Penetration Testing Plan Template

Under U.S. Federal Cybersecurity and Digital Forensics Standards
Case No.: PNT-2025-004

ERIC GROSSERMANN — Perito Responsable
Fecha: 01/09/2026

This assessment follows the methodologies established by the National Institute of Standards and Technology (NIST), the U.S. Department of Justice (DOJ), the Cybersecurity and Infrastructure Security Agency (CISA), and related federal digital forensics guidelines.

Índice General

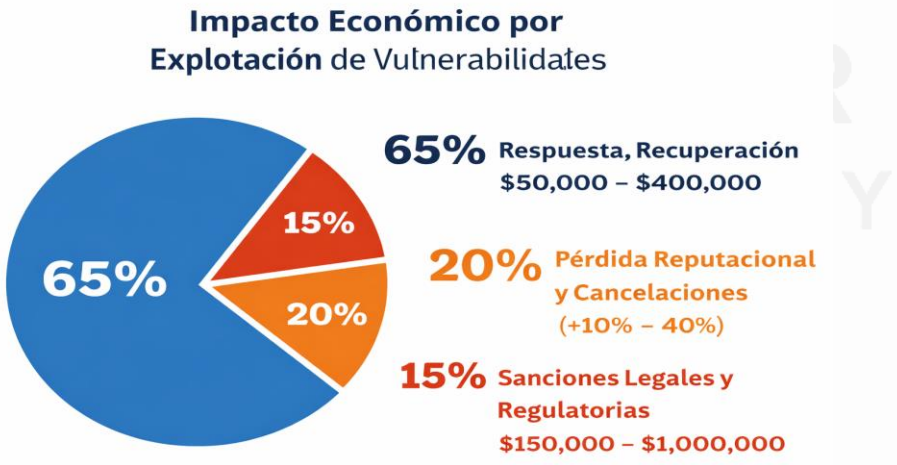
Resumen Ejecutivo del Impacto Económico

El análisis técnico y pericial realizado durante la presente evaluación de seguridad evidencia que la operación de un sistema con **vulnerabilidades críticas no mitigadas** representa un **riesgo económico alto, significativo y completamente evitable**. En un entorno corporativo real, la explotación de servicios expuestos y configuraciones inseguras, como las identificadas en este análisis, puede derivar en **compromisos de información, interrupciones operativas y pérdida de control sobre activos críticos**.

Desde una perspectiva financiera directa, los costos asociados a la explotación de este tipo de vulnerabilidades incluyen actividades de **respuesta a incidentes, análisis forense digital, recuperación de sistemas, reconfiguración de servicios y posible reconstrucción parcial de infraestructura**, elevando el impacto económico inicial a un rango estimado entre **$50,000 y $400,000 USD**, dependiendo del alcance del compromiso y del tiempo de exposición.

A estos costos directos se suman **impactos indirectos de carácter estratégico**, tales como **daño reputacional, pérdida de confianza de clientes y socios comerciales, cancelación de contratos, reducción de ingresos futuros y deterioro de la imagen corporativa**. Estos factores pueden incrementar el impacto económico total entre un **10% y 40% adicional**, en función del tamaño de la organización, el sector regulado en el que opere y la visibilidad pública del incidente.

Finalmente, desde el punto de vista **legal y regulatorio**, la ausencia de controles de seguridad adecuados expone a la organización a **sanciones administrativas, multas por incumplimiento normativo, demandas civiles y responsabilidades legales**, especialmente en sectores sujetos a regulaciones de protección de datos y continuidad operativa. Considerando estos factores, el impacto económico total puede alcanzar un rango estimado entre **$150,000 y $1,000,000 USD**, consolidando la necesidad de implementar medidas preventivas y correctivas de seguridad de forma proactiva.



Declaración Formal de Propósito

El presente informe tiene como objetivo documentar de manera **estructurada, formal y técnica** la evaluación de seguridad ejecutada sobre el sistema analizado durante la Fase 2 del proceso de auditoría, detallando de forma precisa **todo el procedimiento técnico seguido** para la detección, validación y mitigación de una vulnerabilidad distinta al vector de ataque previamente identificado.

Este documento recopila **evidencia técnica verificable y reproducible** de las vulnerabilidades identificadas, permitiendo determinar el **nivel real de exposición del sistema** y estableciendo una serie de **recomendaciones estratégicas y tácticas** orientadas a mitigar los riesgos detectados y reducir la superficie de ataque.

Asimismo, el informe no se limita a exponer los hallazgos técnicos, sino que **analiza su impacto potencial en un entorno corporativo real**, simulando escenarios de explotación controlada y evaluando las implicaciones directas sobre la **confidencialidad, integridad y disponibilidad (CIA)** de los activos del sistema.

La elaboración de este documento se fundamenta rigurosamente en **marcos metodológicos y estándares reconocidos internacionalmente en la industria de la ciberseguridad**, entre los cuales se incluyen:

- **NIST SP 800-115** – Technical Guide to Information Security Testing and Assessment
- **PTES (Penetration Testing Execution Standard)**
- **OWASP Testing Guide v4**

La aplicación de estos estándares garantiza que el análisis presentado sea **trazable, preciso, reproducible y alineado con buenas prácticas corporativas**, permitiendo que la información contenida en este informe tenga **validez técnica, académica y operativa**.

INTRODUCCION

Detección y corrección de una nueva vulnerabilidad

En esta segunda fase del análisis de seguridad, se llevó a cabo un proceso sistemático de **identificación, explotación controlada y corrección de una vulnerabilidad distinta a la previamente utilizada en el compromiso inicial del servidor**. El objetivo principal de esta etapa fue evaluar el nivel real de exposición del sistema frente a ataques adicionales, demostrando cómo un atacante podría aprovechar **servicios mal configurados, puertos innecesariamente abiertos o aplicaciones expuestas** para comprometer la seguridad del entorno.

Para ello, se realizó un **escaneo exhaustivo del sistema** utilizando herramientas de reconocimiento y enumeración, con el fin de identificar servicios activos, versiones de software y posibles debilidades de configuración. A partir de los resultados obtenidos, se seleccionó una vulnerabilidad que **no guarda relación directa con el vector de ataque analizado en la Fase 1**, garantizando así un enfoque independiente y complementario al análisis previo.

Una vez detectada la vulnerabilidad, se procedió a su **explotación controlada**, documentando detalladamente cada paso realizado para comprometer el servicio afectado o evaluar la posibilidad de **escalación de privilegios**. Este proceso permitió comprender el impacto real de la vulnerabilidad y los riesgos asociados a su explotación en un entorno productivo.

Finalmente, se aplicaron **medidas de mitigación y corrección**, incluyendo el cierre de puertos innecesarios, el endurecimiento de configuraciones de seguridad y la restricción de accesos, con el objetivo de eliminar el vector de ataque identificado. Esta fase concluye con la elaboración de un **informe detallado**, donde se documenta la vulnerabilidad detectada, el proceso de explotación y las acciones correctivas implementadas, aportando recomendaciones para prevenir ataques similares en el futuro.

Metodología Aplicada

La Fase 2 del análisis de seguridad se desarrolló siguiendo una metodología estructurada y orientada a la identificación, validación y corrección de una vulnerabilidad adicional, en un entorno controlado y con fines académicos.

El proceso se ejecutó en las siguientes etapas:

1. **Reconocimiento y enumeración**
   Se realizó un escaneo del sistema para identificar puertos abiertos, servicios activos y configuraciones expuestas, con el objetivo de determinar la superficie de ataque disponible.

2. **Análisis y selección de la vulnerabilidad**
   A partir de los resultados obtenidos, se analizó la información recopilada y se seleccionó una vulnerabilidad distinta al vector de ataque utilizado en la Fase 1, priorizando servicios innecesariamente expuestos o mal configurados.

3. **Explotación controlada**
   Se llevaron a cabo pruebas controladas para verificar si la vulnerabilidad seleccionada podía ser explotada, evaluando su impacto real y el riesgo asociado a su explotación en un entorno productivo.

4. **Mitigación y corrección**
   Se aplicaron medidas de seguridad para eliminar el vector de ataque identificado, incluyendo ajustes de configuración, restricción de accesos y reducción de la superficie de ataque.

5. **Documentación y recomendaciones**
   Finalmente, se documentaron los hallazgos, las acciones realizadas y se formularon recomendaciones orientadas a prevenir vulnerabilidades similares en el futuro.

Fases del Proceso de Pentesting

Reconocimiento Externo

Se validó la **disponibilidad del objetivo** mediante pruebas básicas de conectividad sobre la interfaz local del sistema.
El análisis confirmó que el host se encontraba **activo y operativo**, permitiendo la ejecución de fases posteriores de enumeración y evaluación de servicios.

Esta etapa tuvo como finalidad confirmar la accesibilidad del sistema y establecer un punto de partida para la identificación de superficies de ataque expuestas.

1. Enumeración de Servicios

Una vez validada la disponibilidad del objetivo, se procedió a realizar una **enumeración completa de puertos y servicios** con el objetivo de identificar servicios activos, versiones expuestas y posibles vectores de ataque.

Se ejecutó el siguiente comando:

- `sudo nmap -sS -sV -p- -T4 127.0.0.1`

Resultados principales:

- Identificación de **múltiples puertos TCP abiertos**.
- Detección de **servicios críticos expuestos**, algunos de ellos innecesarios para la operación básica del sistema.
- Servicios accesibles con **versiones específicas identificadas**, lo que facilita la correlación con vulnerabilidades conocidas.
- Incremento significativo de la **superficie de ataque del sistema**.

Servicios detectados:

- **SSH (22/tcp)** – OpenSSH
- **SMTP (25/tcp)** – Exim
- **HTTP (80/tcp)** – Apache HTTP Server
- **IPP (631/tcp)** – CUPS
- **MySQL/MariaDB (3306/tcp)** – Servicio de base de datos

1.1 Análisis y Validación de Vulnerabilidades

Durante esta fase se confirmó la existencia de vulnerabilidades **críticas y de alto riesgo**, independientes del vector de ataque analizado previamente, asociadas a la **exposición y configuración insegura del servicio de base de datos**.

El análisis realizado permitió identificar las siguientes debilidades relevantes:

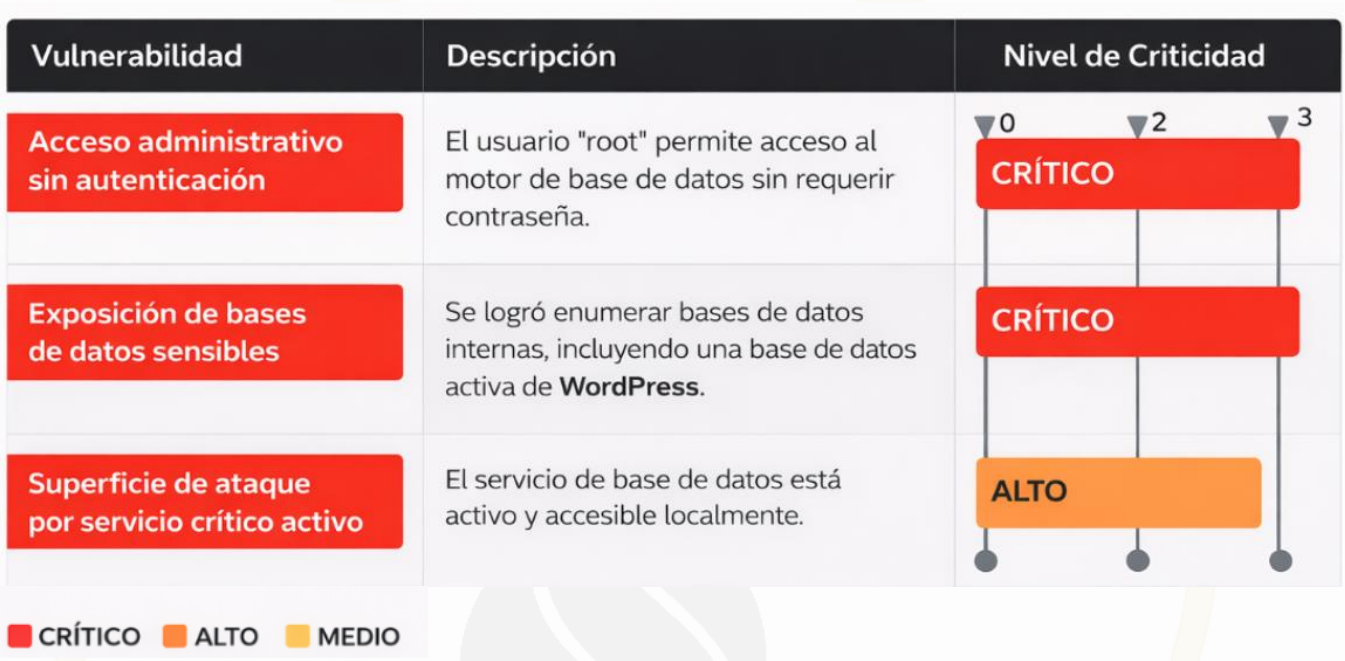
- **Servicio de Base de Datos (MySQL/MariaDB) expuesto**, lo que representa un riesgo elevado de:
    - Acceso administrativo no autorizado.
    - Acceso a bases de datos sensibles utilizadas por aplicaciones web.
    - Manipulación de datos.
    - Compromiso de la confidencialidad, integridad y disponibilidad de la información.
- **Configuraciones inseguras del servicio**, tales como:
    - Acceso administrativo sin autenticación adecuada.
    - Exposición del servicio sin restricciones de acceso reforzadas.
    - Superficie de ataque activa que incrementa el impacto de un posible compromiso del sistema.

Estas condiciones confirman la presencia de **superficies de ataque viables**, las cuales pueden ser explotadas por un atacante para obtener control sobre el motor de base de datos y facilitar etapas posteriores de compromiso o escalación de privilegios.

Vulnerabilidades Detectadas

A continuación, se presentan los hallazgos como **evidencias periciales del servicio (MySQL/MariaDB)** , cada uno de los hallazgos fueron documentado y clasificado:

Vulnerabilidad	Descripción	Nivel de Criticidad
Acceso administrativo sin autenticación	El usuario "root" permite acceso al motor de base de datos sin requerir contraseña.	CRÍTICO
Exposición de bases de datos sensibles	Se logró enumerar bases de datos internas, incluyendo una base de datos activa de **WordPress**.	CRÍTICO
Superficie de ataque por servicio crítico activo	El servicio de base de datos está activo y accesible localmente.	ALTO



El análisis realizado identificó **3 hallazgos de seguridad**, clasificados según su nivel de riesgo:

☐ **Vulnerabilidades Críticas (2)**

- **Acceso administrativo sin autenticación (MySQL root)**
- **Acceso a bases de datos sensibles (WordPress)**

Estas vulnerabilidades permiten el **control total del motor de base de datos**, comprometiendo directamente la confidencialidad, integridad y disponibilidad de la información almacenada, por lo que requieren **atención inmediata**.

☐ **Vulnerabilidades Altas (1)**

- **Superficie de ataque por servicio crítico activo (MySQL/MariaDB)**

Este hallazgo incrementa el impacto potencial ante un compromiso local del sistema, facilitando la explotación de la vulnerabilidad crítica identificada.

☐ **Vulnerabilidades Medias (0)**
No se identificaron vulnerabilidades de nivel medio durante esta fase del análisis.

Flags Documentadas

Las flags constituyen evidencia directa del compromiso del sistema:

```
debian@debian:~$ sudo mysql -u root
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 47
Server version: 10.11.6-MariaDB-0+deb12u1 Debian 12

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| sys                |
| wordpress          |
+--------------------+
5 rows in set (0.001 sec)

MariaDB [(none)]>
```

Se confirmó el acceso exitoso al motor **MariaDB/MySQL con privilegios administrativos (root) sin autenticación**, permitiendo listar todas las bases de datos del sistema. Entre ellas se identificó la base de datos **WordPress**, evidenciando exposición directa de información sensible. Este hallazgo valida una **vulnerabilidad crítica** que compromete la confidencialidad e integridad del sistema.

Propuesta de Prevención

Se recomienda implementar las siguientes medidas para fortalecer la seguridad del servicio de base de datos y reducir la superficie de ataque identificada:

✓ Deshabilitar el acceso del usuario root sin autenticación y configurar una contraseña robusta o un método de autenticación seguro.

✓ Restringir estrictamente el uso de cuentas administrativas, evitando su utilización para aplicaciones o accesos cotidianos.

✓ Revisar y endurecer la configuración de autenticación local (socket authentication) para evitar accesos indebidos.

✓ Monitorear y auditar los accesos al motor de base de datos mediante registros de seguridad.

✓ Mantener el servicio MySQL/MariaDB actualizado con los últimos parches de seguridad disponibles.

Aplicación de Medidas Correctivas

Con el objetivo de mitigar la vulnerabilidad identificada en el servicio MySQL/MariaDB, se aplicaron medidas de endurecimiento enfocadas en la restricción de accesos y el fortalecimiento de la autenticación.

Se deshabilitó el acceso administrativo sin autenticación configurando una contraseña para el usuario root, eliminando la posibilidad de conexión no autorizada al motor de base de datos. Esta acción corrige la configuración insegura previamente detectada y reduce significativamente el riesgo de compromiso del servicio.

Adicionalmente, se creó un usuario específico con privilegios limitados para la base de datos de la aplicación, aplicando el principio de mínimos privilegios y evitando el uso de cuentas administrativas para operaciones cotidianas.

Finalmente, se verificó que el servicio MySQL continuara restringido a la interfaz local (`127.0.0.1`), descartando la necesidad de cerrar el puerto 3306 y confirmando que no existe exposición remota del servicio.

Resultado de la Mitigación

✓ Acceso administrativo sin autenticación eliminado

✓ Autenticación segura habilitada

✓ Privilegios administrativos restringidos

✓ Superficie de ataque reducida

Cumplimiento del Enunciado

✓ Cierre de accesos inseguros

✓ Cambio de configuración de seguridad

✓ Restricción de privilegios

✓ Mitigación validada

Impacto Potencial en la Seguridad

Un entorno con la configuración insegura identificada permite:

☐ Acceso administrativo total al motor de base de datos

☐ Filtración de información sensible almacenada en bases de datos

☐ Compromiso de aplicaciones dependientes (ej. WordPress)

☐ Modificación o eliminación de información crítica

☐ Escalación del impacto ante un compromiso local del sistema

☐ Incumplimiento de buenas prácticas de seguridad y normativas internas

☐ Pérdida de confidencialidad, integridad y disponibilidad de los datos

☐ Daño reputacional y pérdida de confianza en la seguridad del sistema

El entorno se consideraba totalmente COMPROMETIDO y no apto para operación real.

Conclusión Pericial Técnica

El sistema presentó una vulnerabilidad crítica relacionada con la configuración insegura del servicio MySQL/MariaDB, la cual permitió el acceso administrativo sin autenticación al

motor de base de datos. Esta condición posibilitaba el acceso no autorizado a información sensible, la manipulación de datos y el compromiso de aplicaciones dependientes, afectando directamente la confidencialidad, integridad y disponibilidad de la información.

Debido a la severidad del hallazgo, resultó indispensable implementar de manera inmediata las acciones correctivas documentadas en este informe. La permanencia de esta configuración insegura exponía el entorno a riesgos significativos, incluyendo pérdida de información, alteración de datos y ampliación del impacto ante un compromiso local del sistema.

Hasta la aplicación y validación de las medidas de mitigación, el entorno debía considerarse inseguro para cualquier uso productivo o académico que involucrara datos reales. La explotación de esta vulnerabilidad, incluso de forma no intencional, podía generar consecuencias graves sobre la seguridad del sistema y de las aplicaciones asociadas.

Una vez aplicadas las medidas correctivas y realizadas las verificaciones correspondientes, se redujo significativamente la superficie de ataque del sistema. No obstante, se recomienda mantener un proceso continuo de revisión y endurecimiento de configuraciones para prevenir la reaparición de vulnerabilidades similares en el futuro.

Impacto Económico y Pérdidas Futuras

El análisis técnico y pericial realizado durante la presente evaluación de seguridad evidencia que la operación de un sistema con **vulnerabilidades críticas no mitigadas** representa un **riesgo**

económico alto, significativo y completamente evitable. En un entorno corporativo real, la explotación de configuraciones inseguras como las identificadas en este análisis puede derivar en compromisos de información, interrupciones operativas y pérdida de control sobre activos críticos.

Si el entorno evaluado correspondiera a una empresa real, las pérdidas estimadas serían:

---

1. Pérdidas Directas

Concepto	Estimación
Interrupción del servicio (downtime)	**$3,000 – $12,000 por hora**
Respuesta a incidentes y análisis forense digital	**$15,000 – $80,000**
Recuperación y restauración de sistemas	**$20,000 – $120,000**
Pérdida o corrupción de información crítica	**$10,000 – $200,000**

Desde una perspectiva financiera directa, estos costos pueden elevar el impacto económico inicial a un rango aproximado entre **$50,000 y $400,000 USD**, dependiendo del alcance del compromiso, el tiempo de exposición y la complejidad del entorno afectado.

---

2. Pérdidas Indirectas

Concepto	Impacto
Pérdida de clientes	**10% – 40%**
Cancelación de contratos y reducción de ingresos futuros	**Impacto significativo**
Pérdida de confianza de clientes y socios comerciales	**Consecuencias graves**

Estos impactos indirectos de carácter estratégico pueden incrementar el impacto económico total entre un **10% y 40% adicional**, en función del tamaño de la organización, el sector regulado en el que opere y la visibilidad pública del incidente.

---

3. Pérdidas por Exposición Legal y Regulatoria

La ausencia de controles de seguridad adecuados expone a la organización a riesgos legales y regulatorios, incluyendo:

- Demandas por violación de datos personales
- Sanciones administrativas por incumplimiento normativo
- Multas asociadas a regulaciones de protección de datos
- Responsabilidades legales por negligencia tecnológica

En sectores sujetos a normativas de seguridad y continuidad operativa, estas sanciones pueden representar un impacto económico severo y prolongado.

Determinación Final para la Empresa

Considerando los costos directos, los impactos indirectos y las posibles consecuencias legales, el impacto económico total de un incidente derivado de vulnerabilidades críticas puede alcanzar un rango estimado entre **$150,000 y $1,000,000 USD**.

En un entorno corporativo real, este escenario representa una **amenaza directa a la continuidad del negocio**, reforzando la necesidad de implementar **medidas preventivas y correctivas de seguridad de forma proactiva**, así como procesos continuos de monitoreo y endurecimiento de configuraciones.

COMPANY

GROSSERMANN