



Checklist de diagnóstico de conectividad (Red Local)

1. Verificación inicial

- ☐ Confirmar si el problema afecta a un solo usuario, a un grupo o a toda la entidad.
- ☐ Documentar la hora de inicio del incidente y los síntomas reportados.
- ☐ Validar si el usuario afectado tiene restricciones vigentes en el sistema PCPUMA.

2. Capa física y de acceso

- ☐ Revisar cableado y patch cords (RJ45, fibra, conectores sueltos o dañados).
- ☐ Verificar que las luces de enlace (Link/Act) en el switch o AP estén activas.
- ☐ Confirmar que el equipo de préstamo reconoce la interfaz de red (Ethernet/Wi-Fi).
- ☐ En Wi-Fi: comprobar que el usuario está conectado al SSID institucional autorizado.

3. Capa de red (switches y controladores)

- ☐ Validar que el puerto del switch esté en estado up.
- ☐ Revisar que la VLAN asignada al puerto corresponde a la configuración de la entidad.
- ☐ Ejecutar 'show mac address-table interface <puerto>' para verificar aprendizaje de MAC.
- ☐ Comprobar que las ACLs o políticas de seguridad no bloqueen tráfico básico (DHCP, DNS, ICMP).

4. Servicios críticos

- ☐ Probar si el usuario obtiene dirección IP automática (DHCP).
- ☐ Validar conectividad con el gateway local (ping <ip_gateway>).
- ☐ Validar resolución de nombres (nslookup www.unam.mx).
- ☐ Revisar logs del servidor DHCP/DNS local si aplica.

5. Conectividad con PC Puma

- ☐ Probar acceso a la red central de PC Puma (ping <pcpuma.unam.mx> o traceroute).



- ☐ Verificar rutas en el router de borde con 'show ip route'.
- ☐ Asegurar que no haya bloqueos de firewall hacia dominios/servicios PCPuma.

6. Diagnóstico en puntos de acceso (Wi-Fi)

- ☐ Revisar logs del controlador WLAN (ArubaOS / Cisco WLC) para detectar desconexiones o errores.
- ☐ Confirmar niveles de señal (RSSI > -65 dBm, SNR > 20 dB).
- ☐ Verificar saturación de canales o interferencias (microondas, otros APs).
- ☐ Validar política de roaming en múltiples APs.

7. Políticas de seguridad

- ☐ Confirmar que el firewall local permite tráfico hacia servicios críticos (DNS, HTTPS, PCPuma).
- ☐ Revisar reglas de acceso y NAT.
- ☐ Auditar que no haya bloqueos erróneos en ACLs.

8. Escalamiento

- ☐ Si el problema persiste, escalar con evidencia (logs, capturas, traceroute).
- ☐ Incluir hora y lugar del incidente, dispositivo afectado y número de inventario.
- ☐ Reportar al área central PCPuma si involucra servicios comunes.

9. Checklist rápido (resumen operativo)

- ☐ ¿Cables/puertos OK?
- ☐ ¿VLAN y ACL correctas?
- ☐ ¿IP/DNS asignados?
- ☐ ¿Gateway responde?
- ☐ ¿Firewall bloquea?
- ☐ ¿SSID y controlador OK?
- ☐ ¿Incidencia aislada o generalizada?