



# telecom

**BANCO DE LA NACION ARGENTINA**

Pentest (Pruebas de Intrusión)

Informe Ejecutivo

22/05/2025

## Tabla de Contenidos

Objetivos .....	3
Alcance .....	3
Resumen .....	4
Hallazgos .....	5
Conclusiones .....	6
Recomendaciones Generales .....	7
Actividades Realizadas .....	8
Anexo 1: Metodología.....	9

## Objetivos

El objetivo del proyecto consiste en el descubrimiento y posterior ejecución de un **Pentest (Pruebas de Intrusión)** sobre la infraestructura de **BANCO DE LA NACION ARGENTINA** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **21/04/2025** y el **05/05/2025**.

## Alcance

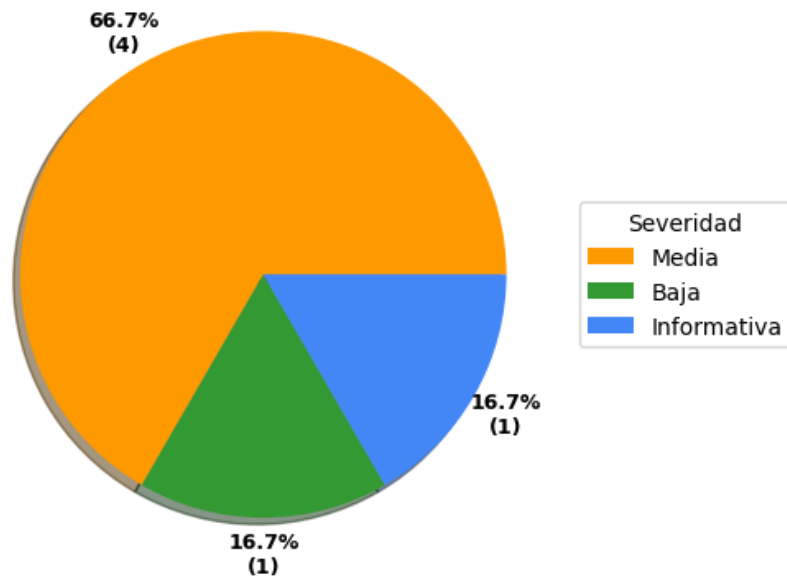
Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Pentest (Pruebas de Intrusión).

**<https://digitaltest.bna.com.ar>**

## Resumen

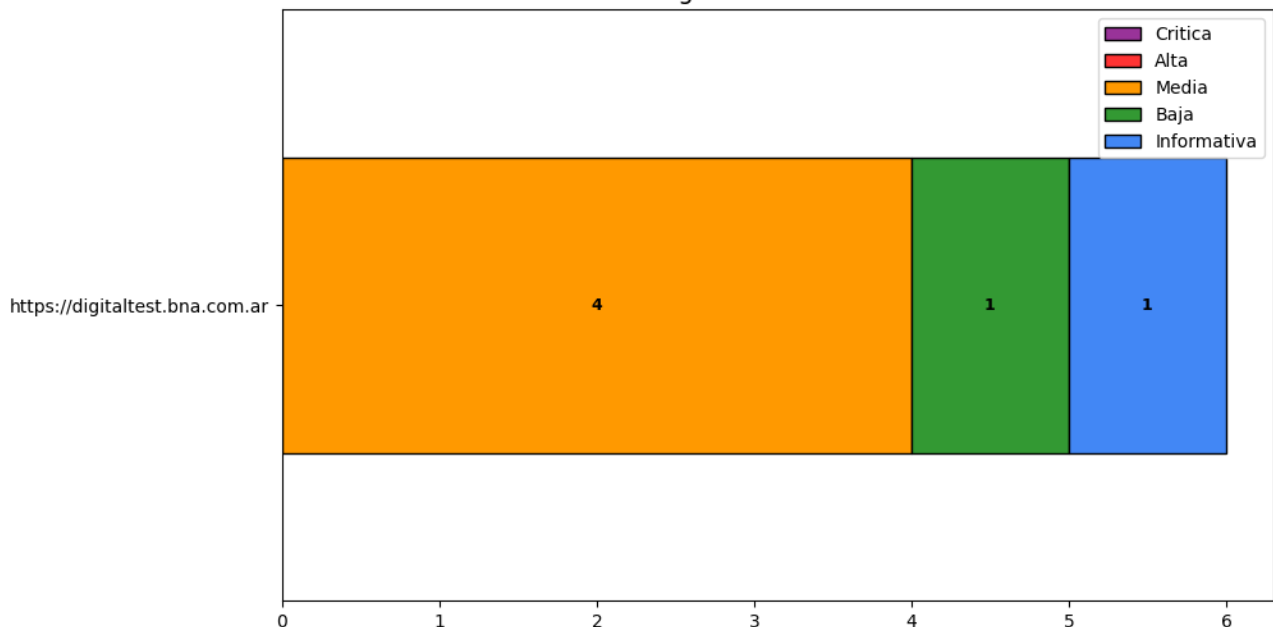
Como resultado del análisis se han identificado **6** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **4** de severidad media, **1** de severidad baja y **1** de carácter informativo.

Vulnerabilidades por Severidad



En el siguiente gráfico se pueden observar los activos afectados que cuentan con mayor cantidad de vulnerabilidades detectadas.

Ranking de Activos Afectados



## Hallazgos

En el siguiente listado se pueden visualizar las vulnerabilidades detectadas en el presente análisis clasificadas por Severidad.

#ID	Nombre	Severidad	Hosts Afectados
#1	Key Management: Hardcoded Encryption Key	Media	1
#2	Information disclosure	Media	1
#3	Debug Enabled For App	Media	1
#4	Frameable response (potential Clickjacking)	Media	1
#5	LUCKY13 – TLS CBC Timing Side-Channel Attack	Baja	1
#6	Data Exposure After Authentication	Informativa	1

## Conclusiones

En base a las vulnerabilidades detectadas y el análisis de las mismas, se puede determinar el siguiente nivel de severidad general, dada la existencia de 4 vulnerabilidades con dicha severidad.

Nivel de Severidad	Media
--------------------	-------

A continuación se ofrece un listado de acciones recomendadas para mejorar la postura de seguridad del sistema y reducir el riesgo de explotación:

Acciones Recomendadas
Priorizar la remediación según la clasificación de riesgo.
Desarrollar un plan de acción para implementar la recomendación o remediación.
Realizar un análisis de la causa raíz.
Realizar entrenamiento de concientización.
Realizar el manejo de excepciones y la aceptación de riesgos para las vulnerabilidades que no se pueden remediar.
Volver a realizar el análisis de vulnerabilidades para identificar si las soluciones aplicadas son eficaces para remediar las vulnerabilidades expuestas.
Tener en cuenta las soluciones y referencias recomendadas en cada vulnerabilidad expuesta en este informe.

En base a los resultados obtenidos durante el análisis, se ofrecen las siguientes sugerencias de remediación para abordar y mitigar las vulnerabilidades identificadas:

Sugerencia de Remediación	Vulnerabilidad Abordada
Dejar de publicar a Internet servicios que no se encuentren en uso o sean innecesarios.	#2 Information disclosure

## Recomendaciones Generales

Más allá de los hallazgos obtenidos a través del análisis realizado, resulta crucial establecer un enfoque holístico y multicapa en ciberseguridad. Las recomendaciones que proponemos buscan reforzar su infraestructura de TI y promover una cultura de seguridad resiliente, alineada con las tendencias y prácticas avanzadas del sector, adaptándose así a las dinámicas de un panorama digital que no cesa de cambiar. Recomendamos:

- **Visibilidad, detección y respuesta** : La habilidad para detectar y responder con celeridad a los incidentes de seguridad es fundamental. Contar con un servicio de SOC asegura que esté siempre un paso adelante de los riesgos potenciales.
- **Fortalecimiento de la Infraestructura de Red** : Los puntos débiles identificados en su red pueden fortalecerse de manera significativa a través de Firewalls de última generación y soluciones de seguridad para endpoints. Estas tecnologías son cruciales para una defensa perimetral robusta y ofrecen una protección proactiva contra una variedad de amenazas.
- **Capacitación y Conciencia de Seguridad** : Fomentar la conciencia sobre seguridad entre el personal es esencial, ya que los usuarios informados son la primera línea de defensa. Los programas de formación pueden disminuir de manera significativa el riesgo de brechas de seguridad al educar a los usuarios sobre las mejores prácticas y políticas de seguridad.
- **Análisis Continuo de Vulnerabilidades** : Es vital realizar análisis de vulnerabilidades y pruebas de penetración de forma regular para identificar y mitigar proactivamente las nuevas vulnerabilidades. Esta práctica garantiza la solidez y la adaptabilidad de su infraestructura frente a las amenazas emergentes.
- **Evaluaciones regulares** : Es vital realizar evaluaciones regulares, mantener la seguridad operativa de las plataformas y hardening de los firewalls para protección contra intrusiones. El cumplimiento de los estándares de seguridad es esencial, al igual que revisar los controles de seguridad IT y practicar una gobernanza y gestión de riesgos efectivas. Además, planes de crisis preparados son clave para una respuesta ágil y minimizar impactos en el negocio. Finalmente, tener planes de gestión de crisis bien desarrollados y probados asegura una respuesta rápida y eficaz ante incidentes imprevistos, mitigando los daños y preservando la continuidad del negocio.

Estas recomendaciones están pensadas para ser integradas dentro de un enfoque estratégico de seguridad, garantizando que no solo se atiendan los puntos débiles actuales, sino que también se establezca una base sólida para la seguridad futura. Nuestro equipo de expertos en ciberseguridad está listo para asesorar y apoyar la implementación de estas soluciones, asegurando que su empresa se mantenga a la vanguardia en protección y cumplimiento.

En Telecom, entendemos los desafíos intrincados de la ciberseguridad y estamos equipados para apoyar su empresa en cada paso del camino. Con nuestro portafolio integral y un equipo de profesionales experimentados, nos dedicamos a ayudarlo a alcanzar y mantener una postura de seguridad que no solo responda a las amenazas actuales, sino que también se anticipe y adapte a los riesgos del mañana.

## Actividades Realizadas

Las actividades que se realizaron para el presente análisis se separaron en las etapas descriptas a continuación:

### **Etapas 1: Reconocimiento y Enumeración**

En esta etapa se recopiló información sobre los activos informados en el alcance, incluyendo la identificación de rangos de IP, dominios, servidores, y cualquier información pública disponible. La enumeración implica descubrir y mapear activos, servicios y aplicaciones en la red para conformar la superficie de ataque. También se utilizó inteligencia de fuentes abiertas (OSINT) para complementar y ampliar la información obtenida.

### **Etapas 2: Análisis de Vulnerabilidades**

Se utilizaron diferentes herramientas de análisis manual para identificar y evaluar los servicios brindados y el tráfico de red en el sistema objetivo. Este proceso puede incluir análisis de código, análisis de vulnerabilidades, y evaluación de configuraciones de seguridad. El objetivo es identificar debilidades que podrían ser explotadas por un atacante.

A continuación se listan algunas de las debilidades buscadas, sin ser el presente un listado exhaustivo:

- Detección de vulnerabilidades conocidas asociadas a la versión de software de los servicios instalados.
- Verificación de vulnerabilidades conocidas sobre el sistema operativo de base instalado.
- Detección de falta de actualizaciones (parches).
- Detección de errores de configuración o configuraciones predeterminadas.
- Utilización de algoritmos de cifrado inseguros, o ausencia de cifrado.
- Exposición de información.
- Tratamiento incorrecto de entradas manipuladas por el usuario (XSS, Inyección de comandos o código, etc)
- Detección de falencias en el proceso de autenticación.
- Errores en manejo de sesiones de usuario.
- Posibilidad de generar ataques de fuerza bruta.
- Credenciales predeterminadas o conocidas.
- Control de acceso inadecuado o inexistente.

### **Etapas 3: Modelado de Amenazas**

Se utilizaron todos los datos recopilados en las fases anteriores para determinar la posibilidad de explotación. Se determinó el riesgo de las vulnerabilidades descubiertas durante esta fase utilizando principalmente la National Vulnerability Database (NVD), creada y mantenida por el gobierno de EE.UU. que analiza las vulnerabilidades de software publicadas en la base de datos Common Vulnerabilities and Exposures (CVE). La NVD clasifica la gravedad de las vulnerabilidades utilizando el Sistema de Puntuación de Vulnerabilidades Comunes (CVSS). Esta etapa se complementó con verificaciones manuales sobre estos equipos a fin de eliminar los “falsos positivos” y corroborar las detecciones.

### **Etapas 4: Explotación**

En esta etapa se intentaron explotar las vulnerabilidades identificadas para evaluar la resistencia del sistema a ataques reales. Se buscó determinar si las contramedidas de seguridad eran efectivas y si las vulnerabilidades podían ser explotadas con éxito para validar la profundidad y el alcance de las mismas.

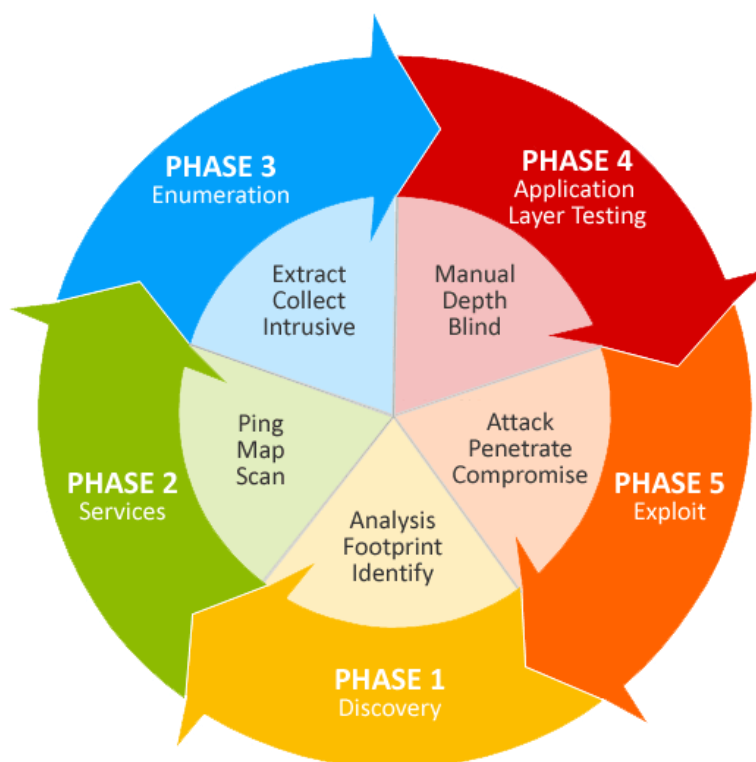
### **Etapas 5: Informes**

Una vez finalizadas las etapas de análisis, se generó un informe ejecutivo con un resumen gerencial de los hallazgos y equipos detectados, junto a un informe técnico donde se describen las vulnerabilidades, detallando el nivel de riesgo asociado, el impacto que estas pudieran tener en la seguridad, las recomendaciones de solución correspondientes, evidencia de las mismas y toda información adicional que fuera considerada útil para su identificación y corrección.



## Anexo 1: Metodología

El enfoque utilizado se basa en el Manual de Metodología de Pruebas de Seguridad de Código Abierto (OSSTMM), e incluye una combinación de pruebas automatizadas (cuando es posible) y de inspección manual (cuando sea necesario) de los servicios expuestos. El OSSTMM es un estándar ampliamente reconocido y utilizado en la industria de la seguridad informática. Fue desarrollado y publicado inicialmente por el ISECOM (Institute for Security and Open Methodologies) en el año 2001. Proporciona un marco completo y estructurado para llevar a cabo pruebas de penetración y evaluación de la seguridad en sistemas, redes y aplicaciones.



OSSTMM proporciona una serie de escenarios de prueba, técnicas y herramientas para realizar evaluaciones exhaustivas de seguridad. Está diseñado para ser utilizado por profesionales de la seguridad, equipos de pruebas de penetración y auditores de seguridad para identificar vulnerabilidades, evaluar la efectividad de las políticas de seguridad y proporcionar recomendaciones para fortalecer la infraestructura de una organización. Gracias a su enfoque cuantitativo y en detalle, el OSSTMM ha sido adoptado por muchas empresas y organizaciones como una metodología confiable para mejorar la seguridad informática y proteger los activos críticos.

Por requerimiento del cliente, las pruebas debieron ejecutarse de manera manual, lo que limitó el uso de herramientas automatizadas o escaneos extensivos. Asimismo, si bien inicialmente se proporcionaron credenciales para la evaluación bajo un enfoque Gray Box, dichas credenciales dejaron de funcionar durante el transcurso del proyecto. Debido a ello, se continuó la ejecución bajo una modalidad Black Box.