DIRECCIÓN GENERAL DE TECNOLÓGICA INDUSTRIAL Y DE SERVICIOS

CENTRO DE BACHILLERATO TECNOLOGICO

industrial y de servicios No. 155

“Ricardo Flores Magón”

Carrera

Soporte y Mantenimiento de Equipo de Cómputo.

VI Semestre

C U A D E R N I L L O

D E

A P R E N D I Z A J E S

E S E N C I A L E S

Modulo IV

Instala y opera redes de computadora

Submódulo II

Opera una red LAN

NOMBRE DEL ALUMNO(A)

Periodo: Febrero 2021 - Julio 2021

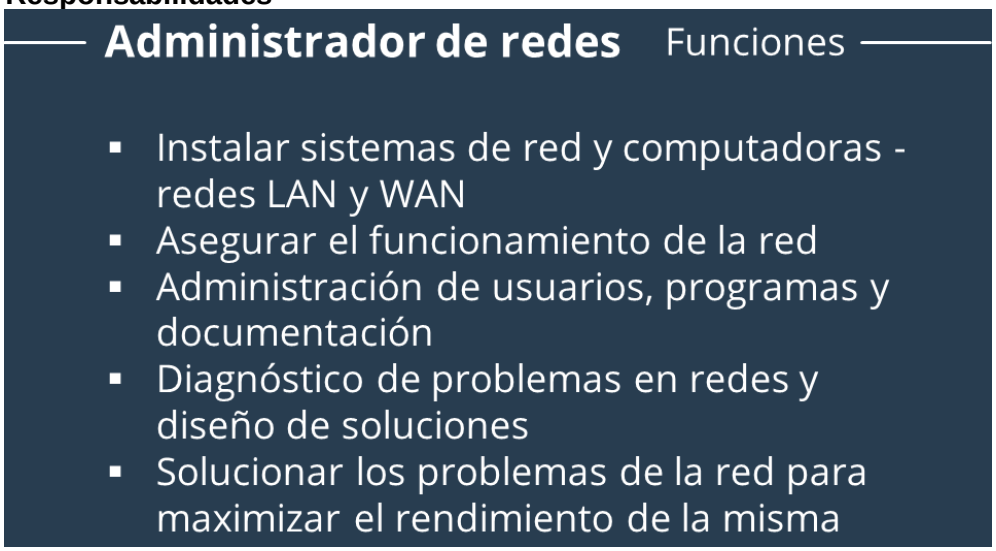
ESTRATEGIA	PRODUCTO
0. Da lectura al documento "Administración de redes LAN" (Anexo 0), debe realizar un cuestionario con sus respuestas, con un mínimo de 15 preguntas.	**0- Cuestionario**

¿QUÉ HACE UN ADMINISTRADOR DE REDES?

Un administrador de redes es responsable de mantener el buen funcionamiento del software y hardware de redes. Estas redes de datos pueden ser redes de área local (LAN), redes de área amplia (WAN), intranets y/o extranets. Veamos más en detalle el trabajo de la administración de redes, sistemas y telecomunicaciones.

¿Qué es la administración de redes?
La **administración de redes informáticas y comunicaciones** consiste en administrar y asegurar el funcionamiento correcto de las redes informáticas.
Lo que busca el **administrador de redes** sobre todo es una red libre de fallos y errores. Para conseguirlo se apoyan en herramientas y tecnologías.
El mayor reto es conseguir **identificar fallos proactivamente**, antes de que afecte a los clientes o usuarios finales.
Este experto en redes concentra sus esfuerzos en **diseñar una red segura**, **implementar soluciones**, **resolver problemas y mantener la infraestructura de redes** para garantizar el rendimiento.
A los expertos en redes se les conoce también como **analistas de redes** o **administradores de redes informáticas** o **administradores de redes y telecomunicaciones**.

Funciones y Responsabilidades

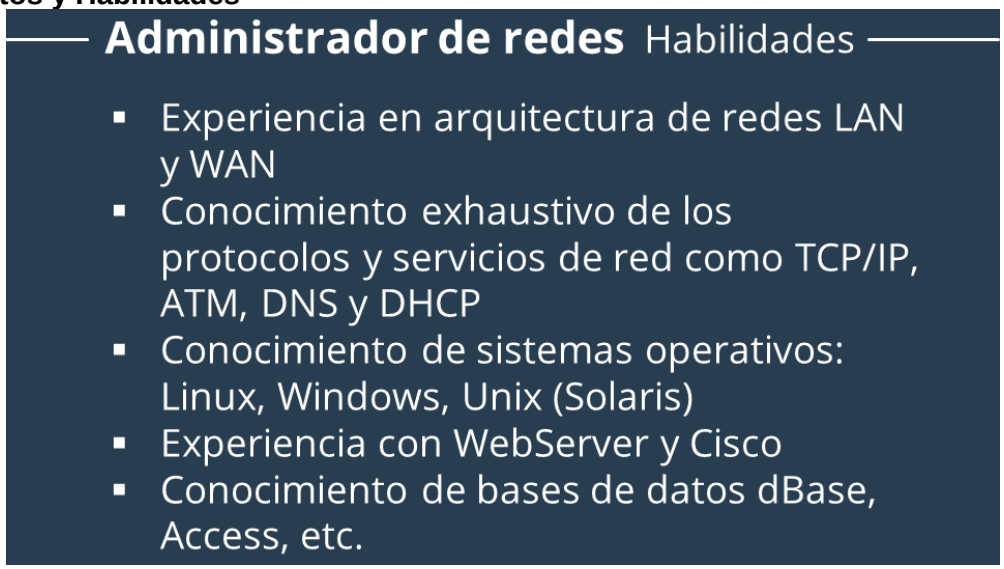


El **administrador de redes** mantiene y el controla las redes de informáticas y cualquier otro entorno informático relacionado con las **configuraciones, programas de hardware y estructuras de software**.
Esto incluye **asignación de protocolos y tablas de ruteo**, configuración y autorización de servicios y el mantenimiento de todo el sistema de redes (con routers, cortafuegos, etc).
A veces se encargan también del mantenimiento de las instalaciones y servidores VPN.
¿Qué hace un administrador de redes y comunicaciones?

- Instalar sistemas de red y computadoras (redes LAN y WAN)
- Asegurar el buen funcionamiento de la red
- Administración de usuarios, programas y documentación
- Diagnóstico de problemas en redes y diseño de soluciones

- Solucionar los problemas de la red para maximizar el rendimiento de la misma
- Administrar los cortafuegos y mantener los sistemas de seguridad informática
- Configuración del router
- Actualización de los servidores de datos y del equipo de red
- Auditoría de direcciones IP
- Monitoreo del funcionamiento para prevención de errores
- Diseñar e implementar nuevas soluciones
- Planificar, implementar y supervisar las redes informáticas

Conocimientos y Habilidades



Los **administradores de redes informáticas** deben tener un buen conocimiento del hardware y de infraestructura red.
Para **administrar las redes de forma eficiente** se apoyarán en **herramientas de redes**. Algunas de las más utilizadas son:

- Wireshark
- TCPDump
- Apache
- NetDot

Además, deberán tener conocimiento en **tecnologías y redes inalámbricas**, incluyendo WiMax, Wi-Fi y WAP.

Por otro lado, también deben tener **habilidades analíticas** y de resolución de problemas y excelentes habilidades de comunicación escrita y verbal.

Conocimientos del administrador de redes y telecomunicaciones

- Comprensión de la infraestructura de la red y el hardware, seguridad de la red
- Experiencia en arquitectura de redes LAN y WAN
- Conocimiento exhaustivo de los protocolos y servicios de red como TCP/IP, ATM, DNS y DHCP
- Conocimiento de sistemas operativos: Linux, Windows, Unix (Solaris)
- Experiencia con WebServer y Cisco
- Conocimiento de control de red como Nessus o Snort
- Conocimiento de bases de datos dBase, Access, etc.
- Experiencia con herramientas de redes – Wireshark, Apache, NMap
- Capacidad de aprender rápidamente sobre nuevas tecnologías y productos
- Capacidades analiticas y de resolución de problemas de las funciones de la red (seguridad, servidores, enrutamiento)
- Organización y liderazgo
- Capacidad de trabajo en equipo

Fuente: https://www.freelancermap.com/blog/es/que-hace-administrador-de-redes/

COMPETENCIA - CONFIGURA DISPOSITIVOS DE INTERCONEXION DE RED
CONTENIDO:

A. Verificando la compatibilidad

ESTRATEGIA	PRODUCTO
1. Comprende los diversos medios para verificar la compatibilidad y la interconexión de los dispositivos de red utilizando una tarjeta de red (NIC) (Anexo 1) elabora un mapa conceptual.	**1- Mapa conceptual**

A N E X O - 1
¿CÓMO ELEGIR UNA TARJETA DE RED?

Comprar una tarjeta de red puede llegar a ser complicado, sobre todo si es la primera vez. Además, existen diferentes tipos de tarjetas de interfaz de red o tarjetas NIC (network interface cards, por sus siglas en inglés) en el mercado, entre las que se incluyen las tarjetas PCIe, los adaptadores de red USB, etc., lo cual hace aún más complicado ¿cómo elegir una tarjeta de red? A continuación, presentamos los factores que puedes considerar a la hora de comprar una tarjeta de interfaz de red.

Ten cuidado con el tipo de bus en la tarjeta NIC

La tarjeta NIC se puede clasificar en PCI, PCI-X, tarjetas de red PCIe y adaptadores de red USB basados en diferentes interfaces de bus. Por lo general, los tres tipos de tarjetas de red basadas en PCI se utilizan para ajustarse a las ranuras correspondientes de la placa madre de dispositivos tales como host y servidores, mientras que el adaptador de red USB o bus universal en serie (universal serial bus, por sus siglas en inglés) es un estándar de bus externo.

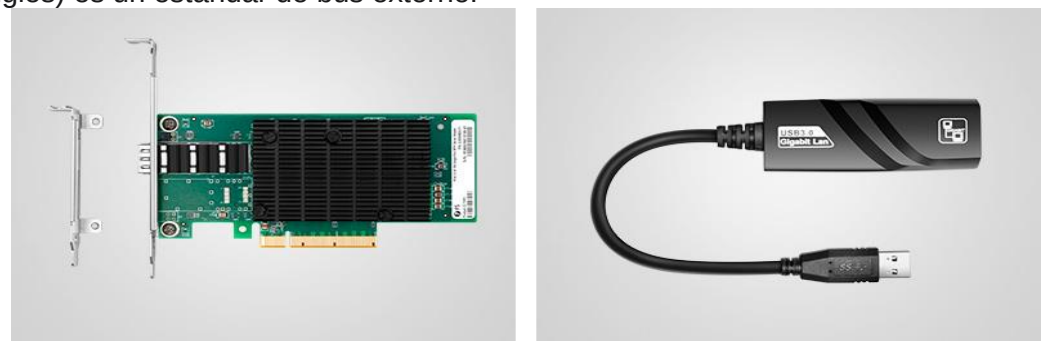


Imagen 1: Tarjeta de red PCIe vs. Adaptador de red USB

La tarjeta de red de interconexión de componentes periféricos o tarjeta PCI (Peripheral Component Interconnect, por sus siglas en inglés) fue desarrollada en 1990 con un ancho fijo de 32 bits (133 MB/s de datos de transmisión) y 64 bits (266 MB/s de datos de transmisión). Pero más adelante, la tarjeta PCI fue reemplazada por la tarjeta PCI-X paulatinamente. La tarjeta de interfaz de red PCI-X (Peripheral Component Interconnect eXtended) es una tecnología de bus PCI mejorada y es compatible con la tarjeta NIC PCI. La tarjeta PCIe (Peripheral Component Interconnect express) es la última tecnología de interfaz estándar compatible únicamente con otras especificaciones de bus PCI. Su disposición de hardware es diferente. Actualmente existen en el mercado cuatro tamaños de tarjetas de red PCIe Express: x1, x2, x4, x8 y x16 (aprende más acerca de los tipos de tarjetas PCIe). Dado que los mecanismos de hardware de las PCIe son diferentes a los de las PCI y PCI-x, no es posible conectar una tarjeta PCIe en una ranura PCI o PCI-X, y viceversa.

Ten en cuenta que las tarjetas de red PCIe son las más populares del mercado; en cambio las tarjetas PCI y PCI-X sólo se utilizan en dispositivos antiguos. Los servidores, ordenadores y otros equipos de última generación suelen estar diseñados con ranuras PCIe. De este modo, las tarjetas de red PCIe se convierten una mejor opción a largo plazo.

Familiarízate con la velocidad requerida para el adaptador de red

Sin duda alguna, este aspecto no debe ser ignorado si estás confundido en cuanto a la elección de una tarjeta de red. Asegúrate de que la velocidad de tu nueva tarjeta NIC se ajuste a la de tu red. Por ejemplo, no puedes esperar alcanzar una velocidad de 10Gb con una tarjeta Ethernet de 10Gb, si tu ISP sólo te ofrece una velocidad de 1Gb. Hoy en día, casi todas las tarjetas de red pueden funcionar con una velocidad de al menos un Gigabit, lo que permitirá satisfacer todas las demandas de la red doméstica.

Pero si piensas utilizar la nueva tarjeta en aquellos servidores que requieren mayor velocidad para manejar más tráfico, es mejor que elijas una tarjeta de red de 10Gb y 25Gb, o incluso una tarjeta de red de 40Gb.

Comprueba el número de puertos que tiene la tarjeta de la red.

Por lo general, una tarjeta de red NIC que tenga un solo puerto es suficiente, ya que puede satisfacer la mayor parte de las demandas de transmisión. Sin embargo, las tarjetas NIC con múltiples puertos son una gran opción para los servidores o estaciones de trabajo destinadas a realizar múltiples tareas. Por ejemplo, un puerto de la tarjeta de interfaz de red puede desplegarse para entregar datos básicos, y los otros puertos pueden utilizarse para transmitir señales normales. Esto puede mejorar la seguridad de la red. Asimismo, las tarjetas NIC multipuerto pueden proporcionar redundancia de red. Si un puerto no funciona, los usuarios pueden utilizar el otro para transmitir los datos.

Verifica el tipo de conector compatible con la tarjeta NIC

Algunas tarjetas de Ethernet están diseñadas con conectores RJ45, y algunas tarjetas de red de fibra utilizan puertos SFP+ o QSFP+, e incluso algunas pueden utilizar BNC (conectores de tuerca de bayoneta).

En el caso de la tarjeta con conector RJ45, por ejemplo, una tarjeta de red 1/10GBASE-T, se deben utilizar cables de Ethernet tales como Cat5e o Cat6 para que funcione. En la imagen 2 se ilustra la conexión. Una tarjeta de 10 Gigabit Ethernet se conecta al servidor del rack RS-7188 y el switch de red FS S5850-48T4Q de 10Gb transmitirá los datos al servidor mediante el cable de conexión Cat6.

Imagen 2: El cable Cat6 se conecta a la tarjeta de red 10GBASE-T para realizar la transmisión

Las tarjetas de red de fibra suelen utilizar fibras monomodo o multimodo como medio de transmisión, tal y como se muestra en la imagen 3. Una tarjeta NIC de 40Gb del servidor se conecta al servidor de red RS-7188. Luego, el switch de fibra FS S5850-48S6Q 10G con puertos QSFP+ entrega señales al servidor RS-7188 a una velocidad de 40Gb a través del cable de fibra MTP OM4. Ten en cuenta que, para las transmisiones de corta distancia, se pueden utilizar cables DAC de 40G en vez de cables MTP y transceptores QSFP+ con el fin de establecer este enlace.

Imagen 3: La tarjeta de red de 40Gb utiliza un cable de fibra MTP para completar la transmisión

Para la tarjeta con conector BNC, se requieren cables coaxiales para realizar la conexión. Ten en cuenta que este tipo de adaptadores de red se ha vuelto obsoleto. Así que no se recomienda comprar una tarjeta de interfaz de red con un conector BNC.

Conoce el sistema operativo que la tarjeta NIC soporta

Los ordenadores personales, los servidores de red y demás hosts de diferentes proveedores son compatibles con diversos sistemas operativos. Por ejemplo, los servidores de red pueden funcionar con Windows Server 2008 R2, Redhat Enterprise Linux Server, etc. Por lo tanto, es importante que te asegures de que tu nuevo adaptador de red es compatible con el sistema operativo que utiliza tu dispositivo antes de comprarlo. De lo contrario, la tarjeta no funcionará.

Descubre cuáles son las funciones quieres en tu tarjeta de red

Asegúrate de que las funciones de la tarjeta de interfaz de red puedan satisfacer tus aplicaciones. Si sólo quieres acceso a Internet, todas las tarjetas NIC pueden hacerlo. Pero si lo que necesitas es compatibilidad con funciones avanzadas tales como FCoE (Fiber Channel over Ethernet), iSCSI o la implementación de PCI-SIG, debes consultar el manual de instrucciones o preguntarle al proveedor directamente para asegurarte de que la tarjeta NIC sea compatible con la función que requieres.

Otros factores no se pueden ignorar al momento de comprar un adaptador de red

El presupuesto siempre constituye un punto importante a la hora de elegir una tarjeta de red. El precio de la tarjeta NIC varía enormemente porque está diseñada con distintos modelos, velocidades, niveles de rendimiento y fabricantes. También es importante que compres tus tarjetas de un proveedor de

confianza, ya que por lo general éste te ofrecerá mejores servicios. Algunos vendedores no son capaces de ofrecerle a los clientes un servicio integral. Elegir un proveedor que te brinde un servicio de atención al cliente y un soporte técnico las 24 horas del día, los 7 días de la semana, y que además incluya servicios de preventa y postventa para resolver todos tus problemas.
Fuente: https://community.fs.com/es/blog/how-to-choose-a-network-card.html

B. Comprobando la comunicación

ESTRATEGIA	PRODUCTO
2. Conoce el uso del comando PING (Anexo 2) desarrolla una tabla comparativa de las pruebas para verificar el funcionamiento, identificar y aislar cualquier error presente.	**2- Tabla comparativa**

A N E X O - 2
COMO USAR EL COMANDO PING DE REDES

Como utilizar el comando PING para probar la conectividad, el funcionamiento, la disponibilidad de una red, saber el tiempo de respuesta en una conexión y conocer la dirección IP correspondiente a un dominio en internet, entre otras tareas posibles.

Ping.exe es una pequeña aplicación disponible en todos los sistemas Windows, que se ejecuta con el comando PING mediante la consola de CMD.
Es usada para probar la conectividad de redes informáticas.
Es uno de las más sencillas y útiles herramientas para ejecutar cualquier diagnostico ante conflictos en la red o simplemente para estar seguros de la funcionalidad de cualquier conexión.
Ping comprueba la conexión enviando paquetes de solicitud de eco y de respuesta, muestra si se ha recibido una respuesta del destino y cuánto tiempo se ha tardado en recibirla.
Si se produce un error en la entrega muestra un mensaje de error.
Es un mecanismo similar al empleado por submarinos y otras naves al utilizar el sonar, en este caso el medio de transmisión no es el agua, sino las redes informáticas.

Usos prácticos del comando PING
Ping es posible utilizarlo en infinidad de tareas en el trabajo en redes, algunos de los usos prácticos más empleados son los siguientes:

- Comprobar la conectividad de una red.
- Medir la latencia o tiempo que tardan en comunicarse dos puntos remotos.
- En internet conocer la dirección IP utilizada por un nombre de dominio.
- Scripts que permiten llevar un registro de la disponibilidad de un servidor remoto.
- Scripts que permiten conocer cuando existe conexión en un equipo.
- En los archivos Batch es empleado ocasionalmente para retrasar la ejecución de comandos un tiempo determinado.

¿Cómo ejecutar el comando PING?
Para ejecutar el comando ping en su forma más elemental utiliza: *PING dirección_ip*
Por ejemplo:
ping 127.0.0.1
Es posible insertar la petición a ping en la consola de cmd o directamente en el cuadro de Inicio o Ejecutar, en estos últimos casos al completarse el comando se cerrará la ventana de cmd y no podremos ver los resultados.
Para ejecutarlo insertándolo en el cuadro de Inicio y lograr que permanezca abierta la ventana con el resultado utiliza:*cmd /k ping dirección_ip* y presiona la tecla Enter.
Por ejemplo:
cmd /k ping 127.0.0.1

Al ejecutar ping sin parámetros, de forma predeterminada se enviarán 4 solicitudes de eco, con el tiempo de espera de 1 segundo, el tamaño de 32 bytes y con la fragmentación permitida.
Para usar otras opciones es necesario especificar los parámetros de acuerdo a la necesidad.
La respuesta obtenida en el caso anterior será algo similar a lo siguiente:

Haciendo ping a dirección IP con 32 bytes de datos:

Respuesta desde 127.0.0.1: bytes=32 tiempo= <10 ms TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo= <10 ms TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo= <10 ms TTL=128
Respuesta desde 127.0.0.1: bytes=32 tiempo= <10 ms TTL=128

TTL= es el tiempo de vida del paquete enviado y su valor óptimo es 128
En la respuesta obtenida de ping pueden aparecer algunos de los siguientes errores:
"Red de destino inaccesible" significa que no existe ninguna ruta al destino.
"Ha terminado el tiempo de espera para esta solicitud" indica errores en la conexión.

Opciones y parámetros más utilizados con el comando PING

Modificador	Uso
-n	Determina el número de solicitudes de eco que se van a enviar. El valor predeterminado es 4.
-w	Permite ajustar el tiempo de espera (en milisegundos). El valor predeterminado es 1.000 (tiempo de espera de un 1 segundo).
-l	Permite ajustar el tamaño del paquete de ping. El tamaño predeterminado es 32 bytes.
-f	No fragmentar en paquetes. De manera predeterminada, el paquete ping permite la fragmentación.
-a	Resolver direcciones en nombres de host
-i	Tiempo de vida o TTL
-r	Registrar la ruta de saltos de cuenta.

Usar el comando PING para probar la conectividad en una red
A pesar de su aparente simpleza es muy efectivo el uso del comando ping para el diagnóstico, detección de fallos y comprobación de la disponibilidad de cualquier red.
A continuación ejemplo de pruebas que se pueden efectuar en una red local para verificar el funcionamiento y para identificar y aislar cualquier error presente.
La supuesta red de ejemplo posee los siguientes parámetros:

- *Dirección IP del equipo: 192.168.137.3*
- *Dirección IP de otra PC en la misma red: 192.168.137.5*
- *Puerta de enlace (equipo en la red con conexión a internet): 192.168.137.1*

Las direcciones IP anteriores es posible conocerlas utilizando el comando IPCONFIG
1- Hacer ping a 127.0.0.1, es la dirección localhost o dirección de loopback de nuestro mismo equipo, en caso de tener éxito demuestra que el protocolo TCP/IP está instalado y funcionando de forma correcta. De no ser así es necesario reinstalarlo.
Para reinstalar el protocolo TCP/IP utiliza:
En Windows XP: **netsh int ip reset resetlog.txt**
En Vista y Windows 7: **netsh interface ipv4 reset**
2- Hacer ping a la dirección IP del equipo: **ping 192.168.137.3**.
De tener éxito demuestra que la tarjeta o adaptador de red funciona correctamente, de no ser así desinstala el dispositivo y reinicia Windows para reinstalarlo automáticamente.
Para desinstalar el dispositivo es necesario acceder al Administrador de dispositivos, para eso introduce en Inicio o Ejecutar *devmgmt.msc* y oprime Enter.

3- Hacer ping a la dirección IP del otro equipo en red: **ping 192.168.137.5**
De tener éxito demuestra que las conexiones físicas entre ellos son correctas.
4- Hacer ping a la dirección IP de la puerta de enlace: **ping 192.168.137.1**
De tener éxito demuestra que existe conexión con el equipo que suministra internet.
5- Hacer ping a la dirección IP de un sitio en internet: **ping 209.190.61.3** (La IP de este sitio web).
De tener éxito demuestra que la conexión a internet funciona.
6- Por último, hacer ping a un dominio en internet: **ping google.com**
De tener éxito demuestra que existe conexión a internet y los servidores DNS configurados en la conexión funcionan correctamente.

Ejemplos prácticos del uso del comando PING

Son múltiples las tareas en las que se puede emplear el comando ping y no solo para diagnosticar la conectividad, para la cual es una magnifica herramienta.
A continuación se irán agregando sucesivamente aplicaciones prácticas en las cuales es posible utilizarlo.

Usar el comando ping para medir la latencia en la red (lejanía de un servidor)

La Latencia es la cantidad de tiempo que demora en transmitirse, una pieza de datos de una localización a otra.
Depende de la distancia física entre dos puntos de internet y del número de saltos entre las distintas redes para establecer la conexión.
Ping permite medir la latencia entre nuestra ubicación y un servidor de internet.

Para eso usa su dirección IP si es posible, por ejemplo:

```
Ping 47.8.4.67
```

O mejor aún:

```
Ping 47.8.4.67 -n 10
```

El promedio del tiempo de respuesta que se muestra en: "Tiempos aproximados de ida y vuelta en milisegundos" debe ser no mayor de 300ms.
Ojo. Si un sitio de internet usa un servicio CDN, al hacer ping al dominio o su dirección IP asociada, la latencia no será la real.
Para eso es necesario hacerlo a la dirección IP del servidor original.

Usar el comando PING para conocer la dirección IP

Para conocer la dirección IP que corresponde a un dominio utiliza:

```
ping -a norfipc.com
```

Usar el comando ping para saber la dirección IP de un email

Para conocer la dirección IP desde donde se ha enviado un correo electrónico o email utiliza:

```
ping mail.dominio
```

Sustituye *dominio* por el utilizado en la dirección electrónica de la cual quieres conocer la dirección IP.
Por ejemplo, el correo fué enviado desde *alejandro@fernandez.es*, utiliza:
ping mail.fernandez.es

Usar el comando ping para comprobar disponibilidad de dominios

Para comprobar dominios utiliza:

```
PING -w 7500 dominio |find "TTL=" && ECHO dominio encontrado
PING -w 7500 dominio |find "TTL=" || ECHO dominio no encontrado
```

Usar el comando ping para comprobar si existe fragmentación en la conexión

Para comprobar si existe desfragmentación en paquetes enviados, usando el valor MTU predeterminado utiliza:

```
ping google.com -f -l 1472
```

```
ping google.com -f -l 576 (conexiones dialup)
```

Usar el comando ping para monitorear disponibilidad de un servidor
Código para crear un archivo Batch que permite monitorear la conexión a un sitio web (ejemplo.com) cada 20 segundos. Útil para monitorear la disponibilidad de un servidor con múltiples caídas. Puede ser utilizado también para comprobar el servicio suministrado por tu ISP (Proveedor de acceso a internet), solo reemplaza ejemplo.com por la dirección IP correspondiente.

```
@echo off
echo Realizando ping, usa CTRL-C para detenerlo
:start
ping -n 1 ejemplo.com | find "TTL=" >>%userprofile%\Desktop\pingtest.txt
echo
ping -n 16 127.0.0.1>nul
goto start
```

Usar el comando ping para conocer si hay conexión a internet
Código para crear un archivo batch que comprueba cada 30 segundos si existe conexión a internet en el equipo local. Se logra el retraso de 30 segundos haciendo ping a una dirección IP 1.1.1.1 inexistente con el parámetro -w 30000 y posteriormente se repite el ciclo.
@echo off

```
color 0E
mode con cols=70 lines=8
: START
SET CONNECT=SI
PING 72.14.204.147 | FIND "TTL=" > NUL
IF NOT ERRORLEVEL 1 GOTO SI
IF ERRORLEVEL 1 SET CONNECT=NO
ECHO %CONNECT% tienes conexión a internet en este momento
PING 1.1.1.1 -n 10 -w 30000 >NUL
CLS
GOTO START
pause>nul
EXIT
:SI
ECHO Estas conectado a internet
PING 1.1.1.1 -n 1 -w 30000 >NUL
CLS
GOTO START
pause>nul
```

Usar el comando ping para pausar la ejecución de un comando
Código para pausar la ejecución de un segundo comando en un archivo batch durante 60 segundos.

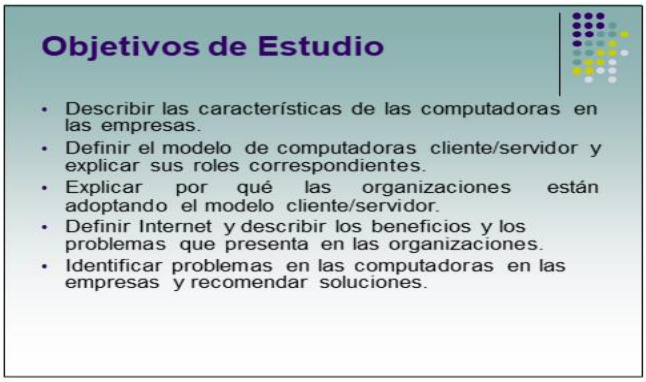
```
@echo off
echo Esperando 60 segundos...
PING -w 10000 -n 1  1.1.1.1>NUL
echo OK ha transcurrido 1 minuto
pause
```

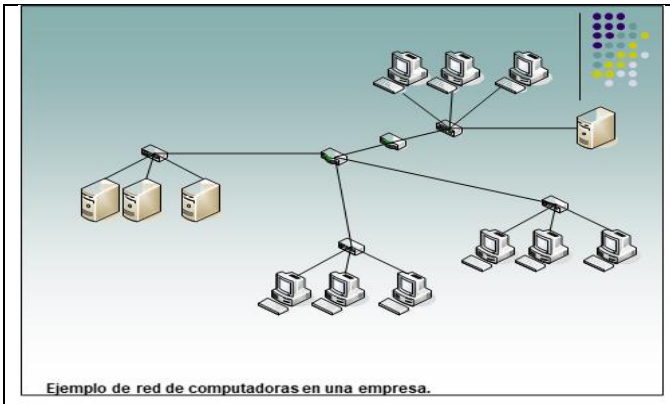
Fuente: **https://norfipc.com/redes/usar-comando-ping.html**

C. Adecuando a las necesidades de la organización

ESTRATEGIA	PRODUCTO
3. Analiza las necesidades de la organización (Anexo 3), identifica cuál de ellas obtiene mayores logros y beneficios, redacta el texto argumentativo como resultado de su análisis. *NOTA: Un texto argumentativo es aquel texto oral o escrito en los que el autor persigue la transmisión de una perspectiva en torno a un tema o una serie de temas específicos, es decir, que tiene como objetivo convencer al lector de asumir una postura determinada.*	**3- Texto argumentativo**

A N E X O - 3
COMO USAR EL COMANDO PING DE REDES





Ejemplo de red de computadoras en una empresa.

Hub

Internet

Es la mejor conocida y más grande interconexión de redes; el enlace de miles de redes individuales de todo el mundo.

El Internet nació como una red del Departamento de Defensa de los Estados Unidos que enlazaría a científicos y profesores de todo el mundo.

El Modelo Cliente – Servidor

Un modelo de computación que divide los procesos entre "clientes" y "servidores" en la red, asignando funciones a la máquina más apta para realizar dicha función.

Cliente: Es el punto de entrada del usuario para la función requerida y es normalmente es una computadora de escritorio, una estación de trabajo o una computadora portátil. El usuario generalmente interactúa directamente solamente con el cliente, típicamente a través de una interfase gráfica, para ingresar, recuperar o analizar datos.

Servidor: Satisface algunos o todos los pedidos de datos o funciones de los usuarios, como almacenar y procesar datos compartidos, o administrar dispositivos periféricos.

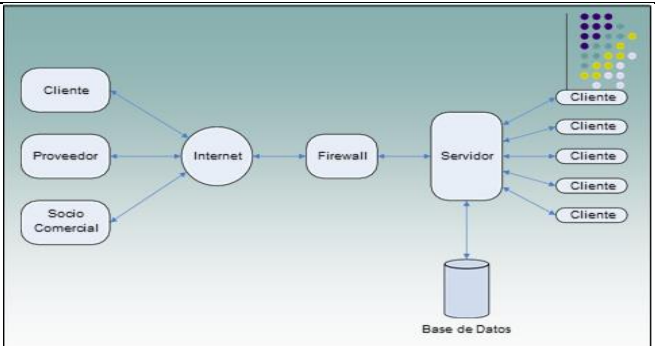
Capacidades de Internet

Capacidad	Funciones que Apoya
Correo Electrónico	Mensajes de persona a persona; compartir documentos.
Grupos de Noticias Usenet	Grupos de discusión en tableros de boletines electrónicos.
LISTSERV	Grupos de discusión empleando servidores de listas de correo electrónico.
Chat (Conversación)	Conversaciones Interactivas.
Telnet	Iniciar sesión en un sistema de computación y trabajar en otro.
FTP	Transferir archivos de una computadora a otra.
Gophers	Localizar información empleando una jerarquía de menús.
P2P, P2M	Transmitir y compartir archivos.

World Wide Web

O simplemente la Web es un sistema con estándares aceptados universalmente para almacenar, recuperar, formatear y exhibir información mediante arquitectura cliente-servidor.

Página de Inicio: Es la pantalla con texto y gráficos de la www que da la bienvenida al usuario y describe la organización que estableció la página.



Modelo de Extranet. **Solo gente selecta accede a la Intranet de la Empresa.**

Intranets y Extranets

Intranet: Es una red interna de la organización capaz de proporcionar acceso a datos de toda la empresa. Utiliza la infraestructura de red de la empresa.

Extranets: Son intranets privadas que se extienden a usuarios autorizados externos a la organización.

Beneficios de Internet para las Organizaciones

Conectividad y alcance global:

Capacidad para conectar de forma fácil y económica a un enorme número de personas de muchos lugares en todo el mundo.

Reducción de los costos de comunicación:

No solo brinda conexión a la empresa, sino que ahorra gastos de teléfono, fax, etc.

Beneficios de Internet para las Organizaciones

Costos de transacción más bajos:

Las transacciones efectuadas electrónicamente cuestan una fracción de los procesos basados en papel.

Reducción en los costos de la agencia:

Reduce el costo de manejar empleados, coordinación de trabajo, de actividades en lugares remotos a escala global.

Modelo de Negocios por Internet

Categoría	Descripción	Ejemplos
Tienda Virtual	Venta de bienes físicos o servicios en línea.	Amazon.com
Concentrador de mercado	Concentra información acerca de productos o servicios de varios proveedores en un punto central.	Internet Mall DealerNet
Corredor de Información	Ofrece información de productos, precios y disponibilidad.	PartNet Travelocity
Corredor de Transacciones	Los compradores pueden consultar tarifas y condiciones pero la actividad del negocio es cerrar la transacción	E*Trade Ameritrade
Subastas	Los consumidores presentan una oferta a los proveedores para adquirir bienes o servicios.	Ebay OnSale
Entrega digital de productos	Venta de software, productos multimedia, y productos digitales.	Built-a-card

Beneficios de Internet para las Organizaciones

Interactividad, flexibilidad, personalización:

Es posible crear aplicaciones interactivas que se pueden adaptar a diversos fines y públicos distintos.

Distribución acelerada de conocimiento:

El acceso a la información es instantánea, por lo que se usa el Internet como correo electrónico, bases de datos, depósitos de conocimiento, etc.

Problemas con el Internet

Seguridad:

El Internet lleva gran cantidad de información, lo que puede incluir estrategias de negocios, contactos de ventas e investigaciones científicas. Puede ser un medio de acceso a sitios restringidos.

Problemas Tecnológicos:

Posibles incompatibilidades en hardware y/o software impiden realizar funciones de ciertos sitios.

Problemas con el Internet

Aspectos Legales:

Piratería informática, comercio fraudulento, derechos de autor, hostigamiento, etc.

Cambios en proceso de negocios:

Se requiere una cuidadosa coordinación de las divisiones, sitios de producción, oficinas de ventas, además de una estrecha relación con clientes y proveedores.

Algunas Soluciones

Disciplinas en Administración de Datos:

Identificar dónde están los datos requeridos, identificar a las personas que tienen acceso a los datos y asegurarse que los datos sean correctos.

Controlar los costos:

Mantener las redes en buen funcionamiento, limitar el acceso a usuarios no autorizados y usar herramientas de administración de redes.

Algunas Soluciones

Administrar el Cambio:

Se debe planificar procesos de negocios, la arquitectura de la información, direccionar los datos.

Educación y Entrenamiento:

Para el buen uso del Internet en las organizaciones, solucionar problemas y apoyo técnico necesario.

¿Preguntas?

VENTANA DE LAS ORGANIZACIONES

EXPLOTING THE INTERNET

JPMorgan

¿Cómo utilizando Internet se pudo ampliar el rendimiento de las empresas presentadas aquí? ¿Cómo han cambiado estas organizaciones?

- J.P. Morgan & Co.
- Seagate Technology Inc.
- Trame Co.
- The Global Sschoolhouse Project

Marco Referencial
- El 5to banco más grande en los EEUU
- Uno de los más prestigiosos a nivel mundial.
- Llegó a usar el Internet muy tempranamente para obtener soporte técnico más eficiente.

Problemas
- La respuesta del soporte técnico del banco frente a un problema tomaba mucho tiempo.

Solución:
- El vicepresidente de la corporación tecnológica decidió que la vía más rápida para reportar problemas técnicos y obtener respuesta rápida era a través del uso de la Net (Internet).

Beneficios
- Problemas que tomaba días en ser solucionados , con el uso del Internet este esta capacidad de respuesta mejora a horas incluso minutos dependiendo del problema.
- Permite obtener y mantener información de las finanzas corporativas y o información proveniente del gobierno.
- Logro poner en línea una guía financiera que es actualizada por lo menos una vez por semana. (RiskMetrics)
  - Información sobre mediciones de riesgo
  - Información de bonos
  - Refinanciación de hipotecas
  - Índices de compras de hipoteca
  - Tasas de interés
  - Cotización de monedas
  - Etc.

Ventaja:
- Información disponible para sus clientes
- Líder proporcionando información financiera
- Posicionamiento como expertos en aspectos financieros
- Reclutamiento de personal

Marco Referencial
- Realiza el diseño, fabricación, y comercialización de discos duros para empresas, computadoras de escritorio y personales, consumidores electrónicos y soluciones calificadas para el mercado de la industria de los discos duros.

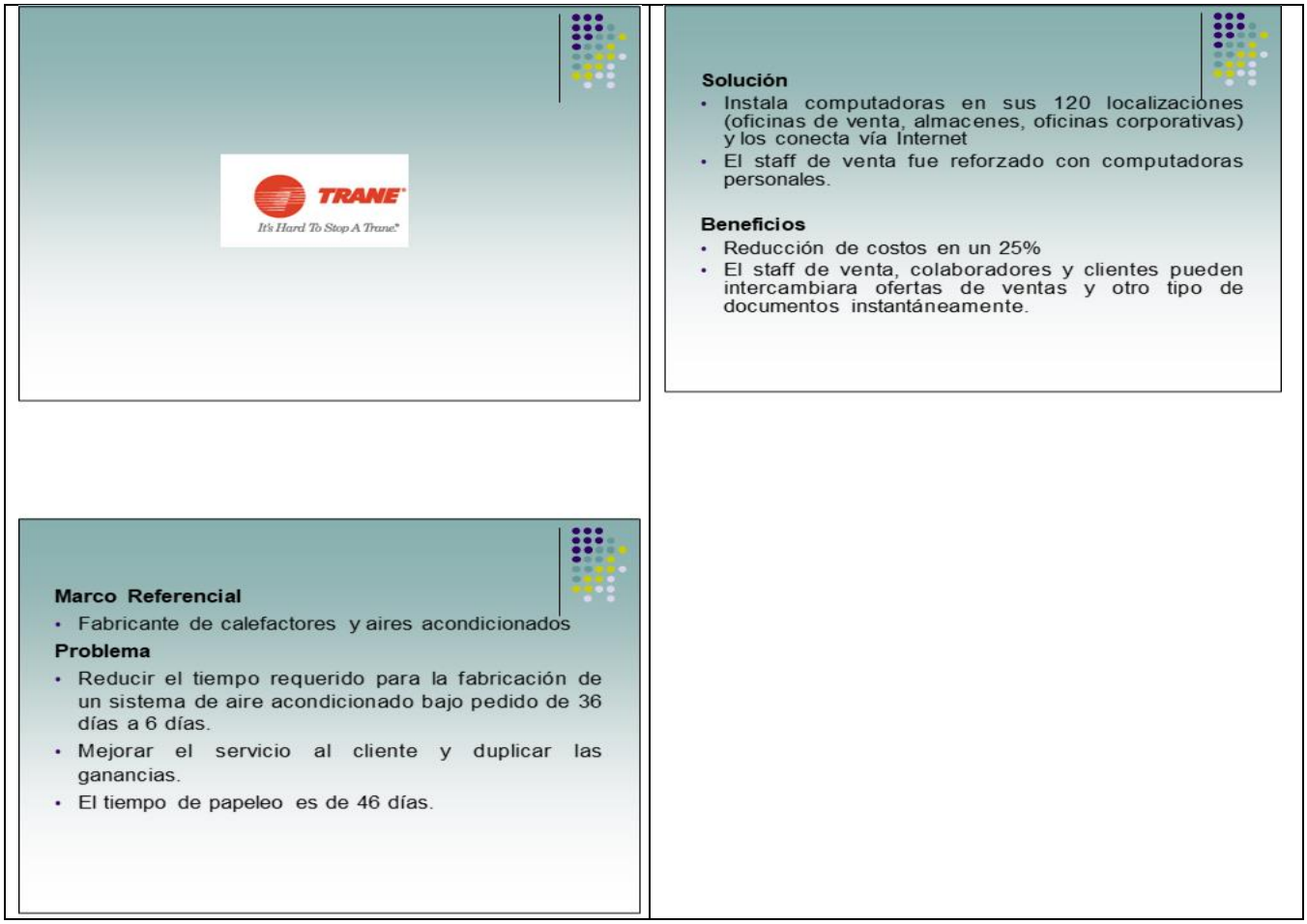
Problema
- Realizar un anuncio de reclutamiento eficiente.
  - La empresa calcula que se gastará $18000 comprando una página completa de anuncio de periódico dominical local.
- Los anuncios en periódicos tiene una vida útil pequeña (2 a 3 días)

Seagate

Solución
- Instala un Sitio Web de 22 páginas por $18000 para reclutar empleados potenciales.

Beneficio
- Los anuncios en la Net tiene una vida útil mucho mayor (3 a 4 semanas)
- Permite situar mayor información como la descripción completa de la compañía, sus objetivos y cultura organizacional.

Ventaja
- Mayor cantidad de prospectos
- Selección más eficiente.



COMPETENCIA - INSTALA DISPOSITIVOS DE INTERCONEXIÓN DE RED
CONTENIDOS:

A. Reconociendo las necesidades de la organización

ESTRATEGIA	PRODUCTO
4. Identifica las necesidades de equipos y dispositivos – periféricos de la estructura de la organización (Anexo 4) realiza la tabla de equipos y dispositivos de interconexión y el Presupuesto. *Nota: Retoma los conocimientos previos, donde conoce la integración del proyecto final (Anexo 5) de la asignatura de Diseña la red LAN en las páginas documento, y el presupuesto en la última página realizar los productos indicados.*	**4- A. Tabla de equipos y dispositivos de interconexión.** **B. Presupuesto**

A N E X O - 4
ESTRUCTURA DE LA ORGANIZACION

La estructura de la organización (por planta) sería la siguiente:

Planta principal (primera):
- Recepción
- Departamento de informática

- Departamento Comercial y atención al agente

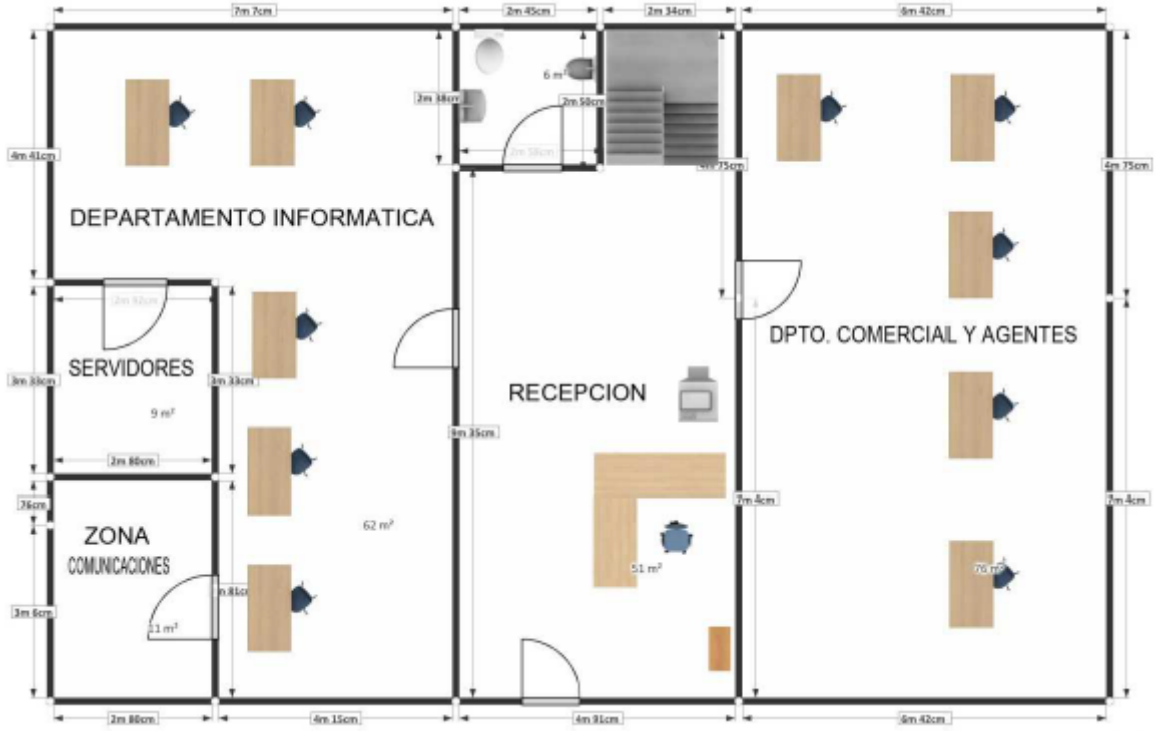


Figura 1-1 Edificio principal de la organización, Planta principal

Segunda planta:

- Atención a clientes (Call-Center)
- Departamento de administración
- Departamento de operaciones

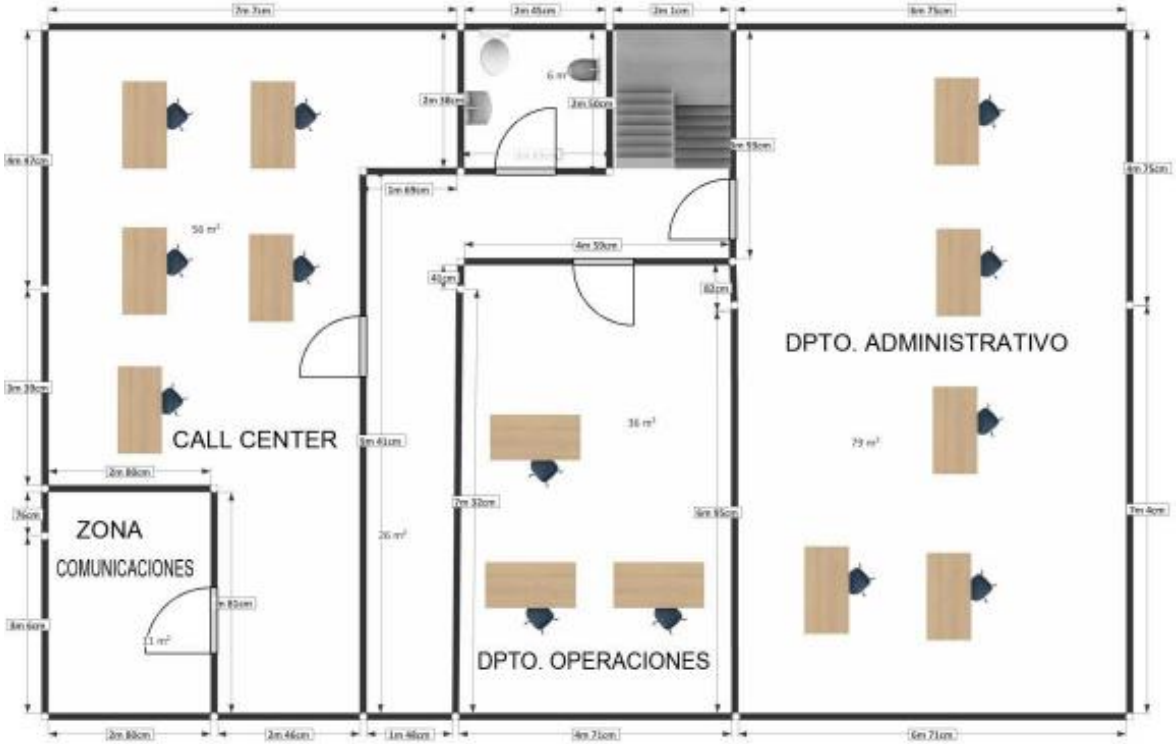


Figura 1-1 Edificio principal de la organización, Segunda planta

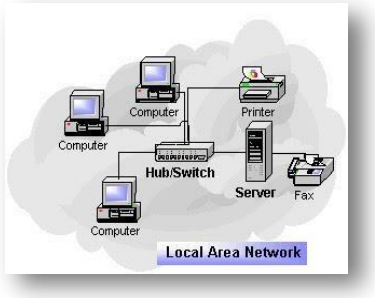
A N E X O - 5
INTEGRACION DEL PROYECTO FINAL DE LA ASIGNATURA DISEÑA LA RED LAN

INTRODUCCION

EN ESTE PROYETO SE VA A LLEBAR A CABO EL DISEÑO DE UNA RED DE AREA LOCAL EN EL CUAL SE APLICARA TODO LO APRENDIDO EN LA ESPECIALIDAD DE SOPORTE Y MANTENIMIENTO DE EQUIPOS DE COMPUTO DONDE UNA RED LAN LAN ES LA ABREVIATURA DE LOCAL AREA NETWORK (RED DE ÁREA LOCAL). UNA RED LOCAL ES LA INTERCONEXIÓN DE VARIOS ORDENADORES Y PERIFÉRICOS. SU EXTENSIÓN ESTA LIMITADA FÍSICAMENTE A UN EDIFICIO O A UN ENTORNO DE UNOS POCOS KILÓMETROS. SU APLICACIÓN MÁS EXTENDIDA ES LA INTERCONEXIÓN DE ORDENADORES PERSONALES Y ESTACIONES DE TRABAJO EN OFICINAS, FÁBRICAS, ETC; PARA COMPARTIR RECURSOS E INTERCAMBIAR DATOS Y APLICACIONES.
Y PARA SU DISEÑO TIENE QUE HABER UNA RED QUE ES UNA INTERCONEXIÓN DE COMPUTADORAS PARA COMPARTIR INFORMACIÓN, RECURSOS Y SERVICIOS. ESTA INTERCONEXIÓN PUEDE SER A TRAVÉS DE UN ENLACE FÍSICO (ALAMBRADO) O INALÁMBRICO.

Características:

* Tecnología broadcast (difusión) conel medio de transmisión compartido.
* Cableado específico instalado normalmente a propósito.
* Capacidad de transmisión comprendida entre 1 Mbpsy 1 Gbps.
* Extensión máxima no superior a3 km (Una FDDI puede llegar a 200km)
* Uso de un medio de comunicación privado.
*La simplicidad del medio de transmisión que utiliza (cable coaxial, cables telefónicos y fibra óptica).
* La facilidad con que se pueden efectuar cambios en el hardware y el software.
* Gran variedad y número de dispositivosconectados.
* Posibilidad deconexión con otras redes.



DESARROLLO
UBICACIÓN FISICA DEL ESPACIO

EL LUGAR DONDE SE ARA EL DISEÑO DE LA RED LAN SE LLEBARA A CABO EN UNA CASA QUE TIENE DIMENSIONES DE 10 X 7 X 3 m. DONDE CUENTA CON 3 PUERTAS PARA USO DE LAS PERSONAS , 1 BAÑO Y 2 VENTANAS PARA SU VENTILACION

EL LUGAR SE ENCUENTRA EN LA LOCALIDAD DE CORTAZAR GTO. EN LA COLONIA DEL VALLE DONDE ESTA BIEN LA UBICACIÓN PARA QUE LAS PERSONAS PUEDAN PUEDAN HACER SUS TRABAJOS EN ESE LUGAR.

EL NUMERO DE EQUIPOS DE COMPUTO QUE ESTARAN DENTRO DE LA RED SERAN 12

Alienware X51™

Poder de Multitareas Y TRABAJOS

Mantente en el filo cortante de tecnología con el procesador de 4ta generación Intel® Core™ i5 y 8 GB s RAM.

Precio desde $18,259 MXN

Opciones de configuración:

- Cuarta generación del procesador Intel® Core™ i5-4460 (6M Cache, up to 3.4 GHz)
- Windows 8.1, 64-bit, Español
- 8 GB Dos canales SDRAM DDR3 a 1600 MHz
- NVIDIA® GeForce® GTX 745 with 4GB DDR3
- Disco Duro SATA de 1TB 7200 RPM (6.0 Gb/s) 64MB Caché

EL NUMERO DE REGULADORES PARA LA PROTECCION DE LOS EQUIPOS DE COMPUTO SERAN 3

AMCR Acondicionador / Regulador de Voltaje Series 5000 y 3000

Opciones complementarias

- Sensor para ahorro de energía
- Bypass de mantenimiento
- Emparalelamiento
- Regulación de entrada hasta (+- 45%)
- Diseño a la medida
- Transformador de Aislamiento / Autotransformador

APLICACIONES DE SOFTWARE PARA LAS COMPUTADORAS

Office 365 Hogar (1 año)
MXN$999.99
Obtén 6 meses GRATIS de Norton Security por la compra de una suscripción anual(12 meses) de Office 365.*

Obtén una suscripción por1 año que incluye Word, Excel, PowerPoint y Outlook, almacenamiento en la nube OneDrive y llamadas por Skype desde tu computadora a teléfonos en todo el mundo, para 5 equipos PC o Mac más 5 iPad o tabletas Windows.

MOBILIARIO QUE SE REQUIERE

Ciber Mueble Doble Económico Funcional Fabricamos Escritorio 6 Pzas.

$ 725.00

Sillas Para Ciber 12 Pzas

$ 300.00

Escritorio 120x60C/cajones

$1,199.99

Silla Ejecutiva En Piel Y Malla Negra Hon

$ 3,799.00

Rack Para Servidor De Aluminio Ligero U.r 42 North00-bkl

$ 2,299.00

Bobina De Cable De Red Utp Rj45 Rollo Cable Cat 305m Dmm

$ 550.00

Roseta Doble Rj45 Para Categoría 5e, Color Blanco 6 Pzas.

$ 65.00

Switch Hp Procurve Switch 2824 24Puertos

$ 2,900.00

Plug Rj-45 Cat5 Blindado FtpBolsa 30pz

$ 90.00

Canaleta Pvc 4cm X2.5cm X 2.5m (10 Metros)

$ 180.00

Access Point Repetidor 7210n Externo 150mbps LargoAlcance

$ 869.99

Multifuncional L555 Tinta ContinuaEpson

$ 4,335.00

Modem Nuevo Lan Internet Inalambrico Infinitum servicio a internet

$ 400.00

CANTIDAD	DESCRIPCION	PRECIO UNITARIO	TOTAL
12	AlienwareX51™	$18,259MXN	$219,108
3	Regulador de Voltaje Series	$4,760	$14,280
1	Office 365 Hogar	$999.99	$999.99
6	Ciber Mueble Doble	$ 725.00	$4,350
12	Sillas Para Ciber	$ 300.00	$3,600
1	Escritorio 120x60C/cajones	$1,199.99	$1,199.99
1	Silla Ejecutiva En Piel	$ 3,799.00	$ 3,799.00
1	Rack Para Servidor De Aluminio	$ 2,299.00	$ 2,299.00
1	Cable De Red Utp Rj45 305m	$ 550.00	$ 550.00
6	Roseta Doble Rj45 Para Categoría 5e	$ 65.00	$ 390.00
1	Switch Hp Procurve 24 Puertos	$ 2,900.00	$ 2,900.00
1	Plug Rj-45 Cat5 Blindado Bolsa30pz	$90.00	$90.00
8	Canaleta Pvc 4cm X2.5cm X 2.5m	$ 180.00	$ 1,440.00
1	Access Point150mbps	$ 869.99	$ 869.99
1	Multifuncional L555 TintaContinua Epson	$ 4,335.00	$ 4,335.00
1	Modem Lan Internet Inalambrico Infinitum servicio a internet	$ 400.00	$ 400.00
			$260,610.97

C. Verificando la compatibilidad de tarjetas de red, Switch y ruteadores

ESTRATEGIA	PRODUCTO
5. Utilizando la tabla de equipos y dispositivos de interconexión de la actividad anterior, extrae las tarjetas de red, los switchs, UBS, ruteadores, Access point, Tarjetas inalámbricas, ETC, para integrar una tabla de compatibilidad con una imagen, nombre de dispositivo, sus especificaciones y características, que permitan comprobar la compatibilidad de los recursos propuestos.	**5- Tabla de compatibilidad**

D. Revisando las condiciones físicas actuales de la organización

ESTRATEGIA	PRODUCTO
6. Lee el documento de las condiciones físicas de trabajo y del diseño del lugar de trabajo (Anexo 6), así como la "Lista de chequeo" (CheckList) (Anexo 7) para identificar o comparar las condiciones dadas en el documento, con el cual debe elaborar una nueva lista de cotejo que vaya acorde a las condiciones de la organización.	**6- Lista de cotejo / Checklist**

A N E X O - 6
LAS CONDICIOES FISICAS DEL TRABAJO Y DEL DISEÑO DEL LUGAR DE TRABAJO

CONDICIONES FISICAS

Ambiente físico: Las condiciones ambientales varían considerablemente de una oficina a otra y de una fábrica a otra. Además, la evidencia indica que aun las variaciones relativamente modestas en temperatura, ruido, iluminación o calidad del aire pueden ejercer efectos apreciables en el desempeño y las actitudes del empleado.

Comprende:

- Temperatura: La temperatura es una variable donde existen grandes diferencias individuales. Así que, para maximizar la productividad, es importante que los empleados trabajen en un ambiente en el cual la temperatura esté regulada de tal manera que caiga dentro del rango aceptable del individuo.

- Ruido: La intensidad del ruido se mide en decibeles, la cual es una escala logarítmica. Una diferencia de 10 decibeles en la intensidad es realmente 10 veces la diferencia en el nivel del sonido. La evidencia de los estudios del ruido indica que ruidos constantes o predecibles generalmente no causan deterioro en el desempeño en el trabajo. Si lo hay, es a niveles de cerca de 90 decibeles, lo cual es equivalente al ruido generado por un tren subterráneo a seis metros.
  Pero los efectos del ruido impredecible parecen ser uniformemente negativos, tienden a interferir con la capacidad de los empleados de concentrarse y poner atención. Los ruidos fuertes y no predecibles también tienden a incrementar la excitación y llevar a una reducción en la satisfacción en el trabajo.

- Iluminación: La intensidad adecuada de luz depende de la dificultad de la tarea y de la precisión requerida.
  De la edad del empleado las ganancias en desempeño a niveles altos de iluminación son mucho más grandes para los viejos que para los empleados jóvenes.
  Los beneficios de un incremento en la iluminación no son lineales. Son mayores a niveles relativamente más bajos de iluminación y disminuyen en magnitud conforme la iluminación se incrementa a moderada y de ahí a niveles altos.

- Calidad del aire: En relación con el desempeño en el trabajo, la evidencia indica que diversos contaminantes pueden reducir la producción o la precisión en muchas tareas.
  La gente parece acostumbrarse al aire contaminado. La gente se vuelve menos interesada acerca de los altos niveles de contaminación y se siente menos amenazada por la exposición prolongada a tales condiciones.

EL DISEÑO DEL LUGAR DE TRABAJO:

Comprende:

- Tamaño: Definido por el metro cuadrado por empleado. el hecho de que el estatus y el espacio estén altamente correlacionados demuestra el valor simbólico que tiene la cantidad de espacio que uno controla.
  En los rangos de la gerencia, el espacio de oficina puede ser la más anhelada y peleada de todas las recompensas que la organización ofrece, después del dinero y los títulos. Debido a que connota logro y rango, no es raro que las organizaciones, especialmente las grandes, definan los metros de espacio para cada nivel en la jerarquía.
  Y debido a que el estatus es le determinante clave en el tamaño del lugar de trabajo, las desviaciones de este patrón probablemente disminuyan la satisfacción en el trabajo para aquellos individuos que se perciben a sí mismo en el límite de la discrepancia.

- Distribución: Se refiere a la distancia entre la gente y las instalaciones, influye de manera significativa en la interacción social.
  Una persona probablemente interactuará más con aquellos individuos que están más cerca físicamente, por tanto, puede influir en la información a la que uno tiene acceso y a la inclusión o exclusión de uno de los eventos de la organización.

- Privacidad/Privacia: Es en parte una función de la cantidad de espacio por persona y la distribución de ese espacio. También está influido por lo muros, divisiones y otras barreras físicas. La mayoría de los empleados desea una gran cantidad de privacía en sus trabajos. Sin embargo, la mayoría de los empleados también quieren oportunidades de interactuar con colegas, las cuales se restringen conforme la privacia aumenta.
  Existe una evidencia cada vez mayor de que el deseo de privacia es fuerte en la mayoría de la gente. La privacia limita las distracciones, las cuales pueden ser particularmente problemáticas para la gente que hace tareas complejas. Sin embargo, la tendencia es claramente hacia menos privacia en el lugar de trabajo. Se necesita más investigación para determinar si los esfuerzos organizacionales por abrir los espacios de trabajo y las preferencias individuales sobre la privacía son o no incompatibles y dan como resultado un desempeño y satisfacción menores del empleado.

Fuente: https://www.eumed.net/libros-gratis/2007a/231/103.htm

A N E X O - 7
LISTA DE CHEQUEO (CHECKLIST)

CENTRO DE TRABAJO			
USO DEL CENTRO			
INSPECCIÓN REALIZADA POR		**FECHA**	

CENTRO DE TRABAJO	SI	NO	NO APLICA	OBSERVACIONES
Características Generales				
Condiciones generales del local				
* Las características constructivas de los locales, ofrecen seguridad frente a: - Resbalones o caídas. - Choques o golpes contra objetos - Derrumbamientos o caída de materiales				
* En situación de emergencia, permiten una rápida y segura evacuación de los trabajadores.				
* Los trabajadores y/o sus representantes han recibido información sobre las medidas de prevención y protección aplicables.				
* Está prohibido el acceso de trabajadores no autorizados lugares con riesgos específicos.				
* Si existe personal con minusvalías, los lugares de trabajo están acondicionados para la autorización segura de los mismos.				
SEGURIDAD ESTRUCTURAL				
* Las condiciones estructurales tienen una solidez adecuada a las actividades previstas.				
* Techos y cubiertas ofrecen garantía suficiente para efectuar los trabajos, o se proporcionan los equipos de protección individual necesarios.				
* El acceso a techos y cubiertas sin suficientes garantías de resistencia, lo realiza personal con los equipos de protección necesarios (EPI´s, redes, plataformas móviles, etc.)				
DIMENSIONES				
* Hay tres metros de altura de suelo a techo (2,5 metros en locales comerciales, oficinas y despachos)				
* 2 m^2 de superficie libre por trabajador.				
* 10 m^3 no ocupados, por trabajador.				
* Si no se dispone de espacio suficiente en el puesto, existe espacio suficiente en las proximidades.				

CENTRO DE TRABAJO	SI	NO	NO APLICA	OBSERVACIONES
Suelos, aberturas y desniveles.				
* Suelos fijos, estables y no resbaladizos.				
* Suelos sin irregularidades ni pendientes peligrosas.				
* Pavimentos perforados con abertura inferior a 8 mm				
* Aberturas y desniveles protegidos				
* Cuando se elimina la protección de las aberturas o desniveles, se dispone de protecciones alternativas, información a los trabajadores y procedimientos de trabajo seguros .				
* Aberturas protegidas en paredes o tabiques con riesgo de caída superior a 2 metros.				
* Barandillas de materiales rígidos, con altura mínima de 90 cm, impiden el deslizamiento de personas por debajo o la caída de objetos (rodapiés) .				
Tabiques, ventanas y vanos				
* Los tabiques transparentes o translúcidos (o acristalados) de lugares accesibles, están señalizados y fabricados con materiales seguros .				
* Las operaciones de apertura, cierre, ajuste o fijación se pueden realizar de forma segura.				
* Si están abiertos no suponen riesgo de choque o caída para los trabajadores.				
* Las operaciones de mantenimiento y limpieza se efectúan sin riesgo, tanto para los trabajadores que las realizan como para los que se encuentran en los alrededores.				
Vías de circulación				
* Dimensiones adecuadas al número de usuarios.				
* Se mantiene un ancho superior a 1 metro en cualquier pasillo.				
* Separación entre paso de peatones y vehículos.				
* Vías de transito de vehículos distanciadas de cruces con puertas, pasillos de peatones, escaleras,...				
* Si procede, está señalizado el ancho de la vía.				
VIAS Y SALIDAS DE EVACUACION				
* Acordes con la normativa específica.				

CENTRO DE TRABAJO	SI	NO	NO APLICA	OBSERVACIONES
* Desembocan lo más directamente posible en la zona segura.				
* Se mantienen libres de obstáculos.				
* Número y dimensiones acordes con el riesgo y la ocupación.				
* Puertas de emergencia con apertura hacia el exterior, con sistema de apertura fácil y señalizadas				
* Disponen de iluminación de emergencia.				
Puertas y portones				
* Puertas transparentes señalizadas a la altura de la vista y de material seguro.				
* Puertas de vaivén permiten la visibilidad a la zona de acceso.				
* De acceder a escaleras, abren sobre descansillos de anchura adecuada.				
* Puertas exteriores de ancho igual o superior a 80 cm.				
Señalización y alumbrado de emergencia				
* Están señalizadas las salidas y vías de evacuación				
* Están señalizados los equipos de protección de incendios.				
* Está señalizado el riesgo eléctrico.				
* Se encuentra señalizada la prohibición de fumar en archivos y almacenes.				
* Está señalizada la ubicación del botiquín.				
* Existe instalación de alumbrado de emergencia				
* Ubicación en escaleras, vías de evacuación, vestíbulos previos y salidas.				
Incendios				
* Disponen de un manual de Autoprotección o plan de emergencia.				
* El plan de emergencia lo conoce todo el personal.				
* Disponen de suficientes vías de evacuación y salidas al exterior para el aforo del local.				
* Disponen de iluminación de emergencia.				
EXTINTORES				
* Son adecuados al tipo de fuego previsible.				
* Emplazamientos visibles y accesibles				
* Colocados sobre parámetros a menos de 1,70 m del suelo.				
* Recorrido desde cualquier punto al extintor más cercano menor de 15 metros.				

CENTRO DE TRABAJO	SI	NO	NO APLICA	OBSERVACIONES
* Precintos intactos.				
* Revisión trimestral, anual y prueba de presión cada cinco años realizada.				
* Documentación/Registro.				
DETECCIÓN Y ALARMA				
* Revisión trimestral de comprobación del correcto funcionamiento de la instalación y mantenimiento de acumuladores.				
* Revisión anual de verificación integral de la instalación.				
* Central de detección continuamente vigilada.				
Instalación eléctrica				
* Los cuadros eléctricos disponen de protección contra sobreintensidades y cortocircuitos (Magnetotérmico)				
* Se dispone de protección diferencial.				
* La instalación dispone de conexión de puesta a tierra.				
* Las puertas de los cuadros eléctricos si son metálicos disponen de conexión de puesta a tierra.				
* Se comprueba periódicamente que al pulsar el botón de comprobación, los diferenciales disparan .				
* Se evita la conexión de conductores desnudos.				
* Se evita sobrecargar los enchufes.				
* Disponen del boletín de la instalación eléctrica.				
* Realizan un mantenimiento periódico y pasan las inspecciones reglamentarias en función de las características de la instalación y uso de la actividad.				
Orden y limpieza				
* Zonas de paso y circulación libres de obstáculos.				
* Limpieza periódica.				
* Se eliminan con rapidez las manchas de residuos y sustancias peligrosas.				
* Las operaciones de limpieza se efectúan garantizando la seguridad y salud de los trabajadores.				
Condiciones ambientales				
* Se evita la exposición a temperaturas y humedades extremas.				

CENTRO DE TRABAJO	SI	NO	NO APLICA	OBSERVACIONES
* Se evitan cambios bruscos de temperatura.				
* Para trabajos sedentarios, temperatura entre 17 y 27ºC.				
* Para trabajos ligeros, temperatura entre 14 y 25ºC.				
* Humedad relativa entre 30 y el 70% (con riesgos por electricidad estática, el límite inferior superará el 50%).				
* Las corrientes de aire no producen molestias a los trabajadores.				
* Renovación de aire limpio de 30 m^3/h/trabajador, para trabajos contaminados por humo de tabaco o ambientes viciados, la renovación será de 50 m^3/h/trabajador .				
* Distribución adecuada de entradas de aire limpio y salidas de aire viciado.				
Iluminación				
* Se dispone de iluminación artificial, en caso que la natural sea insuficiente.				
* Nivel mínimo de iluminancia superior a: - 100 lux para trabajos con baja exigencia visual. - 200 lux para trabajos con exigencia visual moderada. - 500 lux para trabajos con alta exigencia visual. - 1000 lux para trabajos con exigencia visual muy alta. - 25 lux en vías de circulación de uso ocasional. - 50 lux en vías de circulación de uso habitual. - 50 lux en áreas o locales de uso ocasional. - 100 lux en áreas o locales de uso habitual.				
* Distribución uniforme del nivel de iluminación.				
* Contrastes de luminancia evitando variaciones bruscas.				
* Se evita deslumbramientos directos, por luz natural o artificial.				
* Se evitan deslumbramientos indirectos por superficies reflectantes.				
* Se evitan interferencias o efectos estroboscopios.				
Servicios Higiénicos				
* Dimensiones adecuadas para permitir la utilización sin molestias.				
* Fácil acceso y limpieza.				
* Separados para hombres y mujeres.				
* No se utilizan para fines distintos de los que fueron diseñados				

CENTRO DE TRABAJO	SI	NO	NO APLICA	OBSERVACIONES
* Agua potable en cantidad suficiente y accesible.				
VESTUARIOS				
* Provistos de asientos, armarios y taquillas con cierre individual.				
* Taquillas de tamaño adecuado para guardar la ropa y el calzado.				
* Si procede, separación en armarios y taquillas para ropa de trabajo y ropa de calle.				
* De no ser necesarios los vestuarios, se dispondrá de colgadores o armarios para guardar la ropa.				
ASEOS				
* Con espejo y lavabos de agua corriente, jabón y toallas u otros sistemas de secado				
* Duchas de agua corriente caliente y fría si se realizan trabajos sucios, contaminantes o que originen elevada sudoración.				
* Fácil comunicación entre aseos y vestuarios.				
RETRETES				
* Próximos a los puestos de trabajo.				
* Descarga automática de agua y papel higiénico.				
* Recipientes higiénicos en los de mujeres.				
* Cabinas con cierre interior y perchas.				
MATERIAL Y LOCALES DE PRIMEROS AUXILIOS				
* Se dispone de material de primeros auxilios en cantidad y características suficientes para el número de trabajadores y riesgos.				
* Se dispone, como mínimo, de un botiquín portátil.				
* Se revisan periódicamente las existencias de material.				
* Está señalizado el botiquín.				
Documentación Contratas				
* Evaluación de riesgos y planificación de la actividad preventiva para los trabajos contratados.				
* Obligaciones con respecto a los trabajadores:				
- Apto médico				
- Formación en PRL				
- Información en PRL				
- Equipos de protección				
- Contrato trabajo/Alta S.S/Cobro salarios				
* Maquinaria y equipos de trabajo:				
- Marcado CE				
- Manual de instrucciones				
- Libro mantenimiento				
- Información y formación sobre uso seguro				

CENTRO DE TRABAJO	SI	NO	NO APLICA	OBSERVACIONES
- Equipos de protección necesarios				
* Otra documentación:				
•				
•				
•				
•				
•				
•				
•				
Investigación de Incidentes				
* Se han producido incidentes con respecto a la inspección de seguridad anterior y han sido adecuadamente investigados determinándose acciones correctivas.				

S E G U N D O P A R C I A L

COMPETENCIA - REALIZA PRUEBAS DE CONECTIVIDAD

CONTENIDOS:

A. Verificando la comunicación entre el equipo del área de trabajo y el cuarto de comunicaciones

ESTRATEGIA	PRODUCTO
1. Realiza la lectura del documento "Pruebas de verificación" (Anexo 8) y realiza la actividad solicitada mediante el material indicado en el documento "Verifica la comunicación" (Anexo 9), donde entrega dicha actividad con evidencias fotográfica.	**1- Reporte de la actividad**

A N E X O - 8
PRUEBAS DE VERIFICACION

Introducción

Esta sección se dedica a explicar las pruebas de verificación aplicadas a la red inalámbrica para comprobar su correcto funcionamiento, así como del satisfactorio cumplimiento de todos los requerimientos impuestos por nuestro cliente.

Los Tests realizados han sido orientados a la certificación de los siguientes aspectos de la WLAN:

- Alimentación y conexiones de los equipos.
- Integración en la LAN de datos.
- Conectividad

Pasamos a explicarlos a continuación.

1. Alimentación y conexiones de los equipos

Tabla 1: PRUEBAS DE ALIMENTACIÓN Y CONEXIONES

Objetivo

Realizar las pruebas pertinentes para certificar que todos los equipos están adecuadamente alimentados, están encendidos y están funcionando correctamente.

Descripción de las pruebas

- Verificar el estado de las luces de los equipos.
- Verificar las conexiones de sus cables.

Comprobamos que todas las conexiones de cables y equipos son correctas

Resultados obtenidos

Estado de las luces de los APs

APs de la primera y segunda planta [AP8, AP19]

Luz	Estado	Conclusiones
Power	Verde	On
Ethernet	Verde Parpadeando	Conecta do a una red Ethernet Transmitiendo
WLAN	Verde	On

APs de la planta baja [AP1, AP7]

Luz	Estado	Conclusiones
Power	Apagada	**Off**
Ethernet	Apagada	**Sin conexión a una red Ethernet Sin transmisión**
WLAN	Apagada	**Off**

Estado de las luces de los PoE Splitters

Luz	Estado	Conclusiones
Power	Verde	On

PoE Splitters de la primera y segunda planta [PoE-Split-8, PoE-Split-19]

Luz	Estado	Conclusiones
Power	Apagada	**Off**

PoE Splitters de la planta baja [PoE-Split-1, PoE-Split-7]

Estado de las luces del PoE Switch

Luces generales

Luz	Estado	Conclusiones
PWR	Verde	On
SYS	Verde	On
ALM	Apagada	Funcionamiento correctamente

Puertos Ethernet primera y segunda planta [8-19]

Luz	Estado	Conclusiones
LNK/ ACT	Ámbar Parpadeando	Puerto levantado Transmitiendo
POE	Ámbar	Alimentación suministrada al puerto
100/ 1000	Verde	Uplink a 1Gbps levantado
ACT	Verde Parpadeando	Conectado a una red Ethernet Transmitiendo

Puertos Ethernet planta baja [1-7]

Luz	Estado	Conclusiones
LNK/ ACT	Apagado	**Puerto no levantado**
POE	Apagado	**Alimentación no suministrada al puerto**
ACT	Apagado	**Sin conexión a una red Ethernet Sin transmisión**

Incidencia

En la planta baja no hay cobertura de la WLAN ya que sus APs no están funcionando.

Los APs de la planta baja no están siendo alimenta dos

Síntomas

Los PoE Splitters no están recibiendo alimentación

Los puertos Ethernet del switch correspondientes a los APs de la planta baja no están recibiendo alimentación del módulo PoE del switch.

Diagnósticos

1. Los puertos del switch correspondientes a la planta baja no están levanta dos → es descartad o cuando entramos en la configuración del switch y vemos que efectivamente tiene todos sus puertos levantados.

2. El switch no puede alimentar a más de 12 PDs (Powered Devices) simultáneamente → confirmamos el diagnóstico consultando al soporte técnico del fabricante y estudiando las especificaciones del producto:

$$\frac{185 Watios\ /\ switch}{15{,}4 Watios\ /\ PD} = 12 PDs\ /\ switch$$

Solución propuesta

Instalar un segundo PoE Switch y así aumentar la capacidad de alimentación Po E hasta 24 APs simultáneamente.

Repartir las conexiones de los APs entre los dos PoE Switches para repartir el consumo de potencia entre ambos

Actuaciones

Comunicación de la incidencia al cliente y propuesta de la solución

Aprobación del cliente

Modificaciones pertinentes del diseño

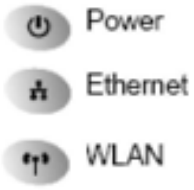
Acopio del material necesario

Configuración, instalación y puesta en marcha

Verificación de la resolución de la avería

Comunicación de la incidencia, propuesta de la solución y aprobación del cliente

Comunicamos al cliente la incidencia surgida y le planteamos la solución que TCNS cree más adecuada para resolverla. Tras un estudio del presupuesto presentado, el cliente la aprueba, por lo que pasamos a ejecutarla.

Tabla 2: NUEVAS PRUEBAS DE ALIMENTACIÓN Y CONEXIONES	
Resultados obtenidos en las nuevas pruebas	**Comprobamos que todas las conexiones de cables y equipos son correctas** Estado de las luces de los APs **APs de la primera, segunda y planta baja [AP1, AP19]**  Estado de las luces de los PoE Splitters **PoE Splitters de la primera, segunda y planta baja [PoE-Split-1, PoE-Split-19]** Estado de las luces del PoE Switch **Luces generales**
Conclusiones	Incidencia resuelta. Los equipos están bien conectados y alimentados

2. Integración en la LAN de datos

Tabla 3: PRUEBAS DE INTEGRACIÓN DE LA WLAN EN LA LAN DE DATOS

Objetivo de las pruebas	Realizar las pruebas pertinentes para certificar que la WLAN de WLTC forma parte de su LAN de datos.
Descripción de las pruebas	- Hacer ping desde el router de la LAN de datos hasta cada uno de los puntos de acceso de nuestra WLAN. - Hacer ping desde un equipo cualquiera de la LAN de datos hasta un equipo asociado a un punto de acceso cualquiera de la WLAN.

Resultados obtenidos	Pings desde el router a cada uno de los APs, es decir, ping a todas las direcciones desde la 10.122.62.101 hasta la 10.122.62.119.
	`C:\>ping 10.122.62.111`
	`Haciendo ping a 10.122.62.111 con 32 bytes de datos:`
	`Respuesta desde 10.122.62.111: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.62.111: bytes=32 tiempo=4ms TTL=255`
	`Respuesta desde 10.122.62.111: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.62.111: bytes=32 tiempo=1ms TTL=255`
	`Estadísticas de ping para 10.122.62.111:`
	`Paquetes: enviados = 4, recibidos = 4, perdidos = 0`
	`(0% perdidos),`
	`Tiempos aproximados de ida y vuelta en milisegundos:`
	`Mínimo = 1ms, Máximo = 4ms, Media = 1ms`
	Los pings al resto de direcciones presentan resultados con el mismo éxito.
	Ping desde un equipo de la LAN de datos hasta un equipo de la WLAN. Por ejemplo, desde un equipo con dirección 10.122.61.141 a un portátil asociado al AP 19 que tiene la dirección 10.122.62.135
	`C:\>ping 10.122.62.135`
	`Haciendo ping a 10.122.62.135 con 32 bytes de datos:`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=4ms TTL=255`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=1ms TTL=255`
	`Estadísticas de ping para 10.122.62.135:`
	`Paquetes: enviados = 4, recibidos = 4, perdidos = 0`
	`(0% perdidos),`
	`Tiempos aproximados de ida y vuelta en milisegundos:`
	`Mínimo = 1ms, Máximo = 4ms, Media = 1ms`

Conclusiones	Certificamos que la WLAN está perfectamente integra da en la LAN de datos del cliente, ya que desde el router hay conectividad con todos los APs, y un usuario de la LAN de datos puede establecer comunicación con un usuario de la WLAN.

3. Conectividad

Tabla 4: PRUEBAS DE CONECTIVIDAD	
Objetivo de las pruebas	Realizar las pruebas pertinentes para certificar que hay conectividad usuario a usuario y usuario a aplicación, además de acceso a Internet.
Descripción de las pruebas	- Hacer ping desde un equipo de la WLAN a la dirección IP de la puerta de enlace predeterminada.
	- Hacer ping desde un equipo de la WLAN a la dirección IP del servidor de aplicaciones de la LAN para comprobar la conectividad usuario a aplicación.
	- Hacer ping desde un equipo de la WLAN a la dirección IP pública de una página web conocida para comprobar el acceso a Internet.
	- Hacer ping desde un equipo de la WLAN a un equipo de la LAN de datos para comprobar la conectividad usuario WLAN a usuario LAN.
	- Hacer ping desde un equipo de la WLAN a otro equipo de la WLAN para comprobar la conectividad entre usuarios de la WLAN.
	- Intentar visitar varias páginas webs desde distintos emplazamientos del edificio

Resultados obtenidos	Ping desde un equipo de la WLAN a la puerta de enlace predeterminad a.
	`C:\>ping 10.122.60.50`
	`Haciendo ping a 10.122.60.50 con 32 bytes de datos:`
	`Respuesta desde 10.122.60.50: bytes=32 tiempo=10ms TTL=255`
	`Respuesta desde 10.122.60.50: bytes=32 tiempo=2ms TTL=255`
	`Respuesta desde 10.122.60.50: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.60.50: bytes=32 tiempo=1ms TTL=255`
	`Estadísticas de ping para 10.122.60.50:`
	`Paquetes: enviados = 4, recibidos = 4, perdidos = 0`
	`(0% perdidos),`
	`Tiempos aproximados de ida y vuelta en milisegundos:`
	`Mínimo = 1ms, Máximo = 10ms, Media = 3ms`

	Ping desde un equipo de la WLAN al servidor de aplicaciones.
	`C:\>ping 10.122.60.60`
	`Haciendo ping a 10.122.60.60 con 32 bytes de datos:`
	`Respuesta desde 10.122.60.60: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.60.60: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.60.60: bytes=32 tiempo=1ms TTL=255`
	`Respuesta desde 10.122.60.60: bytes=32 tiempo=1ms TTL=255`
	`Estadísticas de ping para 10.122.60.60:`
	`Paquetes: enviados = 4, recibidos = 4, perdidos = 0`
	`(0% perdidos),`
	`Tiempos aproximados de ida y vuelta en milisegundos:`
	`Mínimo = 1ms, Máximo = 1ms, Media = 1ms`

	Ping desde un equipo de la WLAN a una página web.
	`C:\>ping www.google.com`
	`Haciendo ping a www.l.google.com [216.239.59.99] con 32 bytes de datos:`
	`Respuesta desde 216.239.59.99: bytes=32 tiempo=81ms TTL=242`
	`Respuesta desde 216.239.59.99: bytes=32 tiempo=87ms TTL=241`
	`Respuesta desde 216.239.59.99: bytes=32 tiempo=82ms TTL=240`
	`Respuesta desde 216.239.59.99: bytes=32 tiempo=90ms TTL=241`
	`Estadísticas de ping para 216.239.59.99:`
	`Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),`
	`Tiempos aproximados de ida y vuelta en milisegundos:`
	`Mínimo = 81ms, Máximo = 90ms, Media = 85ms`

	Ping desde un equipo de la WLAN a otro equipo de la LAN.
	`C:\>ping 10.122.61.141`
	`Haciendo ping a 10.122.61.141 con 32 bytes de datos:`
	`Respuesta desde 10.122.61.141: bytes=32 tiempo=25ms TTL=255`
	`Respuesta desde 10.122.61.141: bytes=32 tiempo=22ms TTL=255`
	`Respuesta desde 10.122.61.141: bytes=32 tiempo=20ms TTL=255`
	`Respuesta desde 10.122.61.141: bytes=32 tiempo=20ms TTL=255`
	`Estadísticas de ping para 10.122.62.141:`
	`Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),`
	`Tiempos aproximados de ida y vuelta en milisegundos:`
	`Mínimo = 20ms, Máximo = 25ms, Media = 21ms`

	Ping desde un equipo de la WLAN a otro equipo de la WLAN.
	`C:\>ping 10.122.61.135`
	`Haciendo ping a 10.122.62.135 con 32 bytes de datos:`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=15ms TTL=255`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=10ms TTL=255`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=10ms TTL=255`
	`Respuesta desde 10.122.62.135: bytes=32 tiempo=10ms TTL=255`
	`Estadísticas de ping para 10.122.62.135:`
	`Paquetes: enviados = 4, recibidos = 4, perdidos = 0 (0% perdidos),`
	`Tiempos aproximados de ida y vuelta en milisegundos:`
	`Mínimo = 10ms, Máximo = 15ms, Media = 11ms`

	Podemos conectarnos a Internet y visitar varias páginas webs desde los distintos emplazamientos del edificio.
Conclusiones	Vistos los resultados obtenidos certificamos que hay conectividad con el router, usuario a usuario (sea de la WLAN o de la LAN cableada), usuario a aplicación, y acceso a Internet.

Fuente: extraído de http://bibing.us.es/proyectos/abreproy/11579/fichero/n.+Secci%C3%B3n+5+-+Pruebas+de+Verificaci%C3%B3n.pdf+

A N E X O - 9
VERIFICA LA COMUNICACION

VERIFICANDO LA COMUNICACIÓN ENTRE EL EQUIPO DEL ÁREA DE TRABAJO
Y EL CUARTO DE COMUNICACIONES

El estudiante realizara las pruebas de verificación de los dispositivos de interconexión, con los recursos que cuenta en casa o en algún lugar donde haya conexión a internet.
El documento Pruebas de verificación consta de 3 aspectos, y muestra ejemplo de cómo obtener las pruebas indicadas.
La actividad consiste en realizar las pruebas mencionadas en cada una de las tablas y realizar la toma de fotografía como evidencias:

En la **tabla 1, pruebas de alimentación y conexiones por medio del cable ethernet**, solicita las pruebas:

1. Verificar el estado de las luces de los equipos.
2. Verificar las conexiones de sus cables.
3. Comprobamos que todas las conexiones de cables y equipos son correctas

En la **tabla 2, nuevas pruebas de alimentación y conexiones inalámbricas**, solicita la prueba:

1. Verificar el estado de las luces de los equipos, observa que considera la conexión por medio a WIFI o inalámbrica.
2. Verificar el estado de las luces de los equipos, por medio de las 2 conexiones: por cable e inalámbrica.

En la **tabla 3, pruebas de integración de la WLAN en la LAN de datos**, solicita las pruebas:
Para obtener la **IP de su router**, mediante el comando ipconfig e **identificando "Puerta de enlace predeterminada"**, es importante, no confundirse con la "Direccion IPv4" es la dirección física de tu equipo, u otro dispositivo conectado a red, lo mismo ocurre con la dirección IPv6.

Enseguida debe seguir con las pruebas indicadas.

1. Hacer ping desde el router de la LAN de datos hasta cada uno de los puntos de acceso de nuestra WLAN.
2. Hacer ping desde el equipo personal de la LAN de datos.
3. Hacer ping desde un **equipo cualquiera** de la LAN de datos hasta un **equipo asociado** a un punto de acceso cualquiera de la WLAN

En la **tabla 4, pruebas de conectividad**, solicita las pruebas:

1. Hacer ping desde un equipo de la WLAN a la dirección IP de la puerta de enlace predeterminada.
2. Hacer ping desde un equipo de la WLAN a la dirección IP pública de una página web conocida para comprobar el acceso a Internet.
3. Hacer ping desde un equipo de la WLAN a un equipo de la LAN de datos para comprobar la conectividad usuario WLAN a usuario LAN.
4. Hacer ping desde un equipo de la WLAN a otro equipo de la WLAN para comprobar la conectividad entre usuarios de la WLAN.

INDICACIONES

- Te puedes apoyar totalmente del anexo 7, para llenar la información de la actividad solicitada
- Se muestra en la parte de abajo el texto que lleva la integración de la actividad y crea un trabajo en tu cuaderno.

VERIFICANDO LA COMUNICACIÓN ENTRE EL EQUIPO DEL ÁREA DE TRABAJO Y EL CUARTO DE COMUNICACIONES

TABLA 1 PRUEBAS DE ALIMENTACIÓN Y CONEXIONES POR MEDIO DEL CABLE ETHERNET

1. Verificar el estado de las luces de los equipos.
   AQUÍ COLOCAS LA EVIDENCIA

2. Verificar las conexiones de sus cables.
   AQUÍ COLOCAS LA EVIDENCIA

3. Comprobamos que todas las conexiones de cables y equipos son correctas
   AQUÍ COLOCAS LA EVIDENCIA

En la tabla 3, pruebas de integración de la WLAN en la LAN de datos, solicita las pruebas:

1. Hacer ping desde el router de la LAN de datos hasta cada uno de los puntos de acceso de nuestra WLAN.
   AQUÍ COLOCAS LA EVIDENCIA

2. Hacer ping desde el equipo personal de la LAN de datos.
   AQUÍ COLOCAS LA EVIDENCIA

3. Hacer ping desde un equipo cualquiera de la LAN de datos hasta un equipo asociado a un punto de acceso cualquiera de la WLAN
   AQUÍ COLOCAS LA EVIDENCIA

En la tabla 4, pruebas de conectividad, solicita las pruebas:

1. Hacer ping desde un equipo de la WLAN a la dirección IP de la puerta de enlace predeterminada.
   AQUÍ COLOCAS LA EVIDENCIA

2. Hacer ping desde un equipo de la WLAN a la dirección IP pública de una página web conocida para comprobar el acceso a Internet.
   AQUÍ COLOCAS LA EVIDENCIA

3. Hacer ping desde un equipo de la WLAN a un equipo de la LAN de datos para comprobar la conectividad usuario WLAN a usuario LAN.
   AQUÍ COLOCAS LA EVIDENCIA

4. Hacer ping desde un equipo de la WLAN a otro equipo de la WLAN para comprobar la conectividad entre usuarios de la WLAN.
   AQUÍ COLOCAS LA EVIDENCIA

B. Comprobando la comunicación entre los dispositivos de interconexión

ESTRATEGIAS	PRODUCTOS
2. Lee la "Conexión de dispositivos de red y verificación de conectividad" (Anexo 10), elabora un resumen; Identifica y subraya donde especifique la verificación de la conectividad.	**2- Resumen**
3. Analiza las "diferentes pruebas de conectividad" (Anexo 11) de la lectura del documento, crea un cuadro comparativo de las pruebas mencionadas.	**3- Cuadro comparativo**

A N E X O - 10
CONEXIÓN DE DISPOSITIVOS DE RED Y VERIFICACIÓN DE CONECTIVIDAD

00:00 conexión de dispositivos de red y
00:02 verificación de conectividad después de
00:06 que se terminaron los cables
00:07 en los patchs panel y el cableado vertical
00:11 en los distribuidores de fibra óptica y
00:13 de que se instalaron los dispositivos de
00:15 red en el bastidor de telecomunicaciones
00:18 la tarea siguiente es conectar los
00:21 cables que vienen desde los puestos de trabajo
00:24 y que están terminados en conectores
00:28 rj45 en el patch panel al puerto
00:31 asignado en el switch o concentrador y
00:34 después conectar el switch al router o
00:37 al cableado vertical de fibra óptica
00:39 para enlazar con otro segmento de la red
00:42 ubicado en otro piso o edificio
00:45 dependiendo de la capacidad y extensión
00:48 de la red de datos se requiere de varios
00:50 dispositivos de red con el propósito de
00:53 enlazar las computadoras y compartir los
00:56 recursos que contienen para enlazar un
00:59 sitio de trabajo al switch primero debes
01:01 conectar un cable de red de la placa de
01:04 pared a la tarjeta de red de la
01:06 computadora después trasladarse al Site
01:10 y mediante un cordón de parche o
01:11 conectar una punta al puerto del patch
01:14 panel que necesitas poner en operación
01:17 y la otra punta a un puerto del switch una
01:21 vez hecho esto de forma inmediata
01:23 comenzará a parpadear un indicador
01:25 luminoso de color verde al frente del
01:27 switch el cual indica que hay un enlace
01:30 entre los dos equipos de no ser así
01:34 verifican los cables de red debes
01:36 realizar el mismo procedimiento para
01:39 conectar los demás sitios de trabajo con
01:41 el switch para conectar el switch a un
01:44 router necesitas un cordón de parche o
01:47 del router hasta el puerto donde se
01:49 localizan los switch que están
01:51 destinados para enlazar a todos los
01:53 usuarios que se conectaron a los pacths
01:56 panel conecta a una punta al router y
01:59 otra punta al switch para conectar el
02:02 servidor necesitas un cordón de parcheo
02:05 el servidor hasta el rack donde se
02:08 localizan los switch
02:10 para hacer un enlace de un piso a otro
02:12 de la misma red lo debes hacer
02:14 utilizando el cableado vertical de fibra
02:17 óptica conectando el puerto óptico del
02:19 router a los puertos ópticos del
02:21 distribuidor de fibras ópticas
02:24 utilizando un jumper de fibra óptica
02:26 multimodo
02:28 para verificar la conectividad entre la
02:30 computadora ubicada en el sitio de
02:32 trabajo y el servidor vamos a considerar
02:35 que ya se realizó la configuración
02:37 básica de la red y que todos los

02:39 dispositivos de red tienen asignada una
02:41 dirección IP entonces debes enviar un
02:45 comando ping al servidor para ejecutar
02:48 comandos del sistema operativo debes
02:50 abrir una ventana de comandos el
02:53 procedimiento es similar para los
02:54 distintos sistemas operativos en los
02:57 ejemplos vamos a utilizar el modo de
03:00 consola de windows para entrar a este
03:02 debes realizar lo siguiente
03:05 haz clic en inicio y luego en ejecutar
03:09 escribe cmd en el cuadro que dice abrir
03:13 y a continuación presiona entrar
03:17 obtén la dirección IP del servidor vamos
03:20 a considerar que es la dirección
192.168.1.102
03:24 ejecuta el comando
03:30 ping escribiendo en la línea de comandos
03:33 ping 192.168.1.102 más la
03:41 tecla entrar
03:43 verifica que se reciba respuesta desde
03:46 la dirección 192.168.1.102
03:52 0% de paquetes perdidos si no hay
03:56 conexión entre el equipo y el servidor
03:58 se presenta el mensaje tiempo de espera
04:02 agotado para su solicitud 100% de
04:04 paquetes perdidos es necesario buscar e
04:08 problema de conectividad el cual puede
04:10 ser causado por la conexión física o por
04:13 la configuración
04:15 recuerda que para realizar la conexión
04:17 física de los dispositivos de red
04:19 debes ubicar el nodo en el sitio de
04:22 trabajo y conectar la computadora a la
04:24 placa de pared utilizando un cable de
04:27 red después debes trasladarse al
04:30 bastidor de telecomunicaciones y ubicar
04:32 en el patch panel el puerto
04:34 correspondiente al sitio de trabajo
04:36 conectar al puerto que tenga asignado en
04:39 el switch utilizando un cordón de
04:41 parcheo y comprobar la conexión
mediante
04:44 el encendido del indicador luminoso
04:46 correspondiente la conexión entre
04:49 switches, routers y la interconexión con
04:51 otros segmentos de la red ubicados en
04:54 otros pisos se realizan mediante el
04:56 cableado vertical la verificación de
04:59 conectividad se recomienda realizarla
05:01 utilizando el comando ping

Fuente: https://www.youtube.com/watch?v=oS2batpy2mE

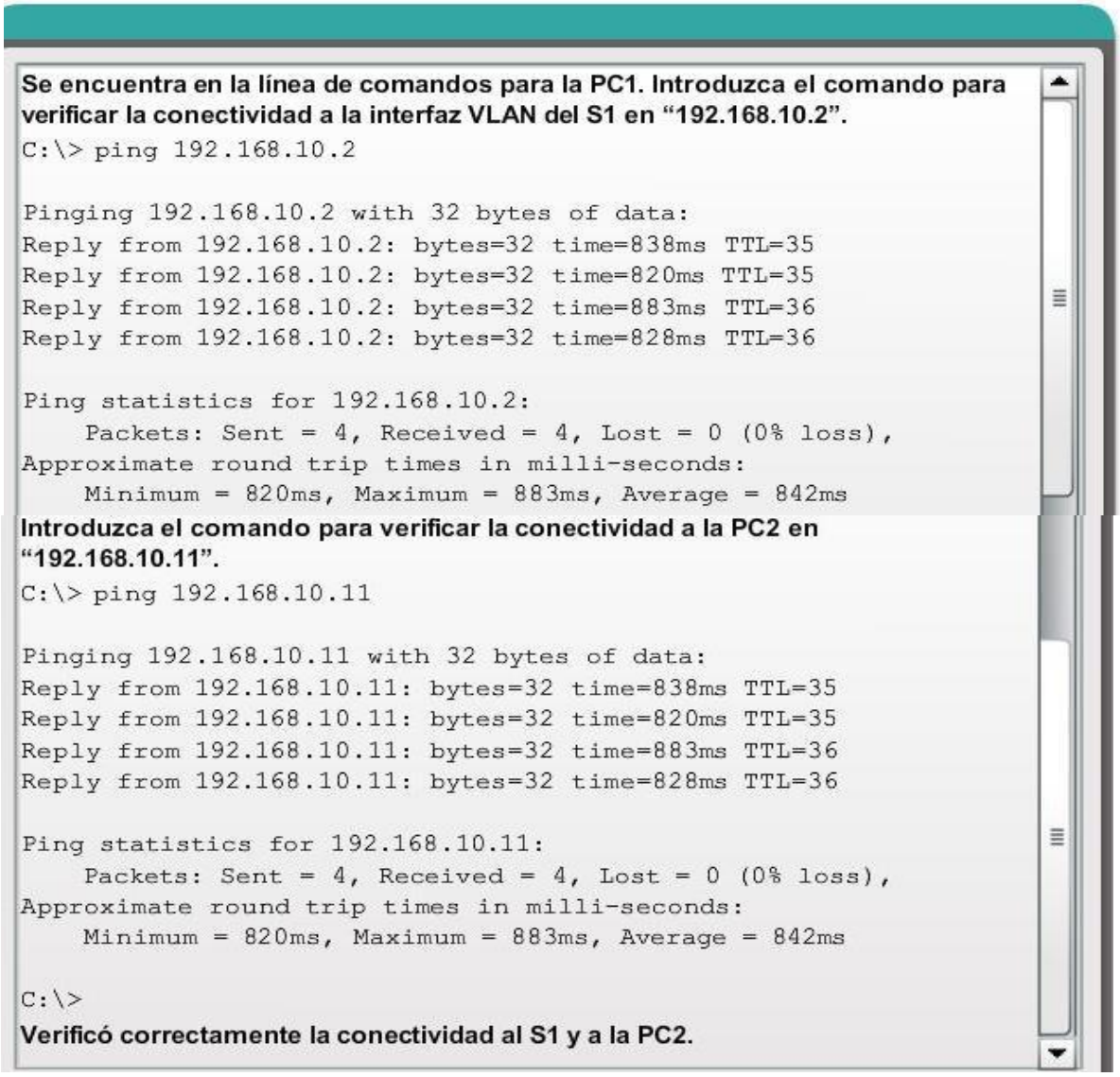
A N E X O - 11
PRUEBAS DE CONECTIVIDAD

REALIZA PRUEBAS DE CONECTIVIDAD

Prueba de la conectividad de extremo a extremo
Prueba de la conectividad de PC a switch
El comando ping se puede utilizar en una PC de la misma forma que en un dispositivo Cisco IOS. En la ilustración, se muestra que el ping de la PC1 a la dirección IP de la interfaz VLAN 1 del S1, 192.168.10.2, debe ser correcto.

Prueba de la conectividad de extremo a extremo
La dirección IP de la PC1 es 192.168.10.10, con una máscara de subred 255.255.255.0 y un gateway predeterminado 192.168.10.1.
La dirección IP de la PC2 es 192.168.10.11, con una máscara de subred 255.255.255.0 y un gateway predeterminado 192.168.10.1.
El ping de la PC1 a la PC2 también debe ser correcto. Si un ping de la PC1 a la PC2 se realiza correctamente, se verifica la conectividad de extremo a extremo en la red.

Prueba de la conectividad de extremo a extremo



Conectividad de extremo a extremo, MAC e IP

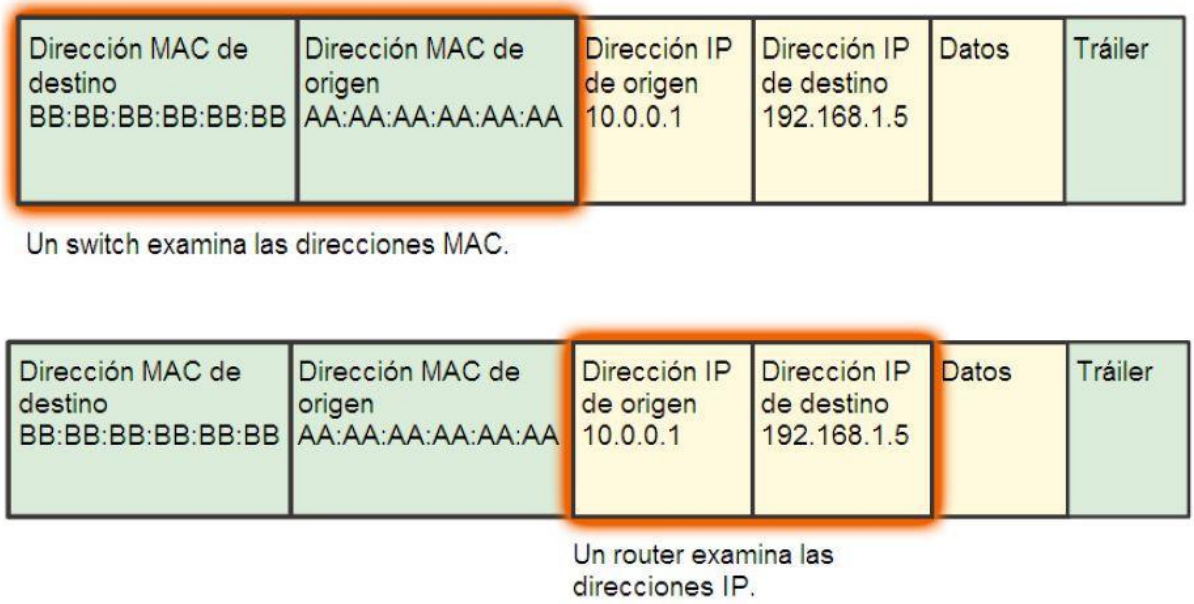
Un dispositivo de origen envía un paquete sobre la base de una dirección IP. El servicio de nombres de dominios (DNS), en el que una dirección IP se asocia a un nombre de dominio, es una de las formas más comunes en que un dispositivo de origen determina la dirección IP de un dispositivo de destino. Por ejemplo, www.cisco.com equivale a 209.165.200.225. Esta dirección IP envía el paquete a la ubicación de red del dispositivo de destino. Los routers utilizan esta dirección IP para determinar el mejor camino para llegar a destino. Entonces, en resumen, el direccionamiento IP determina el comportamiento de extremo a extremo de un paquete IP.

Sin embargo, en cada enlace de la ruta, se encapsula un paquete IP en una trama específica de la tecnología de enlace de datos particular relacionada con ese enlace, como Ethernet. Los dispositivos finales en una red Ethernet no aceptan ni procesan tramas según las direcciones IP. Por el contrario, las tramas se aceptan y procesan según las direcciones MAC.

En las redes Ethernet, las direcciones MAC se utilizan para identificar, en un nivel inferior, los hosts de origen y destino. Cuando un host de una red Ethernet se comunica, envía tramas que contienen su propia dirección MAC como origen y la dirección MAC del destinatario previsto como destino.

Todos los hosts que reciben la trama leerán la dirección MAC de destino. El host procesa el mensaje solo si la dirección MAC de destino coincide con la dirección MAC configurada en su NIC.

En la figura 1, se muestra cómo se encapsula un paquete de datos, que contiene información de la dirección IP, con el entramado de la capa de enlace de datos, que contiene información de la dirección MAC.



Ping para prueba de conectividad a la LAN local

También es posible utilizar ping para probar la capacidad de comunicación del host en la red local. Por lo general, esto se realiza haciendo ping a la dirección IP del gateway del host. Un ping al gateway indica que la interfaz del host y la interfaz del router que cumplen la función de gateway funcionan en la red local.

Para esta prueba, se usa la dirección de gateway con mayor frecuencia, debido a que el router normalmente está en funcionamiento. Si la dirección de gateway no responde, se puede enviar un ping a la dirección IP de otro host en la red local que se sepa que funciona.
Si el gateway u otro host responden, los hosts locales pueden comunicarse correctamente a través de la red local. Si el gateway no responde, pero otro host sí lo hace, esto podría indicar un problema con la interfaz del router que funciona como gateway.

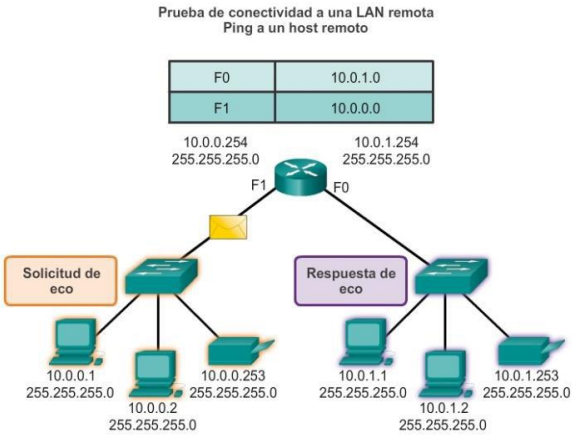
Una posibilidad es que se haya configurado la dirección de gateway incorrecta en el host. Otra posibilidad es que la interfaz del router puede estar en funcionamiento, pero se le ha aplicado seguridad, de manera que no procesa o responde a peticiones de ping.

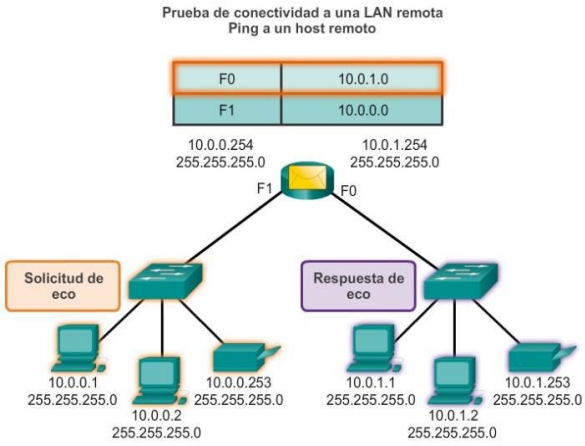
Ping para prueba de conectividad a dispositivo remoto
También se puede utilizar ping para probar la capacidad de un host local para comunicarse a través de una internetwork. El host local puede hacer ping a un host IPv4 operativo de una red remota, como se muestra en la ilustración.

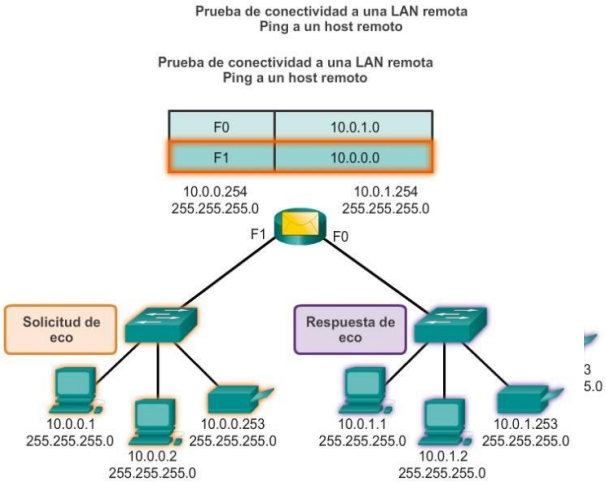
Si este ping se realiza correctamente, se puede verificar el funcionamiento de una amplia porción de la internetwork. Un ping correcto a través de la internetwork confirma la comunicación en la red local, el funcionamiento del router que funciona como gateway y el funcionamiento de todos los otros routers que podrían estar en la ruta entre la red local y la red del host remoto.

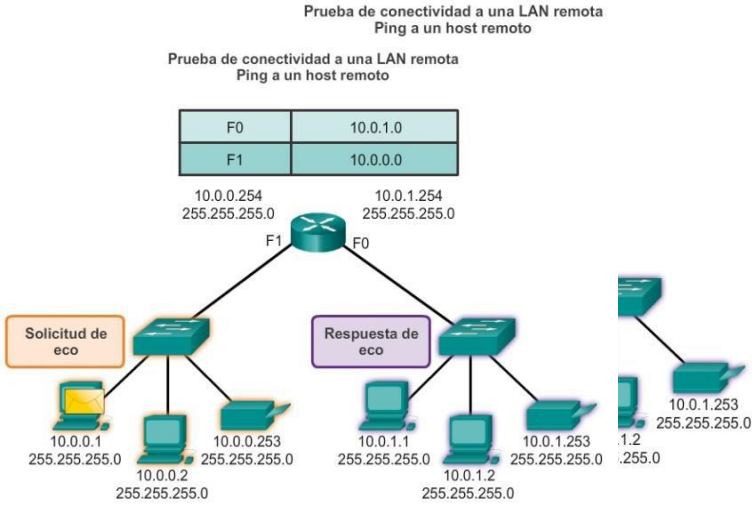
Además, es posible verificar la funcionalidad del host remoto. Si el host remoto no podía comunicarse fuera de la red local, no hubiera respondido.

NOTA: muchos administradores de red limitan o prohíben la entrada de mensajes de ICMP a la red corporativa; motivo por el cual la ausencia de una respuesta de ping podría deberse a restricciones de seguridad.









Habilitación de la conectividad inalámbrica
Para habilitar la conectividad inalámbrica, se debe configurar el modo inalámbrico, el SSID, el canal de RF y cualquier mecanismo de encriptación de seguridad deseado.

Primero, seleccione el modo inalámbrico correcto, como se muestra en la ilustración. Al seleccionar el modo, o el estándar inalámbrico, cada modo incluye una sobrecarga determinada. Si todos los dispositivos en la red utilizan el mismo estándar, seleccionar el modo asociado a ese estándar limita la cantidad de sobrecarga que se genera. También aumenta la seguridad, dado que no permite que se conecten dispositivos con estándares diferentes. No obstante, si necesitan acceder a la red dispositivos que utilizan estándares diferentes, se debe seleccionar el modo mixto. El rendimiento de la red disminuirá debido a la sobrecarga adicional ocasionada por admitir todos los modos.

A continuación, establezca el SSID. Todos los dispositivos que deseen participar en la WLAN deben tener el mismo SSID. Por cuestiones de seguridad, se debe modificar el SSID predeterminado. Para permitir que los clientes detecten la WLAN fácilmente, se transmite el SSID de manera predeterminada. Se puede deshabilitar la característica de transmisión del SSID. Si no se transmite el SSID, los clientes inalámbricos necesitarán configurar este valor manualmente.

El canal de RF utilizado para el router integrado se debe elegir teniendo en cuenta las demás redes inalámbricas que se encuentren alrededor.

Las redes inalámbricas adyacentes deben utilizar canales que no se superpongan, a fin de optimizar el rendimiento. La mayoría de los puntos de acceso ahora ofrecen una opción para permitir que el router localice automáticamente el canal menos congestionado.

Por último, seleccione el mecanismo de encriptación que prefiera e introduzca una clave o una frase de contraseña.

COMPETENCIA - IMPLEMENTA SISTEMA OPERATIVO DE RED
CONTENIDOS:

A. Revisando los requerimientos del usuario

ESTRATEGIA	PRODUCTO
4. Retoma el producto realizado: "Tabla de equipos y dispositivos de interconexión" del primer parcial, identifica los equipos de cómputo que señaló como servidores y crea una tabla con: imagen del equipo servidor, marca, los requerimientos de instalación, características o especificaciones a detalle y completos.	**4- Tabla de Servidor(es)**

B. Verificando la compatibilidad del software y hardware del equipo

ESTRATEGIAS	PRODUCTOS
5. Verifica la compatibilidad (Anexo 12), elabora un cuestionario con su respuesta, siguiendo el orden de los elementos izquierda a derecha de la actividad a resolver (sigue después de las definiciones de redes informáticas) y luego responde la actividad propuesta.	**5- A. Cuestionario** **B. Actividad resuelta**

A N E X O - 12
PRUEBAS DE CONECTIVIDAD

Definición de redes informáticas
Cuando hablamos de **redes informáticas**, redes de ordenadores (o de computadoras) o redes de comunicación de datos, nos referimos a un grupo de sistemas informáticos, es decir, de ordenadores u otros dispositivos de hardware conectados entre sí mediante nexos que pueden ser acoplados físicamente con cables o a través de sistemas inalámbricos.

Esta conexión entre los diferentes sistemas informáticos se establece con el objetivo principal de compartir datos (archivos de todo tipo) y recursos (impresoras, unidades de disco, etc.), es decir, información.

Es evidente, que cuando se prepara una **red informática**, son importantes factores como **la conectividad, la velocidad de red y la seguridad informática.**

Elementos que forman parte de las redes informáticas
En cuanto a la estructura de los componentes que forman parte de las redes informáticas, podemos diferenciar entre varios elementos:

Topología
La topología de red se define como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico.

Hardware
Cuando nos referimos a los elementos de hardware que forman parte de una red informática, hablamos de aquellas piezas físicas que hacen posible la comunicación, como por ejemplo las tarjetas de red, los enrutadores o los módems que sustentan la transmisión de los datos o, en caso de que la conexión sea inalámbrica, las antenas repetidoras que expanden la conexión serían otro ejemplo de hardware.

Tarjeta de interfaz de red
Para comunicarse con el resto de la red, cada computadora debe tener instalada una tarjeta de interfaz de red (Network Interface Card, NIC), llamados también adaptadores de red o sólo tarjetas de red. Son ocho las funciones de la NIC: Comunicaciones de host a tarjeta Buffering Formación de paquetes Conversión serial a paralelo Codificación y decodificación Acceso al cable Saludo Transmisión y recepción
Módem ADSL USB:
Este sistema ha sido el más utilizado hasta la aparición de la ADSL2+ cuando se trataba de conectar a Internet un sólo ordenador.

Antivirus
Se denomina **antivirus** a un **software** utilizado para eliminar programas elaborados con intención destructiva.

Software
Para que las labores de los elementos del hardware funcionen son imprescindibles los elementos de software, que podemos dividir en dos partes:

- El **sistema operativo de red o NOS** (en inglés Network Operating System), que se encarga de posibilitar la interconexión entre ordenadores mediante protocolos que se aplican enviando y

recibiendo conjuntos de datos formateados que se conocen como “paquetes”. Entre otras labores, los sistemas operativos de red son los responsables de proporcionar seguridad al proceso, controlando el acceso de datos y recursos.
- El **software de aplicaciones**, es decir, aquellos programas que se comunican con los usuarios de la Red y posibilitan que se comparta información como datos y recursos.

Cable
La LAN debe tener un sistema de cableado que conecte las estaciones de trabajo individuales con los servidores de archivos y otros periféricos.

Adaptador PCMCIA WiFi:
Los adaptadores PCMCIA (Personal Computer Memory Card International Association) están diseñados específicamente para ordenadores portátiles. Son más fiables y estables que los adaptadores USB, pero dado que actualmente casi todos los portátiles incluyen una tarjeta WiFi cada vez se ven menos.

Router WIFI:
Este dispositivo permite una amplia configuración de la red. En su versión WiFi permite conectarse a él tanto vía Ethernet (suelen tener entre uno y cuatro puertos RJ-45) como vía WiFi.

Servidor
Los servidores (imagen superior) son elementos importantes dentro de las redes informáticas, ya que se encargan de procesar todo el flujo de datos que existe, atendiendo a todos los computadores de la red y centralizando el control de la misma. Algunos servidores comunes son: de archivos, de impresión, de correo, de proxy, de web, de base de datos, de aplicaciones, etc.

Clientes o estaciones de trabajo
Es así como se denominan aquellos ordenadores que no son servidores, sino que simplemente son parte de la red y utilizan los recursos que administra el servidor.

Concentrador:
En comunicaciones, centro de distribución, concentrador. Un Hub es un equipo de redes que permite conectar entre si otros equipos o dispositivos retransmitiendo los paquetes de datos desde cualquiera de ellos hacia todos. Han dejado de utilizarse por la gran cantidad de colisiones y tráfico de red que producen.

Internet
Se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios. Podemos considerar las computadoras simplemente como el medio que transporta la información.
Medios de transmisión
Para que se pueda transmitir la información se requieren medios de transmisión, es decir, cableado u ondas electromagnéticas, según si el sistema es alámbrico o inalámbrico.

Windows 7
Es una de las versiones más recientes de Microsoft Windows, un Sistema Operativo producido por Microsoft para uso en PC, incluyendo equipos de escritorio en hogares y oficinas, equipos portátiles, "tablet PC", "netbooks" y equipos "media center".

ACTIVIDAD A RESOLVER

INDICACIONES:

A continuación se presentan algunos elementos, identifica con una X en la columna de la izquierda los que consideres parte de la red, en la derecha con la letra S si pertenecen a Software y una H si consideras que es Hardware.

Elemento de red		Tipo		Elemento de red		Tipo
	Estación de trabajo				Servidor	
	Cables				Topología	
	Windows 7				Modem	
	Internet				Router	
	Tarjeta de red				Concentrador	
	Office				Antivirus	

C. Instalando el software en el equipo

ESTRATEGIAS	PRODUCTOS
6. Lee ¿Qué es Windows Server? (Anexo 13) para comprender la diferencia entre un SO de red como Windows Server y un SO monousuario para una PC de escritorio, elabora la síntesis.	**6- Síntesis**
7. Lee como hacer una máquina virtual con VMware (Anexo 14) y realiza una infografía con el procedimiento adecuado.	**7- Infografía**
8. Lee la información "instalar Windows Server 2019 en VMware" (Anexo 15) y elabora la guía de instalación de Windows Server 2019, siguiendo el formato agregado (Anexo 16).	**8- Guía de la práctica**

A N E X O - 13
¿QUÉ ES WINDOWS SERVER?

00:21 curso de windows server 2016 y bueno
00:24 vamos con la introducción a windows
00:26 server 2016 carpool sino el curso sería
00:28 de windows 20 y 40 lo primero que vamos
00:32 a ver lo que quiero trabajar en este
00:34 vídeo un poquito después del fondo de
00:36 pantalla lo habéis visto sabéis que el
00:37 agua polar si alguien quiere que solo
00:39 pasé porque lo comenté bueno va para
00:40 allá diferencias con windows texto bien
00:43 hay gente que a veces me pregunta y no
00:45 me podré poner un windows server para
00:47 ponerme aquí que no no puedes porque
00:50 no está pensado para un equipo de
00:52 escritorio un equipo de escritorio pues
00:54 está pensado pues para que sean
00:55 compatibles con tarjetas gráficas de
00:57 sonido con 40.000 placas base con
80.000
01:00 tipos de controladores raros de equipos
01:02 de stop que los windows server tiene los
01:04 suyos, pero son de windows server
01:05 entonces no no podemos utilizar un
01:08 windows server para un equipo de
01:11 escritorio para un equipo de lo que
01:13 sería el día a día para trabajar pues
01:14 como yo para grabar los videos y tal no
01:16 se puede pablo como lo sabe porque ya l
01:19 lo propio ya lo prueba
01:20 efectivamente aun sabiéndolo lo he
01:22 probado y no tiene muchos problemas de
01:24 compatibilidad es luego otras
01:26 diferencias que tienes que, por ejemplo
01:27 un windows 10 pues tienes una serie de
01:29 características que podemos activar y
01:31 desactivar verdad por ejemplo el hyper
01:33 vino movidas de esta solo de internet
01:35 information services hay algunas que se
01:38 comparten con windows server pero las
01:41 características digamos de windows
01:42 desktop están orientadas al propio
01:44 sistema es decir a que el sistema pues
01:46 pueda hacer más cosas en windows
server
01:48 Tenemos los roles que esto ya lo
veremos
01:50 más adelante que dotan de mayor
01:52 funcionalidad al servidor y con ello el
01:54 servidor dota de servicios a la red pues
01:57 por ejemplo uno muy destacado active
01:59 directory o hyper bio windows server
02:02 update services es servidores web
02:04 etcétera de acuerdo que sí que hay
02:06 algunos que se comparten con windows
02:08 10 por ejemplo con windows desktop pero
02:10 su mayoría los roles de windows server

02:12 están orientados a pro a proveer de
02:15 funcionalidades a la red
02:18 de acuerdo con estas funcionalidades
02:20 bueno pues podemos compartir archivos
02:21 contra el acceso a recursos y muchas
02:23 otras cosas que a lo largo del curso
02:25 pues descubriremos luego también tenemos
02:28 las características ok y bueno las
02:31 características pues tenemos cosas
02:32 bastante corrientes digamos para que
02:35 digamos que el servidor pueda hacer otro
02:37 tipo de cosas por ejemplo el cliente
02:39 tener el directo el yo que es el
02:41 servicios de servidor y sms eso es para
02:46 que el servidor pueda hacer o se pueda
02:48 conectar a ciertos tipos de recursos
02:49 tenemos pues también por ejemplo yo
02:51 es el media fundation no tenemos bueno
02:53 hay características ok esto pues es
02:56 interesante que nosotros lo
02:59 investigues o de vez en cuando la di
03:01 su invitación a dar pues voy a mirar
03:03 además si picamos por ejemplo en directo
03:05 dice componentes de direct play bueno
03:07 pues aquí tendríamos que ir al google y
03:09 poner que direct play que no tengo ni
03:10 idea pues tendríamos que ver, por ejemplo
03:12 extensiones y ese de win RM y aquí dice
03:16 la extensión y ese de administración
03:18 remota de WIN RM permite que un
03:20 servidor reciba una solicitud de
03:22 administración de un cliente y bla bla
03:24 esto es importante que lo recordemos
03:26 porque aquí nos va a ir dando un poquito
03:27 una pista una descripción de qué es lo
03:30 que estamos tocando pues hyper-v hyper
03:32 me proporciona los servicios que puede
03:34 usar para crear y administrar máquinas
03:35 virtuales y sus recursos blah
03:37 blah de acuerdo esto en cuanto
03:39 a roles y características bien debemos
03:42 de estar ya un poquito diferenciando
03:44 también es cierto que en windows 10 por
03:46 ejemplo tenemos las versiones pro
03:48 tenemos acá y permite en windows server
03:50 2016 también y alguien puede pensar a
03:53 entonces es lo mismo no, no, no es lo
03:56 mismo no es lo mismo vale como la
03:58 canción del tío ese que canta no es lo
04:00 mismo es bastante diferente en windows
04:04 server tenemos muchas más capacidades
04:06 por ejemplo en el rol de hyper y muchas
04:09 más de las que tiene windows 10 que
04:12 capacidades pues capacidades orientadas
04:14 al trabajo en red migración de máquinas
04:17 en vivo movimiento de máquinas en
04:19 caliente etcétera
04:20 ok almacenamientos etcétera hay muchos
04:23 detallitos hay que hay que tener hay que
04:24 tener en cuenta luego bien más
04:26 diferencia es con windows texto ahí os
04:28 pongo el fondo de pantalla
04:29 para que piglia y la url
04:30 capacidades de hardware un servidor un
04:34 windows server perdón puede administrar
04:36 mucho más hardware que un windows
04:39 desktop es decir puede gestionar
04:42 cantidades de RAM gran mayores, mayor
04:45 número de procesadores más
04:48 potentes más o menos ellos y los xeon
04:51 son compatibles con los windows de esto

04:53 habría que estudiarlo, pero ahora sí que
04:55 sí que gestiona mayor capacidad de
04:57 hardware ok sobre todo en cuanto al tema
04:59 de la memoria RAM ahí si se desmarcan
05:01 muchísimo de lo que son los sistemas de
05:04 esto aparte de que es más compatible o
05:07 está más preparado para trabajar
05:08 con hardware especial como cabinas de
05:11 discos etcétera cosas que windows 10 no
05:13 está bueno pues preparado para ello
05:15 porque es un equipo de trabajo para el
05:17 usuario final es decir para que el
05:19 usuario trabaje directamente pues con su
05:21 photoshop o con sus programas de edición
05:23 o con sus programas de contabilidad ok y
05:25 lo que tiene que hacer windows 10 es dar
05:27 windows desktop es dar soporte a esas
05:29 aplicaciones windows server no está
05:31 pensado para eso, aunque, aunque a veces
05:34 se pueda utilizar bueno pues mediante
05:35 algún rol de los que trae bien más
05:39 detallitos las ediciones vale en windows
05:42 10 tenemos pues la HOME,
05:44 la PRO y la ENTERPRISE bien la HOME
05:47 sería la edición de windows texto para
05:50 casa y la prueba INTERPRISE digamos
05:52 sería para entornos empresariales para
05:55 empresas para organizaciones y demás
05:57 vale no, no hay que tener un intérprete
05:59 en casa que luego hay gente pues que le
06:01 mola porque no se va a decir que tengo
06:03 un ENTERPRISE y luego al final las
06:05 capacidades que te está dando no las
06:06 estás utilizando porque no, no son o no
06:10 están orientadas al usuario doméstico
06:12 bueno pues con windows server 2016
06:14 tenemos un poquito de lo mismo tenemos
06:16 por ejemplo la edición ESSENTIALS la
06:18 ESTÁNDAR y la DATA CENTER
06:20 cada una de estas ediciones le va
06:23 proporcionar al sistema una serie de
06:25 capacidades de acuerdo también va a
06:27 afectar al tema del licenciamiento de
06:29 más, pero esto lo veremos esto lo veremos
06:30 otro día así que tenga un rato no en la
06:32 lección 2 vamos con el licenciamiento y
06:35 luego más adelante pues ya iremos
06:36 viendo un poquito el tema
06:40 de los roles de las características y
06:42 todas estas cosas así que tranquilo que
06:44 lo iremos viendo y luego bueno pues por
06:46 último un poquito me gustaría destacar
06:48 la evolución que ha tenido windows
06:50 server desde hace un rato
06:53 no sé qué windows server te enganchaste
06:56 tú qué estás viendo el vídeo exactamente
06:58 no sé si en la 2012 que hay mucha gente
06:59 que sí y ya quería pues el curso de 2016
07:02 para ir avanzando en esto o en la 2008 o
07:05 en la 2003 o lo mismo eres un veterano
07:08 de este súper veterano y empezaste con
07:11 este server que no lo sé podría ser
07:13 pero bueno si has empezado o empezaste
07:16 con 2003 por ejemplo sí que ha habido u
07:19 un cambio de Microsoft que ya a mí me
07:21 gustaría destacar y que bueno creo que
07:23 ha sido un poquito también pues para
07:24 para entrar en la competencia con Linux
07:28 que siempre se le ha criticado es que
07:29 tus servidores son muy pesados tus

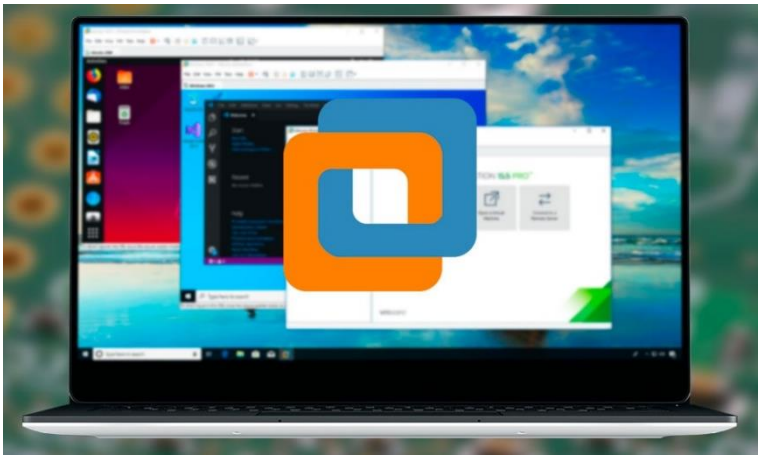
07:32 sistemas son muy pesados consumen
07:34 rmuchos recursos
07:35 tengo un vídeo por ahí que explico esto
07:36 y que lo demuestro que esto no es tan
07:38 así pero bueno esto Microsoft en 2008
07:43 en la versión 2008 pues ya empezó a
07:46 trabajar con windows server, Core server
07:48 Core que era una versión sin entorno
07:50 gráfico en 2012 esto se mejoró salió el
07:53 entorno mixer que es un mix entre el
07:56 entorno gráfico de ventanucas y el y
08:00 solo la consola y ahora en 2016 además
08:02 de esto tenemos también la posibilidad
08:05 de trabajar con los cinco nano servers
08:09 esto lo veremos más adelante en el curso
08:11 si no me equivoco, pero lo tengo en el
08:14 guion, pero bueno esto iremos
08:15 profundizando más adelante de todas
08:17 formas y yo os recomiendo a todos los
08:19 que estáis viendo el videito este que
08:22 seáis curiosos el tío paula ha
08:24 dicho aquí que el windows core server
08:26 no sé cuánto nano micro esto que es me
08:28 voy a mirar me lo apunto a mirar el tema
08:31 de los contenedores por ejemplo o el
08:32 tema de las ediciones web os ha dicho
08:34 que hay una esencia al sexto que es
08:36 usted mente si investigas un poquillo y
08:38 ya vas adelantando camino para cuando
08:40 bueno pues empecemos ya a trabajar
08:42 con el curso un poquito más más fuerte
08:44 siguiente vídeo será sobre licenciamiento
08:47 quiero recordar y comentar aprovecho
08:50 para volver a poner el fondo de pantalla
08:51 no aprovecho para abrir una página web
08:52 mientras que el curso no va a estar
08:55 completo no va a estar completo en
08:57 youtube de acuerdo el curso estará
09:00 completo 100% en soporte TIpro

Fuente: https://youtu.be/pNjDkEmUbx4

A N E X O - 14
MAQUINA VIRTUAL CON VMWARE

INSTALA CUALQUIER SISTEMA OPERATIVO EN TU PC SIN RIESGO CON VMWARE

Seguro que alguna vez nos ha llamado la atención algún sistema operativo. Por ejemplo, alguna distro Linux. Y no nos hemos atrevido a probarla por miedo a que un fallo rompiera nuestro sistema operativo principal. Esto es algo normal, especialmente entre usuarios con poca experiencia dentro de la informática. Sin embargo, este miedo no tiene por qué impedirnos probar otros sistemas operativos. Y es que, gracias a las máquinas virtuales que nos **VMware,** podemos hacerlo fácilmente y con total seguridad.



VMware es uno de los programas más completos que podemos encontrar para **crear máquinas virtuales** (ordenadores dentro de nuestro ordenador) en los que montar y probar todo tipo de sistemas operativos.

Ventajas de una máquina virtual
Las **máquinas virtuales** nos brindan muchas ventajas a la hora de probar y experimentar con sistemas operativos y con el software en general. Una de las ventajas más importantes es que podemos instalar y borrar sistemas operativos con total seguridad, sin poner en peligro nuestro sistema principal, también conocido como host.

Además, todo lo que hagamos dentro de este sistema operativo virtual (guest) no afecta para nada al sistema host. Si, por ejemplo, descargamos un malware y lo ejecutamos en la máquina virtual, este solo afectará al sistema virtual, pero nuestro sistema host estará a salvo.

Siempre que tengamos memoria RAM suficiente podemos ejecutar al mismo tiempo todos los sistemas operativos que queramos. E incluso trabajar con ellos al mismo tiempo. Cuando apagamos la máquina virtual, se liberan todos los recursos y listo.

Por desgracia, no todo son ventajas. Y es que estas máquinas virtuales tienen un inconveniente importante, y es que siempre quedan muy por debajo en rendimiento al que nos ofrecen los sistemas operativos instalados físicamente en el PC.

VMware, el software de virtualización más completo
A diferencia de otros programas, **VMware** es un software profesional pensado especialmente para uso comercial y para grandes empresas. Por ello, este software tiene características y funcionalidades que, por defecto, no encontraremos en otros programas de virtualización como su rival, VirtualBox.

Entre todas las **funciones y características de VMware Workstation** debemos destacar:

- Gran rendimiento 3D. Es compatible con DirectX 10.1 y OpenGL 3.3, lo que mejora enormemente el rendimiento al ejecutar aplicaciones 3D, como juegos, AutoCAD o Solidworks.
- Soporta máquinas virtuales inmensas, con 16 núcleos virtuales, 8 TB de almacenamiento, 64 GB de RAM y 3 GB de memoria gráfica.
- Soporta resoluciones de hasta 4K UHD (3840×2160).
- Permite crear redes virtuales complejas.
- Varias posibilidades para clonar máquinas virtuales. Podemos usar los «Linked Clones» para duplicar una máquina rápidamente y ahorrar espacio, o crear clones completos.
- Las instantáneas, o **snapshots**, nos permiten restaurar la máquina virtual a un estado anterior en segundos.
- La REST API nos brinda más de 20 controlar para gestionar la máquina virtual.
- Integración con vSphere.
- Funciones para compartir configuraciones y máquinas con otros usuarios.
- Una máquina virtual creada en un PC funciona en cualquier otro. Da igual que se haya creado en Windows o en Linux.
- Compatible con máquinas virtuales creadas en otros programas.
- Medidas de seguridad avanzadas.

Y lo más importante. Todo lo que hagamos en estas máquinas virtuales, siempre y cuando no estén conectadas con el sistema operativo host, se hará en un entorno seguro. Si destruimos por algún motivo (un virus) la máquina virtual, esto no afectará para nada al sistema principal.

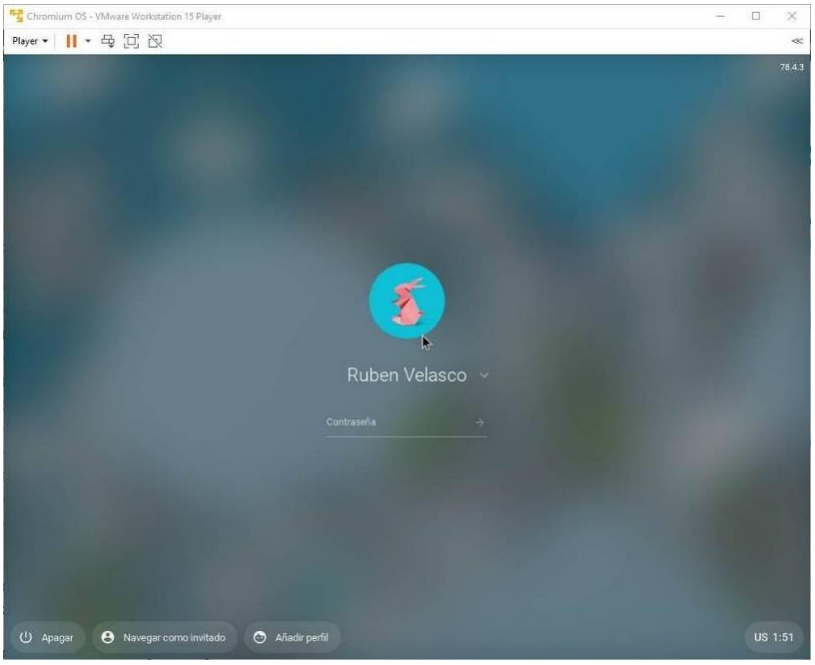
Diferentes versiones de VMware
Aunque VMware como empresa tiene una gran cantidad de programas y servicios relacionados con la virtualización, nosotros vamos a hablar principalmente de los dos productos más interesantes para virtualizar sistemas operativos: **Workstation y Player**.

VMware Workstation Pro
Esta es la versión más completa del software de virtualización de VMware. Este programa de virtualización nos permite crear todas las máquinas virtuales que queramos y ejecutar todos los sistemas operativos que queramos al mismo tiempo por encima de nuestro sistema operativo principal.
Esta es la edición más avanzada de este software de virtualización, teniendo todas las funciones habilitadas y permitiendo a los usuarios más avanzados conectar con otras plataformas, como vSphere, e incluso funcionar con sistemas de virtualización basados en contenedores, como Docker y Kubernetes.
El problema de **VMware Workstation Pro** es que es un programa muy caro. Por suerte, podemos tener la mayoría de sus funciones en una versión gratuita pensada para usuarios domésticos: VMware Workstation Player.

Pro vs Player
Dentro de VMware Workstation podemos encontrar dos modalidades diferentes. La versión Pro es la más cara, pero la que tiene todas las características habilitadas, mientras que la versión Player es mucho más sencilla, aunque carece de algunas funciones.

Las **limitaciones** de la versión Player frente a la Pro son:

- No tiene interfaz basada en pestañas.
- No tiene un modo SSH para Linux que nos permita conectarnos con un clic.
- Imposibilidad de crear o usar máquinas virtuales cifradas.
- No permite renombrar las redes virtuales.
- Carece de Snapshots (instantáneas o copias de seguridad de las VM).
- Solo permite ejecutar una máquina virtual al mismo tiempo.
- No tiene simulador de redes virtuales.
- No permite clonar máquinas.
- La función de compartir no está disponible.
- No se puede conectar a servidores vSphere/ESXi.
- No compatible con vSphere Host Power Control.



La ventana de **VMware Player** es que podemos usarla de forma gratuita para uso personal. Por lo que, si no nos importan las anteriores limitaciones, estamos ante un gran software gratis de virtualización.

VMware Fusion: la opción para macOS
VMware Workstation está disponible para Windows y Linux. Sin embargo, la compañía tiene una versión específica para virtualizar sistemas en los ordenadores de Apple: VMware Fusion.

Este software nos permite instalar cualquier sistema operativo encima de macOS, aunque está pensado sobre todo para ejecutar Windows 10 como si se hiciera de forma nativa. Tiene aceleración 3D completa,

igual que en la máquina host, y es compatible con todas las actualizaciones de Windows 10, y demás sistemas operativos, sin problemas.

Requisitos mínimos, compatibilidad y problemas
Para poder usar este software necesitamos un procesador de 2011, o posterior, que cuente con instrucciones de virtualización. Algunos modelos antiguos de AMD, o los Intel Atom de 2011 y 2012, por ejemplo, no cuentan con estas características. Pero para poder tener un buen rendimiento se recomienda tener un procesador de gama media-alta, de i5 en adelante, con una frecuencia mínima de 1.3 GHz.

Además, aunque en los requisitos mínimos se especifica que el mínimo son 2 GB de memoria RAM, se recomienda tener al menos **4 GB de RAM**. De lo contrario, podremos tener problemas de rendimiento.

VMware está disponible para Windows y Linux. Podemos usarlo en Windows 7, o cualquier versión posterior del sistema operativo de Microsoft. También funciona en varias distros Linux, como Ubuntu 15.04, Red Hat Enterprise Linux 6, CentOS 7.0, Oracle Linux 7.0, openSUSE Leap 42.2 y SUSE Linux 13. Obviamente, también lo hace en sus versiones posteriores.

La lista de sistemas operativos que funcionan en VMware es muy amplia. Podemos usar sus máquinas virtuales para instalar prácticamente cualquier sistema que queramos. Aunque los que mejor funcionan son:

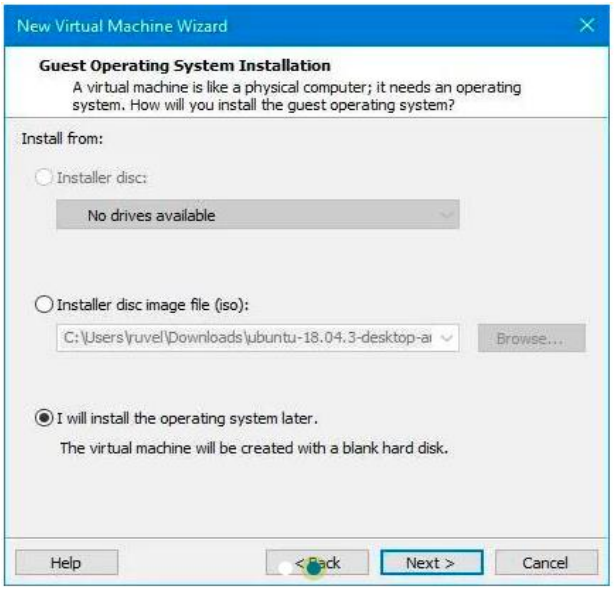
- Windows 10 / 8.x / 7 / XP
- Ubuntu
- Red Hat
- SUSE
- Oracle Linux
- Debian
- Fedora
- openSUSE
- Mint
- CentOS

También hay parches no oficiales para añadir soporte para macOS. E incluso podemos instalar cualquier sistema operativo genérico.

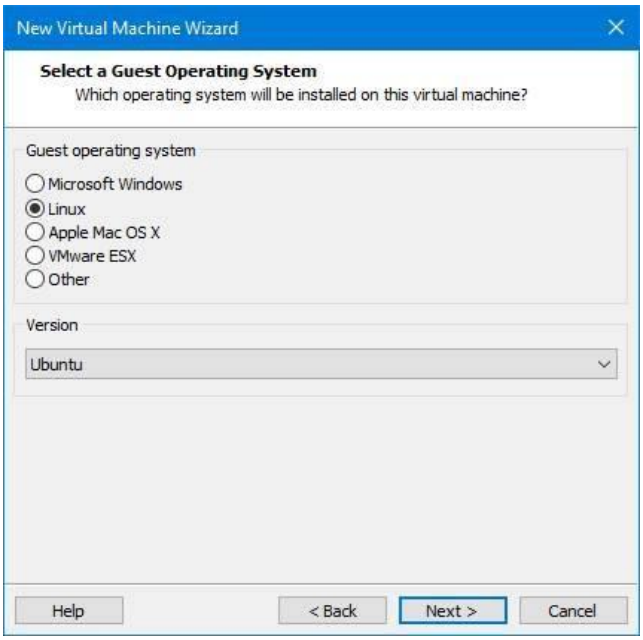
Entre los principales problemas de este software de virtualización debemos indicar que no se lleva bien con Hyper-V, el hipervisor de Microsoft para Windows. Esto significa que si activamos este hipervisor para poder usar el Subsistema Linux para Windows (WSL) o Docker, no podremos usar VMware. A día de hoy, son incompatibles.

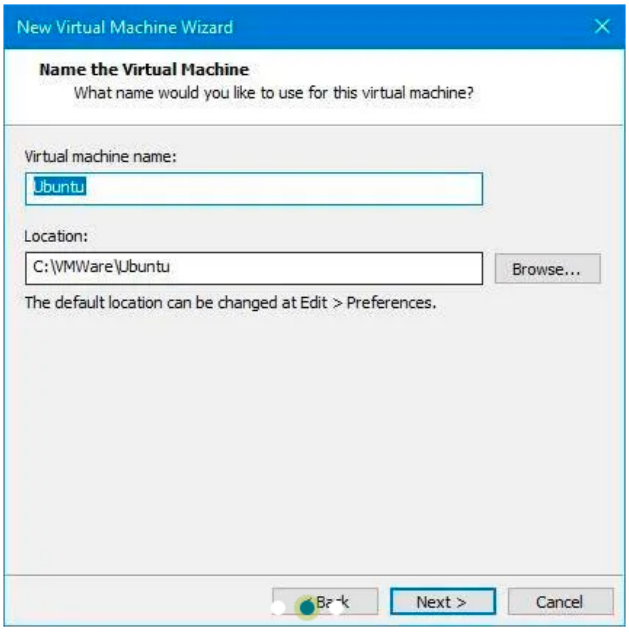
Crear una máquina virtual nueva con unos clics
En un principio, el término «máquina virtual» puede parecer complicado. Sin embargo, en verdad podemos crear una en segundos y con unos pocos clics. Basta con abrir el asistente de creación de máquina virtual de VMware y seguir los pasos que nos van apareciendo en la pantalla.

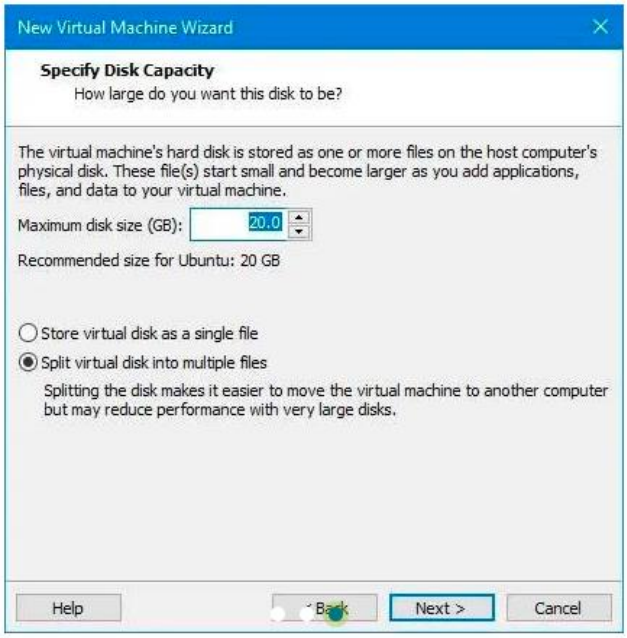
Tendremos que elegir el tipo de máquina virtual que queremos crear.
A continuación, elegir si queremos montar una ISO para instalar el sistema o vamos a instalarlo más tarde.



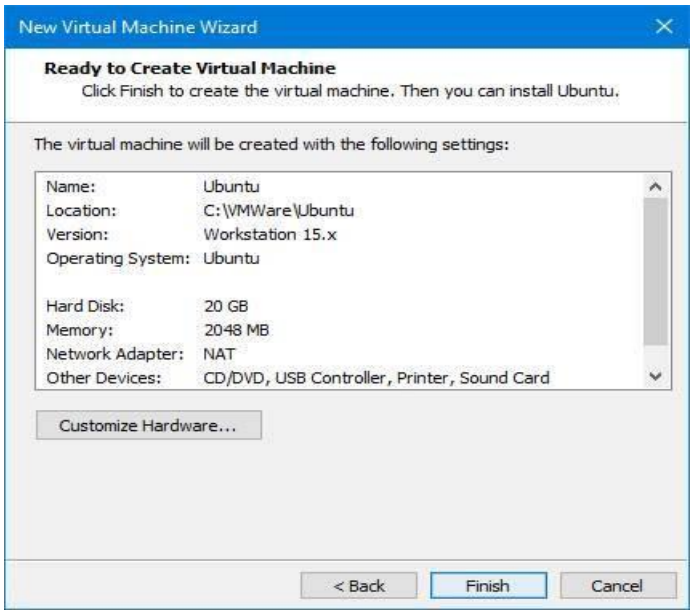
También tendremos que elegir el tipo de sistema operativo que queremos instalar, y el espacio que vamos a dar al disco duro virtual.



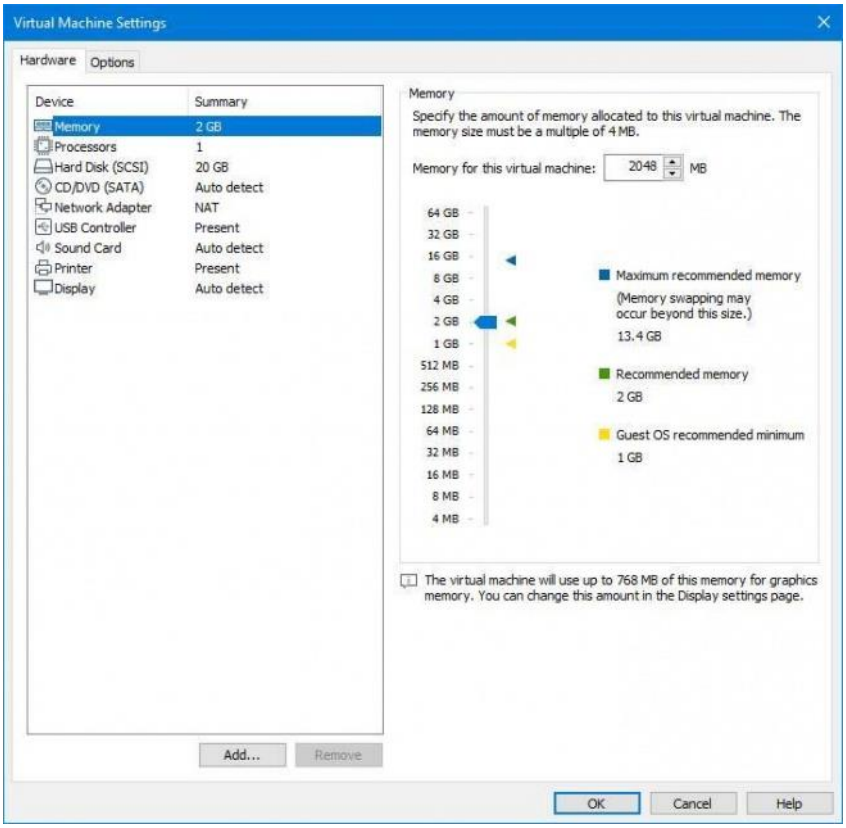


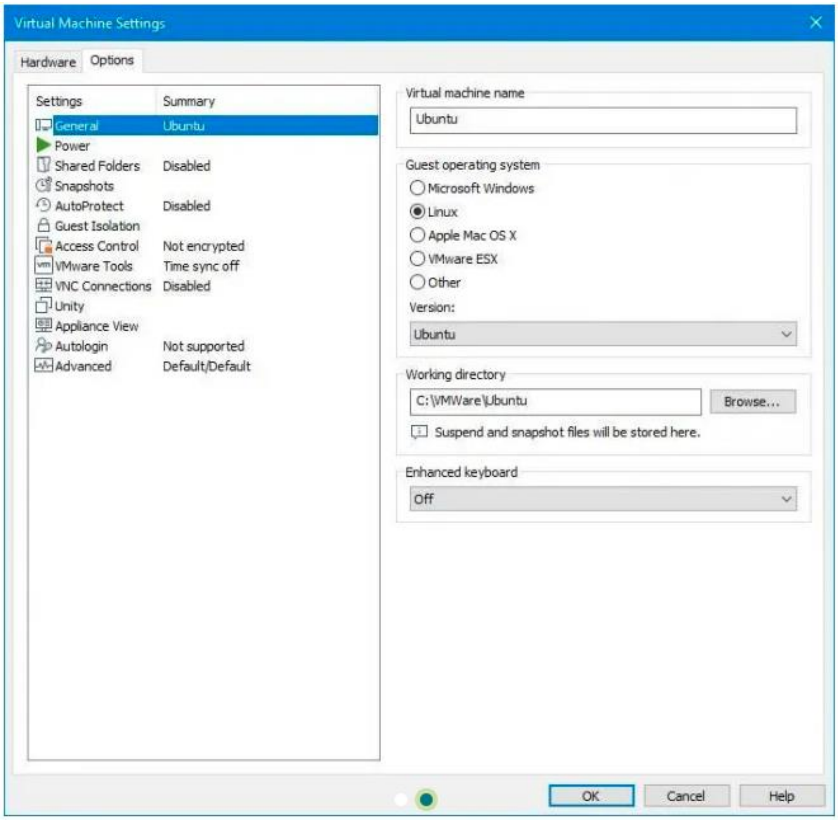


Por último, revisaremos las especificaciones de la máquina virtual y ya la tendremos lista.



Eso sí, podemos modificar las especificaciones en cualquier momento. Podemos aumentar la memoria RAM, los procesadores, el disco duro, montar nuevas unidades (virtuales) e incluso configurar otros aspectos relacionados con el funcionamiento de las máquinas virtuales de VMware.





Cuando tengamos la máquina virtual lista, tan solo debemos arrancarla y empezará a funcionar como un ordenador de verdad, con su BIOS, su gestor de arranque y todo.

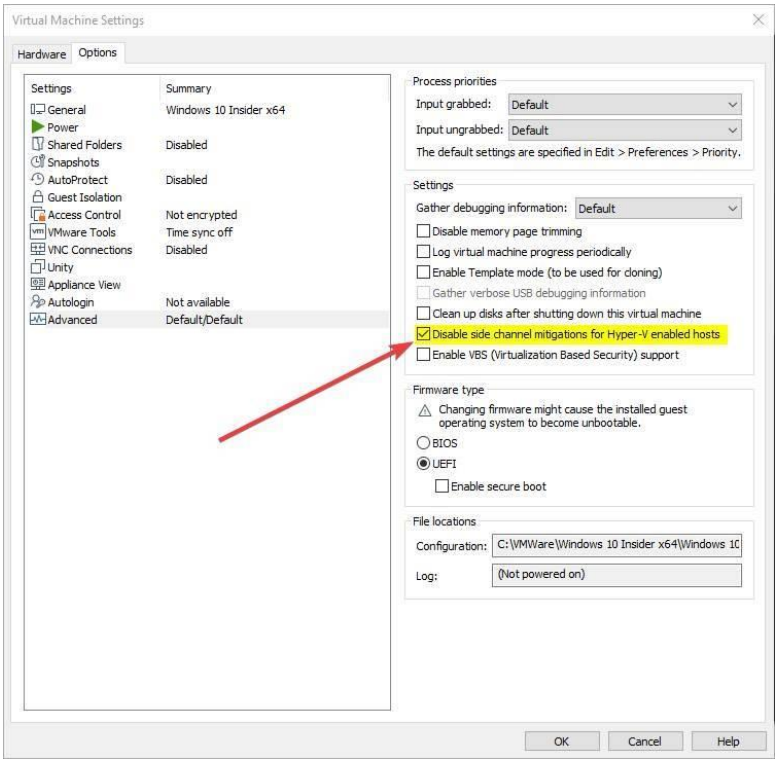
Desactivar mitigaciones para mejorar el rendimiento

A partir de VMware 16 es posible usar Hyper-V junto con este software de virtualización. Sin embargo, por seguridad, este programa aplica por defecto una mitigación contra las vulnerabilidades de Meltdown y Spectre para que usar la máquina virtual sea lo más seguro posible.

Sin embargo, esta medida de seguridad resta bastante rendimiento a las máquinas virtuales, y puede hacer que funcionen realmente mal.

Por lo tanto, si el PC es seguro, podemos desactivarlas para poder conseguir el mejor rendimiento posible al usar nuestras VM.

Para ello, lo que debemos hacer es abrir las propiedades de cualquiera de las máquinas virtuales, e ir a la pestaña «Options», concretamente al apartado «Advanced».



Aquí debemos activar la siguiente casilla para desactivar esta medida de seguridad en el sistema operativo virtualizado. De esta manera, podremos mejorar considerablemente el rendimiento de las VMs, especialmente en lo que a uso de CPU se refiere.

Solo tendremos que preocuparnos de esto si tenemos activado Hyper-V (por ejemplo, para usar WSL). Si no, sí solos usamos el hipervisor de VMware, no tendremos problemas.

Cómo descargar VMware

La última versión de **VMware Workstation** podemos descargarla desde el **siguiente enlace**. Esta edición es la más completa, como hemos explicado, pero también requiere el pago de la licencia del programa para poder utilizarla. Una licencia que, por cierto, no es nada barata (275 euros). Eso sí, si queremos, podemos optar por la versión de prueba gratuita de esta edición.

Por ello, si vamos a usar este programa para uso personal, es mejor optar por la edición **Workstation Player**, que podemos descargar desde **este mismo enlace**.

Además, también se instala como parte de Workstation Pro

Fuente: https://www.softzone.es/programas/sistema/vmware/

A N E X O - 15
INSTALAR WINDOWS SERVER CON VMWARE

Tutorial con un manual completo para poder instalar y configurar Windows Server 2019 en VMware con todos los pasos.

Actualmente podemos ver como los desarrolladores tanto de sistemas operativos como de aplicaciones lanzan nuevos productos, o actualizaciones de los actuales, buscando siempre optimizar el uso, compatibilidad, seguridad y desempeño de estos.

De este modo los recursos a nivel de hardware y software es cada vez más exigente y en vista de que no siempre contamos con los recursos suficientes para lograr administrar y usar estos nuevos productos.
Podemos echar mano de una de las tecnologías más novedosas y prácticas para probar cualquier sistema operativo o aplicación sin que sea necesario invertir grandes cantidades de dinero en equipos poderosos y esta tecnología es la virtualización.

Ventajas de la virtualización
Gracias a la virtualización estamos en la capacidad de implementar la gran mayoría de sistemas operativos conocidos lo cual nos da ventajas como:

- Conocer de antemano el comportamiento de una nueva implementación antes de que este pase a estar en un ambiente productivo.
- Conocer su entorno y desempeño global.
- Validar la compatibilidad con aplicaciones y programas.
- Posibilidad de crear estructuras de red para definir y evaluar ciertos comportamientos y mucho más.

Una de las ventajas más destacadas de la virtualización es que no se requiere de equipos con grandes recursos de hardware, aunque Solvetic recomienda disponer de buena memoria RAM, discos duros y CPU para que el desempeño de la máquina virtual sea el adecuado.

Conectar red local máquina virtual VMware, VirtualBox o Hyper-V

Cómo crear una red local con varias máquinas virtuales en VMware, VirtualBox o Hyper-V.

Una de las plataformas más usadas a nivel de virtualización es VMware la cual está disponible en la versión Player y Pro siendo este último uno de los más versátiles por sus niveles de funciones integradas ya que VMware Workstation 15 Pro está en la capacidad de mejorar el hipervisor de escritorio a través de una interfaz de usuario con valores altos de PPP, una nueva API de tipo REST, y ofrece una compatibilidad con los sistemas operativos Windows y Linux más recientes.

Sistemas soportados por VMware
VMware puede soportar los siguientes sistemas operativos invitados:

Windows 10

- Windows 8.X
- Windows 7
- Windows XP
- Ubuntu
- Red Hat
- .
- SUSE
- Oracle Linux
- Debian
- Fedora
- OpenSUSE
- Mint
- CentOS y muchos más

Ahora, VMware en su versión más actual, 15, puede ser instalado en los siguientes sistemas operativos:

- Ubuntu 14.04 o superior
- Red Hat Enterprise Linux 6 0 superior
- CentOS 6.0 0 superior
- Oracle Linux 6.0 o superior
- openSUSE Leap 42.2 o superior
- SUSE Linux 12 o superior
- Windows 10 Características generales de VMware

A nivel de características generales de uso de VMware encontramos:

- Posibilidad de crear máquinas virtuales de gran tamaño con detalles técnicos como 16 CPU, 64 GB de RAM, 3 GB de VRAM y más.
- Creación de nuevas máquinas virtuales en pocos pasos.
- Compatible con más de 200 sistemas operativos invitados.
- Implementación masiva de máquinas virtuales.
- Ejecución de máquinas virtuales usando diferentes modos de vista según sea necesario
- Uso de gráficos 3D compatibles con DX10 y OpenGL 3.3
- Capacidad de compartir archivos entre hosts e invitados
- Compatibilidad con pantallas 4K
- Compatible con lectores de tarjetas USB inteligentes y dispositivos USB 3.0
- Control de API de tipo REST
- Ejecución de máquinas virtuales cifradas
- Compatibilidad con inicio de UEFI

Descargar VMware

VMware nos ofrece la posibilidad de descargar VMware Workstation Player 15 de forma **gratuita en el siguiente enlace**. Allí será posible descargar VMware para Windows o Linux.

VMWARE WORKSTATION PLAYER 15

Al usar VMware Workstation Player 15 estaremos en la capacidad de aislar los escritorios corporativos, esto en caso de implementarlo como administradores de sistemas. Desde los dispositivos BYO para desactivar las funciones de copiar y pegar, acceso a los dispositivos USB y arrastrar y soltar, carpetas compartidas, también será posible ejecutar máquinas virtuales restringidas las cuales serán cifradas y protegidas con contraseña, esto permite que solo los usuarios con los debidos permisos podrán acceder a los datos corporativos.

Uno de los sistemas operativos compatibles con VMware es el nuevo Windows Server 2019 el cual tiene como versión la 1809 y ha sido desarrollado por Microsoft con nuevas y mejoradas funciones de desempeño, seguridad y escalabilidad.

Qué es y cómo descargar Windows Server 2019
Windows Server 2019 es una versión del Canal de servicio a largo plazo (LTSC) la cual incluye la experiencia de escritorio con el fin de administrar de forma más centralizada todos los objetos que gestionemos en la organización.

Windows Server 2019 puede ser descargado de forma gratuita en el **siguiente enlace**:

WINDOWS SERVER 2019

Cómo configurar e instalar Windows Server 2019

Te explicamos todos los pasos que debes seguir para saber cómo configurar e instalar Windows Server 2019

Características Windows Server 2019

Dentro de las nuevas y mejoradas funciones, roles y características de Windows Server 2019 encontramos:

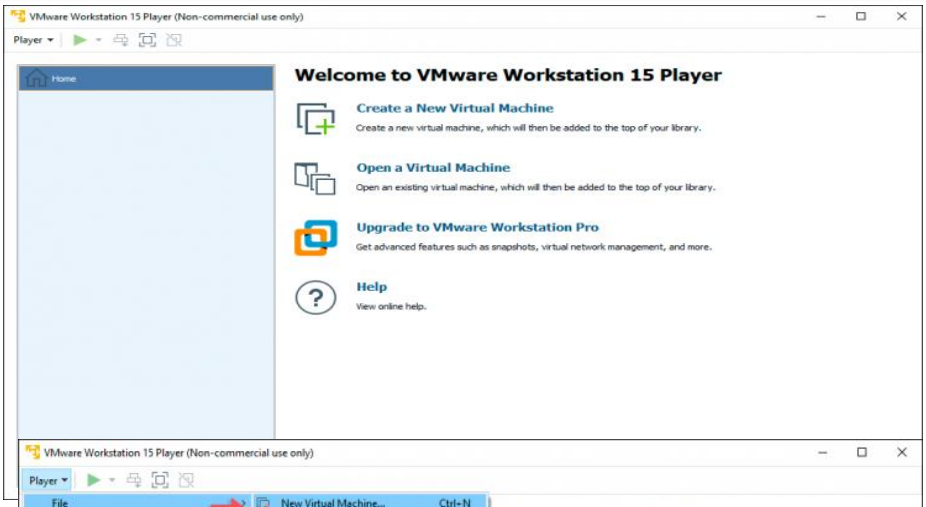
- Mejoras en la experiencia de escritorio.
- Integración de System Insights la cual es una de las nuevas características en Windows Server 2019 y su función es proveer capacidades de análisis predictivo local de forma nativa al sistema operativo Windows Server.
- Compatibilidad de la aplicación Server Core bajo demanda, también conocida como unción a pedido (FOD) de Server Core App Compatibility, la cual mejora la compatibilidad de la aplicación al disponer de la opción de instalación de Windows Server Core a su vez integrando un subconjunto de binarios y componentes de Windows Server en la experiencia de escritorio.
- Nueva función de Protección avanzada contra amenazas de Windows Defender (ATP) (Windows Defender Advanced Threat Protection) la cual busca evitar los ataques a nivel de kernel y memoria a través de la eliminación o no ejecución de archivos maliciosos, así como la terminación de procesos maliciosos detectados.
- Seguridad a través de redes definidas por software (SDN) la cual mejora la ejecución de cargas de trabajo en todo tipo de entornos de uso.
- Integración de HTTP/2 para una navegación web más rápida y segura.
- Mejoras a nivel de máquinas virtuales blindadas la cuales a su vez se reflejan en mejoras en la solución de problemas, mejor soporte de Linux y más.
- Mejoras en el servicio de migración de almacenamiento.
- Soporte de Windows Admin Center.
- Historial de rendimiento.
- Reduplicación y compresión para volúmenes ReFS.
- Migración de clústeres entre dominios.
- Mejoras en la infraestructura del clúster.
- El clúster de conmutación por error ya no hace uso de la autenticación NTLM.
- Soporte de Kubernetes y mucho más.

Ahora aprenderemos a instalar Windows Server 2019 en VMware Player 15.

1. Crear y configurar máquina virtual de Windows Server 2019

Paso 1

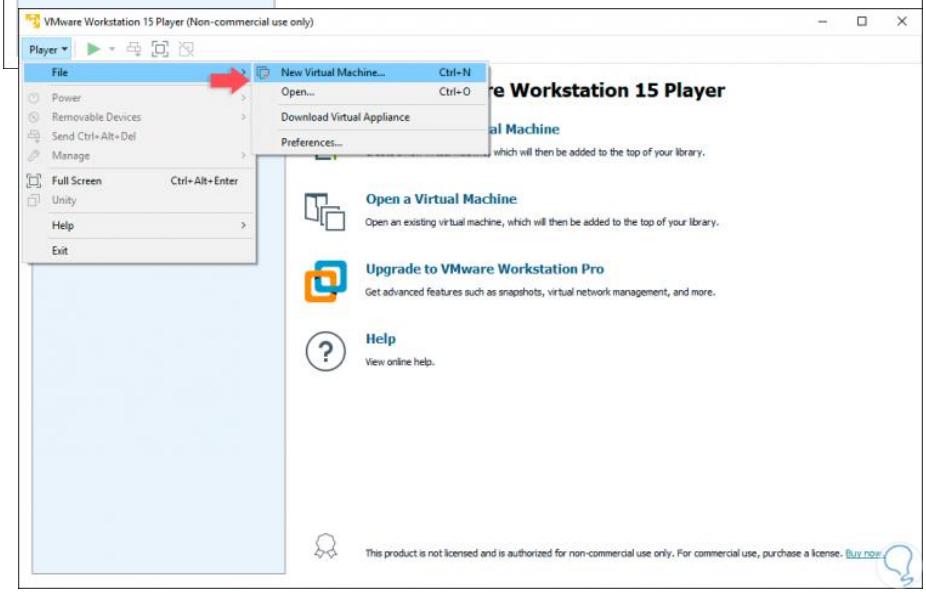
Una vez hayamos descargado e instalado VMware 15, procedemos a su ejecución y será desplegada la siguiente ventana:



Paso 2

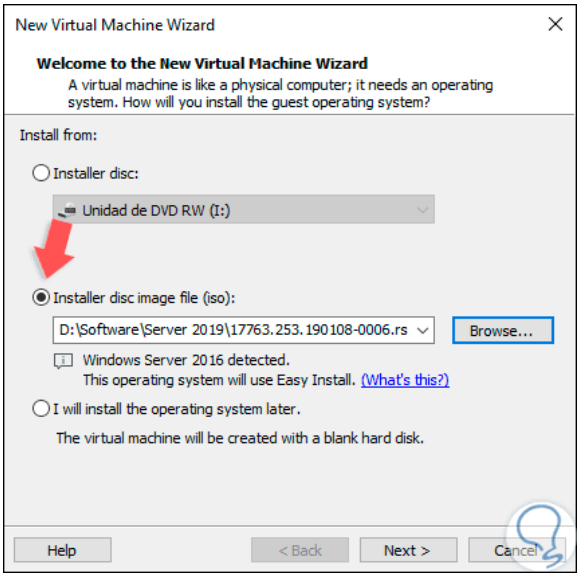
Para crear nuestra máquina virtual de Windows Server 2019 disponemos de las siguientes opciones:

- Dar clic en la línea “Create a New Virtual Machine” en el panel central.
- Pulsar sobre el menú “Player / File / New Virtual Machine”.
- Usar la combinación de teclas Ctrl + N.

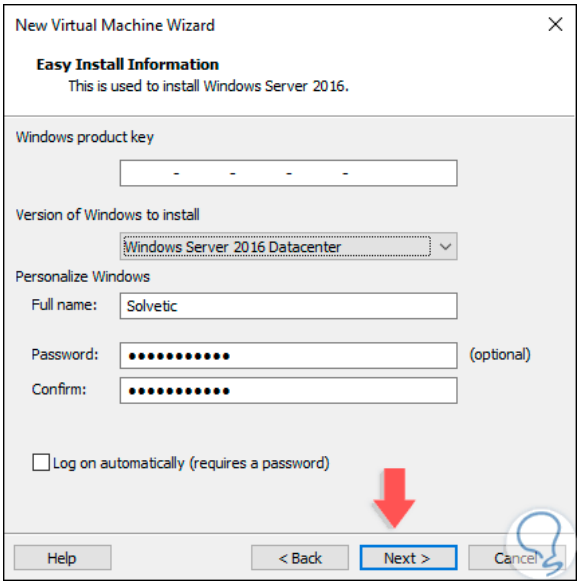


Paso 3

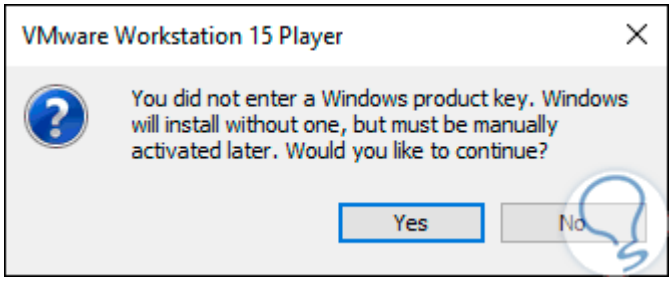
Será desplegada la siguiente ventana donde activaremos la casilla “Installer disc image file (iso)” y procedemos a ir a la ruta donde hemos descargado la imagen ISO de Windows Server 2019:



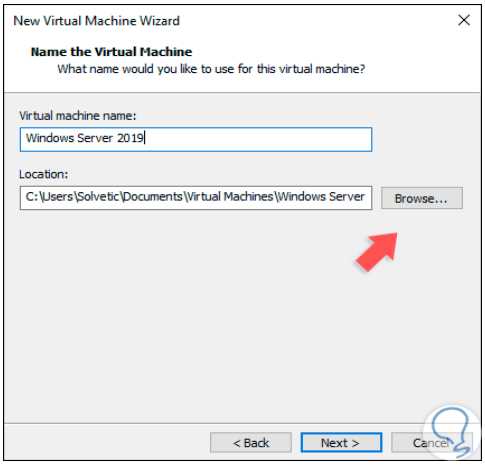
Paso 4
A tener en cuenta, aunque es 2019, VMware Workstation Player lo reconoce como 2016. Damos clic en Next y en la siguiente ventana será posible ingresar la clave del sistema (si la tenemos) así como usuario y contraseña de este:



Paso 5
En el caso de no ingresar ninguna contraseña se desplegará el siguiente mensaje:

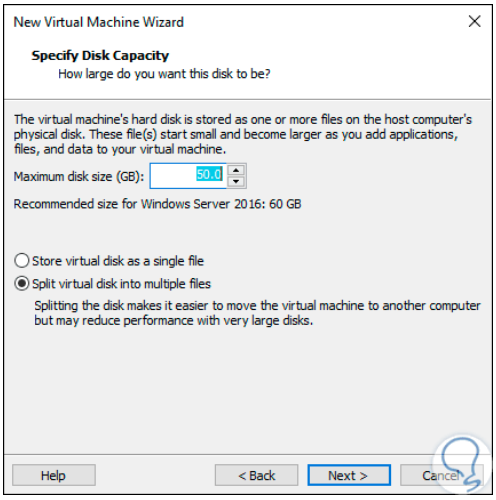


Paso 6
Damos clic en Yes y en la siguiente ventana asignaremos el nombre a la máquina virtual, así como su ubicación en el disco duro:



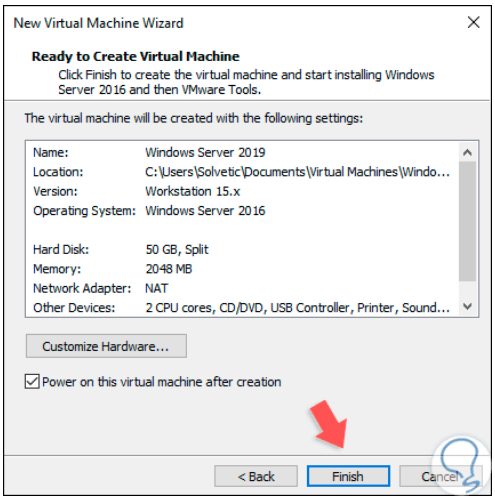
Paso 7

Al dar clic en Next podemos configurar el tamaño que será asignado al disco duro virtual de Windows Server 2019 así como definir el tipo de almacenamiento que este tendrá:



Paso 8

Damos clic en Next y veremos un resumen de la máquina a crear:



Fuente: https://www.solvetic.com/tutoriales/article/7204-como-instalar-windows-server-2019-en-vmware/

A N E X O - 16
GUIA DE LA PRACTICA DE INSTALACION

DE: INSTALACION DE WINDOWS SERVER 2019

No	ACCION / PROCESO	SI	NO	OBSERVACION
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

D. Configurando el software instalado de acuerdo con el manual del fabricante

ESTRATEGIA	PRODUCTO
9. **Da lectura "Tareas post instalación" (Anexo 17) para configurar el programa instalado y un correcto funcionamiento de Windows Server, realiza tres diagramas de flujo para cada uno de los procesos indicados.**	**9. 3 diagramas de flujo**

A N E X O - 17
CONFIGURACION DE WINDOWS SERVER

00:20 curso de Windows server 2016
00:24 para empezar la semana ahora
00:27 pues con materiales interesantes que se
00:28 que este curso os está gustando yo he
00:31 hecho un pequeño resumen 10 tareas
00:34 considero importantes vitales una vez
00:36 hemos terminado la implementación la
00:38 instalación de windows server 2016
00:42 en este caso 2016 pero que aplica
00:44 también por supuesto a otros sistemas
00:48 windows server y bueno una vez hemos
00:51 implementado el servidor o que lo hemos
00:52 instalado yo creo que una de las cosas
00:55 importantes que debemos de hacer es
00:56 verificar el estado de nuestros
00:59 controladores para ello podemos venir
01:02 aquí a la administración de dispositivos
01:04 o administrador de dispositivos y
01:06 verificar que todo se encuentra correcto
01:08 que no tenemos alertas y que no
tenemos
01:10 bueno pues algún conflicto de hardware
01:12 esto no impide esto no quiere decir que
01:16 si tenemos un controlador que el propio
01:18 Fabricante nos ha facilitado debemos de
01:21 instalarlo
01:22 habitualmente y por norma general
01:24 siempre un controlador del fabricante
01:26 aparte más cuando estamos trabajando
01:28 tema de servidores están ya certificados
01:29 por el propio microsoft bueno pues es
01:32 importante instalar este tipo de
01:34 controladores porque es posible que nos
01:35 den alguna funcionalidad adicional o que
01:38 ese dispositivo funcione mejor y aquí
01:41 evidentemente va a depender mucho de
01:43 cómo estemos haciendo el despliegue
01:46 nuestra red de dispositivos tengamos tal
01:49 vez el servidor tenga pues suyo que sea
01:51 un dispositivo para para el tema de
01:53 biometría o tenga un dispositivo para el
01:56 tema de conectar pues no se tiene una
01:59 controladora que conecta por fibra
02:01 óptica no sé cuánto todo esto debemos
02:03 comprobarlo porque es importante que
02:06 nuestro hardware esté perfectamente
02:08 configurado bien el segundo punto que
02:12 creo que es importante es implementar
02:14 evidentemente ya las medidas de
02:15 seguridad antivirus o software de
02:17 protección con el que estamos
trabajando
02:19 de acuerdo hay personas que dicen oye
02:21 pues sí ya vamos a trabajar con un
02:22 firewall externo deshabilitamos el
02:24 interno bueno aquí ya dependería para
02:27 gustos los colores yo creo que
02:29 firewalls son mejor que uno y pues
02:31 aquí entraría un poquito también

02:33 evidentemente el escenario en el que
02:36 estamos trabajando, pero bueno sin
02:38 duda implementar una solución antivirus
02:41 y configurarla actualizarla etcétera este
02:43 sería el segundo punto para mí muy
02:45 importante y una vez que ya tenemos
02:46 nuestros controladores en perfecto
02:48 funcionamiento y nuestro sistema
02:49 antivirus paso número 3 y esto ya lo
02:51 vamos a empezar a realizar renombrar el
02:53 servidor es importante renombrar el
02:55 servidor yo lo veis renombrando vamos a
02:57 ver que muy sencillito este va a ser el
02:59 de c 0 1 hacer sin mayúsculas de 0 1 de
03:03 acuerdo porque de c 0 1 bueno la idea y
03:07 ahora bueno pues ya reiniciando y
03:09 contando y tal es que esto luego forme
03:11 parte de un dominio el dominio que yo
03:13 vaya a elegir seguramente será el
03:14 soporte y punto local como identificar
03:17 ello este servidor en soporte y punto
03:20 local pues simplemente sabré que está
03:22 en de 0 1 punto
03:23 soporte y punto local una forma de poder
03:27 localizarlo de poder identificarlo
03:29 también cuando se empiezan a listar
03:30 todas las máquinas pues va a ser mucho
03:32 más sencillo saber que el tc 01 es un
03:35 controlador de dominio
03:36 igual que si tenemos o no es el pc
03:38 administrativo 1 pues sabemos que ese
03:41 equipo spc pertenece a un administrativo
03:44 pc gestión pc finanzas pc técnico pep lo
03:50 que sea es una forma fácil y sencilla de
03:53 después cuando estemos explorando red
03:55 cuando tengamos que trabajar con estos
03:57 equipos es una forma sencilla de poder
03:59 identificarlos y por supuesto de poder
04:01 acceder a ellos desde bueno pues de
04:03 forma más más fácil también incluso
04:06 para los usuarios para los clientes de
04:08 acuerdo hay veces que nosotros decía
04:10 nada pues si yo me acuerdo porque está
04:11 lo tengo la IP ya, pero los usuarios de
04:14 la red que los usuarios de la red
04:15 también van a tener que trabajar con
04:17 esto van a trabajar en red van a estar
04:19 almacenando datos van a estar haciendo
04:21 un equipo va a estar haciendo al otro y
04:23 es importante que puedan saber qué
04:24 equipo es cuál y a quién pertenece de
04:26 acuerdo bien el tercer perdón el cuarto
04:29 punto sería el tema de los adaptadores
04:32 de red yo me voy a abrir aquí un anfp.cl
04:35 el de siempre y voy a ver cómo está el
04:37 tema de bueno yo tengo dos
adaptadores
04:39 de red uno que dice que está
04:40 identificando y uno que tiene red
04:42 el primero que quiero identificar es el
04:44 que está conectado a internet que es
04:45 este ok genial ya lo tengo identificado
04:49 este va a ser el adaptador one este por
04:52 lo tanto es el adaptador LAN cuál es el
04:55 LAN el que conecta al switch, switch al
04:57 que también van a conectar los clientes
04:59 de esta red LAN oye si tengo siete
05:02 redes 7 adaptadores 77 switches y
05:06 entonces ya si podemos poner la red tal
05:09 LAN de soporte y la informática para
05:14 novatos y ahí vamos identificando vale a
05:17 qué red está conectando este adaptador
05:18 de red la segunda parte será
05:20 evidentemente este bueno especificar
05:23 unas direcciones unas direcciones IP yo
05:25 para ello voy a hacer una trampita me
05:28 voy a abrir aquí un ipconfig /all y
05:31 voy a copiar directamente pues bueno

05:34 IP es que yo tengo aquí porque yo las
05:37 voy a copiar bueno pues yo estoy en otra
05:38 red distinta yo no estoy en una red de
05:41 corporativa y por lo tanto no puedo
05:43 manejar todas las IPs que tengo en la
05:44 red de acuerdo hay más cuando son
05:46 máquinas virtuales etcétera así siempre
05:47 pusiera la misma red
05:49 un momento iba a tener un conflicto
05:50 entonces yo voy a poner las que están
05:51 nosotros evidentemente aquí debemos
05:54 optar por especificar una dirección IP
05:56 que nos permita al final también bueno
05:58 pues un poquito tener como una
06:00 metodología de trabajo pues, ejemplo
06:01 el servidor cuando conectan a LAN yo
06:03 siempre lo voy a poner la IP 90 está
06:06 bien para ti tú puedes usar la 90 no
06:07 tienes que usar la 100 no tienes que
06:09 usar la 10 no tienes que usar a 200 no
06:11 tienes que usar las 648 no utiliza a una
06:14 que a ti te permita saber cuándo tú
06:16 estás trabajando cuál es esa IP cuando
06:19 estés haciendo la documentación va a s
06:20 ser sencillísimo porque ni siquiera vas a
06:23 tener que consultar al servidor tú ya
06:24 sabes que siempre dices que el agua no
06:26 va a tener está y que harán va a tener
06:28 aquella de acuerdo yo no yo voy a
06:30 proceder a rellenar estos valores tal y
06:33 con la información que me está
06:35 facilitando esto y bueno pues vemos
06:38 sencillito esto no nos quita demasiado
06:41 tiempo ya lo sé que me equivoco
192.168.50.1
06:47 bien y la LAN puesta aquí si le voy a
06:49 poner ya unos valores que yo, con los
06:51 que sólo trabajar desde que era joven y
06:53 trabaje con windows server small
06:55 business qué pues que mira me hace
recordar aquellos tiempos,
07:04 perfecto ya hemos configurado las IPs ya
07:07 podemos volver a lanzar el comando y a
07:09 ver si está todo correcto a ver 50 157
07:13 que pum que para dónde estás que no
07:16 encuentro tun vale y el otro que está
07:20 desconectado porque está desconectado
07:23 me das bp no me das la IP el agua aquí
07:25 está vale aquí está que no la encontraba
07:27 que no la encontraba ok
07:29 aquí está otra vez más verde aquí está
07:31 la que aquí está aquí está la 16 100
07:33 aquí estamos viendo y DNS la 16 100
07:36 porque en el DNS pongo la misma
07:39 dirección que la IP porque este servidor
07:41 va a ser el servidor DNS por lo tanto el
07:43 DNS que tiene que utilizar la red LAN es
07:45 el mismo si tuviésemos un servidor DNS
07:48 que estuviese en otra IP, por ejemplo
07:50 este es el segundo servidor que
ponemos
07:52 y este es un servidor que va a dar pues
07:54 no sé un servicio tal bueno la IP más la
07:57 16 100 pues pueden ser las 16 101 y el
08:00 DNS cuál será la 16 100 que es el
08:02 servidor que tiene implementado el
08:04 servicio de DNS aquí lo implementa
08:06 después y tendremos que bueno pues ya
08:09 realizar algunas configuraciones que eso
08:10 lo veremos más adelante quinto paso
08:13 habilitar el acceso remoto muy
08:15 importante muy importante ahora
estamos
08:18 trabajando digamos que a una prima y
08:20 ciudad de delante de la máquina con una
08:21 pantalla delante el cacharro en el pie
08:23 por si le queremos zumbar
08:24 también prepararnos

08:27 por si necesitamos acceder mañana o
08:29 pasado al servidor vía escritorio remoto
08:32 para ello muy sencillito la opción es
08:37 servidor local y dentro del servidor
08:39 local escritorio remoto que como vemos
08:41 está de es habilitado esto habría que
08:44 habilitarlo de acuerdo simplemente
08:46 picamos aquí y permitir las conexiones
08:49 ok dice que permitir sólo las conexiones
08:52 desde equipos que ejecuten escritorio
08:54 remoto con la autenticación a nivel de
08:56 red de acuerdo perfecto
08:59 vamos a ver escritorio remoto
09:01 deshabilitado vamos a actualizar
09:04 perfecto ya está habilitado ok
09:07 recordamos por supuesto el server
09:09 manager hay que tenerlo control aquí
09:11 tenemos un botoncito que nos permita
09:13 actualizar cuando hacemos algún cambio o
09:14 ya que lo cambia y no pone ahí darle al
09:16 botoncito a ver si bien seguimos más
09:19 pasos ahora configuración de windows
09:21 update esto para no esto es impepinable
09:24 esto no se lo puede tratar nadie hay que
09:27 configurar windows update de acuerdo q
09:29 que configurar cambiaron las activas
09:31 a qué horas queremos que el servidor se
09:33 pueda reiniciar que no se pueda
09:34 reiniciar cuando esto va a estar
09:36 buscando actualizaciones vale porque es
09:38 importante porque a lo mejor no
09:40 queremos el servidor se ponga a buscar
09:41 actualizaciones cuando tanto el mundo
09:42 trabajando y navegando
09:44 que esto nos va a quitar ancho de banda
09:47 para los clientes de acuerdo no queremos
09:49 que el servidor se ponga actualizarse en
09:51 hora punta de trabajo esto lo podemos
09:53 configurar opciones de reinicio lo mismo
09:55 usar una hora de inicio personalizada
09:57 bueno pues si yo puedo usar una hora
09:59 de reinicio personalizado cuando ese
10:01 programa reinicio total vamos a ver
10:03 vamos a ver bueno pues no me deja
10:05 cambiarlo esto tendría que verlo esto
10:08 tendría que verlo de acuerdo,
10:10 tendría que porque está desactivado si
10:12 queréis lo podemos ver en un vídeo anexo
10:14 a este ok yo me tomaré nota de hecho
10:16 me voy a tomar nota ya voy a poner aquí
10:19 hora de reinicio personalizado vale esto
10:23 me lo dejaré porque ahora no quiero
10:24 entretenerme con más procedimientos
10:26 seguimos con más configuraciones
10:28 cerramos por aquí la siguiente la
10:31 seguridad mejorada de internet explorer
10:35 a por cierto por cierto en la
10:37 actualización una vez que está
10:38 configurado una vez terminado
10:39 con esto habría que buscar
10:41 actualizaciones y actualizar el servidor
10:43 completamente
10:44 esto es importante que lo tengamos claro
10:46 vale porque si no podemos tener pues
10:50 bueno que estamos instalando un active
10:51 directory que tal y justo que terminamos
10:53 y empieza a actualizarse lo mejor es
10:55 actualizarlo todo ver que todo está
10:56 correctamente funcionando y ya seguir
10:59 trabajando con él
10:59 y luego también tenemos que me había
11:01 saltado opciones avanzadas para aplazar
11:04 actualizaciones de características por
11:06 ejemplo esto para que es para que sólo

11:09 vaya tomando digamos que las
11:11 actualizaciones de seguridad las
11:12 actualizaciones importantes y luego
11:14 también tenemos la opción voy a marcar
11:17 las de ofrecer actualizaciones para
11:20 otros productos de microsoft ok esto es
11:22 bueno si tenemos pues algún exchange
11:25 alguna otra cosa oye que directamente
11:26 que lo busque y que me actualice el
11:29 acuerdo aún si cual tenemos un office
11:31 lo que sea que actualice directamente y
11:33 bueno a la de abajo la que estaba
11:34 comentando aplazar actualizaciones de
11:36 características ok esto lo único que va
11:39 a hacer es las características no las va
11:41 a implementar del tirón no las va a
11:42 implementar en cuanto salgan y las va a
11:44 implementar un poquito después el
11:46 acuerdo, así como opciones que debemos
11:48 de tener en cuenta seguridad mejorada
11:51 explorer esto dónde está vamos a ver
11:54 configuración de seguridad mejorada
11:55 internet explorer vemos que está
11:56 activado bien qué pasa con esto si
11:59 tratamos de navegar automáticamente e
12:02 internet es, pero no se nos va a estar
12:03 diciendo que este sitio no sé cuánto que
12:06 si no queremos tener el problemilla este
12:08 que seguro que se pasa alguna vez
12:09 desactivamos al menos para el
12:11 administrador ok y teniendo por supuesto
12:14 muy en cuenta muy muy en cuenta que
12:18 un servidor no es para que estemos
12:21 accediendo al Facebook para que nos
12:23 estamos metiendo en YouTube o para
12:26 que yo que sé para qué estamos
12:28 haciendo cualquier por internet de
12:30 acuerdo no está pensado para esto
12:32 servidor no se debe utilizar para esto
12:34 nada parece que tal bueno te vas a un
12:35 equipo cliente o te llevas tu equipo te
12:39 conectas a la red lo que te dé la gana
12:40 pero el servidor no a ni para navegar ni
12:43 para descargar programas ni pagos ni
12:45 nada de esos nombres, pero si es un
12:47 programa de microsoft
12:48 vamos a ver lo puedes descargar desde
12:49 otro equipo y pasarlo por la red bien el
12:52 servidor es para lo que es no es para
12:54 jugarnos para navegar y no para
12:55 tonterías así esto lo tenemos claro ella
12:57 que me estáis acá le estoy poniendo
12:59 nervioso nada más que de explicar lo
13:00 vamos seguimos por favor configuración
13:04 horaria fecha y hora y zona y horaria y
13:07 fecha y hora esto es importante también
13:09 aquí tenemos la hora vale que
13:13 configuración de fecha y hora bien cosas
13:16 importantes dónde estamos
13:18 Madrid- Copenhague que para muy bien
13:21 ajustarla ahora automáticamente
13:23 exactamente los domingos me cambias
13:25 hora y las tras las cuatro horas que hay
13:27 que dormir un horario de verano ya
13:29 sabemos notas de estas cosas cambiar
13:30 zona horaria automáticamente pero
13:31 establecer zona horaria
13:33 si queremos bien si no queremos también
13:37 y luego bueno pues cambiar ahora
13:38 automáticamente según el horario de
13:40 verano de acuerdo, me perdón
13:43 porque estoy aquí atrabancado esto es
13:46 para el ajuste de hora de verano esto es
13:48 para que establezca la hora y la zona
13:51 horaria, automáticamente y esto es
13:53 para que ajuste la hora, el solito al

13:55 ella tiene unos servidores ahí que va a
13:57 tratar de utilizar para poder tener la
14:01 hora correcta porque es importante no
14:03 vamos a poder actualizar el antivirus si
14:05 no tenemos la fecha y la hora correcta
14:06 si yo les estoy diciendo que estoy de
14:08 Madrid tengo a la hora de rusia
14:11 el servidor al que me conecté hacer a
14:13 ver si tú estás aquí porque tienes esta
14:15 hora tú estás intentando tirarme y eso a
14:17 mí no me mola me estás tomando el pelo
14:19 y no te doy actualización esto aquí no te
14:21 pues conectar eso puede pasar ok
14:24 aparte porque allá hay muchos servicios
14:25 que dependen de la hora es importante
14:27 tener la hora correctamente
14:29 configurada oye establece esto
14:31 automáticamente vamos a ver que
14:33 termine perfecto ya establecido esto
14:35 automáticamente ya no me va a decir
14:38 cambiar la hora automáticamente si está
14:40 esto ya lo va a hacer él solito ya tiene
14:42 la zona horaria ya he dicho que ajuste
14:44 la hora, perfecto esta es una
14:46 configuración muy válida para muchos
14:49 muchos escenarios
14:51 ok luego bueno cambiar el formato y tal
14:53 y opciones adicionales de nada esto lo
14:55 podéis repasar vosotros es importante
14:57 que se le dé un vistazo, pero no me
14:59 quiero entretener más porque se me está
15:00 estirando mucho el vídeo y no mola bien
15:03 seguimos más detalles más cosas más
15:06 configuraciones luego ella
15:09 los discos los emos particionado los
15:11 discos tenemos hemos conectado a la
15:13 cabina no hemos conectado esto hay
15:15 que hacerlo, pero antes de ponernos a
15:17 instalar cosas
15:19 tu eres mucho yo lo sé que ustedes tu
15:21 estés escuchando te estás poniendo
15:22 nervioso porque es que el lunes y voy
15:24 lanzado voy a lanzar o llevo aquí que se
15:27 me sale y está diciendo pablo
15:29 tranquilízate no me puedo tranquilizar
15:30 porque esto es importantísimo tareas
15:33 post instalación esto es importantísimo
15:38 los discos a configurar los discos vamos
15:40 a ver abrimos un explorador ya que pues
15:42 está la máquina virtual para pegarle una
15:45 patada y ponerla a bailar a bailar
15:47 fandangos vamos a ver este equipo
15:53 si siquiera va a abrir tu tómate tu
15:55 tiempo para que esta máquina la instala
15:57 en un disco mecánico madre mía no se
15:59 nota de uno mecánico a uno a uno sólido
16:02 de estos de una pieza
16:05 bueno pues según esto tengo un disco
16:07 duro y un DVD del windows vamos
16:11 al administrador de discos hoy,
16.13 dos discos porque tengo dos discos
16:15 porque yo cuando encargué el servidor
16:17 este para la empresa que se esté
16:18 instalando ahora para la de soporte tape
16:20 que pase unos digital
16:22 yo dije mira quiero un disco del sistema
16:24 para que el mundo esté tranquilo
16:25 sin hacerle daño a nadie que nadie
16:27 le haga daño a él que está aislado que
16:28 esté en su parte ahí en su rollo y luego
16:30 quiero otro disco duro que lo va a poner
16:33 en línea
16:34 no vaya configurando mientras les estoy
16:36 explicando que lo va a inicializar vale
16:41 exactamente tu sigue así que voy a crear
16:44 un nuevo volumen que se va a llamar
16:45 datos, que datos no por los datos
16:48 del cliente los datos de la empresa ok o

16:51 los datos de lo que sea que tengo seis
16:52 discos de datos bueno pues identificar
16:54 los de alguna manera tronco no me vale
16:56 datos del departamento tal dato de la
16:59 sede de Valencia datos de las sedes de
17:02 Barcelona de Bilbao de Cantabria donde
17:07 sea macho tú ponte ahí, pero identificar
17:10 los troncos y luego dice b pablo
17:11 propósito de los discos duros si pedí
17:13 dos discos duros porque a mí me gusta a
17:15 mí me daban dos a mí me daban dos
17:17 suite a ver qué estáis a mí me daban
17:19 dos entonces digo uno aparato mínimo y
17:22 uno como este disco para qué es
17:25 bueno si no aciertas te suscribes al
17:28 canal y le metes un like copia de
17:30 seguridad propia de seguridad
17:33 si lo ha dicho el tío pablo ya veinte
17:35 mil veces un disco para la copia de
17:37 seguridad ronca
17:39 para que la copia de seguridad de la
17:40 unidad de la unidad de la unidad de dato
17:42 de lo que tú quieras de acuerdo
17:45 qué estás trabajando con una cabina o
17:48 te creas tú los costos para conectarse
17:50 por internet así que lo podemos ver en
17:53 otro momento ahora no ha dicho
17:56 las tareas de instalación habrá muchas
17:58 tareas que van a desarrollarse pues tal
18:00 vez con otras tareas, pero yo voy un
18:03 poquito a lo importante ahora cuando
18:06 termine el vídeo cuando termine la chapa
18:10 haremos un repaso de las 10 tareas que
18:12 toma de apuntadas miradas tengo dos
18:13 idiomas o chuletas no sólo digáis a
18:15 nadie ok pero aquí más o chuletas para
18:18 poder esto tener un poquito control bien
18:19 ya hemos terminado por esto y lo último
18:21 lo último esto es una novedad que
18:24 incorporó a mi lista de tareas como veis
18:26 la voy modificando más o menos poco a
18:28 poco conforme pasa el tiempo conforme
18:30 me voy haciendo más más viajes más
18:32 veteranía y bueno pues la última tarea
18:35 incluye algo con lo que a todos estamos
18:38 más que familiarizados de acuerdo es
18:41 el tema de la virtualización ciudad
18:45 pablo a ver qué virtualización tío
18:49 explícame esto te lo estoy explicando tú
18:51 tranqui este es un servidor virtual sí
18:55 muy bien
18:57 entonces has configurado ya la máquina
19:00 virtual pablo como que se ha configurado
19:01 la máquina virtual que me estás
hablando
19:04 tronco mira lo que te estoy hablando es
19:06 lo que te lo que te voy a enseñar ahora
19:08 es lo que te voy a enseñar ahora esto es
19:10 la configuración de la máquina virtual
19:12 esto Skype virus todo lo tienes que
19:13 hacer con cualquier sistema no es que
19:15 soy de bien web, que tal obra sé
19:17 cuánto OIS en Citrix no sé qué muy bien
19:20 lo que tú quieras, pero configura te la
19:22 máquina virtual, los escáneres o oye un
19:25 procesador estoy poniendo buscarlo va
19:27 lento oye 4 GB de memoria será
19:30 suficiente si no, no sé no, lo sé no
19:33 me acuerdo
19:33 oye ha configurado la memoria dinámica
19:36 no porque está no sí porque está la
19:38 ponderación de la memoria texto la
19:39 configurado es que pablo no sé de qué
19:41 me estás hablando soporte ti búscalo en
19:44 YouTube ahí tienes vídeos de híper-vi
19:46 para echar para abajo y si no en e
19:49 learning en el ring wire si estoy
19:51 conectado y si puedo si puedo completar

19:53 aquí una tarea una tarea sencilla vale
19:56 vamos a ver aquí tienes
19:58 el ning punto soporte y punto net si
20:02 aquí tienes el curso de Hyper y el curso
20:05 bastante completito que te vaya un
20:06 poquito a conocer el sistema ahora
20:08 pablo no yo lo que quiero yo
20:11 quiero todo yo no quiero un cursito vale
20:12 mirar si aquí los tienes unos cursos
20:14 online que están geniales destaca
20:17 y pervivir aquí lo pone curso online the
20:19 Hyper-vi bien no, no, pero yo quiero otro
20:22 de otro tipo de formación bueno
20:25 tiene soporte y punto, pero una página
20:28 web que esto no es una web esto
20:30 es un nuevo abrazo vamos esto es un kit
20:34 de sorpresas y tiene un montón de cosas
20:36 en su interior vale si conseguimos que
20:39 la máquina está despierte porque veo
20:40 está un poquito adelante vienes aquí te
20:43 suscribes espía la suscripción que más
20:45 temores
20:46 si tienen materiales para echar para
20:48 arriba y para abajo servidores fijaos
20:52 Hyper-Vi, 70 410 cursos, cursos de texto
20:56 tales documentos, soporte y punto pro te
20:59 metes ahí y lo triunfas
21:02 y bueno para rematar un repasito que os
21:05 había dicho que ahora bueno pues
21:07 aparecerá unos cartelitos por aquí para
21:08 que me ponga la marca de tiempo
21:11 los 10 puntos que hemos tratado
21:13 estoy un poquito se desenvolvía el
21:15 vasito de agua y no pasan a los 10
21:17 puntos importantes primero verifica el
21:19 estado de controladores de apuntando
21:21 está y manolo apunta venga segundo
21:23 implementar software antivirus a
21:25 actualizar con figura de tera de acuerdo
21:27 esto igual todo, todo lo que todas las
21:29 tareas que diga evidentemente muchas
21:32 conllevan después actualizar configurar
21:33 etcétera de acuerdo bien empieza otra
21:37 vez y ya no me enreda más uno verifica
21:39 el estado de controladores 2
implementar
21:41 software antivirus 3 renombrar el
21:44 servidor para tener control a polar & 4
21:47 renombrar adaptadores de red y
21:49 configurar ok direccionamiento estático
21:52 importante para los servidores quinto
21:54 habilitar acceso remoto sexto configurar
21:58 windows update y lanzar una
21:59 actualización completa ok
22:04 desactivar la seguridad mejorada de
22:06 internet explorer al menos para el
22:08 administrador si vamos a estar
navegando
22:10 mucho que no deberíamos es más yo
22:12 incluso esta opción la tendría muy en
22:15 cuenta, pero bueno octavo configuración
22:18 horaria de acuerdo sabemos fecha, hora
22:20 zona horaria, horario de verano que tuvo
22:21 un quepan que para qué por qué porque
22:23 pam pum y nueve particionar
22:26 discos décimo virtualización es un
22:29 sistema virtualizado a vamos a
22:31 virtualizar con él vamos a virtualizar
22:34 con él vamos a necesitar una unidad
22:36 destinada a almacenar las máquinas
22:37 virtuales vamos a tener que hacer algún
22:40 tema de la red o alguna configuración
22:42 específica, en específico, específica en
22:46 el servidor para las máquinas que vamos
22:48 a hospedar virtuales detalles que hay
22:50 que tener en cuenta

Fuente: https://youtu.be/Up_1TvDtLS8

T E R C E R P A R C I A L

COMPETENCIA - ESTABLECE LOS DERECHOS DEL TRABAJO DE USUARIOS SOBRE LOS RECURSOS DE LA RED

CONTENIDOS:

A. Gestionando permisos de acuerdo a los requerimientos de la organización

ESTRATEGIA	PRODUCTO
1. Lee el documento "permisos y derechos de usuario" (Anexo 18), realiza un mapa conceptual.	**2. Mapa conceptual**

A N E X O - 18

ESTABLECE PERMISOS Y DERECHOS DE TRABAJO DEL USUARIO SOBRE LOS RECURSOS DE RED

En Windows Server, 2000 y XP, lo que pueden hacer las cuentas se dividen en dos partes: derechos y permisos. Los derechos son acciones u operaciones que una cuenta puede o no puede realizar. Los permisos definen los recursos a los que una cuenta puede o no puede acceder y el nivel de dicho acceso. Entendamos que recursos comprenden también a los objetos de Active Directory, objetos de sistema de archivo y llaves del registro. Aunque las cuentas son el eje central de seguridad de Windows, asignarles derechos y permisos directamente es difícil de administrar y muchas veces de solucionar su aplicación o no aplicación tanto de derechos como de permisos. Por ello, siempre se aconseja no asignarlos a cuentas y en su lugar hacerlo sobre grupos y emplazar las cuentas dentro de los mismos.

La creación de una estructura de grupos para administrar la asignación de derechos y permisos es una parte esencial de la seguridad de Windows.

- ***Derechos de usuario y permisos***

Como ya he dicho las acciones que una cuenta puede llevar a cabo y el nivel con que un usuario podrá acceder a la información son determinados por los derechos de usuario y los permisos.

Los administradores podemos asignar derechos específicos a cuentas de grupos o de usuario. Estos derechos autorizan a llevar a cabo acciones específicas, por ejemplo, iniciar sesión, crear copias de seguridad, etc… Se diferencian de los permisos de forma clara e inequívoca, los derechos se aplican a cuentas, los permisos se adjuntan a los objetos.

- **Privilegios**

Un derecho es asignado a una cuenta y especifica las acciones permitidas en la red.

- **Derechos de inicio de sesión**

Derecho asignado a una cuenta y que especifica la forma en que la misma iniciará sesión en el sistema. Por ejemplo: iniciar sesión local.

LOS PRIVILEGIOS

Algunos privilegios pueden sobrescribir los permisos establecidos en un objeto.

Actuar como parte del sistema operativo

Este privilegio permite literalmente a la cuenta o aplicaciones en ejecución bajo la misma ser parte de la base de confianza del cálculo. Esto permite a un proceso autenticarse como cualquier usuario, y por lo tanto obtener acceso a los recursos bajo la identidad del mismo. Sólo los servicios de autenticación de bajo-nivel de mayor confianza deben necesitar este privilegio. El usuario o proceso con este privilegio puede crear tokens que garantizan más derechos que los que normalmente se proporcionan en su contexto de seguridad.

No deberíamos asignar este privilegio a menos que estemos completamente seguros que es necesario.

Administrar los registros de auditoría y seguridad

Permite a un usuario especificar opciones de auditorías de acceso a objetos para recursos individuales, como archivos, objetos de AD y llaves del registro. La auditoría a los objetos no se llevará a cabo a menos que tengamos habilitada la configuración de auditoría que la activa. Un usuario con este privilegio puede ver y limpiar el registro de seguridad en el visor de sucesos.

Agregar estaciones de trabajo al dominio

Permite añadir equipos a un dominio específico. Los usuarios sólo pueden unir hasta 10 equipos de forma predeterminada. Para aumentar este número hay que cambiar una propiedad llamada ms-DS-MachineAccountQuota o también podemos delegar en un usuario la capacidad de crear cuentas de equipo en una OU.

Ajustar cuotas de memoria para un proceso

Este privilegio determina quien puede cambiar la memoria máxima que se puede consumir por un proceso. Útil para un afinamiento del sistema, pero que podría convertirse en un ataque DOS.

Apagar el sistema

Permite al usuario el apagado del sistema local. Quitándoles este derecho a los usuarios de Terminal Server impediremos que apaguen el equipo, sea accidental o intencionadamente.

Bloquear páginas de memoria

Permitir a un proceso mantener datos en la memoria física impidiendo que el sistema los pagine en la memoria virtual en disco. Este privilegio puede afectar al rendimiento del sistema, es obsoleto y no debe usarse.

Cambiar la hora del sistema

Permite al usuario establecer la hora en el reloj interno del equipo. De forma predeterminada, desde Windows 2000, los usuarios del dominio no tienen este privilegio para evitar que cambien la hora de su sistema y ello interfiera en la autenticación Kerberos (una diferencia de 5 o más minutos impediría trabajar correctamente).

Cargar y descargar controladores de dispositivo

Permite a un usuario instalar y desinstalar controladores de dispositivo que no han sido instalados por el administrador de P&P y controlar los dispositivos (iniciarlos o detenerlos). Como los controladores se ejecutan como programas en los que se confía, un mal uso de este privilegio podría servir para la instalación de programas hostiles, como rootkits, y darles acceso a los recursos. No debería concederse en exceso.

Crear objetos compartidos permanentes

Permite a un proceso crear un objeto de directorio en el Administrador de objetos. Este privilegio es útil para los componentes en modo kernel para la ampliación del espacio de nombres. Ya que los componentes que se ejecutan en modo kernel ya disfrutan de este privilegio no parece necesaria su aplicación específica.

Crear objetos globales

Este privilegio se añadió en el SP4 de Windows 2000 y está presente en Windows Server 2003. Controla la creación de objetos del sistema globales por aplicaciones, incluyendo operaciones como el mapeo de archivos en las sesiones de Terminal Server. También se aplica si se crean enlaces simbólicos en el administrador de objetos.

Crear un archivo de paginación

Permite al usuario crear y cambiar el tamaño del archivo de paginación. Esto se hace especificando un tamaño de archivo de paginación para una determinada unidad en el cuadro de diálogo de opciones de Rendimiento, desde el cuadro de diálogo de las propiedades del sistema.

Crear un objeto testigo

Permite a un proceso la creación de un token y usarlo para obtener acceso a recursos locales cuando el proceso use las APIs de creación de token. Predeterminadamente sólo LSA (Local Security Authority) puede crear tokens.

Depurar programas

Permite al usuario adjuntar un depurador a cualquier proceso. Sin este privilegio, podemos depurar los programas propios. Este privilegio proporciona un acceso poderoso a componentes del sistema operativo sensibles y críticos, ¡Así que a ver a quien se le concede!!

Forzar el apagado desde un sistema remoto

Permite al usuario el apagado de un sistema desde cualquier ubicación remota de la red.

Generar auditorías de seguridad

Permite a un proceso generar entradas en el registro de Seguridad (Security log) para auditar el acceso a los objetos. También le permite generar otras auditorías de seguridad. Este registro de seguridad se utiliza para el seguimiento del acceso no autorizado al sistema.

Habilitar las cuentas de equipo y de usuario en las que se confía para delegación

Permite al usuario seleccionar la configuración de 'se confía para delegación' de la configuración de un objeto equipo o usuario. El usuario u objeto al que se le concede este privilegio debe tener permiso de escritura sobre las banderas de control de la cuenta del usuario u objeto. Un proceso de servidor ya se esté ejecutando en un equipo o usuario en los que se confía por delegación puede acceder a recursos en otro equipo. El proceso usa credenciales delegadas de cliente, siempre que la cuenta del cliente no tenga establecida la bandera de control en la cuenta de Account Cannot Be Delegated(la cuenta no puede delegarse). El abuso de este privilegio o sobre los valores de 'se confía para delegación' pueden hacer vulnerable nuestra red a ataques con troyanos.

Hacer copias de seguridad de archivos y directorios

Permite a los usuarios eludir los permisos de archivos y directorios para realizar una copia de seguridad almacenada en el sistema. Algo como asignar los permisos: Recorrer carpeta / Ejecutar archivo, Listar carpeta / Leer datos, Atributos de lectura, Atributos extendidos de lectura y Permisos de lectura, a todos los archivos y carpetas del equipo local.

Incrementar prioridades de planificación de procesos

Permite a un proceso con permiso de escritura sobre otro, elevar la prioridad de ejecución del otro proceso. Un usuario con este privilegio puede cambiar la planificación de prioridad de un proceso usando el Administrador de Tareas.

Modificar valores de entorno de la memoria no volátil(firmware)

Permite la modificación de las variables de entorno del sistema, sea por un proceso o por un usuario desde el cuadro de diálogo de propiedades del sistema.

Omitir la comprobación de recorrido

Permite al usuario navegar entre directorios que de otra forma no tendría acceso. No permite listar los contenidos sólo atravesarlos. Si no se tiene este privilegio el sistema comprueba las ACL del directorio para asegurarse que el usuario dispone del permiso Recorrer carpeta / Ejecutar archivo.

Perfilar el rendimiento del sistema

Permite a un usuario usar las herramientas de rendimiento-monitorización para monitorizar los procesos del sistema. Este privilegio es necesario para el complemento de Rendimiento de la consola MMC si está configurado para recoger datos mediante WMI.

Perfilar un proceso individual

Permite a un usuario usar las herramientas de rendimiento-monitorización para monitorizar procesos que no son del sistema. Este privilegio es obligatorio para el complemento de Rendimiento de la consola MMC en el caso de estar configurado para recoger datos mediante WMI.

Quitar el equipo de la estación de acoplamiento

Permite al usuario desacoplar al portátil mediante el interfaz de usuario. Por supuesto los usuarios sin este derecho podrán anular el acople manualmente o mediante pequeños conectores y sacar el portátil de la estación de acoplamiento.

Realizar las tareas de mantenimiento del volumen

Permite al usuario administrar volúmenes y discos.

Reemplazar un testigo a nivel de proceso

Permite a un proceso reemplazar el testigo predeterminado asociado a un subproceso que se ha iniciado. Este privilegio sólo debería obtenerse mediante la cuenta de Sistema Local. Se usa, entre otras cosas, para crear testigos restringidos.

Restaurar archivos y directorios

Permite a un usuario evitar los permisos de archivo y directorio cuando restaura una copia de seguridad y establecer cualquier objeto principal como el propietario de un objeto.

Sincronizar los datos de Directory Service

Permite a un proceso leer todos los objetos y propiedades en el directorio, a pesar de la protección de los mismos. Este privilegio es necesario para usar sincronización de servicios de directorio LDAP.

Tomar posesión de archivos y otros objetos

Permite a un usuario romar posesión de cualquier objeto asegurable del sistema, incluyendo los objetos de AD, archivos e impresoras, impresoras, llaves del registro, procesos e hilos.

LOS DERECHOS DE USUARIO

Tener acceso a este equipo desde la red

Permite a un usuario conectar con el equipo desde la red.

Denegar el acceso desde la red a este equipo

Deniega la conexión con el equipo desde la red. Predeterminadamente no está asignado a nadie, a excepción de la cuenta integrada de soporte. El mal uso puede llevar al bloqueo de uno mismo o del sistema.

Iniciar sesión como proceso por lotes

Permite a un usuario iniciar sesión usando un archivo por lotes. De forma predeterminada está concedido sólo a los administradores. Cuando uno de ellos usa el asistente de añadir una tarea programada para programar una tarea y ejecutarse bajo un usuario y contraseña particulares, este usuario es asignado automáticamente al inicio de sesión como un derecho de proceso por lotes. Cuando llega el momento de ejecutarse, el programador de tareas inicia la sesión del usuario como un proceso por lotes más que un usuario interactivo, y la tarea se ejecuta en el contexto de seguridad del usuario.

Denegar el inicio de sesión como trabajo por lotes

Deniega al usuario la posibilidad del inicio de sesión usando un proceso por lotes. De forma predeterminada no está concedido a nadie.

Iniciar sesión como servicio

Permite a un objeto principal iniciar sesión como servicio y establecer un contexto de seguridad. Las cuentas de Sistema Local, Servidor de red y Servicio Local siempre retienen el derecho de iniciar sesión como servicio. Cualquier servicio que se ejecute con una cuenta distinta debe serle concedido el derecho.

Denegar el inicio de sesión como servicio

Deniega a un objeto principal la posibilidad de iniciar sesión como servicios y establecer un contexto de seguridad.

Permitir el inicio de sesión local

Permite a un usuario iniciar sesión en el equipo mediante sea con la consola o una sesión de servicios de terminal y con IIS. La configuración de este derecho debe realizarse con precaución puesto que podríamos incluso impedirnos a nosotros mismos acceder al sistema si nos lo quitamos. En Windows Server 2003 es posible que un usuario establezca una conexión mediante una sesión de servicios de terminal contra un equipo específico sin este derecho, debido a la existencia del derecho de 'permitir inicio de sesión a través de Servicios de Terminal Server'.

Denegar el inicio de sesión localmente

Deniega al usuario el inicio de sesión a la consola del equipo. Predeterminado a nadie. También ha de aplicarse con precaución ya que podríamos impedirnos a nosotros mismos acceder al sistema.

Permitir inicio de sesión a través de Servicios de Terminal Server

Permite a un usuario el inicio de sesión usando servicios de terminal en XP y Windows Server 2003. Si concedemos este derecho no es necesario ya añadir al usuario al derecho de inicio de sesión local como lo era en Windows 2000.

Denegar inicio de sesión a través de Servicios de Terminal Server

Deniega el inicio de sesión al usuario usando servicios de terminal. Si tiene el derecho de inicio de sesión local, podrá hacerlo a la consola del equipo.

B. Generando el reporte de control de acceso

ESTRATEGIAS	PRODUCTOS
2. Lee el tema de control de acceso (ACL) (Anexo 19) y elabora un cuadro sinóptico. **3. Da lectura a "Exportar permisos NTFS de carpetas con PowerShell" (Anexo 20), realiza un resumen.**	**1. Cuadro sinóptico** **2. Resumen**

A N E X O - 19
CONTROL DE ACCESO (ACL)

Para la seguridad de las redes de trasmisión de datos TCP/IP de forma general los administradores utilizan *firewalls o cortafuegos* para protegerlas contra el acceso no permitido por la red, aplicando políticas de seguridad para el filtrado de los paquetes que transitan por los canales de trasmisión de datos. Para ello se utiliza lo que se denomina una Lista de Control de Accesos.
Una Lista de Control de Accesos (ACL: *Access Control List*) es una serie de instrucciones que controlan que en un *router* se permita el paso o se bloqueen los paquetes IP de datos, que maneja el equipo según la información que se encuentra en el encabezado de los mismos.

Las ACL configuradas realizan las siguientes tareas:

- Limitan el tráfico de la red para aumentar su rendimiento. En una entidad, por ejemplo, si su política corporativa no permite el tráfico de video en la red, se pueden configurar y aplicar ACL que lo bloqueen, lo que reduce considerablemente la carga de la red y aumenta su rendimiento.
- Proporcionan un nivel básico de seguridad para el acceso a la red. Las ACL pueden permitir que un host acceda a una parte de la red y evitar que otro lo haga a esa misma área.
- Filtran el tráfico según su tipo. Por ejemplo, una ACL puede permitir el tráfico de correo electrónico, pero bloquear todo el tráfico de redes sociales.
- Filtran a los hosts para permitirles o denegarles el acceso a los servicios de red. Las ACL pueden permitirles o denegarles a los usuarios el acceso a determinados tipos de archivos.

Los *routers* no tienen configuradas de manera predeterminada las ACL, por lo que no filtran el tráfico por si, solos si antes no fueron programados. El tráfico que ingresa al *router* se encamina solamente en función de la información de la tabla de ruteo; sin embargo, cuando se aplica una ACL a una interfaz de red, se realiza la tarea adicional de evaluar todos los paquetes de la red a medida que pasan a través de la misma, para determinar si se pueden reenviar.

Funcionamiento: Filtrado de Paquetes
Una Lista de Control de Accesos (ACL) es una enumeración secuencial de instrucciones permit (permitir) o deny (denegar), conocidas como “entradas de control de acceso”, o también con frecuencia como “instrucciones ACL”. Cuando el tráfico de la red atraviesa una interfaz de red configurada con una ACL, el router compara la información dentro del paquete IP con cada entrada de la lista en orden secuencial, para determinar si coincide con alguna. Este proceso se denomina filtrado de los paquetes.
El filtrado de los paquetes controla el acceso a una red mediante el análisis de los paquetes entrantes y salientes, y la transferencia o el bloqueo de estos según criterios determinados. Las ACL estándares filtran sólo en la Capa 3, mientras que las ACL extendidas filtran en las capas 3 y 4 del modelo OSI.
El criterio de filtrado establecido en cada entrada de una ACL es la dirección IP de origen.
Un *router* configurado con una ACL estándar toma la dirección IP de origen del encabezado del paquete y comienza a compararla con cada entrada de la ACL de manera secuencial. Cuando encuentra una coincidencia, el *router* realiza la instrucción correspondiente, que puede ser: permitir o bloquear el paquete, y finaliza la comparación. Si la dirección IP del paquete no coincide con ninguna entrada en la ACL, se bloquea el paquete por definición.
La última instrucción de una ACL es siempre una denegación implícita. Esta sentencia se inserta automáticamente al final de cada ACL, aunque no esté presente físicamente. La denegación implícita bloquea todo el tráfico. Debido a esto, una ACL que no tiene al menos una instrucción *permit* bloqueará todo el tráfico.

Para la configuración de las Listas de Control de Acceso de los *routers*, es importante conocer que estas se aplican para el intercambio de paquetes de datos tanto a las interfaces de red de entrada como de salida. En este sentido:

- Las ACL de entrada: procesan los paquetes entrantes al *router* antes de dirigirse a la interfaz de salida. Constituyen un elemento de eficacia, porque ahorran la sobrecarga de encaminar

búsquedas si el paquete se descarta. Son ideales para filtrar paquetes de datos cuando la red conectada a una interfaz de entrada es el único origen de estos que se deben examinar.
- Las ACL de salida: los paquetes entrantes se enrutan a la interfaz de salida del *router*, y después se procesan mediante la ACL de salida. Las ACL de salida son ideales cuando se aplica un mismo filtro a los paquetes que provienen de varias interfaces de entrada antes de salir por la misma interfaz de salida.

Máscaras *Wildcard* en ACL

Cada entrada de una ACL incluye el uso de una máscara *wildcard* o "comodín". Una máscara *wildcard* es una cadena de 32 dígitos binarios que el *router* utiliza para determinar qué bits de la dirección del paquete debe examinar para obtener una coincidencia.

Como ocurre con las máscaras de subred, los números 1 y 0 en la máscara *wildcard* identifican lo que hay que hacer con los bits de dirección IP correspondientes. Sin embargo, en una máscara *wildcard*, estos bits se utilizan para fines diferentes y siguen diferentes reglas:

- Bit 0 de la máscara *wildcard*: se establece la coincidencia con el valor del bit correspondiente en la dirección IP.
- Bit 1 de la máscara *wildcard*: se omite el valor del bit correspondiente en la dirección IP.

Mientras que las máscaras de subred utilizan 1 y 0 binarios para identificar la red, la subred y la porción del host de una dirección IP las máscaras *wildcard* los utilizan para filtrar direcciones IP individuales o grupos de ellas, permitiendo o denegando el acceso a los recursos.

A las máscaras *wildcard* a menudo se las denomina "máscaras inversas". La razón es que, a diferencia de una máscara de subred en la que el 1 binario equivale a una coincidencia y el 0 binario no, en las máscaras *wildcard* es al revés.

Aunque el cálculo de la máscara *wildcard* puede ser difícil, un método abreviado para determinarla es restar a 255.255.255.255 la máscara de red de la dirección IP.

Para simplificar el trabajo con la márcara *wildcard* se emplean además las palabras clave *host* y *any*, que eliminan la necesidad de introducirlas para identificar un host específico o toda una red, además de facilitar la lectura de la lista de control de accesos, ya que proporcionan pistas visuales en cuanto al origen o el destino de los criterios:

- La palabra *host* reemplaza la máscara *wildcard* 0.0.0.0, la cual indica que todos los bits de la dirección IP deben coincidir para filtrar solo un host.
- La opción *any* sustituye la dirección IP y la máscara 255.255.255.255. Esto establece que se omita la dirección IP completa o que se acepte cualquier dirección.

Tipos de ACL:

Al crear una lista de control de acceso un administrador de red tiene varias opciones; en este sentido, la complejidad del diseño de dicha red determina el tipo de ACL necesaria. Por lo general, existen dos tipos clásicos de ACL:

- **ACL estándar**: que permiten el filtrado de paquetes de datos únicamente verificando la dirección IP de origen. De esta manera, si un dispositivo es denegado por una ACL estándar, se deniegan todos los servicios provenientes de él. Este tipo de ACL sirve para permitir el acceso de todos los servicios de un usuario específico, o LAN, a través de un *router* y a la vez, denegar el acceso de otras direcciones IP. Las ACL estándar están identificadas por el número que se les ha asignado. Para las listas de acceso que permiten o deniegan el tráfico IP, el número de identificación puede variar entre 1 y 99 o entre 1300 y 1999.
- **ACL extendidas**: filtran no sólo según la dirección IP de origen, sino también según la dirección IP de destino, el protocolo y los números de puertos. Con frecuencia son más empleadas que las ACL estándar, porque son más específicas y ofrecen un mayor control. El rango de números de las ACL extendidas va de 100 a 199 y de 2000 a 2699.

Adicionalmente, tanto a las ACL estándar como extendidas es posible hacerles referencia mediante un nombre descriptivo en lugar de un número, lo que se conoce como ACL nombradas.

Existen además otros tipos de ACL, enfocados en propósitos específicos de configuración y manejo del filtrado de los paquetes de datos, como son las ACL dinámicas, reflexivas, basadas en tiempo, y basadas en el contexto, entre otras.

Pautas para la utilización de las ACL

La configuración de la ACL puede ser una tarea compleja. Para cada interfaz de red de un *router*, puede haber varias políticas necesarias para administrar el tipo de tráfico que se tiene permitido ingresar o salir de ella. Como buenas prácticas es recomendable configurar ACL independientes tanto para el tráfico entrante como para el saliente.

Las siguientes son algunas pautas para el uso de las ACL:

- Utilizar la ACL en los *routers* de *firewall* ubicados entre la red interna y la externa (como Internet).
- Emplear la ACL en un *router* ubicado entre dos partes de la red para controlar el tráfico que entra a una parte específica de la red interna o que sale de esta.
- Configurar la ACL en los *routers* de frontera, es decir, los ubicados en los límites de las redes, lo que proporciona una separación básica de la red externa, o entre un área menos controlada y otra más importante de la propia red.
- Configurar la ACL para cada interfaz de red (de entrada, o de salida), del *router* de frontera.

El uso de las ACL requiere prestar atención a los detalles y un extremo cuidado. Los errores pueden ser costosos en términos de tiempo de inactividad, esfuerzos de resolución de problemas y servicio de red deficiente. Antes de configurar una ACL, se requiere una planificación básica.

La correcta conformación de la ACL puede contribuir a que la red funcione de forma eficiente. En este sentido, se deben configurar donde tengan mayor impacto. Las reglas básicas a considerar son:

- Las ACL estándar se colocan cerca del destino del tráfico. Esto se debe a sus limitaciones, pues no se puede distinguir el destino.
- Las ACL extendidas se colocan cerca del origen del tráfico por eficiencia, para evitar tráfico innecesario en el resto de la red.

Fuente: https://infotecs.mx/blog/acl-lista-de-control-de-accesos.html#:~:text=Una%20Lista%20de%20Control%20de%20Accesos%20(ACL%3A%20Access%20Control%20List,el%20encabezado%20de%20los%20mismos

A N E X O - 20
EXPORTAR PERMISOS NTFS DE CARPETAS CON POWERSHELL

00:00 ahora todos bienvenidos a un nuevo vídeo
00:03 me preguntaron de cómo exportar los
00:06 permisos que tiene una carpeta cómo
00:07 saber cuáles son los permisos detallados
00:09 y pues esto no hay mejor forma que
00:12 hacerlo a través de POWER SHELL vamos
00:14 a ver cómo podemos exportar todos los
00:16 permisos de una carpeta sea un recurso
00:17 de compartir una carpeta que tenemos en
00:19 nuestro servidor para poder conocer
00:20 todos los permisos lo vamos a exportar
00:22 un archivo delimitado por como CSV y con
00:25 esto vamos a nosotros a poder filtrar lo
00:27 llevamos allí a un Excel o filtramos
00:29 y podemos conocer qué usuarios
00:31 tienen permisos y qué permisos tienen ok
00:34 entonces para ello tengo una carpeta por
00:36 aquí que se llama company tengo una
00:38 carpeta aquí que se llama company esta
00:40 carpeta tiene ciertos permisos y lo
00:42 bueno de este tema con power si él es
00:44 que nos va a exportar también los
00:45 subcarpetas o los permisos de las
00:47 subcarpetas de nuestro, nuestra carpeta
00:50 principal los permisos NTFS vamos a ir
00:53 de aquí a seguridad y aquí vamos a ver
00:54 todos los permisos que tiene nosotros
00:56 vamos a poder tener también los permisos
00:58 que tiene estas subcarpetas, por ejemplo
01:00 aquí en seguridad vemos que tiene estos

01:01 otros permisos y todo esto
01:03 lo vamos a hacer otra vez de power si el
01:05 día en que la herramienta favorita para
01:06 todo administrador es power si él porque
01:08 nos automatiza muchas cosas y lo vamos a
01:11 hacer a través de una pequeña cadena de
01:13 comandos ok aquí lo que
01:16 vamos a hacer es que vamos a
01:19 a filtrar o vamos a realizar una
01:22 búsqueda o vamos a listar nuestra
01:25 carpeta en este caso que está en ser
01:27 company vemos que la carpeta está en
01:29 facer company y vamos a darle es decirle
01:32 que vamos a realizar vamos a buscar o
01:36 vamos a mostrar todos los accesos las
01:39 listas ACL o los permisos de nuestra
01:41 carpeta donde vamos a seleccionar este
01:44 tema y vamos a exportarlos a un archivo
01:46 CSV que ésta lo vamos a guardar en ce se
01:50 llama NTFS permisos punto CSV ok
01:53 entonces vamos a ejecutar nuestro
01:55 comando vamos a ejecutar nuestros ml ya
01:57 saben que los voy a dejar en la
01:58 descripción del vídeo para que lo tengan
02:00 y facilitó y rápido para que lo ejecuten
02:02 vamos a ejecutarlo y hemos aquí hemos
02:05 ejecutado nuestro comando vamos a irnos
02:07 a buscar en la carpeta ce en este caso y
02:10 vamos que aquí tenemos nuestro permiso
02:12 es un archivo CSV si no tienen excelente
02:15 servidor se nos muestra como un bloc de
02:18 notas, pero lo pueden llevar a un archivo
02:20 a un Excel y lo pueden filtrar un poco
02:23 aquí tenemos nuestro archivo vemos que
02:25 no se filtra
02:26 el tema de los permisos dónde está la
02:28 carpeta cuál es la carpeta qué permiso
02:31 tiene ese usuario, por ejemplo, yo veo
02:33 que aquí en el permiso para
02:36 administradores es full control que
02:38 permite el full control y nosotros aquí
02:40 vamos a tener entonces una lista
02:42 detallada de todos los permisos vemos
02:44 que aquí me va armando por las carpetas
02:47 o subcarpetas y eso los va armando allí
02:50 directamente vemos aquí todos los
02:51 permisos que aplican para la carpeta que
02:53 se llama hola y vemos que tiene todos
02:55 los usuarios administradores se notan
02:57 Gómez existen criaturas aun en el tema
03:01 de usuarios y todos nuestros permisos en
03:04 el permiso entonces aquí nosotros vamos
03:05 a poder mostrar este tema vemos que aquí
03:08 nos muestra que el permiso que tiene
03:09 este usuario o los usuarios en este caso
03:12 en mi dominio solamente es lectura y
03:15 ejecución entonces ahí vamos a poder
03:17 mostrar todos los permisos a través de
03:18 POWER SHELL y así con todas las
03:20 subcarpetas que tenga ese directorio
03:23 vemos aquí nos muestra otra subcarpeta
03:24 que tiene que se llama ISO aquí vemos
03:27 otra subcarpeta dentro de la subcarpeta
03:28 ISO que tiene y todos estos permisos que
03:32 se llama Boot
03:33 vemos entonces cuáles son los permisos
03:35 que tiene toda nuestra carpeta entonces
03:36 aquí ya vamos podemos llevarlo a un
03:38 Excel y lo vamos a poder filtrar vamos a
03:41 poder darle filtros a toda esta
03:43 información y poder buscar cuál es el
03:45 usuario
03:46 en concreto cuáles son los usuarios en
03:47 concreto que quieres mostrar o que

03:49 quieres ver los permisos que tienen
03:51 actualmente esto es muy importante para
03:53 la auditoría de nuestros sistemas saber
03:55 qué permisos tienen nuestros usuarios y
03:57 que son sean permisos que verdaderamente
03:59 necesiten y que no estemos ofreciendo no
04:02 estamos dando información a usuarios que
04:05 no la necesitan ya saben que como
04:07 verdaderos profesionales de TI y que te
04:09 enseña a JPAITPro siempre en buenas
04:11 prácticas es tener todo bien controlado
04:13 y todo bien
04:15 seguridad o bien es seguro nuestra
04:17 información

Fuente: https://youtu.be/NdjudWS4zF4

COMPETENCIA - VERIFICA EL FUNCIONAMIENTO DE LA RED
CONTENIDOS:

A. Elaborando un cronograma de auditoría de acuerdo a los accesos

ESTRATEGIA	PRODUCTO
4. Conoce las etapas de la auditoria de red en el cronograma (Anexo 21), identifica la encuesta y el cuestionario en la auditoria y realiza un nuevo cronograma considerando las actividades propuestas, dando los tiempos indicados y las semanas que se llevara a cabo la auditoria.	**4- Cronograma de actividades**

A N E X O - 21
EXPORTAR PERMISOS NTFS DE CARPETAS

PROGRAMA DE AUDITORÍA INFORMÁTICA DE REDES

PROGRAMA DE AUDITORÍA INFORMÁTICA DE REDES EN LA EMPRESA LPA1			
CODIGO: PAR 001		HOJA Nº 1/1	
EMPRESA: LPA1			
FASE	**ACTIVIDAD**	**HORAS ESTIMADAS**	**RESPONSABLES**
I	ETAPA PRELIMINAR: • Contacto inicial con el cliente • Entrevista con el personal de T.I. • Solicitud de información sobre los factores a auditar en la red. • Definición del Alcance, Objetivos Generales y Específicos de la Auditoria. • Elaboración de Matriz de Análisis. • Diseño de Instrumentos y técnicas de auditoría.	02 Hrs. 02 Hrs. 02 Hrs. 02 Hrs. 04 Hrs. 02 Hrs.	Auditores Senior / Semi Senior
II	DESARROLLO DE LA AUDITORÍA: • Elaboración y Aplicación de Cuestionarios al personal T.I. y Administrador de la Red. • Observación directa de los factores considerados en la auditoria. • Aplicación de técnicas y Recopilación de información. • Análisis de la información.	10 Hrs. 12 Hrs. 16 Hrs. 24 Hrs.	Auditores Junior
III	REVISIÓN Y ELABORACIÓN DEL PRE-INFORME: • Elaboración del Pre-Informe con hallazgos, observaciones y recomendaciones. • Revisión y discusión de los resultados del Pre-Informe. • Corrección de los resultados, observaciones, recomendaciones y conclusiones.	24 Hrs. 04 Hrs. 04 Hrs.	Auditores Semi- Senior
IV	INFORME FINAL: • Elaboración del Informe de Auditoria • Presentación del Informe	10 Hrs. 02 Hrs.	Auditor Senior

CRONOGRAMA DE ACTIVIDADES

AUDITORIA INFORMÁTICA DE REDES DE LA EMPRESA LPA1											
ACTIVIDADES	HORAS	SEMANAS									
		1	2	3	4	5	6	7	8	9	10
Contacto inicial con el cliente	02	X									
Entrevista con el personal de T.I. y Administrador de Redes	02	X									
Solicitud de información sobre los factores a auditar.	02	X									
Definición del Alcance, Objetivos Generales y Específicos de la Auditoria.	02	X									
Elaboración de Matriz de Análisis	04	X									
Diseño de Instrumentos y técnicas de auditoría.	02	X									
Elaboración y aplicación de entrevistas y Cuestionarios al personal T.I. y Administrador de la Red.	08		X								
Observación directa y pruebas sobre los factores considerados en la auditoría.	02		X								
Aplicación de técnicas, Recopilación de información y Análisis de la información.	10		X								
Elaboración del Pre-Informe con los hallazgos encontrados, observaciones y recomendaciones.	10		X								
Revisión y discusión de los resultados del Pre-Informe.	12		X								
Corrección de los resultados de los Hallazgos, observaciones, recomendaciones y conclusiones.	16			X							
Elaboración del Informe de Auditoria	24			X							
Presentación del Informe	24			X							

MATRIZ DE AUDITORIA INFORMÁTICA DE REDES

ALCANCE DE LA AUDITORIA: Auditoria Informática de Redes para evaluar el desempeño de la plataforma de la empresa LPA1, entre los meses de Noviembre y Diciembre del año 2012.

OBJETIVO GENERAL: Realizar Auditoria Informática de Redes para evaluar el desempeño de la plataforma de la empresa LPA1.

MATRIZ DE ANÁLISIS DE AUDITORIA INFORMÁTICA DE REDES				Código: MR-0001
				Página: 1/ 1
OBJETIVOS		DIMENSIÓN	INDICADORES	INSTRUMENTOS
GENERALES	ESPECÍFICOS			
Realizar Auditoria Informática de Redes para evaluar el desempeño de la plataforma de la empresa LPA1	Evaluar el Desempeño de la Red	Tráfico	Cantidad de Nodos	Observación directa; Herramientas Lógicas; Analizadores de Red;
			Volumen de Información	
		Velocidad	Ancho de Banda	
			Tasa de Transferencia	
			Pérdida de paquetes	
		Conectividad	Topología de Red	
			Dispositivos de Comunicaciones	
	Analizar la información recolectada durante el proceso de auditoría	Análisis de la Información	Informe Preliminar	
	Presentar informe con la conclusión de la auditoria y las Recomendaciones	Presentación de Informe	Informe Final	

PROCEDIMIENTOS DE AUDITORIA

PROCEDIMIENTOS DE LA AUDITORIA				PROC-0001			Página: 1/1
Empresa:	LPA1						
Unidad:	Tecnología de la Información						
Área:	DESEMPEÑO DE LA RED						
Período	Desde:	30	11	2012	Hasta:	15	12	2012
Dimensión: Organizacional							

N°	PROCEDIMIENTOS	REF. P/T
1	Aplicar la observación directa para evaluar los componentes y dispositivos de red.	RD-0001
2	Aplicar instrumentos para evaluar el rendimiento y desempeño de la red.	RD-0001
3	Utilizar monitores de red, herramientas propietarias y utilitarios del sistema operativo para validar el rendimiento y comportamiento de la red.	AI-0001
4	Presentar resultados y observaciones.	ISO 27033-1:2009
5	Ofrecer conclusiones y recomendaciones basadas en los resultados obtenidos.	ISO 27033-1:2009

LISTA DE CHEQUEO

LISTA DE CHEQUEO				LC-0001			Página: 1/1
Empresa:	LPA1						
Unidad:	Tecnología de la Información						
Área:	DESEMPEÑO DE LA RED						
Período	Desde:	30	11	2012	Hasta:	15	12	2012

N°	CARACTERÍSTICA A EVALUAR	SI	NO
1	¿Se comprobaron los elementos y dispositivos físicos de la plataforma de red?	X	
2	¿La cantidad de equipos o nodos está acorde con el diseño y configuración de red?	X	
3	¿Existe alguna aplicación diente-servidor en particular que demande recursos y comprometa el desempeño de red?		X
4	¿Se verificó el ancho de banda de la Red?	X	
5	¿Se analizó la tasa de transferencia en la red?	X	
6	¿Se comprobó la existencia de pérdidas de paquetes en la red?	X	
7	¿Se verificó que la topología estuviese acorde al diseño y requerimientos propios de la red?	X	

INSTRUMENTOS DE LA AUDITORIA

		Código:	EAR-0001
Tipo de Documento:	Guía de Evaluación	Página:	1 / 2
Auditor:	Semi Senior / Junior	Fecha :	10/12/2012
Empresa:	LPA1		

Ref.	Actividad	Procedimiento	Herramientas	Observación
A1	Evaluar si los componentes de Red utilizados son de calidad y garantizan un buen rendimiento	Evaluar los equipos y dispositivos de comunicación utilizados Verificar la correcta instalación de los dispositivos de comunicación	- Observación Directa	Luego de la observación y evaluación de los componentes, se determinó que los componentes utilizados facilitan un excelente desempeño de la red.
A2	Verificar la cantidad de Nodos incluidos en la Red	Determinar si la cantidad de equipos está acorde con la estructura y diseño de la red	- Observación directa	La revisión realizada nos permite inferir que la cantidad de estaciones o nodos incluidos en la red, no exceden ni interfieren en el rendimiento de la red, por lo que la misma se encuentra suficientemente dimensionadas.
A3	Identificar el flujo o cantidad de información que viaja por la red.	Evaluar si el flujo o cantidad de información manejada en las estaciones de trabajo pudiese interferir en el normal desenvolvimiento y desempeño de la red.	- Revisión de aplicativos cliente- servidor instalados y demás recursos de software.	Luego de la evaluación, se determinó que no existen herramientas o sistemas cliente-servidor que demanden una gran cantidad de ancho de banda, por lo que no se afecta el rendimiento ni el desempeño de la red.

		Código:	EAR-0001
Tipo de Documento:	Guía de Evaluación	Página:	2 / 2
Auditor:	Semi Senior / Junior	Fecha :	10/12/2012
Empresa:	LPA1		

Ref.	Actividad	Procedimiento	Herramientas	Observación
A4	Verificar el Ancho de Banda de la Red	Verificar a través de herramientas o aplicativos, que el ancho de banda efectivo de la red se encuentre alineado con el teórico	- Herramientas para el análisis y monitoreo de redes (NSAuditor y NViewer)	Luego de ejecutar la evaluación a través de las herramientas de análisis, tanto del sistema operativo como propietarias, se determino que la red trabaja en su ancho de banda teórico de 100 mbps, alineado con los que son los componentes de red utilizados.
A5	Analizar la tasa de transferencia de la Red	Determinar si la tasa de transferencia es la adecuada como para mantener el desempeño de la red, utilizando herramientas de monitoreo y análisis	- Herramientas para el análisis y monitoreo de redes (NSAuditor y NViewer; PING; Tracert)	Por medio de los resultados obtenidos, inferimos que la tasa de transferencia tiene un comportamiento normal no se encontraron evidencias que aseveren algún problema
A6	Determinar si existe algún indicio de pérdida de paquetes que genere retardo y errores en la red.	Ejecutar herramientas de análisis y monitoreo para determinar si existen o no pérdida de paquetes.	- Herramientas para el análisis y monitoreo de redes (NSAuditor y NViewer; PING; Tracert)	No se detectó ninguna anomalía en lo que respecta a la pérdida de paquetes
A7	Comprobar que la topología de red sea la apropiada y se encuentre alineada con el diseño originalmente aprobado.	Cotejar a través de la observación directa el tipo de topología y que la misma sea la aprobada en el diseño original documentado por la empresa.	- Observación directa. - Revisión de plano de red, documentos y diseños.	La topología utilizada es "Estrella". Las estaciones de trabajo están conectadas a un punto central o switch de alto rendimiento tal y como fue indicado en la documentación y el diseño.

		Código:	EAR- 0001
Tipo de Documento:	Encuesta	Página:	1 / 1
Auditor:	Semi Senior / Junior	Fecha :	10/12/2012
Empresa:	LPA1		

Preguntas	(B)ueno / (R)egular / (M)alo
¿Considera que la velocidad para mover/consultar archivos en la red es?	B
¿La velocidad de descarga de información, videos, imágenes, etc. de la red es?	B
¿Cómo considera la velocidad de la conexión?	B
¿La velocidad para enviar/recibir correos es?	B
¿Cómo evalúa la disponibilidad de la red?	B
¿La disponibilidad de los dispositivos o recursos compartidos es?	B
¿El acceso a internet habitualmente es?	B

		Código:	CAR-0001
Tipo de Documento:	Cuestionario	Página:	1 / 1
Auditor:	Semi Senior / Junior	Fecha :	10/12/2012
Empresa:	LPA1		

Preguntas	Si (S) - No (N) - No Observa(N/O)
¿Se observan problemas de pérdida de información?	N
¿Existen intermitencias en la red?	N
¿Ha observado problemas de conexión con equipos u otros dispositivos de red?	N
¿La impresión en red mantiene una velocidad apropiada?	S
¿Considera que los usuarios que concurren a los servicios de la red afectan el rendimiento?	N/O
¿Las aplicaciones o sistema ERP se encuentra siempre disponible?	S
¿Ha observado algún tipo de error al almacenar o registrar su información?	N

Fuente: https://es.slideshare.net/g_quero/auditora-informtica-de-redes

B. Realizando un plan de monitoreo

ESTRATEGIA	PRODUCTO
5. Lee el texto "Monitorización" (Anexo 22), crea una "nube de palabras" (Anexo 23) a partir de las palabras claves que más le resulten interesantes y complementa la actividad realizando un Cuadro sinóptico de las herramientas de monitoreo de red.	**5- A. Nube de palabas B. Cuadro sinóptico**

A N E X O - 22
MONITORIZACION DE LA RED

¿Qué es?
Por definición, la monitorización es la acción y efecto de monitorizar, que, según el Diccionario de la Lengua Española en su vigésima segunda edición, significa observar, mediante aparatos especiales, el curso de uno o varios parámetros fisiológicos o de otra naturaleza, para detectar posibles anomalías.

Por lo que, la monitorización de red, es la acción que nos permite verificar sistemáticamente el desempeño y la disponibilidad de los dispositivos críticos dentro de la red, a través de la identificación y detección de posibles problemas.

Tipos de monitorización
Existen varias formas de monitorización. Las dos más comunes son la monitorización pasiva y la activa.

Ambas tienen ventajas y desventajas.

Monitorización pasiva
La monitorización pasiva solo está al tanto de lo que pasa sin modificar ningún parámetro u objeto. Usa dispositivos para ver el tráfico que está circulando a través de la red, estos dispositivos pueden ser sniffers o en su defecto sistemas incluidos en los switches y ruteadores. Ejemplos de estos sistemas son la monitorización remota (RMON) y el protocolo simple de administración de red. Una de las características de la monitorización pasiva es que no incrementa el tráfico en la red para poder realizar las lecturas. Se puede capturar el tráfico teniendo un puerto espejo (mirror) en un dispositivo de red o un dispositivo intermedio que esté capturando el tráfico.

Monitorización activa
La monitorización activa tiene la capacidad de inyectar paquetes de prueba dentro de la red o enviar paquetes a servidores con determinadas aplicaciones, siguiéndolos para medir los tiempos de respuesta. Por lo tanto, genera tráfico extra lo suficiente para recabar datos precisos. Este tipo de monitorización permite el control explícito en la generación de paquetes para realizar las mediciones, como el control en la naturaleza de generar tráfico, las técnicas de muestreo, frecuencia, tamaño de los paquetes entre otras.

Alarmas
Una alarma es un aviso o señal de cualquier tipo, que advierte de la proximidad de un peligro. Son consideradas como eventos fuera de lo común y por lo tanto, necesitan atención inmediata para mitigar la posible falla detectada. Las alarmas son activadas cuando un parámetro ha alcanzado cierto nivel o se tiene un comportamiento fuera de lo normal.

¿Qué es lo que se debe monitorizar?
Existen personas que se refieren a la "salud de la red" cuando hablan del rendimiento de la red y su capacidad para dar servicio. Existen funciones críticas dentro de los dispositivos de red que necesitan ser monitorizados constantemente y las alarmas que se lleguen a presentar deben ser atendidas tan pronto como sea posible cuando un evento ocurra.

Algunos de los parámetros más comunes son la utilización de ancho de banda, el consumo de CPU, consumo de memoria, el estado físico de las conexiones, el tipo de tráfico que manejan los ruteadores, switches, hubs, firewalls y los servicios de web, correo, base de datos entre otros. También se debe estar pendientes de las bitácoras de conexión al sistema y configuración de los sistemas, ya que aquí se presenta información valiosa cuando un evento sucede.

Estos parámetros deben de ser monitorizados muy de cerca para detectar posibles cambios y tendencias que afecten al usuario final.

Herramientas de monitoreo

1. **Zabbix**
   a. “Este sistema viene con una interfaz web que nos permitirá ver la monitorización, representación de los datos, configuraciones de monitores, alertas y la administración de los usuarios.”(Zabbix, 2016).Zabbix es un sistema completo para la monitorización de cualquier dispositivo que se encuentre conectado en nuestra red. Zabbix tiene entre sus funciones el obtener datos desde sus monitores que ya vienen predefinidos o la creación de alguno que cumpla con nuestras necesidades. Realiza la monitorización usando SNMP en sus dos formas polling o trapping. Para la monitorización en servidores se hace uso de agentes instalados previamente.
   b. Este sistema viene con una interfaz web que nos permitirá ver la monitorización, representación de los datos, configuraciones de monitores, alertas y la administración de los usuarios. Zabbix permite definir la gravedad de una incidencia y en base a esta configuración se tomará acciones. Se puede definir plantillas sobre las cuales se determinará el monitor y el disparador de alerta correspondiente.
   c. Zabbix nos provee plantillas genéricas para servidores Linux, web, correo, switch, etc. Zabbix almacena los valores que se obtuvieron de las monitorizaciones en una base de datos MySQL y a partir de estas elabora las gráficas
2. **SolarWinds**
   a. “SolarWinds Network Configuration Manager proporciona administración de configuración accesible y fácil de usar que se usa en forma independiente o se integra perfectamente con SolarWinds NPM.”(SolarWinds, 2010).Es una herramienta que permite la administración de archivos de la configuración de nuestra red por medio de una interfaz web.
   b. SolarWinds nos permite acceder a la configuración de los dispositivos y da alertas sobre cualquier cambio que se efectué. No es necesario un inicio de sesión por telnet o SSH con el dispositivo para cambiar algún parámetro de configuración.
   c. Todo esto lo hace en tiempo real y da notificaciones de forma instantánea, dando como resultado una visibilidad instantánea y la mejora de seguridad en la red.
3. **Cacti**
   a. “Una herramienta para monitorizar, archivar y presentar estadísticas de redes y servidores” (Center, 2012).
   b. Esta herramienta está basada en RRDTool dando cierto énfasis en la interfaz gráfica. También toda información del monitoreo se guarda en una base de datos MySql y su interfaz está basada en el lenguaje de programación PHP.
   c. Entre las funciones de monitoreo que tiene esta el medir la carga de un CPU y su capacidad. Emite alarmas basándose en umbrales. Organiza la información en estructuras jerárquicas. Usa SNMP para capturar datos o también por medio de scripts. Permite la creación de plantillas para reutilizar las definiciones de gráficos
4. **Nagios**
   a. “Es muy usada por los administradores de sistemas y red para comprobar la conectividad entre los hosts y garantizar que los servicios de la red están funcionando como se esperaba” (Barth, 2008). Nagios es una herramienta orientada a la supervisión de los recursos de la red, enviando notificaciones por vía correo electrónico, mensajes de texto, pop-ups, etc. Una de sus principales funciones es el observar y verificar los comportamientos de los servicios de la red tales como http, SQL, SSH, Etc o al del host como router, switch, impresoras entre otros.
   b. Entre sus funciones esta: •Monitoreo de recursos de red. •Monitoreo de los servicios de la red. •Capacidad para identificación de nodos padres o hijos para detección de problemas. •Log de eventos. •Administración vía web para supervisar los estados de los servicios.
   c. “Nagios Core proporciona un marco de seguimiento riguroso y configurable para realizar controles de una manera consistente y para alertar a las personas apropiadas y sistemas de cualquier problema que detecte.”(Barth, 2008).Al ser un software open source nagios da muchas facilidades para realizar configuraciones según la necesidad del administrador permitiéndole modificar las alertas o desde que vía desea recibirlas.
   d. Nagios al monitorear recursos de red da el alcance de tener vigilado los recursos de sistemas de hardware como el uso de discos, la memoria, los puertos USB y sus estados independientes del sistema operativo.

A N E X O - 23
NUBE DE PALABRAS

CÓMO CREAR EN SEGUNDOS NUBES DE PALABRAS DESDE TU NAVEGADOR

No es fácil presentar bien una información o un conjunto de datos. Pero hay recursos originales como las nubes de palabras o de etiquetas, que permiten mostrar ideas y conceptos en forma de mosaico.

Las nubes de palabras, nubes de etiquetas o mosaicos de palabras (en inglés *tag cloud* o *word cloud*) son un recurso que sirve para **presentar una serie de palabras o etiquetas** de forma gráfica con distintos **colores y tamaños** en función de la relevancia de una palabra.
A nivel visual, las nubes de palabras son muy efectivas, porque llaman mucho la atención. A nivel práctico, son un método diferente para representar palabras o conceptos a modo de resumen de un texto **destacando las palabras más repetidas**.

Las nubes de palabras **empezaron a usarse en la web** como índice de contenido. De un vistazo ves de qué temas se habla en un sitio web y según el tamaño de cada palabra sabes **qué tema es el que más se trata** o el menos habitual.

Pero el diseño y el análisis de datos lo han adoptado para representar información. Por ejemplo, para mostrar países destacando los más poblados con mayor tamaño, resumir un texto a partir de las palabras más repetidas, comparar dos textos a partir de sus palabras clave…

En una presentación, por ejemplo, puedes usar las nubes de palabras como **índice de los temas** que vas a tratar o **a modo de resumen** de cada apartado que trates.

Hay muchas maneras de **generar nubes de palabras**. A continuación, vamos a repasar algunos generadores online para que uses **desde tu navegador web** sin demasiadas complicaciones, ideal para crear nubes de etiquetas en segundos.

WordClouds

WordClouds, o NubeDePalabras en español, puedes diseñar nubes de palabras con las formas que quieras.
El proceso es relativamente simple, si bien cuentas con la ayuda de un asistente que **te guiará paso a paso**. Puedes escribir o pegar un texto o importar un documento Word, PDF o de texto plano TXT.

También tienes la opción de ir por libre y desde **Lista de palabras** escribir palabras sueltas y asignarles un tamaño.
WordClouds también permite **elegir una forma** para la nube, un tema de colores y un **tipo de fuente**.
Cuando acabes, tienes varias opciones: **guardar la nube de palabras** como PNG, JPG, PDF o SVG o compartirla online a través de Facebook, Twitter o Google+.

TagCrowd

Con un diseño más minimalista pero no por ello menos práctico, **TagCrowd** te ofrece varias opciones para introducir un texto: simplemente lo pegas, pegas la URL o subes un archivo de texto plano.
En las **opciones de configuración** debes indicar el idioma del texto, el máximo de palabras a mostrar en la nube, si quieres censurar palabras concretas, etc.

¡Tras pulsar en Visualize! verás el resultado: una nube de palabras de tonos azules donde se destacan las palabras por tamaño. TagCrowd permite guardar la nube de etiquetas en **HTML, versión imprimible o PDF**.

Wordle
A camino entre los dos generadores anteriores tenemos **Wordle**, con un generador sencillo pero que ofrece resultados muy vistosos, como la imagen que inicia este artículo.

En esta ocasión tienes que **pegar un texto** y Wordle se encargará de resaltar las palabras más habituales.

Los resultados son muy vistosos y puedes **ajustarlos desde los menús**: fuente, combinación de colores, eliminar palabras habituales en tu idioma (como preposiciones o artículos), etc.

Al terminar, puedes imprimir la nube de palabras o guardarla en formato PNG.

El único inconveniente de Wordle es que **funciona en Java**, así que necesitarás tener instalada esta tecnología en tu navegador para usarla.

ABCya! Word Clouds
¡Pensado para el público joven, ABCya! **Word Clouds** permite crear nubes de palabras a partir de un texto pegado en el formulario de esta herramienta online.

Una vez generada la nube automáticamente, puedes **definir el límite de palabras**, mezclar de nuevo la combinación de etiquetas, cambiar la forma de la nube, los colores o la fuente de letra.

Aunque tiene un **filtro de palabras** para eliminar preposiciones o artículos, se suelen colar algunos, por lo que tendrás que editar esas palabras desde Menu > Edit.
El último paso será imprimir la nube de palabras o guardarla en formato JPG.

Word Cloud Generator
Si utilizas Google Docs, la herramienta de Google para trabajar con documentos de texto aprovechando Google Drive, puedes generar nubes de palabras en tu navegador Chrome gracias a este complemento, **Word Cloud Generator**.

Al abrir un documento cualquiera desde Google Docs, en el lateral derecho se creará una nube de palabras que puedes personalizar y, luego, descargar a tu ordenador. Además, cuenta con un espacio donde colocar **palabras que quieres obviar**.

Fuente: https://blogthinkbig.com/como-crear-en-segundos-nubes-de-palabras-desde-tu-navegador

C. Elaborando un formato de control

ESTRATEGIA	PRODUCTO
6. Lee al documento "Bitácoras para las Medidas de seguridad" (Anexo 24), para conocer los elementos de cómo se elabora una bitácora para accesos u operación cotidiana y también la bitácora para el control de los sistemas, en base a este último debe diseñar un formato de control de eventos de sistemas de red.	**6- Formato control de eventos de sistemas de red**

A N E X O - 24
BITACORAS PARA LAS MEDIDAS DE SEGURIDAD
(SOPORTE FÍSICO Y SOPORTE ELECTRÓNICOS)

BITÁCORAS PARA ACCESOS Y OPERACIÓN COTIDIANA

Los datos que se registran en las bitácoras:

A. Quién accede a los datos personales, fecha y hora en la que se realiza el acceso o se intenta el mismo, propósito del acceso, así como fecha y hora de salida;
B. Para soportes físicos: Número o clave del expediente utilizado, y
C. Para soportes electrónicos: Operaciones o acciones llevadas a cabo y registros utilizados de la base de datos.
D. Si las bitácoras están en soporte físico o en soporte electrónico
E. Lugar dónde almacena las bitácoras y por cuánto tiempo;
F. La manera en que asegura la integridad de las bitácoras, y
G. Respecto del análisis de las bitácoras:
    - Quién es el responsable de analizarlas (si es el sujeto obligado o si es un tercero) y cada cuándo las analiza, y
    - Para el caso de que las bitácoras estén en soporte electrónico: las herramientas de análisis utilizadas.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes físicos:

El responsable del sistema procura un estricto control y registro de:

1. Las autorizaciones emitidas para facultar el acceso a un servidor público a fin de que éste, en el ejercicio de sus funciones, pueda interactuar con uno o más de los sistemas a su cargo.
2. La asignación, actualización y reemplazo de las llaves que entrega a los autorizados para que éstos puedan abrir el mecanismo de apertura de la puerta en la zona de acceso restringido.
3. Las acciones que los autorizados llevan a cabo en el área de resguardo. Para ello, designa a un Encargado quien anota lo siguiente: Quién solicita el acceso, cuándo se lleva a cabo (fecha y hora de entrada y salida), la razón que lo motiva y número del expediente utilizado.
4. El préstamo de expedientes es asistido por un sistema de cómputo que utiliza códigos de barras en los gafetes del personal autorizado y en los expedientes.
5. El sistema de préstamo de expedientes genera una bitácora electrónica que se respalda diariamente en un servidor dentro del centro de cómputo que administra el área de informática. Su integridad se garantiza copiando dicha bitácora en un CD-R diariamente.
6. El Encargado del sistema es la persona designada para analizar la bitácora cada mes mediante una herramienta adquirida para tal fin.

Ejemplo de medidas de seguridad aplicables a bitácoras para sistemas en soportes electrónicos:

1. El responsable del sistema -en coordinación con las áreas de informática y seguridad de la información- lleva un estricto control y registro de:

a. Las bitácoras de eventos ocurridos a nivel sistema operativo en los equipos (servidores, cortafuegos, almacenamiento masivo) que habilitan la operación del sistema de datos personales. Entre otras, se generan bitácoras para desempeño del servidor: intentos de acceso (exitosos y fallidos); accesos denegados a usuarios y terminales; uso de herramientas para administración del servidor, y fecha y hora de los eventos anteriores.
b. Las bitácoras de eventos generados a nivel software aplicativo del sistema de datos personales. Entre otras, se generan bitácoras para mensajes de error; apertura, modificación y cierre de archivos; violaciones de seguridad detectadas por el software aplicativo, y fecha y hora de estos eventos.
c. Las bitácoras de eventos relativos a las actividades de usuarios (capturistas, Encargados, el propio responsable y el administrador del servidor) en su interacción con el sistema de datos personales. Entre otras, se generan bitácoras para: Archivos, servicios y recursos utilizados; intentos de acceso (exitosos y fallidos); comandos y operaciones iniciadas, y fecha y hora de dichos eventos.
d. Los conjuntos de bitácoras permiten registrar, entre otros, los siguientes datos: Quién accede a los datos personales, desde dónde y con qué; accesos (intentos exitosos y fallidos) y salidas; propósito del acceso (sólo para modificaciones en el software aplicativo); operaciones llevadas a cabo; datos personales (registros y campos) utilizados de la base de datos, y fecha y hora de estos eventos.
e. Las bitácoras arriba mencionadas están todas en soportes electrónicos y se almacenan al menos por dos años en CD-R. Se tiene una copia en el centro de datos y otra se lleva a una bóveda bancaria subcontratada también para los respaldos.

2. La integridad de las bitácoras se garantiza copiándolas en un servidor del centro de datos el cual las graba en CD-R. Algunas se copian cada hora, otras a diario. La integridad de las copias se garantiza además con ―resúmenes‖ creados por un algoritmo ―digestor‖. Se cuenta con una herramienta de software que automatiza estas operaciones.
3. Las áreas de informática y seguridad de la información han designado una persona que se encarga de realizar un análisis de las bitácoras generadas. Las siguientes características aplican al caso:
   a) Se cuenta con la ayuda de una herramienta informática adquirida para tal propósito.
   b) Cada semana se llevan a cabo análisis de bitácoras, pero no de todas ellas.

   Depende de la bitácora y de las amenazas detectadas en el entorno.
4. Se pueden realizar análisis focalizados a mayor profundidad en caso de presentarse un incidente que así lo requiera.

CONTROL DE LAS BITÁCORAS DE LOS SISTEMAS

Hoy en día, los sistemas de cómputo se encuentran expuestos a distintas amenazas, por lo cual las vulnerabilidades de los sistemas aumentan, al mismo tiempo que se hacen más complejos, el número de ataques también aumenta, por lo anterior las organizaciones deben reconocer la importancia y utilidad de la información contenida en las bitácoras de los sistemas de cómputo, así como mostrar algunas herramientas que ayuden a automatizar el proceso de análisis de las mismas.

El crecimiento de Internet enfatiza esta problemática, los sistemas de cómputo generan una gran cantidad de información, conocidas como bitácoras o archivos logs, que pueden ser de gran ayuda ante un incidente de seguridad, así como para el auditor.

Una bitácora puede registrar mucha información acerca de eventos relacionados con el sistema que la genera los cuales pueden ser:

- Fecha y hora.
- Direcciones IP origen y destino.
- Dirección IP que genera la bitácora.
- Usuarios.
- Errores.

La importancia de las bitácoras es la de recuperar información ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas, evidencia legal, es de gran ayuda en las tareas de cómputo forense.

Las bitácoras contienen información crítica es por ello que deben ser analizadas, ya que están teniendo mucha relevancia, como evidencia en aspectos legales.

El uso de herramientas automatizadas es de mucha utilidad para el análisis de bitácoras, es importante registrar todas las bitácoras necesarias de todos los sistemas de cómputo para mantener un control de las mismas.

D. Cumpliendo con las políticas de la organización

ESTRATEGIA	PRODUCTO
7. Realiza la lectura al documento "Políticas de seguridad" (Anexo 25), para enriquecer sus conocimientos debe realizar un mapa mental.	**7- Mapa mental**

A N E X O - 25
POLITICAS DE SEGURIDAD LA ORGANIZACION

Existen políticas de usuarios y de máquinas. Las primeras restringen las acciones de los usuarios una vez que ingresan en la red.
Al aplicar políticas de máquinas, tenemos la opción de estandarizar las propiedades de las PCs de escritorio y los servidores para que tengan una configuración general única.

Políticas Corporativas:

Existen políticas para configurar cualquier aspecto del uso de una máquina o servidor. Encontraremos muchos sitios en Internet con recomendaciones y detalles sobre cada configuración.
Debemos tener en cuenta que, si bien hay muchas políticas, las más utilizadas son, por ejemplo, establecer normas de longitud y detalles en la creación de contraseñas, deshabilitar o habilitar ciertos servicios que funcionan en el sistema operativo, iniciar una aplicación en forma automática luego de que el usuario acceda al sistema o instalar un parche de Windows o algún software.

Políticas avanzadas para Windows Server 2008 a 2019:

Nombraremos los más destacados en cuanto a políticas de seguridad.
Antes, con Windows Server 2003, los scripts de las políticas de inicio de sistema utilizaban el lenguaje vbscript, y no podía emplearse Power Shell. Afortunadamente, ahora sí podemos usarlo, lo que nos otorga mayor flexibilidad y varias configuraciones que antes no podíamos aplicar.
Otro cambio importante es que tenemos la opción de restringir los diseños de las contraseñas para distintos tipos de usuarios. El diseño es la estructura que definimos para que una clave exista.
Con Windows Server 2008 podemos tener distintos tipos de usuarios y configurar restricciones acordes a cada uno.

Acceso al centro de cómputos:

Si dejamos de lado la protección contra un incendio o brindamos total libertad en el acceso al centro de cómputos, estaremos en problemas tarde o temprano. A continuación, haremos una descripción de los puntos importantes para tener en cuenta con respecto a la seguridad física.

Seguridad física en el centro de cómputo:

Puede tener distintos tamaños según la cantidad de equipos que albergue. No sólo tiene equipos servidores, sino que también cuenta con varios elementos que se deben proteger. Tiene un piso técnico (piso flotante por debajo del cual se pasan los cables), racks, armarios, un equipo de control de temperatura, otro para control de energía y uno para controlar incendios.

Es preciso controlar el indicador de temperatura, ya que un equipo puede generar demasiado calor, más del soportable, y hasta alguno puede quemarse. Los racks son capaces de albergar servidores y switches, consolas para conectarse a los equipos y pacheras. Deben estar bien ventilados, refrigerados y ordenados para que todo funcione correctamente.

Debemos protegerlos, entonces, contra intrusos, desastres naturales, incendios, sabotajes, y otros factores. Necesitamos ser cuidadosos con el acceso de intrusos, porque puede haber un sabotaje a los servidores y, también, ataques mucho más graves.

Es necesario considerar acciones, como:

- Al iniciar el día, imprimimos un formulario y vamos hasta el centro de cómputos. Anotamos todo el control en él.
- Verificamos en primer lugar que no haya luces rojas en los servidores. Si las hay, abrimos el panel de luces y buscamos información que indique la causa.
- Comprobamos ahora que no haya luces naranjas en los servidores. Si las hay, buscamos otra vez las causas y completamos el formulario.
- Nos dirigimos al panel de control de electricidad y en él verificamos en forma cuidadosa que no haya ningún indicador encendido.

Plan de contingencia:

Básicamente, el plan de contingencias nos dice qué hacer en caso de que ocurra una situación no deseada. Tiene que contener todas las tareas que debemos realizar para que el centro de cómputos vuelva a su estado original y operativo. El plan contempla posibles incendios, catástrofes, cortes de luz, sabotajes, etc.

El plan de contingencias viene a decirnos los pasos que debemos seguir para que el cambio sea satisfactorio. Nos indica qué palanca mover, hacia dónde y el tiempo que tenemos para hacerlo. El plan de contingencias, generalmente, se extiende del plan general de la empresa. Indica las salidas de emergencia, la ubicación de los manuales de emergencia, los procedimientos por seguir, los responsables y los teléfonos a donde llamar. Podríamos hacerlo teniendo en cuenta los siguientes puntos:

- Pensar en los posibles desastres que pueden ocurrir e identificar los riesgos que la empresa afrontaría en caso de que sucediera alguno. Luego, evaluar las pérdidas económicas, y realizar estadísticas y gráficos.
- Aplicar los conocimientos sobre los sistemas de la empresa, y jerarquizar las aplicaciones en críticas y no críticas.
- Establecer los requerimientos de recuperación. Tomar nota de todo lo necesario y los pasos por seguir con cada sistema. Luego, generar documentación clara.

Normas de Seguridad:

Normas ISSO 9001 y 27001

Las normas ISO 9001 y 27001 son estándares elaborados por la Organización Internacional para la Estandarización, una federación internacional de los institutos de normalización de 157 países; organización no gubernamental con sede en Ginebra (Suiza).

La norma ISO9001 especifica los requerimientos para un buen sistema de gestión de la calidad. Actualmente, existe la cuarta versión de la norma, publicada en el año 2008, razón por la cual se la llama, internacionalmente, ISO9001:2008.

Tanto esta norma como las otras pueden servir a la empresa para trabajar mejor o, en muchos casos, como parte de su plan de marketing. Algunas compañías sólo certifican determinados departamentos o productos específicos, y no, la organización en su integridad. Esto las ayuda a tener mejores ventas con una buena campaña publicitaria, sin realizar el gran esfuerzo que implica certificar todos y cada uno de los procedimientos.

La norma ISO9001 nos da una gran ayuda para mantener una guía de calidad en nuestro trabajo. Aplicarla hasta los límites que podamos hacerlo seguramente nos gratificará tarde o temprano.

La norma 27001 gestiona la seguridad. Se basa en un Sistema de Gestión de la Seguridad de Información, también conocido como SGSI. Este sistema, bien implantado en una empresa, nos permitirá hacer un análisis de los requerimientos de la seguridad de nuestro entorno. Con ellos, podremos crear procedimientos de mantenimiento y puesta a punto, y aplicar controles para medir la eficacia de nuestro trabajo. La norma contempla cada uno de estos requisitos y nos ayuda a organizar todos los procedimientos. Todas estas acciones protegerán la empresa frente a amenazas y riesgos que puedan poner en peligro nuestros niveles de competitividad, rentabilidad y conformidad legal para alcanzar los objetivos planteados por la organización.

ITLL y la norma ISO20000:

ITIL proviene del inglés Information Technology Infrastructure Library, biblioteca de infraestructuras de tecnologías de la información. Es un marco de referencia de mejores prácticas para gestionar operaciones y servicios de IT. ITIL no es un estándar; no existe una certificación ITIL, podemos obtenerla certificación de las normas ISO20000 o BS15000 que se basan en ITIL. Cualquier empresa puede implementar ITIL, pero es recomendable para aquellas que tengan más de cinco personas en el departamento de helpdesk. Fue publicado como un conjunto de libros, cada uno dedicado a un área específica dentro de la gestión de IT.

Los libros de la última versión son los siguientes:

1. Mejores prácticas para la provisión de servicio
2. Mejores prácticas para el soporte de servicio
3. Gestión de la infraestructura de IT
4. Gestión de la seguridad
5. Perspectiva de negocio
6. Gestión de aplicaciones
7. Gestión de activos de software
8. Planeando implementar la gestión de servicios
9. Implementación de ITIL a pequeña escala (complementario)

La ISO20000 fue publicada en diciembre del año 2005. Nos permite concentrarnos en una gestión de problemas de tecnología de la información mediante el uso de un planteamiento de servicio de asistencia. También controla la capacidad del sistema, los niveles de gestión necesarios cuando éste cambia, la asignación de presupuestos, y el control y la distribución del software.

Antivirus Corporativos:

Los antivirus corporativos son una evolución de los comunes, usados fuera de una red empresarial. Tienen una configuración centralizada y varios módulos que detallaremos a continuación.

Características de los antivirus corporativos

Sin dudas, la evolución de los antivirus nació con el estudio de los de escritorio. Es por eso que los de servidores son mucho más potentes, tienen más opciones, más configuraciones, y abarcan la seguridad de la empresa como un todo. Además, centralizan información de toda la red y las descargas de actualizaciones, muy importante para unificar la seguridad. Incorporan todo un grupo de elementos, por ejemplo: antivirus, firewall, antispyware, antispam, analizadores de tráfico de red, etc.

Estos antivirus nos aseguran tener una administración centralizada. Habrá un servidor central, que administre los clientes instalados en servidores y máquinas de escritorio. Los clientes, al querer actualizarse, buscarán las actualizaciones adecuadas en el servidor central de la empresa antes de hacerlo en Internet. Los clientes reportarán todos sus detalles al servidor central, tendremos informes de posibles ataques, informes de programas instalados que puedan poner en riesgo el accionar de la compañía y de programas inseguros que deberán ser desinstalados.

Infraestructura del antivirus:

Las soluciones de antivirus corporativos tienen varios servicios que debemos instalar. Es preciso proteger toda la infraestructura: servidores, máquinas de escritorio, accesos y egresos. Los servidores

y las máquinas de escritorio tendrán instalados clientes, que reportarán a un servidor central, el cual será exclusivo de la aplicación de seguridad. Desde allí vamos a administrar y realizar reportes con la información que nos ofrecen los clientes, así como también con las otras aplicaciones de seguridad. Siempre nuestras instalaciones se dividirán en grandes o chicas, dependiendo del tamaño de la organización.

Firewalls Corporativos:

Los firewalls son las puertas de entrada a nuestra empresa, por lo que debemos controlar el acceso de la manera adecuada, como controlamos el ingreso a nuestra casa.

Firewall Físicos y Lógicos

Estos sistemas están diseñados para bloquear el acceso no autorizado por ciertos canales de comunicación en nuestra red. Pueden limitar el tráfico y también cifrarlo, para ocultar datos hasta el destino. Otra función importante es que se los puede utilizar como gateways (puertas de enlace) entre distintas redes.

Los gateways interconectan redes con protocolos y arquitecturas diferentes. Traducen la información utilizada en un protocolo de red al usado en otra. Cada aplicación utiliza determinados protocolos. Por ejemplo, Internet usa el HTTP y los puertos 80 y 8080, las aplicaciones de FTP utilizan el puerto 21, el servicio de correo electrónico que trabaja con el protocolo POP3 usa el puerto 110, etc. Sin la seguridad del firewall, el tráfico sería un caos, y cualquier paquete de información podría llegar a cualquier puerto de nuestro servidor y, así, entrar sin permiso a la red.

ELABORADO POR:

ING. / ME. EDGARDO YOCUPICIO RUIZ

CBTis No. 155, TIJUANA

BAJA CALIFORNIA