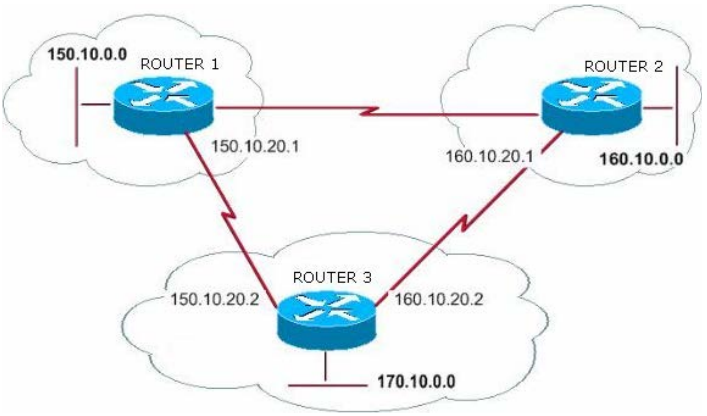


Figura 1.42- Routers interconectando diferentes redes LAN.

Para enrutar la información desde un nodo de origen a un nodo de destino se requiere un sistema de direccionamiento, que normalmente es el basado en las direcciones IPv4.

Una dirección IP se divide en dos campos, el **identificador de red** (utilizado por los routers para encontrar la red de destino en Internet) y el **identificador de host** (un identificador para un host específico) (Figura 1.43).

El número de bits dedicado a cada campo se define por la **máscara** aplicada a una dirección IP, utilizando bits lógicos "1" para la parte de red de la dirección y "0" para la parte de host. El número de bits asignados a la parte de red se utiliza para la identificación de la dirección IP de la red correspondiente (por ejemplo, en la dirección de host 192.168.1.110/24 los primeros 24 bits se asignan para el direccionamiento de red, de modo que 192.168.1.0/24 es la dirección IP de la red a la que pertenece el host).

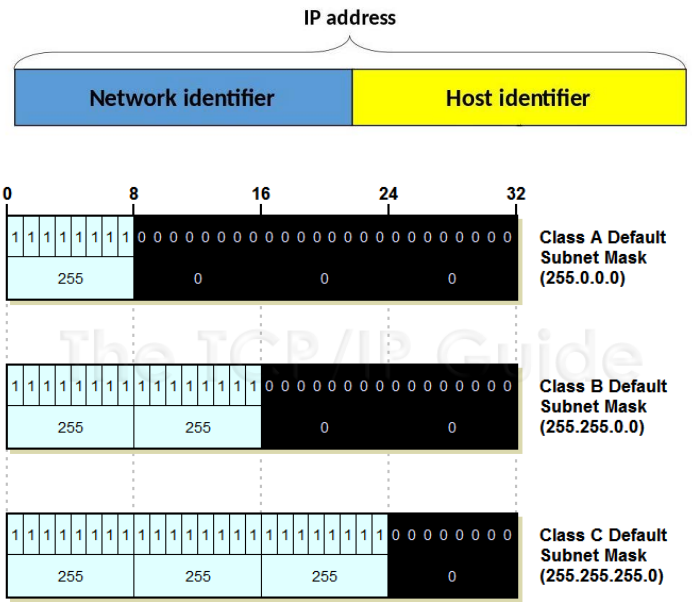


Figura 1.43- clase de dirección IP y su máscara

Una **subred** es una subdivisión lógica (Figura 1.44) de una red IP. Se le llama subnetting a la práctica de dividr una red en dos o más redes.

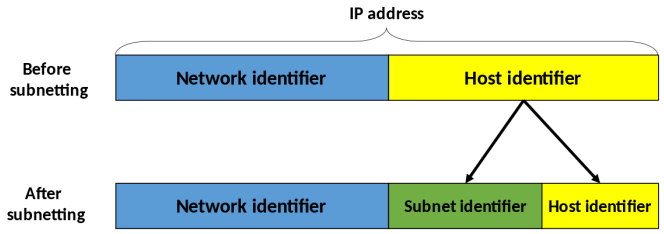


Figura 1.44- identificador de subred IP (fuente: Wikipedia)

Se asignan algunos bits del campo identificador del host (modificando la máscara de red IP para añadir más bits "1" asignados para el campo de subred) para crear un **identificador de subred**. Los ordenadores que pertenecen a la misma subred se dirigen con un identificador de subred idéntico en sus direcciones IP.

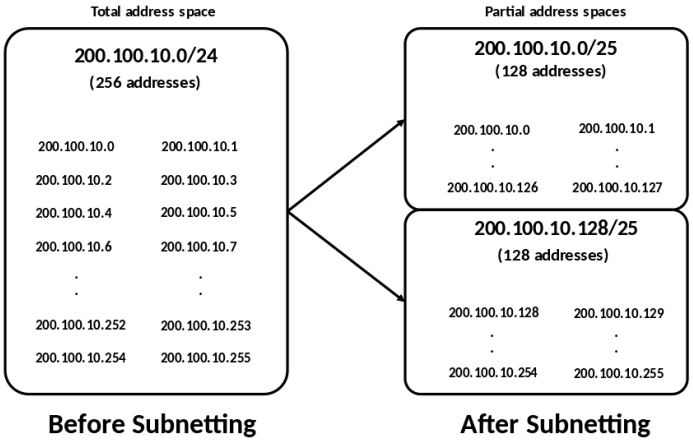


Figura 1.45- Segmentación de subredes IP (fuente: Wikimedia)

Los ordenadores ubicados en diferentes subredes IP necesitan un enrutador para comunicarse entre sí, por lo que la subred es un método válido para segmentar una red en partes aisladas.

Un **firewall (cortafuegos)** es un sistema de seguridad de red que monitorea y controla el tráfico entrante y saliente de la red basado en reglas de seguridad predeterminadas. Un cortafuegos generalmente establece una barrera entre una red interna confiable y una red externa no confiable, como Internet.

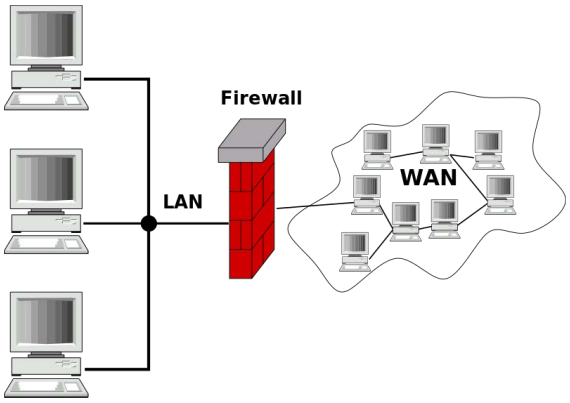


Figura 1.46- Protección basada en firewall (fuente: Wikipedia)

El cortafuegos filtra los paquetes transferidos entre ordenadores. Cuando un paquete no coincide con **las reglas de filtrado**, el cortafuegos rechaza el paquete, de lo contrario se le permite pasar. Los paquetes pueden filtrarse por direcciones de red de origen y destino, protocolos y números de puerto de origen y destino.

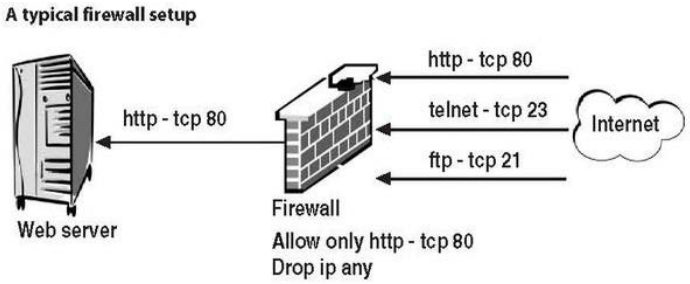


Figura 1.47- reglas de filtrado de un firewall (fuente: Wikimedia)

DMZ o zona desmilitarizada es una subred que contiene los servicios externos de una organización a una red más grande como Internet. El propósito de una DMZ es añadir una capa de seguridad a la LAN de una organización: un nodo de red externo puede acceder sólo a lo que está expuesto en la DMZ, mientras que el resto de la red de la organización está protegida por cortafuegos.

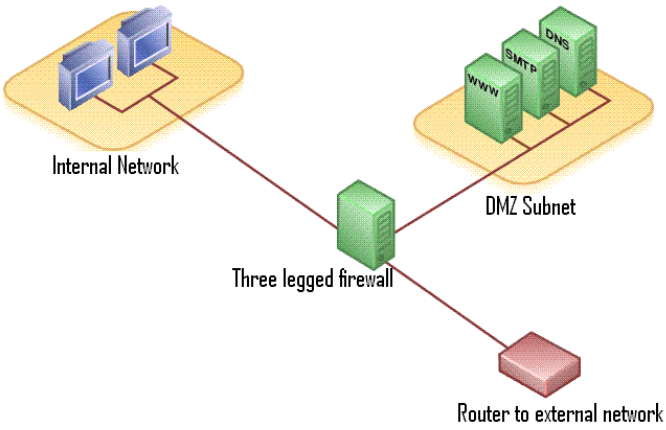


Figura 1.48- DMZ basado en firewall (fuente: Wikimedia)

Un **servicio de acceso remoto (RAS**) es cualquier combinación de hardware y software que permite una conexión entre un cliente y un ordenador central, conocido como servidor de acceso remoto.

Muchos fabricantes ayudan a utilizar este servicio para la **resolución de problemas técnicos de sus clientes.** Varios escritorios remotos profesionales, desarrollados como aplicaciones de código abierto y gratuitas, están disponibles.

Telnet y SSH (Secure Shell) son dos protocolos de red utilizados para conectarse a **servidores remotos** con el fin de facilitar algún tipo de comunicación. Permiten a los administradores de red acceder y gestionar de forma remota un dispositivo que trabaja con un **emulador de termina**l.

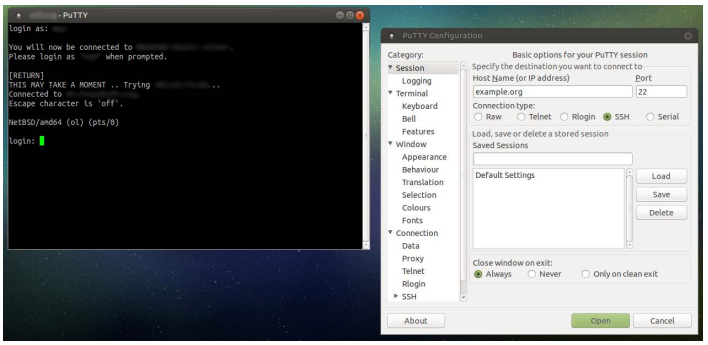


Figura 1.50- terminal remoto basado en Putty

La principal diferencia entre Telnet y SSH es que SSH proporciona mecanismos de seguridad (encripta los datos intercambiados utilizando **criptografía de clave pública**) que protegen a los usuarios estableciendo una conexión segura entre dos hosts remotos a través de Internet, mientras que Telnet no tiene medidas de seguridad ya que los datos de usuario/contraseña no están encriptados.

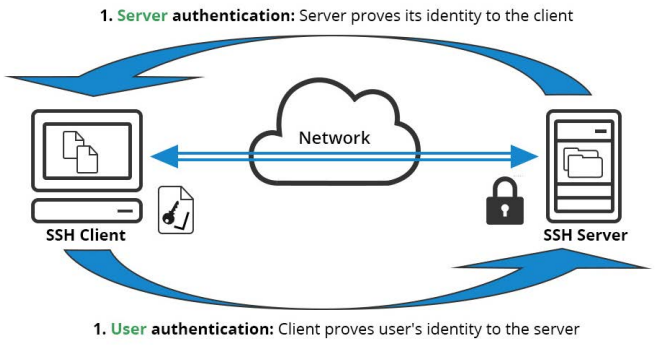


Figura 1.51- comunicación con SSH encriptado

El **escritorio remoto** se refiere a un software que permite que el entorno de escritorio de un ordenador personal se ejecute de forma remota en un sistema mientras se muestra en un dispositivo cliente independiente. Tomar el control de un escritorio de forma remota es una forma de administración remota.

Figura 1.52- control de escritorio remoto (fuente: http://www.itarian.com)

Remote Desktop Protocol (RDP) es un protocolo propietario desarrollado por Microsoft, que proporciona al usuario una interfaz gráfica para conectarse a otro equipo a través de una conexión de red. El usuario emplea software cliente RDP (integrado en muchos sistemas operativos) para este propósito, mientras que la otra computadora debe ejecutar el software servidor RDP (integrado sólo en el sistema operativo Windows). Microsoft se refiere actualmente a su software cliente RDP oficial como Conexión a Escritorio Remoto, anteriormente denominado "Terminal Services Client".

El RDP no actualizado es hoy en día uno de los principales puntos de entrada para el ransomware. Es muy importante mantener Windows actualizado para evitar este tipo de ataques. Hay algunas opciones para asegurarlo. Entra en este enlace para más información

Virtual Network Computing (VNC) es un sistema gráfico de escritorio compartido de código abierto que utiliza el protocolo Remote Frame Buffer (RFB) para controlar de forma remota otro ordenador. Transmite a través de una red los eventos de teclado y ratón de un ordenador a otro, retransmitiendo las actualizaciones de la pantalla gráfica en la otra dirección.

Múltiples clientes pueden conectarse a un servidor VNC al mismo tiempo. Los usos populares de esta tecnología incluyen el soporte técnico remoto y el acceso a los archivos de la computadora del trabajo desde la computadora del hogar, o viceversa.

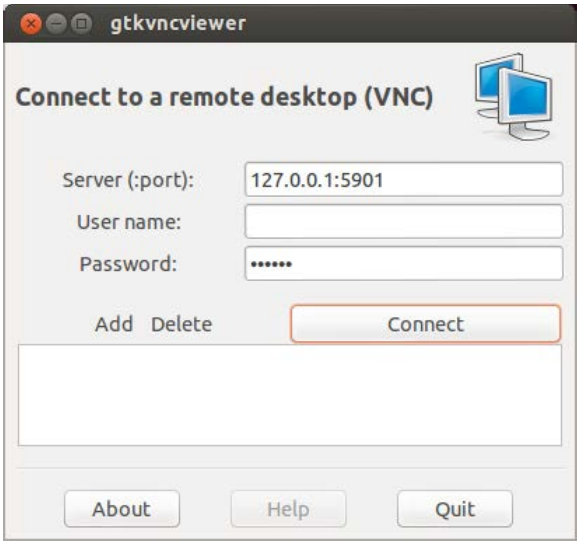


Figura 1.53- conexión de escritorio remoto (fuente: flickr VNC)

TeamViewer es un software propietario para el control remoto, el uso compartido del escritorio, las reuniones en línea, las conferencias web y la transferencia de archivos entre ordenadores. Una vez instalado en un ordenador, permite conexiones remotas a usuarios con permiso.

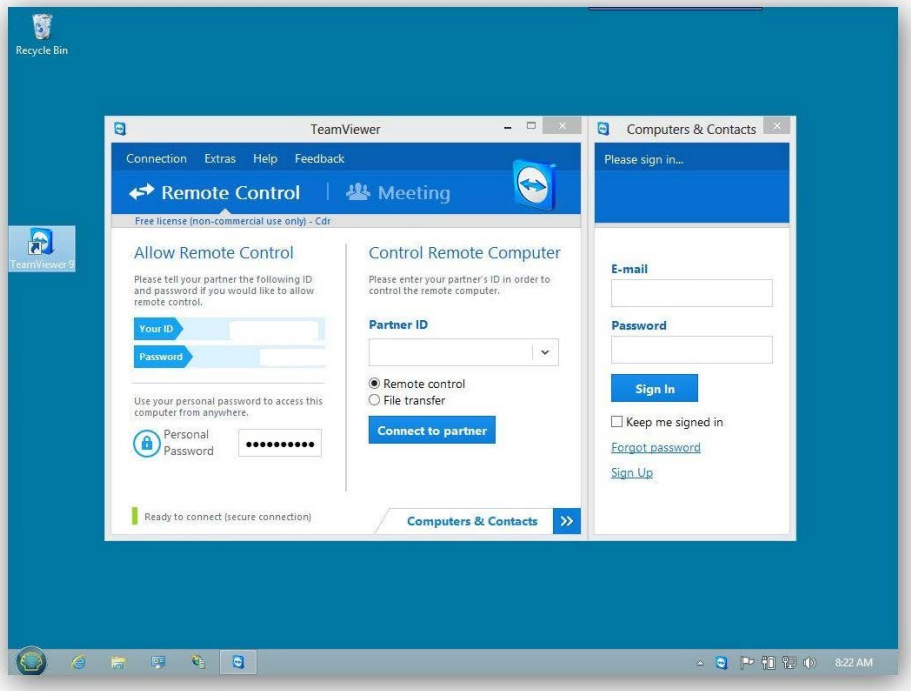


Figura 1.54- configuración de conexión remota Teamviewer

Una **red privada virtual (VPN)** extiende una red privada a través de una red pública y permite a los usuarios enviar y recibir datos a través de redes compartidas o públicas como si sus dispositivos informáticos estuvieran conectados directamente a la red privada.

Para garantizar la seguridad, la conexión de red privada se establece utilizando un **protocolo de túnel por capas cifrado** y los usuarios de VPN utilizan métodos de autenticación, incluidas contraseñas o certificados.

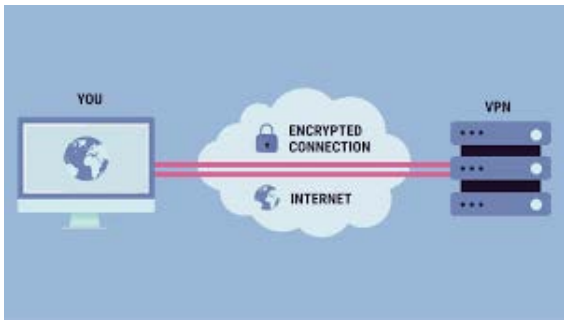


Figura 1.55- conexión VPN (fuente: http://hardzone.es)

1.3 Protocolos de redes industriales

Description

1.3 Protocolos de redes industriales

Table of contents

Fieldbus (bus de campo) es el nombre de una familia de protocolos de red de ordenadores industriales utilizados para el control distribuido en **tiempo real**.

En un sistema de control industrial suele haber una interfaz hombre-máquina (HMI) en la parte superior de la jerarquía, conectada a una capa intermedia de controladores lógicos programables (PLC) a través de un sistema de comunicaciones que no es crítico en cuanto al tiempo (por ejemplo, Ethernet). En la parte inferior del sistema de control se encuentra el bus de campo que conecta los PLCs (Nivel 1) con los componentes que realmente realizan el trabajo (Nivel 0), tales como sensores, actuadores, motores eléctricos, luces de consola, interruptores, válvulas y contactores.

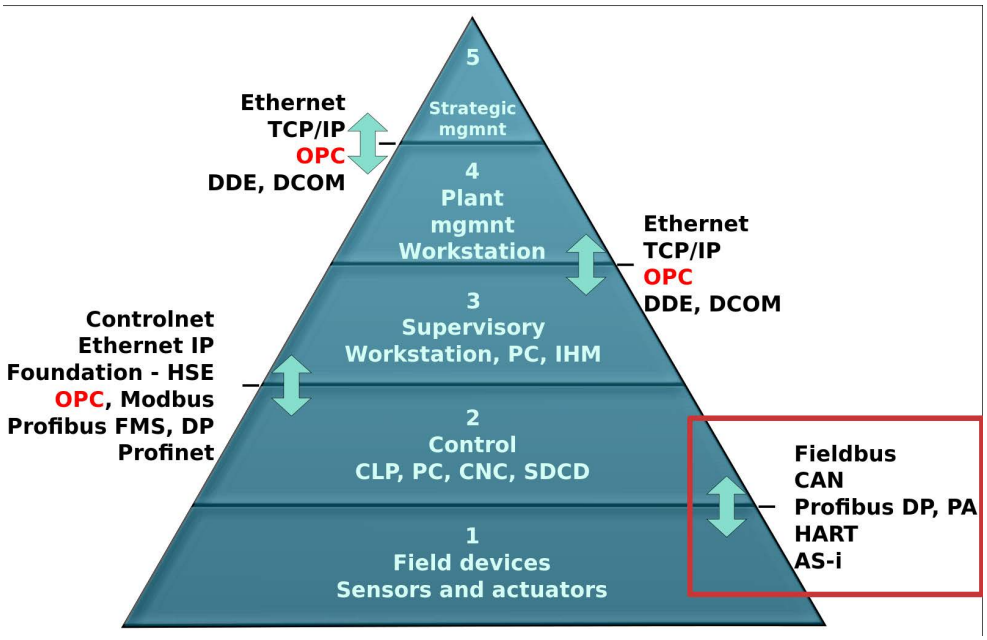


Figura 1.56- esquema de niveles del bus de campo (fuente: Wikimedia)

Fieldbus es un sistema de red industrial para el control distribuido en tiempo real y es el equivalente de las conexiones actuales de tipo LAN, que requieren sólo un punto de comunicación a nivel de controlador y permiten conectar varios dispositivos al mismo tiempo.

Modbus es un protocolo de comunicaciones serie (normalmente implementado sobre RS-232 o RS-485) utilizado para comunicar PLCs. Se ha convertido en un protocolo de comunicación estándar y es ahora un medio comúnmente disponible para conectar dispositivos electrónicos industriales debido a las siguientes razones:

- publicado abiertamente y libre de regalías,
- mueve bits o palabras sin procesar sin poner muchas restricciones a los vendedores.

Modbus se utiliza a menudo para conectar un ordenador de supervisión (maestro) con una RTU remota (esclavo) en sistemas SCADA. Se define como un protocolo maestro/esclavo (Figura 1.57), lo que significa que un dispositivo que funciona como maestro controlará a uno o más dispositivos que funcionan como esclavos. Esto significa que un dispositivo esclavo no puede ofrecer información de forma voluntaria; debe esperar a que se le pida. El maestro escribirá los datos en los registros de un dispositivo esclavo y leerá los datos de los registros de un dispositivo esclavo.

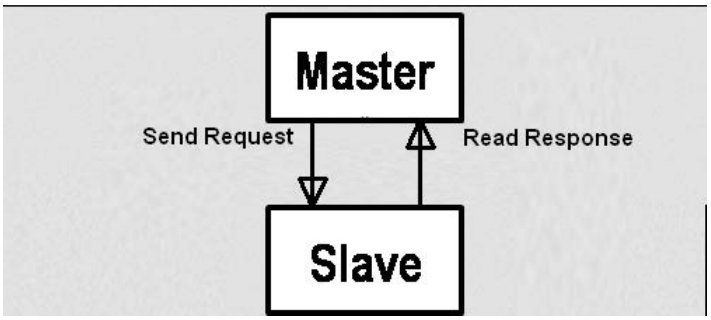


Figura 1.57- comunicación maestro-esclavo

Cada intercambio de datos consiste en una petición del maestro, seguida de una respuesta del esclavo. Como se muestra en la Figura 1.58, cada paquete de datos, ya sea petición o respuesta, comienza con la dirección del dispositivo o dirección del esclavo, seguido por el código de función, seguido por los parámetros que definen lo que se está pidiendo o proporcionando. Los formatos exactos de la solicitud y la respuesta se documentan detalladamente en la especificación del protocolo Modbus.

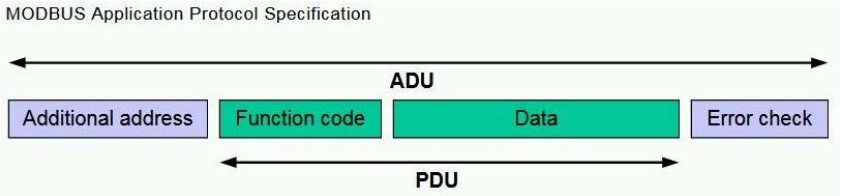


Figura 1.58- estructura de paquete de datos Modbus (fuente: Modbus Organization)

Como muestra la Figura 1.59, el protocolo **Modbus TCP** encapsula los paquetes de datos de petición y respuesta Modbus RTU en un paquete TCP transmitido a través de redes Ethernet estándar. La dirección de mayor importancia en este caso es la dirección IP. El puerto estándar para Modbus TCP es 502, pero a menudo se puede reasignar el número de puerto si se desea.

En el caso de Modbus TCP, la suma de comprobación y la gestión de errores se realizan a través de Ethernet.

La versión TCP de Modbus sigue el modelo de referencia de red OSI. Modbus TCP define las capas de presentación y aplicación en el modelo OSI.

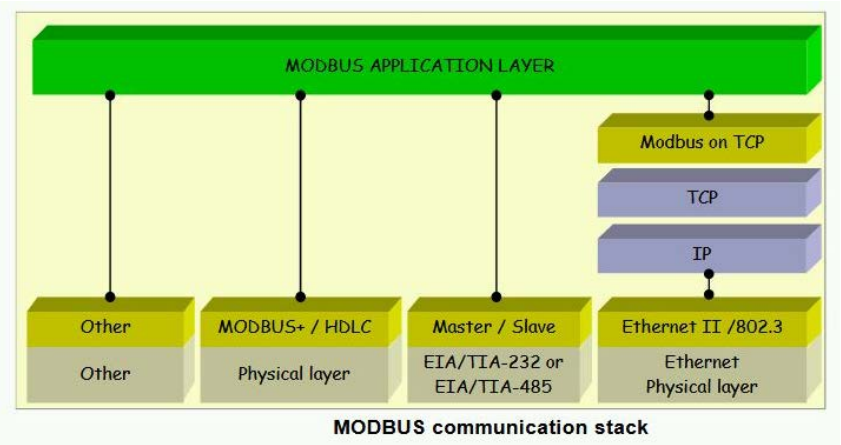


Figura 1.59- conjunto de protocolos Modbus (fuente: Modbus Organization)

Modbus TCP se ejecuta en Ethernet (enlace de datos y capa física), y Modbus RTU es un protocolo de nivel serie (capa física). Para comunicar ambas redes se necesita una **pasarela (gateway)** (Figura 1.60) para convertir un protocolo a otro añadiendo o quitando un encabezado de 6 bytes que permita enrutar en Modbus TCP.

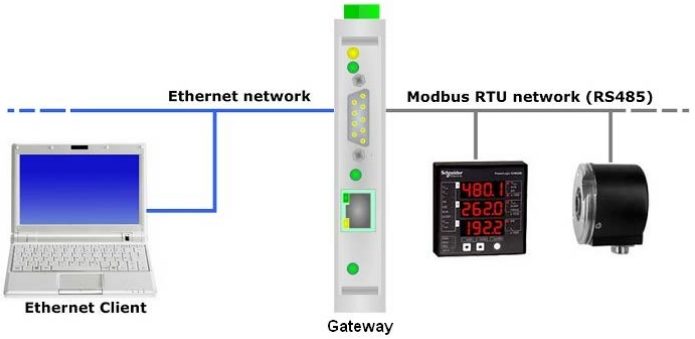


Figure 1.60- pasarela de comunicación TCP-RTU (fuente: Modbus Organization)

Modbus TCP es el protocolo común que conecta el resto de las opciones de Modbus a través de pasarelas.

Profibus (Process Field Bus) es un estándar para la comunicación de bus de campo en la técnica de automatización. No debe confundirse con el estándar de Profinet para Ethernet industrial.

Hay dos variaciones de Profibus en uso hoy en día (Figura 1.62); la más comúnmente utilizada es Profibus DP:

- **PROFIBUS DP** (Periféricos descentralizados) se utiliza para operar sensores y actuadores a través de un controlador centralizado en un sistema automatizado de producción.

- **PROFIBUS PA** (Process Automation) se utiliza para supervisar los equipos de medición en aplicaciones de automatización de procesos. Esta variante está diseñada para su uso en áreas con riesgo de explosión (Ex-zone 0 y 1). La capa física cumple con la norma IEC 61158-2, que permite la entrega de energía a través del bus a los instrumentos de campo, al tiempo que limita los flujos de corriente para que no se creen condiciones que puedan producir una explosión, incluso si se produce un mal funcionamiento.

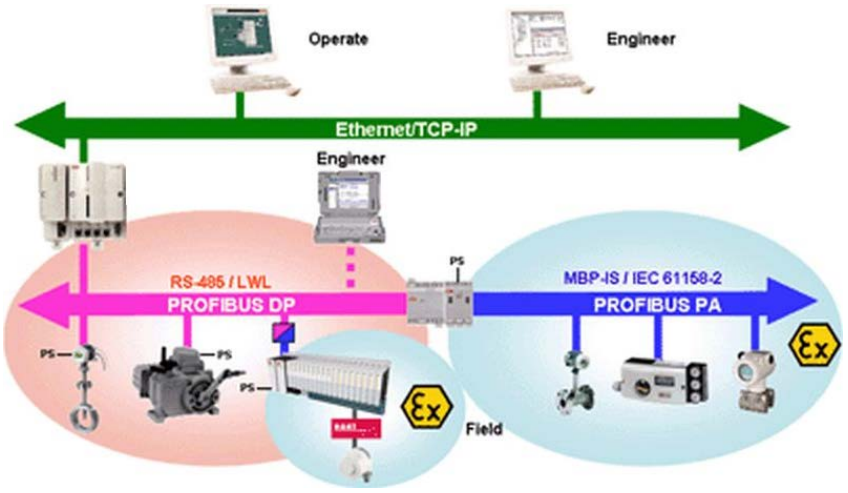


Figura 1.62- Profibus DP/PA

Profibus se desarrolla sobre la capa 1, 2 y 7 de OSI (Figura 1.63):

OSI-Layer		PROFIBUS		
7	Application	DPV0	DPV1	DPV2
6	Presentation	--		
5	Session			
4	Transport			
3	Network			
2	Data Link	FDL		
1	Physical	EIA-485	Optical	MBP

Figura 1.63- comparativa niveles modelo OSI model-Profibus

Capa 1:

Se especifican tres métodos diferentes para la capa de transmisión de bits:

- Con transmisión eléctrica según EIA-485. Pueden utilizarse velocidades binarias de 9,6 kbit/s a 12 Mbit/s. La longitud del cable entre dos repetidores está limitada de 100 a 1200 m, dependiendo de la velocidad de bits utilizada. Este método de transmisión se utiliza principalmente con PROFIBUS DP.

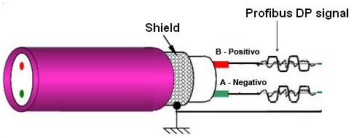


Figura 1.64- Profibus RS-485 por cable

- Con transmisión óptica por fibra óptica, se utilizan topologías de estrella, bus y anillo. La distancia entre los repetidores puede ser de hasta 15 km. Se necesitan convertidores de fibra óptica-RS485 (Figura 1.65)

Figura 1.65- Convertidor de fibra óptica-RS485

- Con la tecnología de transmisión MBP (Manchester Bus Powered), los datos y la potencia del bus de campo se alimentan a través del mismo cable. Esta tecnología se utiliza en Profibus PA.

En las redes Profibus se utilizan normalmente conectores tipo Sub-D de 9 pines.

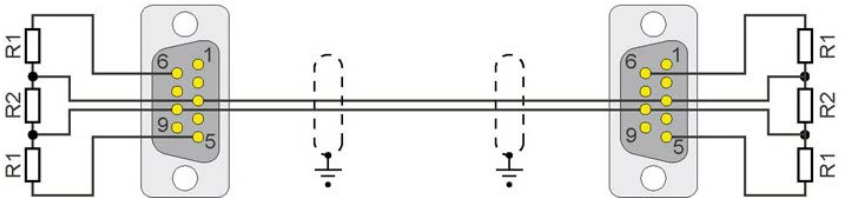


Figura 1.67- Conector Profibus RS485 de 9 pines tipo D (fuente: Wikimedia)

Capa 2:

La capa de enlace de datos se denomina **FDL (Field bus Data Link)** y funciona con un método de acceso híbrido que combina el paso de testigo con un método maestro-esclavo. En una red PROFIBUS DP, los controladores o sistemas de control de procesos son los maestros y los sensores y actuadores son los esclavos. (Figura 1.68)

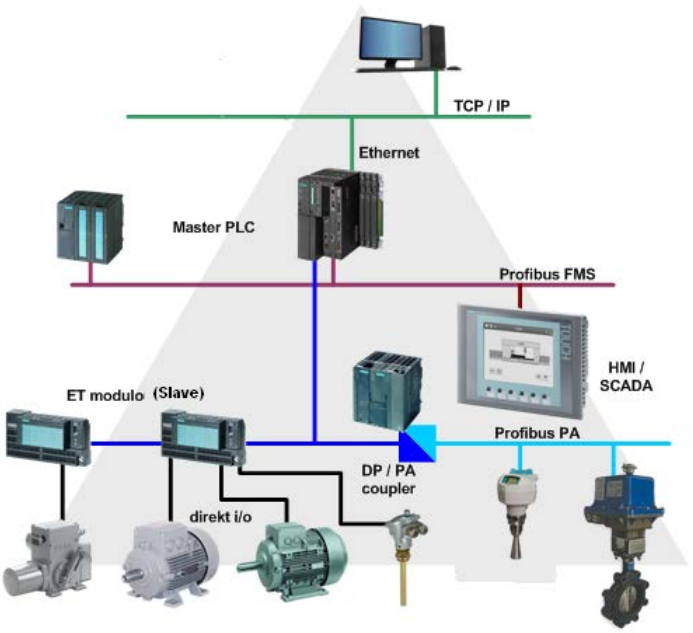


Figura 1.68- Arquitectura maestro-esclavo de Profibus (fuente: Wikimedia)

Profibus puede conectarse a otras redes de bus de campo utilizando la pasarela necesaria (Figura 1.69).

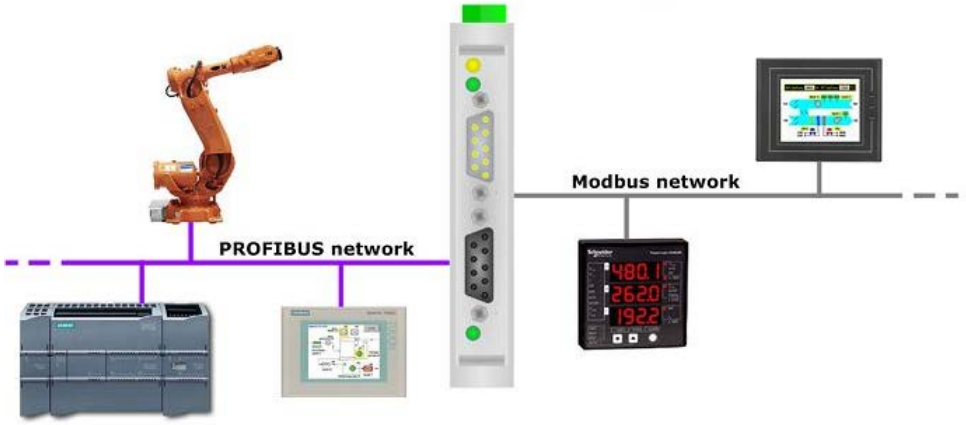


Figura 1.69- Interconexión de Profibus y Modbus vía gateway

Ethernet Industrial utiliza los estándares desarrollados para Ethernet y los implementa para la fabricación de comunicaciones de red (Figura 1.70). La modificación de la capa de enlace de datos (Media Access Control) Ethernet Industrial proporciona **determinismo y control en tiempo real (baja latencia)**, lo que no es crítico en un entorno informático (IT) pero si es necesario en un entorno de automatización industrial (OT).

Además, debe proporcionar **interoperabilidad** de los niveles superiores del modelo de interconexión de sistemas abiertos y seguridad contra intrusiones ajenas a la planta y contra el uso no autorizado dentro de la planta.

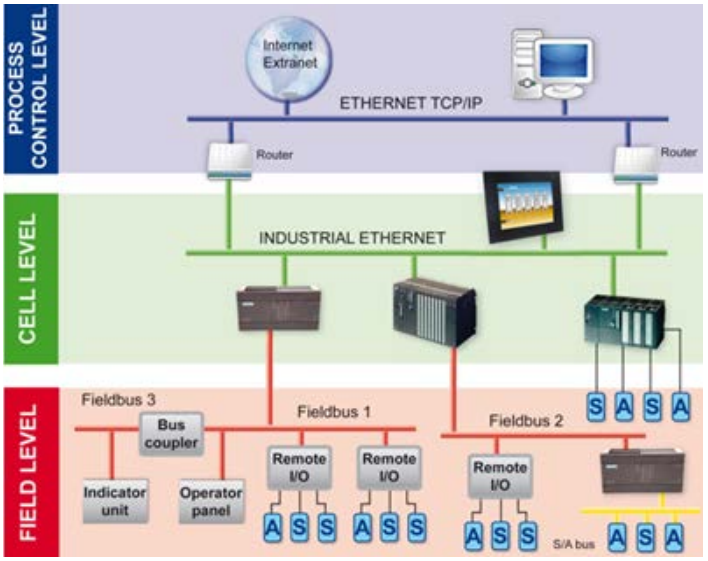


Figura 1.70- Arquitectura de red de Ethernet industrial (fuente: Industrial Ethernet Book)

Los equipos de Ethernet industrial están diseñados para **entornos hostiles**, por lo que necesitan características especiales, como conectores robustos y conmutadores de temperatura ampliados, necesarios en un entorno industrial. Los componentes utilizados en las áreas de proceso de la planta deben estar diseñados para trabajar en temperaturas extremas, humedad y vibración que excedan los rangos de los equipos de TI.

El uso de fibra óptica (puertos **SFP**) Ethernet reduce los problemas de ruido eléctrico y proporciona aislamiento eléctrico.

Figura 1.71- Industrial Ethernet switch (fuente: Wikipedia)

Profinet es el estándar abierto de Ethernet Industrial de la asociación internacional Profibus y uno de los estándares de comunicación más utilizados en redes de automatización.

Profinet permite la compatibilidad con las comunicaciones Ethernet (más típicas de los entornos informáticos), pero hay que tener en cuenta la diferencia de velocidad que tiene una comunicación Ethernet en una red corporativa frente al rendimiento en tiempo real que requiere una red industrial.

El uso de Profinet puede ofrecer las siguientes ventajas:

- Mejora la escalabilidad de las infraestructuras.
- Facilita el acceso a dispositivos de campo de otras redes
- Ejecución de tareas de mantenimiento desde cualquier lugar a través de conexiones seguras (VPN) para el mantenimiento remoto.

El protocolo PROFINET consta básicamente de tres dispositivos (Figura 1.72):

- IO Controller: Maestro, donde se ejecuta el programa de control
- Dispositivo IO: Dispositivo de campo remoto que mantiene la comunicación con un controlador
- IO Supervisor: dispositivo gráfico programable donde se realiza el análisis de la red.

No existe ningún tipo de jerarquía entre estos dispositivos, lo que significa que cada IO tiene la misma importancia en una red PROFINET.

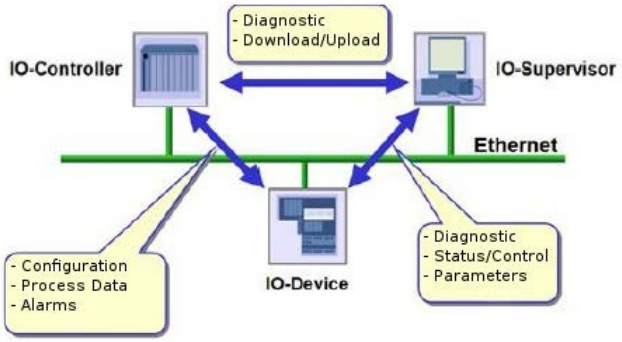


Figura 1.72- tipos de dispositivos Profinet (fuente: www.semanticscholar.org)

Profinet incorpora diferentes **perfiles** a través de una interpretación específica para cada caso de los datos transmitidos, modificando el nivel 7 de OSI (aplicación). Existen 3 versiones de Profinet:

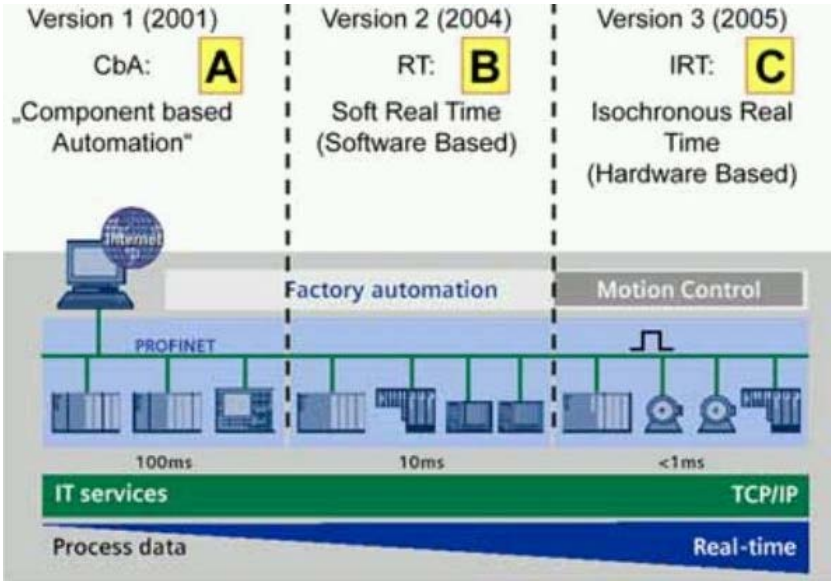


Figura 1.73- perfiles de Profinet (fuente: www.semanticscholar.org)

- Versión 1 (Clase A): **Automatización basada en componentes (CBA)**

Su tiempo de ciclo típico es de 100 ms, y se utiliza para la parametrización, no se utiliza para la comunicación de datos de proceso. ya no es compatible con Profibus.

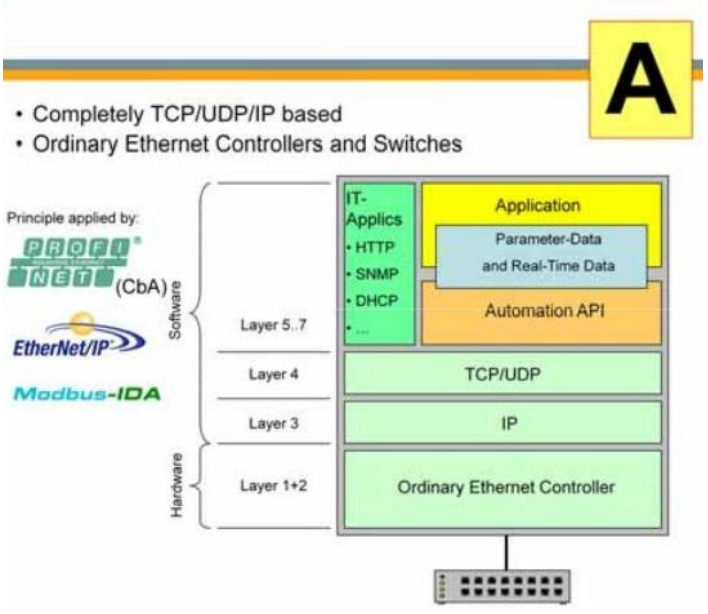


Figura 1.74- arquitectura Profinet CBA (fuentee: www.ethercat.org)

- Versión 2 (Clase B): **Tiempo Real (RT)**

Su tiempo de ciclo típico es de 10 ms, similar al Profibus, y se utiliza para la comunicación de datos de proceso.

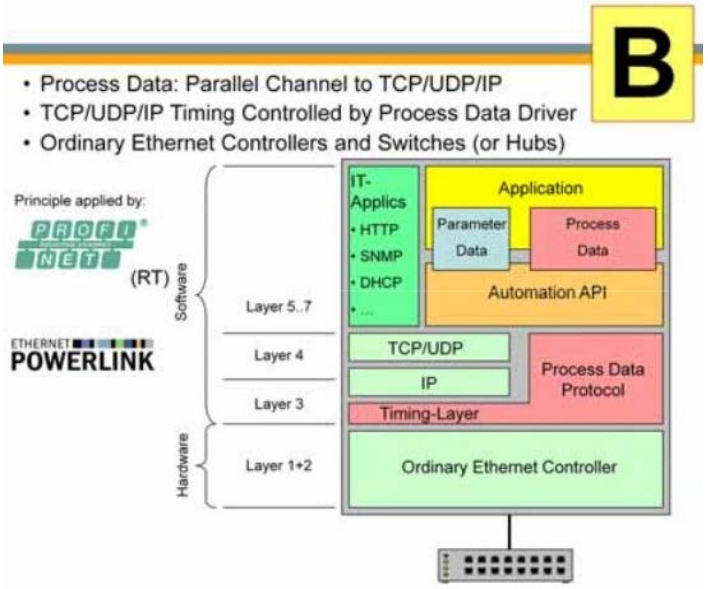


Figura 1.75- arquitectura Profinet RT (fuente: www.ethercat.org)

- Versión 3 (Clase C) : **Tiempo Real Isócrono (IRT)**

Su tiempo de ciclo típico es de 1 ms. La diferencia con la comunicación en tiempo real es esencialmente el alto grado de determinismo, de modo que el inicio de un ciclo de red se mantiene con alta precisión.

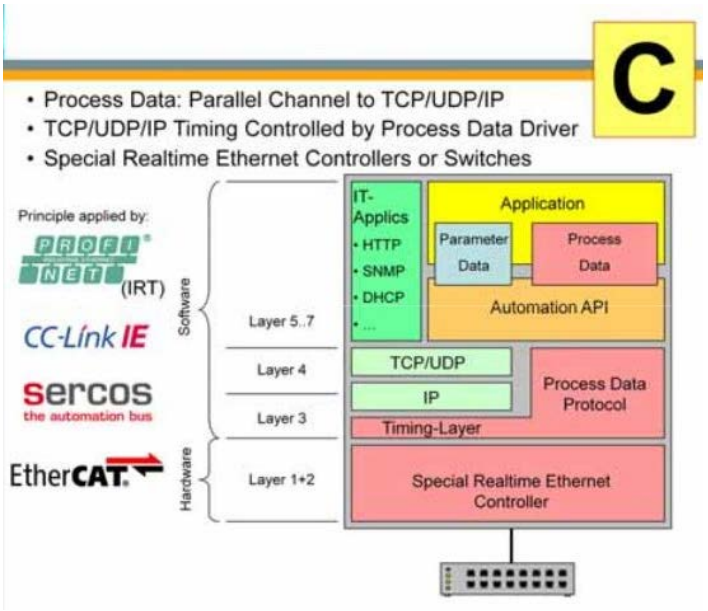


Figura 1.76- arquitectura Profinet IRT (fuente: www.ethercat.org)

OPC (Open Platform Communications) es el estándar de interoperabilidad para el intercambio seguro y fiable de datos en la automatización industrial, es independiente de la plataforma y garantiza un flujo de información sin fisuras entre dispositivos de múltiples proveedores.

Estas especificaciones definen la interfaz entre clientes y servidores, así como entre servidores y servidores, incluyendo el acceso a datos en tiempo real, el seguimiento de alarmas y eventos, el acceso a datos históricos y otras aplicaciones.

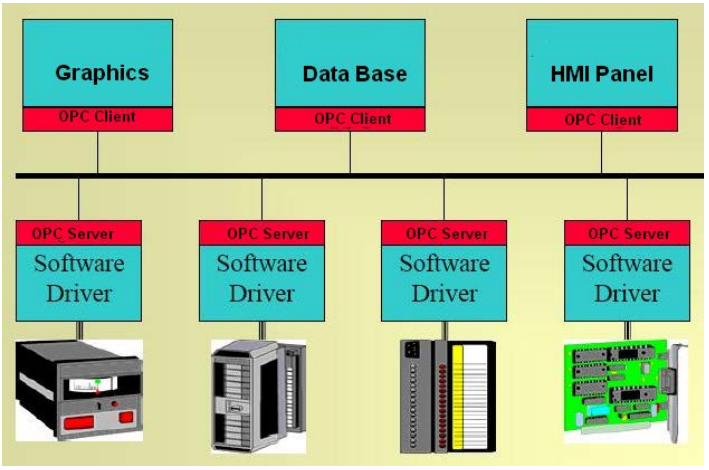


Figura 1.77- arquitectura OPC servidor/cliente (fuente: Wikipedia)

OPC está diseñado para proporcionar un **puente común** para aplicaciones de software y hardware de control de procesos para acceder a los datos de campo de los dispositivos de planta de la planta (Figura 1.78).

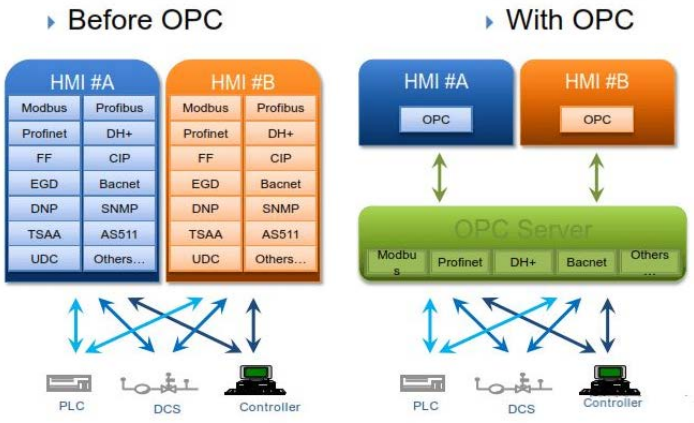


Figura 1.78- arquitectura OPC (fuente: www.theautomization.com)

Un **servidor OPC** para un dispositivo de hardware proporciona los mismos métodos para que un **cliente OPC** acceda a sus datos. Una vez que un fabricante de hardware desarrolló su servidor OPC para el nuevo dispositivo de hardware, su trabajo se hizo para permitir que cualquier"extremo superior" accediera a su dispositivo, y una vez que el productor de SCADA desarrolló su cliente OPC, su trabajo se hizo para permitir el acceso a cualquier hardware con un servidor compatible con OPC.

La **Arquitectura Unificada OPC (UA)** es una arquitectura orientada a servicios independiente de la plataforma que integra toda la funcionalidad de las especificaciones individuales de OPC Classic en una estructura extensible.

Las tecnologías y metodologías innovadoras, como nuevos protocolos de transporte, algoritmos de seguridad, estándares de codificación o servicios de aplicaciones, pueden incorporarse a la UA OPC, manteniendo al mismo tiempo la compatibilidad retrospectiva.

Ejercicio 1. Configuración del equipo

En este primer ejercicio vas a ver cuál es la configuración de red de tu equipo.

Abre una ventana de interfaz de comandos (Ejecutar>command). Te saldrá una ventana como ésta:

Recuerda como se abre porque te hará falta más adelante.

Escribe “ipconfig” (sin las comillas) y pulsa Enter. El comando te devolverá los datos de configuración de red de tu PC. Rellena esta tabla con la respuesta:

Dirección IP	
Máscara de subred	
Puerta de enlace predeterminada (router)	

Escribe “ipconfig /?” Para ver las opciones del comando.

Escribe “ipconfig /all” para que te devuelva la configuración avanzada. Esta misma información se puede ver ejecutando winipcfg (Inicio/ejecutar/winipcfg). Rellena la tabla.

Configuración IP de Windows	
Nombre del host	
Sufijo DNS principal	
Enrutamiento habilitado	
Adaptador Ethernet	
Dirección física	
DHCP habilitado	

Rellena la tabla con los datos de tus compañeros de la derecha y la izquierda (si estás en una esquina, pregunta a otro compañero). Mira qué valores son iguales, y cuáles distintos.

Compañero izquierda

Configuración IP de Windows	
Nombre del host	
Sufijo DNS principal	
Enrutamiento habilitado	
Adaptador Ethernet	
Dirección física	
DHCP habilitado	
Dirección IP	
Máscara de subred	
Puerta de enlace predeterminada (router)	
Servidores DNS	

Compañero derecha

Configuración IP de Windows	
Nombre del host	
Sufijo DNS principal	
Enrutamiento habilitado	
Adaptador Ethernet	
Dirección física	
DHCP habilitado	
Dirección IP	
Máscara de subred	
Puerta de enlace predeterminada (router)	
Servidores DNS	

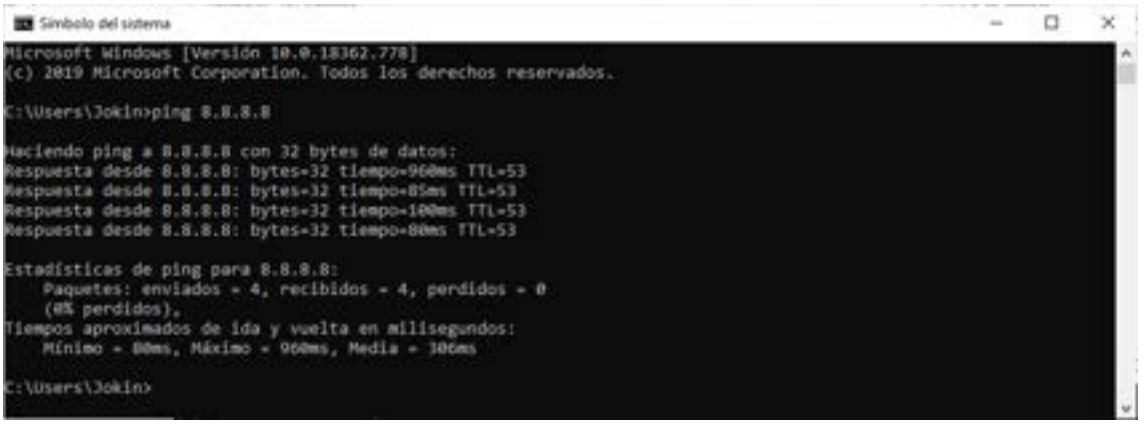
Ejercicio 2. Direccionamiento IP

En Internet los ordenadores están se identifican con la dirección IP (Internet Protocol ó Protocolo de Internet). Esta compuesta por 4 números, separados por 3 puntos. Cada uno de los 4 números puede valer desde 0 a 255. (Ej: 192.168.2.3, ó 158.42.4.2).

Además, existe otro tipo de identificación, utilizando nombres de dominio (por ejemplo www.google.com). Gracias a un protocolo llamado DNS, el ordenador sabe qué dirección IP, en este caso la dirección IP 216.58.201.164, corresponde a ese nombre.

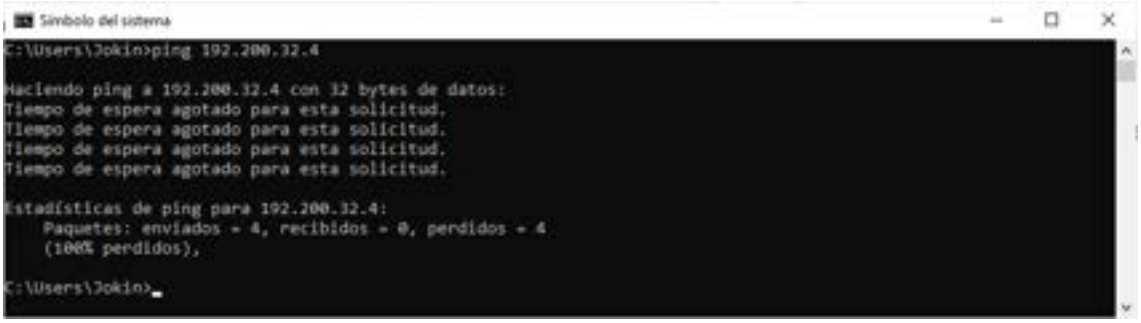
Abre una ventana de interfaz de comandos (Ejecutar>command). Te saldrá una ventana como ésta:

Ejecuta el comando “ping 8.8.8.8” y comprueba que el resultado es parecido a este.

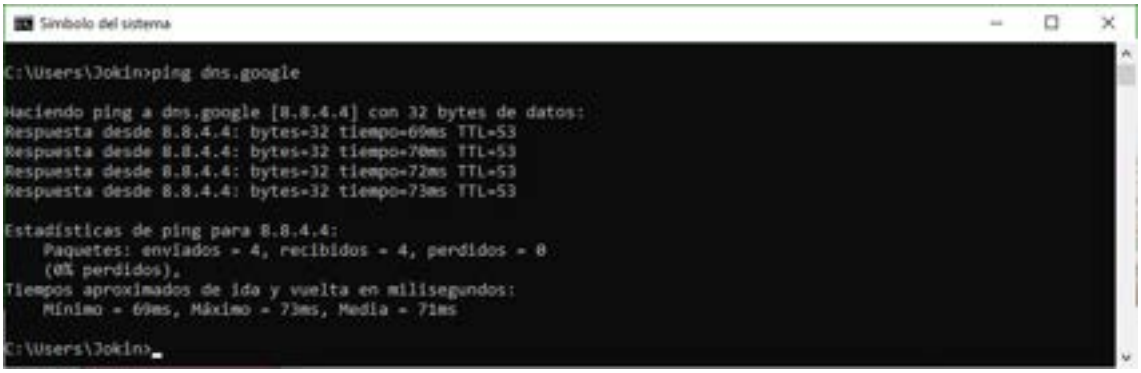


El parámetro de respuesta “tiempo” indica el tiempo (normalmente milisegundos) que tarda un paquete ICMP (corresponde al comando *ping*) en llegar al destino (en este caso al ordenador con dirección IP 8.8.8.8) y volver al remitente (nuestro equipo).

Si no existe conectividad entre el remitente y el destino, el mensaje de error es algo parecido a lo siguiente.



Comprueba que ocurre al ejecutar el comando “ping dns.google”, debería traducirse el nombre *dns.google* a su dirección IP equivalente, ¿cuál es esa IP?



Ahora ejecuta “ping www.google.com”, ¿cuál es su IP?

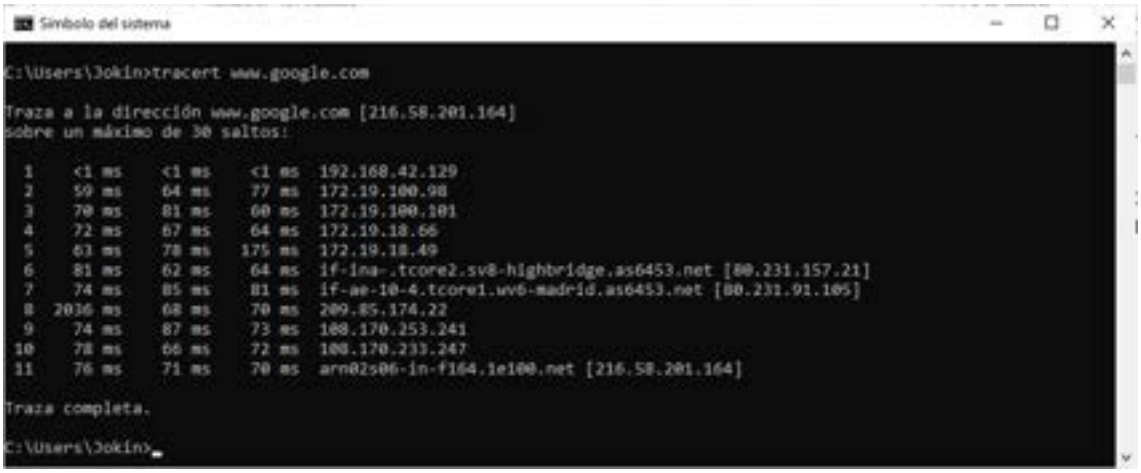
Ejercicio 3. Comando tracert

Internet está formado por muchas redes, unidas entre sí por unos equipos de comunicaciones llamados routers. Cuando se envía información por Internet, los datos van pasando entre routers para llegar desde el origen al destino. Cada vez que se cambia de red a través de un router, se dice que la información ha dado un salto.

Para saber por qué equipos se pasan para llegar a algún destino, se puede utilizar el comando tracert (del inglés trace route). Este comando funciona igual que el ping. En una ventana de interfaz de comandos hay que ejecutar tracert seguido de la dirección IP o nombre de dominio sobre el que queremos preguntar. Si se pregunta por un dominio, también hace la resolución a dirección IP.

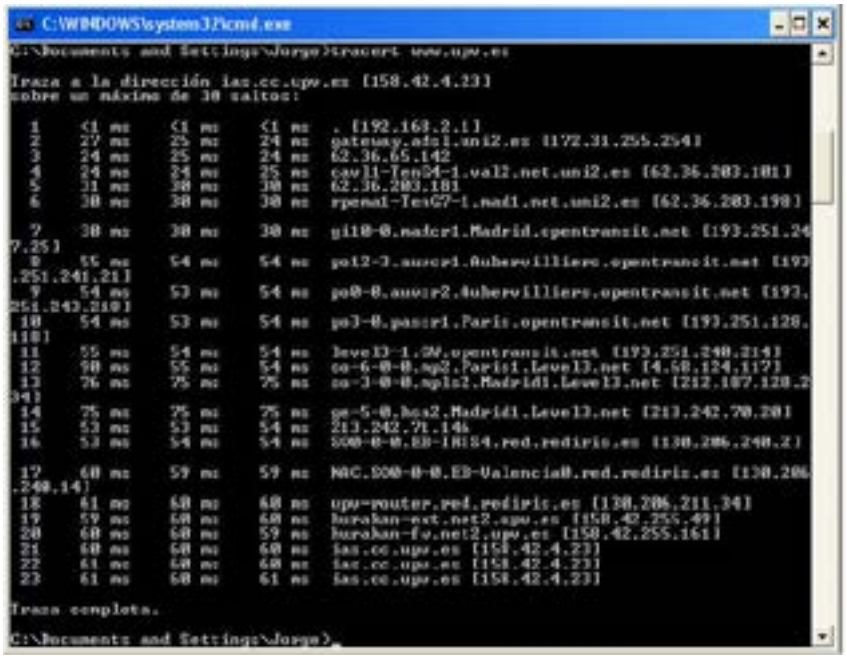
Por ejemplo, para saber cómo llegamos al servidor web de Google ejecutamos

“tracert www.google.com”



En la respuesta se indican las direcciones IP de los router por los que pasa la petición de respuesta hasta llegar al destino y los tiempos de respuesta de cada uno de ellos.

Con el comando tracert se pueden encontrar cosas “curiosas”, como que no siempre se sigue el camino más corto para llegar a un destino. En el ejemplo siguiente se puede ver que para llegar desde Bilbao hasta el servidor de la UPV, que está en Valencia, ha pasado por varios routers de Paris.



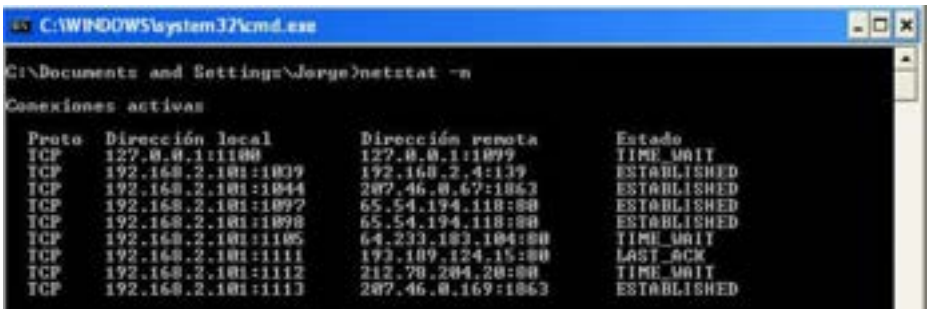
Rellena la siguiente tabla realizando un tracert a los dominios indicados

Nombre	Número de saltos
www.elpais.com	
www.upv.es	
www.marca.com	
Smtp.correo.yahoo.es	
www.google.com	

Ejercicio 4. Comando netstat

El comando Netstat muestra las conexiones que tiene abiertas el ordenador con otros ordenadores, por ejemplo al conectarte a una página web o descargar el correo electrónico.

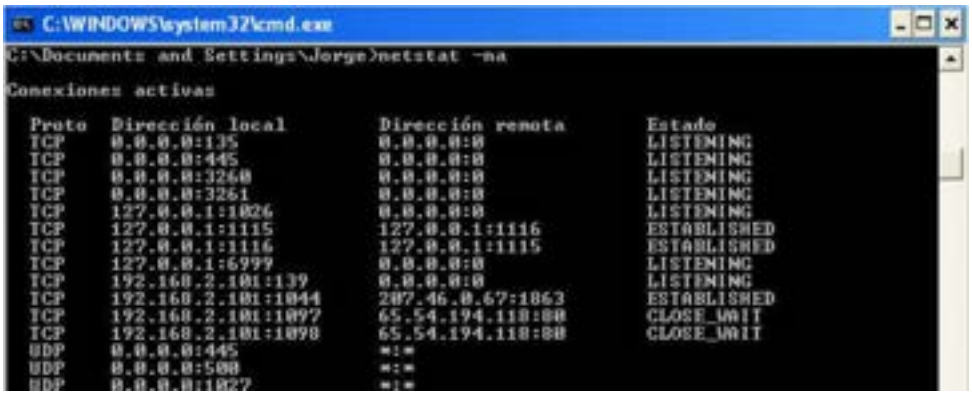
Ejecuta el comando “netstat -n” y comprueba las conexiones que tiene abiertas tu ordenador.



En la respuesta del comando Netstat, tanto la dirección local como remota se indican con la IP o nombre del ordenador, seguido de dos puntos y el número del puerto. El puerto es un número que indica la aplicación o protocolo que se está utilizando.

Por ejemplo, el puerto 80 es el del protocolo http, para páginas web; o el 1863 es el puerto del Messenger (aplicación de mensajería en desuso).

Una opción del comando netstat es -a. Con ella, te dice qué puertos tienes abiertos en tu ordenador. Son aplicaciones que están escuchando como servidores en tu ordenador, y que permitirían a otras personas conectarse a tu ordenador (por ejemplo si tienes compartida alguna carpeta). Se diferencian porque el estado es *listening* o escuchando.



Ejecuta netstat -na en tu línea de comandos, ¿Cuántas conexiones hay? ¿Cuáles son sus direcciones IP y puertos?

Ejercicio 5. Cómo conectarse por SSH / Telnet a un router para una configuración avanzada con PuTTY

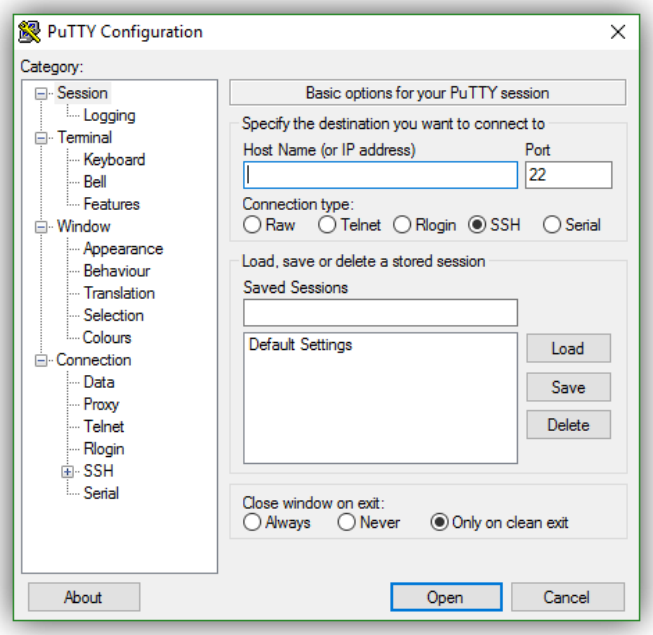
Hoy en día, prácticamente todos los routers del mercado cuentan con una interfaz web desde donde podemos realizar todo tipo de configuraciones: cambiar usuario/contraseña, configurar el Wi-Fi, abrir los puertos, etc. Esta interfaz está pensada principalmente para usuarios domésticos, sin demasiados conocimientos avanzados ya que, además de ser muy sencilla de utilizar, solo muestra las opciones principales y las más utilizadas de los routers, quedando un gran número de funciones más ocultas y sin poder acceder a ellas, al menos a través de esta interfaz.

Prácticamente todos los routers cuentan con un servidor Telnet que nos permite comunicarnos con el router desde línea de comandos, ideal para los usuarios expertos y con más conocimientos, ya que desde allí vamos a poder controlar prácticamente todas las configuraciones internas del router en caso de que necesitemos acceder a ellas. De igual modo, los modelos de routers algo más avanzados cuentan con soporte para el protocolo SSH, un protocolo que nos permite conectarnos de igual forma que por Telnet, pero cifrando todas las conexiones.

Aunque Windows permite habilitar en el sistema un cliente Telnet y SSH, existen aplicaciones de terceros mucho más sencillas de utilizar que nos van a permitir gestionar correctamente estas conexiones, como es el caso de PuTTY.

PuTTY es una aplicación gratuita, portable y de código abierto desarrollado para facilitar la conexión a través de los protocolos SSH / Telnet desde Windows. A continuación, vamos a ver cómo podemos conectarnos de forma remota a un router a través de estos protocolos.

Lo primero que debemos hacer es descargar la versión más reciente de PuTTY desde su página web principal. Como es portable no necesita instalación, por lo que una vez descargada lo único que debemos hacer es ejecutarla y veremos una ventana similar a la siguiente.



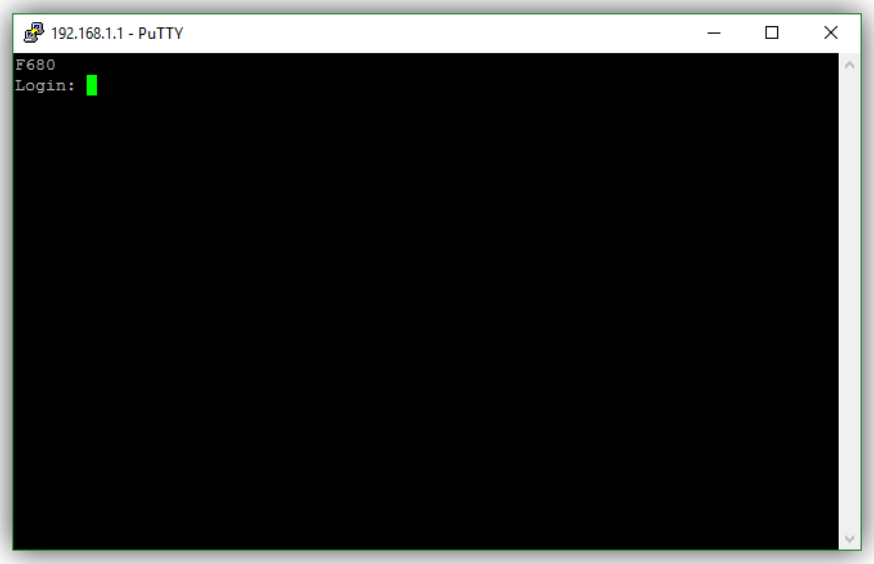
Lo primero que debemos hacer es introducir la dirección IP de nuestro router que, por lo general, suele ser 192.168.1.1 o 192.168.0.1, dependiendo de modelos y configuraciones.

Justo debajo del apartado para introducir la IP tenemos «**Connection type**«, un apartado en el que debemos especificar el protocolo que vamos a utilizar, siendo los más conocidos, como hemos dicho, SSH y Telnet. Si

nuestro router se conecta mediante puerto serie, PuTTY también nos permitirá establecer conexión con él para configurarlo por comandos.

Una vez introducida la IP y seleccionado el protocolo de conexión pulsamos sobre «**Open**» y el programa se conectará con el router.

Si la conexión está permitida y se ha podido establecer, el propio PuTTY nos mostrará una ventana como la siguiente.



Ahora, lo único que nos queda por hacer es iniciar sesión con nuestro usuario y contraseña para empezar a controlar el dispositivo.

Es posible que el usuario y la contraseña Telnet / SSH no sea el mismo que en la interfaz web, especialmente en los routers de las operadoras.

Co-funded by the
Erasmus+ Programme
of the European Union

MÓDULO 2

Conceptos de Ciberseguridad en entornos industriales, Integración IT/OT

2.1 Seguridad en Infraestructuras Críticas

Description

2.1 Seguridad en Infraestructuras Críticas

Table of contents

La seguridad de la planta garantiza que los edificios que participan en el progreso de la fabricación están bien protegidos ante el acceso prohibido. Algunas contramedidas tomadas pueden serlo:

- **Vallas**

Lo más común es que las instalaciones de la planta estén rodeadas por una valla (Figura 2.1).

Figura 2.1 Zona industrial con una valla fuente

Lo habitual es que la valla de una planta establezca los límites de la propiedad de la planta, pero su uso principal es proporcionar una primera medida de seguridad contra posibles intrusos. Aunque una valla por sí sola no previene a un intruso, si se usa junto con otras medidas de seguridad puede ser una buena solución de seguridad. Hoy en día, las vallas se están volviendo «inteligentes». Esto significa que los sensores dispuestos a lo largo de la valla pueden identificar si un intruso ha entrado en el área prohibida. Esta nueva generación de vallas se puede conectar a una red.

G

- **Guardias.**

Th

La presencia de guardias depende principalmente del tipo y tamaño de la instalación. Dependiendo de la ley, también pueden estar armados. Normalmente hay un puesto de avanzada en la puerta principal de la fábrica y los guardias permiten o no la entrada del personal y de los visitantes. Otra parte de sus obligaciones podría ser el patrullaje a lo largo de la planta, especialmente cuando la fábrica está cerrada.

- **Tornos**

Un torno (Figura 2.2) puede estar presente en la puerta principal de la fábrica. Evita que los visitantes de la planta entren en la instalación sin control y también retrasa a los intrusos. Las últimas implementaciones proporcionan a los tornos capacidad de conectarse a la red .

Figura 2.2: un torno - Fabtron - CC BY-SA 4.0 fuente

Ø

- **CCTV cameras**

CCTV significa circuito cerrado de televisión. Las cámaras de seguridad (Figura 2.3) se colocan alrededor del perímetro exterior de la planta (generalmente en bóvedas sobre la valla exterior) para registrar cualquier actividad las 24 horas del día, los 7 días de la semana. También se colocan cámaras de seguridad en el edificio, en la entrada principal y, en muchos casos, también en las zonas de trabajo. En grandes instalaciones (con un gran número de cámaras de seguridad) existe una sala de control, donde personal autorizado y capacitado hace un seguimiento de las cámaras para detectar conductas delictivas. Todos los datos capturados en las cámaras se almacenan en discos duros en un grabador de vídeo digital (DVR) o en un grabador de vídeo en red (NVR). En este último caso, los técnicos de instalación y el personal de supervisión deben tener mucho cuidado, ya que el NVR puede ser fácilmente el blanco de un ciberataque.

Figura 2.3 camaras de seguridad

- **Lectores biométricos**

Se colocan en el exterior de puertas, portones principales, etc. Los datos biométricos típicos utilizados para identificar a una persona incluyen: las huellas dactilares, el iris de los ojos y la forma de la cara. Dado que todas las características biométricas mencionadas anteriormente son únicas para cada persona, se supone que los lectores biométricos proporcionan un nivel de seguridad muy bueno. Sin embargo, existe el riesgo de que los lectores biométricos también se vean comprometidos, especialmente cuando están conectados a la red. Los lectores biométricos también se pueden utilizar junto con una tarjeta RFID o una contraseña (Figura 2.4). Los últimos lectores biométricos tienen capacidad de red, por lo que el riesgo de convertirse en blanco de un ataque cibernético es relativamente alto

Ø 

Figura 2.4 lector biométrico - fuente

Ø

- **Controles de acceso**

Estos sistemas de seguridad se utilizan para proporcionar acceso al personal autorizado o a los visitantes. Son programables y pueden definir diferentes derechos de acceso según el plan de seguridad de la industria. Los distintos empleados pueden tener diferentes derechos de acceso en cuanto a las áreas que pueden visitar, los horarios de visita, etc. Como todos los métodos mencionados anteriormente, los controles de acceso también tienen capacidades de red. Se pueden utilizar lectores RFID, tarjetas magnéticas inteligentes o incluso lectores biométricos.

Seguridad de la red

- Se refiere tanto al hardware como al software
- Se centra en una variedad de amenazas
- Evita el acceso no autorizado a las redes
- Supervisa el acceso a la red

Los **tipos comunes de seguridad de red** son:

- Software de seguridad de Internet (antivirus, anti-malware, protección de ransomware, etc.)
- Seguridad de las aplicaciones utilizadas en el sistema
- Evitar la pérdida de datos
- Seguridad del correo electrónico
- Cortafuegos - Segmentación de redes - Seguridad Web de redes privadas virtuales (VPN)
- Seguridad inalámbrica
- Control de acceso a la red

La integridad del sistema se refiere a todas las medidas/políticas adoptadas para proteger los sistemas y componentes de automatización contra el acceso no autorizado (físico o remoto). Algunas de las medidas podrían ser:

- Software antivirus y de listas blancas
- Procesos de mantenimiento y actualización
- Autenticación de usuarios para operadores de plantas o máquinas
- Mecanismos de protección de acceso integrados en los componentes de automatización

2.2. Integración IT/OT

Description

2.2. Integración OT/IT

Table of contents

La **Tecnología de Operación (OT)** en cualquier entorno industrial se define como el hardware y software que detecta o causa un cambio a través de la monitorización o control directo de dispositivos físicos, procesos y eventos en la empresa. Básicamente, OT es la utilización de equipamiento digital e informático para monitorear o cambiar la condición física de un sistema. Ejemplos de tecnología operativa:

- PLC
- SCADA
- Equipamiento científico
- DCS

La **Tecnología de la Información (TI)** se refiere a todo lo que se identifica con el registro de la innovación en la tecnología informática, equipos de PC, programación de software, administración de hardware y sistemas, etc. La programación de software incorpora todos los programas de PC (códigos y directrices) dentro de un PC. Los PCs no funcionan sin programación. El hardware informático, mencionado en esta situación, alude a los segmentos físicos de un PC. La (pantalla), el ratón y la placa base, y hay otros dispositivos en los que son dispositivos de hardware.

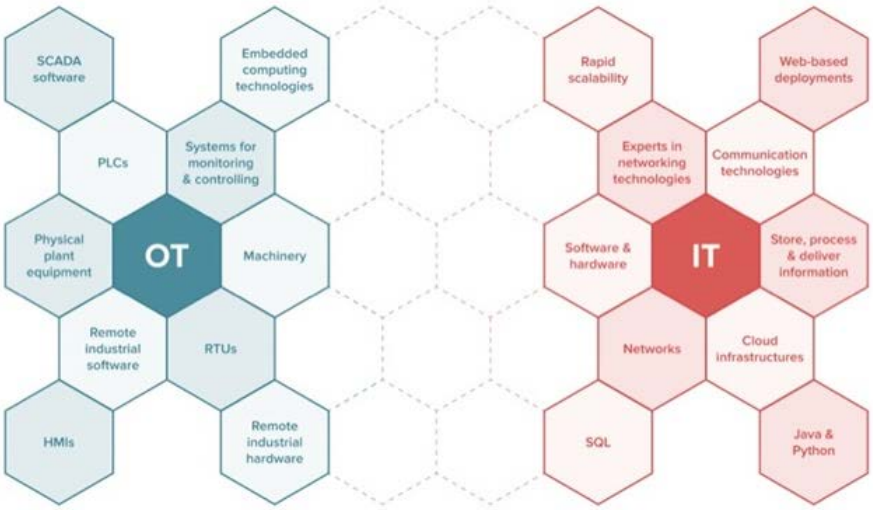


Figura 2.5- tecnologías IT/OT (fuente)

Las tecnologías IT incluyen comunicaciones, hardware, software del sistema que almacenan, procesan y transmiten datos a todas las partes de una organización. Los expertos en TI pasan un tiempo significativo en el progreso, por ejemplo, de bases de datos en la nube, aplicaciones web y tecnologías de programación (Python, SQL, Java, C++) etc.

OT incluye dispositivos y equipos físicos, hardware y software industrial. Los expertos de OT se centran en los sistemas utilizados para la automatización, supervisión y el control. En este entorno se utilizan PLC's, Interfaces Hombre-Máquina (HMIs), tecnologías de computación embebidas, Unidades Terminales Remotas (RTU's), Sistemas de Control y Adquisición de Datos (SCADA).

Los sistemas SCADA recopilan información de varios procesos en la planta de producción. Los individuos que trabajan en OT deben saber cómo integrar cada uno de los sistemas para cooperar juntos. Puesto que la mayoría de las innovaciones de OT son propietarias de un fabricante, los sistemas SCADA pueden ser difíciles de integrar.

PROFINET (red OT) y Ethernet (red IT) son dos protocolos muy extendidos que pueden ser interconectados (más información en el Modulo 1). El único problema cuando estos dos protocolos están interconectados es que puede reducir la disponibilidad.

Para más información sobre las contramedidas de seguridad, visita: https://www.iso.org/isoiec-27001- information-security.html

Aumenta la producción y ahorra tiempo

Las tecnologías IT han ayudado a mejorar la rentabilidad de los negocios, lo que implica una mejor remuneración y unas condiciones de trabajo menos tediosas.

Mejora la comunicación

Las herramientas de las Tecnologías de la Información y la Comunicación (TIC), como el correo electrónico, las videoconferencias, los teléfonos móviles, los ordenadores portátiles, etc., permiten la comunicación directa dentro de una empresa. Esto permite una mayor conectividad a través de las estructuras interiores y exteriores.

Mejora el almacenamiento de datos, la gestión de archivos y la generación de informes y análisis de datos.

Las empresas utilizan servicios Cloud que facilitan a las empresas el almacenamiento y la copia de seguridad de los datos para reforzar la información empresarial. Además, ahorra tiempo y facilita la transferencia y el acceso a los datos desde cualquier lugar y en cualquier momento de forma remota. Con servicios como Dropbox, las empresas pueden obtener su información en cualquier momento. Además, las bases de datos de hoy en día tienen en cuenta un mejor análisis de una gran cantidad de datos que avanzan hacia una mejor toma de decisiones y con un efecto positivo sobre el desarrollo de la empresa.

Reducir los costes operativos

Las tecnologías de la comunicación y las redes sociales han hecho que el avance comercial y el lanzamiento de productos sean asequibles. Numerosas compañías utilizan las redes sociales con el fin de elevar el conocimiento de su marca y conseguir más clientes a un coste insignificante. Elementos como el coste juegan un papel decisivo en el avance y desarrollo de un negocio. En este sentido, la utilización de las innovaciónes de las tecnología TIC para reducir los costes operativos traerán el desarrollo empresarial.

Mejora la competitividad del negocio

El uso de la tecnología en los negocios se debe a que se pretenden obtener ventajas competitivas. Las empresas que avanzan y adoptan la innovación para seguir siendo productivas y mejorar sus procesos normalmente gozan una alta confianza por parte de sus clientes, ya que pueden satisfacer mejor los deseos de sus clientes.

Sin embargo, la integración OT/IT también tiene desventajas:

Costes de implementación

Las pequeñas empresas a veces tienen una tecnología básica y tratan de mantenerla para poder competir con otras empresas de su sector, al mismo tiempo que disponen de los fondos y recursos necesarios.

Eliminación de empleo

Como bien se sabe, el crecimiento de las tecnologías ha sustituido a las personas en varios puestos de trabajo.

Violaciones de la seguridad

Dado que las empresas almacenan su información en servidores remotos en la nube a los que se puede acceder con un nombre de usuario y una contraseña secreta, existe la posibilidad de que se pierda esa información debido a fallos de seguridad o hackers.

Para garantizar la seguridad y la fiabilidad, es importante contar con prácticas bien documentadas para la instalación de actualizaciones de software. La siguiente tabla ofrece reglas para las copias de seguridad, administrar el proceso de actualización y planificar las actualizaciones.

El mantenimiento de un calendario estándar de actualizaciones, así como la aplicación de correcciones básicas y la detección de vulnerabilidades, es vital para mantener la seguridad corporativa. Con la llegada de amenazas como ransomware, la realización de actualizaciones de seguridad y la creación de copias de seguridad es importante para garantizar el correcto funcionamiento del negocio.

En la Tabla 1 aparece un ejemplo de las medidas de seguridad que deberían tomarse para proteger adecuadamente un ordenador.

Tabla 1: Política de seguridad en un ordenador

Actualizaciones semanales	
Acción:	Actualizaciones y parches de seguridad para las aplicaciones instaladas.
Fecha planificada:	Todos los jueves (o un día concreto) empezando a las 8 PM.
Estado de alimentación:	El PC debe estar encendido para recibir las actualizaciones.
Estado de sesión:	El PC instalará las actualizaciones independientemente de que haya un usuario o no trabajando en el sistema. Debe guardar su trabajo ya que el PC se reiniciará haya o no aplicaciones en marcha.
Fallo en la actualización:	Si el equipo no se enciende durante la actualización programada, las actualizaciones de la aplicación se aplicarán la próxima vez que se encienda el equipo.
Copia de seguridad:	Realizar copia de seguridad de archivos importantes dos veces al mes
Si un usuario tiene una sesión abierta	
Descripción general:	El equipo intentará instalar las actualizaciones,se le dará al usuario una serie de opciones de instalación y opciones de reinicio que se adapten al plan de trabajo. Se aplicarán actualizaciones y se reiniciará el equipo si no se responde a las indicaciones.
Tiempo límite de la interrupción:	Si la actualización no se interrumpe en 30 minutos, comenzará a instalarse automáticamente.
Interrupción del reinicio:	Si se aplica una actualización que requiere reiniciar el PC, el usuario puede reiniciar el sistema hasta siete (7) veces antes de que el ordenador se reinicie automáticamente para completar la instalación. La interrupción puede durar 30 minutos antes de que se informe al usuario

Tiempo límite de reinicio:	Si el reinicio no se interrumpe en 30 minutos, el equipo volverá a solicitarlo en 120 minutos (es decir, otra repetición). Después de las siete (7) repeticiones mencionadas anteriormente, el usuario se verá obligado a reiniciar el ordenador.
Frecuencia de reinicio:	Si una actualización requiere un reinicio, el PC se reiniciará una vez automáticamente.
Impacto en el rendimiento:	Las actualizaciones de la aplicación varían en número y tamaño en cualquier momento. El impacto en el rendimiento del ordenador es generalmente insignificante con un posible reinicio después de la instalación.

Si no hay una sesión de usuario abierta

Descripción:	El PC instalará las actualizaciones y se reiniciará si es necesario.
Frecuencia de reinicio:	Si se instala una actualización que requiera reiniciar el PC. se reiniciará una vez.

Los PLC (automata programable) son tan importantes en las redes de sistemas de control como lo serían en cualquier otro entorno de red. Es esencial que se gestionen con la máxima prioridad. Cualquier acceso, mantenimiento, actualización, prueba, modificación, tiempo de inactividad de los PLCs debe ser contabilizado y estas políticas deben ser aplicadas.

Principios básicos de la política de seguridad en PLC´s

- **Corrección de contraseñas predeterminadas**

Cambiar todas las contraseñas predeterminadas. No modificar las contraseñas predeterminadas de fábrica es uno de los errores más comunes que cometen las organizaciones en lo que a las contraseñas se refiere.

- **Asegurarse de que sólo haya personas autorizadas en el entorno del sistema de control.**

Por razones de seguridad, sólo deben estar presentes las personas que tienen acceso autorizado al sistema de control de la empresa.

- **Limitación del acceso a las unidades de memoria USB y acceso seguro**

A menudo debe informarse a los usuarios sobre las limitaciones en el uso de los dispositivos USB y las tecnologías de acceso remoto.

- **Actualizar el firmware a la última versión**

Una actualización común del sistema operativo/actualización de firmware es una actualización de seguridad, que se emite para proteger su ordenador/sistema contra vulnerabilidades que podrían explotar los hackers y los virus.

Figura 2.6- PLC fuente)

Figura 2.7- PLC (fuente)

2.3 Ataques en Sistemas Industriales

Description

2.3 Ataques en Sistemas Industriales

Table of contents

DOS es el acrónimo de **Denegación de Servicio** (Denial of Service). Es un tipo de ataque que tiene lugar en un ordenador o red, impidiendo que los recursos del sistema sean accesibles a los usuarios. Apaga el sitio (servidor web) al que se dirige. Para lograr este objetivo se crean muchas peticiones de servicio al mismo tiempo de modo que el servidor que no responde a todas las peticiones. Por lo tanto, mientras haya un ataque DoS, el tráfico regular del sitio web será lento o inactivo.

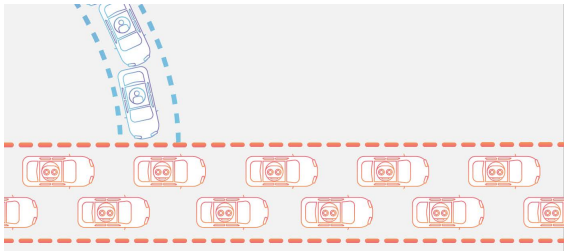


Figura 2.8- tráfico debido a ataque DOS (fuente)

Bloquear algunos servicios de la web puede conducir a una gran pérdida económica ya que Internet y las redes informáticas conectan con sus clientes a un gran número de organizaciones. El comercio electrónico y los servicios de pago dependen de Internet para funcionar como negocio.

Hay dos tipos de ataques:

- **DoS**: este tipo de ataque es realizado por un solo host. (Figura 2.9)
- **Distributed DoS(DDoS)**: se logra enviando un gran número de peticiones innecesarias al sistema o a los recursos de la red desde muchas fuentes diferentes. (Figura 2.10)

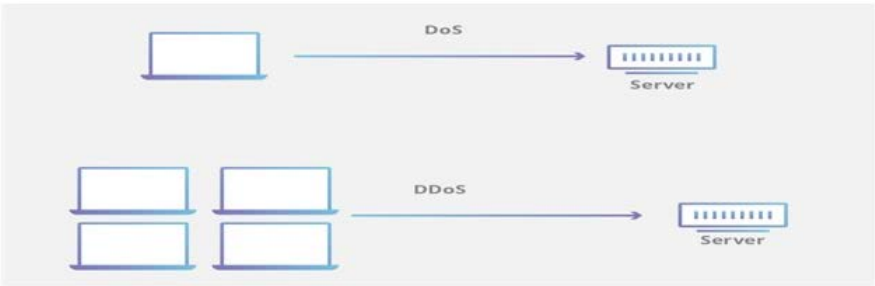


Figura 2.9- tipos de ataque DoS (fuente)

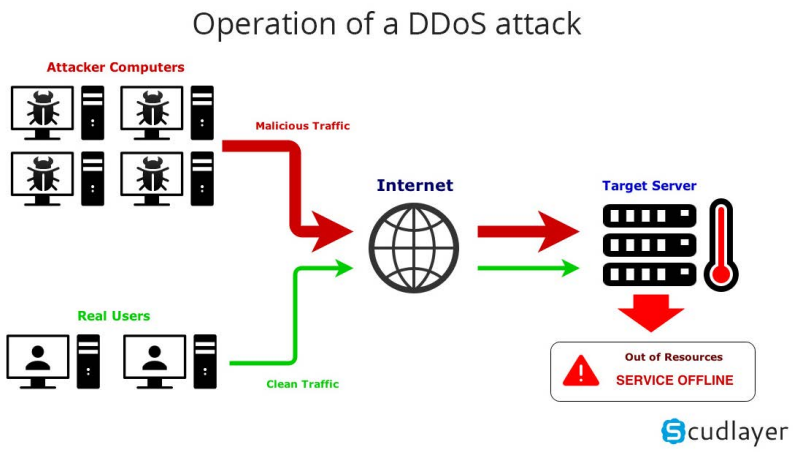


Figura 2.10- funcionamiento de un ataque DDos (fuente)

Hay tres tipos de ataquesf DDoS:

- **Ataques basados en Volumen**
- **Ataques de Protocolo**
- **Ataques del nivel de Aplicación**

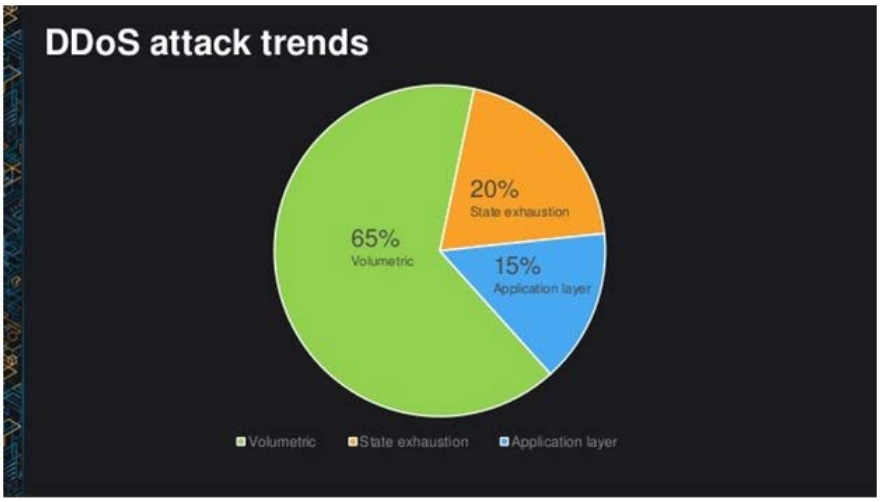


Figura 2.11- tendencia de ataques DDos (fuente)

Ataques basados en volumen, como su nombre indica, **se basan en el volumen de peticiones maliciosas generadas que "inundan" la red**; estos ataques también son llamados **ataques de Capa 3 y 4**.

El atacante utiliza tácticas muy básicas y la mayoría de los recursos disponibles se pueden consumir en este"juego". Si consiguen sobrecargar los recursos disponibles, los servidores se quedan sin capacidad de respuesta y por lo tanto los servicios se "bloquean". Para la mayoría de los propietarios de sitios, es fácil quedarse sin recursos. La magnitud del ataque se mide en **Bits por Segundo (bps).**

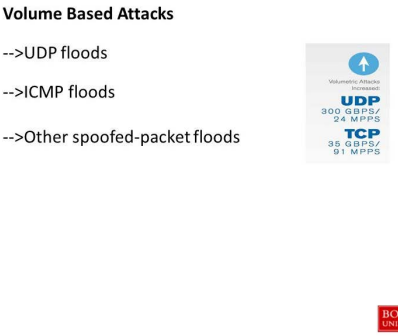


Figura 2.12- ataques basado en volumen (fuente)

Algunas de los "**inundaciones"** de tráfico indeseado (**floods**) son:

- **Flood de UDP:**

Un ataque de flood de UDP implica el **envío** de un gran número de **paquetes UDP** (datos de nivel 4) a los puertos aleatorios de una computadora, especialmente al puerto número 53. El ordenador atacado tendrá que determinar si alguno de sus servicios está escuchando en ese puerto y si no responde debe **responder** con un **paquete ICMP** indicando que el destino es inalcanzable. Por lo tanto, la afluencia de un gran número de paquetes UDP al ordenador atacante le obliga a responder con un número igualmente grande de paquetes ICMP, lo que en última instancia impide que otros usuarios ordinarios utilicen sus servicios. Los cortafuegos especializados pueden utilizarse para filtrar o bloquear paquetes UDP maliciosos.

- **Flood ICMP:**

El atacante envía paquetes de solicitud ICMP a un servidor remoto. Para que este ataque tenga éxito, el atacante debe tener más ancho de banda que la víctima. Si la víctima responde con un paquete ICMP de respuesta (ICMP Echo Reply) a cada paquete de petición Ping (ICMP Echo Request), entonces consume todo su ancho de banda y, en consecuencia, los servicios que ofrece ya no están disponibles para los usuarios.

Una táctica para lidiar con este ataque es la de en lugar de rechazar todos los paquetes de ping, se registra el número de paquetes que recibe el cortafuegos, y si se encuentra que ese número excede un límite predefinido, entonces el cortafuegos comienza a rechazarlos.

- **Flood HTTP:**

El ataque de flood HTTP es un tipo de ataque de denegación de servicio en el que el atacante manipula los protocolos HTTP y POST para atacar un servidor web o una aplicación.

Este tipo de ataque está dirigido a los protocolos de comunicaciones. Esta categoría incluye **Synflood, Ping of Death, DNS flood** y otros. La magnitud del ataque se mide en **paquetes por segundo**.

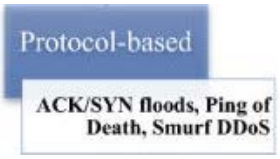


Figura 2.13 Ataques de protocolo

- **Inundación de DNS:**

El atacante se las arregla para enviar un gran número de solicitudes de DNS (peticiones para resolver un nombre de dominio y obtener la dirección IP de un servidor) al objetivo, que aparentemente es un servidor DNS. El resultado es que la víctima recibe tantas peticiones DNS al mismo tiempo que no puede manejarlas y por lo tanto termina cayendo debido a sobrecargas principalmente en su memoria y CPU.

- **SYN Flood:**

El atacante envía múltiples peticiones SYN (peticiones para establecer una sesión en un servidor remoto) a una víctima. El equipo víctima asigna un lugar en sus tablas para cada solicitud que llega y envía un paquete de respuesta SYN + ACK. Si el atacante no responde, o si ha ocultado su dirección IP real, la posición en la tabla permanecerá reservada hasta que expire el tiempo de espera. Si el intruso envía miles de peticiones SYN, la memoria del ordenador de la víctima se llenará y las conexiones legítimas no podrán pasar.

La forma más eficaz de hacer frente a este riesgo es registrar el número de conexiones que cada cliente ha iniciado y prohibir la creación de nuevas conexiones cuando ese número supere un límite predefinido. No obstante, si el atacante en cada nueva petición SYN da una dirección IP de remitente diferente, el método anterior no funciona.

- **Ping of Death:**

Un paquete de Ping es normalmente de 64 bytes (u 84 bytes si se añade la cabecera que añade el protocolo IP). Muchos tipos de ordenadores no pueden manejar paquetes de ping de más de 65535 bytes, que es el máximo permitido por el protocolo IP. Como resultado, el ataque de Ping of Death implica el envío continuo de grandes paquetes de ping a un ordenador hasta que el sistema falla.

Para contrarrestar este ataque, es importante comprobar si los paquetes son válidos al ensamblar los paquetes IP. De esta manera es posible rechazar paquetes IP que son más grandes de lo permitido y así evitar el riesgo de este tipo de ataque.

Este tipo de ataques se centran en las vulnerabilidades en software como Windows, Apache, OpenBSD, etc., para ejecutar el ataque y bloquear el servidor. La magnitud del ataque se mide en **peticiones por segundo**.

- **Ataque a aplicaciones**

También llamado Layer 7 Attack, es uno de los tipos más populares de ataques dirigidos a vulnerabilidades específicas de aplicación de las aplicaciones. Todo lo que se necesita es una pequeña modificación del código y un pequeño ajuste para empezar a enviar información a los hackers. Es extremadamente difícil reconocer los asaltos de nivel 7, ya que se producen después de un tráfico genuino.

- **Slowloris**

Se utiliza para llevar a cabo un ataque DDoS. Envía un gran número de peticiones HTTP al servidor de destino (servidor web). El objetivo mantiene todas las conexiones abiertas y por lo tanto hay un desbordamiento de la conexión concurrente.

- **Ataques DDoS de día cero**

Son un nuevo tipo de ataques que aprovechan vulnerabilidades para las que aun no se ha lanzado ningún parche. El ejemplo más común es explotar vulnerabilidades en las máquinas Linux.

En un ataque SYN Flood el atacante envía múltiples peticiones SYN (sincronización) a la víctima con una dirección IP falsa. El protocolo TCP requiere los siguientes tres pasos para conectarse entre dos ordenadores:

1. El remitente envía el paquete SYN (Synchronize)
2. El destinatario responde con un paquete SYN-ACK (Synchronize Acknowledge)
3. El remitente envía un paquete ACK reciente y la conexión se considera correcta.

El atacante envía múltiples peticiones SYN y no envía ACK, por lo que el proceso continúa, con el objetivo de desperdiciar importantes recursos informáticos e impedir que sirva a otros usuarios.

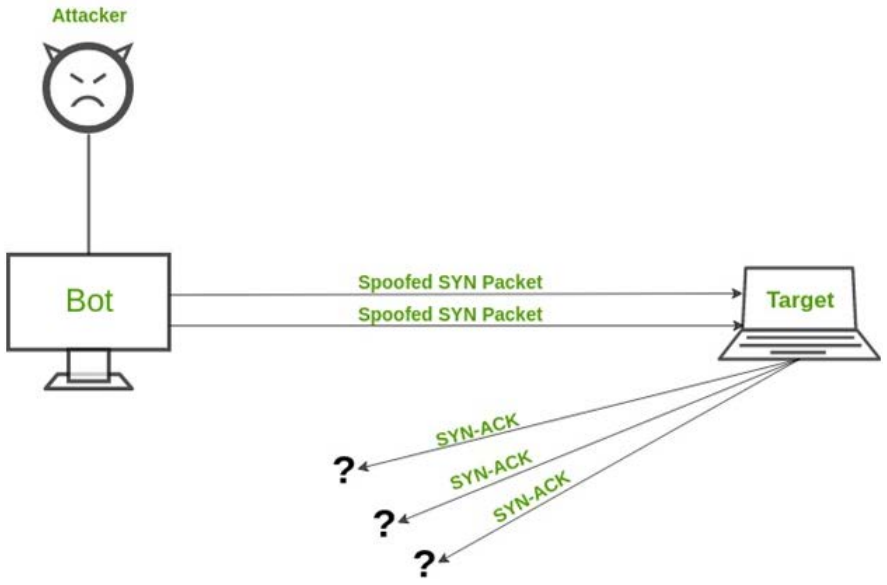


Figura 2.14 ataque de inundación SYN (fuente)

En un **ataque de flood HTTP** se envían múltiples peticiones HTTP GET o POST para atacar un servidor web o una aplicación. El ataque obliga al servidor o a la aplicación a dedicar el máximo de recursos posibles en respuesta a cada petición.

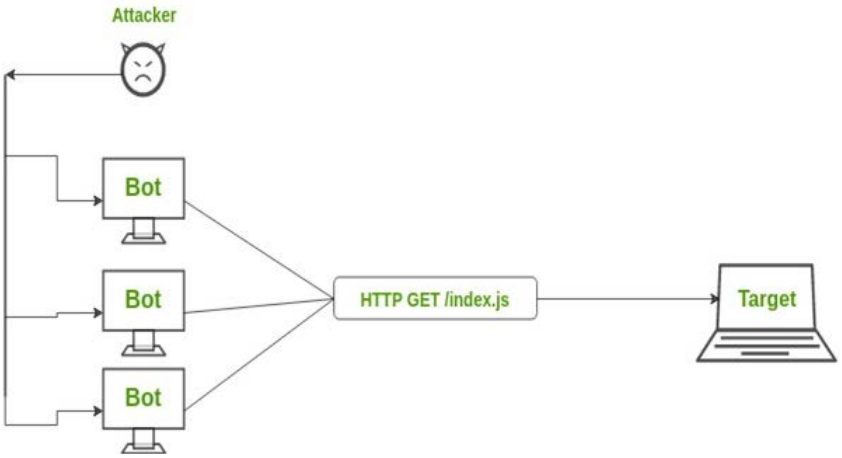


Figura 2.15- ataque de inundación HTTP (fuerte)

Estos ataques son muy populares hoy en día y se observan en las capas 3 y 4. Utilizan servidores DNS ampliamente disponibles de diferentes partes del mundo para inundar el servidor atacado con tráfico de respuesta DNS. El servidor está sobrecargado con una confusión de respuestas y tiene dificultades para funcionar ya que sus recursos disponibles se reducen, lo que hace que no pueda responder adecuadamente al tráfico DNS normal.

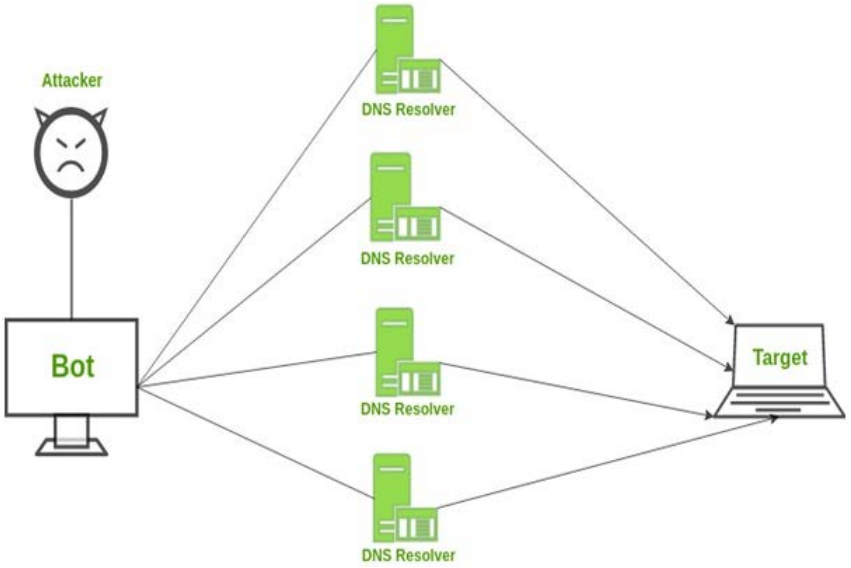


Figura 2.16- ataque de inundación por DNS (fuente)

La prevención de ataques DDoS es más difícil que la prevención de los ataques DoS debido a que el tráfico se origina en numerosas direcciones IP (fuentes maliciosas de datos). Algunas de las técnicas de prevención que se pueden utilizar son:

- **Enrutamiento de agujeros negros**

En el enrutamiento de agujeros negros, el tráfico de red se dirige a un"agujero negro". En este caso, tanto el tráfico malicioso como el tráfico no malicioso se pierde en el agujero negro. Esta contramedida es útil cuando el servidor está experimentando un ataque DDoS y todo el tráfico se desvía para el mantenimiento de la red.

- **Límite de velocidad**

La limitación de velocidad implica el control de la velocidad del tráfico que se envía o recibe a través de una interfaz de red. Es eficaz para reducir el ritmo de los analizadors de sitios web(web scrapers), así como los esfuerzos de inicio de sesión por fuerza bruta. Pero, es poco probable que solo mediante una limitación de la velocidad podamos prevenir los ataques de DDoS.

- **Listas negras/listas blancas**

La lista negra es el mecanismo para bloquear las direcciones IP, URL, nombres de dominio, etc. mencionados en la lista y permitir el tráfico de todas las demás fuentes. Por otra parte, las listas blancas se refieren a un mecanismo que permite a todas las direcciones IP, URLs, nombres de dominio, etc. mencionados en la lista y que niega a todas las demás fuentes el acceso a los recursos de la red.

Una organización puede adoptar las siguientes estrategias para protegerse contra los ataques de Denegación de Servicio.

- Los ataques de SYN flood explotan errores en el sistema operativo (Windows, Linux, etc.) Instalar **parches de seguridad** puede ayudar a disminuir las probabilidades de dichos ataques.
- Los **sistemas de detección de intrusos (IDS)** pueden usarse para hacer un seguimiento de actividades ilegales.
- Los **enrutadores** pueden configurarse a través de la Lista de Control de Acceso para restringir el acceso en la red y eliminar el tráfico ilegal.
- Los **cortafuegos** pueden ser utilizados para detener un ataque DoS al obstaculizar todo el tráfico que se origina de un ataque mediante el reconocimiento de su IP.

Figura 2.17- mitigación de ataques DoS (fuente)

Supongamos que usamos el terminal de Windows (cmd) y tenemos dos ordenadores en la misma red. Los ataques DOS son ilegales en sistemas/redes que no están autorizados. Esta es la razón por la que debes organizar tu propio sistema para hacerlo.

Simplemente abre la línea de comandos de Windows (cmd)

Elegimos otro ordenador (en este caso el de IP 10.128.131.108) como víctima e inundamos esta dirección IP paquetes de 65000 bytes utilizando el comando Ping.

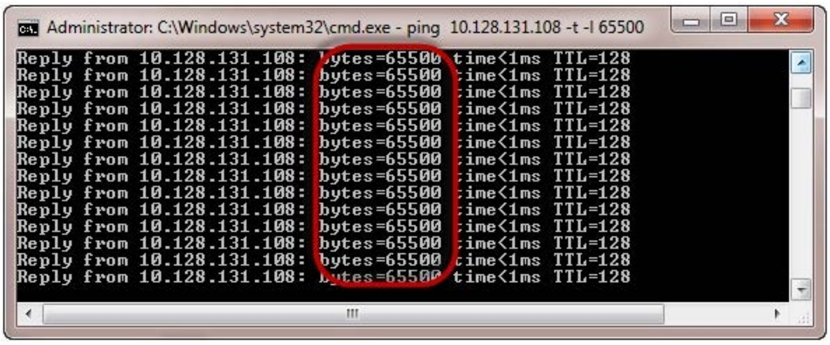


Figura 2.18- inundación DoS

Atacar desde un solo ordenador tiene poco efecto de cara al objetivo a conseguir. Para ser más eficaz necesita más ordenadores atacantes (ataque DDoS).

Este ataque se utiliza a menudo contra servidores web, routers, etc.

Puedes comprobar si el ataque tiene efectos en la víctima. Simplemente abre el administrador de tareas y haz clic en la pestaña de red.

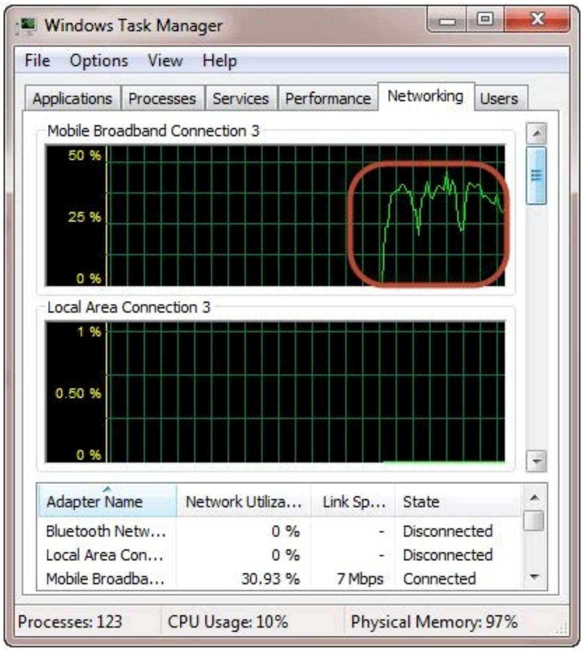


Figura 2.19- actividad de red del ordenador atacado

Como podemos ver, la actividad de la red aumentó cuando el ataque tuvo éxito.

El objetivo de un ataque DOS es **negar a los clientes reales el acceso a un recurso**, por ejemplo, a un sistema, servidor, etc.

Hay dos tipos de ataques, **DOS y DDoS.**

Un ataque DOS se puede llevar a cabo utilizando **HTTP flood, DNS flood, SYN flood, Application attack, buffer overflow**. etc.

Las **actualizaciones** de sistemas operativos, **cortafuegos**, sistemas de monitorización como **IDS** (sistemas de detección de intrusos) y configuraciones de **router/switch**, pueden utilizarse para protegerse contra ataques DOS.

Un ataque de **Hombre en Medio/Man-in-the-Middle (MITM)** ocurre cuando una entidad externa intercepta una comunicación entre dos sistemas. Puede ocurrir en cualquier red o en cualquier forma de comunicación en línea, como por ejemplo correo electrónico, redes sociales, navegación web, banca online, etc.

El objetivo común de un ataque es **robar información** personal, obtener credenciales de inicio de sesión, detalles de cuenta y números de tarjetas de crédito o recursos digitales.

El protocolo ARP

La forma en que funciona el protocolo ARP, es la razón por la que está abierto para un ataque MITM. Por lo tanto, para entender el ataque, se requiere una comprensión básica de este protocolo.

ARP significa "protocolo de resolución de direcciones" (Address Resolution protocol), que ayuda a un equipo de red a hacer una traducción de la dirección IP (capa 3) a la dirección MAC (capa 2). Es necesario para que los datos pasen de la capa de red del modelo OSI (capa 3) a la capa de enlace de datos (capa 2).

Supongamos que la Máquina A necesita transferir datos a la Máquina B. Viendo de cerca los niveles inferiores del modelo OSI, necesitaría pasar a través de la capa de Red, la capa de Enlace de Datos y la capa Física (capa 1). Para que la Máquina A pueda comunicarse con la Máquina B, ¿la Máquina A necesitaría saber la dirección IP de la Máquina B? Información que se conoce en la capa de red.

La capa de enlace de datos se comunica mediante direcciones MAC. Por lo tanto, la conversión debe realizarse desde la dirección IP a la dirección MAC de la máquina B (y viceversa en la máquina receptora). Esto se ilustra en la imagen de a continuación:

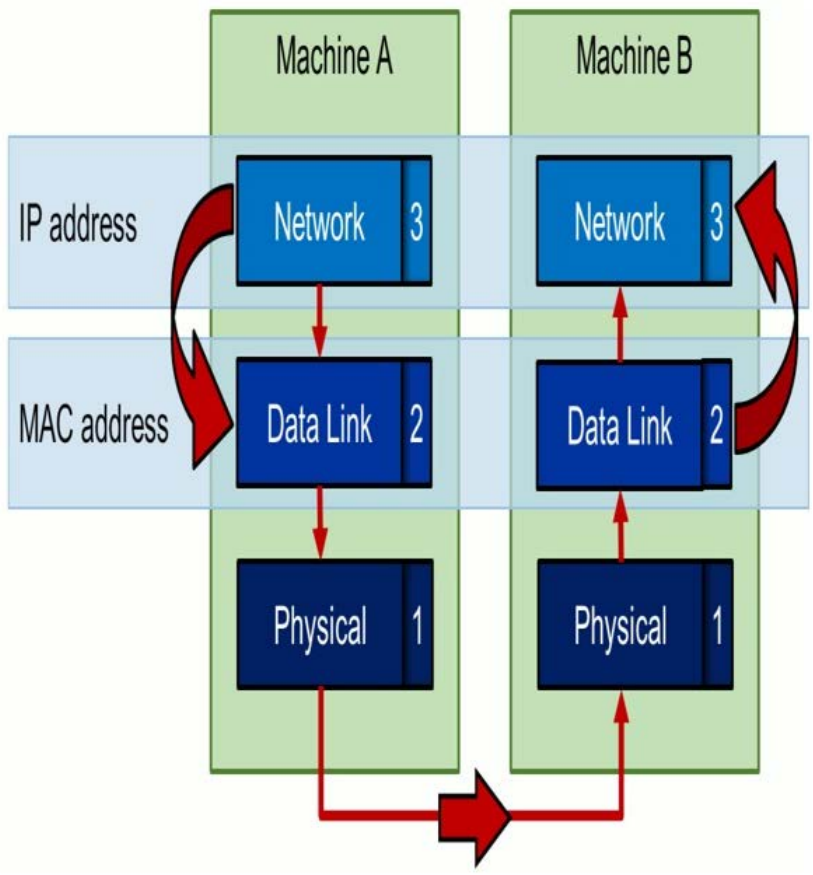


Figura 2.20- capas 1-3 del modelo OSI (fuente)

La conversión de, o mejor dicho la resolución de, la dirección IP en dirección MAC (y viceversa) es donde entra en juego el protocolo ARP. Ambas máquinas tendrán una tabla ARP donde se almacenan las direcciones IP y MAC correspondientes de todas las máquinas conocidas.

Entonces, ¿cómo obtiene la máquina A la dirección MAC correspondiente a la dirección IP de la máquina B?. La máquina A pedirá que se

responda desde el equipo con la IP buscada con la dirección MAC correspondiente.

Una simplificación del protocolo ARP se muestra en la siguiente animación:

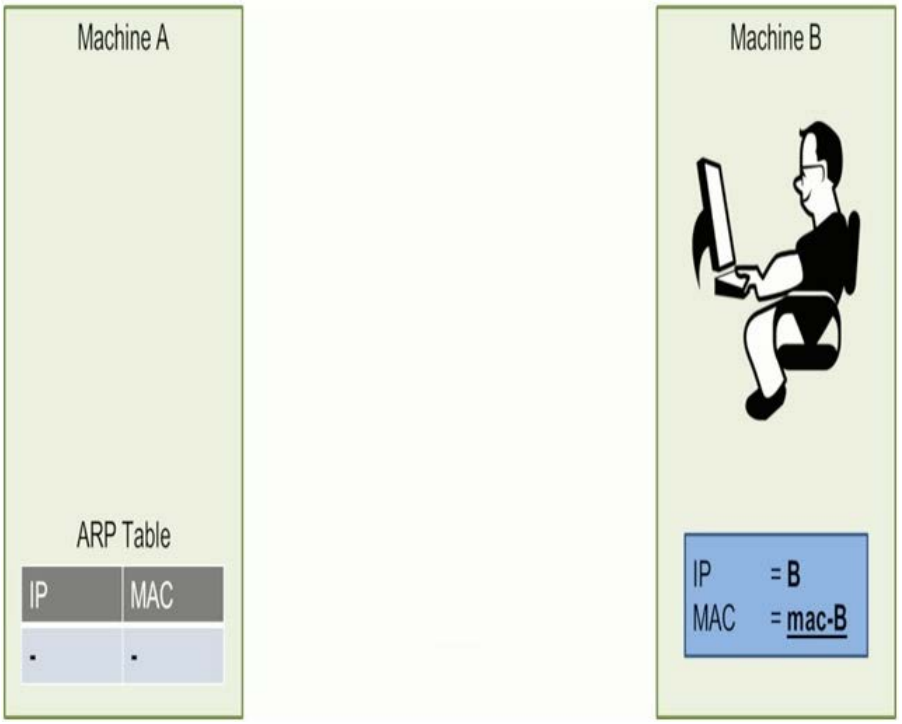


Figura 2.21- protocolo ARP (fuente)

Existen tres pasos:

1. En el primer paso del protocolo ARP, la Máquina A envía una **solicitud ARP**. Esta es una transmisión a la red con la pregunta «¿Quién tiene la dirección MAC para la dirección IP de la Máquina B?»
2. La Máquina B tiene este conocimiento y envía una **respuesta ARP** que dice "MAC-B es la dirección MAC de la Máquina B".
3. La máquina A recibe la respuesta ARP y escribe (o actualiza) la entrada en su **tabla ARP**.

El último paso es exactamente dónde se encuentra el problema con este protocolo. Sin embargo, antes de sumergirnos en sus problemas, echaremos un vistazo a los paquetes ARP que se están transmitiendo a través de la red.

La siguiente imagen muestra una parte de una captura de red realizada con un analizador de tráfico de red Wireshark.

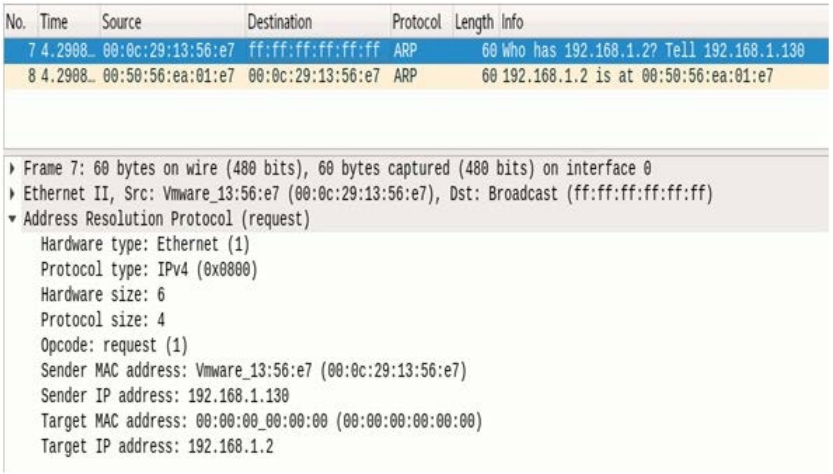


Figura 2.22- captura de tráfico ARP (fuente)

Obviamente podemos observar dos paquetes con los números 7 y 8.

- El primer paquete (7) contiene la **petición ARP** de un ordenador con dirección MAC de origen 00:0c:29:13:56:e7 y con dirección MAC de destino ff:ff:ff:ff:ff:ff:ff:ff, lo que significa un mensaje de difusión (dirigido a todos los equipos de la red). Entonces, la lógica es "¿Quién tiene 192.168.1.2? Responda al emisor de IP 192.168.1.130".
- El segundo paquete (8) es la **respuesta ARP** de un ordenador con dirección MAC 00:50:56:ea:01:e7 y con dirección MAC de destino la del origen del paquete 7. Wireshark sabe que " el IP 192.168.1.2 tiene la dirección MAC 00:50:56:ea:01:e7".

El hecho de que la Máquina A actualice su tabla ARP con la información de una respuesta ARP **sin ninguna duda** sobre la validez de esta información, abre la puerta a la **suplantación** de ARP (también conocida como **envenenamiento ARP**).

Un atacante puede enviar una respuesta ARP falsa, sin ninguna solicitud previa, que contenga su propia dirección MAC y la dirección IP de otro equipo. La máquina a la que se dirigió la respuesta actualizará su tabla ARP sin ninguna otra comprobación.

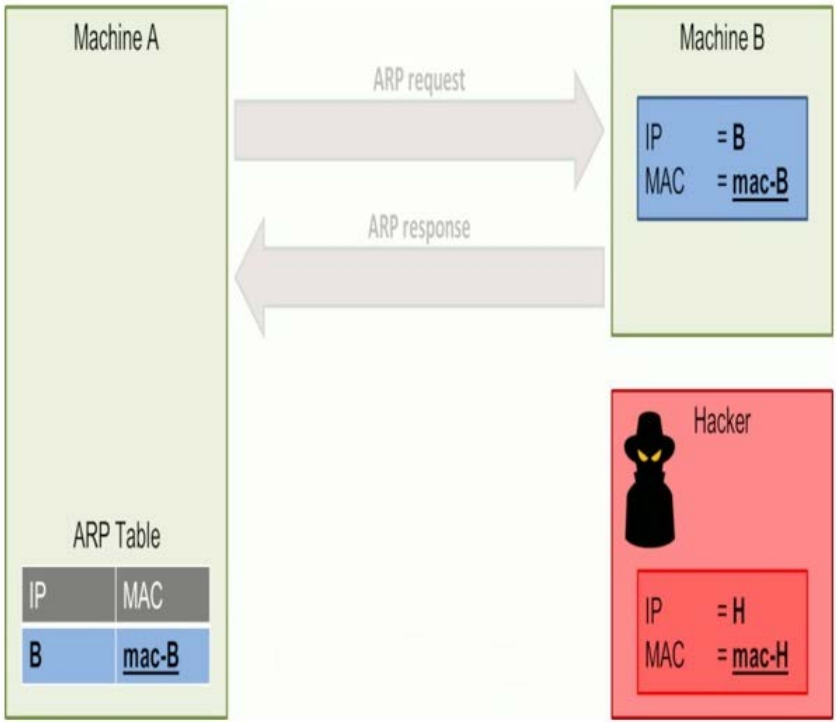


Figura 2.23- suplantación ARP (fuente)

La imagen de arriba muestra el mismo escenario en el que se produce un ataque con suplantación ARP. Un hacker se ha unido a las máquinas A y B de la red. El hacker ha hecho su trabajo en las fases de reconocimiento y escaneo, sabe que las máquinas A y B existen en la red y qué direcciones IP tienen.

En este ejemplo, el propio hacker tiene la dirección IP-H y dirección MAC-H. Envía su respuesta ARP maliciosa dirigida a la Máquina A con el mensaje "mac-H es la dirección MAC de la dirección IP B". La máquina A actualiza su tabla ARP y la dirección IP B está ahora vinculada a la dirección MAC H.

De ahora en adelante, cada vez que la Máquina A quiera enviar un mensaje a la Máquina B, traducirá la dirección IP de la Máquina B a la dirección MAC H y será enviada al hacker en lugar de a la Máquina B. Este es un caso del ataque **Man-in-the-middle.**

Supongamos que tenemos el siguiente escenario:

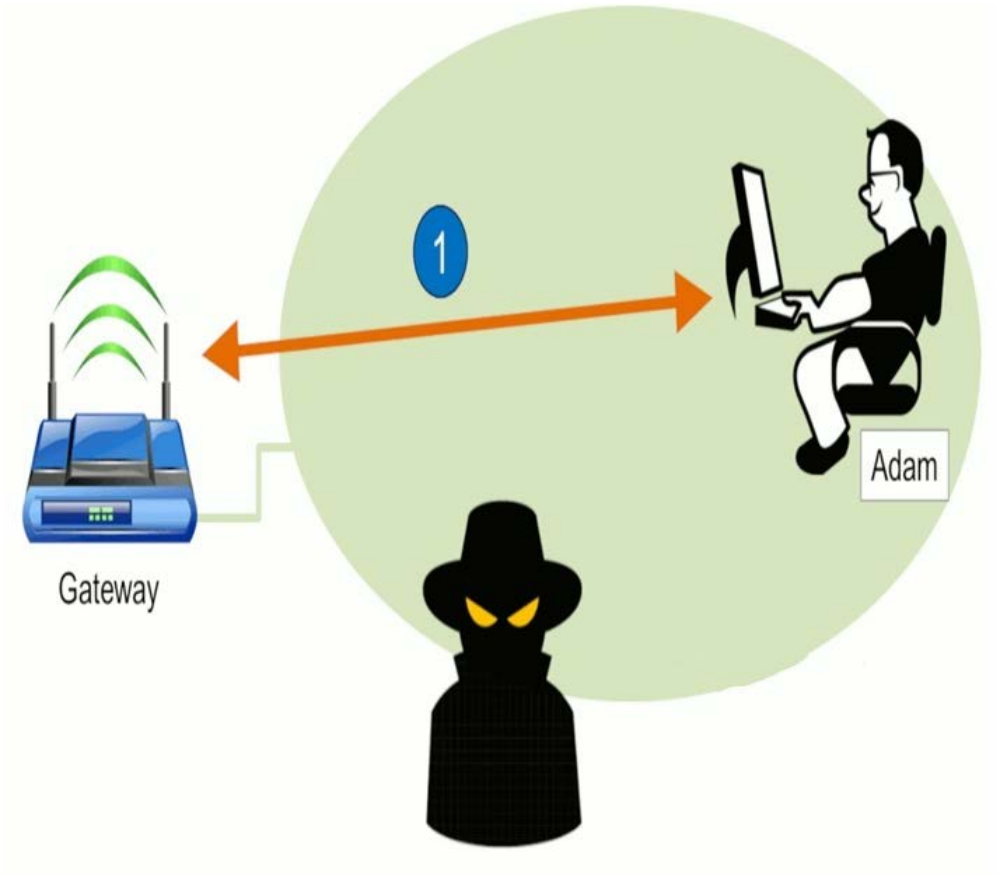


Figura 2.24- escenario suplantación ARP (fuente)

Tenemos un Gateway , un hacker y Adam.

1. En el primer paso Adam se conectó en la red. En esta progresión, el atacante hará un escaneo en la red para descubrir quién más está disponible y qué direcciones IP y MAC tiene.
2. Luego, el hacker envía una respuesta ARP maliciosa a ambos (Gateway y Adam). Básicamente, el hacker le dice al Gateway que él es Adam y simultáneamente le dice a Adam que él es el Gateway.
3. Tanto Gateway como Adam actualizarán sus tablas ARP con su nueva información. A partir de entonces, estos nodos comenzarán a enviar sus datos al hacker en lugar de uno al otro. ¡Simulación del ARP completada!

El atacante deberá tomar algunas medidas antes de poder comenzar a interceptar los datos correctamente.

En el escenario del subcapítulo anterior donde el pirata informático se encuentra entre Gateway y Adam, el hacker podría ver todo el tráfico de ambas partes. Si Adam navega a un sitio web, el hacker puede ver todos los datos enviados y recibidos de los sitios web con los que se está contactando.

¿Qué hay del **HTTPS**? Eso es HTTP sobre TLS (o HTTP sobre SSL) Significaría que todos los datos que pasan a través de la línea estarían **encriptados**, Es cierto, y el descifrado en tiempo real aún no es remotamente factible. Por lo tanto, el hacker no sería capaz de ver el contenido cifrado del tráfico HTTPS.

Para evitar el cifrado el hacker podría **obligar a la víctima a comunicarse a través de HTTP,** que es texto sin cifrar, en lugar de HTTPS.

Antes de explicar cómo se puede hacer esto, echemos un vistazo a cómo se configura una sesión HTTPS cuando navega a www.google.com (por ejemplo):

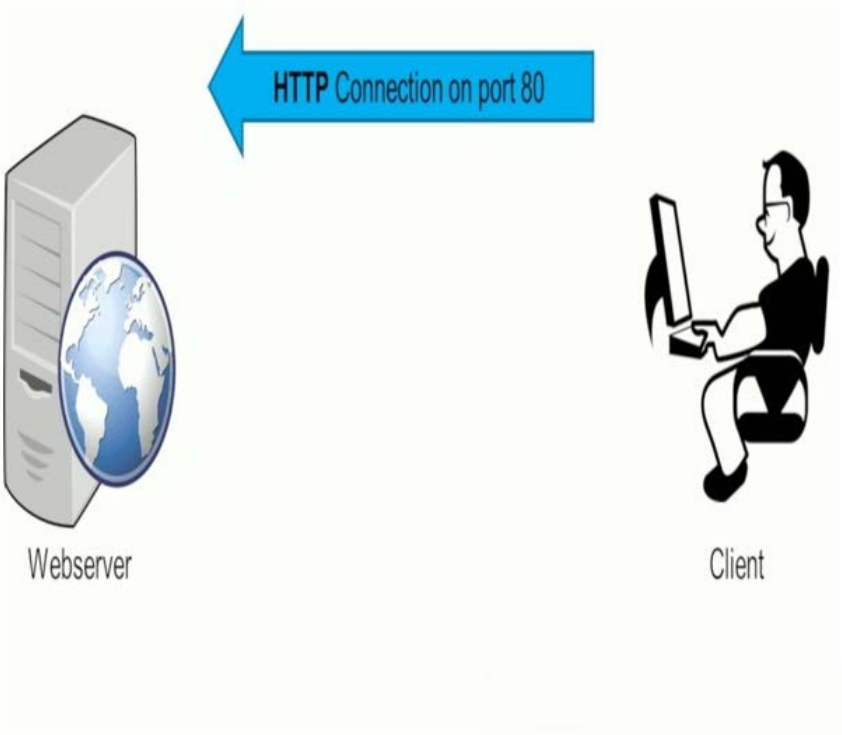


Figura 2.25- sesión HTTPS (fuente)

Escribir www.google.com en la barra de direcciones de un navegador web hará que el navegador realice una conexión HTTP (en el puerto 80) a www.google.com.Dado que google.com sólo permite conexiones HTTPS, el sitio solicitará al usuario que realice una conexión HTTPS en su lugar y, a continuación, el cliente que utilice HTTPS en el puerto 443 volverá a conectarse. En el último paso google envía el certificado.

Imagina el escenario en el que un hacker se encuentra en algún punto entre la comunicación del servidor web y el cliente. El hacker podrá leer el contenido del tráfico web hasta el momento en que el cliente configure la conexión HTTPS. Después de esto, todos los datos serán encriptados y el hacker no podrá leerlos. Anteriormente hemos dicho que se podría evitar forzando al cliente a seguir comunicándose a través de HTTP. Utilizaremos SSLStrip para conseguirlo.

SSLStrip, creado por Moxie Marlinspike, secuestrará de forma transparente el tráfico HTTP en una red, vigilará los enlaces HTTPS y los convertirá en enlaces HTTP similares.

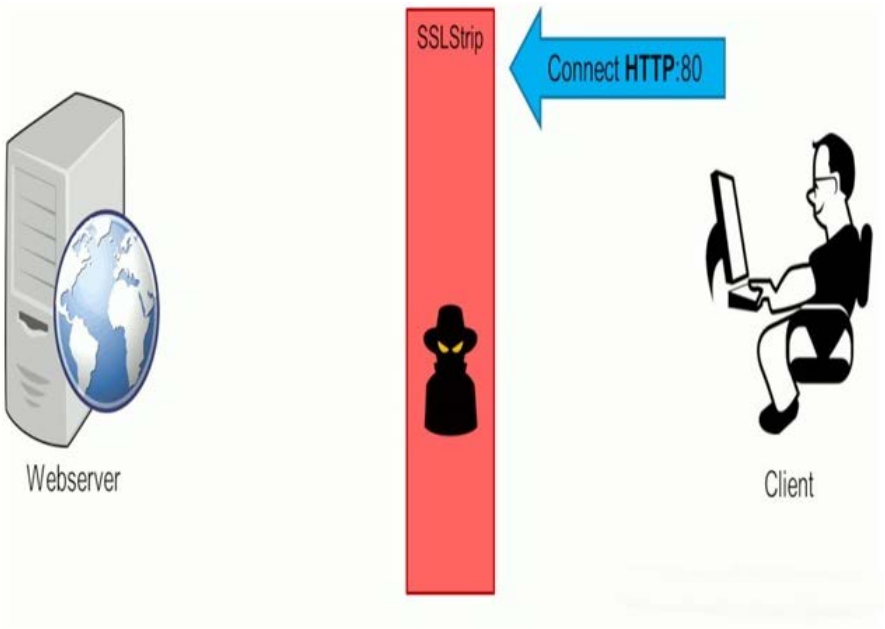


Figura 2.26: SSLStrip (fuente)

Como antes, el cliente escribe www.google.com en el navegador web, que intentará establecer una conexión HTTP con el sitio web. Ahora con SSLStrip en el centro, esta conexión se reenvía al destino deseado. Sin embargo, en lugar de que toda proceso de HTTPS se realice en el equipo del cliente, SSLStrip se encarga de ello en el equipo del hacker. Una vez establecida la conexión HTTPS entre el cliente y el hacker, SSLStrip devolverá un HTTP-OK al cliente. El navegador del cliente piensa que esto es aceptable ya que nunca vio la redirección HTTPS y continuará comunicándose a través de HTTP; un formato que el hacker puede leer sin esfuerzo.

HTTP con seguridad estricta en el transporte

Al tener habilitada la seguridad de transporte estricto HTTP (**HSTS**) , se informará al navegador para que siempre se comunique utilizando HTTPS. Esto se realiza a través de una **cabecera de respuesta HSTS** especial. En pocas palabras, el navegador mantiene una lista de sitios web de los que ha recibido este encabezado, conociendo así qué sitios son más seguros. Para estos sitios web, el navegador hará inmediatamente una conexión HTTPS independientemente de cómo el usuario haya intentado conectar. Esto evitará que los usuarios realicen la conexión HTTP en primer lugar, evitando que SSLStrip realice este truco.

Puede ocurrir que la primera visita de un cliente a un sitio web se realice a través de HTTP y un atacante puede eliminar el encabezado HSTS de la respuesta. Esta es la razón por la que la mayoría de los navegadores modernos tienen una lista precargada de sitios HSTS.

Un **ataque de diccionario** es un ataque que intenta determinar una contraseña probando palabras de una lista predefinida, o diccionario, de contraseñas probables.

El ataque de diccionario es el ataque de descifrado de contraseñas más simple y rápido. Utiliza un archivo que contiene palabras, frases o contraseñas comunes que puedan haber sido utilizadas por alguien como contraseña. Los hackers tienen acceso a bases de datos que tienen 100.000 (o más) contraseñas principales o pueden crear y encontrar archivos más grandes. El ataque hace hash (un proceso que sirve para cifrar datos) a estas contraseñas y compara con el hash de la contraseña cifrada que se desea descifrar. Este es un método más rápido que otros.

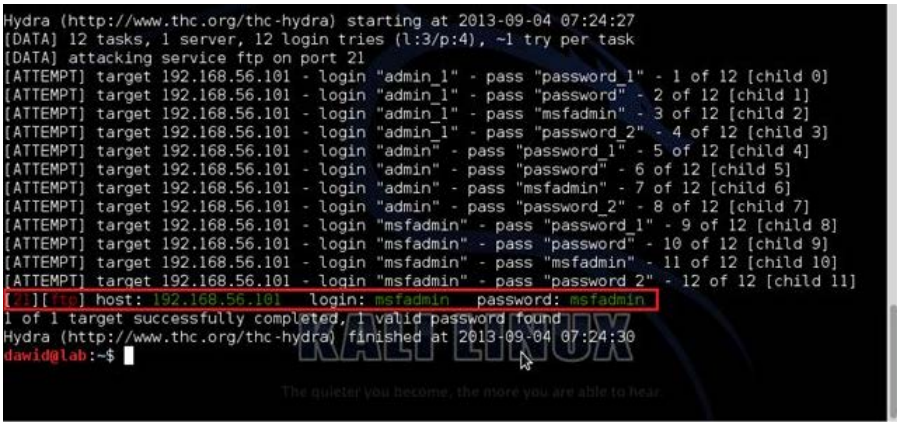


Figura 2.27: ejemplo de ataque de diccionario

Phishing

El phishing es un ejemplo de **ingeniería social** utilizado para obtener información confidencial del usuario (datos de identificación personal), generalmente en forma de nombres de usuario, contraseñas, números de tarjetas de crédito, información de cuentas bancarias u otros datos importantes con el fin de utilizar o vender la información robada, que se utilizará para engañar a los sistemas. Los intentos de phishing suelen comenzar con un **correo electrónico** que intenta obtener información confidencial a través de la interacción del usuario, como hacer clic en un enlace malicioso o descargar un archivo adjunto infectado.

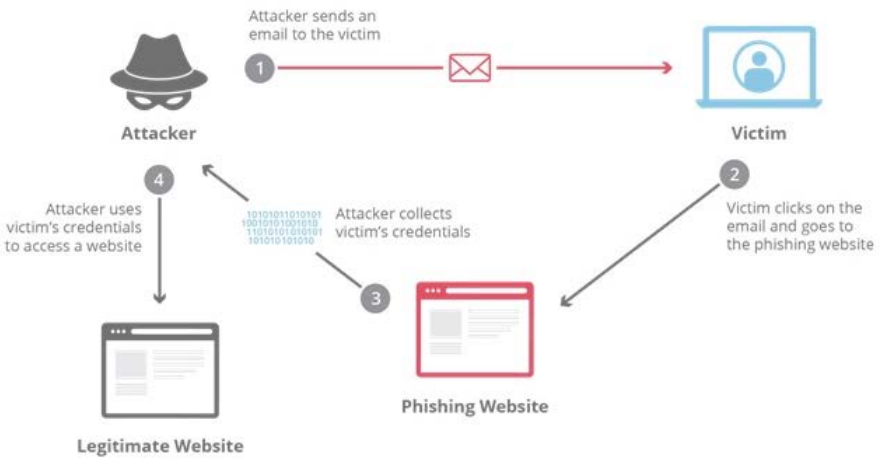


Figura 2.28- ataque por phishing (fuente)

Para contrarrestar los ataques de phishing, las organizaciones y las empresas deben proporcionar a los empleados formas de identificar estos ataques y contrarrestar estos ataques. Los ataques de phishing más comunes son los correos electrónicos, los archivos adjuntos de virus y los enlaces de virus que conducen a virus y dejan caer el ancho de banda de la conexión. Los atacantes están constantemente actualizados sobre nuevos ataques, por lo que es necesario proporcionar el conocimiento de los empleados para evitar tales ataques.

La **inyección SQL (SQLi)** es un tipo de ataque de inyección que permite ejecutar sentencias SQL (un lnguaje de gestión de bases de datos) maliciosas. Estas sentencias controlan un **servidor de base de datos** detrás de una aplicación web. También pueden utilizar las vulnerabilidades de SQL Injection para añadir, modificar y eliminar registros en la base de datos. Los ataques de inyección SQL son una de las vulnerabilidades de aplicaciones web más antiguas, prevalentes y peligrosas. También pueden usar la inyección SQL para **agregar, modificar y eliminar registros en la base de datos.**

Una vulnerabilidad de inyección SQL puede afectar a cualquier sitio web o aplicación web que use una base de datos SQL como **MySQL, Oracle, SQL Server** u otros. Los delincuentes pueden usarlo para obtener acceso no autorizado a sus datos confidenciales: información del cliente, datos personales, secretos comerciales, propiedad intelectual y más.

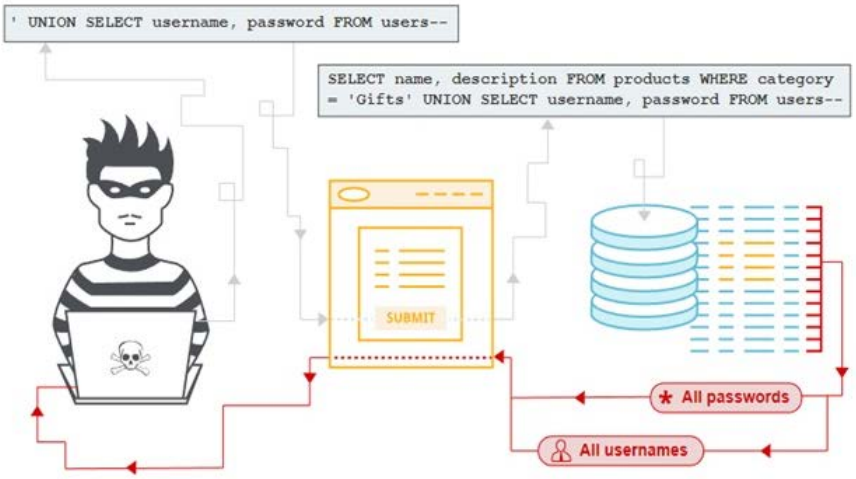


Figura 2.29 SQL injection (fuente)

Algunas características centrales del lenguaje SQL se implementan de la misma manera en plataformas de bases de datos comunes, y muchas formas de detectar y explotar vulnerabilidades de inyección SQL funcionan de manera idéntica en diferentes tipos de bases de datos.
Sin embargo, también hay muchas diferencias entre las bases de datos comunes. Esto significa que algunas técnicas para detectar y explotar la inyección SQL funcionan de manera diferente en diferentes plataformas

¿Qué pueden hacer los ataques de inyección SQL?

Hay muchas cosas que un atacante puede hacer cuando explota una inyección SQL en un sitio web vulnerable. Al aprovechar una vulnerabilidad de inyección SQL, dadas las circunstancias correctas, un atacante puede hacer lo siguiente:

- Omite los mecanismos de autorización de una aplicación web y extrae información confidencial
- Controla fácilmente el comportamiento de la aplicación que se basa en los datos de la base de datos.
- Inyecta más código malicioso para que se ejecute cuando los usuarios accedan a la aplicación
- Agrega, modifica y elimina datos, corrompiendo la base de datos y haciendo que la aplicación sea inservible
- Obtiene los datos de autenticación de un usuario registrado en un sitio web y usa los datos en ataques a otros sitios

Figura 2.30- SQL injection ataque (fuente)

Las siguientes acciones pueden resultar de la inyección SQL:

- Hackear la cuenta de otra persona.
- Robar y copiar datos confidenciales del sitio web o del sistema.
- Cambio de datos confidenciales del sistema.
- Eliminar los datos confidenciales del sistema.
- El usuario puede iniciar sesión en la aplicación como otro usuario, incluso como administrador.
- El usuario puede ver información privada que pertenece a otros usuarios, p. ej. detalles de los perfiles de otros usuarios, sus detalles de transacción, etc.
- El usuario podría cambiar la información de configuración de la aplicación y los datos de los otros usuarios.
- El usuario podría modificar la estructura de la base de datos; incluso eliminar tablas en la base de datos de la aplicación.
- El usuario podría tomar el control del servidor de la base de datos y ejecutar comandos a voluntad.

Figura 2.31 SQL prevención (fuente)

Las siguientes medidas pueden ayudar a prevenir ataques de SQL Injection:

- Descubre las vulnerabilidades de inyección SQL con las diversas técnicas disponibles para este ataque.
- Repara vulnerabilidades de inyección SQL mediante consultas parametrizadas. La base de datos siempre los tratará como datos en lugar de como parte de un comando SQL.
- Remedia las vulnerabilidades de inyección de SQL mediante el uso de caracteres de escape para que se ignoren los caracteres especiales.
- Mitiga el impacto de las vulnerabilidades de inyección de SQL al imponer el menor privilegio en la base de datos, de esta manera cada componente de software de una aplicación puede acceder y afectar solo a los recursos que necesita.
- Usa un firewall de aplicaciones web (WAF) para aplicaciones web que acceden a bases de datos. Esto puede ayudar a identificar los intentos de inyección SQL y, a veces, ayudar a evitar que los intentos de inyección SQL lleguen a la aplicación también.

Modbus es un protocolo de comunicaciones industriales muy extendido con una especificación disponible públicamente, basado en una arquitectura maestro/esclavo. Actualmente no existen restricciones extensivas sobre el tiempo en el que los bloques de datos se pueden administrar en un sistema industrial; implementar esto sería sencillo y requeriría poco desarrollo. Actualmente hay dos implementaciones: Serie Modbus (con modos de operación: ASCII y RTU) y Modbus/TCP.

Deficiencias del protocolo

En Modbus, el modo de operación de los elementos esclavos consiste en responder siempre a los paquetes que reciben. La herramienta **Modscan** aprovecha esta característica, dirigiendo las peticiones TCP (por lo tanto, sólo disponibles para implementaciones Modbus/TCP) al puerto estándar Modbus, 502, y descubriendo así los esclavos conectados a la red, como puede verse en la siguiente imagen.

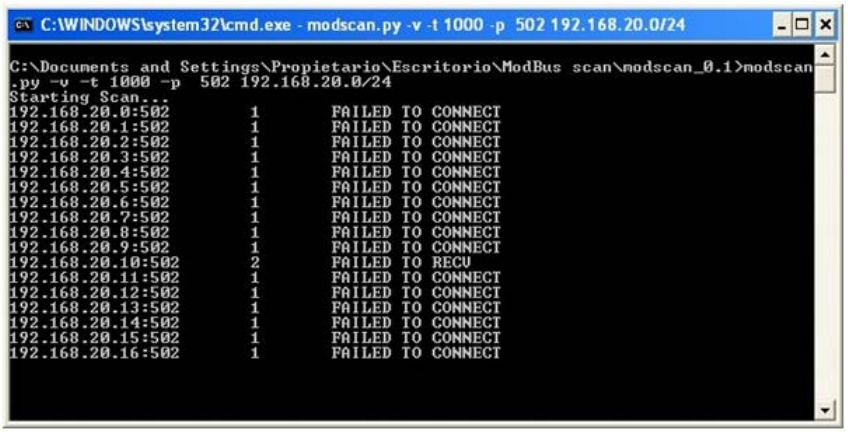


Figura 2.32- descubrimiento de IP de esclavos Modbus con Modscan

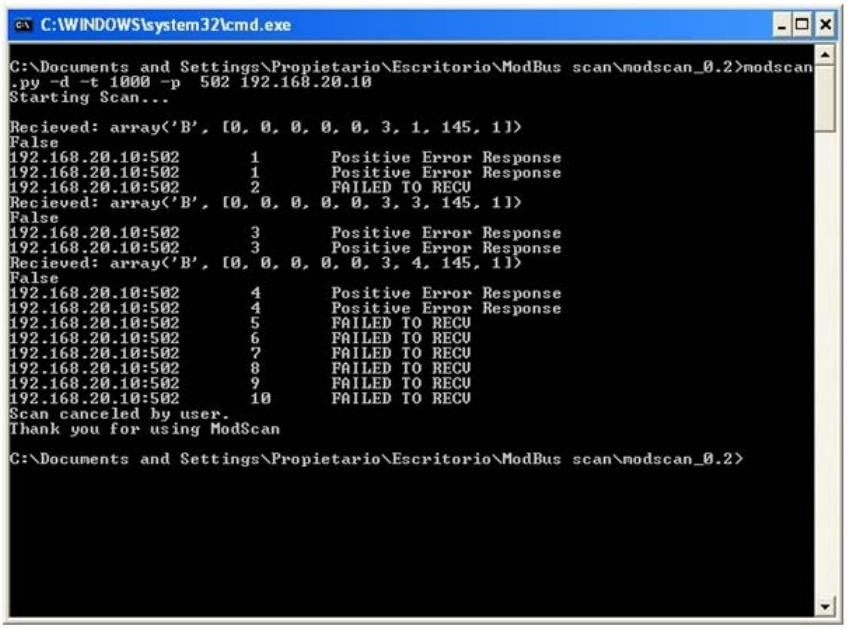


Figura 2.33- Ajuste de la búsqueda de esclavos y la identificación de los ID de Modbus

Una vez identificados los esclavos, es fácil capturar tráfico con cualquier herramienta diseñada para capturar tráfico de red. El análisis de captura muestra que las comunicaciones no están cifradas, lo que significa que es posible identificar y analizar directamente la información dada y el modo de operación. La siguiente imagen muestra una captura de tráfico con un análisis del flujo.

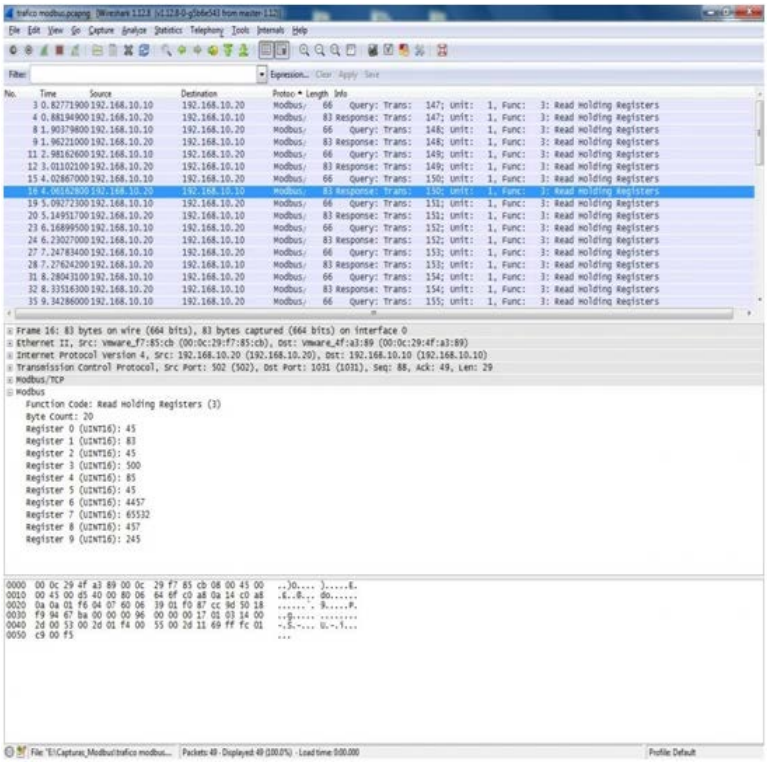


Figura 2.34- Analisis de tráfico Modbus

Las debilidades de Modbus son intrínsecas al protocolo; como no se prevén cambios en la especificación, es por lo tanto necesario introducir elementos de seguridad adicionales para ayudar a mitigar sus fallos de seguridad.

La primera medida a considerar es la adopción de una estrategia de **encriptación** para las comunicaciones. El cifrado de las comunicaciones impedirá que la información sea analizada en tránsito, en caso de que el tráfico sea capturado.

Los dispositivos que implementan este protocolo generalmente no son capaces de encriptar las comunicaciones, por lo que deben utilizar herramientas externas, que pueden encriptar y descifrar la información que circula por la red.

Aunque esta solución es efectiva, en la práctica es difícil, ya que el uso de herramientas de encriptación trae problemas de gestión y distribución de contraseñas; además, la encriptación y desencriptación de la información debe ser permitida por todos los equipos industriales a los que se va a utilizar el protocolo Modbus.

Por lo tanto, para controlar el tráfico entre los esclavos y el maestro, los **cortafuegos** son la solución más popular. Los cortafuegos convencionales permiten el control del tráfico a nivel de red, lo que significa que las direcciones del maestro y de los esclavos se pueden establecer como autoridades, evitando así ciertos tipos de ataques de suplantación de identidad. Los cortafuegos de aplicación permiten la inspección de la red, incluida la sección de datos que genera los datos.

Modbusfw (Modbus Firewall) es un módulo para las tablas de direccionamiento IP que filtra el tráfico a nivel de capa de aplicación para asegurar redes utilizando el protocolo Modbus/TCP. Permite filtrar los paquetes de tráfico Modbus, identificándolos mediante el ID del esclavo, el código de función, el tamaño del paquete o el número de referencia. De esta manera, es posible evitar escribir en equipos que sólo deben recibir lecturas o viceversa, y filtrar el uso de códigos de función de diagnóstico (como los que se utilizan en determinadas herramientas de exploración de redes Modbus), etc.

Los cortafuegos permiten el control del tráfico en diferentes redes, pero es útil utilizarlos junto con los **sistemas de detección y prevención de intrusiones (IDS/IPS)** para detectar otros tipos de acciones.

Para el Snort IDS, y para todos los que se basan en él, hay una extensión para interpretar el protocolo Modbus. Es posible definir normas de control de tráfico para Modbus basándose en valores que deben contener diferentes bytes de datos en un flujo Modbus/TCP.

El uso de sistemas IDS/IPS para supervisar el protocolo Modbus permite reconocer el uso de funciones no permitidas, así como reconocer cuándo se envían paquetes de datos desde direcciones IP no controladas, ayudando, por ejemplo, a detectar posibles ataques DoS.

2.4 Legislación sobre Comercio Electrónico y Servicios Digitales en la Sociedad de la Información

Description

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce).

- In order to ensure legal certainty and consumer confidence, this Directive must lay down a clear and general framework to cover certain legal aspects of electronic commerce in the internal market.
- The free movement of information society services can in many cases be a specific reflection in Community law of a more general principle, namely freedom of expression as enshrined in Article 10(1) of the Convention for the Protection of Human Rights and Fundamental Freedoms, which has been ratified by all the Member States; for this reason, directives covering the supply of information society services must ensure that this activity may be engaged in freely in the light of that Article, subject only to the restrictions laid down in paragraph 2 of that Article and in Article 46(1) of the Treaty; this Directive is not intended to affect national fundamental rules and principles relating to freedom of expression.

The official and complete law:

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=EN

Table of contents

Ley de Servicios de la Sociedad de la Información y Comercio Electrónico es la Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico).

Estos son algunos párrafos de dicha ley:

- Para garantizar la seguridad jurídica y la seguridad de los consumidores, la presente Directiva debe establecer un marco claro y general que abarque determinados aspectos jurídicos del comercio electrónico en el mercado interior.
- La libre circulación de los servicios de la sociedad de la información puede ser en muchos casos un reflejo específico en el Derecho comunitario de un principio más general, a saber, la libertad de expresión consagrada en el apartado 1 del artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, que ha sido ratificado por todos los Estados miembros. Por este motivo, las directivas relativas a la prestación de servicios de la sociedad de la información deben garantizar que esta actividad pueda ejercerse libremente a la luz de dicho artículo, sin perjuicio de las restricciones previstas en el apartado 2 de dicho artículo y en el apartado 1 del artículo 46 del Tratado; la presente Directiva no se dirige a las normas y principios fundamentales nacionales relativos a la libertad de expresión.

Servicios de la sociedad de la información: Objeto de la Ley

Esta ley establece los requisitos para los proveedores de servicios de la sociedad de la información, la organización de la supervisión y la responsabilidad por la violación de esta ley. Más información sobre la ley:

http://unpan1.un.org/intradoc/groups/public/documents/un-kmb/unpan041622~1.htm

Comercio electrónico: normas estándar de la UE

La Directiva sobre comercio electrónico (Directiva 2000/31/CE sobre comercio electrónico), adoptada en 2000, establece un marco para el mercado interior del comercio electrónico, que proporciona seguridad jurídica tanto a las empresas como a los consumidores. Más información en:

https://eur-lex.europa.eu/legal-content/en/TXT/?uri=LEGISSUM%3Al24204

Objetivo de la Directiva sobre comercio electrónico

La Directiva se introdujo para aclarar y armonizar las normas del comercio en línea en toda Europa. El objetivo de la Directiva es, en última instancia, fomentar un mayor uso del comercio electrónico eliminando las barreras que existen en toda Europa y reforzar la confianza de los consumidores aclarando los derechos y obligaciones tanto de los consumidores como de las empresas.

Ámbito de aplicación del Reglamento sobre comercio electrónico (Directiva CE) de 2002

El Reglamento de Comercio Electrónico (Directiva CE) de 2002, que entró en vigor el 21 de agosto de 2002, incorpora los principales requisitos de la Directiva de Comercio Electrónico a la legislación del Reino Unido.
Los Reglamentos se aplican a los «servicios de la sociedad de la información». «Se definen como todo servicio prestado normalmente a cambio de una remuneración a distancia, mediante equipos electrónicos para el tratamiento (incluida la compresión digital) y el almacenamiento de datos, a petición individual de un destinatario de un servicio».

Esto incluye la mayoría de los tipos de servicios en línea y de información, tales como:

- Publicidad de bienes o servicios en línea (es decir, a través de Internet, correo electrónico, televisión interactiva o teléfono móvil).
- Venta de bienes o servicios en Internet o por correo electrónico, independientemente de que los bienes o servicios se entreguen electrónicamente.
- Transmisión o almacenamiento de contenidos electrónicos o acceso a una red de comunicaciones

Se puede encontrar la ley completa en:

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031rom=EN

En las recomendaciones de la Unión Europea para la lucha contra los ciberataques se aplican las siguientes **directrices**:

- ENISA: «INDUSTRY 4.0 Ciberseguridad: desafios y recomendaciones. Mayo 2019»:

https://www.enisa.europa.eu/publications/industry- 4-0-cybersecurity-challenges-and-recommendations/at_download/fullReport

La apropiación de las propuestas de niveles significativos propuestas por ENISA tiene por objeto mejorar la ciberseguridad de la industria 4.0 en la Unión Europea y sentar las bases de los próximos trabajos pertinentes, así como servir de base para futuros desarrollos. En este breve documento, ENISA persigue una forma holística y extensa de abordar los problemas identificados con la ciberseguridad en la Industria 4.0, en la que las dificultades y propuestas se relacionan con una de las clases que la acompañan: Personas, procesos y tecnologías.

- Directrices y mejores prácticas de seguridad cibernética para servicios de emergencia. Junio de 2018:

https://eena.org/wp-content/uploads/2018/11/Cybersecurity- Guidelines-and-Best-Practices-for-Emergency-Services.pdf

Este documento de EENA (Asociación Europea de Números de Emergencia) espera expandir la atención entre las asociaciones de Seguridad Pública sobre los efectos identificados de las vulnerabilidades, riesgos y amenazas cibernéticas, y ofrece algunas sugerencias para mitigarlos. A los efectos del presente documento, se entenderá por ciberseguridad las tecnologías, procesos y prácticas destinados a proteger a los usuarios, redes, ordenadores, programas y datos de ataques, daños o accesos no autorizados.

- ISACA, «Auditoría sobre Ciberseguridad»

https://m.isaca.org/About-ISACA/advocacy/Documentos/CiberseguridadAuditoría_mis_Eng_1017.pdf

Esta guía se centra en tres partes: revisión de la gestión, evaluaciones de riesgos y auditorías de los controles de seguridad cibernética. También incluye cuestiones de seguridad primaria y control para la ciberseguridad, controles y amenazas para la ciberseguridad.

- Estudio de ENISA: «Buenas prácticas para la seguridad de Internet de las cosas en el contexto de la fabricación inteligente, noviembre de 2018»

https://www.enisa.europa.eu/Publicaciones/buenas prácticas para la seguridad de losiot/at_download/fullReport

Este estudio de ENISA tiene por objeto abordar los retos de seguridad y privacidad relacionados con la evolución de los sistemas y servicios industriales precipitados por la introducción de las innovaciones de la IO. Los principales objetivos eran recopilar buenas prácticas para garantizar la seguridad de la IO en el contexto de Industria 4.0/Fabricación inteligente, al tiempo que se cartografiaban los retos, amenazas, riesgos y escenarios de ataques en materia de seguridad y privacidad.

- NIST Internal Report 8228 (Draft) «Consideraciones para gestionar los riesgos de privacidad y ciberseguridad de Internet de las cosas (IdC) en septiembrede 2019»

  https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8228-draft.pdf

El propósito de este documento es ayudar a las empresas a comprender y manipular mejor los peligros de la ciberseguridad y la privacidad asociados a los dispositivos de Internet de las Cosas (IO) durante sus ciclos de vida. Asimismo, el texto dice lo siguiente sobre la ciberseguridad y las consideraciones de riesgo para la privacidad, así como sobre los desafíos que plantean los dispositivos de IO en materia de ciberseguridad y mitigación de los riesgos para la privacidad.

- Departamento Digital, Cultura, Medios y Deporte «Código de prácticas para la seguridad de IdC del consumidor, Octubre de 2018»:

https://assets.publishing.service.gov.uk/government/uploads

/system/uploads/attachment_data/file/773867

/Código_de_práctica_para_la_seguridad_de_los_consumidores_Octubre_2018.pdf

El Código de prácticas del Gobierno para la seguridad de los fabricantes en la Internet de los objetos de consumo (IO), con orientaciones para los consumidores sobre los dispositivos inteligentes del hogar.

Inyección SQL

Existen herramientas automatizadas que puedes utilizar para comprobar si un sitio web es vulnerable a ataques de inyección SQL.

Estas herramientas incluyen:

- **SQLMap**
- **Havij**

Este link te llevará a una demo para practicar.

http://testphp.vulnweb.com/artists.php?artist=1

Lo primero que debemos hacer es poner una comilla simple al final del url

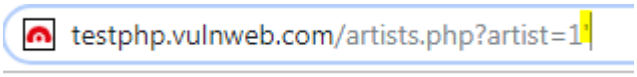


Figura 1- Comprobación de la Inyección SQL

y recibimos el error.

De este modo comprobamos que el sitio es vulnerable a los ataques de Inyección SQL.

El siguiente enlace es otra demo más detallada para entender mejor el ataque.

SQL demo

Ataque de diccionario

Un ataque de diccionario es un ataque rápido y simple mediante el uso de contraseñas creadas para acceder a una cuenta privada.

Los atacantes pueden crear sus propios diccionarios con contraseñas o descargar otros ya existentes.

Existen herramientas para crear una lista de contraseñas y tratar de acceder a la cuenta atacada. Kali-Linux es un conjunto de herramientas creado para probar el grado de ciberseguridad de un sistema, entre esas herramientas se encuentra Crunch, utilizada para crear un conjunto de posibles contraseñas.

Creando una lista de palabras con Crunch – Kali linux

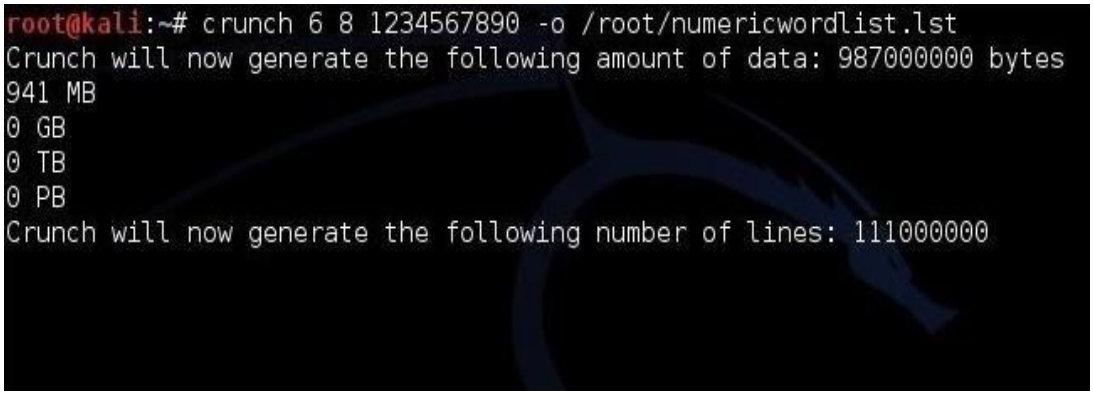


Figura 2- Creación de contraseñas con Crunch

Donde el primer número (6) es la longitud de la palabra más corta y el segundo (8) es la longitud de la palabra más larga. Los caracteres van de 0 a 9.

El comando que necesitamos para las minúsculas de la *a* a la *z* es el siguiente

crunch 6 8 abcdefghiklmnopqrstuvwxyz -o /root/loweralpha.lst

En las siguientes figuras se muestra un ejemplo de desciframiento del servicio ssh (puerto 22)

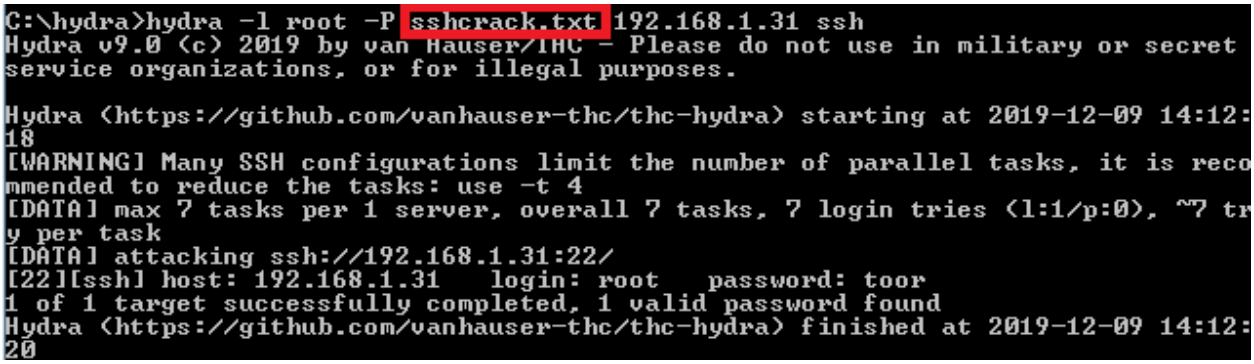


Figura 2- SSH descifrando desde Windows

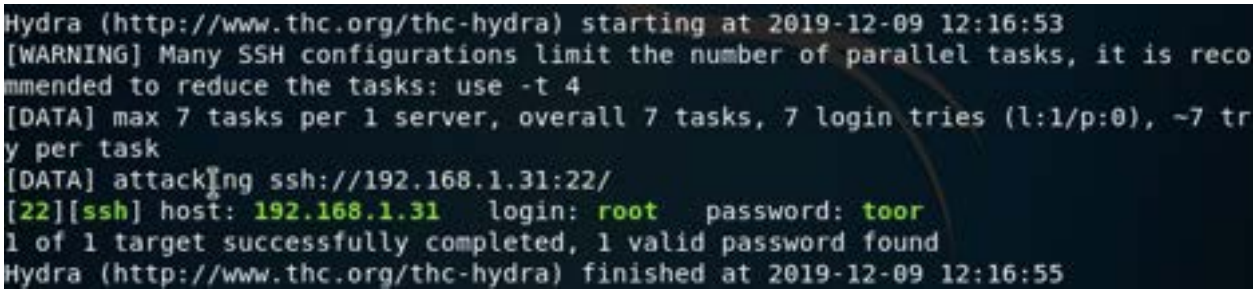


Figura 4- SSH descifrando desde Linux

Intenta hacer lo mismo utilizando una lista de palabras ya creada que se llama "rockyou"! (Rockyou link de descarga)

¡Recordatorios básicos sobre contraseñas!

1) Contraseñas sólidas
Nuestra contraseña debe contener al menos 12 caracteres (como mínimo), y ha de combinar letras, números y caracteres especiales. Algunas letras deben ser mayúsculas y otras minúsculas.

2) Contraseñas diferentes
Debes tener una contraseña única para las diferentes cuentas. Nunca utilices la misma contraseña para todas tus cuentas.

3) Contraseña caleidoscópica
Tu contraseña debe actualizarse, al menos, una vez cada tres meses. Nunca utilices de nuevo una contraseña antigua.

Ataque DOS

Ataque DOS: El ataque Denegación De Servicio (DoS por sus siglas en inglés) es un ataque que está preparado para dejar fuera de servicio una máquina o una red, hacienda que esta sea inaccesible para los usuarios.

hping3 es una herramienta de red capaz de enviar paquetes TCP/IP personalizados y reproducirlos en respuestas objetivo como hace el programa ping con las respuestas ICMP. hping3 controla la fragmentación, los paquetes arbitrarios de cuerpo y tamaño, y se puede utilizar para transferir archivos encapsulados por protocolos aceptados.

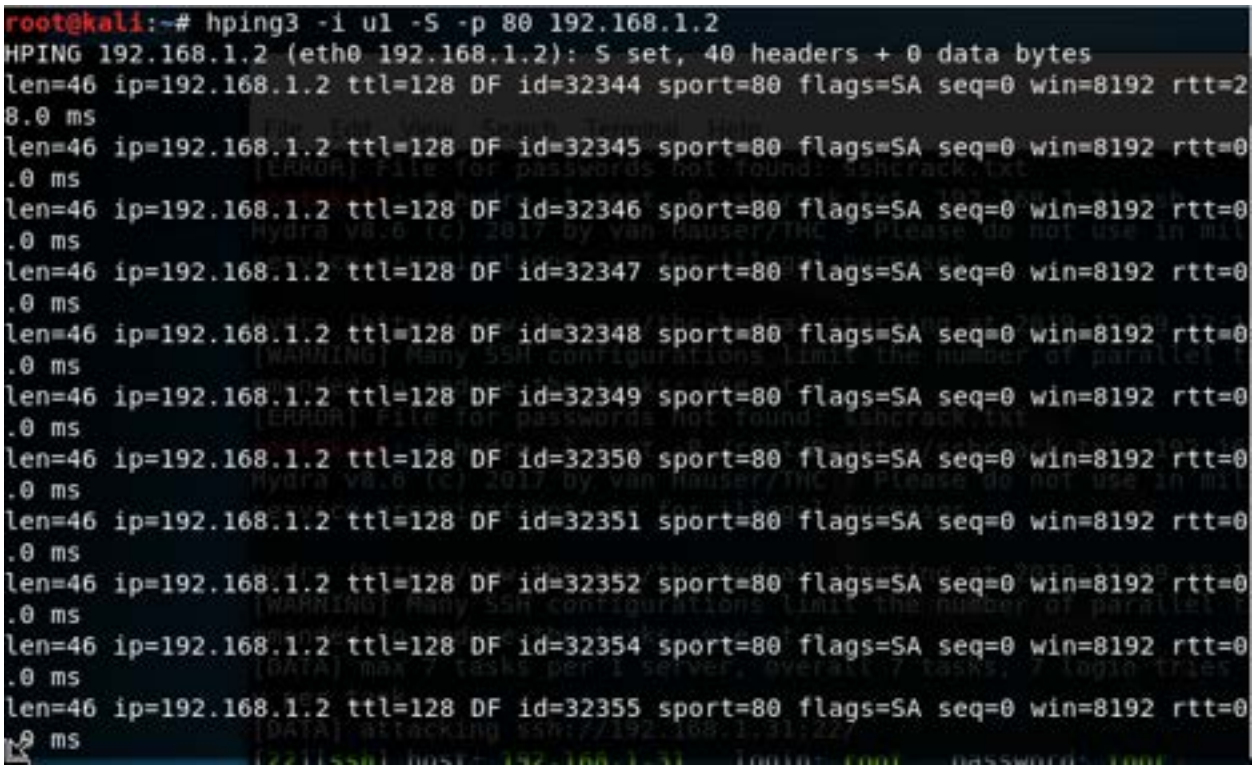


Figura 3- hping3 en acción

El comando utilizado es **hping3 –I u1 –S –p 80 192.168.1.2**

-i u1 indica que se envia un paquete cada 1 microsegundo.

-S indica que el paquete enviado es tipo Syn .

-p 80 indica que el ataque se hace contra el Puerto 80.

192.168.1.2 es la dirección IP del equipo atacado.

Con ese commando hemos atacado nuestra red local durante un tiempo limitado

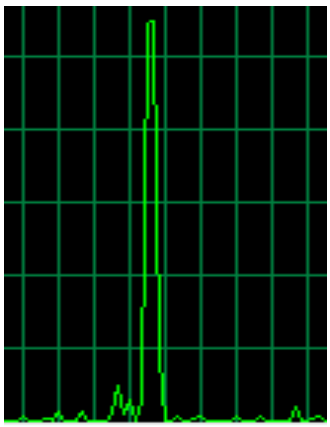


Figura 6- Practicando ataque de red después de 15-20 segundos

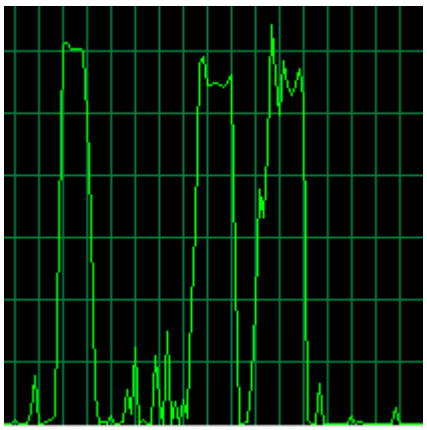


Figura 7- Después de 1-2 minutos

Como podemos comprobar, la actividad de red se ha incrementado de manera significante al producirse el ataque satisfactoriamente.

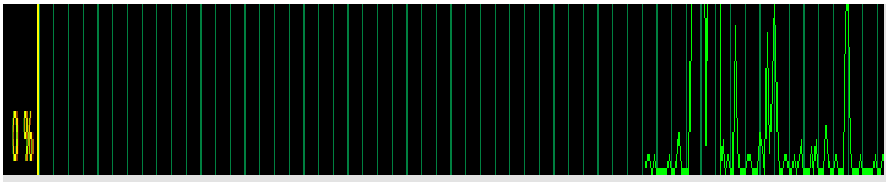
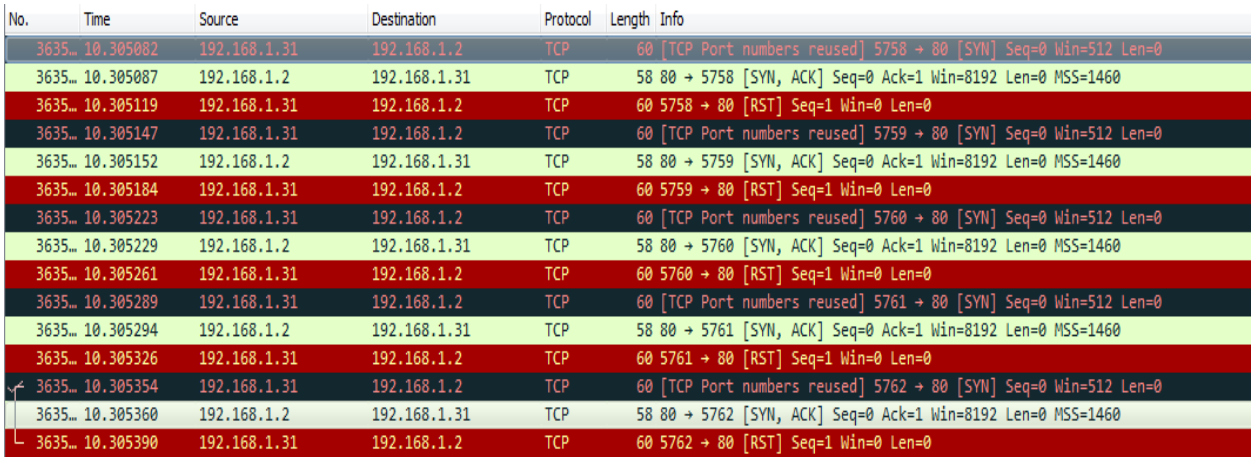


Figura 8- Flujo de red normal

Wireshark es un programa de monitorización de tráfico de red (este tipo de programas se conocen como **sniffer**), mediante su uso se puede ver claramente que nuestra máquina está enviando paquetes SYN (ataque DOS) continuamente a la máquina de destino.



No.	Time	Source	Destination	Protocol	Length	Info
3635…	10.305082	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5758 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305087	192.168.1.2	192.168.1.31	TCP	58	80 → 5758 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305119	192.168.1.31	192.168.1.2	TCP	60	5758 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305147	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5759 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305152	192.168.1.2	192.168.1.31	TCP	58	80 → 5759 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305184	192.168.1.31	192.168.1.2	TCP	60	5759 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305223	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5760 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305229	192.168.1.2	192.168.1.31	TCP	58	80 → 5760 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305261	192.168.1.31	192.168.1.2	TCP	60	5760 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305289	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5761 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305294	192.168.1.2	192.168.1.31	TCP	58	80 → 5761 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305326	192.168.1.31	192.168.1.2	TCP	60	5761 → 80 [RST] Seq=1 Win=0 Len=0
3635…	10.305354	192.168.1.31	192.168.1.2	TCP	60	[TCP Port numbers reused] 5762 → 80 [SYN] Seq=0 Win=512 Len=0
3635…	10.305360	192.168.1.2	192.168.1.31	TCP	58	80 → 5762 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
3635…	10.305390	192.168.1.31	192.168.1.2	TCP	60	5762 → 80 [RST] Seq=1 Win=0 Len=0

Figura 9- Wireshark ha capturado los paquetes del ataque

El siguiente enlace describe con detalle el funcionamiento de hping3.

[Funcionamiento de hping3]

Phishing por correo electrónico

En general, el *phishing* ocurre cuando alguien intenta robar tu información personal en línea de diferentes maneras. Normalmente se produce vía correo electrónico y el remitente no es quien dice ser.

Veamos un ejemplo real. El típico *phishing* por correo electrónico es parecido al siguiente

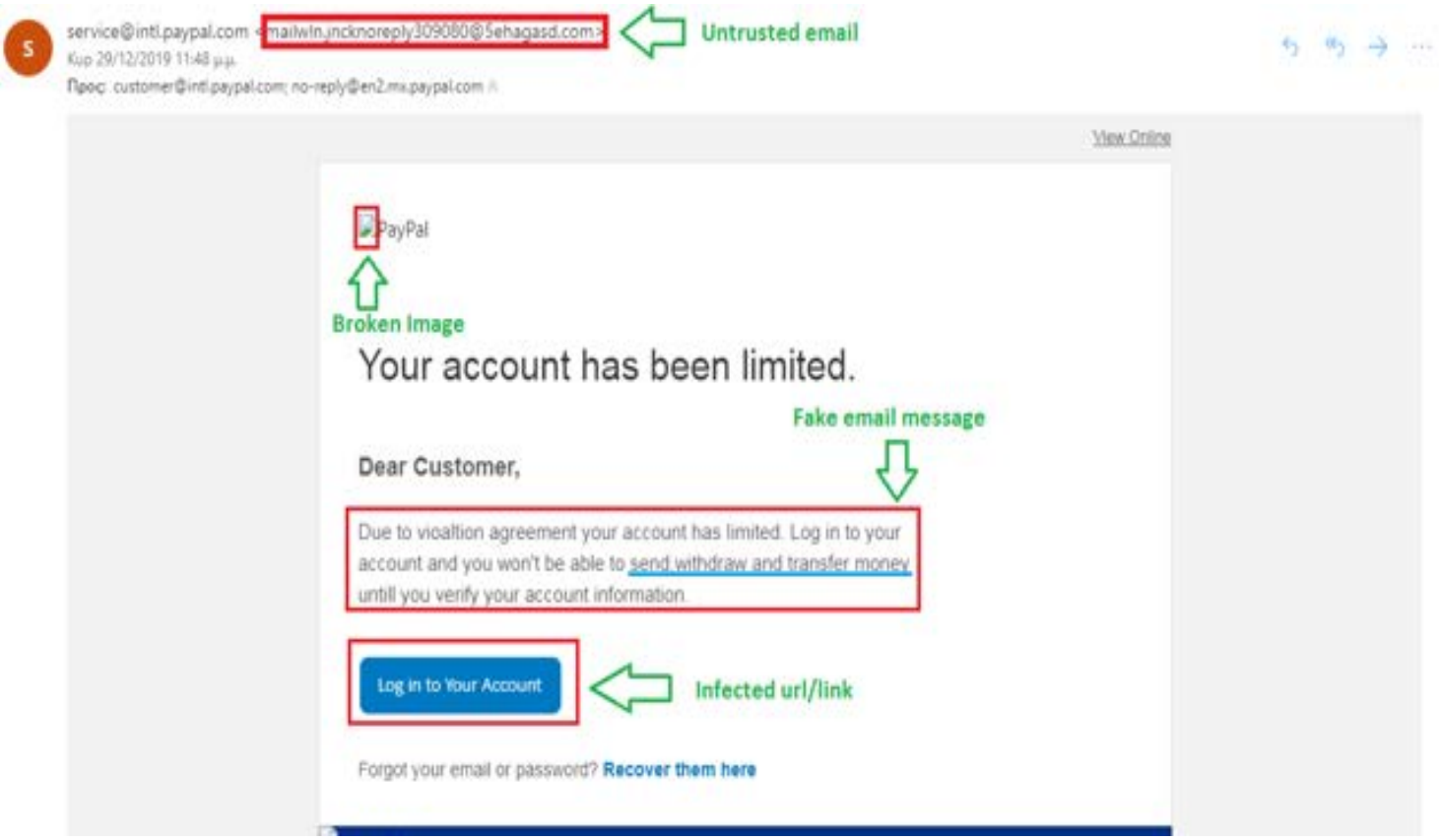


Figura 10 Ejemplo de un correo falso de Paypal

También existen otras categorías de *phising* por correo electrónico.

Las más básicas son:

- Archivos adjuntos infectados (extensiones .JS, .DOC, .HTML).
- Macros con cargas útiles en documentos word.
- Las Redes Sociales aprovechan para instalar extensiones maliciosas del navegador.
- Ataques *phising* de Linkedin (robar las credenciales del usuario).

He aquí una buena demo online para saber si un correo es real o no (*phising*):

Phishing demo

Co-funded by the
Erasmus+ Programme
of the European Union

MÓDULO 3

Confidencialidad, integridad y disponibilidad en entornos industriales

3.1 Disponibilidad

Description

3.1 Disponibilidad

Table of contents

La **continuidad del negocio** depende de muchos factores. En el campo de la administración de sistemas, es totalmente necesario preocuparse por el impacto que la infraestructura tecnológica tiene en el negocio.

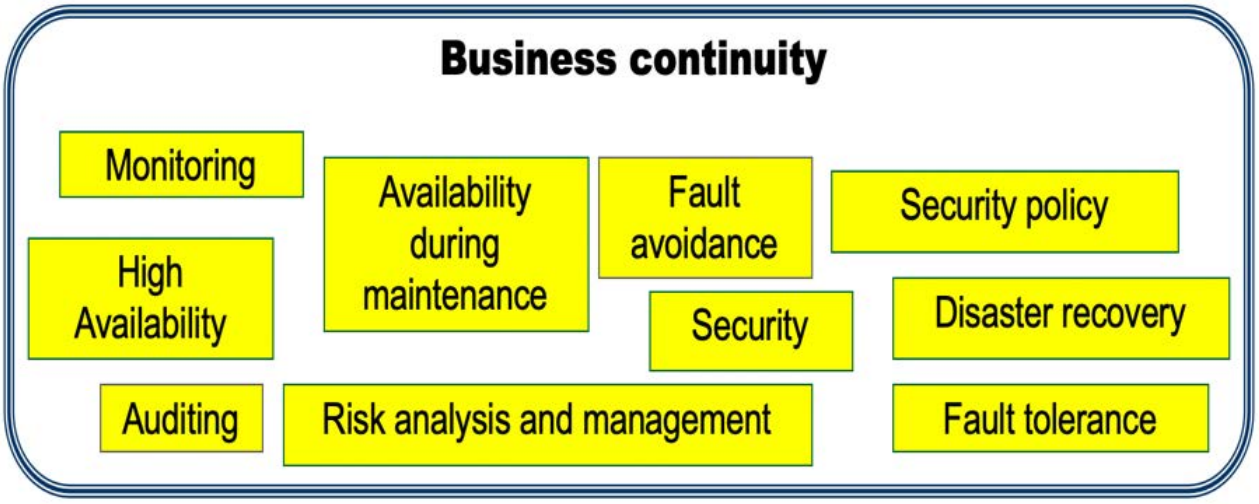


Figura 3.1- continuidad del negocio

La infraestructura tecnológica debe garantizar la continuidad del negocio sin interrupciones dentro de los **parámetros previstos** para el negocio soportado por esta infraestructura.

Se considera un **sistema seguro** (infraestructura tecnológica segura) el que se mantiene en funcionamiento dentro de los parámetros cualitativos y cuantitativos esperados (SLA: Service Level Agreement). Cualquier desviación en estos parámetros se considera un fallo.

Estos parámetros involucran la tríada de la seguridad informática: **confidencialidad, integridad y disponibilidad.**

La planificación de un sistema seguro que garantice la continuidad del negocio implica **sopesar los costes y los beneficios para obtener una probabilidad aceptable de fallo.**

No existen sistemas totalmente seguros hasta el punto de que existan garantías totales de que nunca se producirá un fallo (0 % de probabilidad de fallo).

Aunque la probabilidad de fallo es un dato útil, se suele utilizar **MTBF** (Mean Time Between Failures; Tiempo medio entre fallos), que indica el tiempo medio transcurrido entre fallos, expresado normalmente en horas.

La disponibilidad de un sistema es la relación entre la suma de los períodos de tiempo en los que el sistema funciona sin fallos y el tiempo total considerado (normalmente un año o un mes).

$$\text{Disponibilidad} = \frac{\text{tiempo de funcionamiento sin errores}}{\text{tiempo total}}$$

Figura 3.2.- Disponibilidad

Si un servidor falla 18 días en un año (más o menos 5 %) del tiempo de operación (un año equivale a 365 días), Disponibilidad= (365-18)/365 = 0.95

Su disponibilidad se puede definir como 95 %.

La tolerancia total a fallos garantiza que un fallo de un componente no afecte a los parámetros de funcionamiento.

Ejemplo: RAID1.

La matriz redundante de discos independientes (RAID) es un ejemplo común de tolerancia a fallos basada en la redundancia. RAID 1 (Mirroring) que utiliza una matriz de N discos idénticos (al menos 2), todos ellos con la misma información. Es capaz de soportar fallos simultáneas de N - 1 discos.

La **tolerancia a fallos** se consigue normalmente mediante la **redundancia** de los componentes. La sustitución perfecta e instantánea del componente defectuoso no siempre es posible.

En este caso se produce una degradación temporal de los parámetros de funcionamiento (Degradación gradual). Si esta degradación es significativa o prolongada, el sistema pasa a llamarse "fallos blandos, no tolerante a fallos" **(Fail soft , no Fault Tolerant).**

Un sistema se denomina "a salvo de fallos" (**Fail safe**) si el fallo causa indisponibilidad pero no compromete su integridad.

Ejemplo: UPS (batería de apoyyo) sin generador.

La **prevencion de fallos** tiene por objeto evitar que se produzcan fallos. Se basa en varias medidas de sentido común:

- Uso de componentes de **calidad** probada
- Control **ambiental** (temperatura, humedad, polvo)
- Control de potencia (estabilidad y filtrado)
- Control de **acceso físico**, incluyendo líneas de comunicación
- Control de **acceso remoto** (firewall, autenticación)
- Prevención y lucha contra **incendios**
- Realización de pruebas antes de la puesta en marcha de los componentes
- **Simplificar** la administración del sistema, por ejemplo, con la virtualización.
- Controlar los permisos y privilegios de administración
- **Divulgación** de la Política de Seguridad y formación de usuarios y operadores
- Aplicación de todas las **actualizaciones** de software
- Garantías de **autenticidad** (mecanismos sólidos de autenticación)
- **Monitoreo** (permite la detección de puntos potenciales de fallo)
- Control de la utilización de los recursos (limitación/reserva), como son la CPU; RAM; el disco, la red

Por muy cuidadosas que sean las medidas adoptadas en las áreas de **prevención de fallos y tolerancia a fallos**, no se pueden eliminar totalmente, por lo que el último recurso es la **reducción del impacto de los fallos**.

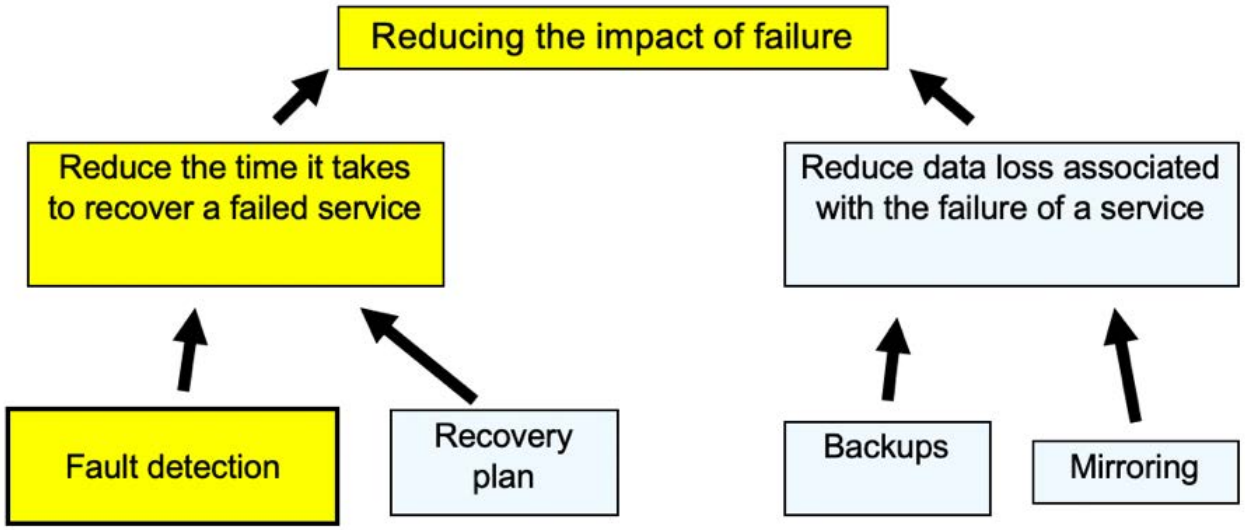


Figura 3.3- reducción del impacto de los fallos

Para más detalles sobre la duplicación, consulte la Sección 1.2 Tolerancia a fallos.

Por varias razones, la detección de fallos está directamente relacionada con las tres líneas complementarias de fallo, como puede verse en la figura 3.4.

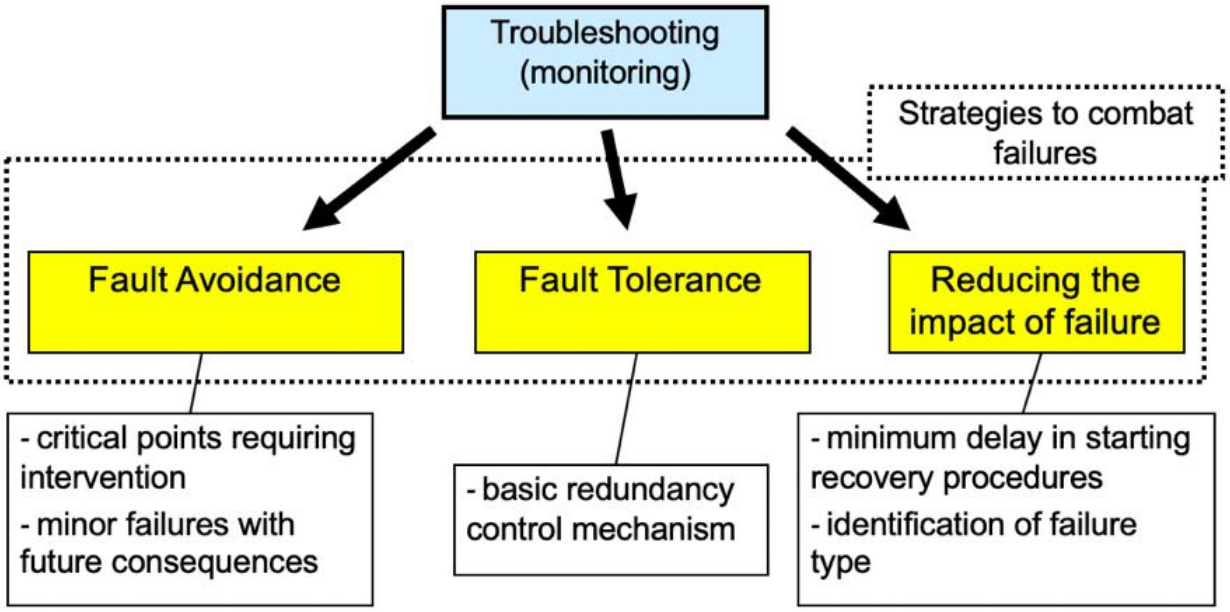


Figura 3.4. - resolución de problemas

Monitorización

La detección de fallos debe ser automatizada las 24 horas del día, los 7 días de la semana. Este proceso consiste en la ejecución periódica de pruebas sobre los componentes de la infraestructura informática:

- Tiempos de respuesta del servicio
- Estado de los dispositivos internos
- Medidas (temperaturas, etc.)
- Anomalías en los registros de actividad
- Volúmenes y tipos de tráfico de red
- Detección de anomalías e intrusos

Una vez detectada una anomalía, el sistema de monitorización debe notificar a los administradores lo antes posible para que se pueda iniciar el proceso de recuperación. Normalmente, se utiliza el correo electrónico, pero es preferible complementar esta opción con una forma de mensajería instantánea.

En algunos sistemas puede ser posible definir mecanismos de recuperación automática para algunas anomalías.

El propósito del **Plan de Continuidad del Negocio (BCP)** es definir un conjunto de condiciones y procedimientos destinados a asegurar la continuidad del negocio.

El **Plan de Recuperación de Desastres (DRP)** es uno de los elementos más importantes del BCP (a veces confuso), pero el BCP es más completo.

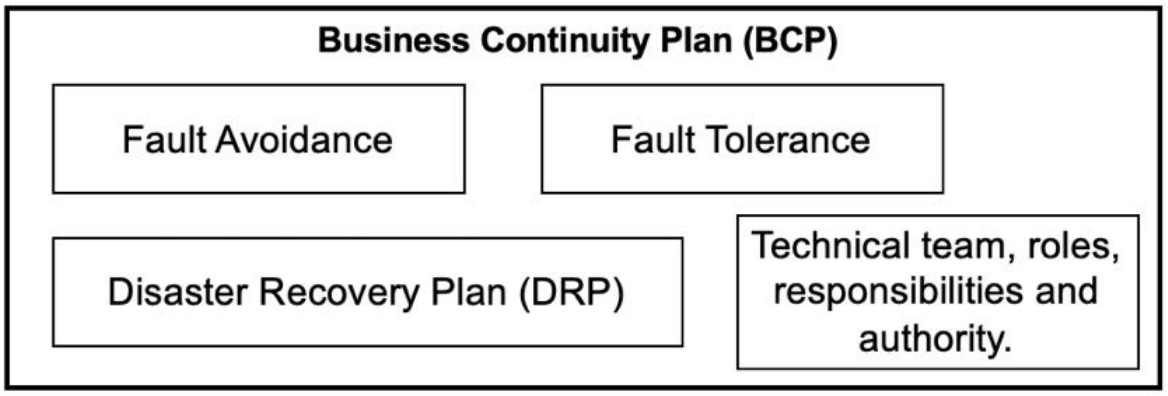


Figura 3.5- Plan de Continuidad del Negocio

Un plan de continuidad de negocio debe estar compuesto por:

- Prioridades y responsabilidades
- Principales riesgos y medidas de minimización
- Estrategias sugeridas
- Plan de Respaldo
- Funciones y responsabilidades
- Condiciones de activación del Plan de Continuidad de Negocio
- Procesos de recuperación de emergencia

La evaluación de riesgos puede realizarse mediante formularios/encuestas que, al cuantificar un conjunto de parámetros, permiten una cuantificación abstracta del riesgo en el ámbito analizado.

.

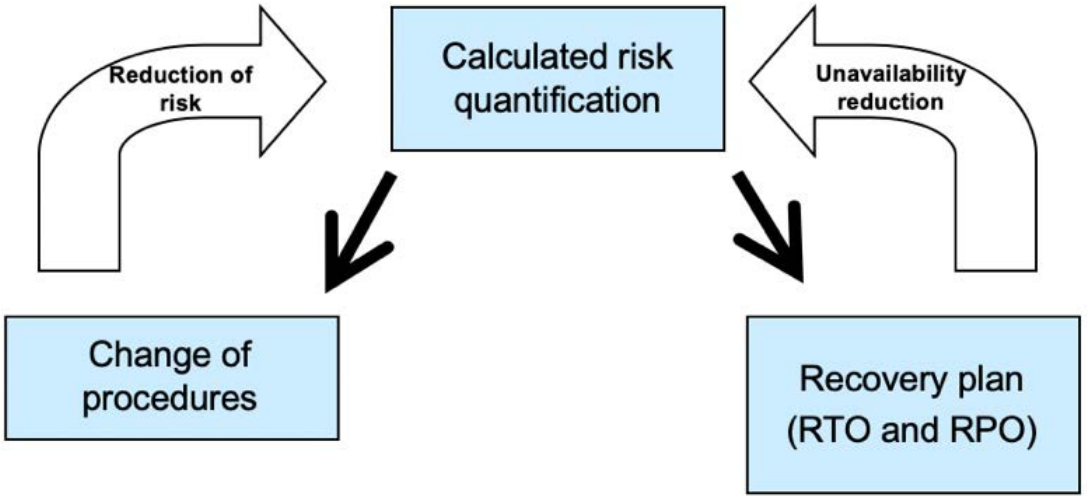


Figura 3.6.- evaluación de riesgos

Para los servicios en los que se permite la pérdida de datos en caso de desastre, el **objetivo de punto de recuperación (RPO)** especifica la cantidad máxima de datos que se pueden perder. RPO especifica un tiempo de operación previo al desastre a partir del cual se perderán todos los cambios realizados.

El tiempo entre copias de seguridad nunca puede ser mayor que RPO. Si se usa **mirroring** (copias redundantes de los datos) el RPO es nulo o muy cercano a cero (si el mirroring es sincrono, el RPO es nulo).

El **objetivo de tiempo de recuperación (RTO)** es, por lo tanto, el tiempo máximo que se supone que el sistema está inoperativo.

En caso de fallo, debe iniciarse un proceso de recuperación (incluso si es un componente de un sistema redundante).

El término **recuperación de desastres** está más orientado a eventos de alto impacto que incluyen desastres naturales catastróficos con destrucción física casi total.

La recuperación de desastres es crítica para la continuidad del negocio, el objetivo es **minimizar el tiempo de inactividad y la posible pérdida de datos.**

La recuperación después de un desastre se basa en la preparación y la planificación de medidas como las siguientes:

- Mirroring (copia de datos redundante)
- Copias de seguridad periódicas almacenadas en una ubicación remota
- Reservar hardware almacenado en una ubicación remota
- Preveer escenarios de desastres y sus planes de recuperación.

El propósito del **Plan de Recuperación de Desastres (DRP)** es minimizar el tiempo de inactividad y la pérdida de datos en caso de desastre. DRP define escenarios de desastre y procedimientos de recuperación para cada uno de ellos. Esto también debe tener un tiempo máximo, se supone que el sistema está inoperativo.

Copia de seguridad/restauración

La copia de seguridad permite que después de un desastre con pérdida de datos o configuraciones de software, se puede recrear un sistema con el mismo estado que la fecha en que se hizo la última copia.

La frecuencia con la que se realizan las copias de seguridad debe depender de la frecuencia de los cambios en los datos y, por lo tanto, debe ajustarse adecuadamente a cada elemento de la infraestructura.

El tiempo exacto de la copia de seguridad debe ajustarse al horario laboral. Para las copias diarias, por lo general, las más apropiadas son las que se hacen fuera de horario.

Los medios de almacenamiento lentos causan problemas durante la realización de copias, lo que hace que la operación lleve mucho tiempo. Las operaciones de copia de seguridad pueden afectar a la disponibilidad del sistema. Por lo general, los objetos como archivos deben bloquearse para evitar que se realicen cambios en ellos durante la copia.

Plan de copia de seguridad/restauración

Una forma de reducir la longitud de las operaciones de copia es utilizar copias incrementales o copias diferenciales. En cualquier caso, el punto de partida es siempre una copia completa.

Una **copia incremental** contiene los datos que se han modificado desde la copia incremental anterior (o copia completa si es la primera).

Una **copia diferencial** contiene datos que se han modificado desde la última copia completa.

Se debe mantener un gran número de copias incrementales; además del espacio ocupado, la operación de sustitución consume mucho tiempo. Copias diferenciales: el volumen de la copia diferencial crece a medida que se acumulan los cambios con respecto a la copia integral.

También en este caso hay que respetar el horario de trabajo, a menudo la opción es hacer una copia completa el domingo y copias incrementales o diferenciales durante los otros días de la semana (pero depende del horario de trabajo en cuestión).

Una copia de seguridad **nunca debe eliminarse sin que se haya completado correctamente la siguiente copia de seguridad**. Incluso es deseable conservar al menos una copia previa, a menudo optando por conservar varias.

La copia de seguridad anterior se puede mover a un medio de almacenamiento más económico antes de hacer una nueva copia.

Aunque la copia de seguridad puede dejarse sin mantenimiento en un recinto a prueba de incendios, lo ideal es que sea en una ubicación geográfica separada (fuera del emplazamiento).

Debe tenerse en cuenta al hacer las copias de seguridad:

- Seguridad: es necesario garantizar la autenticación y la confidencialidad (por ejemplo, utilizar VPN).
- Velocidad de acceso: afecta al tiempo necesario para la copia.
- Fiabilidad de la conexión: la recuperación sólo es posible si la conexión de red está operativa.

El plan de contingencia es una parte importante del plan de continuidad de negocio (BCP) y define metodologías alternativas para mantener el negocio en marcha cuando los recursos «normales» no están disponibles.

En las organizaciones que dependen en gran medida de los sistemas informáticos, puede ser difícil de implementar. Debes definir:

- Qué tipo de desastre debe conducir al inicio del plan de contingencia.
- Definir los pasos exactos a seguir.
- Definir las necesidades en términos de personal y materiales o equipos.
- Qué procedimientos «normales» están previstos en el plan de contingencia y cuáles no estarán disponibles (restricciones en la operación del negocio).
- ¿Cómo se integrarán en el sistema los procedimientos realizados durante el plan de contingencia después de su recuperación?

La política de seguridad es un documento que establece un conjunto de normas obligatorias destinadas a la protección de las infraestructuras y los datos.

Es un elemento importante para garantizar la continuidad del negocio, especialmente en el campo de la prevención de fallos.

La Política de Seguridad debe ser más abstracta que un manual de usuario, debe **indicar «lo que no se puede hacer», «lo que se puede hacer», pero no debe incluir «cómo hacerlo».**

Por razones de seguridad y para facilitar su adaptación a la evolución de la organización, no debe contener aspectos técnicos de la implementación.

La Política de Seguridad debe ser concisa y fácil de leer e interpretar; sugerimos el uso de las que en inglés son las 5 Ws del periodismo: Quién (who), Qué (what), Dónde (where), Cuándo (when), Por qué (why).

El carácter más o menos restrictivo de la política de seguridad debe resultar de una evaluación previa del potencial de riesgo para la seguridad. Es posible cuantificar un nivel de riesgo de ataque, a través de cuestionarios sobre la organización/negocio y su infraestructura.

Características del Plan de Seguridad:

- Documento público, de fácil acceso para todos los usuarios
- Lectura obligatoria para todos los usuarios
- Identifica los diferentes actores de la organización (usuarios, administradores,...)
- Define claramente los objetivos de seguridad
- Alerta a los usuarios de las diversas amenazas a las que está sujeto el sistema. 3.
- Subraya la importancia de que todos, sin excepción, respeten las normas
- Justifica la razón de las reglas impuestas (los actores deben estar de acuerdo)
- Identifica contactos para la aclaración de preguntas dudosas
- Define el tratamiento de las situaciones que faltan en la «política de seguridad».
- Establece las consecuencias de la violación de las normas (de manera abstracta, ya que puede entrar en conflicto con la legislación o los acuerdos laborales).
- Destaca el mantenimiento de registros de actividades para las auditorías
- Es consistente con la profundidad del enfoque multifacético
- Es posible imponer a los actores (es posible controlar el cumplimiento de las normas)

Una política de seguridad debe definir lo que se permite y por ende, prohibir todo lo demás. Es más arriesgado decir lo que está prohibido y por ende, permitir todo lo demás.

Las políticas deseguridad comprenden:

- **Autenticación**
- **Acceso físico**
- **Acceso lógico**
- **Uso interno de la red (conexión de dispositivos a la red, ...)**
- **Uso de Internet (acceso a páginas web, control de contenidos,...)**
- **Contraseñas (reglas en la definición, almacenamiento y manipulación)**
- **Uso del correo electrónico**
- **Privacidad (confidencialidad; registros de actividad y acceso a ellos)**
- **Gestión de los sistemas de trabajo.**

3.2 Confidencialidad de los datos

Description

3.2 Confidencialidad de los datos

Table of contents

La confidencialidad puede definirse como la garantía de que existe un nivel adecuado de secreto en cada nodo de procesamiento y de que se **evita la fuga de información**.

La confidencialidad debe ser implementada en todo el sistema y no sólo en algunas partes. Puede obtenerse a través de:

- Cifrado de los datos almacenados y transmitidos
- Comunicaciones seguras

La confidencialidad puede ser anulada por:

- Monitorización de la comunicación
- Ingeniería social
- Robo de contraseñas

El almacenamiento de datos es una parte clave de un sistema informático/industrial en el que las necesidades y la importancia de la información aumentan día a día. Hoy en día, en muchos casos, la información es el activo más valioso de una empresa.

Son varios los medios disponibles para almacenar datos. Estos medios difieren en capacidad, calidad y precio. En los sistemas profesionales es importante elegir medios que aseguren que no se produzca una pérdida de información.

Los pendrives y los discos externos son los medios de almacenamiento más **baratos** del mercado. Tienen algunos problemas como resultado de la calidad de la infraestructura y porque no son muy bien tratados/utilizados por los usuarios.

Estos medios se pueden utilizar para almacenar **información no crítica**. Sin embargo, es aconsejable tener una copia de seguridad en otro medio.

Este tipo de equipo normalmente **no implementa la seguridad o el cifrado de los datos**, por lo tanto, si se pierde o alguien lo roba, los datos cruciales pueden llegar a estar disponibles públicamente.

Figura 3.7- PenDrive

«**Cloud (nube) computing** es un término general para cualquier cosa que implique la prestación de servicios alojados a través de **Internet**. Estos servicios se dividen en tres categorías: **Infraestructura como servicio** (IaaaS), **Plataforma como servicio** (PaaS) y **Software como servicio** (SaaS). El nombre "cloud computing" se inspira en el símbolo de la nube que se utiliza a menudo para representar a Internet en diagramas y diagramas de flujo.

Un servicio en la nube tiene tres características distintas que lo diferencian del alojamiento web tradicional. Se vende bajo **demanda**, típicamente por minuto o por hora; es **elástico**, un usuario puede tener tanto o tan poco servicio como quiera en cualquier momento dado; y el servicio lo **administra totalmente el proveedor**(el consumidor sólo necesita una computadora personal y acceso a Internet). Las innovaciones significativas en virtualización y computación distribuida, así como la mejora del acceso a Internet de alta velocidad, han acelerado el interés en la computación en nube.

Una nube puede ser **privada o pública**. Una nube pública vende servicios a cualquiera en Internet. (Actualmente, Amazon Web Services es el mayor proveedor de nube pública.) Una cloud privada es una red propietaria o un centro de datos que proporciona servicios alojados a un número limitado de personas. Privado o público, el objetivo del cloud computing es proporcionar un acceso fácil y escalable a los recursos informáticos y a los servicios de TI.

La nube privada es un tipo de cloud computing que ofrece ventajas similares a la nube pública, incluyendo escalabilidad y autoservicio, pero a través de una arquitectura propietaria. A diferencia de las nubes públicas, que ofrecen servicios a múltiples organizaciones, una nube privada está dedicada a las necesidades y objetivos de una sola organización.

Como resultado, **la nube privada es lo mejor para las empresas** con necesidades informáticas dinámicas o impredecibles que requieren un control directo sobre sus entornos, normalmente para cumplir con los requisitos de seguridad, gobernanza empresarial o cumplimiento normativo».

[1] Fuente: searchcloudcomputing.techtarget.com

El **almacenamiento en red (en inglés, NAS)** es un tipo de almacenamiento que se utiliza habitualmente en las empresas porque es una forma económica de proporcionar un gran espacio de almacenamiento para múltiples usuarios.

Las características más importantes son:

- Rápido de instalar y configurar.
- Método fácil de asegurar la redundancia RAID para múltiples usuarios.
- Le permite establecer permisos para acceder a las carpetas y archivos de los usuarios.
- Alta utilización de los recursos de almacenamiento.

Este tipo de almacenamiento tiene también algunos inconvenientes:

- Utiliza recursos de red (tiene al menos una dirección IP).
- Problemas de latencia y potencialmente de transferencia de datos.
- Rendimiento afectado por la disponibilidad de la red.

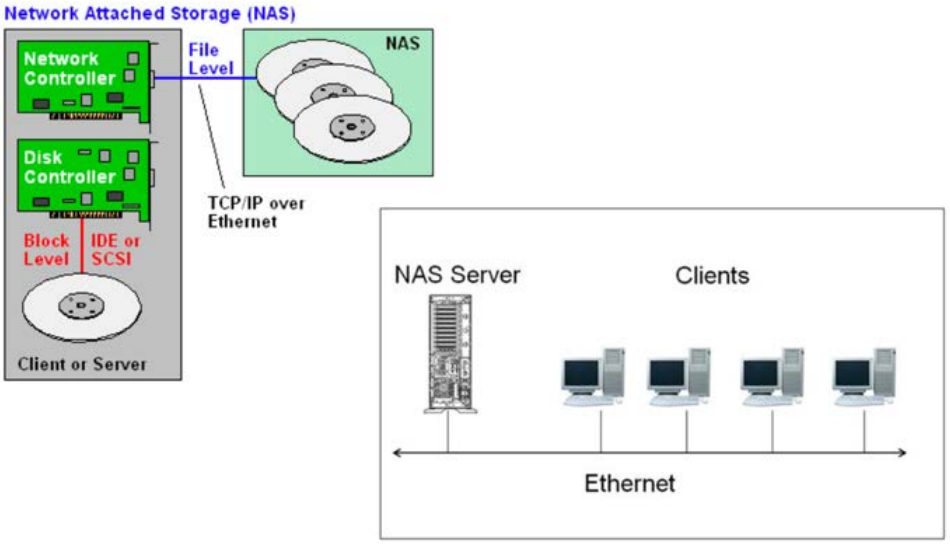


Figura 3.8- Almacenamiento en red / Network Attached Storage (NAS)

Las redes son por su naturaleza un medio privilegiado para llevar a cabo ataques:

- Al ser una transmisión de información significa que puede ser utilizada para atacar remotamente sistemas que están protegidos del acceso físico a la Red de Entrega de Contenido.
- Son extensas, por lo que es muy difícil controlar eficientemente el acceso físico, lo que hace que incluso sea una misión imposible para las redes inalámbricas. Aunque el control de acceso físico no ofrece garantías, nunca debe pasarse por alto.

La **autenticación y el cifrado** son dos herramientas clave para contrarrestar muchos de los ataques, pero pueden no ser suficientes. La **segmentación** de las redes en distintas zonas de nivel de seguridad es esencial, normalmente se pueden considerar tres zonas:

- Red de Entrega de Contenido (donde se encuentran los servidores)
- Red interna de usuarios (intranet)
- Redes externas (Internet)

La separación entre zonas se asegura a través de la interconexión mediante routers que analizan y filtran la información, designados por cortafuegos.

Conexiones Wifi

En las redes inalámbricas, el control de acceso físico es totalmente imposible (en este tipo de redes, la señal se transmite por ondas de radio disponibles en el espectro a interceptar). Aunque las redes de área local por cable soportan actualmente la conmutación de paquetes a nivel 2 (por ejemplo, Ethernet), estos conmutadores no separan los dominios de difusión y su funcionamiento puede verse comprometido. Desde el punto de vista de la seguridad, este tipo de infraestructura debe considerarse siempre equivalente a una red de medio de transmisión compartida: cualquier paquete emitido en un nodo determinado se entrega en todos los demás nodos de la red.

En el mercado están disponibles un conjunto de algoritmos que permiten implementar seguridad y encriptación a los paquetes que circulan en redes WIFI.

Los ejemplos más comunes de estos algoritmos de seguridad son:

- **WEP** (Wired Equivalent Privacy) (se utilizó entre 1999 - 2004, pero al ser muy vulnerable a los ciberataques ha sido abandonada)
- **WPA** (Wifi Protected Access) . Version mejorada de WEP. Fácil de romper.
- **WPA2** - (Wifi Protected Access) versión 2. La encriptación AES (Advanced Encryption Standard) es la mejora más importante realizada en WPA2 sobre WPA.

Transporte seguro de datos: Firmas digitales

Una firma digital es una forma de garantizar la autenticación o confidencialidad basada en un certificado digital compuesto por 2 claves (una privada que sólo el propietario del certificado debe conocer y una clave pública que debe ser conocida públicamente). Este método se denomina encriptación asimétrica porque un mensaje encriptado sólo se puede desencriptar con la clave del otro par.

PKI (Infraestructura de Clave Pública)

Utilizado para encriptar, descifrar y autenticar (firma digital)

La clave pública se divulga libremente y puede utilizarse para el cifrado.

El descifrado se realiza con la clave privada (secreta).

No es bidireccional porque un par de claves sólo permite la confidencialidad en cierto sentido.

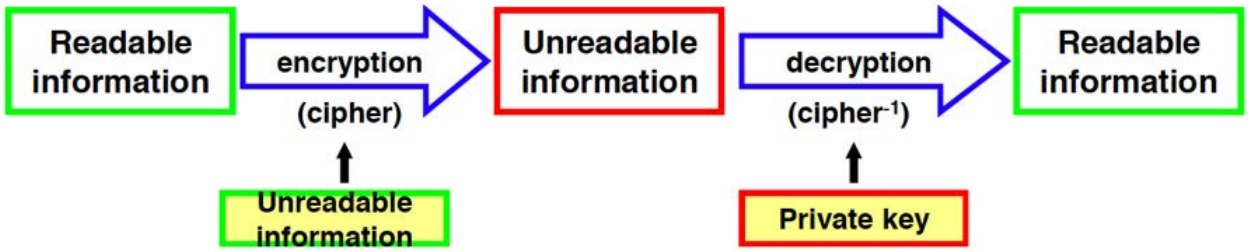


Figura 3.9- Firma digital

Un par de claves públicas/privadas sólo garantiza la confidencialidad unidireccional, para obtener la confidencialidad bidireccional se necesitan dos pares de claves. La aplicación de encriptación asimétrica con la clave privada a un código hash sólido permite implementar de forma sencilla todas las funcionalidades de una firma digital, certificando:

- Integridad del contenido
- Autenticación de autor
- No repudio (sólo el autor posee la clave privada)

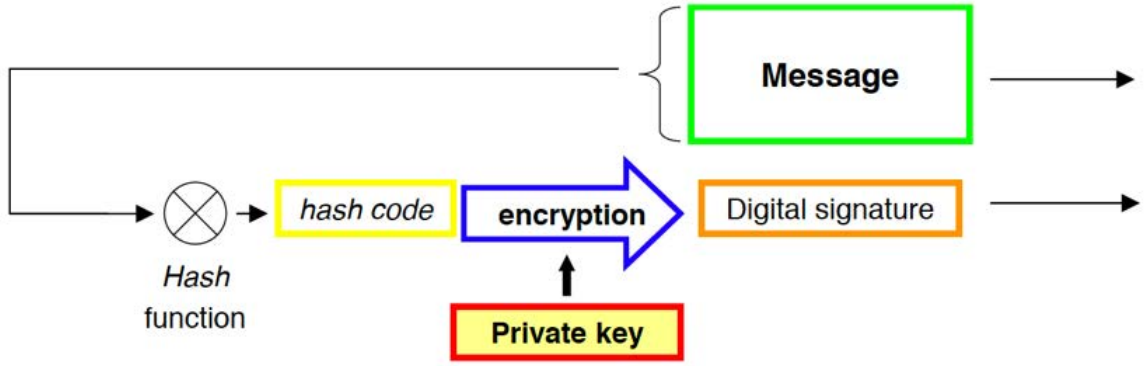


Figura 3.10- integridad y autenticación

Confidencialidad con cifras clave asimétricas

El uso de una clave pública de alguien para encriptar un mensaje permite garantizar la confidencialidad, ya que el mensaje encriptado sólo se desencriptará con la clave privada del usuario.

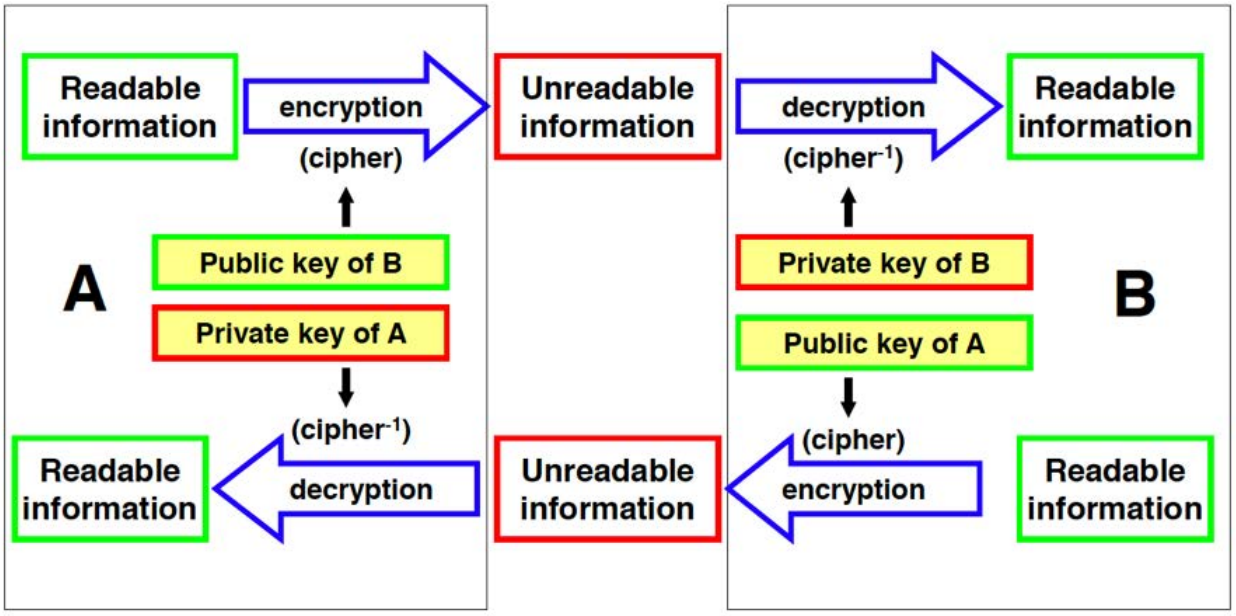


Figura 3.11- confidencialidad con cifrado de clave asimétrica

3.3 Integridad de los datos

Description

Table of contents

La **integridad** puede definirse como la confianza en la precisión y fiabilidad del sistema y en la prevención de cambios de datos no autorizados.

Se asegura de que los ataques y errores no comprometen la información, y la integridad del sistema se puede obtener a través de:

- La buena gestión de las capacidades del sistema
- Mecanismos de detección de intrusos
- Controles de acceso adecuados

Sin garantía de integridad, un sistema puede funcionar con datos incorrectos, sin que nadie sea consciente de ello.

La **copia de seguridad y el almacenamiento de datos** es una de las medidas más importantes que una empresa debe tomar para proteger su negocio.

Es importante tomar las siguientes medidas:

- Hacer copias de seguridad de los datos regularmente (esta periodicidad debe ser evaluada en cada caso).
- Crear copias de seguridad en **medios fiables** o en las nubes de la empresa (estas nubes deberían tener copias de seguridad redundantes).
- Si utiliza varios medios para realizar copias de seguridad, mantenga los dispositivos en una **ubicación segura y externa**.

Elegir un lugar seguro para la copia de seguridad

El lugar donde se encuentran las copias de seguridad es una parte clave del proceso de copia de seguridad. Debido a desastres impredecibles, las copias de seguridad deben mantenerse en más de un lugar. Las empresas pueden mantener una copia de seguridad local en sus instalaciones, pero deben tener otra copia en una ubicación externa (puede ser una nube u otra instalación de la empresa).

Hacer *hash* de los archivos de la copia de seguridad

Los archivos de copia de seguridad resultantes se deben verificar con un *hash*. El ***hashing*** es una técnica que sirve para garantizar que el contenido del archivo no ha sido modificado.

Este proceso implica la utilización de un algoritmo criptográfico como MD5. La aplicación de este tipo de algoritmos a un fichero devuelve un número/código que puede considerarse como un identificador. Si se cambia el archivo, el resultado de la aplicación de algoritmo será diferente y es posible detectar que se ha realizado algún cambio no autorizado.

Cuando se realiza una copia de seguridad se debe generar un código hash basado en la aplicación de un algoritmo criptográfico. Más tarde este hash puede ser usado para evaluar si el archivo fue cambiado.

Prueba de las copias de seguridad [2]

<<Imagínate que estás conduciendo por la carretera y, de repente, oyes un sonido extraño que viene de la parte trasera de tu coche. A medida que el coche se vuelve cada vez más difícil de manejar, empiezas a entender lo que ha pasado: Tienes una rueda pinchada. No hay problema. Busca un lugar seguro y saca el repuesto de emergencia del maletero. Oh, la rueda de repuesto también está desinflada.>>

Una crisis similar enfrenta un número incalculable de administradores de almacenamiento cada día. Debido a un descuido, un error o un fallo de un medio de almacenamiento principal, de repente surge la necesidad de acceder a un conjunto particular de archivos almacenados en un medio de copia de seguridad. Pero los datos de la copia de seguridad no están completos, están obsoletos o son defectuosos. Al igual que un controlador infortunado, el administrador de almacenamiento se enfrenta ahora a un problema que podría haberse evitado fácilmente con una planificación anticipada, en forma de pruebas de copias de seguridad.

Esto es lo que tienes que hacer para no tener problemas con las copias de seguridad:

- Entender lo necesarias que son las **pruebas de copia de seguridad periódicas**.

Así como es importante probar una rueda de repuesto para asegurar que funcione cuando más se necesita, también es necesario probar las copias de seguridad, según Girish Dadge, director de administración de productos de Sungard Availability Services. «Probar tus copias de seguridad también te da la oportunidad de asegurarte de que tus políticas y programas de copias de seguridad funcionan correctamente», añadió.

- **Crea un plan de pruebas de respaldo documentado**.

La familiaridad con un plan de pruebas documentado garantiza que los empleados tengan las habilidades y la experiencia necesarias para realizar con éxito la recuperación de datos y proporciona confianza a la organización, observó Eamonn Fitzmaurice, líder mundial de protección de datos en la empresa de servicios de TI HPE Pointnext.

- **Haz de las copias de seguridad de las pruebas una rutina**.

Para asegurar la validez e integridad de cualquier copia de seguridad, es esencial llevar a cabo pruebas periódicas de restauración. «No es inusual encontrar organizaciones que tienen sistemas que de manera inadvertida, no están siendo protegidos mediante una programación de copias de seguridad», explicó Fitzmaurice. Las pruebas de respaldo rutinarias y exhaustivas son una estrategia que puede resaltar las anomalías, para que se puedan tomar medidas correctivas.

- **Adopta un enfoque holístico**.

Las organizaciones necesitan entender la disposición de sus datos y por qué están haciendo copias de seguridad. Luego necesitan desarrollar un plan de respaldo de prueba para cumplir con sus objetivos deseados.

- Cada organización tiene **diferentes objetivos de respaldo**.

«Por ejemplo, la industria bancaria necesita copias de seguridad para el cumplimiento, la auditoría y los asuntos legales», dijo Dadge. «Las organizaciones de la salud tienen datos personales, así que deben centrarse en la seguridad, la retención y los requisitos legales.» Todas las pruebas de restauración y recuperación deben incluir pruebas de datos, aplicaciones y estado del sistema, recomendó Dadge.

- **Realiza pruebas con frecuencia** de acuerdo con los horarios regulares.

Lo ideal es que se realice una prueba después de que se complete cada copia de seguridad para garantizar que los datos se puedan proteger y recuperar correctamente. No obstante, esto a menudo no es práctico debido a la falta de recursos disponibles o a limitaciones de tiempo. «Cada organización debe, como mínimo, comprometerse a un programa regular de restauraciones semanales o mensuales de sistemas, aplicaciones y archivos individuales con comprobaciones para garantizar que los datos son válidos y accesibles según lo previsto», declaró Marty Puranik, CEO de Atlantic.Net, un proveedor de cloud hosting. «Esto también le dará a tu organización un tiempo realista para la recuperación cuando ocurra un desastre.»

- **No todos los datos se crean de la misma manera,**

Un hecho que debería afectar la frecuencia de las pruebas de copias de seguridad. «Algunos datos son más importantes que otros», señaló Atif Malik, director de la unidad de asesoramiento del CIO de KPMG. Por ejemplo, el cumplimiento de la Ley Sarbanes-Oxley y los datos de los reguladores pueden considerarse más importantes que los datos de marketing. «Se deben establecer controles para mitigar los riesgos en función de la importancia de esos datos», aconsejó Malik.

- **Aprovecha al máximo la automatización**.

La automatización debe jugar un papel clave en cualquier estrategia de pruebas de respaldo. «Las organizaciones deben esforzarse por automatizar la mayor parte posible de sus pruebas de copia de seguridad para garantizar la coherencia y la validez de los datos y reducir la carga del personal encargado de probar las copias de seguridad», sugirió Puranik. «Prueba la restauración de sistemas completos en máquinas virtuales, aplicaciones, bases de datos y archivos individuales», añadió.

- Asegúrate de que la **prueba de copia de seguridad cubra todas las bases**.

Si la prueba de copia de seguridad no prueba toda la carga de trabajo que se está restaurando, no se puede considerar una prueba real. «Muchas organizaciones simplemente restaurarán uno o dos archivos del archivo y lo considerarán un éxito», señaló Chris Wahl, tecnólogo jefe del proveedor de gestión de datos en nube Rubrik. «Este flujo de trabajo no tiene relación con la realidad de la restauración de aplicaciones complejas y debe evitarse cuando se considera una prueba de copia de seguridad real.»

- Haz de las copias de seguridad de pruebas una **parte integral del desarrollo y la implementación de aplicaciones** internas.

Las pruebas de copia de seguridad deben estar en la mente de todos al desarrollar e introducir nuevas aplicaciones en la organización. «Las estrategias de gestión de datos empresariales más exitosas implican saber cómo y cuándo realizar pruebas de validación de copias de seguridad antes de permitir que los datos pasen a una carga de trabajo de producción», explicó Wahl.

- **Garantizar la precisión de la copia de seguridad.**

Cuando se recuperan los datos, los administradores de almacenamiento y los administradores de bases de datos pueden realizar una «comprobación de la sanidad» inicial de los datos. «No obstante, los usuarios finales de las aplicaciones empresariales suelen estar mejor posicionados para destacar si los datos restaurados son precisos y coherentes», observó Fitzmaurice.

- **Ten copias de seguridad redundantes**.

No hagas nunca una copia de seguridad de una sola cinta o juego de cintas. «Si utilizas cintas, reemplázalas regularmente», recomendó Brian Engert, desarrollador senior de aplicaciones del desarrollador de software del cliente Soliant Consulting.

[2] Fuente: https://searchdatabackup.techtarget.com/tip/Ten-important-steps-for-testing-backups

Ejercicio 1. Información crítica de las copias de seguridad

En Internet hay disponibles varias soluciones de copia de seguridad.

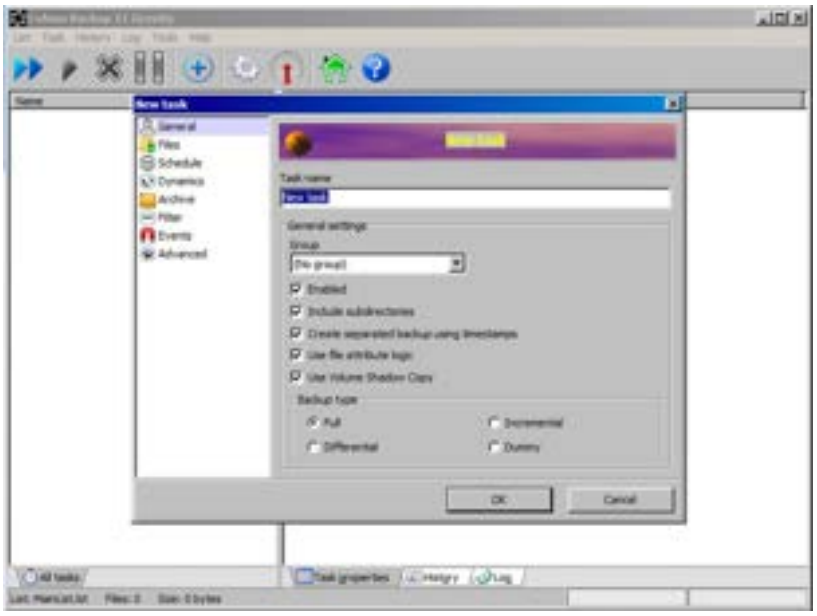
Algunos ejemplos son:

- COBIAN BACKUP (https://www.cobiansoft.com)
- GOOGLE BACKUP AND SYNC (https://www.google.com/intl/enGB_ALL/drive/download/backup-and-sync)
- ACRONIS (https://www.acronis.com/en-us/business/overview/)

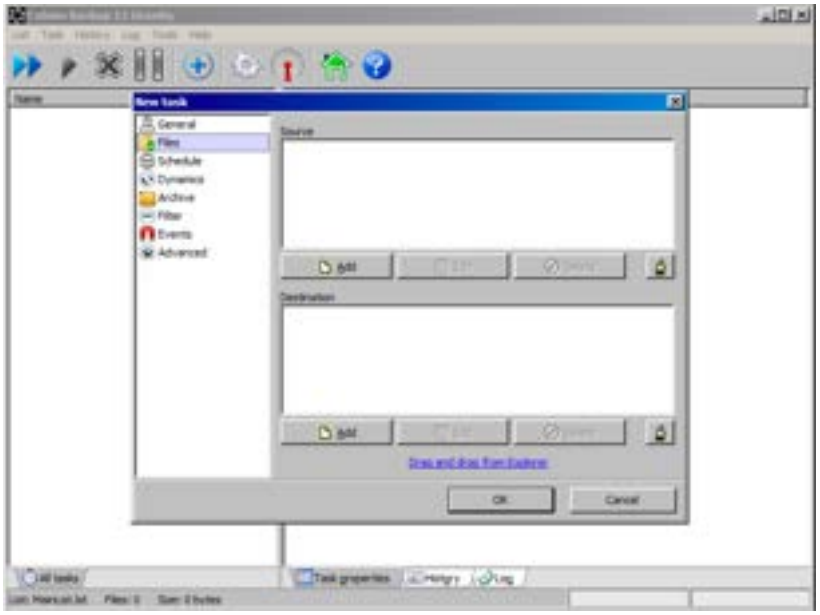
Por favor, utilice uno de estos para crear una copia de seguridad local en una ubicación externa (Disco duro, pendrive, Tarjeta SD, etc.) y para crear una copia de seguridad remota en una ubicación externa.

Ejemplo de Cobian Backup:

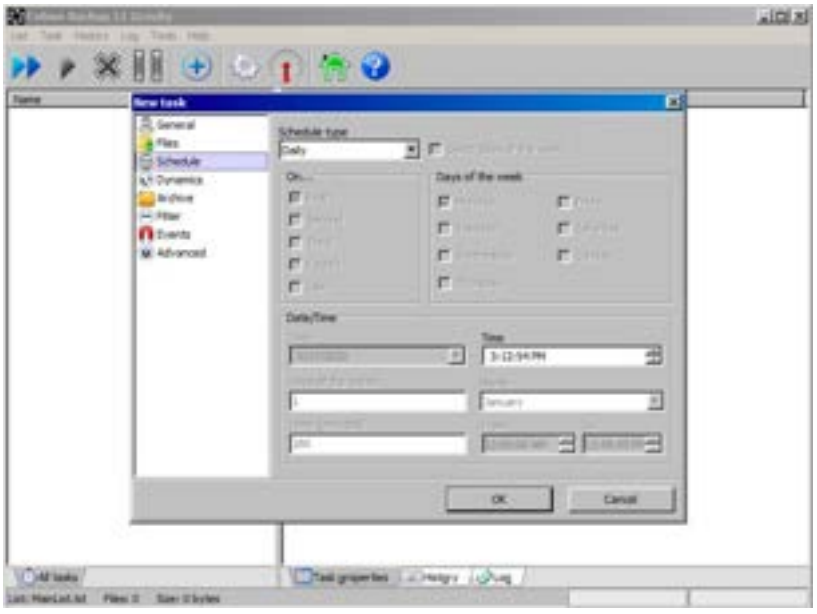
1. Descargue e instale el software.
2. Cree una nueva tarea (Tarea, Nueva Tarea) y elija el tipo de copia de seguridad (Completa, Incremental y diferencial).



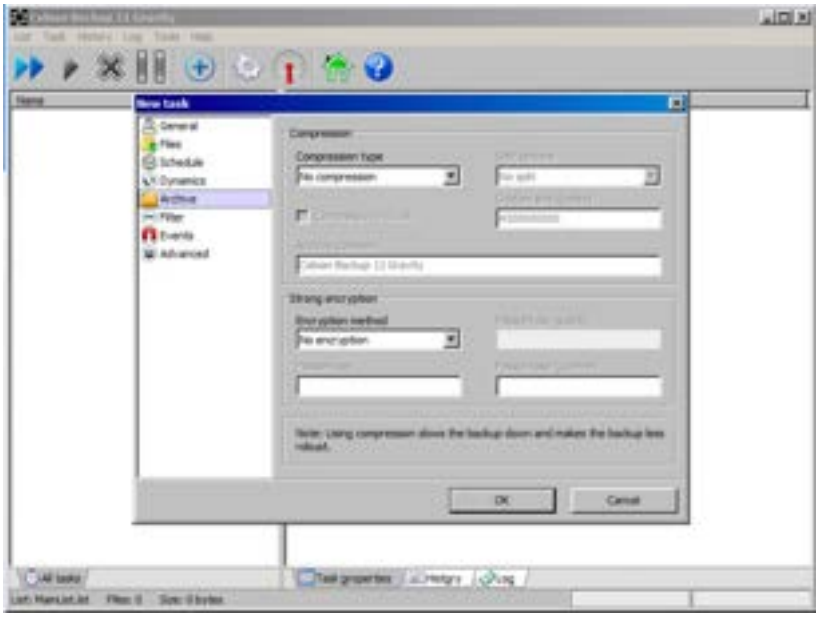
3. En el menú archivos elija los archivos que se incluirán en la copia de seguridad y el destino de la copia de seguridad (puede ser un directorio local o en una unidad externa) o una ubicación ftp remota).



4. En el menú programación, se puede elegir la frecuencia de la copia de seguridad (normalmente diaria, semanal o mensual).



5. En el menú archivo. Se puede elegir la compresión si es importante comprimir los datos antes de la copia de seguridad.



Notas

Nota 1: Las copias de seguridad con la información de la empresa deben realizarse con conocimiento y autorización de la administración.

Nota 2: Las copias de seguridad deben cumplir con las regulaciones de la UE descritas en el **reglamento general de protección de datos. Por ejemplo, es importante comprender si puede hacer una copia de seguridad de los datos relacionados con personas para ubicaciones fuera de la UE (y en el caso de que necesite hacerlo, que condiciones debe garantizar).**

Ejercicio 2: Comunicaciones seguras por correo electrónico.

Para recibir un correo electrónico cifrado o enviar un correo electrónico firmado digitalmente, debe tener un certificado digital.

Para instalar su certificado digital en **Mozilla Thunderbird** para firmar o cifrar digitalmente correos electrónicos, siga estas instrucciones.

1. Dentro de Thunderbird, haga clic en “Menú” y luego coloque el cursor sobre la sección “Opciones” y “Preferencias”.
2. Haga clic en la sección “Configuración de la cuenta”; luego haga clic en la pestaña “Seguridad”.
3. Haga clic en el botón “Ver certificados”; luego haga clic en el botón “Importar”.
4. Busque el archivo de copia de seguridad de su certificado y haga clic en “Abrir”.
5. Se le pedirá que ingrese la contraseña del certificado; luego haga clic en “Aceptar”. (La contraseña del certificado es la contraseña que eligió al exportar el certificado).

Configurar Thunderbird con un certificado predeterminado

1. Dentro de Thunderbird, haga clic en “Menú” y luego coloque el cursor sobre la sección “Opciones” o “Preferencias”.
2. Debajo de “Encabezado de la cuenta de correo electrónico” (es posible que deba ampliarlo), haga clic en “Seguridad”.
3. Junto a la casilla “Use este certificado para firmar digitalmente los mensajes que envíe”, haga clic en “Seleccionar”.
4. Elija el certificado digital correcto para utilizarlo. Tenga en cuenta que la dirección de correo electrónico en su cuenta de correo electrónico debe coincidir con la dirección en el certificado.
5. Junto a la casilla de “Usar este certificado para cifrar y descifrar los mensajes que se le envíen”, haga clic en “Seleccionar”.
6. Al redactar un nuevo correo electrónico, haga clic en el menú Seguridad y seleccione Firmar digitalmente este mensaje.

Puede ver más instrucciones sobre cómo usar certificados digitales en Mozilla Thunderbird aquí:

https://support.mozilla.org/en-US/kb/digitally-signing-and-encrypting-messages#w_sending-a-digitally-signed-and-or-encrypted-emai

Cifrar/Descifrar un correo electrónico

Podrías dar la parte de codificación a todos los que conoces. Cuando alguien quiere enviarte un mensaje secreto, usa tu clave pública que todo el mundo conoce para codificarla. Solo tu clave privada (que nunca debe compartirse con nadie) permitirá que el mensaje sea descifrado y leído. Un certificado digital le permite obtener, pero no enviar, correo electrónicos encriptados.

La comunicación bidireccional segura se logra cuando ambas partes de la comunicación tienen un certificado digital y cada una de ellas conoce la clave pública de la otra. Estas dos personas tienen ahora la misma capacidad y pueden enviarse mensajes cifrados entre si utilizando la clave pública del otro y descifrarlos con su propia clave privada (esta clave nunca debe ser entregada nadie).

Si dispone de un certificado digital de su país (en su tarjeta de identificación de ciudadano) o de su institución, intente utilizarlo para firmar sus correos electrónicos y cifrarlos para comprender la diferencia entre estos dos enfoques.