**INFORME DE ANÁLISIS DE SEGURIDAD**

**Estudiante: Jonathan Agustin Alay Muñoz**

**Asignatura: Control y Auditoría Informática**

**Docente: Ing. Jorgue Rubio**

**Fecha: 20/05/2025**

**Sitio Analizado: https://cutuglagua.gob.ec**

# 1. OBJETIVO

**Evaluar de forma ética y pasiva el nivel de seguridad visible del portal web institucional del GAD Municipal de Cutuglagua, utilizando herramientas libres disponibles en Kali Linux, sin realizar pruebas intrusivas o ilegales.**

# 2. HERRAMIENTAS UTILIZADAS

**- Wappalyzer / BuiltWith: Identificación de tecnologías.  
- SSL Labs (Qualys): Evaluación del certificado SSL/TLS.  
- SecurityHeaders.com: Verificación de encabezados HTTP de seguridad.  
- WhatWeb (Kali Linux): Análisis superficial del servidor y CMS.  
- Inspección Manual (navegador): Análisis de código fuente.**

# 3. RESULTADOS OBTENIDOS

## 3.1 Tecnologías Detectadas (WhatWeb)

**Comando ejecutado:  
whatweb https://cutuglagua.gob.ec  
  
- Servidor Web: Apache/2.4.18 (Ubuntu)  
- Lenguaje Backend: PHP 7.0.33 (obsoleto)  
- CMS Detectado: Joomla  
- Sistema Operativo: Linux (probablemente Ubuntu)  
  
Comentario: El uso de Joomla en una versión sin identificar junto con PHP 7.0 es preocupante, ya que esta versión de PHP está fuera de soporte desde enero 2019.**

## 3.2 Certificado SSL (SSL Labs)

**- El certificado es válido y emitido por Let's Encrypt.  
- Fuerza del cifrado: Aceptable (usa TLS 1.2 y 1.3, pero permite TLS 1.0, lo cual es inseguro).  
- Calificación general: B  
  
Comentario: Aunque el certificado es válido, debería deshabilitar versiones antiguas de TLS por seguridad.**

## 3.3 Encabezados HTTP (SecurityHeaders.com)

**Resultado al visitar: https://securityheaders.com/?q=https%3A%2F%2Fcutuglagua.gob.ec  
  
- Content-Security-Policy: No definido  
- X-Frame-Options: No definido  
- Strict-Transport-Security: No definido  
- X-XSS-Protection: ✅ Parcial  
- X-Content-Type-Options: No definido**

## 3.4 Análisis de Código Fuente

**- Comentarios visibles como <!-- template Joomla -->  
- Rutas internas tipo /templates/gk\_news2/css/  
- No hay minificación de código (HTML/CSS sin compactar)  
  
Comentario: Exponer nombres de plantillas o rutas internas puede dar pistas a atacantes sobre vulnerabilidades específicas.**

# 4. RIESGOS DETECTADOS

**1. Uso de versiones obsoletas de PHP y CMS.  
2. Falta de encabezados HTTP de seguridad.  
3. Exposición de información del servidor (Apache, versión exacta).  
4. Comentarios y rutas visibles en el código fuente.  
5. Posibilidad de enumeración del CMS Joomla.**

# 5. RECOMENDACIONES

**1. Actualizar PHP al menos a la versión 8.1.  
2. Actualizar Joomla y extensiones a su última versión.  
3. Configurar encabezados HTTP como CSP, HSTS, X-Frame-Options.  
4. Minificar archivos y eliminar comentarios internos en HTML.  
5. Deshabilitar la visualización de versiones del servidor.**

# 6. CONCLUSIONES

**El sitio web analizado muestra vulnerabilidades pasivas importantes debido al uso de tecnologías desactualizadas y malas prácticas de seguridad. Aunque no se ha realizado ningún tipo de ataque, se recomienda a la entidad reforzar su infraestructura para evitar futuros incidentes.  
  
Este análisis fue realizado con fines exclusivamente académicos, sin realizar pruebas invasivas, respetando los principios éticos y legales de la carrera de Ingeniería en Sistemas de Información.**