



# telecom

## **BCRA BANCO CENTRAL DE LA REPUBLICA ARGENTINA**

Análisis de Vulnerabilidades

Informe Ejecutivo

08/09/2025

## 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 **Análisis de Vulnerabilidades** sobre la infraestructura de **BCRA BANCO CENTRAL DE LA REPUBLICA ARGENTINA** especificada en el alcance, con la finalidad de identificar debilidades y proponer las recomendaciones de remediación

Las actividades fueron realizadas entre el **07/07/2025** y el **11/07/2025**.

## Alcance

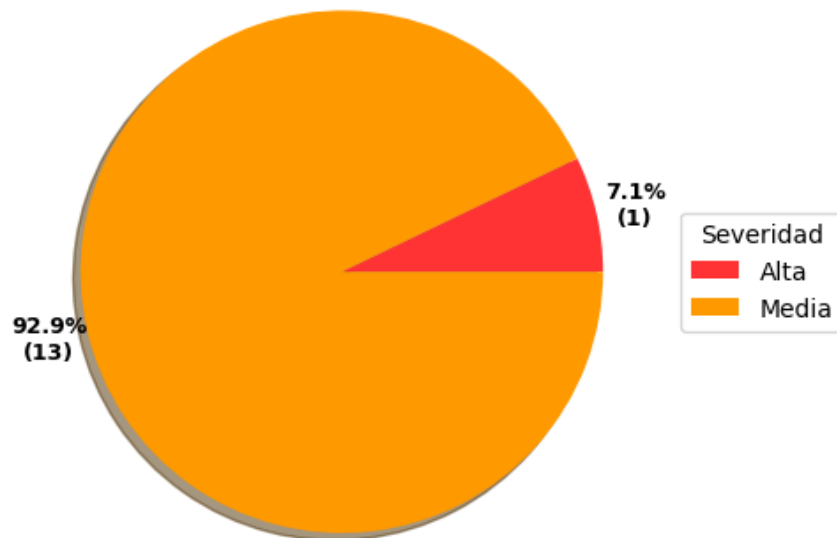
Las siguientes direcciones IP y/o URLs fueron suministradas para realizar una evaluación del tipo Análisis de Vulnerabilidades.

	45.235.96.40
45.235.96.101	45.235.96.44
45.235.96.103	45.235.96.50
45.235.96.104	45.235.96.53
45.235.96.108	45.235.96.58
45.235.96.109	45.235.96.64
45.235.96.110	45.235.96.8
45.235.96.111	45.235.96.9
45.235.96.117	45.235.97.1
45.235.96.118	45.235.97.100
45.235.96.151	45.235.97.101
45.235.96.158	45.235.97.108
45.235.96.160	45.235.97.109
45.235.96.169	45.235.97.150
45.235.96.18	45.235.97.152
45.235.96.201	45.235.97.169
45.235.96.21	45.235.97.201
45.235.96.25	45.235.97.25
45.235.96.253	45.235.97.253
45.235.96.27	45.235.97.26
45.235.96.28	45.235.97.28
45.235.96.29	45.235.97.40
45.235.96.31	45.235.97.53
45.235.96.35	45.235.97.7
45.235.96.36	45.235.97.8
45.235.96.4	

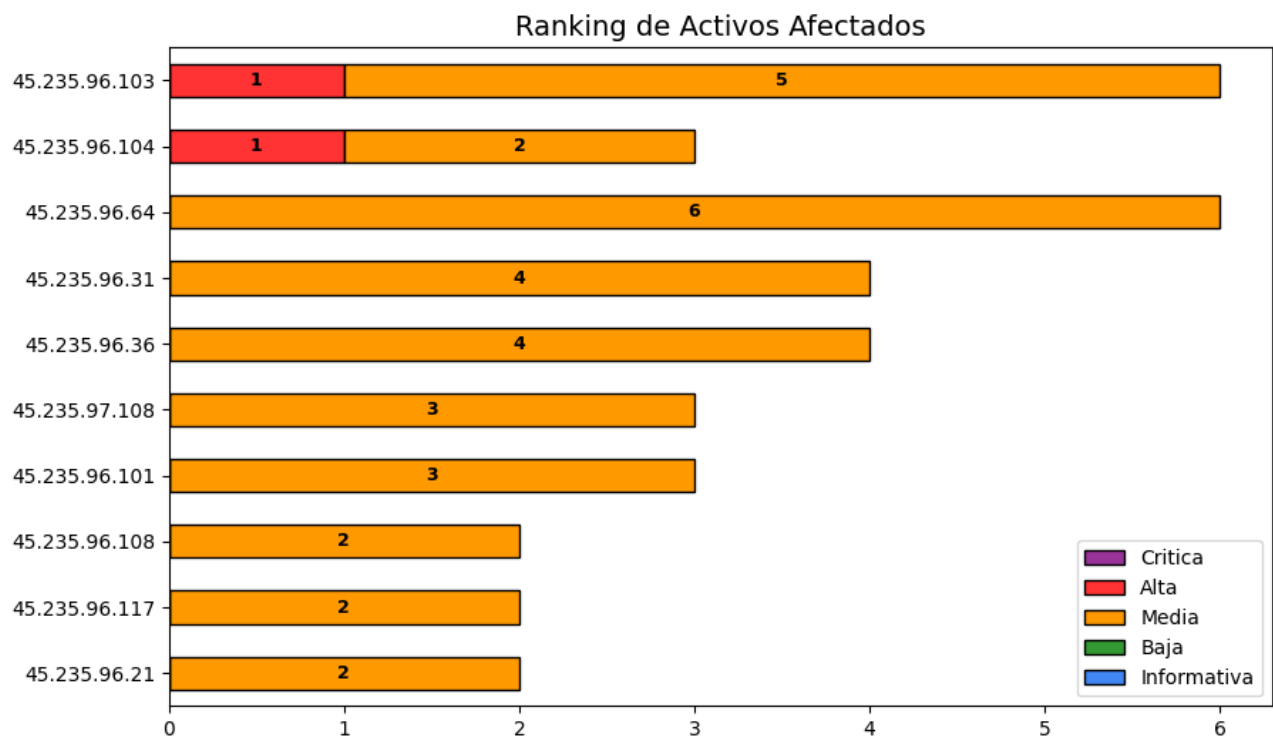
## Resumen

Como resultado del análisis se han identificado **14** vulnerabilidades, las cuales presentan la siguiente distribución en cuanto a su severidad: **1** de severidad alta y **13** de severidad media.

### Vulnerabilidades por Severidad



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



## Resumen de Hallazgos

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

#ID	Nombre del hallazgo	Severidad	Hosts Afectados
#1	EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected	Alta	2
#2	Incomplete SSL Certificate Chain Vulnerability	Media	35
#3	SSL Certificate - Invalid Maximum Validity Date Detected	Media	1
#4	SSL Certificate - Self-Signed Certificate	Media	1
#5	SSL Certificate - Signature Verification Failed Vulnerability	Media	2
#6	Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)	Media	2
#7	GIT Detected	Media	2
#8	Information disclosure	Media	6
#9	HTTP Security Header Not Detected	Media	6
#10	Account Brute Force Possible Through IIS NTLM Authentication Scheme	Media	2
#11	Deprecated Public Key Length	Media	1
#12	Microsoft ASP.NET Custom Errors Found Turned Off	Media	2
#13	Frameable response (potential Clickjacking)	Media	1
#14	Weak SSL/TLS Key Exchange	Media	1

## Conclusiones y recomendaciones finales

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

Acciones de Remediación	Severidad	Vulnerabilidad Abordada
Aplicar parches o actualizar el software obsoleto o con vulnerabilidades conocidas a las versiones recomendadas por los fabricantes.	Alto	#1 EOL/Obsolete Software: Microsoft Internet Information Services (IIS) 8.5 Detected
Configurar el servidor para enviar la cadena de certificados completa (incluyendo todos los intermedios necesarios hasta la CA raíz de confianza).	Medio	#2 Incomplete SSL Certificate Chain Vulnerability
Instalar un certificado que no exceda la validez máxima recomendada acorde a las buenas prácticas de seguridad.	Medio	#3 SSL Certificate - Invalid Maximum Validity Date Detected
Instalar un certificado de servidor firmado por una autoridad de certificado de terceros de confianza.	Medio	#4 SSL Certificate - Self-Signed Certificate
	Medio	#5 SSL Certificate - Signature Verification Failed Vulnerability
Deshabilitar el uso de protocolos (SSLv3, TLS1.0, TLS1.1) y algoritmos de cifrado considerados débiles o vulnerables (DES, 3DES, IDEA, CBC, RC2, RC4, MD5, SHA1), en favor de protocolos criptográficamente más fuertes.	Medio	#6 Secure Sockets Layer/Transport Layer Security (SSL/TLS) Server supports Transport Layer Security (TLSv1.0)
	Medio	#14 Weak SSL/TLS Key Exchange
Eliminar o restringir el acceso al directorio .git en entornos productivos.	Medio	#7 GIT Detected
Dejar de publicar a Internet servicios que no se encuentren en uso o sean innecesarios.	Medio	#8 Information disclosure
Configurar el servidor web para utilizar todos los encabezados de seguridad HTTP acordes a las buenas prácticas de seguridad.	Medio	#9 HTTP Security Header Not Detected
Configurar los servicios utilizados de acuerdo a las buenas prácticas y recomendaciones de seguridad indicadas por los fabricantes.	Medio	#10 Account Brute Force Possible Through IIS NTLM Authentication Scheme
Utilizar claves públicas de longitudes consideradas seguras (mínimo 2048 bits)	Medio	#11 Deprecated Public Key Length

## 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 descritas 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 determinar la superficie de ataque.

### **Etapas 2: Detección de Vulnerabilidades**

Se utilizaron herramientas automatizadas para identificar y evaluar vulnerabilidades en los sistemas auditados. Este proceso puede incluir análisis de código, escaneo de vulnerabilidades, y evaluación de configuraciones de seguridad. El objetivo es identificar debilidades que podrían ser explotadas por un atacante.

A continuación se listan algunos de los elementos buscados, 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.

### **Etapas 3: Análisis de Resultados**

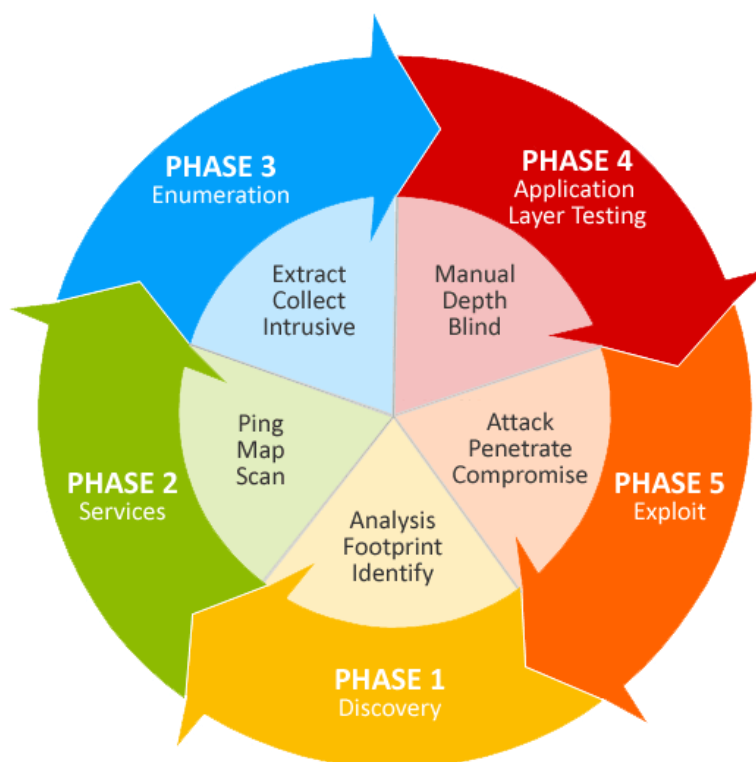
Se realizó un análisis detallado de las vulnerabilidades detectadas con verificaciones manuales, a fin de eliminar los “falsos positivos”, corroborar las detecciones y obtener la evidencia necesaria.

### **Etapas 4: 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, destacando el impacto que estas pudieran tener en la seguridad, las recomendaciones de solución correspondientes, evidencia de las mismas y toda información asociada necesaria 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.

Si bien se trata de un proceso mayoritariamente manual, durante el análisis se utilizaron una serie de herramientas automatizadas que permitieron disminuir los tiempos necesarios para la finalización de las tareas, como así también permitieron la manipulación del tráfico enviado a los servicios analizados.