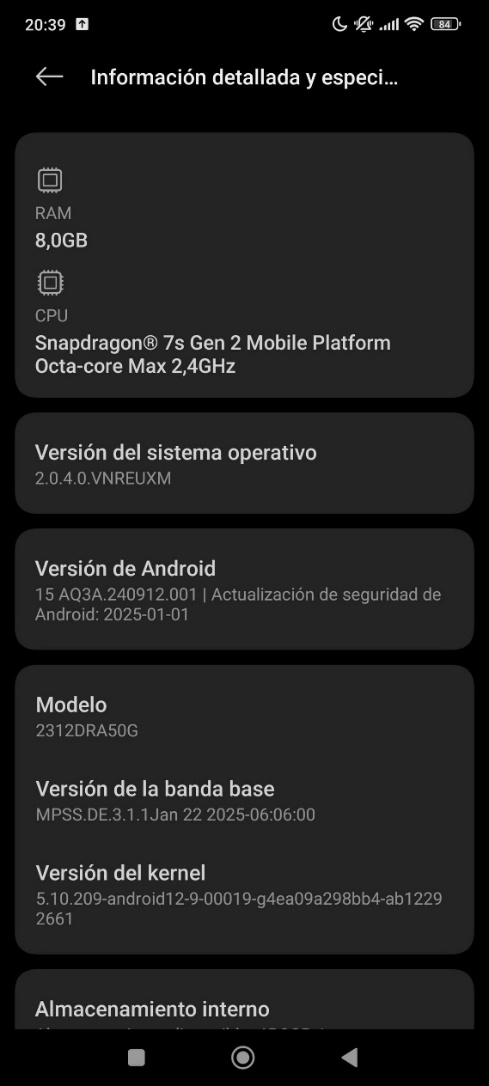
# Auditoria de Hardening Endpoints BYOD

## Dispositivo Móvil

### Detalles del Dispositivo

* **Modelo:** Redmi Note 13 Pro 5G
* **Almacenamiento interno:**   
  **Total:** 128 GB   
  **Disponible:** 45,2 GB (82,7 GB utilizados)
* **Sistema operativo:** Xiaomi HyperOS 2.0.4.0
* **Versión del sistema operativo:** 2.0.4.0. VNREUXM
* **Versión de Android:** 15 AQ3A.240912.001
* **Actualización de seguridad de Android:** 01 de enero de 2025

**Ilustración 1. Detalles del Dispositivo**



* **Procesador (CPU):** Snapdragon® 7s Gen 2 Mobile Platform Octa-core, hasta 2,4 GHz
* **Memoria RAM:** 8,0 GB
* **Código del modelo:** 2312DRA50G
* **Versión del kernel:** 5.10.209-android12-9-00019-g4ea09a298bb4-ab12292661
* **Versión de la banda base:** MPSS.DE.3.1.1 (22 de enero de 2025 - 06:06:00)

**Ilustración 2. Especificaciones Técnicas**

### Estado de Seguridad

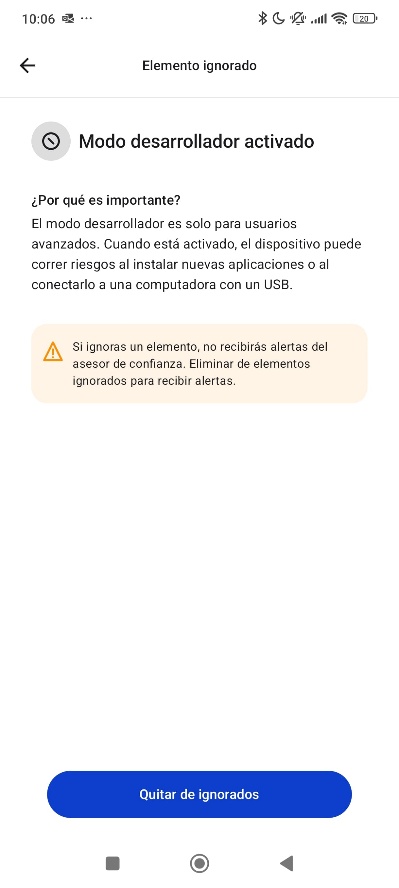
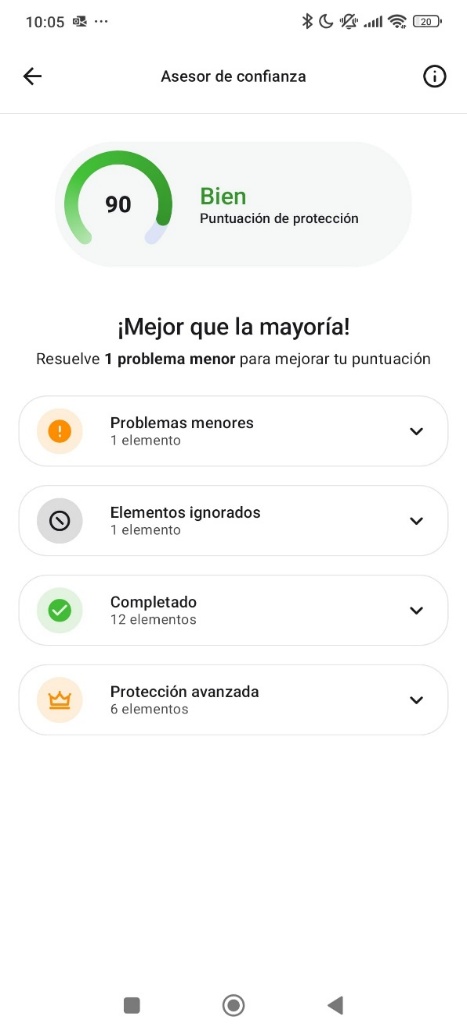
**Actualización de seguridad**: Última actualización instalada (01/01/2025). **Estado:** Actualizado y protegido contra vulnerabilidades conocidas.

#### Análisis de Malwarebytes

* Último análisis**:** *18 de marzo de 2025*.
* Puntuación inicial**:** **56** (Deficiente) debido a:
  + Malware detectado: "Duolingo By ModsManiac" (en lista blanca).
  + Modo desarrollador activado (en elementos ignorados).

##### Acciones tomadas**:**

* + Se añadió "Duolingo By ModsManiac" de la lista blanca, permitiendo que Malwarebytes lo mantenga en monitorización, ya que es indispensable para el auditor, ya que quiere llevar su “Hardening” de idiomas al siguiente nivel 😉.
  + Puntuación mejorada a **90** (Bien) tras resolver el problema del malware y resolver casi todos los problemas menores.

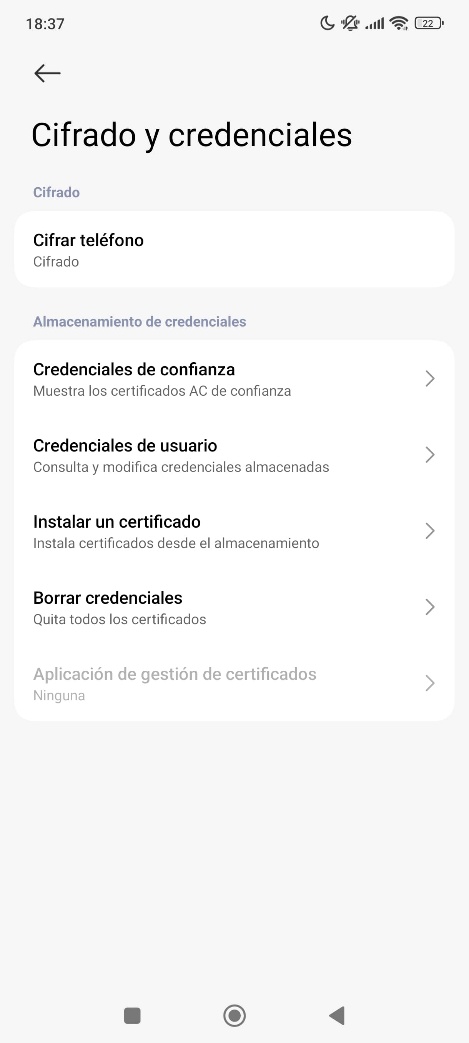
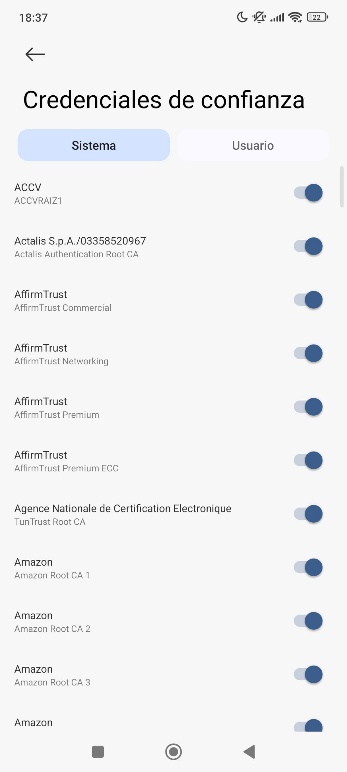


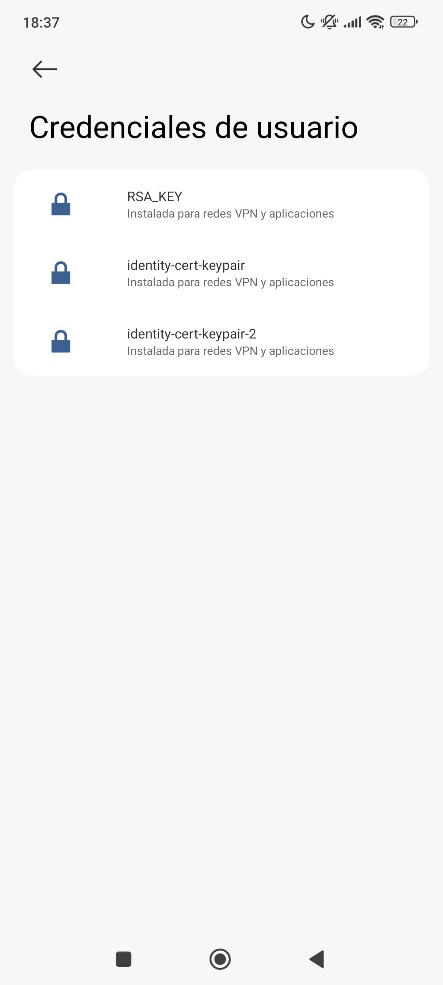


* **Estado actual:**
  + Sin amenazas activas.
  + Elementos ignorados: 2 (Modo desarrollador y otro elemento no especificado, pero no representan una amenaza activa).
  + Nivel de Hardening: **100**

##### Cifrado

* **Estado:** Cifrado activado (confirmado en "Cifrar teléfono").
* **Credenciales de confianza:** Varias CA instaladas (ACCVRAIZ1, Actalis, AffirmTrust, Amazon Root CA, etc.). Todas parecen estándar, pero se recomienda desactivar las que no sean necesarias.
* **Credenciales de usuario:** Tres credenciales instaladas para VPN (RSA-KEY, identity-cert-keypair, identity-cert-keypair-2). Si no usas VPN, considera eliminarlas.





##### Políticas de Red

* **Wi-Fi:** Conectado a "vodafoneD1D0" con WPA/WPA2-Personal. Se recomienda actualizar a WPA3 si el router lo soporta.
* **Velocidad:** 866 Mbps (excelente).
* **Proxy:** Ninguno (seguro).
* **Privacidad:** Dirección MAC aleatoria activada (buena práctica).
* **IP:** Configuración DHCP (estándar y segura).

### Check

1. Respecto a la configuración del dispositivo:

No tener habilitada la instalación de software de orígenes desconocidos

No tener el dispositivo móvil rooteado o jailbreak

Tener instaladas todas las actualizaciones del fabricante del dispositivo del sistema operativo y de la aplicación browser

No conectarse a redes Wifi sin seguridad adecuada o con SSID oculta

No tener activado el dispositivo Bluetooth durante las conexiones Web

2. Respecto a las aplicaciones instaladas:

No tener instaladas aplicaciones maliciosas o sospechosas de serlo.

No tener abiertas conexiones de red de aplicaciones diferentes al browser y que se consideren sospechosas

No tener habilitados permisos de otras aplicaciones para lectura de información sobre lo que el browser se descarga/envía.

### Resumen

El **Redmi Note 13 Pro 5G** ha alcanzado un nivel de seguridad excelente (puntuación 100 en Malwarebytes) tras resolver el problema con el malware "Duolingo By ModsManiac". El dispositivo está cifrado, actualizado (enero 2025), y la configuración de red es razonablemente segura con WPA/WPA2 y MAC aleatorio. Sin embargo, hay áreas de mejora, como desactivar el modo desarrollador si no es necesario, actualizar a WPA3, y revisar los permisos de aplicaciones. Siguiendo las recomendaciones, el dispositivo estará aún más protegido.

## Dispositivo Portátil

### Detalles del Dispositivo

#### PC Físico (Windows 11 Home)

* **Modelo:** Victus by HP Laptop PC D0041NS
* **Procesador:** 11th Gen Intel Core i5-11400H @ 2.70GHz
* **RAM:** 16.0 GB (15.6 GB usable)
* **Sistema operativo:** Windows 11 Home, versión 24H2
* **Almacenamiento:** 175GB de 476GB Disponibles

#### Máquina Virtual Oracle Virtual Box

* **Sistema operativo:** Ubuntu 24.04.2 LTS (64-bit)
* **Memoria base:** 8192 MB (8 GB)
* **Procesadores:** 4
* **Orden de arranque:** Disquete, Óptica, Disco duro
* **Aceleración:** Paginación anidada, Paravirtualización KVM
* **Memoria de video:** 16 MB
* **Controlador gráfico:** VMSVGA
* **Controlador: IDE** **secundario 0:** ubuntu-24.04.2-desktop-amd64.iso (5.91 GB)
* **Controlador: SATA** **Puerto SATA 0:** Linux.vdi (Normal, 14.50 GB)

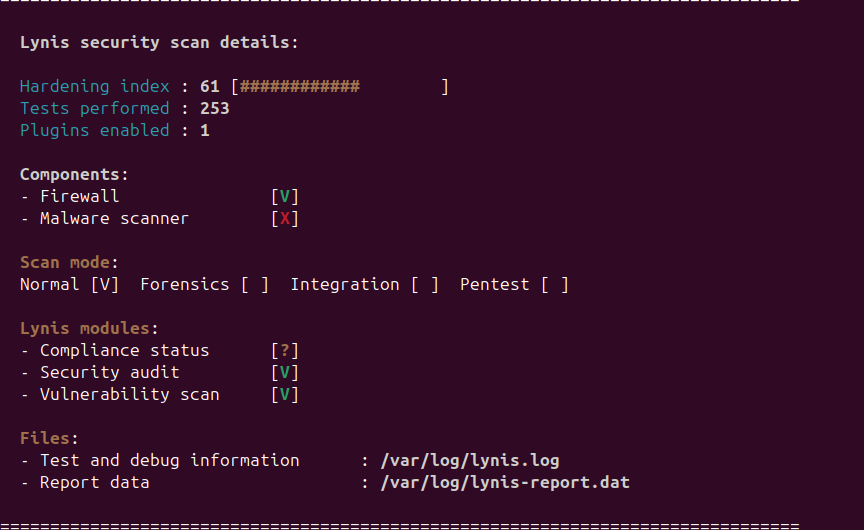
### Estado de Seguridad

#### Analisis de Lynis

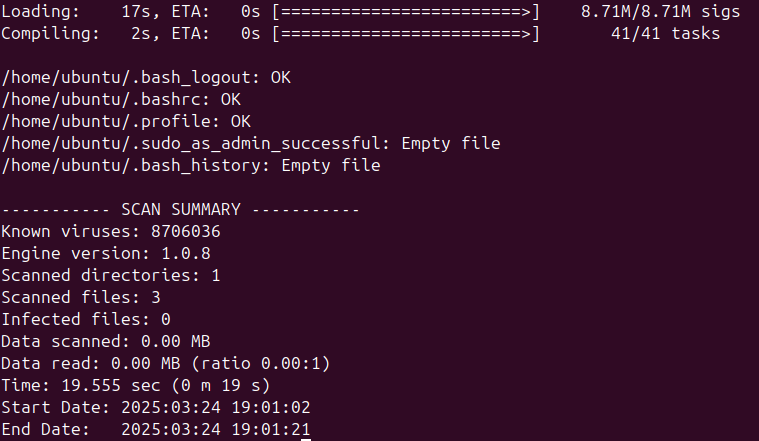
##### Metodología

* Actualización del sistema con ***apt update*** y ***apt upgrade***.
* Instalación de **Lynis** y auditoría.
* Resolución de warnings identificados por **Lynis** .
* Instalación de un malware scanner (**ClamAV**).
* Fortificar el navegador web (**Firefox**).
* Realizar un nuevo escaneo con **Lynis** para verificar el **Hardening** **Index** final

##### Resultados Iniciales

* ***apt update***: 171 paquetes disponibles para actualizar.
* ***apt upgrade***: 169 paquetes actualizados, 7 nuevos instalados, 2 no actualizados.
* **Hardening Index Inicial:** .

##### Acciones Realizadas

* **Actualización del sistema:** Se actualizaron 169 paquetes y se instalaron 7 nuevos.
* **Instalación de Lynis:** Herramienta instalada para realizar la auditoría.
  + ***lynis audit system***
* **Instalación de** [**ClamAV**](https://www.strsistemas.com/blog/deteccion-de-virus-y-malware-en-linux-con-clamav)**:** Se instaló un malware scanner y se actualizó su base de datos.
  + ***apt install clamav clamav-daemon***
  + ***freshclam*** actualiza manualmente la base de datos.
  + ***clamscan -r / --bell -i*** Escanea el sistema completo
    - ***-r*** Escanea recursivamente.
    - ***/***: Escanea desde la raíz del sistema.
    - ***--bell***: Emite un sonido si encuentra amenazas.
    - ***-i***: Solo muestra archivos infectados.
  + ***systemctl enable clamav-daemon*** Escaneos Automáticos en segundo plano
* **Configurar Firewall(ufw):** Usa ufw:
  + ***ufw enable*** Controlar trafico de red – *El cortafuegos esta activo y habilidado en el arranque del sistema*
  + ***ufw allow ssh*** Regla añadida(v6)
  + ***ufw deny out to any*** Regla añadida(v6)
* **Auditoria final de Lynis para obtener el índice igual o superior a 69 como lo establecido en la política de seguridad de la empresa**

### Check Seguridad Firefox:

#### Activar Protección Mejorada contra Rastreo

* + *Configuración > Privacidad y Seguridad > Protección mejorada contra el rastreo > Estricta.*

#### Deshabilitar el Almacenamiento de Contraseñas:

*Configuración > Privacidad y Seguridad > Inicios de Sesión y Contraseñas > Pedir que se guarden los inicios de sesión y contraseñas para sitios web.*

#### Habilitar Navegación Segura:

*Configuración > Privacidad y Seguridad > Seguridad > Bloquear contenido peligroso y engañoso && Advertir sobre software no deseado o poco común*

#### Deshabilitar Telemetría:

Configuración > Privacidad y Seguridad > Recopilación y uso de datos de Firefox

#### Configuración de Políticas Corporativas

##### Crear un Archivo de Políticas

1. ***sudo mkdir -p /etc/firefox/policies.json***
2. ***sudo nano /etc/firefox/policies/policies.json***

##### Justificación

* **DisableTelemetry** y **DisableFirefoxStudies**: Evita la recopilación de datos.
* **BlockAboutConfig**: Impide que los usuarios accedan a configuraciones avanzadas que podrían debilitar la seguridad.
* **WebRTC**: Deshabilita WebRTC para evitar fugas de IP.
* **DisableFormFill** y **DisablePasswordManager**: Evita el almacenamiento de datos sensibles.
* **SanitizeOnShutdown**: Limpia datos temporales al cerrar Firefox, reduciendo el riesgo de exposición.

##### Verificar la Aplicación de Políticas

* Reiniciar Firefox y verificar que las configuraciones se hayan aplicado, por ejemplo, intentar acceder a about:config que debería estar bloqueado.
* Visitar un [sitio de prueba seguro](como%20https:/www.phishing.org/test-your-phishing-iq) para confirmar que Firefox bloquea contenido sospechoso.

### Resumen

La máquina virtual con **Ubuntu 24.04.2 LTS** fue auditada y bastionada siguiendo las mejores prácticas de seguridad. Se actualizó el sistema, se instaló un malware scanner (**ClamAV**), se configuró un firewall con **ufw**, se fortaleció el navegador **Firefox**, y se resolvieron los warnings identificados por **Lynis**.

El **Hardening Index** final ***69*** superó el objetivo de ***69***, cumpliendo con la **Política de Seguridad de la empresa**. Además, se ajustaron configuraciones de VirtualBox para minimizar riesgos desde el host.