EDUCACIÓN
SECRETARÍA DE EDUCACIÓN PÚBLICA

TECNOLÓGICO NACIONAL DE MÉXICO

AUDITORIA
INFORMÁTICA

Docente: Dra. Luz María Lugo Méndez

Noveno Piso del Edificio Hospitalario
New City Medical Plaza
Consultorio Dental

Integrantes del Equipo:

Lara de la O Geovani - 21212346
León Cruz Jorge Joshua - 21212347
Muñoz Cervantes Berenice - 21212601
Torres Lagunas Ezequiel - 21212369

Diciembre 2025

Índice de
CONTENIDOS

INTRODUCCIÓN

Del proyecto

Contexto:

- Auditoría técnica de seguridad informática.
- Aplicación de la metodología OSSTMM.
- Ubicación: Consultorio 903, 9no piso, New City Medical Plaza.
- Propietaria: Dra. Diana Torres.

Objetivo

- Evaluar seguridad humana, física, inalámbrica, telecomunicaciones y redes de datos.
- Identificar vulnerabilidades.
- Calcular riesgos con matriz RAV.
- Proponer un plan de mejora.

METODOLOGÍAS

OSSTMM V 2.1 Open Source Security Testing Methodology Manual
(Manual de Metodología de Pruebas de Seguridad de Código Abierto)

OSSTMM V 2.1

01 **Evaluación basada en canales de interacción**

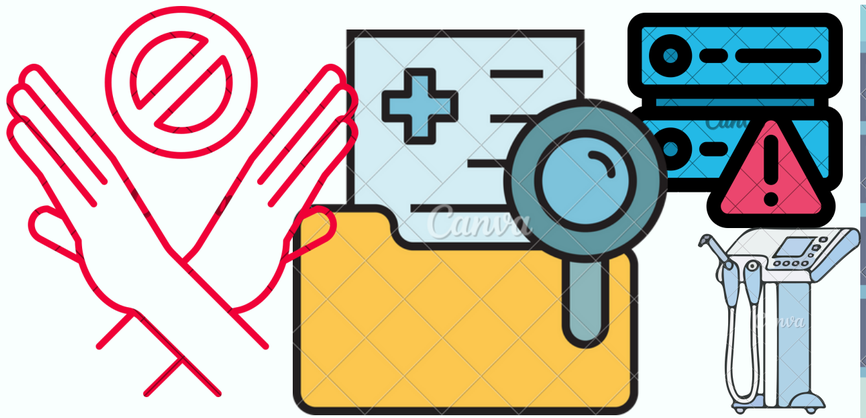
02 **Medición cuantitativa del riesgo con métricas RAV**

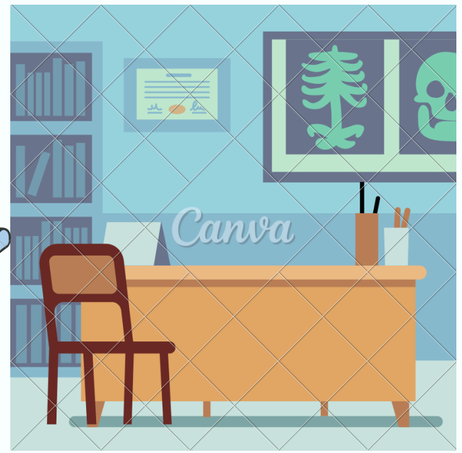
03 **Pruebas de seguridad sin sesgos, repetibles y verificables**

04 **Enfoque en seguridad operacional realista**

- **ISO 27001**
- **Observación directa**
- **Entrevista**
- **Revisión documental**
- **Investigación digital**
- **Pruebas Técnicas**

ALCANCE Y REGLAS DE COMPROMISO





BITÁCORA

Datos Generales			
Fecha de Inicio:	17 nov 2025	**Fecha de Finalización:**	21 nov 2025
Ubicación:	Consultorio 903, Piso 9 – Edificio Hospitalario New City Medical Plaza, Ave. Paseo del Centenario 9580, Zona Urbana Río Tijuana.		
Nombre de la Empresa:	Sinergía Dental		
Giro:	Servicios Odontológicos		
Propietaria:	Dra. Diana Torres Lagunas		
Correo:	dtorreslagunas@gmail.com		

BITÁCORA

Datos de la Auditoría			
Fecha:	17/ Noviembre/ 2025	**Hora de Inicio:**	14:00 hrs
Responsable:	C. Ezequiel Torres Lagunas	**Hora de Finalización:**	19:00 hrs

Metodología Aplicada

- ☑ OSSTMM
- ☑ Observación directa
- ☑ Entrevista
- ☑ Revisión documental
- ☑ Pruebas técnicas
- ☑ ISO 27001

Notas y Evidencias

1. Llegada al edificio por el acceso vehicular para poder ingresar por el acceso principal:

E.2 -Verificación de Redes Inalámbricas

Preguntas

1. ¿Qué dispositivos se conectan actualmente a la red WiFi del consultorio?
Principalmente el televisor inteligente, la cámara de seguridad o en algunas ocasiones cuando hago uso de la computadora.

2. ¿Ha cambiado recientemente la contraseña del WiFi o mantiene la misma desde su instalación?
Se mantiene la misma contraseña desde que el proveedor instaló el servicio; no se ha modificado.

3. ¿Cómo suele compartir la contraseña del WiFi cuando un paciente o visitante la solicita?
Si la solicita se le proporciona al paciente.

4. ¿Cuenta con una red separada para invitados o todos los dispositivos utilizan la misma red? Desconozco del tema.

5. ¿Ha notado si la señal llega a zonas como pasillos o baños fuera del consultorio? Sí, la señal se mantiene fuerte en los pasillos y áreas externas cercanas.

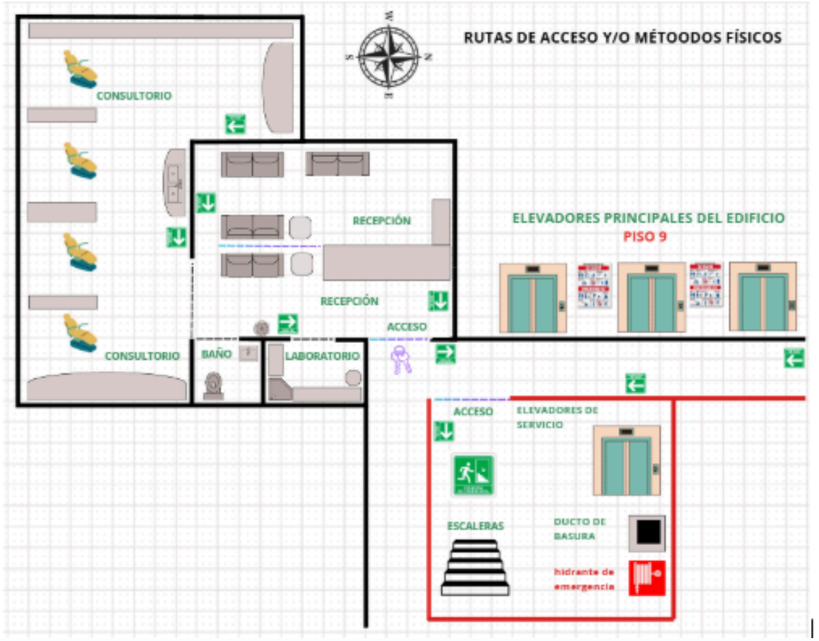
6. ¿Realiza algún monitoreo de los dispositivos conectados al WiFi?
No, no reviso qué dispositivos están conectados; solo uso la red para trabajar.

7. ¿Ha recibido instrucciones del proveedor sobre seguridad inalámbrica o configuración avanzada? No, únicamente dejaron el módem funcionando. Nunca se modificaron opciones avanzadas.

BITÁCORA

F3. Evaluación de Controles de Acceso

El mapa de *Rutas y Métodos Físicos* evidencia que el consultorio depende de accesos estándares a través de elevadores, pasillo común y, en caso de emergencia, escaleras presurizadas de evacuación. El acceso principal no cuenta con mecanismos avanzados de control como autenticación por tarjeta, bloqueo biométrico o bitácora de entrada, por lo que la seguridad se fundamenta en cerraduras convencionales y presencia del personal. No se identifican esclusas, zonas de retención ni puntos redundantes de control de identidad, lo cual es adecuado para un consultorio pequeño pero no para un entorno con alta sensibilidad de datos.



Criterios Evaluados

Sección A. Seguridad de la Información

- ☑ A.1 Revisión de Inteligencia Competitiva
- ☑ A.2 Revisión de Privacidad
- ☑ A.3 Recolección de Documentos

Sección B. Proceso de Seguridad

- ☑ B.1 Testeo de Solicitud
- ☑ B.2 Testeo de Sugerencia Dirigida
- ☑ B.3 Testeo de las Personas Confiables

Sección C. Tecnologías de Internet y su Seguridad

- ☑ C.1 Logística y Controles
- ☑ C.2 Exploración de Red
- ☐ ~~C.3 Identificación de los Servicios del Sistema~~
- ☑ C.4 Búsqueda de Información Competitiva
- ☑ C.5 Revisión de Privacidad
- ☑ C.6 Obtención de Documentos
- ☑ C.7 Búsqueda y Verificación de Vulnerabilidades
- ☐ ~~C.8 Testeo de Aplicaciones de Internet~~
- ☑ C.9 Enrutamiento
- ☐ ~~C.10 Testeo de Sistemas Confiados~~

RESULTADOS

RAV Por Canal

1.- Información
2.- Proceso Humano
3.- Tecnologías de Internet
4.- Comunicaciones
5.- Inalámbrico
6.- Físico

Estrellas	Pts RAV
☆☆☆☆☆	0
★☆☆☆☆	20
★★☆☆☆	40
★★★☆☆	60
★★★★☆	80
★★★★★	100

- **Alto:** 200 - 300
- **Medio:** 100 - 199
- **Bajo:** 1 - 99
- **Crítico:** ≤0

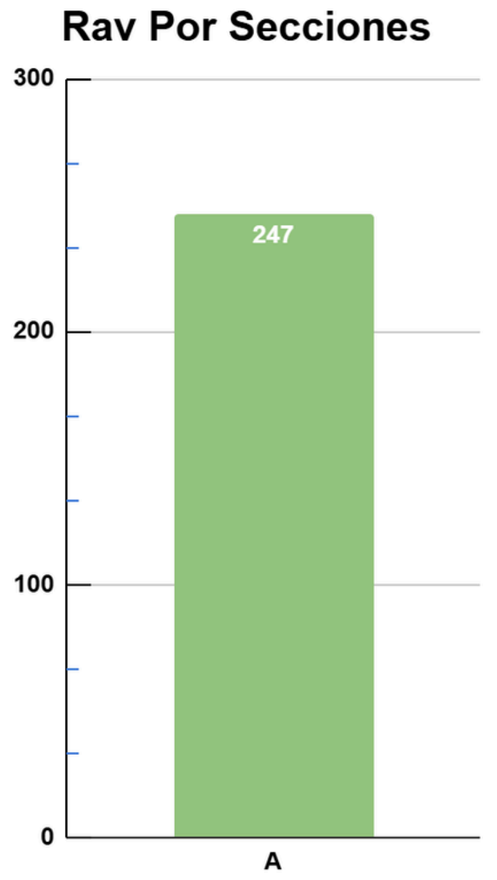
Evaluado	Sección	Nº	Req.	Diligencia	Control	Visibilidad	Limitaciones	Descr.	Exposición	Obs.	RAV Parcial	Nivel

C A N A L

Información

Esta sección representa el mejor desempeño del consultorio, debido a sus siguientes fortalezas:

- Buen control documental.
- Baja exposición de información.
- Procesos claros y aplicados correctamente.



C A N A L

Proceso Humano

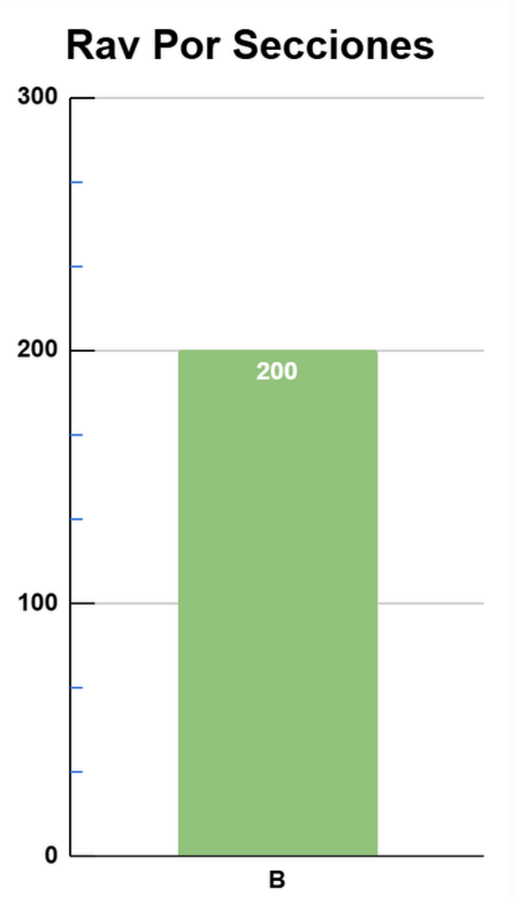
Los procedimientos con testeo de solicitudes, sugerencias y personas muestran un nivel adecuado y en su mayoría bien implementado:

Fortalezas:

- Procedimientos establecidos
- Controles aplicados.
- Buena gestión operativa.

Áreas de mejora:

- Mayor control de accesos a documentación importante.
- Formalización de controles preventivos.



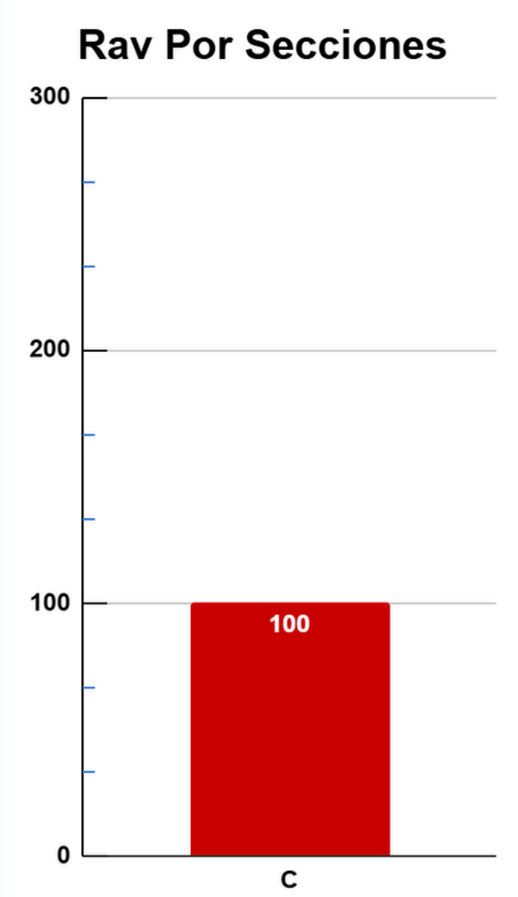
C A N A L

Tecnologías de Internet

Esta sección presenta el puntaje más bajo, ya que el desempeño aún se mantiene por debajo del 40% de cobertura de seguridad, lo que indica que existen debilidades importantes.

Riesgos identificados:

- Altas exposiciones en infraestructura y servicios.
- Falta de controles robustos en aplicaciones.
- Escasa visibilidad de red.
- Gestión reactiva en lugar de preventiva.



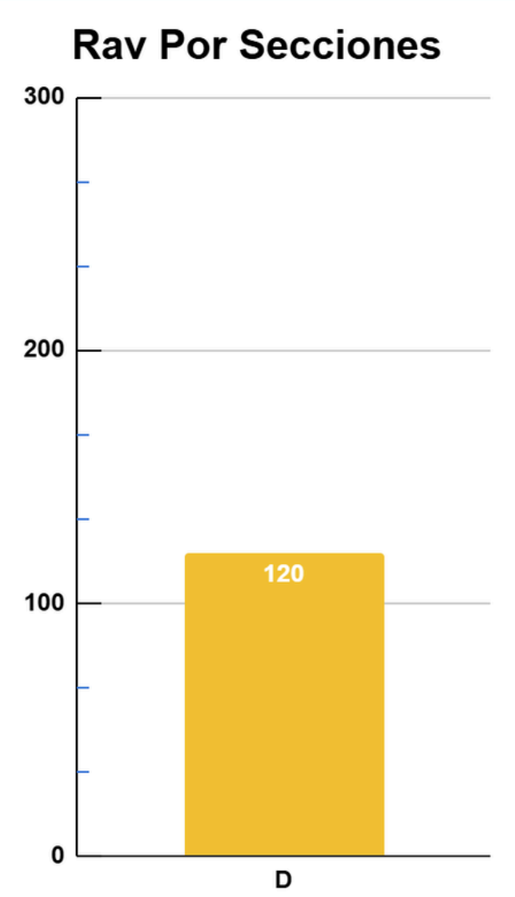
C A N A L

Comunicaciones

Debido a cuestiones de accesibilidad y permisos otorgados para la auditoría, para esta sección solo se evaluó un criterio, aún así, la puntuación indica que el hospital presenta **debilidades importantes** en la configuración y uso de su módem.

Riesgos identificados:

- Tecnologías antiguas sin controles.
- Servicios que podrían ser explotados fácilmente.
- Baja visibilidad de uso y monitoreo.



CANAL

Inalámbrico

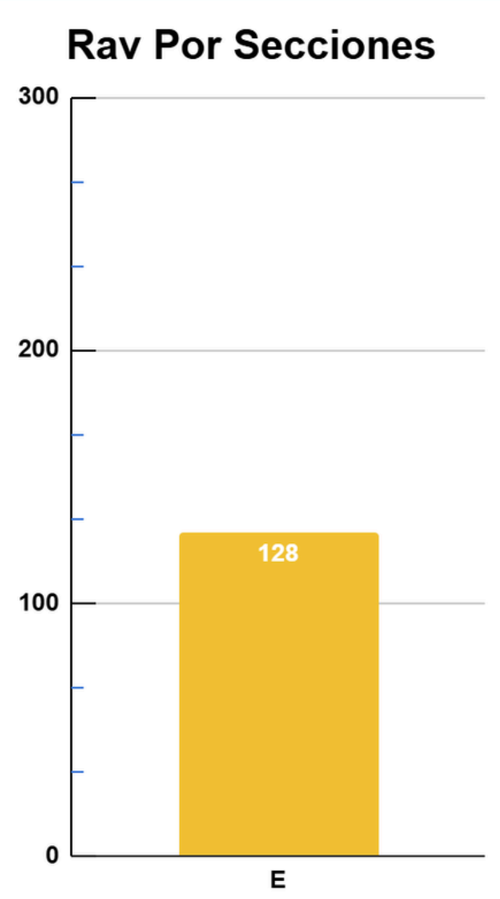
Durante la evaluación se detectaron deficiencias en la gestión de redes WiFi y dispositivos inalámbricos.

Riesgos identificados:

- Falta de controles en redes inalámbricas.
- Uso de dispositivos no monitoreados.
- Riesgos elevados en comunicaciones sin cable.

Áreas de mejora:

- Políticas de uso de dispositivos más estrictas.
- Mejor cifrado y segmentación de redes.
- Detección de acceso no autorizado.



CANAL

Físico

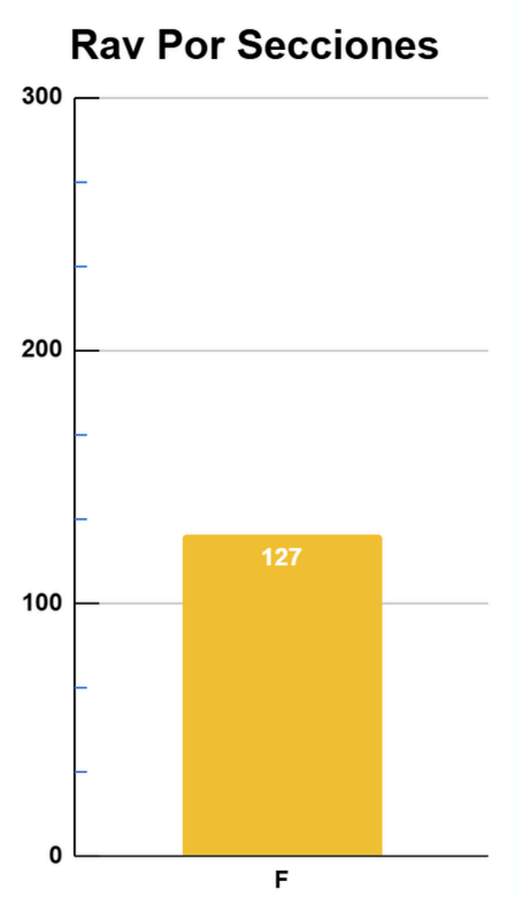
Los controles físicos como perímetro, monitoreo, alarmas y acceso presentan un nivel moderado. Aunque existen medidas implementadas, aún se detectan limitaciones y exposiciones relevantes.

Fortalezas:

- Controles básicos presentes.
- Infraestructura física parcialmente protegida.

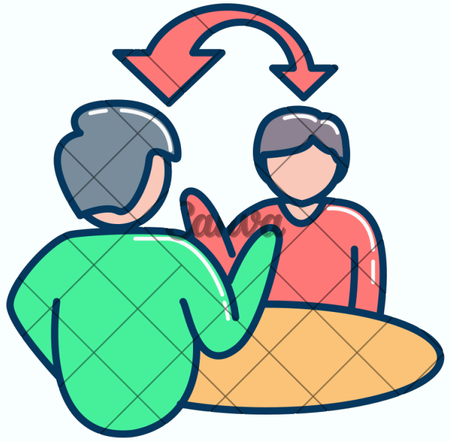
Áreas de mejora:

- Mayor integración con sistemas de seguridad electrónica.
- Mejorar alarmas, vigilancia y respuesta a incidentes.



RIESGOS IDENTIFICADOS

- Información sensible expuesta.
- WiFi sin control ni segmentación.
- Cámaras y equipos en la misma red.
- Sin verificación de identidad.
- Sin protocolos de contingencia ni destrucción segura.
- Controles físicos mínimos y sin monitoreo.
- Privacidad y manejo de datos débiles.



RECOMENDACIONES

1.- Fortalecer la seguridad tecnológica

2.- Capacitación del personal

3.- Monitoreo y alertas

4.- Procedimientos operativos claros

5.- Revisión periódica de riesgos

CONCLUSIONES

La auditoría técnica aplicada al consultorio 903 de la New City Medical Plaza, siguiendo la metodología OSSTMM, permitió obtener una visión clara del estado actual de la seguridad en sus componentes humanos, físicos, inalámbricos, de telecomunicaciones y de red. El análisis permitió identificar vulnerabilidades relevantes y valorarlas mediante la matriz RAV, lo que facilitó priorizar los riesgos según su impacto real en la operación del consultorio. Con base en estos resultados se establecieron recomendaciones orientadas a fortalecer los controles existentes y elevar el nivel de protección de la información manejada, contribuyendo a una operación más segura y alineada con buenas prácticas de seguridad informática.

REFERENCIAS

Herzog, P. (2003). OSSTMM 2.1: Manual de la Metodología Abierta de Testeo de Seguridad. Instituto para la Seguridad y las Metodologías Abiertas (ISECOM).

Caballé, X. (2003, noviembre). Versión en castellano de la metodología OSSTMM

v2.1 y metodología para el análisis de redes inalámbricas. Una Al Día. https://unaaldia.hispasec.com/2003/11/version-en-castellano-de-la-metodologia-osstmm-v2-1-y-metodologia-para-el-analisis-de-redes-inalambricas.html Una Al Día

Elsevier. (s. f.). Open Source Security Testing Methodology Manual. In ScienceDirect Topics. https://www.sciencedirect.com/topics/computer-science/open-source-security-testing-methodology-manual

RESEARCH. (2024). https://www.isecom.org/research.html

Diciembre 2025

MUCHAS
GRACIAS

Auditoría de la Seguridad Informática

ITT