Contrato de Autorización para Ejecución de Pruebas de Seguridad Informática (Pentesting)

No. de Contrato: PTAA-UC-RAIL-2026-001
Lugar y Fecha: Bogotá D.C., 15 de mayo de 2026
Propietarios del Sitio Web: - Luis Alberto Diuche, identificado con la cédula de ciudadanía No.1192802712 - David Eduardo Martínez, identificado con la cédula de ciudadanía No. 1034576055 - Elizabeth Pérez González, identificada con la cédula de ciudadanía No. 1025060768 - Sergio Numael Linares Ducuara, identificado con la cédula de ciudadanía No. 1239845239 Actuando en calidad de propietarios y desarrolladores del sitio web https://web-production-ff1b5.up.railway.app/
Equipo Auditor (Equipo de Seguridad): Los mismos individuos: Luis A. Diuche, David E. Martínez, Sergio N. Linares Ducuara y Elizabeth Pérez González, actuando como equipo interno de auditoría de seguridad en calidad de estudiantes de la asignatura de Hacking Ético (44391427) en la Universidad Central, bajo la supervisión del docente Carlos Ivan Pinzon Romero.
Dominio Autorizado (Sitio Web Auditado): https://web-production-ff1b5.up.railway.app/
Objeto del contrato: Autorizar al equipo de estudiantes de la Universidad Central a realizar una auditoría de seguridad ofensiva (pentesting) sobre el sitio web mencionado, con el fin de verificar vulnerabilidades de configuración, software y diseño, documentarlas y proponer remediaciones en el marco académico.

Declaramos y Acordamos:

Cláusula Primera - Objeto:

El presente contrato tiene por objeto otorgar autorización expresa, voluntaria e informada al Equipo Auditor para ejecutar pruebas de penetración (Penetration Testing / Ethical Hacking) sobre el sitio web identificado previamente, incluyendo su infraestructura de red, servicios web y aplicación WordPress, con fines exclusivamente académicos dentro de la asignatura de Hacking Ético (44391427). Ambas partes son copropietarias del sistema auditado y actúan en roles diferenciados de “Propietarios Autorizantes” y “Equipo Auditor”, con el fin de cumplir los requisitos éticos, metodológicos y legales del ejercicio académico.

Cláusula Segunda - Alcance Técnico Autorizado:
Las actividades autorizadas se limitan estrictamente a las que se detallan en la siguiente tabla:

#	Actividad Autorizada	Herramientas y Detalle Técnico
1	Reconocimiento pasivo y activo de red	Ping ICMP, Traceroute TCP/ICMP, nslookup, curl ipinfo.io
2	Escaneo de puertos y servicios	nmap -F / -sV / -A sobre el dominio objetivo
3	Consultas DNS y WHOIS	nslookup tipos A, MX, NS, TXT; búsqueda WHOIS del registrador (hostingersite.com)
4	Análisis de certificados SSL/TLS	openssl s_client -connect :443, SSLShopper online
5	Pruebas OWASP Top 10 – 2021 (A01–A10)	A01 a A10 aplicadas al sitio WordPress objetivo
6	Escaneo WordPress con WPScan	nikto sobre el dominio objetivo
7	Pruebas de inyección controladas	SQLMap (nivel 1-2) con --batch, solo sobre formularios del sitio objetivo
8	Análisis de cabeceras (headers) HTTP	curl -I, nikto sobre el dominio objetivo
9	Enumeración de directorios	gobuster, dirb
10	Fuerza bruta controlada	Hydra (máximo 10 intentos por usuario sobre formulario de login)

Dominio e IPs autorizados:

- Dominio principal: https://web-production-ff1b5.up.railway.app/
- IPs públicas asociadas al dominio (obtenidas mediante resolución DNS y confirmadas con ping y nslookup, subdominios).
- Rango permitido: únicamente la(s) IP(s) que resuelvan en el momento de la prueba.
- Período autorizado: 10 de mayo de 2026 – 20 de mayo de 2026
- Puertos autorizados: 80 (HTTP) y 443 (HTTPS).
- Horario de ejecución: De 06:00 a 22:00 (hora Colombia)

Métodos permitidos:

- Escaneo pasivo (ping, traceroute, nslookup, whois).
- Escaneo activo no intrusivo (nmap -sS, -sV, -A; nikto; wpscan).
- Consultas DNS (`nslookup`, `dig`, `whois`)

- Análisis de certificados SSL/TLS (`openssl s_client`, SSL Labs)
- Enumeración de directorios (`gobuster`, `dirb`)
- Escaneo de vulnerabilidades (`wpscan`, `nikto`)
- Pruebas controladas de inyección en formularios propios (sin modificar la base de datos).
- Fuerza bruta limitada a 10 intentos por usuario sobre el formulario de login, únicamente con credenciales de prueba del equipo.
- Verificación de configuraciones: cabeceras HTTP, archivos sensibles (.env, wp-config.php, xmlrpc.php, .git/).

Cláusula Tercera - Restricciones:

Queda expresamente y estrictamente **PROHIBIDO** al Equipo Auditor, bajo pena de nulidad del contrato y las responsabilidades legales correspondientes:

- Destruir, modificar, exfiltrar o eliminar datos del servidor o de la base de datos del sitio.
- Ejecutar ataques de Denegación de Servicio (DoS/DDoS) de cualquier tipo o magnitud.
- Compartir hallazgos, credenciales o información de infraestructura con terceros no autorizados, ni escalar privilegios sin autorización previa.
- Extender las pruebas a dominios, IPs o sistemas diferentes a los explícitamente autorizados en la Cláusula 2.
- Instalar backdoors, webshells, malware o cualquier artefacto persistente en el servidor.
- Ejecutar pruebas fuera del horario y fechas establecidas sin notificación previa escrita a los Propietarios.
- Intentar ataques de ingeniería social sobre usuarios reales del sitio web.
- No se explotarán vulnerabilidades más allá de la verificación de existencia (por ejemplo, no se ejecutará `sqlmap` con opciones peligrosas como `--dump`o --os-shell).
- Todo hallazgo será confidencial y solo se compartirá con el docente y los miembros del equipo y compañeros de la clase de Hacking.
- Los hallazgos se reportarán en un documento académico bajo normas APA.

Cláusula Cuarta - Confidencialidad y Uso de los Resultados:

Los hallazgos realizados durante la auditoría (vulnerabilidades, credenciales, datos de usuarios, arquitectura del sistema, etc.) serán utilizados únicamente para la elaboración del informe de pentesting que será entregado al Docente de la asignatura de Hacking Ético y evaluado junto con nuestros compañeros en clase y no serán divulgados a terceros sin el consentimiento explícito de todos los Propietarios; manteniendo un carácter estrictamente confidencial dado la sensibilidad de los datos. Queda prohibida su publicación en redes sociales, repositorios públicos o cualquier medio de comunicación (salvo los casos anteriormente mencionados).

Cláusula Quinta - Marco Legal Aplicable:

Las partes involucradas declaran conocer y comprometerse a actuar dentro del marco legal colombiano vigente, en particular: (a) Ley 1273 de 2009 - Delitos Informáticos correspondientes a la protección de la información y de los datos: sanciona conductas como el acceso no autorizado, interceptación de datos y daño informático; (b) Ley 1266 de 2008 – Habeas Data: regula el manejo de información personal contenida en bases de datos personales, en especial la financiera, crediticia y comercia y (c) Ley 1581 de 2012 – Protección de Datos Personales: establece disposiciones sobre el tratamiento de datos personales en Colombia. El incumplimiento de cualquiera de las cláusulas establecidas en el presente contrato por parte del equipo Auditor expone al infractor a las consecuencias penales establecidas en la normativa citada. Adicionalmente el equipo auditor se compromete a reportar de inmediato cualquier hallazgo que represente un riesgo crítico para la información del sitio.

Por último, los propietarios reconocen que el sitio es de su propiedad y que las pruebas se realizan con fines meramente educativos, académicos y formativos. E**l equipo de seguridad no se hace responsable por la interrupción temporal del servicio debido a escaneos autorizados** (por ejemplo: nmap -A).

Cláusula Sexta - Responsabilidad y Gestión de Incidentes:

El Equipo Auditor se compromete a: (a) detener inmediatamente cualquier prueba que genere impacto no previsto en el funcionamiento del sitio; (b) reportar de inmediato al Docente Supervisor cualquier hallazgo de Severidad CRÍTICA (CVSS $\geq$ 9.0); (c) no continuar con pruebas destructivas una vez identificada la vulnerabilidad; (d) restaurar cualquier configuración modificada de forma accidental. Los Propietarios eximen al Equipo Auditor de responsabilidad civil por daños resultantes del ejercicio normal de las pruebas autorizadas.

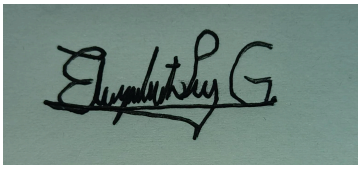
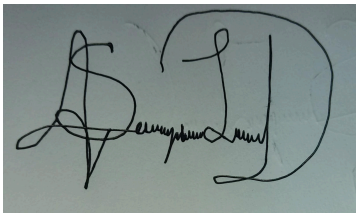
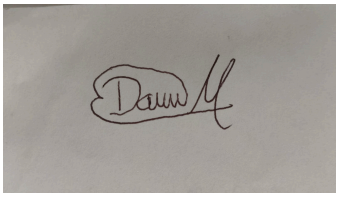
Cláusula Séptima - Vigencia:

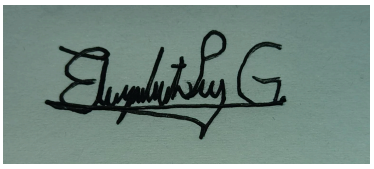
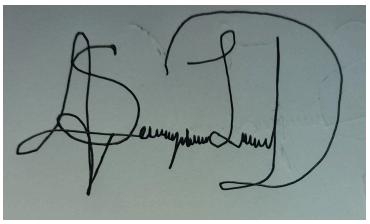
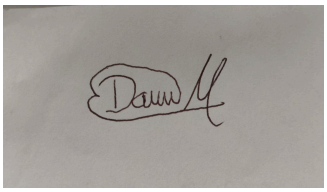
El presente contrato tiene vigencia desde el 10 de mayo de 2026 hasta el 20 de mayo de 2026. Cualquier extensión deberá ser acordada por escrito y firmada por las partes con mínimo 48 horas de anticipación.

Se estipula que por medio de la presente, nosotros, Luís Alberto Diuche Peña, David Eduardo Martinez Moya, Sergio Numael Linares Ducuara y Elizabeth Pérez González, estudiantes de noveno semestre del programa de Ingeniería de Sistemas de la Universidad Central, en calidad de propietarios y administradores del sitio web desarrollado en el marco de la asignatura Hacking Ético, autorizamos de manera expresa y voluntaria la ejecución de pruebas de seguridad informática (pentesting) acorde a todo lo estipulado en este contrato.

Firmas:

Luis Alberto Diuche Peña **Propietario/Autorizante**	David Eduardo Martínez Moya **Propietario/Autorizante**	Sergio Numael Linares Ducuara **Propietario/Autorizante**	Elizabeth Pérez González **Propietario/Autorizante**

Luis Alberto Diuche			
10 de abril de 2026	10 de abril de 2026	10 de abril de 2026	10 de abril de 2026

Luis Alberto Diuche Peña **Auditor/Pentester**	David Eduardo Martínez Moya **Auditor/Pentester**	Sergio Numael Linares Ducuara **Auditor/Pentester**	Elizabeth Pérez González **Auditor/Pentester**
Luis Alberto Diuche			
10 de abril de 2026	10 de abril de 2026	10 de abril de 2026	10 de abril de 2026