APC Colombia

ANEXO 2 “ALCANCE Y CONDICIONES TÉCNICAS”

CONTRATAR EL SERVICIO ESPECIALIZADO EN ETHICAL HACKING Y ANÁLISIS DE VULNERABILIDADES PARA LA EVALUACIÓN DE LA POSTURA DE SEGURIDAD DE LA AGENCIA PRESDIDENCIAL DE COOPERACIÓN INTERNACIONAL DE COLOMBIA, APC COLOMBIA

2025

Tabla de contenido

1. ALCANCE 3
1.1. Sede APC Colombia 3
1.2. Entregables 3
2. CONDICIONES TÉCNICAS DEL SERVICIO 3

1. ALCANCE

El servicio tiene por objeto evaluar la postura de seguridad de la APC-Colombia mediante pruebas de ethical hacking y análisis de vulnerabilidades sobre sus principales activos tecnológicos, identificando riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información, y generando recomendaciones técnicas para fortalecer el Sistema de Gestión de Seguridad de la Información conforme a la norma ISO/IEC 27001:2022.

1.1. Sede APC Colombia

Numero	Ubicación
Una sede Principal	Carrera 10 #97A - 13 Torre A - Piso 6, edificio Trade Center Bogotá D.C.

1.2. Entregables

Item	Entregables
1	Plan de ejecución de pruebas
3	Informe técnico
4	Documentación de buenas prácticas y plan de mejora continua

2. CONDICIONES TÉCNICAS DEL SERVICIO

CATEGORÍA	ESPECIFICACIONES / REQUERIMIENTOS
Alcance del servicio	• Realizar una (1) **prueba de Ethical Hacking controlada** sobre la infraestructura tecnológica crítica de APC Colombia. • Incluir la evaluación de hasta **10 activos principales** definidos por la entidad, (caja blanca). ▪ **Primer activo**: Pagina web https://www.apccolombia.gov.co/ ▪ **Segundo activo**: Intranet ▪ **Tercer activo**: Firewalls ▪ **Cuarto activo**: Sistema de información Ciclope (interno - externo). ▪ **Quinto activo**: Servicio de VPN. ▪ **Sexto activo**: Sistema de conocimiento. ▪ **Séptimo activo**: Sistema de gestión documental Hermes. ▪ **Octavo activo**: redes inalámbricas. ▪ **Noveno activo:** Servidor base de datos. ▪ **Decimo activo:** Servidore DNS primario. • Ejecutar **pruebas de penetración sobre redes inalámbricas (hasta 4 SSID críticos)** para verificar seguridad de autenticación, cifrado y segmentación. • Desarrollar un **análisis de vulnerabilidades integral** mediante herramientas automatizadas y validaciones manuales de especialistas. • Simular ataques externos (desde Internet) e internos (red corporativa) para validar escenarios reales de riesgo.
Metodología	• Aplicar el estándar internacional **PTES (Penetration Testing Execution Standard)** en todas las fases: planificación, recolección de información, modelado de amenazas, explotación y reporte. • Incorporar los lineamientos de **OWASP Top 10 y OWASP Testing Guide** en la revisión de aplicaciones web y APIs. • Emplear metodologías mixtas: **manuales (explotación dirigida por expertos)** y **automatizadas (escáneres profesionales con licencia)**. • Revisión alineada a estándares de cumplimiento como **ISO 27001, NIST SP 800-115, PCI DSS** (cuando aplique).

CATEGORÍA	ESPECIFICACIONES / REQUERIMIENTOS
Objetivos principales	• **Identificar vulnerabilidades críticas** que comprometan la confidencialidad, integridad y disponibilidad de la información. • **Evaluar la postura de seguridad actual** de APC Colombia frente a ciberataques avanzados. • **Simular ataques reales** externos e internos bajo técnicas comúnmente usadas por ciberdelincuentes. • **Priorizar acciones correctivas** basadas en criticidad, impacto y probabilidad de explotación. • **Cumplir con normativas y estándares** de ciberseguridad aplicables al sector público en Colombia. 6. **Proporcionar lineamientos estratégicos y técnicos** para el fortalecimiento continuo de la seguridad institucional.

Entregables	• - **Informe técnico completo**, con:
	  ○ Listado de vulnerabilidades encontradas.
	  ○ Evidencias técnicas de explotación.
	  ○ Clasificación de riesgo (crítico, alto, medio, bajo).
	  ○ Recomendaciones técnicas detalladas para mitigación
	• **Documentación de buenas prácticas y plan de mejora continua** adaptado al entorno de la entidad.

Plazo y vigencia	• Duración estimada de ejecución: **10 días hábiles.** • Entrega de resultados: máximo **10 días hábiles** posteriores a la finalización de las pruebas.
Condiciones técnicas mínimas del proveedor	• Empresa con experiencia comprobada en pruebas de intrusión y análisis de vulnerabilidades. - Equipo técnico conformado por **ingenieros certificados** (ej. CEH, OSCP, CISSP, ISO 27001 Lead Auditor/Implementer). • Uso de herramientas **con licencia vigente**. • Confidencialidad y cumplimiento de normativa local en protección de datos. • Capacidad de emitir informes en español, adaptados al contexto normativo colombiano.

VIJALBA CABALLERO WILLY ALEXANDER

Firmado digitalmente por VIJALBA CABALLERO WILLY ALEXANDER
Fecha: 2025.10.22 15:49:31 -05'00'

Fin del documento.