Administración de redes

Estimado colega:

Es un placer darte la bienvenida al curso de Administración de redes. El objetivo de este curso es proporcionar las herramientas necesarias para la administración y manejo eficiente de los recursos de comunicación en una organización. La competencia de este curso consiste en desarrollar soluciones a través del uso de herramientas y estándares para administrar redes.

En el curso, el libro de texto que se utilizará será el del autor Ariganello bajo el título *Redes Cisco: Guía de estudio para la certificación CCNA Security*, el cual contiene los temas del curso sobre el uso de la tecnología actual (en cuanto a telecomunicaciones se refiere) de manera completa, clara y actualizada.

En algunos temas del curso utilizarás software de apoyo, como PuTTY, Nagios y NsClient++, para realizar algunas actividades simulando estar en una situación real y que permitirá a los alumnos entender mejor la parte conceptual de los temas.

Por otro lado, en el transcurso de las explicaciones de los temas, también utilizarás el laboratorio de redes o computación, en donde acompañarás a tus alumnos en la realización de sus actividades y así centrar su aprendizaje en la práctica, para así reforzar todo lo aprendido en la parte conceptual.

En el primer módulo del curso iniciarás con la importancia de tener una administración total de redes, manejando conceptos básicos, uso de los comandos para determinar el estado de la conectividad de la red, manejo y control de accesos, estándar Syslog, empleo de las herramientas de monitoreo, disponibilidad y rendimiento de una red.

En el segundo módulo del curso se empleará el uso de diversas herramientas, como lo son de testeo, seguridad y detección de intrusos, empleo de redes VPN, la importancia de documentar una red y la evolución de las herramientas de redes basadas en ambientes Linux y Windows.

D.R. © Universidad Tecmilenio®

Módulo 1. Administración básica de redes

Introducción al módulo

En este módulo se dará seguimiento a los conceptos fundamentales de redes, ya que se conocerán las conexiones remotas y su procedimiento. Se aprenderá el manejo de los comandos esenciales para conocer la conectividad de un equipo de cómputo para permitir acceso autorizado y, finalmente, detectar con herramientas de monitoreo situaciones extrañas dentro de la red de una organización.

Tema 1. Administración básica de redes

Notas de enseñanza para la modalidad presencial (profesor):

En este tema se sugiere que realices análisis con el grupo sobre los conceptos básicos de redes, como el tipo de redes, protocolos, entre otros, para así explicar lo que es una conexión remota, en qué casos se debe de efectuar este tipo de conexiones, qué protocolos de comunicación se debe de utilizar y la importancia de tener cuidado al efectuar este tipo de conexiones.
Procura que la explicación conceptual del tema sea comprendida a través de un ejemplo que hayas utilizado en la organización para la cual trabajas o que hayas vivido, para que de esta manera puedan entender el significado de una conexión remota.
Es importante que apoyes a los alumnos en la instalación del software PuTTY y con ellos realices una pequeña muestra de cómo funciona y qué información es la que puedo enviar a través de esta herramienta.
A continuación, se te pide revisar el siguiente enlace, el cual te ayudará a realizar una instalación correcta del software:

Los siguientes recursos son materiales de apoyo adicionales al contenido del curso; al entrar a cada sitio deberás considerar los términos y condiciones que rigen al mismo.

Rubio, V. (2016, 12 de noviembre). *SSH y PuTTY en Windows 10 Español* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=DyXqfa80gfw

Como cierre, realiza una reflexión con el grupo acerca de este y otros tipos de herramientas de conexiones remotas que existen en el mercado.

D.R. © Universidad Tecmilenio®

Tema 2. Conectividad de la red

Notas de enseñanza para la modalidad presencial (profesor):

En este tema aportarás tu conocimiento y habilidad en el manejo de los comandos de Windows, prepararás una lista de los comandos más utilizados, explicarás su uso y, de ser posible, realizarás una demostración en el laboratorio de su uso y las diferentes combinaciones de opciones que es posible utilizar en cada uno de ellos.

También puedes apoyarte, para que este tema quede bien entendido, en la exposición de una breve situación sobre su uso y analizar la información que proporciona el comando. Recuerda darle una mayor importancia al comando ping y traceroute. A continuación, se te pide revisar el siguiente enlace sobre el comando ping y traceroute:

Los siguientes recursos son materiales de apoyo adicionales al contenido del curso; al entrar a cada sitio deberás considerar los términos y condiciones que rigen al mismo.

Cisco. (2006). *Comprensión de los comandos ping y traceroute*. Recuperado de http://www.cisco.com/c/es_mx/support/docs/ios-nx-os-software/ios-software-releases-121-mainline/12778-ping-traceroute.html

Como cierre, pregunta a tres alumnos las ventajas y desventajas de utilizar el comando ping y traceroute.

Actividad 1 (temas 1 y 2)

Esta actividad consiste en reunir en equipos de trabajo al grupo. De acuerdo al número de alumnos, son los equipos que se formarán.
También se requiere que se tengan ciertos privilegios por parte del área de informática del campus, por lo que previamente debes exponerle la actividad que se realizará para que te proporcione accesos, sin perjudicar la operación de la red y de los servidores.

Para la parte 1 y 2 se debe realizar lo siguiente:

- Llevar a clase la información solicitada en los requerimientos de la actividad.
- Solicitar al encargado de informática del campus apoyo para establecer una comunicación con un servidor no crítico para realizar la actividad con el software PuTTY, ya que es necesario contar con una dirección IP para su conexión.
- Leer el caso planteado.
- Reunirse en equipo y formar los grupos de acuerdo al número de alumnos.
- Responder las preguntas y recabar la información que se solicita de cada inciso por cada grupo formado.
- Para realizar la infografía, se puede sugerir a los alumnos utilizar Word, PowerPoint o algún software disponible en línea, como es Canva.

D.R. © Universidad Tecmilenio®

Para la parte 2, realizarás lo siguiente:

- De acuerdo a lo respondido en la parte 1, solicitarás a los grupos formados su respuesta y discutir si, además de utilizar PuTTY, es posible realizar los incisos de la parte 1 y 2 utilizando Telnet.
- Apoyarás a los alumnos a utilizar una herramienta o comando para identificar la dirección IP de las computadoras. El comando que puedes emplear es **ipconfig /all**

Para la parte 3, se realizará un cuadro comparativo de las distintas herramientas de acceso remoto, a continuación, se te comparte:

Criterios	TeamViewer	RealVNC	TightVNC	Radmin	LogMeIn
Principales características	Control remoto y realización de reuniones.	Se basa sólo en un cliente que controla el servidor, un servidor que comparte su pantalla y un protocolo de comunicación (RFB, Remote Frame Buffer) que utiliza sencillas órdenes gráficas y mensajes de eventos.	Compatible con implementaciones de servidor y cliente de VNC.	Se considera una herramienta de acceso remoto que ofrece funcionalidades como el mantenimiento de un servidor, asistir de manera remota y trabajar desde cualquier lugar.	Aplicación para acceder a una computadora a través de dispositivos móviles o desde una computadora.
Usos	Administración de servidores y estaciones de trabajo. Conexión a otras plataformas como Mac, Os y Linux. Compartir el escritorio para reuniones de trabajo o trabajo en equipo.	Transferencia de archivos y optimización del sistema operativo.	Visualización y manejo de escritorios remotos. Grabación y monitoreo en video. Multiplataforma.	Comunicación con un usuario mediante el chat de texto multiusuario o por voz. Transferir archivos hacia y desde el equipo remoto. Encendido y apagado de una computadora. Acceso al BIOS.	Se utiliza para ser ejecutado a través de cualquier dispositivo móvil, sin necesidad de hacerlo de una computadora personal a otra. Sino que es posible compartir archivos desde este dispositivo.
Puerto utilizado	80	5900 para su conexión de administración y 5800 para su conexión por medio de un navegador.	5900 para su conexión de administración y 5800 para su conexión por medio de un navegador.	4899	443
Seguridad	Validación del ID, el cual es generado por el mismo software y comprobado para evitar conexiones falsas. Protege de ataques llamados botnets.	No cuenta con mucha seguridad, ya que está limitado a ocho caracteres para una clave.	No cuenta con mucha seguridad, ya que está limitado a ocho caracteres para una clave.	Cuentas de usuario protegidas por contraseñas, así como tener el control de los permisos de cada contraseña. Limitar el acceso remoto a ciertas tareas.	Las contraseñas se codifican mediante algoritmos de longitud variable de 128 bits a 256 bits. La autenticación está sujeta a pocos intentos de inicio de sesión incorrectos, en caso de que así suceda, la cuenta y dirección IP se bloquean.

D.R. © Universidad Tecmilenio®

Limitaciones	No permite conectarse en modo invisible. Generación de un password fijo para la conexión.	No es compatible con texto Unicode, por lo que el texto se debe transferir mediante el uso del juego de caracteres Latin-1.	No es compatible con texto Unicode, por lo que el texto se debe transferir mediante el uso del juego de caracteres Latin-1.	Se requiere licencias por grupo de máquinas y de licencias corporativas.	Se necesitan dos cuentas, una de para la cuenta de LoginMe y otra para la computadora destino. Se requiere de una conexión mínima de 1.5 Mbit/s en cada extremo.
Cifrado	Basado en llaves públicas/privadas RSA y AES (256 bits).	Plugin de código abierto.	Compresión JPEG	256-bit AES	256 bits
Protocolo utilizado	UDP, TCP	TCP	TCP	TCP/IP	SSL/TLS (OpenSSL)

A manera de reflexión, deberás guiar a los equipos de trabajo para escuchar su respuesta de cada uno de los incisos.
Finalmente, se debe realizar un cuadro de doble entrada o comparativo, el cual permita sistematizar la información para organizarla y, a su vez, contrastar varios elementos relacionados al mismo tema. En este caso, la tabla se realizará en función de los dispositivos que en ese momento cuenten los alumnos en el laboratorio y lleven consigo, aplica para cualquier dispositivo.

Tema 3. Control de acceso

Notas de enseñanza para la modalidad presencial (profesor):

El control de acceso es un recurso empleado en redes para validar la autenticación de los usuarios en la red y, así mismo, registrar en una bitácora los movimientos de cada uno de los usuarios para que en caso de que surja alguna incidencia, se conozca de dónde proviene el problema, con la finalidad de garantizar seguridad a la organización.

En este tema se abordarán aspectos regulatorios, como lo es el Marco AAA, TACACS+, RADIUS. La mejor manera de que los alumnos comprendan cómo entran en acción estos marcos regulatorios es exponiendo una situación real de una organización o de tu centro de trabajo en donde se haya implementado cada uno de ellos, por ejemplo, puede ser alguna auditoría en cuanto a procesos y operaciones informáticas.

D.R. © Universidad Tecmilenio®

Para asegurar la comprensión de los alumnos puedes realizar una actividad en la cual, por equipos, realicen un cuadro comparativo de las situaciones en las que se pueden implementar estos marcos regulatorios y en cuáles no es recomendable utilizarlos y por qué. Al final de la actividad realiza una reflexión con la siguiente pregunta detonante:

¿Es posible utilizar los tres marcos regulatorios a la vez?

Tema 4. Estándar Syslog

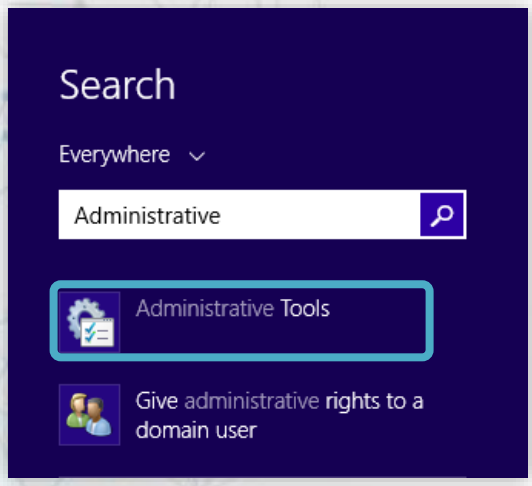
Notas de enseñanza para la modalidad presencial (profesor):

Syslog, como se menciona en la explicación del tema, es un estándar que registra los eventos del sistema. Adicionalmente, el tema menciona los aspectos que permiten a cualquier administrador de sistemas detectar a tiempo cualquier actividad maliciosa en la red, de tal manera que no perjudique las operaciones de la organización y, en caso de que sea detectada alguna, sea posible mitigar cualquier impacto que puede provocar una caída de red e inclusive pérdida de información.

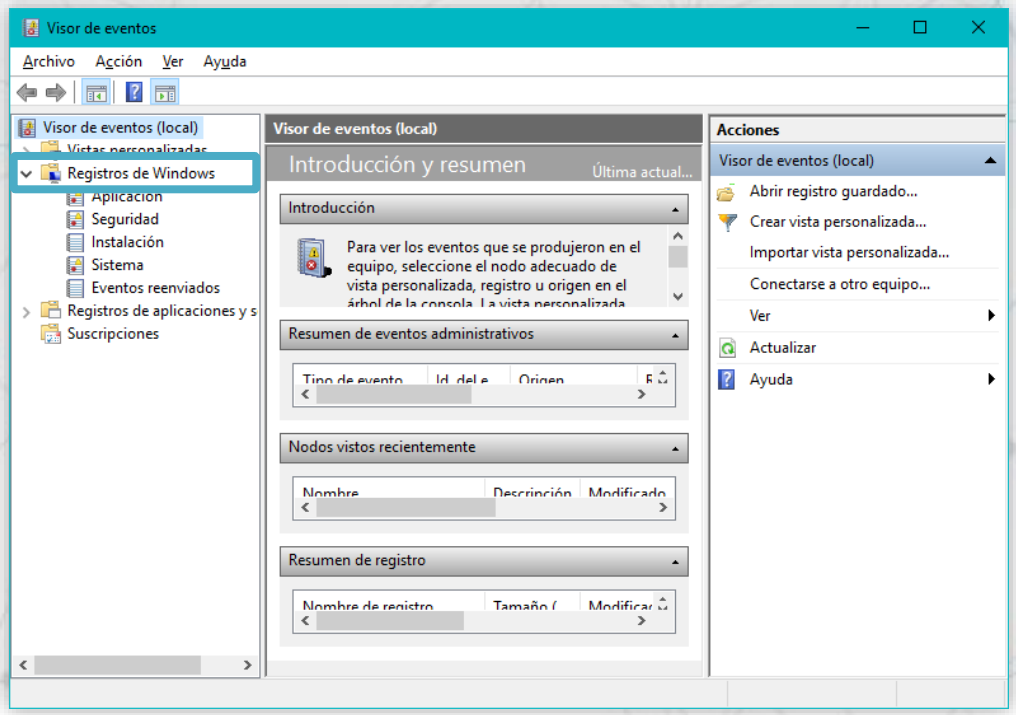
Como ejercicio con el grupo, puedes explicar los errores que aparecen en el entorno Windows cuando una aplicación falla, por ejemplo, el navegador, Office, una aplicación contable, entre otras. Cuando fallan, qué mensaje es el que aparece en pantalla y cómo dentro de los eventos se van registrando cada uno de ellos, para ello accede al **Visor de eventos de Windows** realizando los siguientes pasos:

Paso 1. Teclea Windows, busca **Herramientas administrativas**, posteriormente selecciona el **Visor de eventos** (Event Viewer).

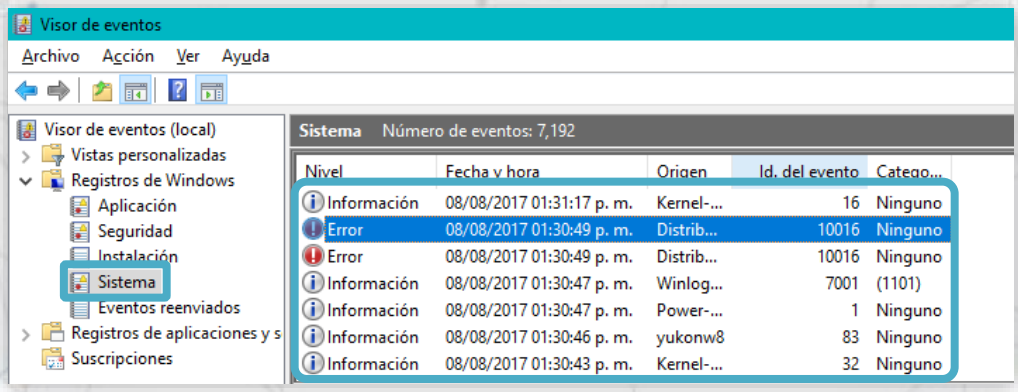
Esta pantalla se obtuvo directamente del software que se está explicando en la computadora, para fines educativos.



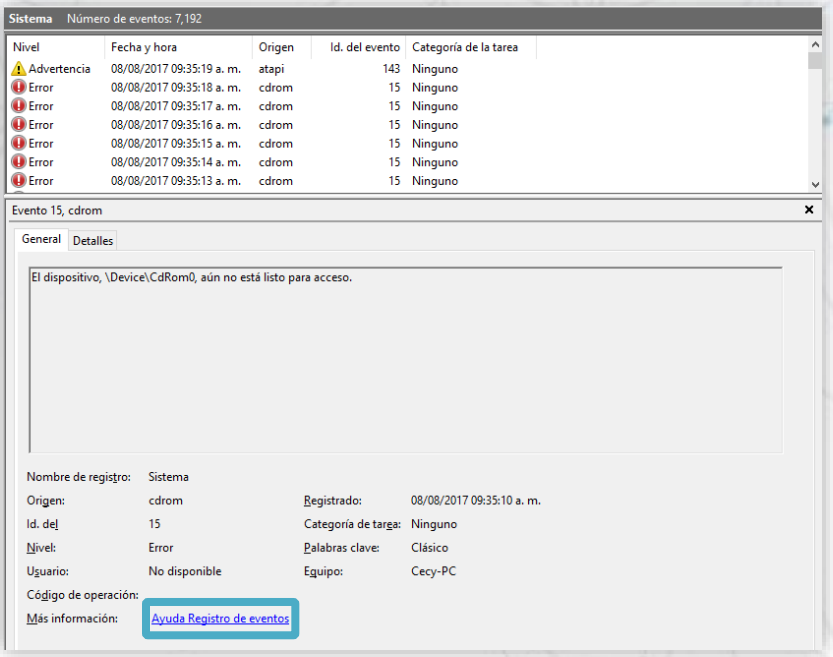
Paso 2. A continuación, haz clic en la carpeta **Registros de Windows** que se encuentra ubicada en el menú del lado izquierdo.



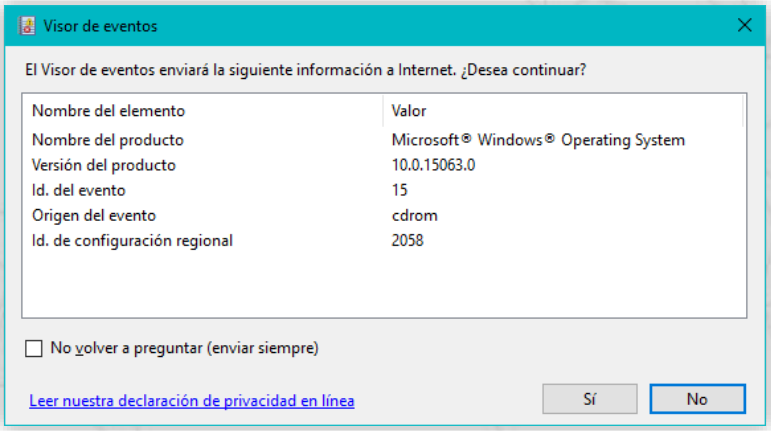
Paso 3. De la lista desplegable selecciona la opción **Sistema**. Observa la lista de eventos y el nivel o tipo de suceso que está presentando a través de los iconos de error, información y advertencia.



Paso 4. Posteriormente, dirígete a la parte inferior de la pantalla y da clic sobre **Ayuda Registro de eventos**.



Paso 5. Después, se despliega en pantalla la ventana **Visor de eventos**, aquí se muestra el dispositivo que está causando algún conflicto, así como información más a detalle.



Como puedes ver, de esta manera puedes identificar aquellos sucesos que están causando conflicto y, a través del visor, corregir el problema que está presentando; en algunos casos esto se debe a posibles actualizaciones que el sistema requiere. Con el **Id. del evento** es posible buscar en la web su origen y solución de la falla presentada.

Realiza este ejercicio con tus alumnos en el laboratorio de computación y, dependiendo de cada computadora, revisen los eventos registrados; finalmente compartan sus resultados.

Tema 5. Monitoreo de disponibilidad de la red

Notas de enseñanza para la modalidad presencial (profesor):

En este tema abordarás aspectos relacionados, como el monitoreo de una red a través de herramientas que permitan detectar algunas intrusiones que están afectando su rendimiento y que puede ser causa de una fuga de información importante para la organización.

La herramienta de monitoreo Nagios permite hacer una monitorización pasiva, ya que permite alertar sobre el comportamiento de cada uno de los equipos y servicios; su uso es libre, por lo mismo lo hace la más utilizada en el mercado. Se sugiere que con el grupo realices la instalación de esta herramienta y ejecutes la aplicación para que, posteriormente, la analicen desde cada computadora asignada a ellos en el laboratorio la información.

Actividad 2 (temas 3, 4 y 5)

Esta actividad consiste en reunir en equipos de trabajo a los alumnos, para dar una respuesta a los incisos del caso planteado.

En la parte 1, se les pide a los equipos de trabajo lo siguiente:

- Listar cuatro elementos para restringir acceso a los responsables de cada servidor existente en cada sucursal:
    - Proporcionar accesos únicos no transferibles.
    - Monitorear, por parte del gerente de sistemas, las operaciones realizadas durante la transferencia.
    - Establecer horario idóneo para las transferencias.
    - Tener un registro o bitácora de accesos.
- Hecho el punto anterior, los equipos de trabajo deberán responder los incisos del punto 3, estas respuestas no pueden ser únicas, ya que se pueden lograr diferentes criterios.
- En el punto 4, los equipos de trabajo deberán establecer sus puntos de vista relacionado a Nagios como herramienta de apoyo para el monitoreo de los equipos de la red.
- En el punto 5, deberás guiar a los equipos de trabajo sobre la información que muestra Nagios cuando se emplea para el propósito de monitoreo.

En la parte 2, se les pide a los equipos de trabajo lo siguiente:

- En el punto 6 y 7 se deberá realizar un documento, en el cual incluyan cómo los marcos regulatorios AAA, TACACS+ y RADIUS pueden ser implementados en el caso planteado. Una vez terminado su documento hay que hacer la dinámica de intercambiar documentos para revisar las conclusiones de los demás equipos para, finalmente, elegir uno y justificar el motivo por el cual es el más completo.

En la parte 3, se les pide a los equipos de trabajo considerar los incisos del punto 8 para realizar una infografía, apoyándose en herramientas como Word, PowerPoint e inclusive una herramienta de uso en internet como es Canva. Las infografías varían dependiendo de la creatividad y sentido de observación de cada uno de los miembros de los equipos.

D.R. © Universidad Tecmilenio®

A continuación, se incluye un modelo de la infografía, cabe mencionar que este diseño va a variar de acuerdo a la creatividad y presentación de la información por parte de los alumnos.

Módulo 2. Documentación de los sistemas de administración de redes

En este módulo se tratarán temas relacionados al monitoreo de redes, qué tipo de herramientas se consideran idóneas para su implementación y detectar algún comportamiento extraño dentro de la red que esté provocando su bajo rendimiento.

También se abordarán los dispositivos que se deben implementar y configurar correctamente como medidas de seguridad, como lo es el firewall, conmutador o ruteador y así evitar la intrusión de accesos no autorizados que están ocasionando este rendimiento de muy bajo nivel o robo de información.

Es importante saber decidir qué opción es la mejor y cómo se puede evitar que un agente extraño realice un monitoreo externo de la red.

Tema 6. Monitoreo del rendimiento de la red

Notas de enseñanza para la modalidad presencial (profesor):

En este tema es importante abordar a los alumnos sobre los aspectos de seguridad que se deben considerar al momento de trabajar en una organización y cómo una mala ejecución o decisión respecto a protocolo de seguridad puede ocasionar daños irreversibles. Por ello, se te sugiere analizar las siguientes preguntas al grupo:

- ¿Es recomendable conectarse a una red pública?
- ¿Cuáles serían las consecuencias de navegar por esta red?

En el cierre del tema considera tomar las tres mejores respuestas del grupo.

Tema 7. Herramientas de rendimiento de red

Notas de enseñanza para la modalidad presencial (profesor):

En este tema abordarás la herramienta Nagios y realizarás una breve explicación de su uso en el entorno Windows y Linux.

Para Windows se utiliza el agente NSClient++, por lo que es necesario que en la explicación del tema revises su instalación paso a paso. Y, para que los alumnos comprendan su uso, realices con ellos un ejemplo sobre el uso de la memoria, carga de la CPU, uso en disco duro, estados de los servicios, entre otros. Windows también posee una herramienta, pero su información es muy generalizada.

D.R. © Universidad Tecmilenio®

Con Nagios NSClient++ es más completa la información de resultados de los servicios monitoreados. Esta actividad de ejemplo la puedes hacer primero tú, como muestra de los resultados obtenidos en el informe y, posteriormente, guiarás al grupo a realizarlo para así analizar los resultados obtenidos.

También puedes realizar este ejercicio con la herramienta de Monitor de recursos, contenida en Windows y comparar si la información resultante es la misma, tanto del Monitor como de NSClient++.

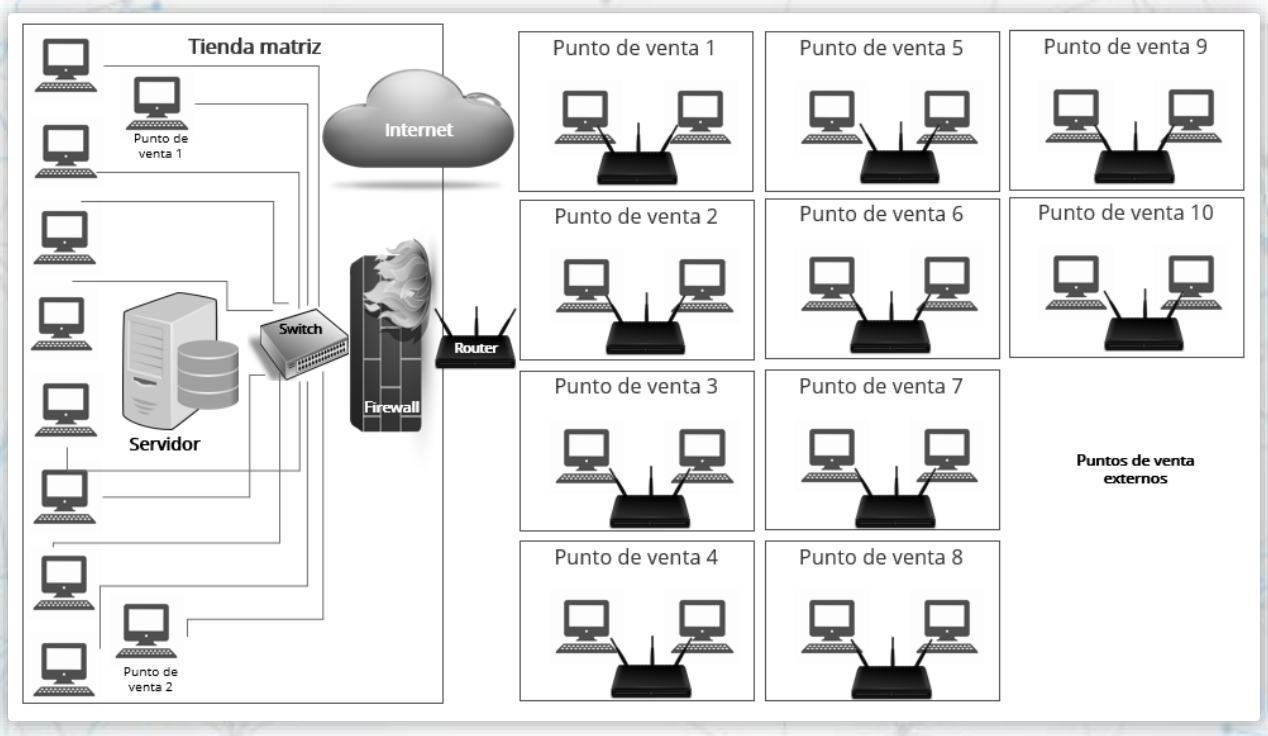
Actividad 3 (temas 6 y 7)

En esta actividad se les pide a los alumnos realizar equipos de trabajo, en donde cada miembro efectúa su aportación al análisis del caso planteado.

En la parte 1, una vez analizado el caso planteado, dan respuesta a los incisos. Es importante considerar que las respuestas pueden diferir, ya que cada equipo de trabajo tendrá su propio análisis y percepción.

Como apoyo en el inciso b de esta parte, además de realizar el ejercicio con la herramienta Nagios para determinar el número de procesos que tiene la computadora, también es posible utilizar el software Advanced IP Scanner.

En la parte 2, hay que apoyarse en alguna herramienta, como PowerPoint, para realizar el diagrama de red que muestre los elementos que se enlistan. A continuación, se comparte el diagrama de red:



Este diagrama puede variar en cuanto a su diseño de los componentes requeridos, ya que dependerá de la comprensión del alumno sobre el caso planteado.
En la parte 3, se realizará un plan de acción, el cual incluya los puntos que se piden en los incisos para determinar cómo es posible evitar tráfico en la red para agilizar los procesos en la zapatería.

Tema 8. Network Security Testing

Notas de enseñanza para la modalidad presencial (profesor):

En este tema se explican las herramientas iniciales y que son fundamentales en una red de comunicación, se considera que se debe explicar al grupo por qué es importante dar mantenimiento a una red, exponerles el escenario de qué pasaría si la red del campus no tuviera este tipo de proceso.

También se debe abordar la importancia y conveniencia de contar con una política de seguridad en cualquier centro de datos, realizar una lluvia de ideas sobre qué considera el alumno que debe contener, como puntos esenciales, una política de seguridad.

Otro aspecto a tratar en este tema es el uso de herramientas para la gestión de redes, las cuales permiten detectar vulnerabilidades. Además de las herramientas mencionadas, propone a los alumnos buscar otras herramientas que tal vez sea posible emplear en un entorno Windows y Linux.

Tema 9. Seguridad en dispositivos de red: enrutadores y conmutadores

Notas de enseñanza para la modalidad presencial (profesor):

En este tema se recomienda dar una breve introducción de la operación y concepto de router y switch, exponerles a los alumnos en qué casos es importante su empleo y para qué propósito. De ser posible, considerar realizar una actividad en donde se detallen tres características de cada uno de ellos, para así mostrar de una forma más sencilla su ventaja de uso y bajo qué circunstancias.

Otro aspecto que te sugiero comentarles a los alumnos, es que hay un comando que permite conocer las tablas de enrutamiento de una red y que este comando se emplea tanto en los entornos de Linux, como de Windows.

Es posible realizar este ejercicio del comando a través de la opción Símbolo de sistema de Windows, el comando para realizarlo es: **netstat-r,** para ello debes asegurarte que los alumnos cuenten con una computadora dentro del laboratorio y comparar si el obtenido es el mismo para cada uno de ellos.

D.R. © Universidad Tecmilenio®

Finalmente, cerrar este tema haciendo la reflexión sobre el firewall y su importancia, mantenerlo activo en la computadora para el monitoreo de cualquier intruso o vulnerabilidad.

Tema 10. Sistemas IDS (Intrusion Detection System)

Notas de enseñanza para la modalidad presencial (profesor):
Este tema plantea la parte conceptual de las amenazas en una red y que, gracias a esto, hace posible la creación de herramientas que, de acuerdo a su función, es la solución que ofrecen.

Los sistemas IDS se consideran una herramienta de seguridad en la que es posible monitorear aquellos eventos ocurridos y su finalidad es buscar intentos por romper la seguridad instalada en ese equipo de cómputo e inclusive en una red.

Se sugiere que, para una amplia comprensión de este tema, se realice un ejercicio sobre el firewall de Windows y observar su comportamiento cuando se activa y desactiva. Para reforzar este tema comparte el siguiente enlace, en el cual se habla sobre el IDS y sus clasificaciones:

Los siguientes recursos son materiales de apoyo adicionales al contenido del curso; al entrar a cada sitio deberás considerar los términos y condiciones que rigen al mismo.

ISO Training Institute. (2017, 23 de enero). *IDS - Intrusion Detection System*. Recuperado de https://www.youtube.com/watch?v=VDYEvyuJtKc

Para cerrar este tema se sugiere que cinco alumnos definan, en una palabra, la idea de IDS.

Actividad 4 (temas 8, 9 y 10)

En la parte 1 se pretende que, de manera individual, el alumno realice lo siguiente:

- De acuerdo a su conocimiento, explique el procedimiento a seguir por parte del administrador de redes para la adquisición de un sistema IDS. Es decir, qué es lo que el administrador debe considerar y tener documentado. También el alumno analizará si conoce alguna herramienta que desempeñe el papel como herramienta de intrusos e identifique si existe alguna diferencia entre IDS y Firewall.
- Se llenará la tabla considerando tres herramientas y tres de firewall. Para ello se recomienda revisar, de forma personal, los siguientes enlaces que tratan sobren las herramientas open source disponibles para la detección de intrusos y que serán de apoyo para este punto:

Los siguientes recursos son materiales de apoyo adicionales al contenido del curso; al entrar a cada sitio deberás considerar los términos y condiciones que rigen al mismo.

Ortego Delgado, D. (2017). *Las 8 mejores herramientas open source de detección de intrusión*. Recuperado de https://openwebinars.net/blog/las-8-mejores-herramientas-open-source-de-deteccion-de-intrusion/

Alejandro. (2017). *Mejores IDS Opensource para detección de Intrusiones*. Recuperado de https://protegermipc.net/2017/02/22/mejores-ids-opensource-deteccion-de-intrusiones/

También se pide revisar el siguiente enlace, que será de apoyo para conocer los sistemas firewall gratuitos:

Los siguientes recursos son materiales de apoyo adicionales al contenido del curso; al entrar a cada sitio deberás considerar los términos y condiciones que rigen al mismo.

Román Hernández, J. (2011). *10 firewalls gratuitos alternativos.* Recuperado de https://www.emezeta.com/articulos/10-firewalls-gratuitos-alternativos

En la parte 2, ya formados en equipo, se expone un caso de una empresa de seguridad, en la cual se pretende realizar lo siguiente para los puntos 6, 7 y 8:

- Para estos puntos se debe realizar la entrega, por parte de los equipos de trabajo, de un reporte sobre la situación analizada, en donde se deben considerar los incisos incluidos en el punto 6.
- Este punto se asemeja a una auditoria, para que finalmente se discuta qué proceso del análisis realizado previamente es el que tiene un alto nivel de riesgo.

En la parte 3, realiza lo siguiente:

- Un reporte que incluya los incisos incluidos como apoyo en este punto para que, finalmente, este reporte sea entregado a la empresa de seguridad industrial y se puedan tomar las medidas necesarias para evitar alguna vulnerabilidad, ataque e inclusive robo de información.

Módulo 3. Documentación de la red

Este módulo se enfoca en conocer sobre el entorno de las redes privadas virtuales, esto significa: en qué casos se utiliza, cómo puedo decidir los tipos de accesos con los que se debe contar, entre otros aspectos.

Por otro lado, la importancia de documentar la instalación, incidencias, mantenimientos, seguridad, diagramas y otros aspectos de la red, conocer las ventajas y desventajas que me permitan, en una situación dada, contar con esta información para dar una solución inmediata sin necesidad de esperar a una persona externa que realice un diagnóstico y análisis de la situación.

Finalmente, daremos paso a los entornos Windows y Linux, esto significa desde sus inicios y cómo han ido mejorando en cuanto a seguridad se refiere, para su uso en las organizaciones; también permitir tomar la decisión de cuál de estos los sistemas operativos es conveniente implementar en la organización y para qué situaciones se recomienda su uso.

Tema 11. Redes privadas virtuales

Notas de enseñanza para la modalidad presencial (profesor):

En este tema se detalla la implementación de una red privada virtual, mejor conocida como VPN; explicarás la manera en que opera este tipo de red y en qué situaciones se recomienda su uso. Para que los alumnos comprendan este tipo de redes se sugiere plantear un ejemplo, en el cual se utilice este tipo de red. Uno de estos ejemplos puede ser la implementación de una red en una empresa, en la cual los empleados tengan acceso a ella para compartir sus aplicaciones dentro de esa misma oficina y alguna sucursal.

Si es posible, puedes agregar a la situación y a manera de análisis, que además de una VPN se pueda implementar una red LAN o MAN. Discutan qué tipo de red es la idónea para este tipo de situación.

Tema 12. Documentación de la red

Notas de enseñanza para la modalidad presencial (profesor):

Este tema explicará a los alumnos lo importante que es contar con una documentación completa de toda la operación de la red, sus procesos, su diseño, su seguridad, mantenimiento, entre otros aspectos. Se detallará a los alumnos en qué tipo de software se pueden apoyar para hacer el diseño, qué tipo de formatos se deben emplear para su documentación y quién será el responsable de mantener en resguardo esta información.

D.R. © Universidad Tecmilenio®

Para ello se sugiere, a manera de ejemplo, que realicen en equipo una documentación sobre la red del campus y presentar un reporte de todo lo encontrado. Para realizar esta actividad se pueden apoyar del encargado de informática para que les proporcione la información que requieren. Al finalizar la actividad, cada equipo debe presentar a sus compañeros su documentación a través de una presentación de PowerPoint.

Finalmente, entre todos decidan cuál presentación de la documentación es la más completa.

Actividad 5 (temas 11 y 12)

Notas de enseñanza para la modalidad presencial (profesor):

En la parte 1 se realizará lo siguiente:

- Para el punto 1 hay que realizar un crucigrama junto con el grupo. Este punto se puede hacer de manera manual o buscar en la web algún sitio de apoyo, donde sea posible realizarlo de manera gratuita. A continuación, se incluye el diseño del crucigrama y su resultado:

Across

4 Documento en el que se incluye el etiquetado, longitud y tipo de cada cable.

5 Documento cuyo propósito es contar con los detalles de instalación y configuración de cada paquete de software.

6 Autenticación. Valida el origen en la VPN IPSec, asegura que el otro extremo de la VPN es quien debe ser.

7 Término en que se basa una infraestructura compartida y con la misma norma que una red privada.

8 Paso siguiente del proceso de instalación de una red, determina lo que se debe recordar en el futuro sobre el trabajo realizado.

10 Documento que se divide en parte blanda y dura.

11 Documento que especifica lo que está y lo que no está permitido hacer por parte de los usuarios.

12 Comunicación sobre una infraestructura que usa conexiones dedicadas y que, una vez autenticadas, tienen un nivel de acceso parecido al de una red local.

Down

1 Conexión segura y bajo costo, son aspectos que González (2014) menciona.

2 Documento en el que se tiene una lista de reparaciones a computadoras y a la red.

3 Ampliación del protocolo IP, establece conexiones seguras en VPN y pertenece a la capa 3.

9 Conjunto de dispositivos interconectados entre sí, a través de un medio para compartir recursos e intercambiar información.

18 Conducto para transmitir datos de un sitio a otro.

13 Infraestructura privada de modo virtual a través de comunicaciones públicas.

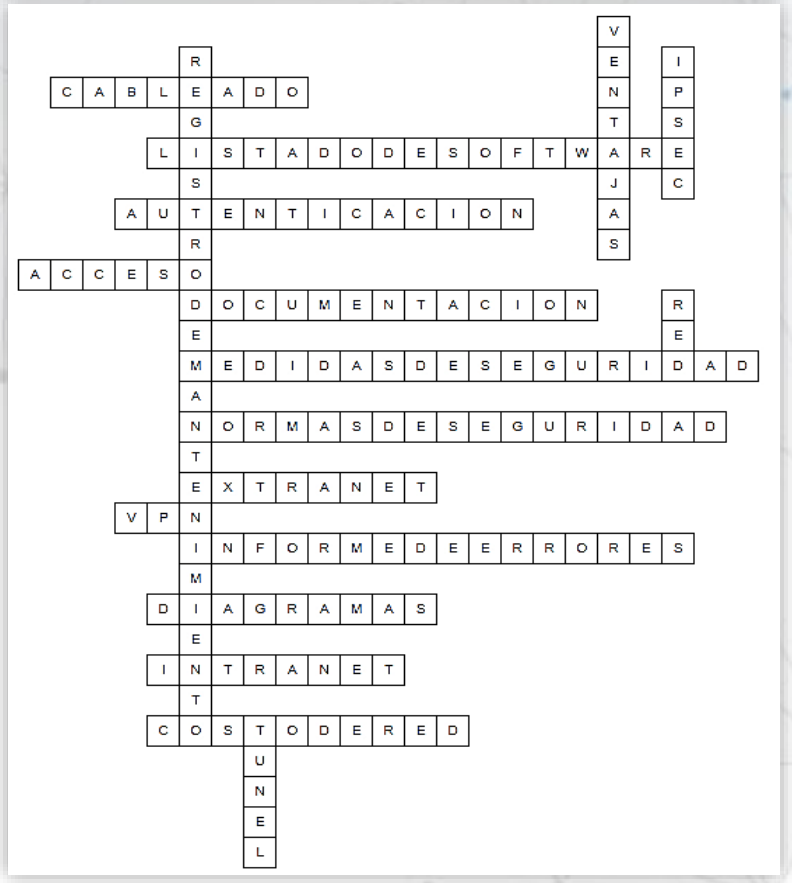
14 Documento que proporciona soluciones a problemas recurrentes que ya han sido resueltos y también apoyan al administrador a justificar el personal contratado o bien, la adquisición de un nuevo equipo de cómputo.

15 Herramienta que se utiliza para representar, de forma gráfica, los dispositivos que se utilizan de forma física y lógica y cómo están conectados entre sí.

16 Comunicación sobre una infraestructura compartida que utiliza conexiones dedicadas.

17 Documento que muestra los factores de crecimiento de la red, formación técnica y de usuario, reparaciones y despliegue de software.

A continuación, se muestra un diseño y el resultado del crucigrama. Es importante considerar que el diseño sufrirá cambios, ya que se pide realizarlos a criterio de los alumnos, sería de apoyo compartirles a los alumnos las preguntas para los términos que se están empleando en este punto.



- Para el punto 2, se realiza un mapa conceptual de tipo nivel 2, por lo que se deben considerar todos los términos repartidos en los incisos. Este diagrama debe mostrar, de una manera clara y breve, cada concepto y las herramientas que se solicitan.

En la parte 2, se debe realizar lo siguiente:

- Para el punto 3, una tabla comparativa con definiciones, ventajas y desventajas de los apartados que debe contener una documentación de redes, es decir, los puntos que son relevantes en cualquier tipo de documentación. Y, finalmente, mostrar la reflexión de dos puntos, en los cuales se explique qué puede suceder si no se tiene esta documentación.
- Para el punto 4, hay que diseñar un formato en el cual se recabe información relacionada con las características del hardware contenido en el servidor y estaciones de trabajo; este proceso debe ser simulando que se está en un área de informática e inclusive los alumnos se pueden apoyar con el personal de informática del campus.
- Para el punto 5, se plantea un caso, en el cual se debe crear una aplicación para agilizar los procesos de la empresa y mantener actualizada la información, de tal manera que la comunicación sea interna y para sus clientes que utilizan el servicio.
  En este punto debes guiar al alumno en la selección del lenguaje de programación para realizar la aplicación, recuérdales considerar conceptos como la navegabilidad, accesibilidad y usabilidad. Aquí los alumnos deberán realizar una especie de prototipo y presentación, donde incluyan los aspectos que se solicitan en los incisos y justificarlo para su aprobación al área de informática. Se pretende implementar una red privada de tipo extranet.

Tema 13. Herramientas: diagramas de redes

Notas de enseñanza para la modalidad presencial (profesor):

En este tema se explicará la importancia de contar, dentro del área de informática o de sistemas, los diagramas de las redes que se encuentran en la organización; este tipo de diagramas ayudan en el caso de que se requiera hacer un cambio, extensión o definitivamente implementar algún dispositivo de comunicación.

Para crear los diagramas de red, se darán a conocer a los alumnos las herramientas que existen en el mercado, además de las que vienen en la explicación de este tema. Se sugiere que se tome una herramienta de la lista que viene en la explicación del tema y se explique cómo se trabaja en ella; para realizar el análisis toma como ejemplo el ejercicio de documentación de la red que se realizó en el tema anterior.

A manera de cierre, pregunta a tres alumnos que te enlisten tres ventajas que se obtienen al contar con el diseño de una red dentro de una organización.

Tema 14. Herramientas basadas en Linux

Notas de enseñanza para la modalidad presencial (profesor):

Este tema aborda todos los aspectos relacionados con el entorno Linux. Es importante considerar una breve explicación desde sus inicios hasta la actualidad, ya que es considerado como uno de los más seguros.

Te recomiendo especificar el motivo por el cual Linux es, hoy en día, un sistema operativo utilizado por la mayoría de las organizaciones, se puede detallar cuáles son sus ventajas y desventajas de uso, qué información es la que se puede almacenar y operar con las distintas herramientas que existen. Se sugiere que compartas el siguiente enlace, el cual habla de la historia de Linux:

Los siguientes recursos son materiales de apoyo adicionales al contenido del curso; al entrar a cada sitio deberás considerar los términos y condiciones que rigen al mismo.

Linux2puntocero. (2013, 10 de noviembre). *Código Linux- Revolution OS Subtitulos en Español Documental* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=9ip3UA_04LM

Te sugiero que una vez terminado el video, se pregunte al grupo lo siguiente:

¿Creen que Linux debe ser el sistema operativo principal en todos los equipos de cómputo que se comercializan? ¿Por qué?

Tema 15. Herramientas basadas en Windows

Notas de enseñanza para la modalidad presencial (profesor):

Este tema se enfoca al nacimiento de Windows y su evolución como un sistema operativo, el cual se considera muy robusto y completo. También se detallan sus versiones, por lo que es importante hacer mención a los alumnos en qué casos se debe emplear una versión y otra. Otro de los puntos es explicar a los alumnos por qué es el más utilizado en la industria, qué ventajas y desventajas proporciona.

Es importante considerar que, a diferencia de Linux, éste no es de distribución libre, ya que hay que pagar un precio por su uso y de acuerdo a la versión adquirida. A manera de ejemplo, se sugiere que en el laboratorio se revise en cada uno de los equipos de cómputo las características con las que cuenta la versión instalada y ver que más se puede hacer con las características presentadas. Te sugiero que compartas el siguiente enlace, el cual habla de la historia de Windows:

Los siguientes recursos son materiales de apoyo adicionales al contenido del curso; al entrar a cada sitio deberás considerar los términos y condiciones que rigen al mismo.

Windows Green. (2015, 30 de julio). *Historia y Evolución de Microsoft Windows. MS-DOS al Windows 10.-2015 HD* [Archivo de video]. Recuperado de https://www.youtube.com/watch?v=xlDxnBwiDbs

Actividad 5 (temas 13, 14 y 15)

Notas de enseñanza para la modalidad presencial (profesor):

En la parte 1, se realizará lo siguiente:

- En el punto 1 y 2, hay que dar una respuesta a las preguntas introductorias de manera individual.
- En el punto 3, se debe analizar el caso planteado, ya reunidos en equipos, se deben realizar los puntos posteriores en los que se pide realizar un diagrama de red con la información y croquis proporcionado y, asimismo, decidir los elementos que hacen falta en el diagrama

de red y la seguridad que se pretende incluir. Estas respuestas varían de acuerdo al análisis efectuado por los equipos de trabajo.

- En el punto 7, se debe realizar un cuadro comparativo sobre las herramientas de diagramas de red, como los son los enlistados en la instrucción; se sugiere emplear este diseño:

	Software				
Criterios	**Dia**	**Edraw Max**	**yEd**	**Gliffy**	**Diagram Designer**
Función					
Características					
Ventajas					
Desventajas					

En la parte 2, en los incisos:

- En el punto 8 y 9 se retoma el caso planteado y, utilizando cualquier herramienta de diseño, por equipos de trabajo se realiza un diagrama de red, en el cual se incluyan elementos indispensables que se utilizan en cualquier conectividad de una red.
- En el punto 10 y 11, los equipos de trabajo deberán incluir y describir tres herramientas para administrar redes en el entorno Windows y tres herramientas para el entorno Linux, todo lo anterior considerando los puntos que se enlistan.
- En el punto 12, hay que realizar un reporte en el cual establezca, en forma de tabla, la lista de comandos descrita, incluyendo su explicación y ejemplo. A continuación, se te comparte esta información:

Comando	Explicación	Ejemplo
sshd	Es un proceso del servidor OpenSSH. Escucha las conexiones entrantes, utilizando el protocolo SSH y actúa como servidor para ese protocolo. Se encarga de autenticar usuarios, cifrado, conexiones de terminal, transferencias de archivos y tunelización.	• service sshd start • /usr/sbin/sshd
ssh-agent	Se utiliza para autenticar la clave pública SSH. Es un programa que realiza un seguimiento de las claves de identidad del usuario y sus frases de acceso. Utiliza las claves para iniciar sesión en otros servidores sin que el usuario escriba su contraseña, esto lo hace al inicio de sesión.	• eval ssh-agent
ssh-add	Se utiliza para agregar claves privadas SSH al agente de autenticación SSH, para implementar el inicio de sesión único con SSH.	• ssh-add
scp	Copia archivos entre computadoras. Utiliza el protocolo SSH y se incluye de manera predeterminada en las distribuciones de Linux y Unix.	• scp file host : path
ssh	Protocolo que permite conectarse de forma segura a un servidor para administrarlo. Garantiza que la conexión se realiza desde los equipos deseados y establece una comunicación cifrada entre el cliente y servidor.	• ssh <equipo>

ssh-keygen	Herramienta para crear nuevos pares de claves de autenticación para SSH. Estos pares de claves se utilizan para automatizar los inicios de sesión, inicio de sesión único y autenticar los hosts.	• ssh-keygen • ssh-keygen -t rsa (para crear los pares de claves)
sendmail	Es un agente MTA (Agente de Transferencia de Correo) para la entrega de los mensajes, ya estén destinados a usuarios del mismo sistema o a usuarios ubicados en destinos remotos. Transfiere de forma segura los correos electrónicos entre los hosts, mediante el protocolo SMTP.	sendemail -f nombrecuenta@gmail.com -t cuentadestino@isp.com -s smtp.gmail.com:587 -u \ "Asunto" -m "Cuerpo del mensaje" -a archivoadjunto -v -xu nombrecuenta -xp clavecuenta -o tls=yes Donde: cuenta@gmail es la cuenta remitente. cuentadestino@gmail.isp.com es la cuenta destino. En “Asunto” va justamente el asunto del correo (si va entre comillas) y en “Cuerpo del mensaje” lo que se quiere escribir (también entre comillas) La opción -a va si se quiere enviar un archivo adjunto. “nombrecuenta” es el nombre de nuestra cuenta de GMail sin el @ “clavecuenta” es nuestra clave de acceso a nuestra cuenta de GMail
man	Muestra las páginas de ayuda (manuales) de los distintos comandos.	• man -k awk (busca la palabra awk entre los distintos manuales de los comandos)
info	Se utiliza para mostrar la documentación de lectura en línea para el comando especificado.	• info -n (especifica los nodos en el primer archivo info visitado) • info -f (especifica el archivo info a visitar)
raw	Se utiliza para enlazar un dispositivo de caracteres raw de Linux a un dispositivo de bloque.	• /dev/raw/raw<N>
exportfs	Permite que los directorios locales estén disponibles para que los clientes NFS puedan montarse. Este comando se invoca durante el inicio del sistema por el archivo /etc/rc.nfsfile y utiliza información en el archivo /etc/exports para exportar uno o más directorios.	• /usr/sbin/exportfs
mount	Permite montar una unidad de almacenamiento y enlazarlo al sistema principal de archivos.	• mount | column -t
ipconfig	Configura la dirección del host o proporciona información sobre la configuración actual.	• ipconfig /all
ping	Sirve para enviar mensajes a una dirección de red concreta que se especifica como argumento, con la finalidad de realizar un test a la red utilizando el protocolo ICMP	• ping <dirección ip>
netstat	Network statics, muestra un listado de las conexiones activas, tanto internas (localhost) como externas, los sockets abiertos y las tablas de enrutamiento.	• netstat-p • netstat-l • netstat-s

- En el punto 14, se describe un caso en el cual se deberá realizar una memoria técnica de acuerdo a la información recabada a través del caso y dando cumplimiento a los puntos que se enlistan. Esta memoria debe contener descripción detallada de lo encontrado y diagramas gráficos, es decir, algo similar a una auditoría.