



TLP: AMBER

Análisis de vulnerabilidades

Impacto: Alto
Credibilidad y Confianza: A1
Sector de Infraestructura Crítica: todos los componentes y sistemas tecnológicos que forman parte de la red y operación de una organización.
Tipo de Reporte: Operacional

Tipo de incidente:
Entidad evaluada:
Dominio afectado:
URL específica:
Tipo de spam:
Críticidad:
Estado actual:
Indicadores detectados:

Emitido por:

Fecha emisión:
Referencia:

SEO Spam / Defacement encubierto (Pharma Hack)
Bucaramanga (comentarios)
www.bucaramanga.gov.co
https://www.bucaramanga.gov.co
Pharma (replica rolex)
Alta
ACTIVO ●
4 keywords spam detectados en HTML (indonesio, pharma)
COLCERT-MinTIC — Equipo de Respuesta a Incidentes
08/06/2026 Bogotá
COLCERT-REV-20260608-SEOSPAM-BUCARAMANGAC

1. Resumen del Hallazgo

El sitio web institucional www.bucaramanga.gov.co continúa comprometido con SEO Spam (Pharma (replica rolex)). En la revalidación del 08/06/2026 se confirma que el spam sigue ACTIVO: se detectan 4 ocurrencias de keywords de spam en el HTML. Es urgente iniciar acciones de remediación.

El atacante está utilizando la reputación del dominio institucional .gov.co para posicionar contenido publicitario malicioso (apuestas online, casinos, juegos de azar, productos farmacéuticos sin licencia, según el tipo detectado) en los resultados de búsqueda. Esta técnica se conoce como 'Pharma Hack' o 'Japanese SEO Spam' y es uno de los vectores de defacement más comunes en sitios basados en CMS desactualizados (WordPress, Joomla, Drupal).

2. Evidencia Técnica

Indicador técnico

URL específica comprometida
Tipo de SEO Spam detectado
Código HTTP servido a Googlebot
Tamaño del HTML servido (bytes)
Keywords spam contadas
Estado actual del compromiso

Valor observado

https://www.bucaramanga.gov.co
Pharma (replica rolex)
200
770.778
4 ocurrencias en el HTML
ACTIVO ●

3. Impacto sobre la Entidad

El compromiso del sitio institucional con SEO Spam genera múltiples impactos negativos:

- Reputacional: el dominio institucional .gov.co aparece en resultados de búsqueda asociado a contenido publicitario ilegal (apuestas, casinos, productos farmacéuticos no autorizados).
- Pérdida de posicionamiento SEO: Google penaliza activamente los sitios comprometidos, reduciendo su visibilidad y mostrando advertencias "Este sitio podría haber sido vulnerado".
- Posibilidad de listado en Google Safe Browsing: si Google detecta el compromiso de forma persistente, marca el sitio como peligroso y los navegadores muestran advertencias rojas al visitarlo.
- Indicador de compromiso más amplio: el SEO Spam suele ser síntoma de un compromiso de mayor alcance — el atacante ya tiene acceso de escritura al servidor o a la base de datos del CMS.
- Riesgo de exfiltración de datos: si el atacante puede modificar el sitio, también puede acceder a información sensible almacenada (datos de ciudadanos, formularios, credenciales).
- Posible incumplimiento normativo: la Ley 1581 de 2012 (Habeas Data) y el Decreto 1078 de 2015 requieren protección de datos de los ciudadanos; un sitio comprometido viola dichos requisitos.

4. Acciones Inmediatas (0-72 horas)

1. Aislar el servidor: si es viable, mover el sitio detrás de mantenimiento o página en construcción mientras se investiga.
2. Backup inmediato del servidor completo: archivo y base de datos, antes de hacer cualquier limpieza.
3. Revisar logs del servidor web (Apache/Nginx/IIS) buscando: peticiones desde IPs sospechosas, accesos a /wp-admin, /administrator, /admin, archivos PHP modificados recientemente.
4. Buscar archivos PHP/HTML añadidos recientemente: ejecutar `'find /ruta/sitio -mtime -30 -type f'` para encontrar archivos modificados en los últimos 30 días.
5. Cambiar TODAS las contraseñas: admin del CMS, base de datos, cPanel/Plesk, FTP/SFTP. Usar contraseñas fuertes y únicas.
6. Cerrar accesos no esenciales: deshabilitar wp-admin de forma temporal, restringir SSH a IPs específicas.
7. Notificar a las áreas internas: oficina TIC, jefe inmediato, Oficina de Comunicaciones (para preparar respuesta pública).
8. Reportar el incidente a COLCERT-MinTIC (csirtgob@mintic.gov.co) con la referencia de este informe.

5. Acciones de Remediación (3-15 días)

1. Identificar el vector de entrada: revisar versiones del CMS (WordPress, Joomla, Drupal) y plugins. Buscar vulnerabilidades conocidas (CVE) en las versiones instaladas.
2. Actualizar el CMS y TODOS los plugins/themes a sus versiones más recientes. Eliminar plugins/themes inactivos.
3. Limpiar el código malicioso: revisar archivos comunes donde se inyecta SEO Spam — wp-content/themes/*/header.php, footer.php, functions.php; archivos .htaccess con redirecciones; tabla wp_options campo siteurl.
4. Eliminar TODAS las páginas spam encontradas: pueden estar como archivos sueltos en el filesystem o como entradas en la base de datos.
5. Verificar integridad de los archivos del CMS: comparar contra una instalación limpia del mismo CMS y versión. Cualquier diferencia debe ser investigada.
6. Restaurar desde backup limpio: si tienes un backup previo al compromiso, restaurar el sitio completo desde allí (después de aplicar todas las actualizaciones).
7. Implementar WAF (Web Application Firewall): Cloudflare gratuito, Sucuri, ModSecurity con reglas OWASP CRS.
8. Solicitar a Google la reindexación: usar Google Search Console — Solicitar revisión de seguridad, Solicitar eliminación de URLs spam de la caché.

6. Acciones Preventivas (1-3 meses)

1. Establecer política de actualización mensual de CMS, plugins, themes y librerías. Suscribirse a feeds de seguridad del vendor.
2. Implementar autenticación de dos factores (2FA) para TODOS los usuarios administrativos.
3. Habilitar monitoreo de integridad de archivos (FIM - File Integrity Monitoring) para detectar modificaciones no autorizadas.
4. Configurar respaldos automáticos diarios con retención de 30 días, almacenados fuera del servidor.
5. Implementar Web Application Firewall (WAF) corporativo con reglas activas (no solo modo alerta).
6. Suscribirse a Google Search Console y monitorear las alertas de seguridad de Google.
7. Realizar análisis de vulnerabilidades trimestral con herramientas como Tenable WAS, OWASP ZAP, o solicitar el servicio a COLCERT-MinTIC.
8. Capacitar al equipo técnico en OWASP Top 10 y secure coding.

7. Recomendación a la Alta Dirección

COLCERT-MinTIC ALERTA a la Alta Dirección de Bucaramanga (comentarios): el incidente de SEO Spam registrado en mayo de 2026 NO ha sido remediado. La revalidación del 08/06/2026 confirma que el spam sigue activo en el sitio institucional. Es URGENTE iniciar las acciones de remediación descritas en este informe y reportar el avance a COLCERT-MinTIC.

Se recomienda designar un responsable técnico que coordine las acciones de remediación con el apoyo del COLCERT-MinTIC, y reportar a la Alta Dirección el avance semanal del cierre del incidente hasta su resolución completa, incluyendo la solicitud de reindexación a Google para limpiar los resultados de búsqueda comprometidos.

NOTA: El COLCERT ofrece dentro de su portafolio de servicios la capacidad de ejecutar análisis especializados de vulnerabilidades en sitios web, servidores y otros activos de información. Este proceso tiene como objetivo identificar de manera proactiva brechas de seguridad, configuraciones deficientes y exposiciones críticas. Los hallazgos se consolidan en informes técnicos que permiten al equipo de TI implementar acciones de hardening, aplicar parches de seguridad y fortalecer la postura de ciberseguridad de los sistemas evaluados.

Canales de Atención

Si tiene alguna consulta técnica, puede comunicarse con CSIRT Gobierno de tratarse de una entidad del Estado, o con COLCERT si pertenece a cualquier otro sector de la economía, a través de los siguientes canales:

- Buzón de correo: contacto@colcert.gov.co / csirtgob@mintic.gov.co – Entidades de Gobierno -
- Línea directa: +57 601 344 2222
- Sitio web: <https://www.colcert.gov.co> @colCERT