A continuación se enlistan 6 actividades para el Recursamiento de la materia Opera una RED LAN

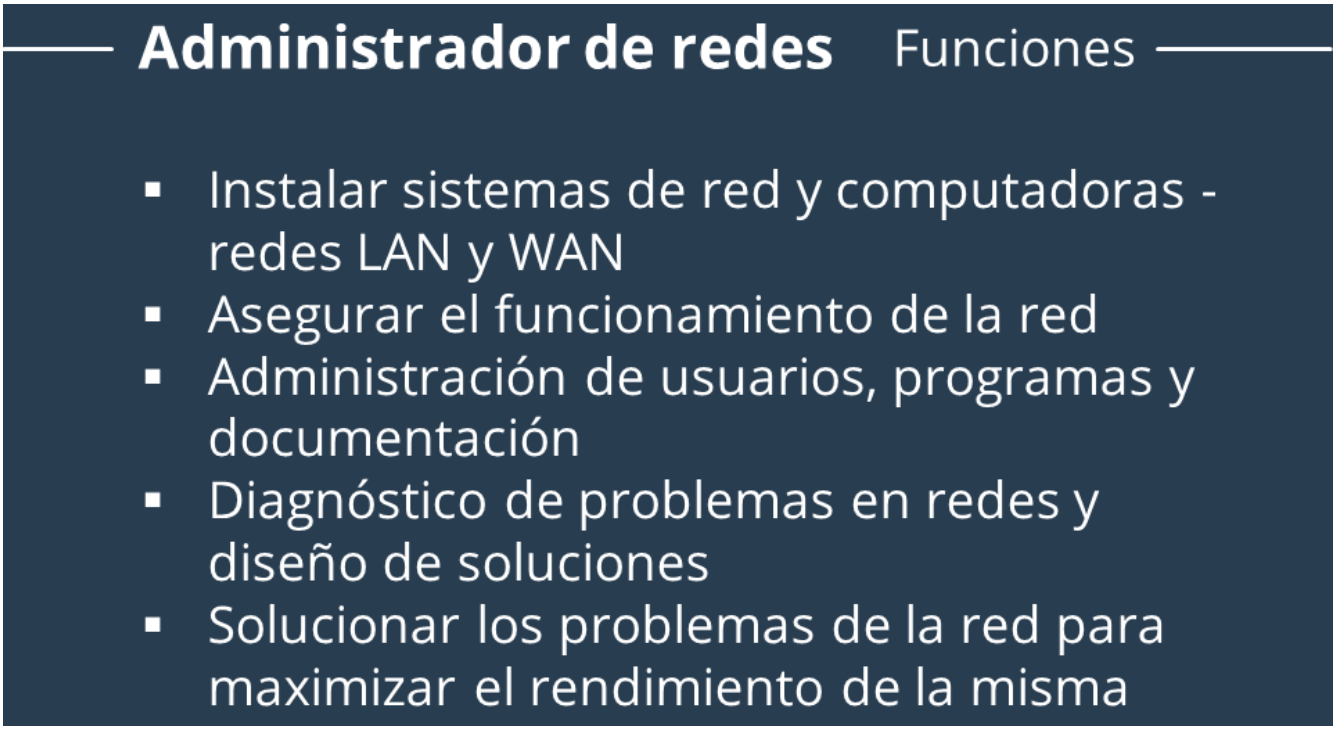
Lee con atención

1. Las actividades se entregan unicamente Vía WhatsApp al numero 56 30 06 57 16
2. NO se recibirán o evaluaran actividades vía correo
3. La fecha de entrega limite es el día 24 de Noviembre
4. No se realizaran clases presenciales unicamente entrega de actividades por el medio antes mencionado

1. El administrador de la RED

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

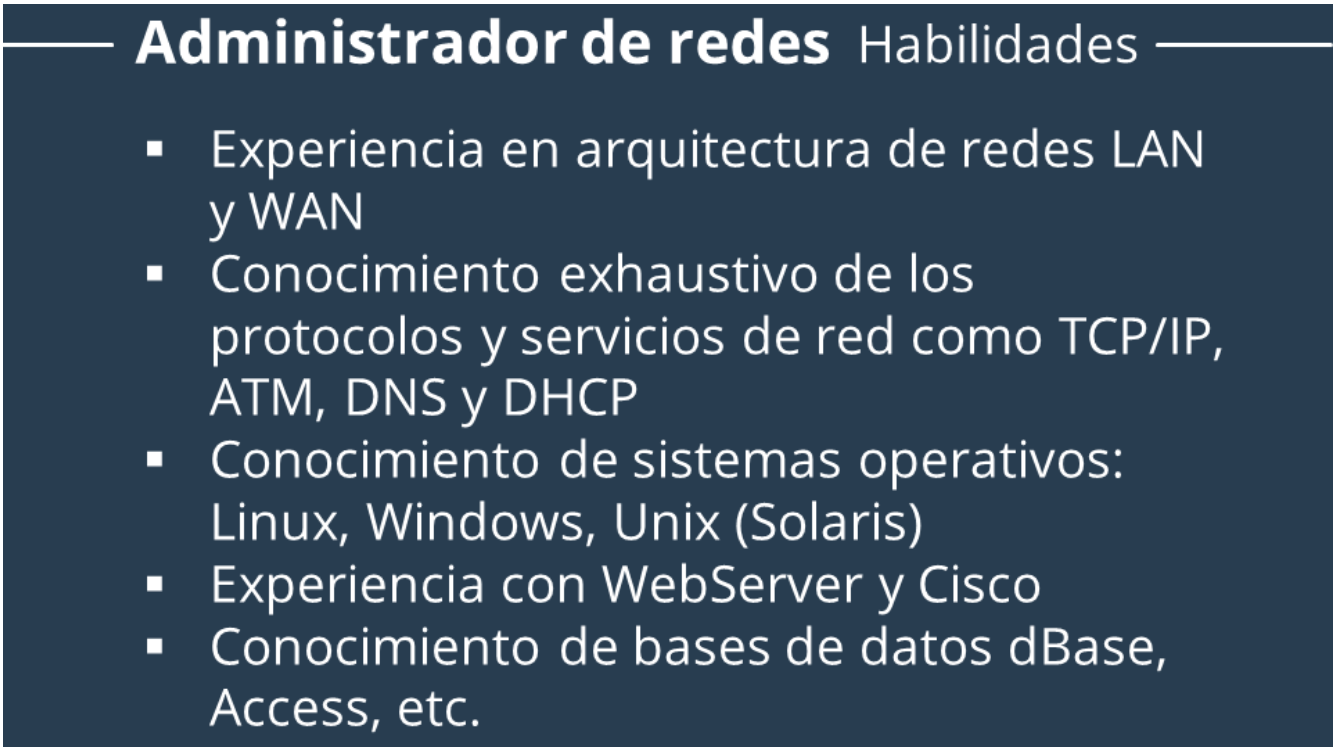


El **administrador de redes** mantiene y el controla las redes de informáticas y cualquier otro entorno informático relacionado con las **configuraciones, programas de hardware y estructuras de software**.
Esto incluye **asignación de protocolos y tablas de ruteo**, configuración y autorización de servicios 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

2. Eleccion de una tarjeta de red

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**

¿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.

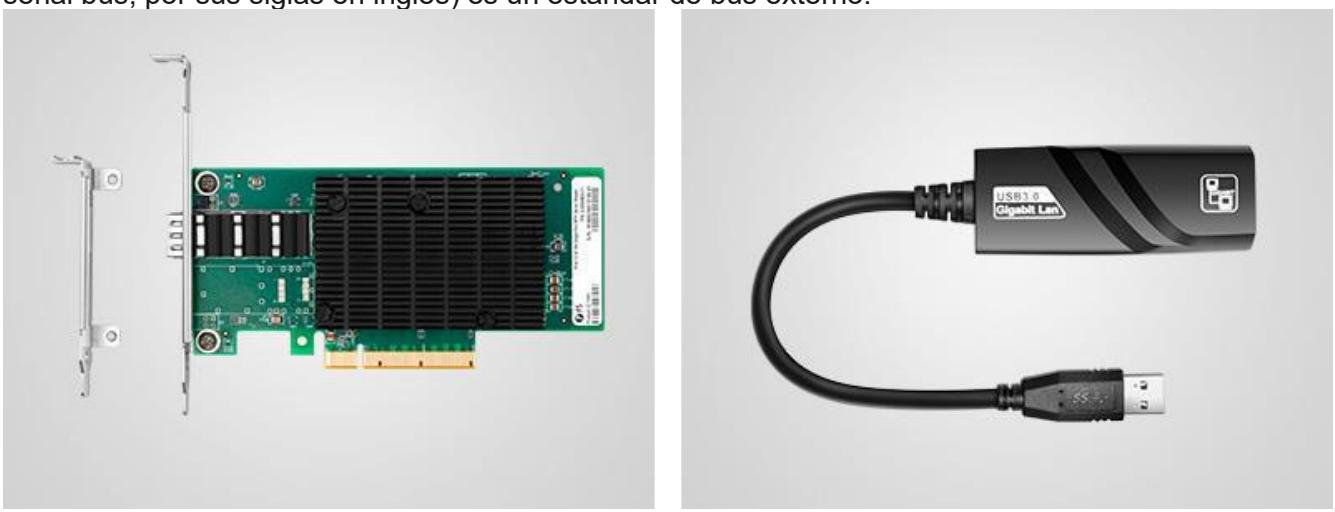


Imagen 1: Tarjeta de red PCIe vs. Adaptador de red USB

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 n**ueva 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

3. Conoce el uso del comando PING

Investiga el comando Ping, realiza un resumen de sus caracteristicas y funcionalidad y desarrolla una tabla comparativa de las pruebas para verificar el funcionamiento, identificar sus parámetros, tales como ttl, ms, etc.. y sus respuestas (destination unrachable, request timeout), para poder identificar los errores en la Red

Incluye el comando completo , la sintaxis del mismo y la pantalla de salida con su explicacion

4. Observa el video del enlace

"Conexión de dispositivos de red y verificación de conectividad", transcribe la información presentada, o elabora un resumen de la transcripción del video señalado (anexo10); Identifica y subraya donde especifique la verificación de la conectividad.
Enlace al video: https://www.youtube.com/watch?v=oS2batpy2mE

5. Lee el documento "Políticas de seguridad" donde se señalan todas las políticas de usuarios, equipo de cómputo, infraestructura, ISO, normas, Etc., las cuales le permiten al estudiante conocer los aspectos relevantes de cada política; Realiza un mapa mental.

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.

6. Sistemas operativos de RED

ESTRATEGIA	PRODUCTO
4. Elabora una tabla comparativa, en donde indiques el sistema operativo, si es un sistema de red multi usuario o si es un sistema Monousuario	**4- Tabla de Servidor(es)**

Sistema Operativo	Multiusuario o Mono usuario