Análisis de métricas e indicadores en una empresa de diseño gráfico

---

🏢 Escenario – Empresa Creativa S.L.

Empresa Creativa S.L. es un estudio de diseño gráfico con sede en Madrid. Cuenta con **50 trabajadores**, la mayoría diseñadores y animadores, que utilizan aplicaciones de alto rendimiento como **Adobe After Effects, Photoshop, Blender y DaVinci Resolve**.

La infraestructura técnica de la empresa incluye:

- 1 servidor de almacenamiento centralizado (NAS de 60 TB)
- 1 servidor de backups local y otro en la nube
- 2 servidores para renderizado (con GPUs potentes)
- 50 estaciones de trabajo con Windows 10/11
- Red LAN de alta velocidad (10Gbps)
- Zabbix como herramienta de monitorización, ya instalada

El equipo de IT quiere definir **indicadores y métricas claras** para controlar el rendimiento del sistema y anticiparse a problemas de saturación o fallo.

📝 Tareas para la gestión

🔹 1. Identificación de objetos a monitorizar

Pregunta:
¿Qué **componentes clave** del sistema deben ser monitorizados en esta empresa? Enumera al menos **cinco** e indica por qué es relevante monitorizarlos en un entorno de diseño gráfico intensivo.

👉 *Consejo: piensa en CPU, GPU, red, almacenamiento, servicios de render, etc.*

Identificación de objetos a monitorizar:

1- Uso de GPU en los servidores de renderizado

Relevancia: tareas de animación y renderizado dependen fuertemente del rendimiento gráfico. Un cuello de botella ahí, impacta la entrega de proyectos.

2- Espacio libre en el servidor NAS de 60 TB

Relevancia: se almacenan proyectos pesados; un llenado del NAS puede bloquear flujos de trabajo.

3- Uso de CPU en estaciones de trabajo

Relevancia: After Effects, Blender y DaVinci usan CPU intensivamente para efectos.

4- Velocidad y errores en la red LAN (10Gbps)

Relevancia: una red lenta o con errores afecta la transferencia de archivos pesados y la colaboración.

5- Estado del servidor de backups (local y nube)

Relevancia: si falla el backup, el riesgo de pérdida de trabajo es crítico.

6- Usuarios conectados y sesiones activas en servidores

Relevancia: ayuda a detectar accesos no autorizados, sesiones abandonadas o uso indebido fuera del horario laboral.

7- Tráfico anómalo en la red LAN

Relevancia: en redes de alta velocidad, un volumen anormal de tráfico o conexiones inusuales puede indicar exfiltración de datos o movimientos laterales de un atacante.

8- Eventos del firewall y registros de Zabbix relacionados con accesos externos

Relevancia: se pueden detectar intentos de conexión remota no autorizada, escaneos o ataques dirigidos, sobre todo si hay herramientas colaborativas abiertas al exterior.

🔹 **2. Propuesta de indicadores**

Pregunta:
Define **tres indicadores específicos**, indicando para cada uno:

- El objeto que monitoriza (ej: CPU del servidor de renderizado)
- La unidad de medida (ej: % de uso)
- El umbral de alerta razonable (ej: > 90%)
- Por qué sería importante vigilarlo

👉 *Ejemplo de inicio: "Uso de GPU en servidor de render: % de uso, umbral crítico >95%"*

Indicador 1: Espacio libre en el servidor NAS

- **Objeto monitorizado:** Capacidad de almacenamiento disponible en el NAS de 60 TB
- **Unidad de medida:** % de espacio libre

- **Umbral de alerta:** Crítico si < 10%
- **Importancia:** Si se agota el espacio, los proyectos no se pueden guardar ni versionar. Además, puede interrumpir procesos automáticos como backups o sincronizaciones, afectando la disponibilidad de datos clave.

Indicador 2: Uso de CPU en estaciones de trabajo

- **Objeto monitorizado:** CPU de estaciones de trabajo con Windows 10/11
- **Unidad de medida:** % de uso
- **Umbral de alerta:** Crítico si > 90% durante más de 5 minutos
- **Importancia:** Un uso excesivo afecta directamente la productividad de los diseñadores. Puede indicar problemas de optimización del software, procesos colgados o necesidad de actualizar hardware.

Indicador 3: Sesiones activas y usuarios conectados a servidores

- **Objeto monitorizado:** Cantidad y origen de sesiones activas en servidores
- **Unidad de medida:** Nº de sesiones simultáneas y su IP
- **Umbral de alerta:** Crítico si hay conexiones fuera del horario habitual o desde IPs no autorizadas
- **Importancia:** Ayuda a detectar accesos no autorizados, posibles brechas de seguridad internas o intentos de fuerza bruta, especialmente si se combinan con eventos del firewall.

Indicador 4: Tasa de errores de red (LAN 10Gbps)

- **Objeto monitorizado:** Porcentaje de paquetes perdidos o errores.
- **Unidad de medida:** % de errores sobre total de paquetes
- **Umbral de alerta:** Crítico si > 0.5%
- **Importancia:** Indica posibles fallos de cableado, congestión o ataques de red (como DoS). Afecta directamente la colaboración y acceso a archivos.

Indicador 5: Eventos críticos del firewall (accesos no autorizados)

- **Objeto monitorizado:** Reglas disparadas por tráfico sospechoso o escaneos
- **Unidad de medida:** Nº de eventos por hora
- **Umbral de alerta:** Crítico si > 10 eventos/hora

- **Importancia:** Permite detectar intentos de intrusión externos o malware que intenta conectarse a C2 (Command and Control).

Indicador 6: Estado del backup (última copia válida)

- **Objeto monitorizado:** Fecha y éxito del último backup (local y en la nube)
- **Unidad de medida:** Horas desde el último backup exitoso
- **Umbral de alerta:** Crítico si > 24 h sin copia válida
- **Importancia:** Si no hay una copia reciente, se corre el riesgo de pérdida masiva de datos ante fallo del NAS o ransomware.

🔹 **3. Análisis de riesgos extremos**

Pregunta:
¿Cuál consideras que sería el **indicador más crítico o extremo** en esta infraestructura? Justifica tu respuesta con base en el impacto que tendría si supera su umbral.

Análisis de riesgos extremos

Indicador más crítico: Estado del backup (última copia válida)

Justificación:
El backup es la última línea de defensa ante varios escenarios críticos: fallos de hardware (NAS), corrupción de archivos, errores humanos o ciberataques (como ransomware). Si se detecta que no hay una copia válida reciente —por ejemplo, desde hace más de 24 horas—, la empresa queda totalmente vulnerable.

En un entorno de diseño gráfico, donde se manejan archivos grandes y únicos (renders, animaciones, proyectos colaborativos), **la pérdida de datos puede implicar semanas de trabajo perdido**, afectación a clientes y daños económicos y reputacionales graves. Además, la restauración desde cero (sin backup) sería prácticamente inviable sin copias.

Este indicador no solo refleja un problema técnico, sino **un riesgo directo a la continuidad del negocio**.

🔹 **4. Definición de frecuencia de medición**

Pregunta:
Para cada uno de los tres indicadores anteriores, indica **cada cuánto tiempo** crees que debería recogerse el dato (frecuencia) y **por cuánto tiempo** debería conservarse ese histórico.

👉 *Piensa en el equilibrio entre carga del sistema y utilidad del dato.*

Indicador	Frecuencia de medición	Retención de histórico	Justificación
Espacio libre en el servidor NAS	Cada 10 minutos	90 días	Útil para detectar patrones de llenado, crecimiento continuo o picos anómalos.
Uso de CPU en estaciones de trabajo	Cada 1 minuto	30 días	Requiere alta granularidad para correlacionar con bloqueos o caídas de rendimiento.
Sesiones activas y usuarios conectados a servidores	Cada 5 minutos	60 días	Permite auditoría de accesos sospechosos y análisis forense ante incidentes.
Tasa de errores de red (LAN 10Gbps)	Cada 2 minutos	30 días	Detecta fallos intermitentes o congestión en momentos clave de trabajo.
Eventos críticos del firewall	En tiempo real (streaming)	180 días	Es clave mantener trazabilidad ante amenazas externas persistentes.
Estado del backup (última copia válida)	Cada 1 hora	180 días	Registro necesario para auditorías y recuperación tras incidentes o ransomware.

Frecuencia de medición

- *Indicadores muy dinámicos (como **uso de CPU**) se miden cada 1 minuto porque pueden variar rápidamente y afectan la productividad.*
- *Indicadores más estables (como **espacio en disco o estado del backup**) se miden cada 10 minutos o cada hora porque no cambian tan frecuentemente, y hacerlo más seguido implicaría una carga innecesaria.*

Retención del histórico

- *Indicadores que pueden ser útiles para trazabilidad forense o auditorías (**eventos del firewall**, **sesiones de usuario**, **estado del backup**) se conservan por más tiempo (60 a 180 días).*
- *Indicadores más operativos o de rendimiento (**uso de CPU**, **errores de red**) se conservan menos tiempo (30 días) porque su valor disminuye con el tiempo y*

generan más volumen de datos.

🔹 **5. Diseño de cuadro de mando básico**

Pregunta:
Diseña un **cuadro de mando simplificado** con los siguientes elementos:

- Nombre del indicador
- Valor actual (puede ser ficticio)
- Semáforo de estado (verde, amarillo, rojo)
- Observaciones o alertas

👉 Puedes usar este formato de tabla como modelo:

Indicador	Valor actual	Estado	Observación
Uso CPU render servidor 1	97%	🔴 Rojo	Saturación total, colas de trabajo
Espacio libre NAS (60TB)	12%	🟡 Amarillo	Riesgo de llenado en 10 días
Tasa de error de red	0.2%	🟢 Verde	Dentro del rango esperado

Indicador	Valor actual	Estado	Observación
Espacio libre en el servidor NAS	8%		Riesgo crítico de llenado. Se requiere limpieza o ampliación inmediata.
Uso de CPU en estaciones de trabajo	93% (promedio alto)		Exceso de carga en tareas. Posible cuello de botella en diseño/render.
Sesiones activas y usuarios en servidores	5 sesiones nocturnas		Conexiones fuera del horario habitual. Revisión de accesos en curso.
Tasa de errores de red (LAN 10Gbps)	0.3%		Dentro del rango aceptable. No hay errores relevantes detectados.
Eventos críticos del firewall	12 eventos/hora		Detección de escaneo externo persistente. Se están aplicando bloqueos.
Estado del backup (última copia válida)	18 horas		Último backup correcto. Dentro del umbral seguro.