CHECKLIST DE SEGURIDAD PARA REDES

SIELSIC

V.002/2025

En un mundo cada vez más conectado, tu red inalámbrica actúa como puerta de entrada a tu vida digital. Protegerla es esencial para salvaguardar tu privacidad, datos financieros y comunicación personal. Esta lista de verificación presenta los pasos fundamentales —desde la configuración del router y cifrado de la Wi-Fi hasta segmentación de dispositivos, monitoreo continuo y respuesta ante incidentes— para prevenir accesos no autorizados, ataques cibernéticos y fugas de información.

Siguiendo estas recomendaciones podrás fortalecer la defensa de tu red doméstica u oficina, manteniéndola segura y confiable frente a las amenazas actuales. simeononsecurity.com+5securechecklist.com+5cybersecurityconsultingops.com+5

1. 🔧 HARDWARE Y ROUTER

- **Actualiza el router cada 5 años:** Los dispositivos antiguos ya no reciben parches y pueden tener vulnerabilidades – UC Davis recomienda renovar el hardware cada cinco años para mantener la seguridad (iet.ucdavis.edu).
- **Actualizaciones automáticas de firmware:** Activa las actualizaciones automáticas si el router lo permite; sino, revisa mensualmente con tu proveedor .
- **Reinicios periódicos:** Realiza un reinicio mensual o semanal para limpiar errores temporales .
- **Desactiva administración remota, UPnP y WPS:** Son puntos de explotación conocidos, desactívalos salvo que sean estrictamente necesarios (cisa.gov).
- **Habilita firewall y filtrado web:** Configura controles del firewall del router y bloquea sitios maliciosos (iet.ucdavis.edu).

Todo el mundo.

www.reallygreatsite.com

SIELSIC

2. 🛡️ CONFIGURACIÓN WI-FI

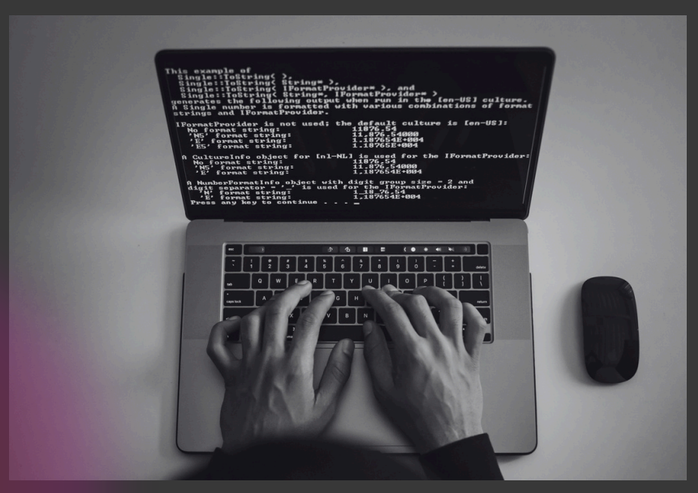
- Usa cifrado WPA3 (o WPA2-AES si no está disponible): Proporciona la protección más robusta frente a ataques mediante fuerza bruta .

- Cambia SSID y contraseñas fuertes:
  - SSID no debe revelar información personal ni el modelo del router (cisa.gov, medium.com).
  - Contraseña de 16–30 caracteres con mayúsculas, minúsculas, números y símbo
  - los; idealmente renovarla cada 6–12 meses (datalyst.net).

- Redes separadas:
  - Invitados: Acceso a internet sin riesgo de acceder a tu red principal (lifewire.com).
  - Dispositivos IoT: Segmenta cámaras, asistentes y otros en otra red para reducir riesgo (medium.com).

---

3. 🔍 MONITOREO Y AUDITORÍA



- **Revisa dispositivos conectados:**

Identifica y bloquea equipos desconocidos regularmente .

- **Auditorías de seguridad:**

1. Realiza encuestas del sitio inalámbrico (site survey) para detectar filtraciones de señal o puntos ciegos (greyhatinfosec.com, allabouttesting.org).
2. Revisiones de protocolos: asegúrate que WPA2/3 estén correctamente activados .
3. Detecta puntos de acceso "rogue" con sistemas de prevención de intrusiones (WIDS/WIPS) (en.wikipedia.org).

CHECKLIST DE SEGURIDAD PARA REDES

SIELSIC

4. 🧩 DISPOSITIVOS Y USUARIOS

- **Actualiza sistemas y antivirus:** Mantén todos los dispositivos con software protegido y antimalware activo (astound.com).
- **Gestiona contraseñas y MFA:**
  a) Usa gestores de contraseñas para crear credenciales únicas (astound.com).
  b) Activa autenticación multifactor en cuentas críticas .
- **Segmentación de permisos:** Otorga accesos específicos según necesidad (padres, niños, empleados)
- **Educación:** Enseña buenas prácticas (phishing, descargar archivos, redes desconocidas) a los usuarios.

5. 🔒 CONFIGURACIONES AVANZADAS

- DNS seguro y filtrado: Utiliza servicios como Cloudflare 1.1.1.3, OpenDNS o NextDNS para bloquear contenido malicioso (medium.com).
- Filtrado por MAC/IP/DHCP: Lista blanca de dispositivos y rango reducido de DHCP para aumentar seguridad .
- Control de potencia y ubicación del router: Colócalo en un área central, lejos de ventanas exteriores, y ajusta la potencia de señal para evitar fugas .
- VPN para acceso externo: Si necesitas conexión remota, utiliza VPN con cifrado robusto.

SIELSIC

6. 💾 COPIAS DE SEGURIDAD Y RESPUESTA

1. **Backups regulares y cifrados:** Haz copias en la nube o discos externos y asegúralas con cifrado .
2. **Plan de respuesta y registro:**

- Registra eventos del router y dispositivos.
- Utiliza herramientas de análisis (logs, SIEM básico).
- Define plan con roles y flujos en caso de incidente .

✓ RESUMEN DE VERIFICACIÓN

Área	Acción
Hardware	Router <5 años, firmware actualizado, reinicios programados
Redes Wi-Fi	WPA3, contraseñas robustas, SSID anónimo
Segmentación	Separar invitados e IoT
Monitoreo	Revisar dispositivos, auditorías regulares
Dispositivos	Antivirus, MFA, gestión de contraseñas
Avanzado	DNS filtrado, MAC control, VPN
Respaldo	Backups cifrados + plan de respuesta