



## AC03 Asume el rol de especialista en TI de tu hogar

Ingeniería Tecnologías de la Información

9°A

INTEGRANTES:

|                             |            |
|-----------------------------|------------|
| - Mendieta Chimal Sony Luis | MCS0220598 |
| - Nava Sanchez Axel         | NSA0220388 |

Docente: Enrique Solano García

Materia: Seguridad Informática

08/05/2025

## 1. Diagnóstico de la red y los dispositivos del hogar

A continuación una lista de los dispositivos con los que contamos en el hogar.

| Dispositivo     | Tipo       | Sistema Operativo    | Antivirus           | Actualizado |
|-----------------|------------|----------------------|---------------------|-------------|
| PC Escritorio   | PC         | Windows 11           | Windows Defender    | Sí          |
| Laptop personal | Laptop     | Arch Linux 6.14.4    | No                  | Sí          |
| Smartphone A    | Smartphone | Android 13           | Google Play Protect | Sí          |
| Smartphone B    | Smartphone | iOS 17               | Integrado           | Sí          |
| Tablet          | Tablet     | Android 11           | No                  | No          |
| Smart TV        | Smart TV   | WebOS                | No                  | No          |
| Cámara IP       | Seguridad  | Firmware propietario | No aplica           | Sí          |

## **Configuración de Red Wi-Fi**

En nuestra red Wi-Fi se mantienen los ajustes predeterminados proporcionados por el proveedor, incluyendo el nombre de la red (SSID) y la contraseña. Por lo tanto, las respuestas a las siguientes preguntas se detallan de la siguiente manera:

### **¿Tiene contraseña segura?**

Generalmente, las contraseñas predeterminadas asignadas por los proveedores cumplen con los requisitos básicos de seguridad, como un mínimo de 8 caracteres y la inclusión de al menos un símbolo especial.

### **¿Está oculta o visible?**

La red es visible, ya que el nombre del Wi-Fi aparece en la lista de redes disponibles. Sin embargo, el módem está en una ubicación no accesible para las visitas, lo que limita el acceso físico a la información de la red.

### **¿Se usan protocolos de seguridad como WPA2 o WPA3?**

Sí, actualmente la red utiliza el protocolo de seguridad WPA3, que es uno de los más avanzados y seguros disponibles.

## 2. Identificación de riesgos y vulnerabilidades

### **Prácticas Inseguras Detectadas**

- Uso de contraseña default en el router o que esta misma se muestra en el modem.
- Contraseñas similares o repetidas en cuentas personales.
- Tablet sin antivirus ni actualizaciones.
- Smart TV sin actualizaciones.
- Descarga ocasional de archivos desde sitios de origen desconocido.
- La red se ha compartido con visitas sin supervisión.

### 3. Propuesta de medidas de seguridad informática.

#### Plan de Acción

| Medida                                     | Descripción   | Justificación   |
|--|---|---|
| <b>Red Wi-Fi Segura</b>                    | Cambiar la contraseña o que la contraseña no sea visible en el modem.                   | Previene accesos no autorizados a la red.                       |
| <b>Contraseñas fuertes y únicas</b>        | Usar combinaciones largas y únicas, con gestores de contraseñas como Bitwarden.         | Reduce riesgo de acceso a cuentas personales por reutilización. |
| <b>Actualizar SO y antivirus</b>           | Habilitar actualizaciones automáticas en todos los dispositivos.                        | Protege contra vulnerabilidades conocidas.                      |
| <b>Antivirus en todos los dispositivos</b> | Instalar software de protección confiable en tablet y otros dispositivos sin antivirus. | Mejora la detección de amenazas y malware.                      |
| <b>Autenticación en dos pasos (2FA)</b>    | Activar 2FA en cuentas de correo, banca, redes sociales.                                | Añade una capa de protección ante filtraciones de contraseña.   |
| <b>Firewall activo</b>                     | Asegurar que el firewall esté habilitado en todos los dispositivos.                     | Filtra tráfico malicioso o no deseado.                          |
| <b>Educación digital en familia</b>        | Capacitar a todos los miembros sobre navegación segura, verificación de enlaces.        | Mejora la cultura de ciberseguridad en el hogar.                |

#### 4. Entrega de informe

- Realizar auditorías trimestrales de los dispositivos conectados y su seguridad.
- Cambiar contraseñas cada 6 meses y no repetirlas entre servicios.
- Revisar permisos de las aplicaciones móviles periódicamente.
- Hacer copias de seguridad automáticas y almacenarlas en la nube o en discos duros externos.

