INDEPORTES ANTIOQUIA	**ANEXO I FICHA TÉCNICA**	Código:	F-CA-08
		Versión:	1
		Aprobación:	7/03/2019
Objeto:	*Prestación de servicios de Ethical Hacking para INDEPORTES ANTIOQUIA*		

1. CLASIFICACIÓN UNSPSC

Los servicios y/o ítems a adquirir están codificados en el clasificador de bienes y servicios UNSPSC como se indica a continuación.

A continuación se deberá relacionar la clasificación general de los bienes, obras y/o servicios que se pretenden adquirir.

Clasificación	UNSPSC	Segmento	Familia	Clase
Seguridad de los computadores, redes o internet	81111801	81000000	81110000	81111800
Servicio de análisis de sistemas	81111808	81000000	81110000	81111800

2. FÍCHA TÉCNICA

A continuación se relaciona la ficha técnica de cada uno de los bienes y/o servicios a contratar.

No. del Producto	1
Nombre del Producto	Pruebas de Ethical Hacking
Clasificación UNSPSC	81111801 - 81111808
Características	Se realizaran pruebas de ethical hacking y analisis de red sobre la infraestructura para identificar vulnerabilidades tecnicas; con base en los hallazgos, se emitiran recomendaciones priorizadas y, posteriormente, se efectuará un retest para verificar la efectividad de las medidas adoptadas y la mitigación del riesgo identificado. Superficie de ataque ASM: Identificación de activos y monitoreo de infraestructura. Análisis de Infraestructura: Evaluación e identificación de vectores de ataque. Hacking: Evaluación de aplicaciones para identificar vulnerabilidades. Explotación controlada: Pruebas ofensivas sin comprometer la disponibilidad. Análisis de impacto: Categorización de hallazgos y correlación de riesgos.

	Documentación:Informe técnico detallado y resumen ejecutivo. Se realizará 1 retest de las vulnerabilidades identificadas. FASE 1: Diagnóstico y Análisis de Vulnerabilidades. Se auditan los sistemas para descubrir, analizar y documentar todas las vulnerabilidades de seguridad existentes. Esta fase se centra en la ejecución de pruebas exhaustivas para identificar, clasificar y evaluar las debilidades de seguridad en la infraestructura y aplicaciones de la Entidad. **1. -Ethical Hacking:** - Ejecutar pruebas de penetración bajo las modalidades de Caja Negra (sin información interna) y Caja Gris (con conocimiento parcial) sobre los activos de información definidos. - Pentesting Web: Realizar pruebas sobre cuatro (4) aplicaciones web críticas: el portal institucional principal y tres portales adicionales (referidos como Lottired, Devoluciones y SID). - Pentesting de API: Evaluar la seguridad de las interfaces de programación de aplicaciones (APIs) de la organización. - Pentesting de Red Interna y Externa: Realizar pruebas sobre la infraestructura interna y externa, incluyendo componentes de red, servidores, equipos de cómputo, sistemas de usuario final, cámaras IP, impresoras, sistemas de telefonía VoIP y videoconferencia. Esto incluye el análisis de servicios expuestos como FTP, SSH, Telnet y SMTP. - Pentesting de Entornos Cloud: Ejecutar pruebas de penetración en los entornos de nube de la Entidad. **2. Escaneo de Infraestructura:** - Realizar actividades de captura de tráfico y pruebas de suplantación de identidad (Man-in-the-Middle). - Analizar la seguridad de las redes inalámbricas de la organización. - Analizar los controles de acceso a la red cableada. 3. Evaluación de superficie de ataque. Evaluación e identificación de vectores de ataque. 4. Inteligencia de Amenazas y fraude digital: - Realizar un estudio de filtraciones en la Deep Web y Darknet para detectar "fugas" de credenciales y exposición de datos confidenciales de la Entidad cliente. **Entregables de la Fase 1** a. Informe Técnico Detallado: - Descripción pormenorizada de las pruebas realizadas y sus resultados - Listado completo de vulnerabilidades detectadas, con su respectiva evidencia. - Referencias a las debilidades utilizando los estándares CWE (Common Weakness Enumeration) y CAPEC (Common Attack Pattern Enumeration and Classification). - Valoración de vulnerabilidades usando CVE (Common

	Vulnerabilities and Exposures). b. Informe Ejecutivo: - Descripción de alto nivel de las pruebas realizadas. - Análisis sobre el estado general de seguridad de la infraestructura y sitios web evaluados. - Resumen del número de vulnerabilidades identificadas, clasificadas por nivel de criticidad. - Conclusiones y recomendaciones claras para la corrección y mitigación de los hallazgos. c. Matriz de Hallazgos y Riesgos: - Una matriz técnica en formato “xlsx” con descripciones detalladas y priorización de las vulnerabilidades encontradas, recomendaciones claras de mitigación. - La matriz debe permitir la priorización efectiva de riesgos e identificar amenazas potenciales. - Un mapa de calor que represente visualmente los riesgos identificados según su nivel de criticidad. - Una matriz de criticidad que asocie el inventario de activos de información con su calificación de seguridad. FASE 2: Mitigación y ruta estratégica: Se crea la hoja de ruta estratégica para corregir las fallas encontradas, priorizando las acciones según el nivel de riesgo. 1. Ingeniería Social 2. Evaluación de fraude Digital 3. Plan de Remediación Esta fase consiste en la consolidación de los hallazgos de la Fase 1 en un plan de acción estratégico y táctico para la mitigación de los riesgos identificados. **Actividades:** a. Ingeniería Social: - Ejecutar una campaña de simulación de phishing controlada y personalizada para 100 usuarios (cuentas de correo electrónico). - Monitorear y realizar un análisis estadístico de los resultados de la campaña, evaluando tasas de apertura, clics y entrega de credenciales. - Elaborar recomendaciones claras y precisas para la corrección y mitigación de cada uno de los hallazgos documentados. - Diseñar y ejecutar un plan de evaluación de fraude digital. - Diseñar y documentar un plan de acción que defina la estrategia para tratar los riesgos identificados, con una priorización basada en su criticidad. - Generar recomendaciones de concientización en seguridad para el personal, basadas en los resultados de la campaña de phishing. **Entregables FASE 2** - Resumen Gerencial: Una sinopsis del estado general de la seguridad de las aplicaciones móviles y su impacto potencial en los usuarios y la organización.

	- Análisis de Criticidad: Gráficos y tablas que resumen el número de vulnerabilidades por su nivel de riesgo, facilitando la toma de decisiones - Conclusiones Estratégicas: Recomendaciones de alto nivel sobre mejoras en el ciclo de vida de desarrollo seguro (SSDLC) para aplicaciones móviles. b. Fraude Digital: Informe detallado de las actividades, recomendaciones y conclusiones del plan ejecutado de fraude digital. c. Informe de la Campaña de Phishing: Informes detallados con el análisis estadístico y los resultados de la simulación, con las recomendaciones específicas para mejorar la cultura de seguridad y reducir la vulnerabilidad humana ante ataques de ingeniería social d. Plan de Remediación Detallado: Un documento (en formato .xlsx según el contrato) que contenga la estrategia documentada, las acciones de corrección y mitigación, y la priorización de los hallazgos para su tratamiento.
Presentación	SERVICIO

3. ESPECIFICACIONES TÉCNICAS
Relacionar las demás condiciones que el proveedor deberá observar durante la ejecución del contrato:
Condiciones Generales y/o Particulares

El alcance del objeto comprende la ejecución de una evaluación integral de seguridad ofensiva de la superficie tecnológica, mediante pruebas de penetración internas y externas, bajo un enfoque de Red Team que simule tácticas, técnicas y procedimientos de actores maliciosos fin vulnerabilidades, validar controles defensivos y fortalecer la postura de ciberseguridad de la organización. Para esto el contratista debe ejecutar las siguientes actividades:

1. Ethical Hacking: Identificar vulnerabilidades en aplicaciones web.
2. Escaneo de Infraestructura: Identificar vulnerabilidades en servidores y servicios críticos.
3. Evaluación de superficie de ataque (ASM): Identificación de activos públicos, dominios y servicios expuestos.
4. Inteligencia de amenazas y fraude digital: Detección de amenazas y análisis de actores maliciosos.

La evaluación comprende el análisis e identificación de vulnerabilidades en la infraestructura tecnológica interna y externa de la organización, incluyendo:

Sistema de Gestión documental
Sharepoint
Office365
Microsoft TEAMS
Certilaboral
Sevidores Web (2)
Paginas Web (4)
Base de datos (4)
Controlador de Dominio
Cámaras (103)

Tipo de entrega, lugar y periodicidad:

Las pruebas se pueden realizar de forma remota al igual que la entrega de los resultados.

Líneas de Servicio al Cliente:

N/A

Facturación y Pago:

La Entidad pagará el valor total del contrato mediante un pago único, una vez se hayan entregado todos los informes y productos objeto del presente contrato, y presentación del informe de ejecución de actividades desarrolladas con su respectivo soporte, certificación del pago de la seguridad social, informe de supervisión y certificación en formato de calidad F-GF-09 de recepción a conformidad por parte del supervisor del contrato.

Reposición y/o ajuste de Productos:

N/A

Plazo:

El plazo del contrato será de dos (2) meses, contados a partir del inicio en la plaftaforma SECOP II, sin exceder el 31 de diciembre de 2025.

Garantías:

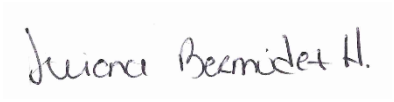
Cumplimiento de las obligaciones surgidas del Contrato Estatal.
Calidad del servicios.
Pago de salarios y prestaciones sociales, e indemnizaciones laborales.

Autorizaciones, permisos y licencias requeridos por el proveedor para la ejecución

Certificados de personal

4.LISTA DE PRODUCTOS

N.	Producto	Presentación	Cantidad
1	*Pruebas de Ethical Hacking*	*UNIDAD*	*1*



Juliana Bermúdez
Rol Técnico Oficina de Sistemas
Indeportes Antioquia