IFCT0109. SEGURIDAD INFORMÁTICA

MF0490_3 GESTIÓN DE SERVICIOS EN EL SISTEMA INFORMÁTICO

UD05

CONFECCIÓN DEL PROCESO DE MONITORIZACIÓN DE SISTEMAS Y COMUNICACIONES

DOCENTE: BENITO MANUEL GONZÁLEZ RODRÍGUEZ

CONTENIDOS

1. **INTRODUCCIÓN**
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

1. INTRODUCCIÓN

UNA **GESTIÓN Y MONITORIZACIÓN** DE LOS **SISTEMAS DE INFORMACIÓN ES FUNDAMENTAL** EN LA TOMA DE DECISIONES EN UNA ORGANIZACIÓN.

OTRO FACTOR IMPORTANTE ES EL **SISTEMA DE COMUNICACIONES,** RESPONSABLE DE HACER LLEGAR TODA LA INFORMACIÓN AL DESTINO ESPECIFICADO Y DE UN MODO CORRECTO.

UN ESTUDIO DEL SISTEMA DE COMUNICACIONES JUNTO CON SU MONITORIZACIÓN SERÁ VITAL PARA QUE LA INFORMACIÓN SEA ENVIADA Y SE PUEDA RECIBIR CORRECTAMENTE SIN INCURRIR EN PROBLEMAS DE SEGURIDAD.

1. INTRODUCCIÓN

SE VA A ESTUDIAR TODO **EL PROCESO DE ESTABLECIMIENTO DE UN BUEN SISTEMA DE COMUNICACIONES**, DESDE LOS DISPOSITIVOS HASTA LOS DISTINTOS PARÁMETROS QUE HAY QUE CONFIGURAR Y LAS DIVERSAS HERRAMIENTAS QUE SE PUEDEN UTILIZAR PARA OPTIMIZAR EL RENDIMIENTO DEL SISTEMA.

ESTOS SISTEMAS CONECTAN LA ORGANIZACIÓN CON EL EXTERIOR Y ELLO IMPLICA QUE HAYA **PELIGRO DE INTRUSIONES NO DESEADAS.**

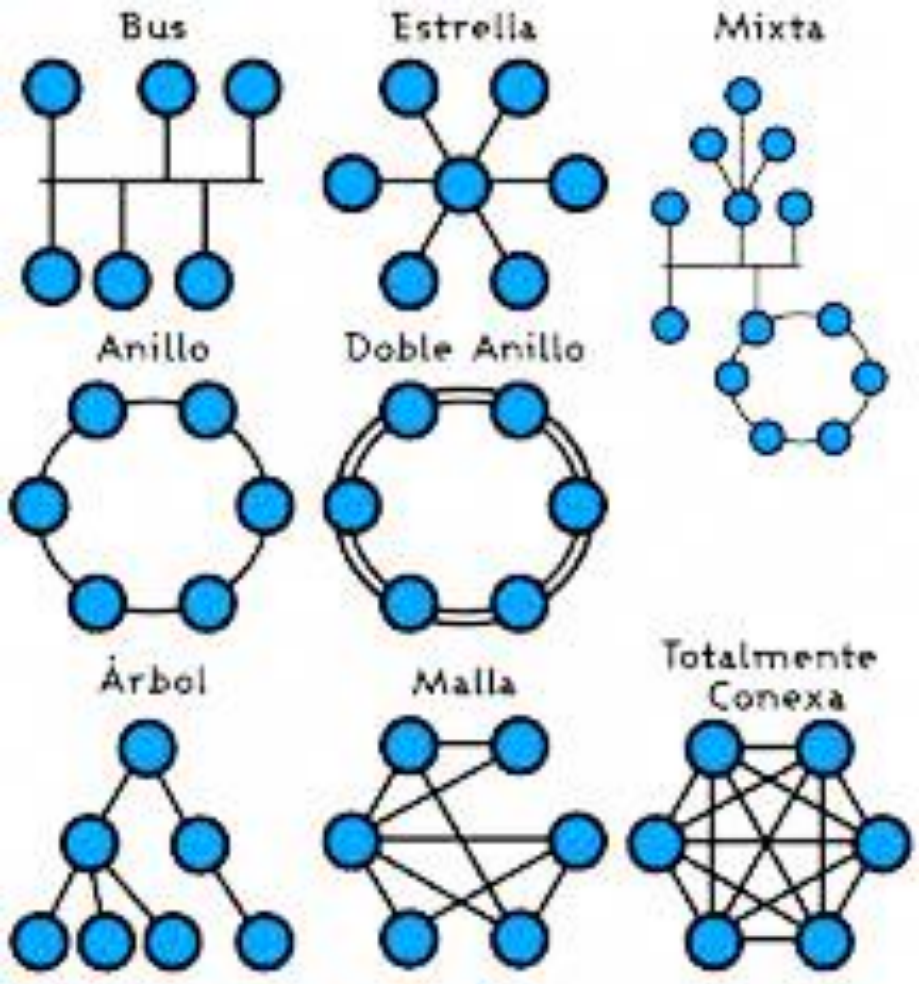
CONTENIDOS

1. INTRODUCCIÓN
2. **IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES**
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

UNA RED ES UN **CONJUNTO DE DISPOSITIVOS FÍSICOS (HARDWARE) Y DE PROGRAMAS (SOFTWARE) MEDIANTE EL CUAL SE COMUNICAN VARIOS ORDENADORES PARA COMPARTIR INFORMACIÓN**.

CADA UNO DE LOS ORDENADORES CONECTADOS A LA RED SE DENOMINA **NODO**.



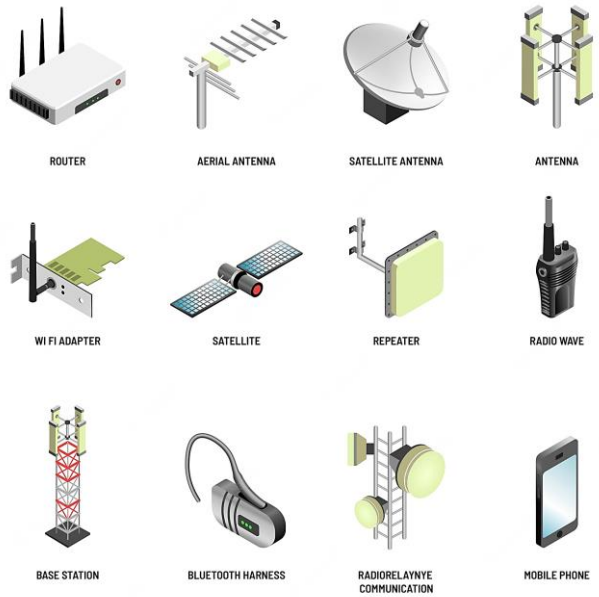
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

LOS **DISPOSITIVOS DE COMUNICACIÓN** SON LOS DISTINTOS **PERIFÉRICOS Y MEDIOS** QUE SON NECESARIOS **PARA LOGRAR QUE LOS ELEMENTOS DE UNA RED SE COMUNIQUEN** ENTRE ELLOS Y PUEDAN INTERCAMBIAR INFORMACIÓN

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

LOS DISPOSITIVOS DE RED SE CLASIFICAN EN TRES GRUPOS:

- **EQUIPOS DE RED**
- **MEDIOS DE COMUNICACIÓN**
- **CONECTORES**



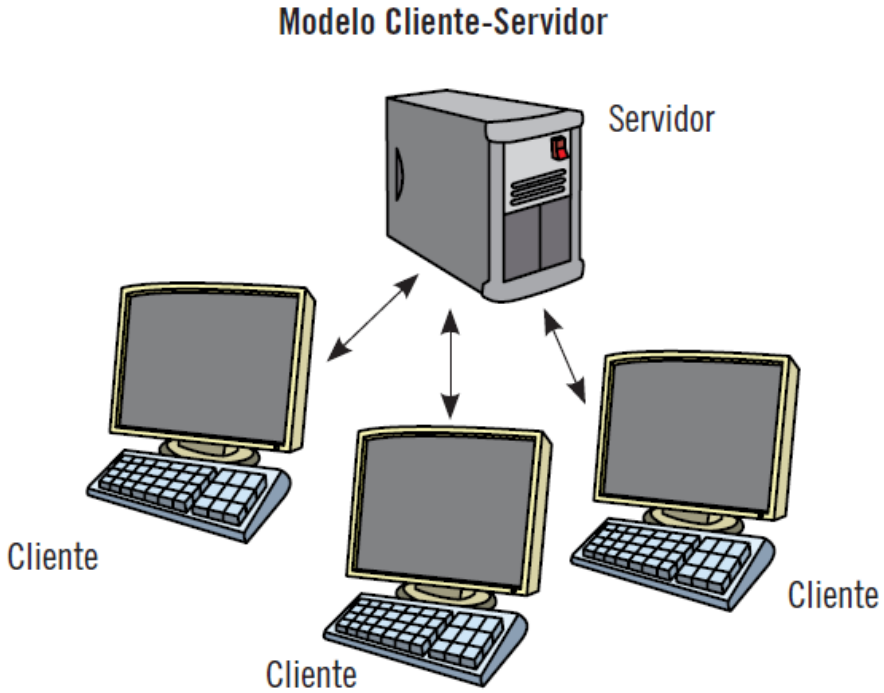
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

EQUIPOS DE RED

SON AQUELLOS COMPONENTES QUE EMITIRÁN Y RECIBIRÁN LA INFORMACIÓN

SERVIDORES

NODOS CUYA FUNCIÓN PRINCIPAL ES FACILITAR INFORMACIÓN COMO **RESPUESTA A SOLICITUDES EXTERNAS DE** OTROS NODOS, LLAMADOS **CLIENTES**.



ORDENADORES

COMPONENTES QUE EMITEN O RECIBEN LOS DATOS TRANSMITIDOS. SON LOS ELEMENTOS DE ORIGEN O DE FINALIZACIÓN DE LA TRANSMISIÓN.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

SON LOS DISPOSITIVOS DE LA RED A TRAVÉS DE LOS CUALES SE PRODUCE EL PROCESO DE COMUNICACIÓN DE DATOS.

Modem

Concentrador o Hub

Enrutador o router

Pasarela o gateway

Tarjeta de interfaz de red

Conmutador o switch

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

MÓDEMS

DISPOSITIVOS QUE PERMITEN A LOS NODOS COMUNICARSE ENTRE SÍ A TRAVÉS DE LÍNEAS TELEFÓNICAS MEDIANTE LA MODULACIÓN Y DEMODULACIÓN DE SEÑALES ELECTRÓNICAS QUE PUEDEN PROCESAR LOS ORDENADORES.

PUEDEN SER EXTERNOS O INTERNOS (INTEGRADOS EN EL ORDENADOR) Y HAY DE VARIOS TIPOS:

INALÁMBRICOS, ADSL, RDSI, USB, ETC.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

TARJETAS DE INTERFAZ DE RED (NIC, NETWORK INTERFACE CARD)

ELEMENTOS QUE CONECTAN EL ORDENADOR O EL SERVIDOR AL CABLE DE LA RED.

SON TARJETAS QUE MANTIENEN CONECTADA TODA LA RED LOCAL Y PERMITEN LA TRANSMISIÓN DE DATOS A ELEVADAS VELOCIDADES.

HAY VARIAS TIPOLOGÍAS DE TARJETAS DE INTERFAZ DE RED, DEBIENDO ELEGIR ENTRE UNA U OTRA SEGÚN EL TIPO DE RED EN LA QUE SE QUIERA IMPLANTAR.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

CONCENTRADORES O HUBS

COMPONENTES BÁSICOS DE LA RED QUE PERMITEN LA INTERCONEXIÓN DE VARIOS ORDENADORES O RECURSOS PARA FORMAR UNA RED.

PERMITEN CENTRALIZAR EL CABLEADO DE UNA RED Y PODER AMPLIARLA, ES DECIR, CON ESTOS DISPOSITIVOS SE RECIBE LA SEÑAL Y SE EMITE POR SUS DISTINTOS PUERTOS, HACIÉNDOLA LLEGAR A VARIOS ORDENADORES.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

REPETIDORES O REPEATERS

DISPOSITIVOS ELECTRÓNICOS QUE CONECTAN DOS TRAMOS DE RED.

SE ENCARGAN DE REGENERAR SEÑALES PARA EL MEDIO AL QUE ESTÁN CONECTADOS, DE MODO QUE SE AMPLIFICA LA SEÑAL DE LA RED, ELIMINANDO, ADEMÁS, LOS RUIDOS QUE GENERA.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

PUENTES O BRIDGES

DISPOSITIVOS QUE CONECTAN A NIVEL DE ENLACE REDES CON TOPOLOGÍAS Y PROTOCOLOS DIFERENTES.

TIENEN DOS O MÁS PUERTOS QUE SE UTILIZAN COMO REPETIDORES INTELIGENTES.

LOS PUENTES RECIBEN LA INFORMACIÓN Y LA ENVÍAN AL DESTINATARIO ASIGNADO, PERO EN CASO DE NO ENCONTRAR DESTINATARIO LA ENVÍAN A TODOS LOS DEMÁS PUERTOS Y ESPERAN HASTA QUE RECIBEN UNA RESPUESTA DEL DESTINO.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

CONMUTADORES O SWITCHES

DISPOSITIVOS QUE OFRECEN LAS MISMAS POSIBILIDADES DE INTERCONEXIÓN QUE LOS CONCENTRADORES, PERO DE UN MODO MÁS EFICIENTE, MEJORANDO EL RENDIMIENTO GLOBAL DE LA RED.

A DIFERENCIA DE LOS HUBS, QUE DIFUNDEN LA INFORMACIÓN A TODOS LOS PUESTOS DE LA RED, LOS SWITCHES SOLO LA ENVÍAN AL DESTINATARIO DESEADO.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

ENRUTADORES O ROUTERS

DISPOSITIVOS DE RED QUE CONECTAN UNAS REDES CON OTRAS UTILIZANDO EXCLUSIVAMENTE UN PROTOCOLO IP, CONFIGURADO PARA ELEGIR LA RUTA ÓPTIMA ENTRE EL EMISOR Y EL DESTINATARIO.

LA COMUNICACIÓN DE LOS DATOS LA REALIZAN INTENTANDO LOCALIZAR LA RUTA MÁS EFICIENTE PARA ENTREGAR LA INFORMACIÓN AL EQUIPO DESTINATARIO.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

MEDIOS DE COMUNICACIÓN

PASARELAS, PUERTAS DE ENLACE O GATEWAYS

DISPOSITIVOS CUYA FINALIDAD PRINCIPAL ES INTERCONECTAR REDES CON PROTOCOLOS Y ARQUITECTURAS DIFERENTES A TODOS LOS NIVELES DE COMUNICACIÓN.

TRADUCEN LA INFORMACIÓN DEL PROTOCOLO DE LA RED QUE EMITE LOS DATOS AL PROTOCOLO DE LA RED RECEPTORA

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

CONECTORES

LOS CONECTORES SON EL CONJUNTO DE COMPONENTES QUE CONECTAN LOS EQUIPOS DE RED Y LOS MEDIOS DE COMUNICACIÓN. SON LOS COMPONENTES A TRAVÉS DE LOS QUE "VIAJA" LA INFORMACIÓN.

HAY VARIOS TIPOS DE COMPONENTES DISTINTOS:

- **SISTEMA DE CABLEADO**
- **CABLEADO DE FIBRA ÓPTICA**
- **ENLACES INALÁMBRICOS**

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

CONECTORES

SISTEMA DE CABLEADO

ESTRUCTURA DE CABLES QUE SE UTILIZAN PARA CONECTAR ENTRE SÍ LOS DISTINTOS RECURSOS, COMPONENTES Y ESTACIONES DE TRABAJO QUE FORMAN PARTE DE UNA RED.

CABLEADO DE FIBRA ÓPTICA

TIPO DE CABLEADO ESPECIAL POR EL QUE LOS DATOS SE TRANSMITEN A TRAVÉS DE LA LUZ. ESTE TIPO DE CABLEADO PERMITE LA TRANSMISIÓN DE UN MAYOR VOLUMEN DE DATOS, A MÁS VELOCIDAD Y ELIMINANDO AL COMPLETO LAS INTERFERENCIAS ELECTROMAGNÉTICAS DE LOS OTROS TIPOS DE CABLES. ES EL MEDIO DE TRANSMISIÓN MÁS UTILIZADO EN ALGUNOS TIPOS DE REDES.

2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES

CONECTORES

ENLACES INALÁMBRICOS

ENLACES QUE PERMITEN LA TRANSMISIÓN DE LA INFORMACIÓN A TRAVÉS DE ONDAS ELECTROMAGNÉTICAS SIN NECESIDAD DE TENER UNA CONEXIÓN FÍSICA.

CON LOS ENLACES INALÁMBRICOS SE REDUCE LOS COSTES DE INSTALACIÓN DE LA RED, AL EVITAR LA INSTALACIÓN DE GRAN PARTE DEL CABLEADO FÍSICO DE LA MISMA, Y SON MÁS FLEXIBLES QUE LAS REDES CON CABLEADO, PORQUE PERMITEN AGREGAR NODOS A UNA RED EXISTENTE Y DESPLAZAR LOS EQUIPOS DENTRO DE UNA ZONA DELIMITADA SIN QUE QUEDE AFECTADA LA TRANSMISIÓN DE LOS DATOS.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. **ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES**
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

PROTOCOLO

UN SERVICIO DE COMUNICACIÓN ES LA ACTIVIDAD FINAL A LA QUE SE DESTINA LA INFORMACIÓN RECIBIDA EN UN DISPOSITIVO DE DESTINO.

PARA QUE LAS DISTINTAS ENTIDADES SE COMUNIQUEN ENTRE ELLAS Y TRANSMITAN LA INFORMACIÓN **ES NECESARIO SEGUIR UN CONJUNTO DE NORMAS Y REGLAS ESTABLECIDAS.**

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

PROTOCOLO

AL CONJUNTO DE NORMAS Y REGLAS ESTABLECIDAS QUE PERMITE LA COMUNICACIÓN ENTRE VARIAS ENTIDADES SE LE DENOMINA **PROTOCOLO**.

EL PROTOCOLO **DEFINE LA FORMA EN LA QUE LA INFORMACIÓN CIRCULA EN UNA RED DE ORDENADORES.**

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

PROTOCOLO

LOS PROTOCOLOS DE COMUNICACIÓN POSIBILITAN QUE HAYA FLUJO DE INFORMACIÓN ENTRE EQUIPOS QUE UTILIZAN LENGUAJES DISTINTOS.

DOS ORDENADORES QUE UTILICEN PROTOCOLOS DISTINTOS NO PODRÁN ESTABLECER UNA COMUNICACIÓN ENTRE ELLOS.

PARA QUE ESO SEA POSIBLE, ES NECESARIO QUE AMBOS EQUIPOS UTILICEN UN MISMO LENGUAJE, LO QUE SE CONSIGUE CON EL **PROTOCOLO**.

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

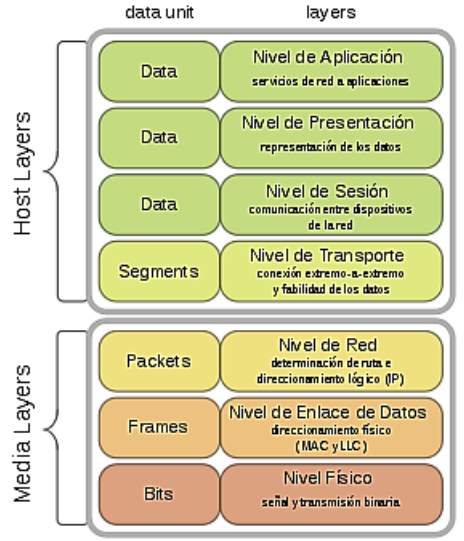
PROPIEDADES DE LOS PROTOCOLOS

- DETECCIÓN DE LA CONEXIÓN FÍSICA SOBRE LA QUE SE REALIZA LA CONEXIÓN
- DEFINICIÓN DE LOS PASOS NECESARIOS PARA COMUNICARSE (HANDSHAKING)
- NEGOCIACIÓN DE LAS CARACTERÍSTICAS DE LA CONEXIÓN
- CÓMO INICIAR Y CÓMO TERMINAR UN MENSAJE
- DETERMINACIÓN DEL PROCEDIMIENTO DE FORMATEO DE LOS MENSAJES
- DEFINICIÓN DEL SISTEMA DE CORRECCIÓN DE ERRORES QUE SE VA A UTILIZAR
- CÓMO DETECTAR LA PÉRDIDA INESPERADA DE LA CONEXIÓN Y QUÉ HACER
- DETERMINACIÓN DE LA TERMINACIÓN DE LA SESIÓN/CONEXIÓN
- DEFINICIÓN DE LAS ESTRATEGIAS QUE GARANTIZARÁN LA SEGURIDAD DE LA COMUNICACIÓN CON TÉCNICAS COMO AUTENTICACIÓN O CIFRADO
- CÓMO SE CONSTRUYE UNA RED FÍSICA
- CÓMO LOS DISTINTOS ORDENADORES SE CONECTAN A LA RED

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI

EL PRIMER PASO PARA LA ESTANDARIZACIÓN INTERNACIONAL DE LOS PROTOCOLOS NECESARIOS PARA ESTABLECER UNA COMUNICACIÓN DE RED SE HIZO EN **1978,** CUANDO **LA INTERNATIONAL STANDARDS ORGANIZATION (ISO)** INTRODUJO EL MODELO **OSI (OPEN SYSTEM INTERCONECTION O MODELO DE INTERCONEXIÓN DE SISTEMAS ABIERTOS)**



3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI

HAY UNA SERIE DE **PRINCIPIOS** QUE FUERON LOS QUE FORMULARON LA CREACIÓN DEL MODELO:

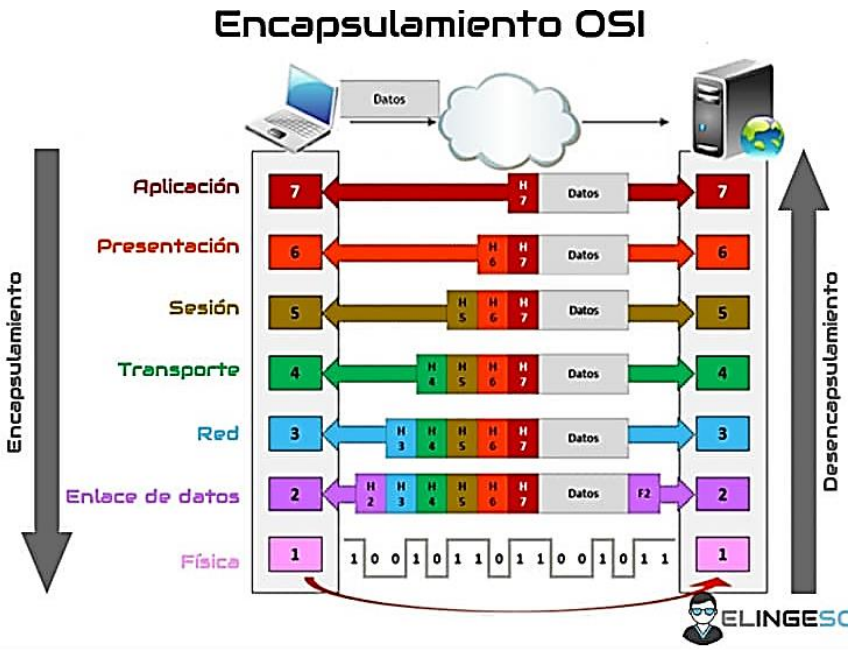
- CADA CAPA SE REFIERE A UN NIVEL DE ABSTRACCIÓN DISTINTO.
- CADA CAPA TIENE QUE REALIZAR UNA FUNCIÓN DEFINIDA CON CLARIDAD.
- LA FUNCIÓN DE CADA CAPA SE DEBE DEFINIR TOMANDO EN CONSIDERACIÓN QUE SE ESTÁ CREANDO LA DEFINICIÓN DE PROTOCOLOS ESTANDARIZADOS.
- EL NÚMERO DE CAPAS TIENE QUE SER LO SUFICIENTEMENTE PEQUEÑO PARA QUE LA ARQUITECTURA NO SEA DIFÍCIL DE GESTIONAR, PERO TAMBIÉN LO SUFICIENTEMENTE GRANDE PARA QUE CADA FUNCIÓN DISTINTA DE LA ARQUITECTURA SE REALICE EN UNA CAPA.
- LOS LÍMITES DE CADA CAPA DEBEN FACILITAR EL FLUJO DE LA INFORMACIÓN MEDIANTE LA UTILIZACIÓN DE LAS INTERFACES.

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI

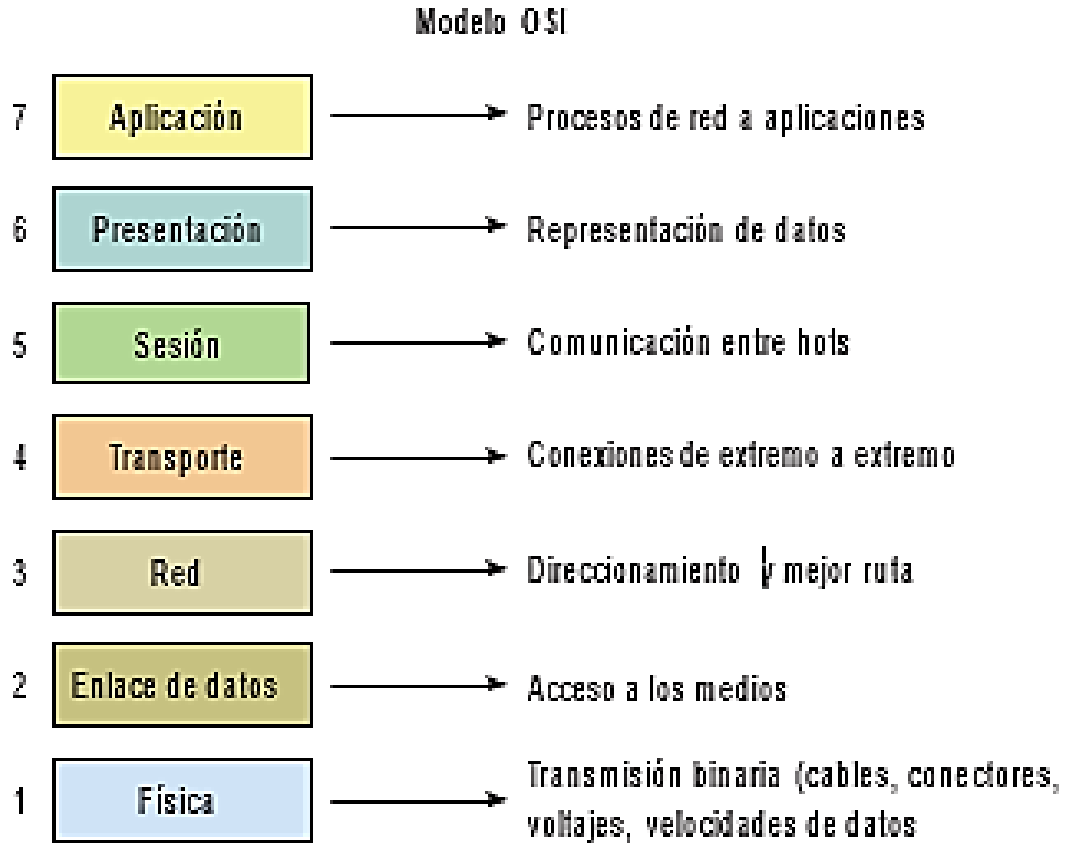
ESTE MODELO ES EN LA ACTUALIDAD UN MARCO DE REFERENCIA PARA LA DEFINICIÓN DE ARQUITECTURAS EN LA INTERCONEXIÓN DE LOS SISTEMAS DE COMUNICACIONES.

ESTÁ FORMADO POR **SIETE NIVELES (CAPAS),** CADA UNO DE ELLOS CONSTITUIDO POR UN CONJUNTO ESPECÍFICO DE **FUNCIONES** DE RED ASIGNADO Y CON UNA SERIE DE DIRECTRICES DE IMPLEMENTACIÓN DE LAS **INTERFACES** ENTRE CAPAS.



3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI



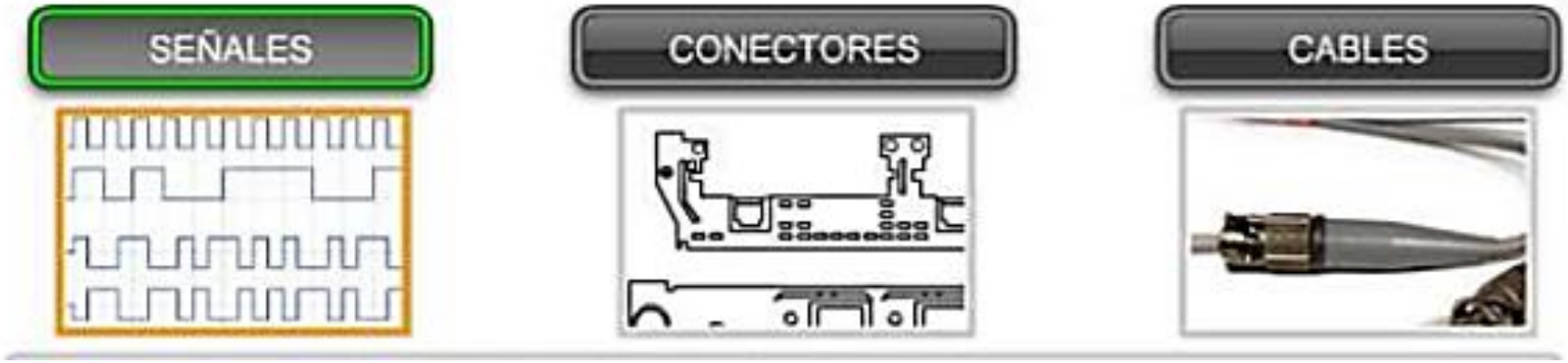
MODELO OSI	
NIVEL – CAPA	DESCRIPCIÓN
FÍSICA	Se ocupa de transmitir el flujo de bits a través del medio (cables, tarjetas y repetidores).
ENLACE	Divide el flujo de bits en unidades con formato mediante el uso de protocolos (puentes -bridges-).
RED	Establece las comunicaciones y determina la ruta de los datos en la red (enrutador -router-).
TRANSPORTE	Asegura la correcta recepción de la información.
SESIÓN	Establece, mantiene y finaliza la comunicación entre las aplicaciones en el momento apropiado.
PRESENTACIÓN	Convierte las distintas representaciones de datos para que puedan ser entendibles por el usuario.
APLICACIÓN	Ofrece a las aplicaciones la posibilidad de acceder a los servicios de red para realizar el trabajo encomendado.

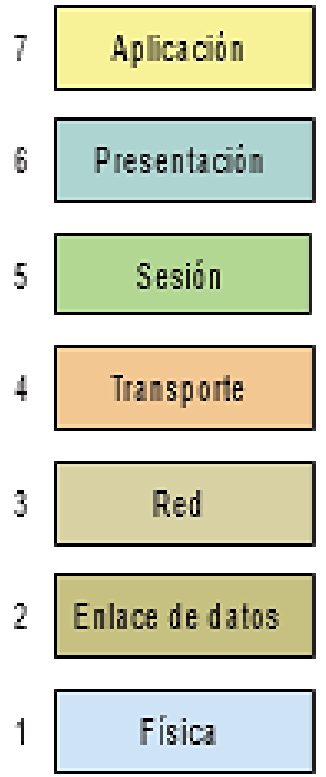
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. CAPA 1. FÍSICA

LA CAPA FÍSICA ES LA ENCARGADA DE LA TOPOLOGÍA DE LA RED Y DE LAS CONEXIONES FÍSICAS DEL EQUIPO CON LA RED.

EN ELLA **SE DEFINEN LAS CARACTERÍSTICAS DEL MEDIO FÍSICO** (TIPO DE CONECTORES, TIPO DE CABLE, **ETC.) Y EL MODO EN EL QUE SE TRANSMITIRÁ LA INFORMACIÓN**.



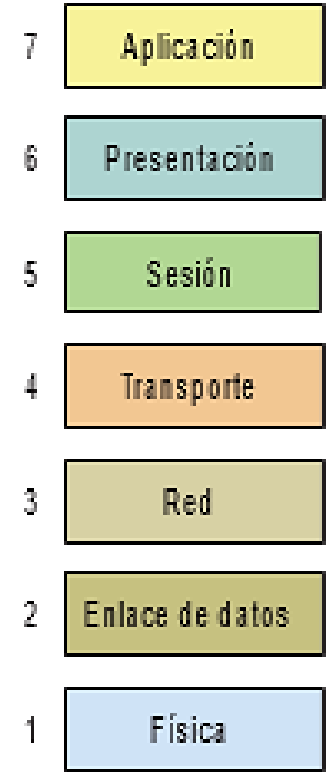


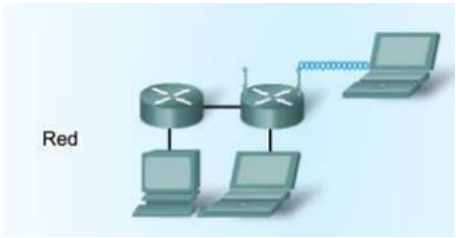
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. CAPA 2. ENLACE DE DATOS

LA CAPA DE ENLACE DE DATOS ES UNA DE LAS MÁS IMPORTANTES, YA QUE EN ELLA SE REGULA LA FORMA DE LA CONEXIÓN QUE HABRÁ ENTRE LOS EQUIPOS.

ESTA CAPA **SE ENCARGA DE DAR A LAS CAPAS SUPERIORES ACCESO A LOS MEDIOS, DE CONTROLAR LA UBICACIÓN Y RECEPCIÓN DE LOS DATOS EN LOS MEDIOS Y DE LA DETECCIÓN DE ERRORES EN LA DISTRIBUCIÓN DE LOS DATOS POR TRAMAS**.



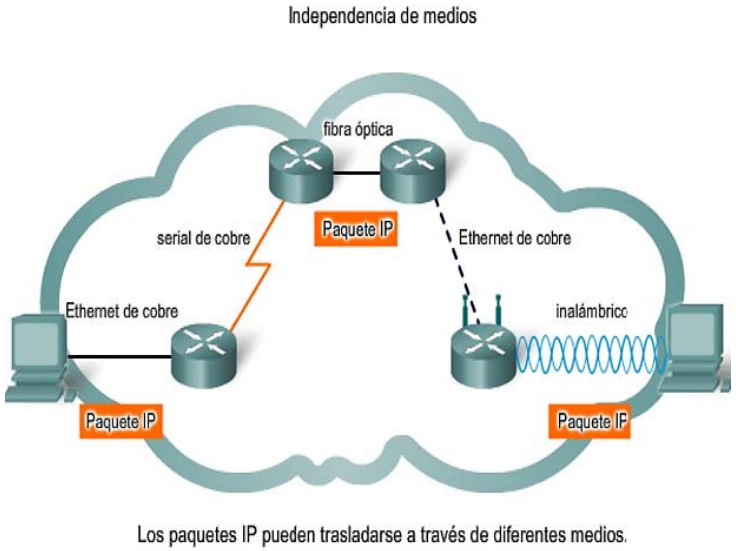


3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

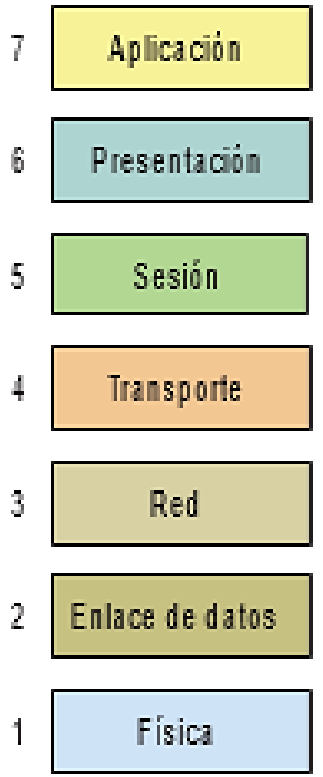
EL MODELO OSI. CAPA 3. RED

RESPONSABLE DE IDENTIFICAR EL ENRUTAMIENTO ENTRE UNA O VARIAS REDES Y DEL ENVÍO DE ENTRE REDES.

SE ENCARGA DE ESTABLECER, MANTENER Y TERMINAR LAS CONEXIONES (ENCARGARSE DE QUE LOS DATOS LLEGUEN DESDE SU PUNTO DE ORIGEN AL DESTINO MARCADO).



Los paquetes IP pueden trasladarse a través de diferentes medios.

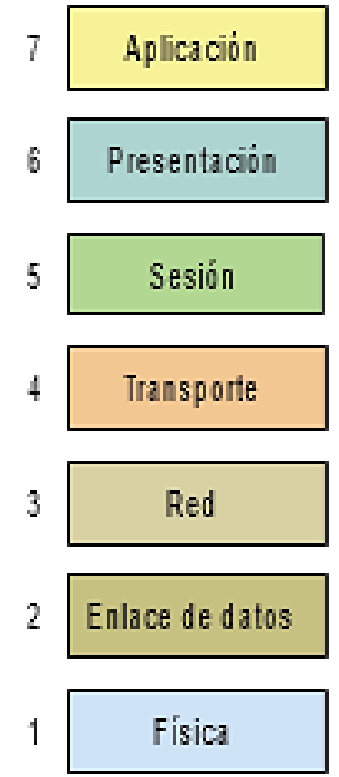


3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. CAPA 4. TRANSPORTE

LA FUNCIÓN PRINCIPAL ES **TRASLADAR LOS DATOS, ASEGURANDO QUE ESTOS LLEGAN CORRECTAMENTE DEL ORIGEN AL DESTINO,** INDEPENDIENTEMENTE DEL TIPO DE RED FÍSICA QUE SE UTILICE.

ACTÚA COMO **PUENTE ENTRE LOS TRES NIVELES INFERIORES** (ORIENTADOS A LAS COMUNICACIONES) **Y LOS TRES NIVELES SUPERIORES** (ORIENTADOS AL PROCESAMIENTO DE LA INFORMACIÓN).

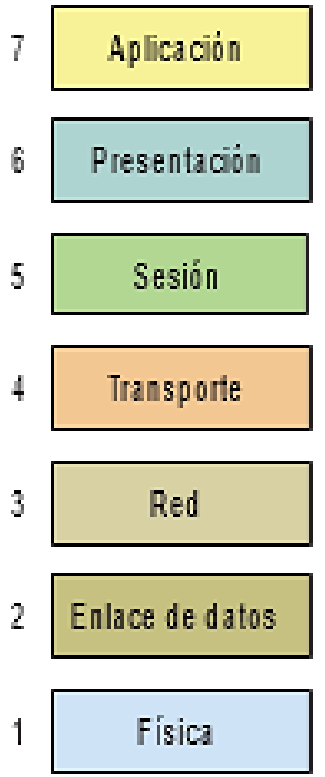


3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. CAPA 5. SESIÓN

SE ENCARGA DE ESTABLECER, GESTIONAR Y TERMINAR LAS CONEXIONES ENTRE LOS USUARIOS FINALES: MANTIENE Y CONTROLA EL ENLACE ESTABLECIDO ENTRE DOS EQUIPOS QUE TRANSMITEN DATOS DE CUALQUIER TIPO.

ASEGURA QUE SE MANTENGA LA COMUNICACIÓN ENTRE DOS EQUIPOS, PERMITIENDO SU REANUDACIÓN EN CASO DE HABER ALGÚN TIPO DE INTERRUPCIÓN.



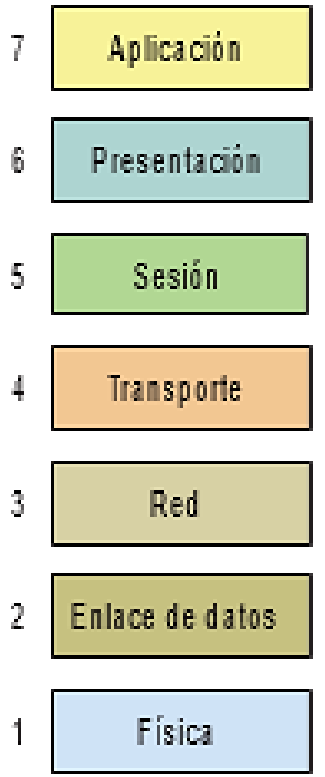
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. CAPA 6. PRESENTACIÓN

PROPORCIONA EL MISMO FORMATO A TODOS LOS DATOS AUNQUE PROVENGAN DE EQUIPOS DISTINTOS CON FORMATO DISTINTO.

TRABAJA MÁS CON EL CONTENIDO DE LA COMUNICACIÓN QUE CON LA MANERA EN LA QUE SE ESTABLECE LA MISMA.

EN LA CAPA DE PRESENTACIÓN SE TRATAN ASPECTOS COMO LA SEMÁNTICA Y LA SINTAXIS DE LOS DATOS TRANSMITIDOS, ACTUANDO COMO TRADUCTORA.

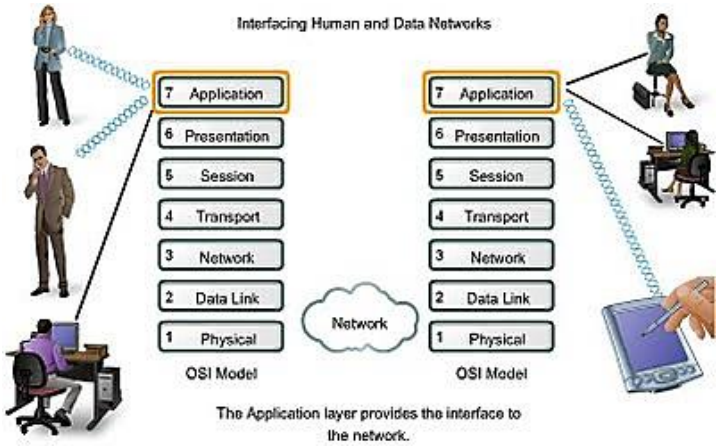


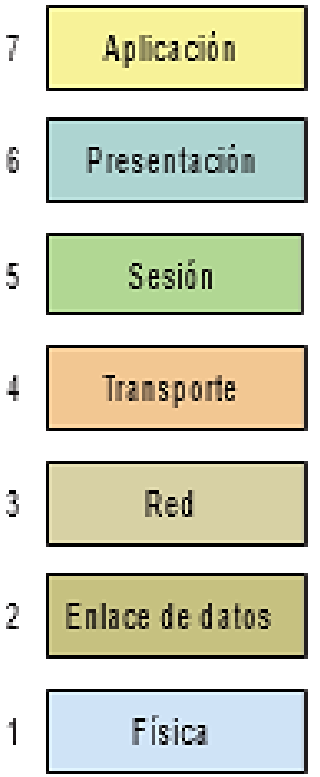
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. CAPA 7. APLICACIÓN

ES LA ENCARGADA DE FACILITAR SERVICIOS A LOS USUARIOS. SE RESPONSABILIZA DE GESTIONAR LOS PAQUETES DE DATOS DE LAS APLICACIONES PARA QUE PUEDAN ACCEDER A LAS APLICACIONES DE RED.

TAMBIÉN **SE ENCARGA DE DEFINIR LOS PROTOCOLOS QUE COMUNICAN LAS APLICACIONES CON LOS SERVICIOS DE RED PARA EL INTERCAMBIO DE DATOS**.



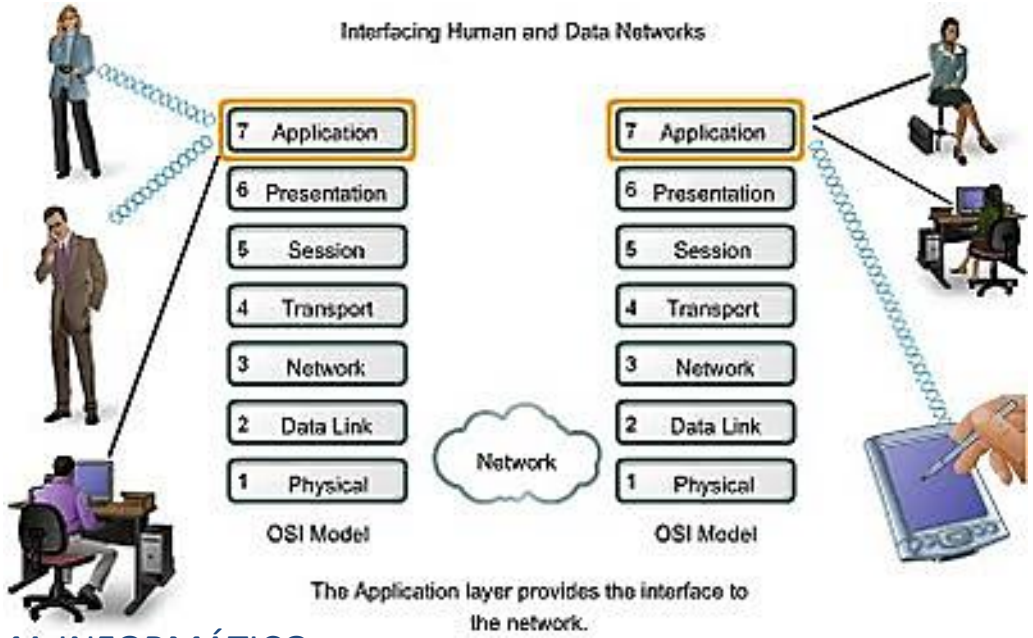


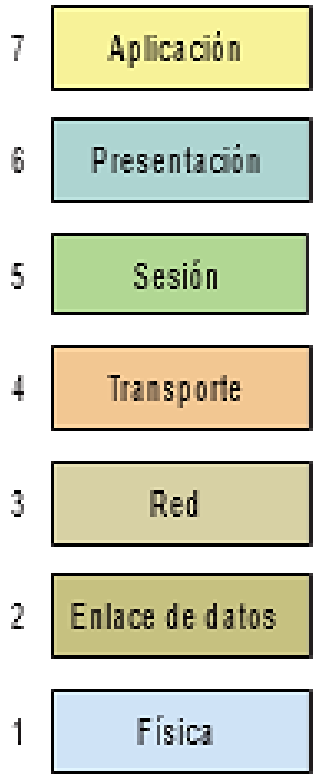
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. CAPA 7. APLICACIÓN

EL USUARIO NO INTERACTÚA DIRECTAMENTE CON EL NIVEL DE APLICACIÓN.

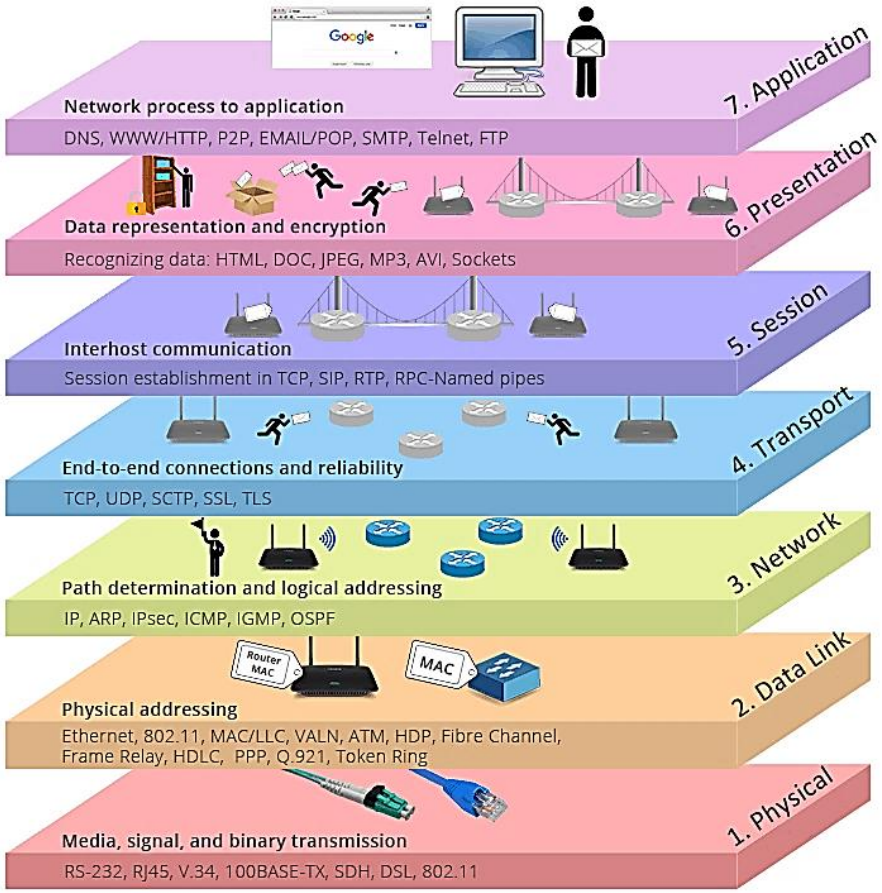
LO HABITUAL ES QUE INTERACTÚE CON APLICACIONES QUE SEAN LAS QUE TRATEN DIRECTAMENTE CON EL NIVEL DE APLICACIÓN



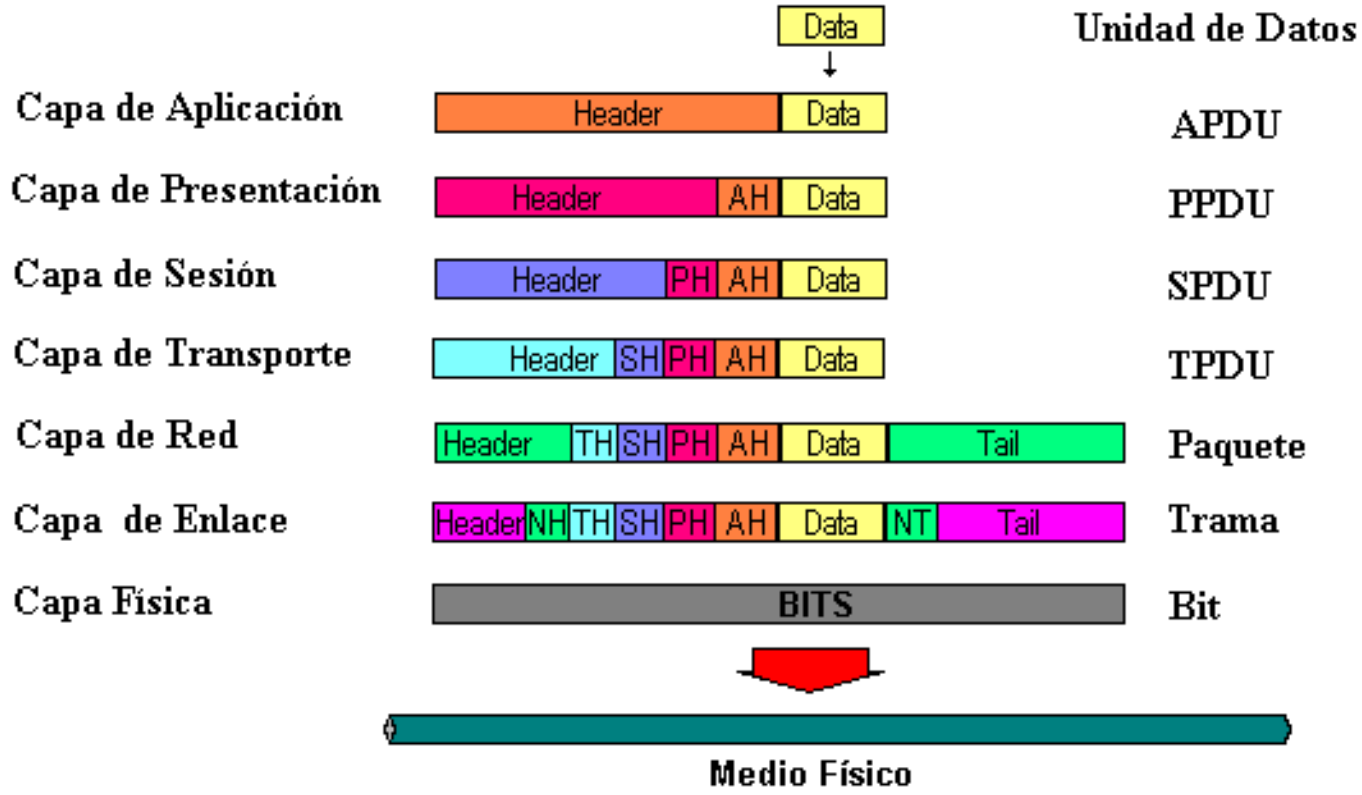


3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

EL MODELO OSI. PROTOCOLOS Y ENCAPSULAMIENTO



PROTOCOLOS



ENCAPSULAMIENTO

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

LA ARQUITECTURA TCP/IP Y SU COMPARACIÓN CON EL MODELO OSI

TAMBIÉN ES UN MODELO DE DESCRIPCIÓN DE PROTOCOLOS DE RED.

SE CREÓ EN **1970** Y SE DESARROLLÓ POR ENCARGO DE UNA AGENCIA DEL DEPARTAMENTO DE DEFENSA DE LOS ESTADOS UNIDOS, SIENDO PREDECESOR DE LA ACTUAL RED **INTERNET**.

ESTE MODELO TAMBIÉN DESCRIBE UN CONJUNTO DE GUÍAS GENERALES DE DISEÑO E IMPLEMENTACIÓN DE PROTOCOLOS DE RED, QUE PERMITE LA COMUNICACIÓN ENTRE VARIOS EQUIPOS DENTRO DE UNA MISMA RED. EN ÉL SE INDICA CÓMO LOS DATOS DEBERÍAN SER FORMATEADOS, DIRECCIONADOS, TRANSMITIDOS, ENRUTADOS Y RECIBIDOS POR EL EQUIPO DESTINATARIO.

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

LA ARQUITECTURA TCP/IP Y SU COMPARACIÓN CON EL MODELO OSI

MIENTRAS QUE EL MODELO OSI TIENE SIETE CAPAS, EL **MODELO TCP/IP TIENE** SOLO **CUATRO CAPAS**:

CAPA 1 O CAPA DE ACCESO AL MEDIO

DEFINE LAS RUTINAS PARA ACCEDER AL MEDIO FÍSICO. SE CORRESPONDE CON LAS CAPAS **1 Y 2** DEL MODELO **OSI**.

CAPA 2 O CAPA DE INTERNET

DEFINE EL DATAGRAMA Y GESTIONA EL ENRUTAMIENTO DE LA INFORMACIÓN. ES SIMILAR A LA CAPA **3** DEL MODELO **OSI**.

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

LA ARQUITECTURA TCP/IP Y SU COMPARACIÓN CON EL MODELO OSI

CAPA 3 O CAPA DE TRANSPORTE

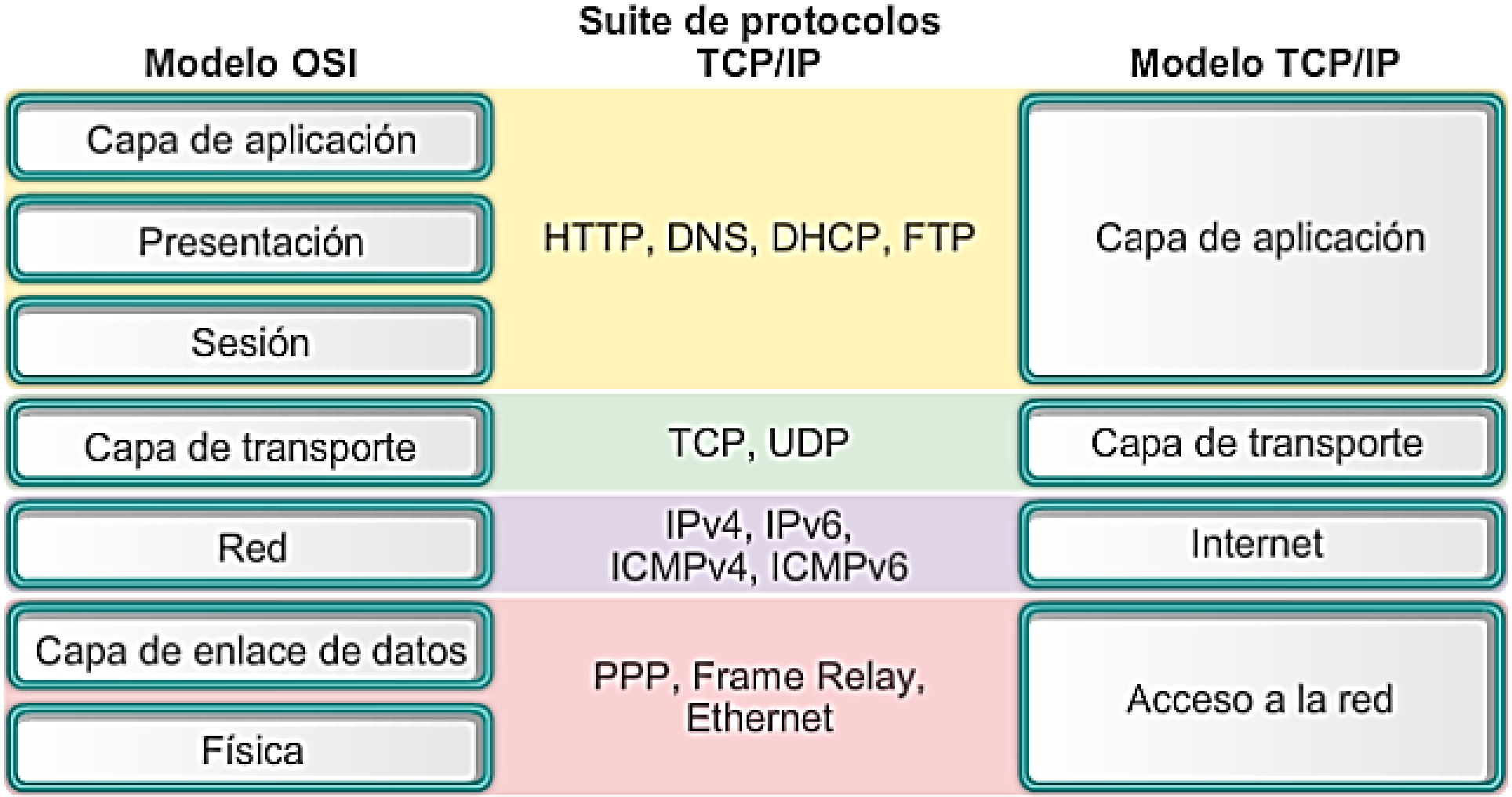
SE OCUPA DE LOS SERVICIOS DE ENTREGA DE LOS DATOS ENTRE LOS NODOS QUE FORMAN PARTE DE LA RED. ES SIMILAR A LA CAPA **4** DEL MODELO **OSI**.

CAPA 4 O CAPA DE APLICACIÓN

CAPA EN LA QUE SE DEFINEN Y GESTIONAN LAS APLICACIONES Y LOS PROCESOS QUE ESTÁN UTILIZANDO LA RED. MANEJA ASPECTOS DE REPRESENTACIÓN, CONTROL, CODIFICACIÓN Y CONTROL DE DIÁLOGO. ES ASIMILABLE A LAS CAPAS **5, 6** Y **7** DEL MODELO **OSI.**

3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES

LA ARQUITECTURA TCP/IP Y SU COMPARACIÓN CON EL MODELO OSI



CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. **PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES**
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

LA ARQUITECTURA **TCP/IP** EN LA PRÁCTICA ES LA MÁS UTILIZADA EN LA ACTUALIDAD. CONSTA DE CUATRO CAPAS Y CADA UNA PROPORCIONA UNA SERIE DE SERVICIOS CONCRETOS A LOS PROTOCOLOS DE LAS CAPAS SUPERIORES PARA QUE SE PRODUZCA UNA CORRECTA TRANSMISIÓN DE LA INFORMACIÓN.

CADA CAPA DEL MODELO **TCP/IP** INCORPORA SERVICIOS DE:

- CONTROL DE ERRORES
- CONTROL DEL FLUJO DE DATOS
- FRAGMENTACIÓN
- GESTIÓN DEL ESTABLECIMIENTO DE LA CONEXIÓN
- DIRECCIONAMIENTO
- MULTIPLEXACIÓN
- NOMENCLATURA

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

EL PROTOCOLO **TCP/IP** ESTÁ FORMADO POR DOS PROTOCOLOS:

PROTOCOLO DE CONTROL DE TRANSMISIÓN (TCP)

ES UN PROTOCOLO DE LA CAPA DE TRANSPORTE QUE SE ENCARGA DE ASEGURAR QUE SE RECIBE EXACTAMENTE LO QUE SE HA ENVIADO Y QUE EL ENVÍO SE HA REALIZADO CORRECTAMENTE

PROTOCOLO DE INTERNET (IP)

ES EL PROTOCOLO DE LA CAPA DE RED QUE PERMITE QUE LAS APLICACIONES SE EJECUTEN SOBRE REDES INTERCONECTADAS

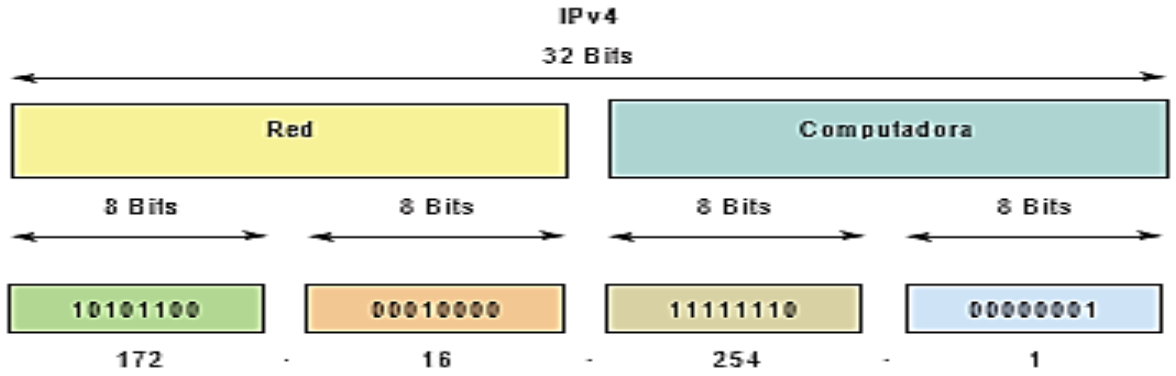
PERMITE LA DISTINCIÓN ÚNICA DE TODOS LOS ORDENADORES CONECTADOS A INTERNET OTORGÁNDOLES UNA **DIRECCIÓN IP PROPIA**

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

LA VERSIÓN ACTUAL DEL PROTOCOLO IP ES LA **4 (IPV4).** ESTA VERSIÓN YA SE ESTÁ AGOTANDO Y COMO SOLUCIÓN SE HA CREADO LA VERSIÓN A **(IPV6),** YA FINALIZADA Y EN SUS PRIMERAS FASES DE IMPLEMENTACIÓN.

LAS DIRECCIONES **IPV4** SE COMPONEN DE **32** BITS, AGRUPADOS EN **4** GRUPOS DE **8.** LOS GRUPOS DE **8** BITS GENERAN UN NÚMERO DECIMAL QUE TOMA VALORES ENTRE **0** Y **255**

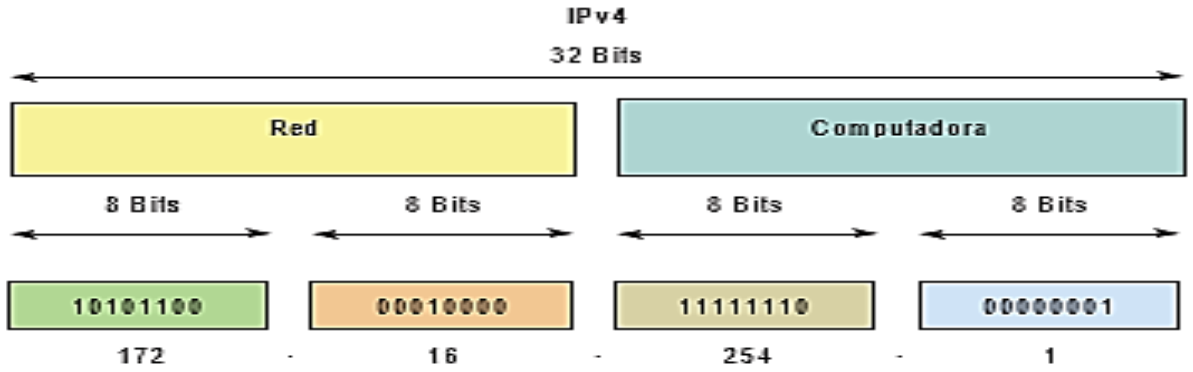


4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

LA DIRECCIÓN IPV4 SE DIVIDE EN DOS PARTES:

- IDENTIFICADOR DE LA RED DONDE SE ENCUENTRA EL EQUIPO
- IDENTIFICADOR DEL EQUIPO EN LA RED (HOST)



EL MODO EN EL QUE LOS BITS SE DISTRIBUYEN ENTRE EL IDENTIFICADOR DE LA RED Y EL IDENTIFICADOR DEL EQUIPO HACE DISTINGUIR LAS DIRECCIONES IPV4 ENTRE VARIAS CLASES

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

CLASE A

LOS 8 PRIMEROS BITS (QUE ES LO MISMO QUE 1 BYTE) IDENTIFICAN LA RED Y LOS 24 RESTANTES (3 BYTES) IDENTIFICAN AL EQUIPO DE LA RED

CLASE B

LOS 16 PRIMEROS BITS (2 BYTES) IDENTIFICAN LA RED Y LOS OTROS 16 AL EQUIPO

CLASE C

LOS 24 PRIMEROS BITS CORRESPONDEN A LA IDENTIFICACIÓN DE LA RED Y LOS OTROS 8 A LA IDENTIFICACIÓN DEL EQUIPO

CLASE D

DIRECCIONES IP QUE ENVÍAN LA INFORMACIÓN A VARIAS INTERFACES DISTINTAS

CLASE E

DIRECCIONES IP RESERVADAS PARA SU USO EN INVESTIGACIÓN

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

Clase	Rango	Nº redes	Nº host por red	Máscara de subred	Dirección broadcast	Uso
A	0.0.0.0-127.255.255.255	128	16777214	255.0.0.0	x.255.255.255	Redes grandes
B	128.0.0.0-191.255.255.255	16384	65534	255.255.0.0	x.x.255.255	Redes medianas
C	192.0.0.0-223.255.255.255	2097152	254	255.255.255.0	x.x.x.255	Redes pequeñas
D	224.0.0.0-239.255.255.255	Histórico				Multicast
E	240.0.0.0-255.255.255.255	Histórico				Investigación

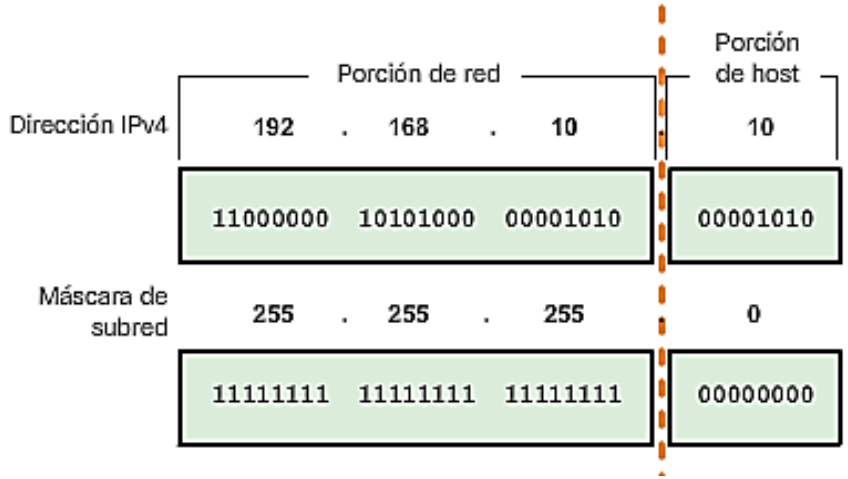
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

LA **MÁSCARA DE SUBRED** ES AQUELLA QUE **PERMITE DISTINGUIR LOS BITS QUE IDENTIFICAN LA RED Y LOS QUE IDENTIFICAN EL HOST DE UNA DIRECCIÓN IP**.

SU FUNCIÓN PRINCIPAL ES PERMITIR DIFERENCIAR LOS BITS DE LA RED Y LOS BITS DEL HOST.

ESTÁ **FORMADA TAMBIÉN POR 32 BITS, DE LOS CUALES TENDRÁN VALOR 1 AQUELLOS QUE IDENTIFIQUEN LA RED Y VALOR 0 AQUELLOS QUE IDENTIFIQUEN AL HOST**.



4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

PARÁMETROS BÁSICOS PARA CONFIGURAR UNA RED:

DIRECCIÓN BROADCAST

DIRECCIÓN QUE SIRVE PARA ENVIAR UN PAQUETE A TODOS LOS HOSTS DE UNA RED.

ESTA DIRECCIÓN TIENE LOS BITS CORRESPONDIENTES A HOST IGUALES A 1.

DIRECCIÓN IP DE LA PUERTA DE ENLACE

ES LA DIRECCIÓN DEL ROUTER DE LA RED.

PUEDE TOMAR CUALQUIERA DE LAS DIRECCIONES DE UN RANGO.

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

DIRECCIÓN DE RED

DIRECCIÓN QUE TIENE LOS BITS DE HOST IGUALES A CERO.

SIRVE PARA DEFINIR LA RED EN LA QUE SE UBICA.

DIRECCIÓN DE BUCLE LOCAL O LOOPBACK

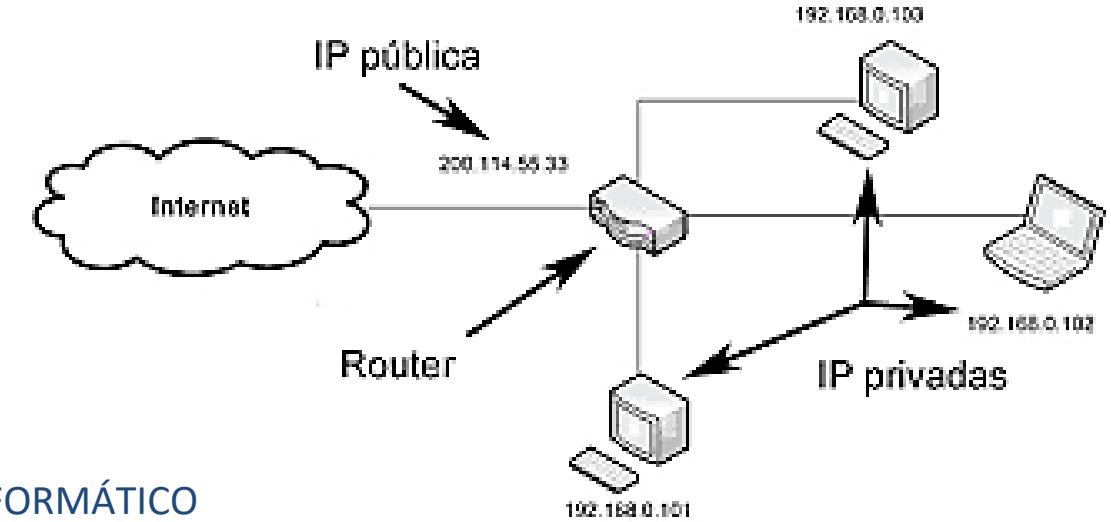
SON DIRECCIONES “127.X.X.X” QUE SE RESERVAN PARA DESIGNAR LA PROPIA MÁQUINA.

SE SUELEN UTILIZAR PARA COMPROBAR LAS PROPIAS INTERFACES DE RED.

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

DIRECCIÓN IPV4

TAMBIÉN SE DISTINGUE ENTRE DIRECCIONES DE RED PÚBLICAS Y PRIVADAS. UNA RED LOCAL SE IDENTIFICA EN INTERNET CON UNA SOLA **DIRECCIÓN IP PÚBLICA** (ASIGNADA POR EL PROVEEDOR DE ACCESO A INTERNET) Y LOS DISPOSITIVOS QUE COMPONEN ESTA RED SE IDENTIFICAN ENTRE SÍ MEDIANTE **DIRECCIONES IP PRIVADAS** (DIRECCIONES INTERNAS).



4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

CONFIGURACIÓN DE UNA RED IPV4

UNA VEZ INSTALADA TODA LA RED FÍSICA EN CUANTO A EQUIPOS, CONECTORES Y MEDIOS, SE PUEDE PROCEDER A SU CONFIGURACIÓN SIGUIENDO UNA SERIE DE PASOS:

1. LO MÁS HABITUAL ES QUE SEA **TCP/IP.**
2. DEFINIR LOS DISTINTOS PARÁMETROS DEL PROTOCOLO, QUE SERÁN:
   A. DIRECCIÓN DE RED IP.
   B. MÁSCARA DE RED.
   C. DIRECCIÓN DE LA PUERTA DE ENLACE.
   D. DIRECCIÓN DE BROADCAST.
   E. RANGO DE DIRECCIONES IP QUE SE PODRÁN USAR PARA EL HOST.

4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

CONFIGURACIÓN DE UNA RED IPV4

3. ESTABLECER CUÁLES SERÁN LOS RECURSOS COMPARTIDOS DE LA RED: CARPETAS, IMPRESORAS Y EQUIPOS.
4. ESTABLECER SERVICIOS DE RED (WEB, FTP, ETC.)
5. DEFINIR LOS ASPECTOS DE SEGURIDAD DE LA RED (ACCESO RESTRINGIDO A RECURSOS, CONTROL DE ACCESOS, ETC.)

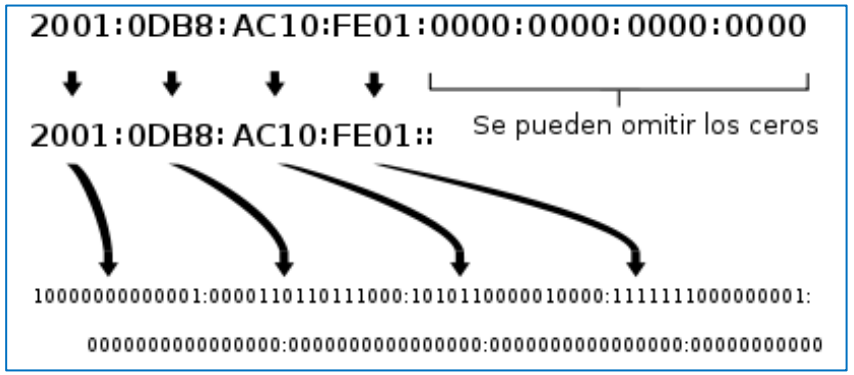
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES

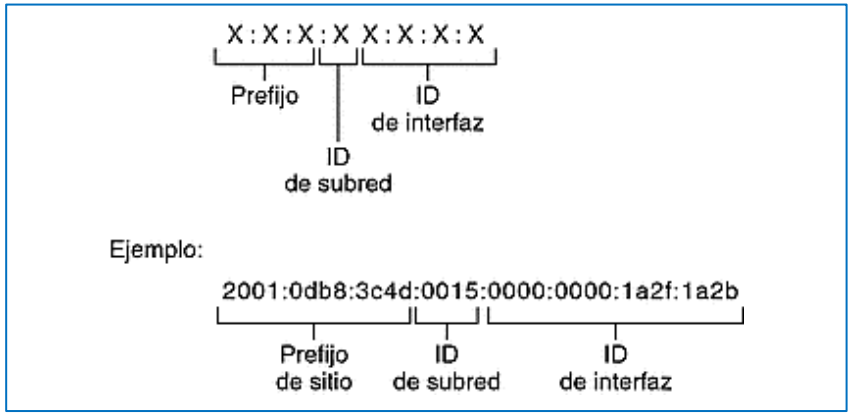
DIRECCIÓN IPV6

LA FUNCIÓN DE LA DIRECCIÓN **IPV6** ES LA MISMA QUE LA DE SU PREDECESORA, LA **IPV4.**

LA DIFERENCIA FUNDAMENTAL ES QUE ESTA ESTÁ FORMADA POR 128 BITS AGRUPADOS DE 16 EN 16, SEPARADOS POR ":".

DEL MISMO MODO QUE LAS DIRECCIONES IPV4, EN LAS IPV6 TAMBIÉN HAY BITS QUE IDENTIFICAN LA RED (EN ESTE CASO LOS 64 PRIMEROS) Y BITS QUE IDENTIFICAN AL HOST (LOS SIGUIENTES).





CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. **PROCESOS DE MONITORIZACIÓN Y RESPUESTA**
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

COMO YA VIMOS, LA **MONITORIZACIÓN DE LOS PROCESOS** ES IMPORTANTE PARA LLEVAR UN CONTROL CORRECTO Y CONSEGUIR RENDIMIENTOS ADECUADOS.

EN EL CASO DE **LAS REDES, LA ADMINISTRACIÓN DEL RENDIMIENTO DE LOS PROCESOS TIENE COMO OBJETIVO RECOLECTAR Y ANALIZAR EL TRÁFICO DE LA RED** PARA DETERMINAR SU COMPORTAMIENTO EN VARIOS ASPECTOS, TANTO A TIEMPO REAL (EN UN MOMENTO ESPECÍFICO) COMO EN UN INTERVALO DE TIEMPO DETERMINADO.

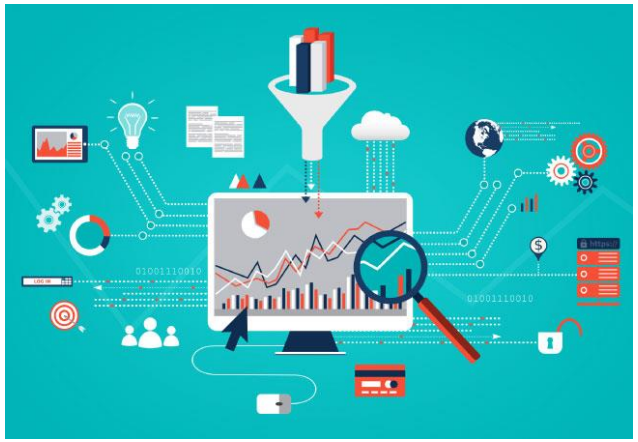
ESTO, DEL MISMO MODO QUE EN LA MONITORIZACIÓN DE PROCESOS DE INFORMACIÓN, PERMITIRÁ A LOS RESPONSABLES TOMAR DECISIONES CORRECTAS SEGÚN EL COMPORTAMIENTO OBSERVADO DE LA RED.

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED SE DIVIDE EN DOS FASES:

- **MONITORIZACIÓN**
- **ANÁLISIS DE RESULTADOS**



5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

MONITORIZACIÓN

CONSISTE EN RECOLECTAR TODA LA INFORMACIÓN DEL COMPORTAMIENTO DE LA RED. ALGUNOS DE LOS ASPECTOS A OBSERVAR SON LOS SIGUIENTES:

UTILIZACIÓN DE ENLACES

SE OBSERVA LA CANTIDAD DE ANCHO DE BANDA UTILIZADA POR CADA ENLACE DE ÁREA LOCAL. SE PUEDE OBSERVAR SOLO UN ELEMENTO O POR TODA LA RED.

CARACTERIZACIÓN DE TRÁFICO

SE PUEDE ESTABLECER UN PATRÓN DEL USO DE LA RED OBSERVANDO LOS TIPOS DE TRÁFICO QUE CIRCULAN SOBRE LOS SERVICIOS DE RED.

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

MONITORIZACIÓN

PORCENTAJE DE TRANSMISIÓN Y RECEPCIÓN DE INFORMACIÓN

OBTENER INFORMACIÓN SOBRE LOS ELEMENTOS DE LA RED QUE MÁS SOLICITUDES HACEN Y ATIENDEN.

UTILIZACIÓN DE PROCESAMIENTO

CONSISTE EN OBSERVAR LA CANTIDAD DE PROCESADOR QUE UN SERVIDOR CONSUME PARA ATENDER UNA APLICACIÓN PARA OBSERVAR EL RENDIMIENTO DE LA CPU.

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

ANÁLISIS

HAY QUE INTERPRETAR LA INFORMACIÓN A PARA ANALIZAR EL COMPORTAMIENTO DE LA RED Y PODER DEFINIR PATRONES DETERMINADOS.

CON UN ANÁLISIS ADECUADO, YA SE PUEDE HACER UNA TOMA DE DECISIONES PARA MEJORAR EL RENDIMIENTO DE LA RED.

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

ANÁLISIS

CON EL PROCESO DE ANÁLISIS SE PUEDEN DETECTAR COMPORTAMIENTOS DE LA RED TALES COMO:

- **TRÁFICO INUSUAL**
- **ELEMENTOS PRINCIPALES DE LA RED**
- **UTILIZACIÓN ELEVADA**
- **CONTROL DE TRÁFICO**
- **CALIDAD DEL SERVICIO**

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

ANÁLISIS

TRÁFICO INUSUAL

DEFINIR UNA SERIE DE PATRONES DEL COMPORTAMIENTO DE LA RED, SU ANÁLISIS AYUDA A DETECTAR TRÁFICO INUSUAL O FUERA DEL PATRÓN

ELEMENTOS PRINCIPALES DE LA RED

SE PUEDEN OBTENER CUÁLES SON LOS QUE MÁS DATOS RECIBEN Y TRANSMITEN Y NECESITAN UN CONTROL MÁS EXHAUSTIVO CON MONITORIZACIÓN

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

ANÁLISIS

UTILIZACIÓN ELEVADA

LA DETECCIÓN DE UN INCREMENTO EN LA UTILIZACIÓN DE ALGÚN ENLACE PUEDE SER SÍNTOMA DE ALGÚN ATAQUE DE SEGURIDAD QUE HAYA SATURADO EL ENLACE POR TRÁFICO GENERADO MALICIOSAMENTE

CONTROL DE TRÁFICO

UNA HERRAMIENTA DE CONTROL DE TRÁFICO ADECUADA PERMITE REENVIAR LA INFORMACIÓN O RUTEARLA POR OTRO LADO AUTOMÁTICAMENTE CUANDO ENCUENTRE SATURACIÓN EN ALGÚN ENLACE O CUANDO ALGUNO ESTÉ FUERA DE SERVICIO

5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA

FASES DE LA ADMINISTRACIÓN DEL RENDIMIENTO DE LA RED

ANÁLISIS

CALIDAD DEL SERVICIO

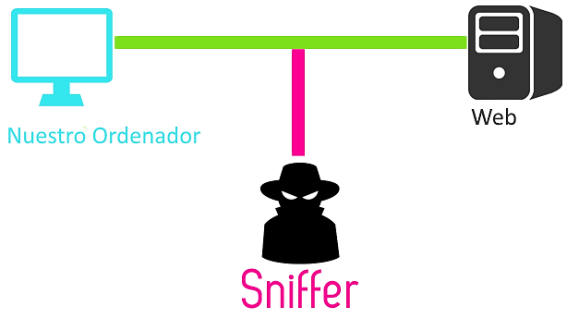
UNA CORRECTA MONITORIZACIÓN Y LA UTILIZACIÓN DE HERRAMIENTAS ADECUADAS PERMITIRÁ OFRECER UNA ÓPTIMA CALIDAD DEL SERVICIO.

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. **HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER**
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER

UN **SNIFFER** ES **UN PROGRAMA QUE CAPTURA TODOS LOS DATOS QUE CIRCULAN A TRAVÉS DEL MEDIO FÍSICO, LOS DISPOSITIVOS Y LOS EQUIPOS QUE FORMAN PARTE DE UNA RED**.



LOS PROPIOS ORDENADORES SON LOS ENCARGADOS DE ACEPTAR O NO LA INFORMACIÓN SEGÚN SI SON LOS DESTINATARIOS.

LO QUE HACE EL SNIFFER **ES PONER LA TARJETA DE RED EN MODO PROMISCUO,** UN MODO EN EL QUE NO HAY FILTRADO DE DATOS DE ENTRADA, YA QUE HACE QUE LA TARJETA CAPTURE TODOS LOS PAQUETES, AUNQUE NO VAYAN DIRIGIDOS A ELLA.

6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER

LOS **SNIFFERS** PUEDEN LEER TODA LA INFORMACIÓN QUE SE INTERCAMBIE ENTRE DOS ORDENADORES DE LA RED.

HAY QUE TENER MUCHO CUIDADO, PUEDE HACERSE UN USO MALINTENCIONADO DE ESTA INFORMACIÓN E INCURRIR EN GRAVES PROBLEMAS DE SEGURIDAD Y PUEDAN COMETER CUALQUIER TIPO DE DELITO ELECTRÓNICO.

6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER

FUNCIONALIDADES DE UN SNIFFER

- ANÁLISIS DE FALLOS, QUE SIRVE PARA ENCONTRAR PROBLEMAS EN LA RED.
- MEDICIÓN DEL TRÁFICO DE DATOS, PERMITIENDO LA DETECCIÓN DE LOS CUELLOS DE BOTELLA.
- CAPTURA DE NOMBRES DE USUARIOS, EN LA RED Y DE CONTRASEÑAS ENVIADAS SIN CIFRAR.
- EN LAS APLICACIONES CLIENTE-SERVIDOR, ANALIZAR LA INFORMACIÓN REAL QUE SE TRANSMITE POR LA RED

6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER

HERRAMIENTAS

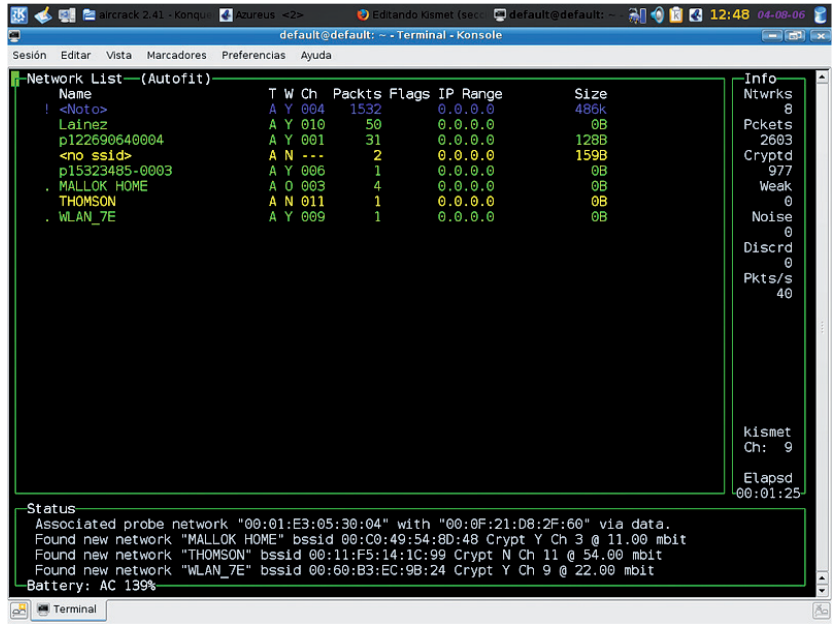
ALGUNAS APLICACIONES TIPO SNIFFER MÁS HABITUALES SON LAS SIGUIENTES:

WIRESHARK, TCPDUMP, TPROXY, NETWORKMINER, FIDDLER, WINDUMP, BRUTESHARK, OMNIPEEK, CAPSA, ETHERAPE, COMMVIEW, WIFI EXPLORER, KISMET

VEAMOS ALGUNAS DE ELLAS:

KISMET

SNIFFER QUE CONTIENE UN SISTEMA DE DETECCIÓN DE INTRUSIONES PARA REDES INALÁMBRICAS.

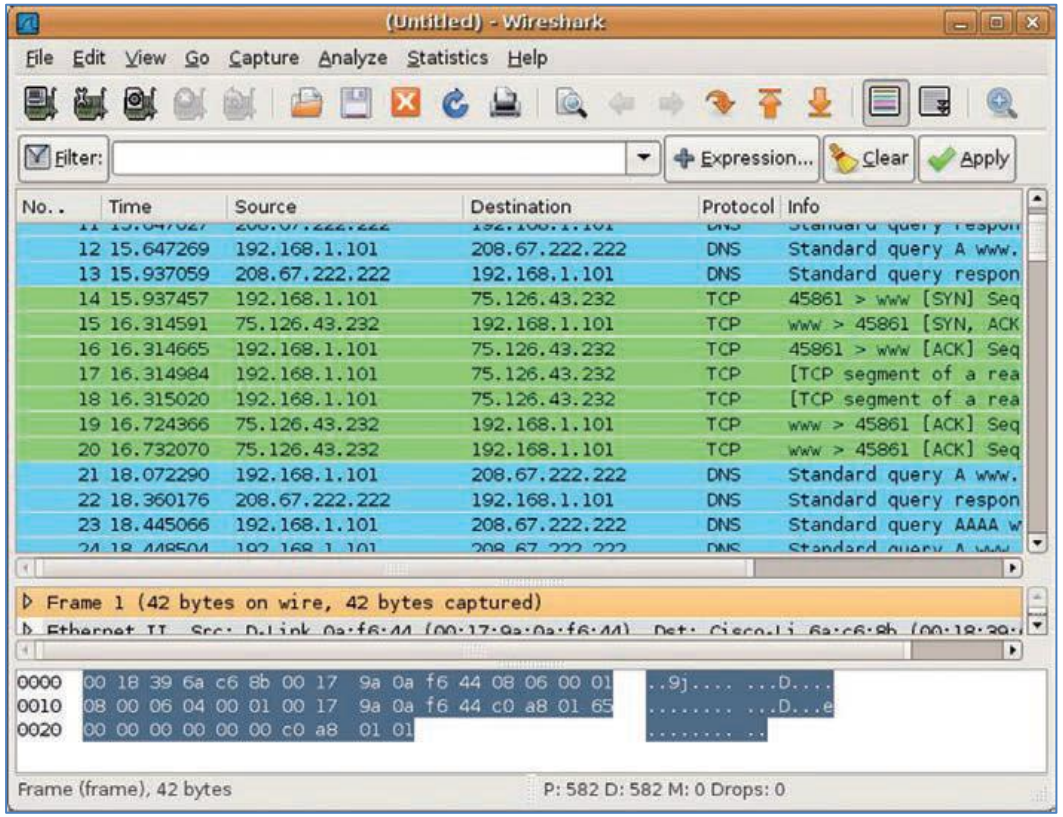


6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER

HERRAMIENTAS

WIRESHARK

ES UN ANALIZADOR DE PROTOCOLOS QUE SE UTILIZA PARA REALIZAR ANÁLISIS Y SOLUCIONAR PROBLEMAS EN REDES DE COMUNICACIONES PARA DESARROLLO DE SOFTWARE Y PROTOCOLOS. EXAMINA Y PERMITE ANALIZAR LA INFORMACIÓN CAPTURADA MEDIANTE LOS DETALLES Y SUMARIOS DE CADA PAQUETE.

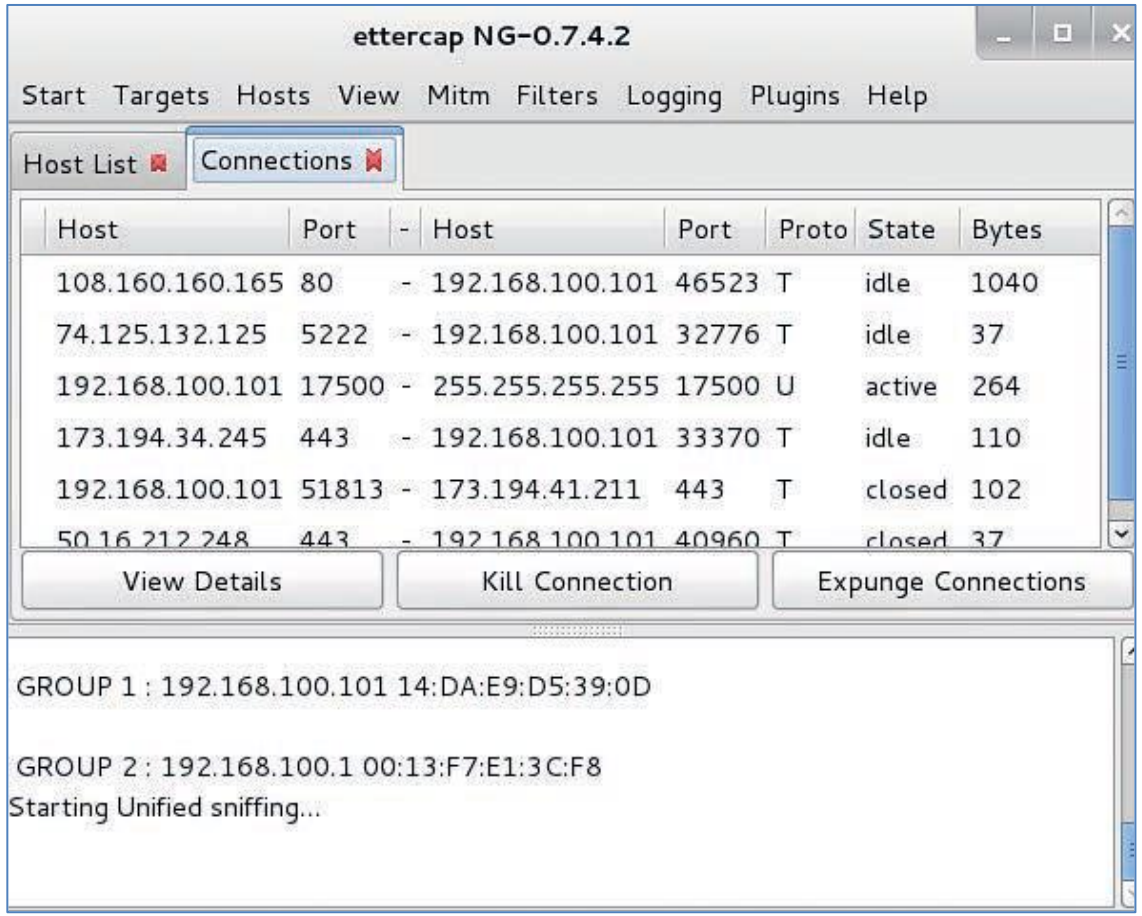


6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER

HERRAMIENTAS

ETTERCAP

ES UN INTERCEPTOR/SNIFFER/ REGISTRADOR PARA REDES DE ÁREA LOCAL CON SWITCH. SOPORTA DIRECCIONES ACTIVAS Y PASIVAS DE VARIOS PROTOCOLOS Y POSIBILITA LA INYECCIÓN DE DATOS EN UNA CONEXIÓN ESTABLECIDA. LINUX Y WINDOWS

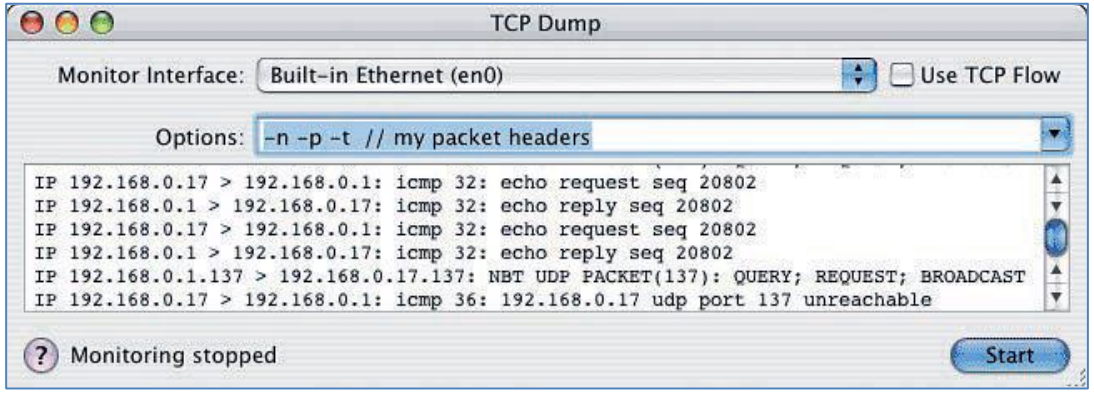


6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER

HERRAMIENTAS

TCPDUMP

HERRAMIENTA EN LÍNEA DE COMANDOS QUE ANALIZA EL TRÁFICO QUE CIRCULA POR LA RED Y QUE OFRECE AL USUARIO LA POSIBILIDAD DE CAPTURAR Y MOSTRAR A TIEMPO REAL LOS PAQUETES TRANSMITIDOS Y RECIBIDOS EN LA RED A LA QUE ESTÁ CONECTADO EL ORDENADOR. PARA WINDOWS, **WINDUMP.**



CONTENIDOS

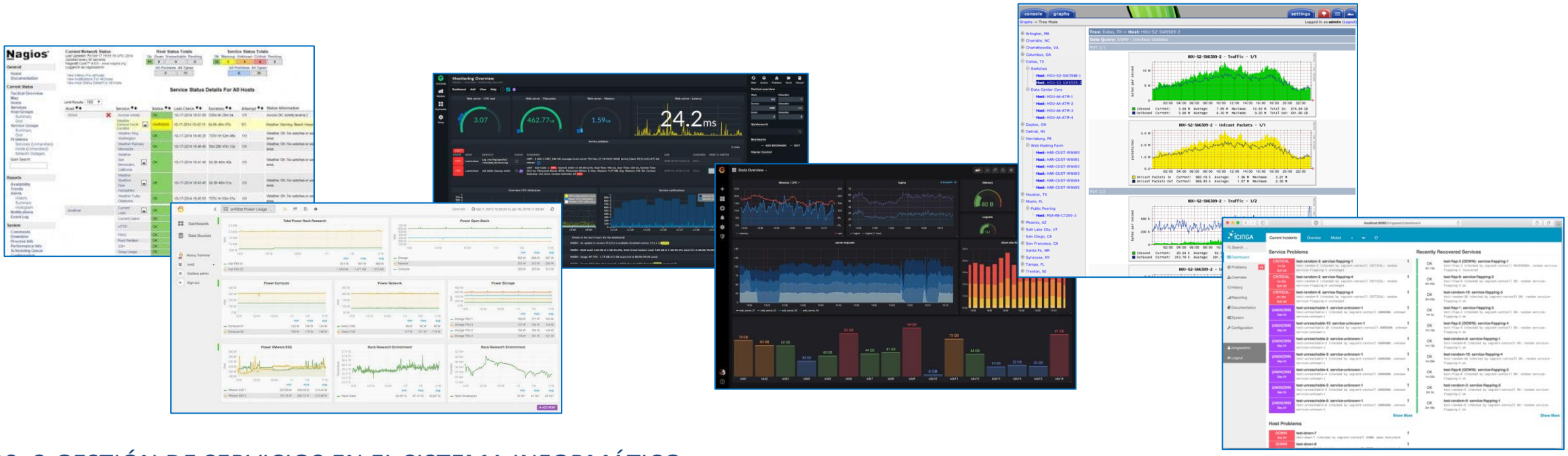
1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. **HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI**
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

ALGUNAS APLICACIONES DE MONITORIZACIÓN MÁS HABITUALES SON LAS SIGUIENTES:

NAGIOS, ZABBIX, CHECKMK, ROMETHEUS + GRAFANA, CACTI, OPENNMS, ICINGA, NETDATA, M/MONIT, LIBRENMS, GROUNDWORK, PRTG NETWORK MONITOR

VEAMOS ALGUNAS DE ELLAS:



7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

HOBBIT

HOBBIT MONITOR ES UN SISTEMA DE MONITORIZACIÓN BAJO LICENCIA LIBRE MEDIANTE EL CUAL SE PUEDE MONITORIZAR CUALQUIER COSA, DESDE REDES PEQUEÑAS HASTA SISTEMAS DE GRANDES MAGNITUDES. ACTUALMENTE ES LLAMADA **HOBBIT-XYMON**.

SU USO ES BASTANTE SENCILLO Y PERMITE GESTIONAR HOSTS, SERVICIOS DE RED Y DISPOSITIVOS DE RED MEDIANTE EXTENSIONES INCLUIDAS DENTRO DEL MISMO SOFTWARE.

7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

HOBBIT

EL FUNCIONAMIENTO DE ESTA HERRAMIENTA SE BASA EN EL ENVÍO PERIÓDICO DE PETICIONES Y EL CORRESPONDIENTE REGISTRO DE LA RESPUESTA RECIBIDA.

SI RECIBE UN VALOR QUE NO ESTÁ EN EL RANGO ESPERADO ENVÍA UNA ALERTA AL ADMINISTRADOR MEDIANTE UN CORREO ELECTRÓNICO.

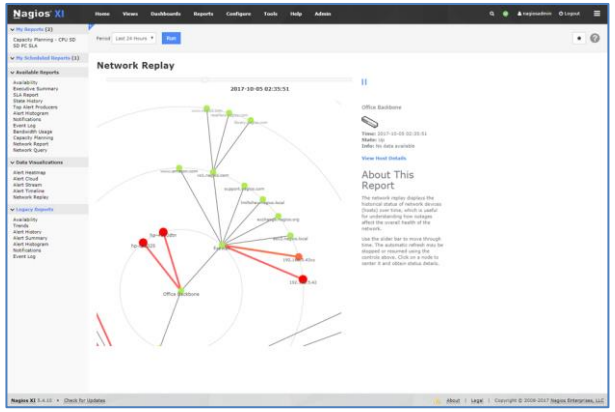
ADEMÁS, MONITORIZA TAMBIÉN EL USO DE DISCOS LOCALES, FICHEROS DE REGISTRO Y PROCESOS.

7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

NAGIOS

NAGIOS ES UNA HERRAMIENTA UN POCO MÁS COMPLICADA QUE HOBBIT, YA QUE REQUIERE MÁS TIEMPO PARA CONFIGURARLA CORRECTAMENTE. COMO VENTAJA DESTACA SU MAYOR POTENCIA RESPECTO A LA OTRA HERRAMIENTA.

ESTA APLICACIÓN ES UN SISTEMA DE MONITORIZACIÓN DE REDES, DE CÓDIGO ABIERTO Y, POR TANTO, GRATUITA, CUYA FUNCIÓN PRINCIPAL ES VIGILAR LOS EQUIPOS Y SERVICIOS ESPECIFICADOS, ENVIANDO ALERTAS CUANDO HAY UN COMPORTAMIENTO FUERA DE LO ESPERADO.



7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

NAGIOS

COMO CARACTERÍSTICAS PRINCIPALES DESTACAN LAS SIGUIENTES:

- MONITORIZACIÓN DE SERVICIOS DE RED (SMTP, POP3, HTTP, ETC.)
- MONITORIZACIÓN DE LOS RECURSOS DE LOS SISTEMAS HARDWARE (USO DE LOS DISCOS, MEMORIA, ESTADOS DE LOS PUERTOS, RENDIMIENTO DEL PROCESADOR, ETC.).
- INDEPENDENCIA DE SISTEMAS OPERATIVOS, PUDIENDO UTILIZARSE EN LA GRAN MAYORÍA DE ELLOS.
- MONITORIZACIÓN REMOTA.
- POSIBILIDAD DE PROGRAMACIÓN DE PLUGINS ESPECÍFICOS PARA NUEVOS SISTEMAS, QUE PERMITAN AL USUARIO LA ADAPTACIÓN DE LA APLICACIÓN A SUS NECESIDADES.
- REVISIÓN DE SERVICIOS PARALIZADOS.
- POSIBILIDAD DE DEFINICIÓN DE LA JERARQUÍA DE LA RED.
- ROTACIÓN AUTOMÁTICA DEL ARCHIVO DE REGISTRO.

7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

NAGIOS

- SISTEMA DE NOTIFICACIÓN A LOS USUARIOS EN EL MOMENTO EN EL QUE OCURRE ALGÚN TIPO DE PROBLEMA, ADEMÁS DE NOTIFICACIÓN CUANDO ESTE PROBLEMA HA SIDO SOLUCIONADO (MEDIANTE SMS, CORREO ELECTRÓNICO U OTRO SISTEMA ESTABLECIDO PREVIAMENTE POR EL USUARIO).
- POSIBILIDAD DE DEFINICIÓN DE GESTORES DE EVENTOS, ENCARGADOS DE EJECUTAR UN EVENTO AUTOMÁTICAMENTE QUE SOLUCIONE PROBLEMAS DEFINIDOS PREVIA-MENTE.
- SOPORTE PARA IMPLEMENTAR HOSTS DE MONITORES REDUNDANTES.
- VISUALIZACIÓN DEL ESTADO DE LA RED EN TIEMPO REAL MEDIANTE LA INTERFAZ WEB.
- GENERACIÓN DE INFORMES Y GRÁFICAS DE COMPORTAMIENTO, VISUALIZACIÓN DE HISTORIAL DE PROBLEMAS Y VISUALIZACIÓN DEL LISTADO DE NOTIFICACIONES EN-VIADAS.

7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

CACTI

ES UNA HERRAMIENTA DE CÓDIGO ABIERTO QUE PERMITE MONITORIZAR Y VISUALIZAR GRÁFICAS Y ESTADÍSTICAS DE DISPOSITIVOS CONECTADOS A UNA RED QUE TENGAN HABILITADO EL PROTOCOLO **SNMP** (SIMPLE NETWORK MANAGEMENT PROTOCOL) ES UN PROTOCOLO QUE PERMITE GESTIONAR DISPOSITIVOS DE RED, DIAGNOSTICAR PROBLEMAS Y PLANEAR SU CRECIMIENTO.

ES UNA HERRAMIENTA IDEAL CUANDO EL USUARIO NECESITA VISUALIZAR GRÁFICOS DEL ESTADO DE SU RED EN ELEMENTOS COMO: ANCHO DE BANDA CONSUMIDO, DETECCIÓN DE CONGESTIONES O PICOS DE TRÁFICOS.

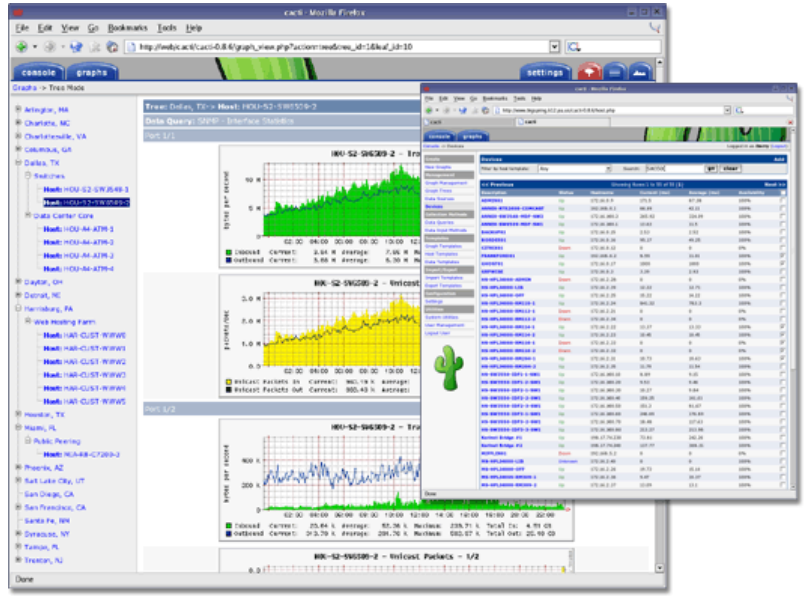
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI

CACTI

SU INTERFAZ ES INTUITIVA Y COMPRENSIBLE, Y SU FUNCIONAMIENTO ES BASTANTE SENCILLO:

LA APLICACIÓN SONDEA CADA UNO DE LOS HOSTS QUE TIENE INSTALADOS, SOLICITANDO LOS VALORES DE LOS PARÁMETROS QUE TIENE DEFINIDOS Y ALMACENANDO EL VALOR.

EL ADMINISTRADOR PUEDE CONFIGURAR EL PERÍODO DE SONDEO ADEMÁS DE DETERMINAR OTROS CONCEPTOS COMO LA PRECISIÓN DE LA INFORMACIÓN A VISUALIZAR.



CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. **SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)**
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)

LOS **SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN SIM (SECURITY INFORMATION MANAGEMENT)** SON PROCEDIMIENTOS DE SUPERVISIÓN QUE SE ENCARGAN DE **RECOLECTAR, CORRELACIONAR Y ANALIZAR LA INFORMACIÓN DE SEGURIDAD EN DIFERIDO**, MEDIANTE LA CREACIÓN DE UN REPOSITORIO INDEXADO CON DATOS OBTENIDOS DE LOS DISPOSITIVOS SUPERVISADOS.

8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)

SUS **FUNCIONES PRINCIPALES** SON LAS SIGUIENTES:

- RECOLECCIÓN, ORDENAMIENTO Y CORRELACIÓN DE LA INFORMACIÓN SOBRE EL ESTADO DE LA RED.
- AUTOMATIZACIÓN DE LA COLECCIÓN DE EVENTOS DE SISTEMAS Y DISPOSITIVOS DE SEGURIDAD.
- CENTRALIZACIÓN, CORRELACIÓN Y PRIORIZACIÓN DE EVENTOS PARA CONSEGUIR:
- ESTANDARIZACIÓN DE EVENTOS.
- REDUCCIÓN DE TIEMPO EN LA DETECCIÓN DE ATAQUES Y VULNERABILIDADES EN LA RED.
- MINIMIZACIÓN DE LA CANTIDAD DE INFORMACIÓN A PROCESAR.

8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)

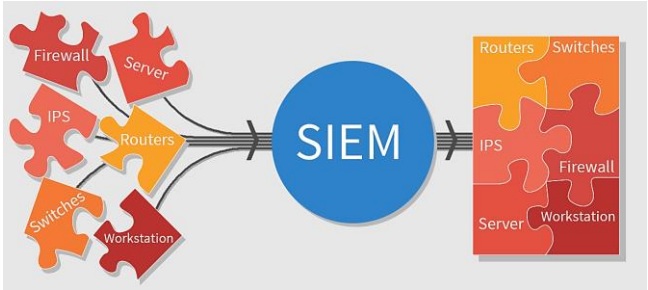
LAS HERRAMIENTAS **SEM** **MONITORIZAN Y GESTIONAN LISTAS DE ACTIVIDADES A TIEMPO REAL** COMO APOYO A LAS ORGANIZACIONES. SUS **BENEFICIOS** PRINCIPALES SON:

- ACCESO A TODOS LOS REGISTROS MEDIANTE UNA INTERFAZ CENTRAL CONSISTENTE.
- ALMACENAMIENTO SEGURO DE LOS REGISTROS, MANTENIENDO LA INTEGRIDAD DEL ARCHIVO DE LOS REGISTROS DE EVENTOS.
- REPRESENTACIÓN GRÁFICA DE LA ACTIVIDAD QUE PERMITE UNA ELABORACIÓN MÁS SENCILLA DE INFORMES.
- ACTIVACIÓN DE ALERTAS PROGRAMADAS.
- CON UN SEM SE PUEDEN GESTIONAR LOS EVENTOS DE VARIOS SISTEMAS OPERATIVOS.
- EN CASO DE BLOQUEO DEL SISTEMA O DE ELIMINACIÓN ACCIDENTAL O MALINTENCIONADA DE REGISTROS, LAS HERRAMIENTAS SEM PERMITEN SU RECUPERACIÓN

8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)

LOS SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD O **SIEM** (SECURITY INFORMATION AND EVENT MANAGEMENT) ENGLOBAN FUNCIONALIDADES DE **SIM Y SEM:**

RECOGEN O RECIBEN LOS REGISTROS DE ACTIVIDAD (LOGS) DE TODOS LOS DISPOSITIVOS MONITORIZADOS, **LOS ALMACENAN A LARGO PLAZO** Y, ADEMÁS, **AGREGAN Y CORRELACIONAN EN TIEMPO REAL** LA INFORMACIÓN RECIBIDA **PARA UNA DETECCIÓN Y ACTUACIÓN** SOBRE LOS EVENTOS MÁS EFICAZ, MEDIANTE ALERTAS, RESPUESTA AUTOMÁTICA, ETC.



8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)

ALGUNOS **SIEM** MÁS HABITUALES SON L0S SIGUIENTES:

FUSION SIEM, MICROSOFT SENTINEL, GRAYLOG, IBM QRADAR, LOGRHYTHM, SOLARWINDS, SPLUNK, ELASTIC SECURITY, INSIGHTSIDR, SUMO LOGIC, NETWITNESS, ALIENVAULT OSSIM

VEAMOS ALGUNAS DE ELLOS:

FUSION SIEM

OFRECE ALMACENAMIENTO DE REGISTROS BASADO EN LA NUBE, INFORMES DE CUMPLIMIENTO DETALLADOS Y BÚSQUEDA GUIADA Y RÁPIDA PARA QUE PUEDA CUMPLIR CON LOS REQUISITOS DE AUDITORÍA Y EL CUMPLIMIENTO NORMATIVO, INCLUIDOS GDPR, HIPAA, PCI, NERC, NYDFS O NIST CON FACILIDAD.

8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)

SOLARWINDS

OFRECE MONITOREO TRABAJANDO 24/7 PARA ENCONTRAR ACTIVIDADES SOSPECHOSAS Y RESPONDER A ELLAS EN TIEMPO REAL.

CON UNA INTERFAZ DE USUARIO INTUITIVA, CONTENIDO LISTO PARA USAR E IMPLEMENTACIÓN VIRTUAL OBTENER INFORMACIÓN VALIOSA DE SUS REGISTROS EN UN TIEMPO MÍNIMO.

UTILIZA HERRAMIENTAS E INFORMES COMPROBADOS POR AUDITORÍAS PARA ORGANISMOS REGULADORES COMO PCI DSS, HIPAA Y SOX.

8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)

MICROSOFT SENTINEL

ES UNA SOLUCIÓN ESCALABLE Y NATIVA DE NUBE QUE PROPORCIONA:

- ADMINISTRACIÓN DE EVENTOS E INFORMACIÓN DE SEGURIDAD (SIEM)
- RESPUESTA AUTOMATIZADA DE ORQUESTACIÓN DE SEGURIDAD (SOAR)

PROPORCIONA ANÁLISIS DE SEGURIDAD INTELIGENTE E INTELIGENCIA SOBRE AMENAZAS A TODA LA EMPRESA.

PERMITE OBTENER UNA VISTA GENERAL DE TODA LA EMPRESA

Microsoft Sentinel

CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. **GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)**

9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

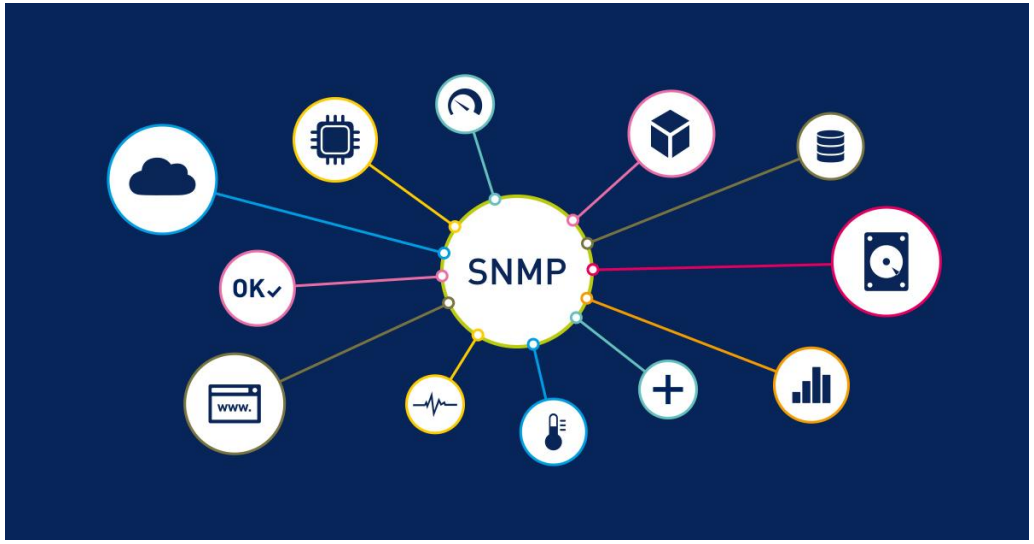
CON EL PROTOCOLO **SNMP** ***(SIMPLE NETWORK MANAGEMENT PROTOCOL)*** SE PUEDE OBTENER INFORMACIÓN DE ROUTERS Y SWITCHES COMO:

- LOS BYTES ENTRANTES Y SALIENTES MEDIANTE EL CÁLCULO DEL TRÁFICO DE DATOS POR SEGUNDO.
- EL NIVEL DE CARGA DE LA CPU.
- LA MEMORIA UTILIZADA Y LA MEMORIA DISPONIBLE.
- EL TIEMPO DE CADA OPERACIÓN.
- EL ESTADO DE LAS SESIONES BGP (EL BGP ES EL PROTOCOLO DE ENCAMINAMIENTO MÁS UTILIZADO EN INTERNET).
- TABLAS ARP (TABLAS QUE ESTABLECEN ENLACES ENTRE LAS CAPAS DE PROTOCOLO Y LAS CAPAS DE ENLACE).
- TABLAS DE REENVÍO DE EVENTOS.

9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

SNMP TAMBIÉN SE UTILIZA PARA CAMBIAR LOS VALORES DE CIERTOS ATRIBUTOS, COMO EL APAGADO Y ENCENDIDO DE PUERTOS EN SWITCHES Y EL REINICIO REMOTO DE DISPOSITIVOS.

SU PRINCIPAL VENTAJA ES QUE SE **PUEDE AUTOMATIZAR LA GESTIÓN DE LA RED.**



9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

EN UN ENTORNO GLOBALIZADO, CON UN GRAN NÚMERO DE SOFTWARE MALICIOSO EN LAS REDES, SE HACE IMPRESCINDIBLE QUE LAS ORGANIZACIONES PUEDAN **FILTRAR LA INFORMACIÓN QUE DEBE ENTRAR EN LOS EQUIPOS Y LA QUE NO**.

PARA ELLO, UNA CORRECTA GESTIÓN DEL FILTRADO DE INFORMACIÓN DE UNA RED **SE LLEVA A CABO MEDIANTE DOS TIPOS DE HERRAMIENTAS**:

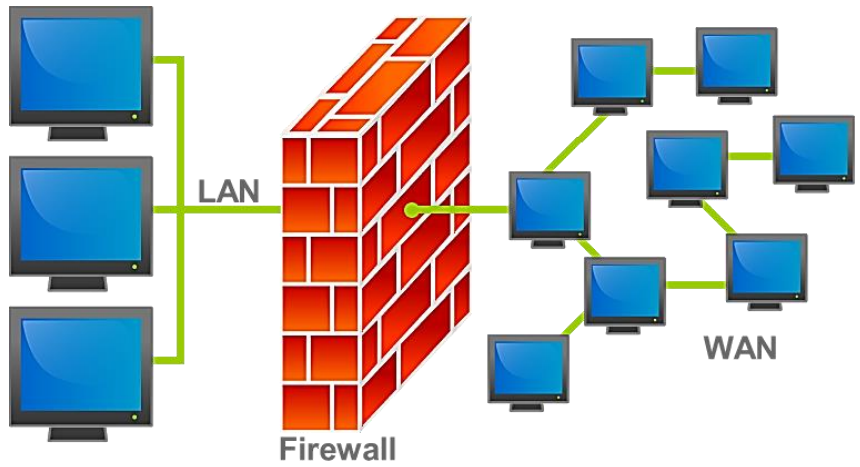
- **FIREWALL (O CORTAFUEGOS)**
- **IDS/IPS**

9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

FIREWALL (O CORTAFUEGOS)

ES UN MECANISMO DE CONTROL DE ACCESOS FORMADO POR COMPONENTES HARDWARE Y SOFTWARE CUYA FUNCIÓN PRINCIPAL ES **SEPARAR LA RED INTERNA DE LOS EQUIPOS EXTERNOS MEDIANTE EL CONTROL DEL TRÁFICO** (DENEGANDO INTENTOS DE CONEXIÓN NO AUTORIZADOS), PARA CONSEGUIR UNA BUENA PREVENCIÓN DE ATAQUES DESDE EL EXTERIOR HACIA EQUIPOS INTERNOS



9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

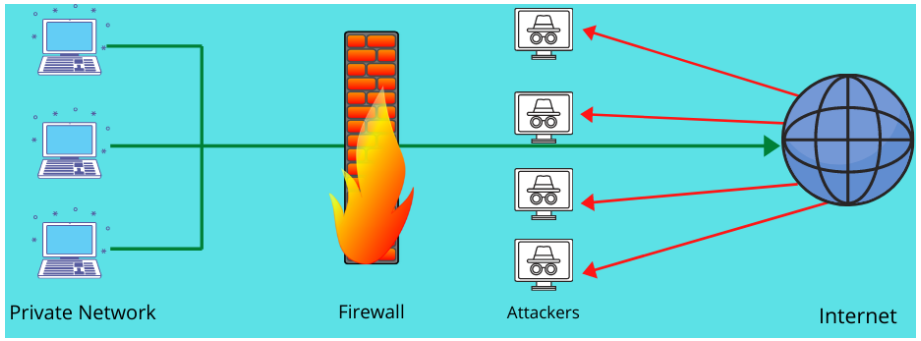
GESTIÓN DE FILTRADO DE RED FIREWALL (O CORTAFUEGOS)

ALGUNOS FIREWALLS DE RED MÁS HABITUALES SON L0S SIGUIENTES:

PFSENSE, OPNSENSE, IPFIRE, SMOOTHWALL

TAMBIÉN HAY DISPOSITIVOS HARDWARE FIREWALLS:

BITDEFENDER BOX, CISCO FIREPOWER, FORTINET FORTIGATE, NETGEAR PROSAFE



9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

FIREWALL (O CORTAFUEGOS)

PFSENSE

ES UNA SOLUCIÓN DE FIREWALL OPEN-SOURCE BASADA EN FREEBSD, CUENTA CON UN KERNEL PERSONALIZADO, EL CUAL ES POSIBLE INSTALAR EN LA MÁQUINA DE TU PREFERENCIA.

PUEDES OPTAR POR LA ALTERNATIVA DE MONTAR UNA MÁQUINA VIRTUAL (VMWARE, VIRTUAL BOX Y OTROS) Y REALIZAR LA INSTALACIÓN DE PFSENSE MEDIANTE LA IMAGEN **ISO**.

9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

FIREWALL (O CORTAFUEGOS)

OPNSENSE

ES UNA SOLUCIÓN DE FIREWALL OPEN-SOURCE QUE TAMBIÉN ESTÁ BASADA EN FREEBSD.

TIENE UNA GRAN CANTIDAD DE SERVICIOS

PODEMOS INSTALAR OPENSENSE EN CUALQUIER SISTEMA CON 64 BITS, ADEMÁS, TAMBIÉN PODEMOS OPTAR POR LA ALTERNATIVA DE MONTAR UNA MÁQUINA VIRTUAL MEDIANTE LA IMAGEN **ISO**.

9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

FIREWALL (O CORTAFUEGOS)

CON LA UTILIZACIÓN DE LOS CORTAFUEGOS SE PUEDEN CONTROLAR ASPECTOS COMO:

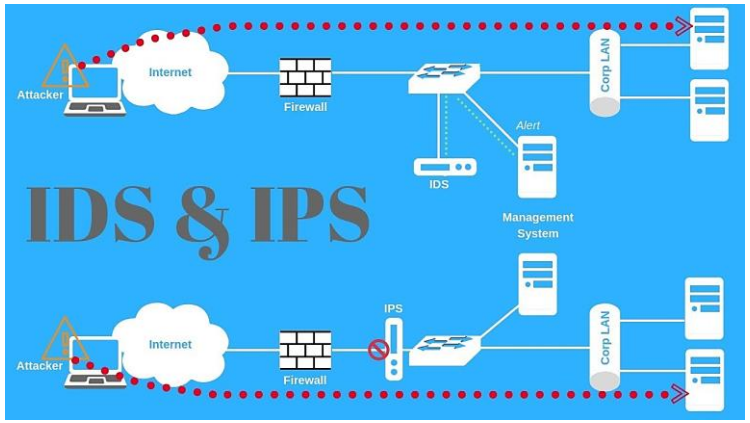
- CONTROL DE SERVICIOS
- CONTROL DE DIRECCIONES
- CONTROL DE USUARIOS
- CONTROL DE COMPORTAMIENTO

9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

IDS/IPS

LOS **IDS (INTRUSION-DETECTION SYSTEMS**) SON PROGRAMAS USADOS PARA DETECTAR ACCESOS NO AUTORIZADOS A UN COMPUTADOR O A UNA RED Y TIENEN COMO FUNCIÓN PRINCIPAL MONITORIZAR EL TRÁFICO DE RED Y ENVIAR ALERTAS SOBRE LAS ACTIVIDADES SOSPECHOSAS.



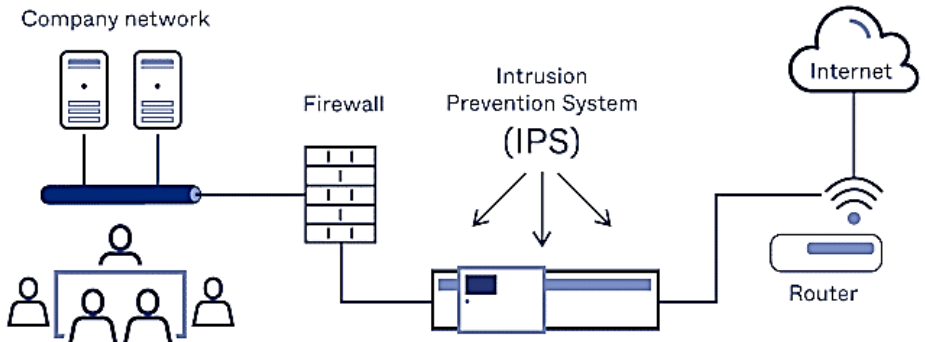
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

IDS/IPS

EL **IPS** PREVIENE E IDENTIFICA LA ACTIVIDAD MALICIOSA, ADEMÁS DE BLOQUEARLA Y MANDAR UN INFORME DEL ATAQUE QUE SE HA PRODUCIDO.

SE CONSIDERAN EXTENSIONES DE LOS SISTEMAS DE DETECCIÓN DE INTRUSOS (IDS), YA QUE EL TRÁFICO DE RED ES EL QUE CONTROLA TODAS LAS ACTIVIDADES QUE PASAN POR ELLA Y EL SISTEMA IPS SE SITÚA DENTRO DEL TRÁFICO DE RED CON LA FINALIDAD DE PREVENIR ESTE TIPO DE INTRUSIONES.

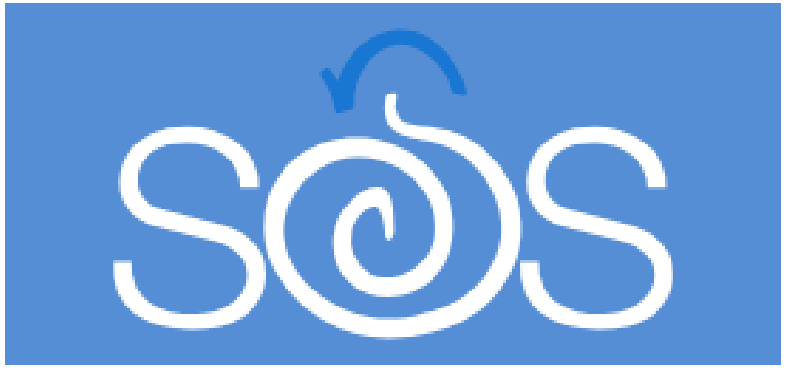


9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

GESTIÓN DE FILTRADO DE RED

ALGUNOS IDS/IPS MÁS HABITUALES SON L0S SIGUIENTES:

ZEEK, SNORT, MANAGEENGINE EVENTLOG ANALYZER, SECURITY ONION, SURICATA, FIREEYE, ZSCALER, GOOGLE CLOUD IDS



CONTENIDOS

1. INTRODUCCIÓN
2. IDENTIFICACIÓN DE LOS DISPOSITIVOS DE COMUNICACIONES
3. ANÁLISIS DE LOS PROTOCOLOS Y SERVICIOS DE COMUNICACIONES
4. PRINCIPALES PARÁMETROS DE CONFIGURACIÓN Y FUNCIONAMIENTO DE LOS EQUIPOS DE COMUNICACIONES
5. PROCESOS DE MONITORIZACIÓN Y RESPUESTA
6. HERRAMIENTAS DE MONITORIZACIÓN DE USO DE PUERTOS Y SERVICIOS TIPO SNIFFER
7. HERRAMIENTAS DE MONITORIZACIÓN DE SISTEMAS Y SERVICIOS TIPO HOBBIT, NAGIOS O CACTI
8. SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (SIM/SEM)
9. GESTIÓN DE REGISTROS DE ELEMENTOS DE RED Y FILTRADO (ROUTER, SWITCH, FIREWALL, IDS/IPS, ETC.)

RESUMEN

UNA **RED** ES UN **CONJUNTO DE DISPOSITIVOS FÍSICOS Y DE APLICACIONES MEDIANTE EL CUAL SE COMUNICAN LOS ORDENADORES PARA COMPARTIR INFORMACIÓN Y ESTABLECER UN SISTEMA DE COMUNICACIÓN EN UNA ORGANIZACIÓN**.

SON VARIOS LOS DISPOSITIVOS QUE FORMAN PARTE DE UNA RED, DISTINGUIENDO ENTRE **EQUIPOS DE RED** (*SERVIDORES, ORDENADORES*), **MEDIOS DE COMUNICACIÓN** (ROUTERS, SWITCHES...) **Y CONECTORES** (SISTEMA DE CABLEADO, ENLACES INALÁMBRICOS...).

RESUMEN

PARA QUE LOS DISTINTOS EQUIPOS DE RED SE COMUNIQUEN ENTRE ELLOS Y PUEDAN TRANSMITIR LA INFORMACIÓN **ES NECESARIO EL ESTABLECIMIENTO DE UNA SERIE DE NORMAS Y REGLAS**: ESTE CONJUNTO DE NORMAS Y REGLAS FORMAN EL **PROTOCOLO**.

LA VARIEDAD DE PROTOCOLOS ES MUY AMPLIA Y TIENEN BASTANTES DIFERENCIAS ENTRE ELLOS, AUNQUE LO HABITUAL ES QUE COMPARTAN ALGUNA PROPIEDAD FUNDAMENTAL.

RESUMEN

EL PRIMER PASO PARA LA ESTANDARIZACIÓN DE LOS PROTOCOLOS FUE CON EL **MODELO OSI** (OPEN SYSTEM INTERCONNECTION), UN MODELO TEÓRICO QUE EN LA ACTUALIDAD FORMA UN MARCO DE REFERENCIA PARA LA DEFINICIÓN DE ARQUITECTURA EN LA INTERCONEXIÓN DE LOS SISTEMAS DE COMUNICACIONES.

NO OBSTANTE, EN LA PRÁCTICA SE UTILIZA **EL MODELO TCP/IP** PARA LA DESCRIPCIÓN DE PROTOCOLOS DE RED.

RESUMEN

PARA TENER UN **CONTROL** DE LOS DISTINTOS PARÁMETROS DE UN SISTEMA DE COMUNICACIONES ES NECESARIO **SU MONITORIZACIÓN**, PARA OBTENER DATOS DE RENDIMIENTO DE LOS DISTINTOS COMPONENTES DE LA RED, REALIZAR UN ANÁLISIS DE LOS MISMOS Y TOMAR DECISIONES PARA SEGUIR CON LA ESTRATEGIA DE RED DEFINIDA O, POR EL CONTRARIO, REALIZAR MODIFICACIONES EN CASO DE SER NECESARIO.

RESUMEN

POR ELLO, HAY SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (**SIM**), SISTEMAS DE GESTIÓN DE EVENTOS (**SEM**) Y SISTEMAS DE GESTIÓN DE INFORMACIÓN Y EVENTOS DE SEGURIDAD (**SIEM**).

ESTO ES TODO