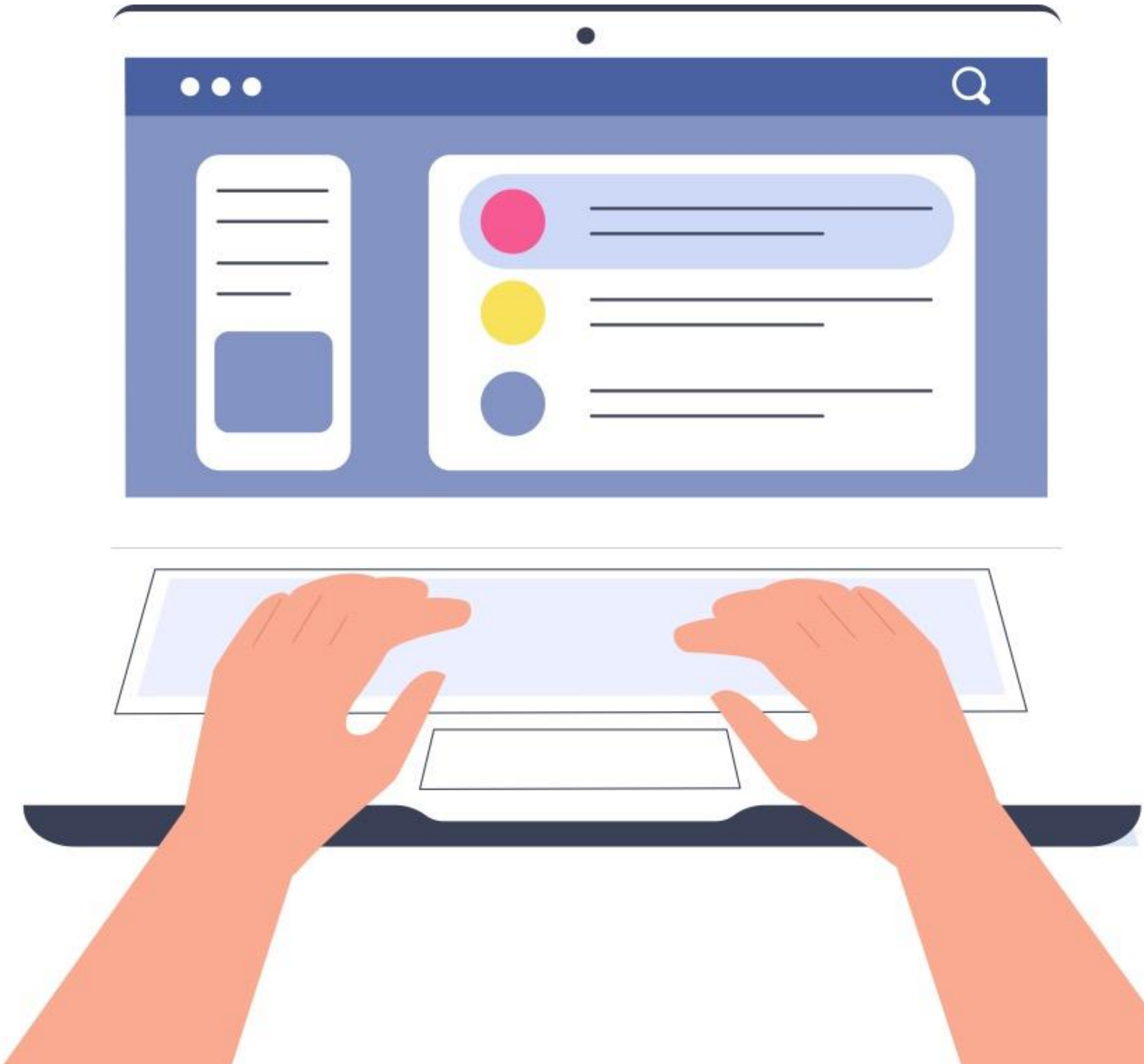


Monitoreo de un sistema de red Simple Network Management Protocol (SNMP)".

Módulo 5: Configuración de la seguridad en redes de área local.

 **Conectividad y Redes**



Objetivos de Aprendizaje de la Especialidad

Módulo 1	<p>OA1 Leer y utilizar técnicamente proyectos de conectividad y redes, considerando planos o diagramas de una red de área local (red LAN), basándose en los modelos TCP/IP y OSI.</p> <p>OA3 Instalar y mantener cableados estructurados, incluyendo fibra óptica, utilizados en la construcción de redes, basándose en las especificaciones técnicas correspondientes.</p> <p>OA7 Instalar y configurar una red inalámbrica según tecnologías y protocolos establecidos.</p>	Módulo 6	<p>OA9 Mantener y actualizar el hardware de los computadores personales y de comunicación, basándose en un cronograma de trabajo, de acuerdo a las especificaciones técnicas del equipo.</p>
Módulo 2	<p>OA2 Instalar y configurar sistemas operativos en computadores personales con el fin de incorporarlos a una red LAN, cumpliendo con los estándares de calidad y seguridad establecidos.</p> <p>OA11 Armar y configurar un equipo personal, basándose en manuales de instalación, utilizando las herramientas apropiadas y respetando las normas de seguridad establecidos.</p>	Módulo 7	<p>OA10 Mantener actualizado el software de productividad y programas utilitarios en un equipo personal, de acuerdo a los requerimientos de los usuarios.</p>
Módulo 3	<p>OA8 Aplicar herramientas de software que permitan obtener servicios de intranet e internet de manera eficiente.</p>	Módulo 8	<p>OA6 Aplicar procedimientos de recuperación de fallas y realizar copias de respaldo de los servidores, manteniendo la integridad de la información.</p>
Módulo 4	<p>OA4 Realizar pruebas de conexión y señales en equipos y redes, optimizando el rendimiento de la red y utilizando instrumentos de medición y certificación de calidad de la señal, considerando las especificaciones técnicas.</p>	Módulo 9	<p>No esta asociado a Objetivos de Aprendizaje de la Especialidad (OAE), sino a Genéricos. No obstante, puede asociarse a un OAE como estrategia didáctica.</p>
Módulo 5	<p>OA5 Aplicar métodos de seguridad informática para mitigar amenazas en una red LAN, aplicando técnicas como filtrado de tráfico, listas de control de acceso u otras.</p>		

Perfil de Egreso – Objetivos de Aprendizaje Genéricos

<p>A- Comunicarse oralmente y por escrito con claridad, utilizando registros de habla y de escritura pertinentes a la situación laboral y a la relación con los interlocutores.</p>	<p>B- Leer y utilizar distintos tipos de textos relacionados con el trabajo, tales como especificaciones técnicas, normativas diversas, legislación laboral, así como noticias y artículos que enriquezcan su experiencia laboral.</p>	<p>C- Realizar las tareas de manera prolija, cumpliendo plazos establecidos y estándares de calidad, y buscando alternativas y soluciones cuando se presentan problemas pertinentes a las funciones desempeñadas.</p>
<p>D- Trabajar eficazmente en equipo, coordinando acciones con otros in situ o a distancia, solicitando y prestando cooperación para el buen cumplimiento de sus tareas habituales o emergentes.</p>	<p>E- Tratar con respeto a subordinados, superiores, colegas, clientes, personas con discapacidades, sin hacer distinciones de género, de clase social, de etnias u otras.</p>	<p>F- Respetar y solicitar respeto de deberes y derechos laborales establecidos, así como de aquellas normas culturales internas de la organización que influyen positivamente en el sentido de pertenencia y en la motivación laboral.</p>
<p>G- Participar en diversas situaciones de aprendizaje, formales e informales, y calificarse para desarrollar mejor su trabajo actual o bien para asumir nuevas tareas o puestos de trabajo, en una perspectiva de formación permanente.</p>	<p>H- Manejar tecnologías de la información y comunicación para obtener y procesar información pertinente al trabajo, así como para comunicar resultados, instrucciones e ideas.</p>	<p>I- Utilizar eficientemente los insumos para los procesos productivos y disponer cuidadosamente los desechos, en una perspectiva de eficiencia energética y cuidado ambiental.</p>
<p>J- Emprender iniciativas útiles en los lugares de trabajo y/o proyectos propios, aplicando principios básicos de gestión financiera y administración para generarles viabilidad.</p>	<p>K- Prevenir situaciones de riesgo y enfermedades ocupacionales, evaluando las condiciones del entorno del trabajo y utilizando los elementos de protección personal según la normativa correspondiente.</p>	<p>L- Tomar decisiones financieras bien informadas, con proyección a mediano y largo plazo, respecto del ahorro, especialmente del ahorro previsional, de los seguros, y de los riesgos y oportunidades del endeudamiento crediticio así como de la inversión.</p>



Marco de Cualificaciones Técnico Profesional (MCTP) Nivel 3 y su relación con los OAG

HABILIDADES

1. Información

1. Analiza y utiliza información de acuerdo a parámetros establecidos para responder a las necesidades propias de sus actividades y funciones.

2. Identifica y analiza información para fundamentar y responder a las necesidades propias de sus actividades.

2. Resolución de problemas

1. Reconoce y previene problemas de acuerdo a parámetros establecidos en contextos conocidos propios de su actividad o función.

2. Detecta las causas que originan problemas en contextos conocidos de acuerdo a parámetros establecidos.

3. Aplica soluciones a problemas de acuerdo a parámetros establecidos en contextos conocidos propios de una función.

3. Uso de recursos

1. Selecciona y utiliza materiales, herramientas y equipamiento para responder a una necesidad propia de una actividad o función especializada en contextos conocidos.

2. Organiza y comprueba la disponibilidad de los materiales, herramientas y equipamiento.

3. Identifica y aplica procedimientos y técnicas específicas de una función de acuerdo a parámetros establecidos.

4. Comunicación

4. Comunica y recibe información relacionada a su actividad o función, a través de medios y soportes adecuados en contextos conocidos.

APLICACIÓN EN CONTEXTO

5. Trabajo con otros

1. Trabaja colaborativamente en actividades y funciones coordinándose con otros en diversos contextos.

6. Autonomía

1. Se desempeña con autonomía en actividades y funciones especializadas en diversos contextos con supervisión directa.

2. Toma decisiones en actividades propias y en aquellas que inciden en el quehacer de otros en contextos conocidos.

3. Evalúa el proceso y el resultado de sus actividades y funciones de acuerdo a parámetros establecidos para mejorar sus prácticas.

4. Busca oportunidades y redes para el desarrollo de sus capacidades

7. Ética y responsabilidad

1. Actúa de acuerdo a las normas y protocolos que guían su desempeño y reconoce el impacto que la calidad de su trabajo tiene sobre el proceso productivo o la entrega de servicios.

2. Responde por cumplimiento de los procedimientos y resultados de sus actividades.

3. Comprende y valora los efectos de sus acciones sobre la salud y la vida, la organización, la sociedad y el medio ambiente.

4. Actúa acorde al marco de sus conocimientos, experiencias y alcance de sus actividades y funciones

CONOCIMIENTO

8. Conocimientos

1. Demuestra conocimientos específicos de su área y de las tendencias de desarrollo para el desempeño de sus actividades y funciones.



Metodología seleccionada

Demostración guiada

- Esta presentación te servirá para avanzar paso a paso en el desarrollo de la actividad propuesta.

Aprendizaje Esperado

- **5.2** Supervisa una red de área local a través de técnicas de análisis y filtrado de tráfico (protocolos), listas de control de acceso, monitoreo de red u otras, respetando la normativa legal vigente.



¿Qué vamos a lograr con esta actividad para llegar al Aprendizaje Esperado (AE)?

- Identificar software de monitoreo de red como herramienta de detección, diagnóstico y solución de problemas en la red.
- Identificar los tipos de alertas y procedimientos correspondientes a los datos obtenidos en monitores de red.



Pregunta o actividad para detectar qué saben del tema, o atraer el interés de estudiantes al tema.

¿Cómo creen que se hace el proceso de monitoreo en las empresas grandes, donde es difícil hacer un monitoreo de forma manual?



¿Por qué monitorear la red?

- La respuesta es muy sencilla, el monitoreo de red nos facilita:
 - a) La administración del equipamiento.
 - b) Mantenerse informado sobre el estado físico de las conexiones.
 - c) Mantenerse informado sobre el consumo de memoria, CPU, entre otras.
- A su vez, el monitoreo permite, en el momento de ocurrir una falla, poder generar alertas y ser mucho más eficiente en los tiempos de respuesta a la hora de un incidente.



¿Qué monitorear en la red?

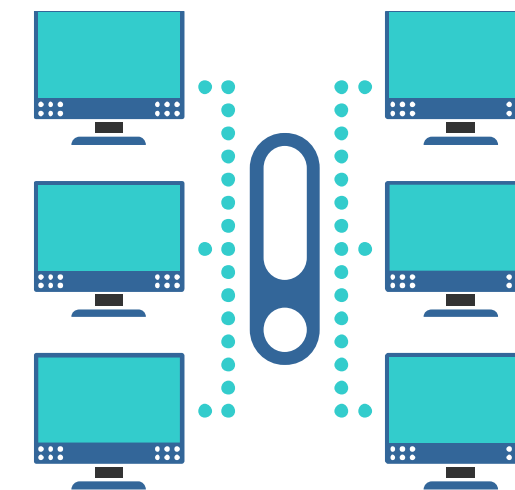
- Los sistemas de monitoreo pueden detectar una serie de parámetros de un dispositivo. **Por ejemplo:**
 - Consumo de CPU.
 - Consumo de memoria.
 - Estado de los servicios.
 - Estado físico de las conexiones.
 - Estado, si está encendido o apagado un dispositivo.



¿Qué monitorear en la red?

01

- Los sistemas en base a la información recopilada por el monitoreo pueden diagnosticar y generar alarmas sobre algún aspecto particular.



¿Existe algún protocolo para el proceso de monitoreo de red?

- 01
- El protocolo (**SNMP, Simple Net Management Protocol**) simple de administración de redes sirve para que los administradores de red puedan administrar dispositivos tales como servidores, estaciones de trabajo, routers, switches y dispositivos de seguridad. Permite que los administradores de redes monitoreen y administren el rendimiento de la red, detecten y resuelvan problemas de red.

- 02
- SNMP es un protocolo de capa de aplicación y trabaja con los puertos 161 y 162 UDP.



¿Qué software detecta, diagnostica y soluciona problemas en la red?

- Cuando hablamos de software para el monitoreo, hay variados tipos. Hay algunos que detectan, diagnostican y generan la alarma, y otros que además de lo indicado anteriormente, pueden solucionar el problema.
- Existen variados software en el mercado. Muchos open source y otro pagados.
- **Por ejemplo:**
 - Nagios.
 - Zabbix.
 - Zenoss.
 - PRTG network monitor.



¿Cuál es el proceso del software para detectar, diagnosticar y solucionar problemas en la red?

- Primero que nada, existe un equipo servidor y todos los equipos clientes que envían la información al server, quien detecta esta información, compara con los parámetros establecidos sobre un aspecto particular, hace un diagnóstico y genera una alerta.

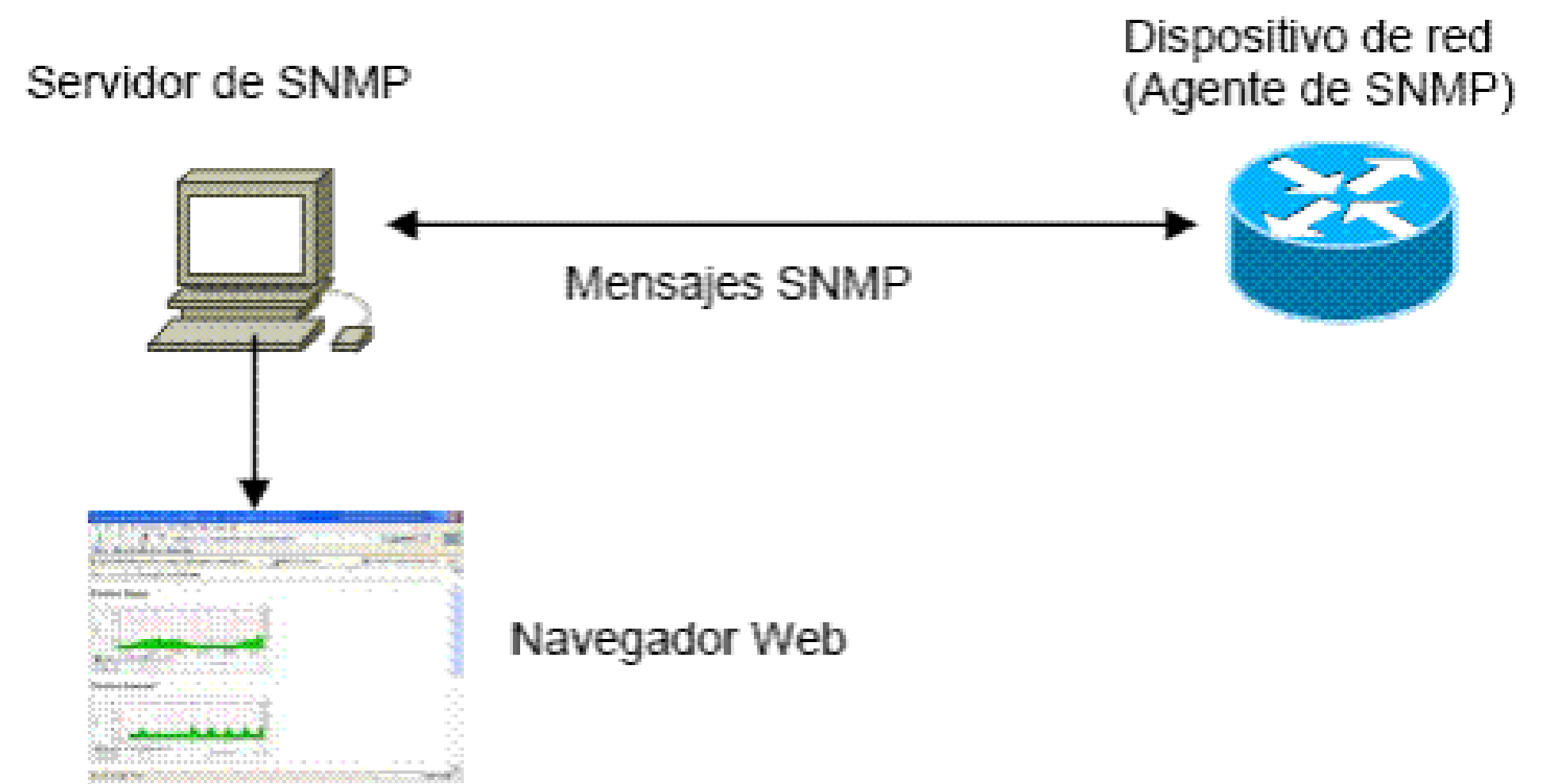
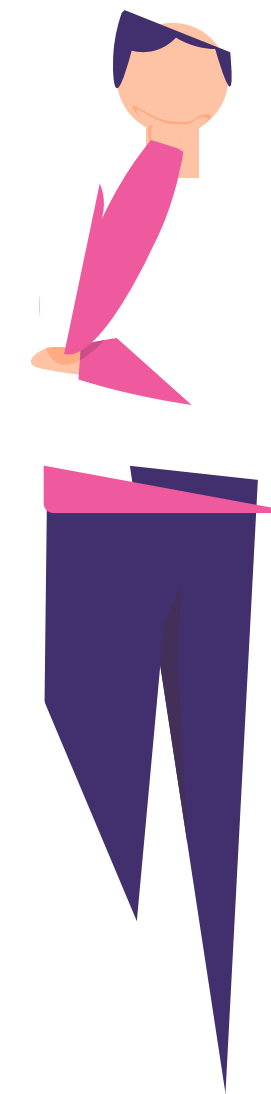


Imagen: <https://www.monografias.com/trabajos95/recursos-red-y-su-monitoreo/recursos-red-y-su-monitoreo.shtml>

Pregunta de reflexión

¿Por qué es tan importante una detección oportuna y el diagnóstico de un incidente en una red?



Tipo de alertas según datos recopilados

- Según los datos recopilados con el software, se pueden establecer diferentes alertas. **Por ejemplo:**

- OK.
- WARNING.
- CRITICAL.



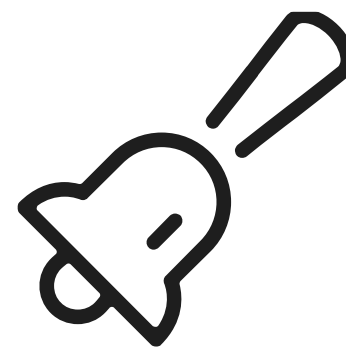
Hosts	Services	Status	Duration	Last Check	Tries	Status information
06-DC-01	CPU	CRITICAL	11m 25s	06/05/2017 00:32:45	3/3 (H)	CPU utilization percentage - 94.5%
	Disco C	OK	21m 10s	06/05/2017 00:36:45	1/3 (H)	Disk OK - C: TOTAL: 39.510GB USED: 22.16.599GB (43%)
	Disco E	WARNING	12s	06/05/2017 00:36:58	3/3 (H)	Disk WARNING - E: TOTAL: 1023.997GB (86%) FREE: 137.118GB (14%)
	Interfaz VMXNET3	OK	10m 39s	06/05/2017 00:36:31	1/3 (H)	Traffic in : 32.24 Mb/s (3.2 %), Out : 87.10
	Memoria RAM	CRITICAL	19s	06/05/2017 00:36:51	3/3 (H)	Disk CRITICAL - Physical Memory TOTAL: 3.764GB (94%) FREE: 0.235GB (6%)
	Memoria Swap	OK	25s	06/05/2017 00:36:45	1/3 (H)	Disk OK - Virtual Memory TOTAL: 6.415Gi (79%) FREE: 1.303GB (21%)
	Ping	OK	8h 3m 22s	06/05/2017 00:34:53	1/3 (H)	PING OK - rtt min/avg/max/mdev = 0.116/
	Proceso iniciado FacturaScripts	OK	6h 44m 56s	06/05/2017 00:32:15	1/3 (H)	2 process matching httpd.exe (> 1) (<= 2)

Imagen: <https://www.bujarra.com/nagios-monitorizando-procesos-activos-windows-linux/>

¿Qué hacer ante las alertas?

Cada alerta implica un procedimiento a seguir

Por ejemplo:



- Si estoy monitoreando el uso de disco duro de una máquina (**HDD**) y señala que está por sobre el 90% de uso de capacidad, el sistema detecta, hace un diagnóstico y genera una alarma crítica. Así el procedimiento será ampliar la capacidad del disco o cambiar por otro.

Ticket de salida

01

De manera individual responde, ¿en qué tuviste más dificultades al implementar un monitoreo del sistema? ¿Cómo lo resolviste?

02

Indica 2 eventos que lograste monitorear.

03

De manera individual responde, si te preguntaran sobre el porqué monitorear un sistema, ¿qué razones darías?

04

Con tu grupo de trabajo respondan a esta pregunta: ¿Qué aspectos del trabajo en equipo facilitaron la tarea?

05

En tu grupo de trabajo respondan, si pudiéramos repetir el trabajo ¿qué aspectos mejoraríamos para ser más prolijos?

Referencias

- <https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-1-9780135792735>
<https://www.ciscopress.com/store/ccna-200-301-official-cert-guide-volume-2-9781587147135>