**INFORME DE ANÁLISIS PREVENTIVO ANTE INCIDENTES DE SEGURIDAD**

# 1. Introducción

Este informe presenta un análisis preventivo ante incidentes de seguridad basado en el entorno comprometido de una máquina Debian utilizada como ejercicio práctico en el proyecto final de ciberseguridad. El objetivo es anticipar posibles vectores de ataque y fortalecer la postura de seguridad antes de que se materialicen amenazas, basándose en las vulnerabilidades reales detectadas en el análisis.

# 2. Identificación de Riesgos Potenciales

- Acceso anónimo al servidor FTP con posibilidad de escritura.  
- Credenciales débiles en MySQL y almacenamiento de contraseñas en texto plano.  
- Servicio SSH con autenticación por contraseña y posibilidad de login como root.  
- Permisos inseguros en archivos de configuración sensibles (ej. wp-config.php).  
- Directorios web accesibles y listables desde el navegador.  
- Credenciales guardadas automáticamente en el navegador.  
- Software desactualizado con CVEs conocidos (vsFTPd, WordPress).

# 3. Evaluación del Impacto

La combinación de configuraciones inseguras, contraseñas débiles y servicios expuestos sin medidas de protección representa un alto riesgo de:  
- Ejecución remota de código (RCE).  
- Filtración de información sensible.  
- Acceso no autorizado al backend de WordPress.  
- Persistencia del atacante dentro del sistema.  
- Pérdida o manipulación de datos críticos.  
- Reputación comprometida ante terceros o clientes en un entorno real.

# 4. Recomendaciones Preventivas

- Deshabilitar accesos anónimos y servicios no utilizados como FTP.  
- Aplicar hardening del sistema: restringir permisos, desactivar root en SSH, cambiar puertos por defecto.  
- Implementar autenticación por clave pública y 2FA.  
- Aplicar cifrado en transmisiones y almacenamiento (SSL/TLS, backups cifrados).  
- Utilizar gestores de configuración para mantener versiones seguras y estandarizadas.  
- Monitorear continuamente con herramientas como Wazuh para detectar comportamientos anómalos.  
- Planificar auditorías mensuales y simulacros de incidentes.  
- Capacitación del personal técnico en prácticas de seguridad y respuesta inmediata.

# 5. Conclusión

La anticipación y mitigación temprana de vulnerabilidades son claves para mantener un entorno seguro. Este informe, basado en el análisis detallado del entorno Debian comprometido, evidencia la necesidad de adoptar una postura de defensa activa y continua. Las recomendaciones aquí planteadas deben integrarse dentro de un SGSI efectivo para asegurar la resiliencia y continuidad operativa ante amenazas cada vez más sofisticadas.