ANEXO TÉCNICO

REQUERIMIENTOS TÉCNICOS PARA CONTRATAR LOS SERVICIOS PARA REALIZAR LAS ACTIVIDADES DE ACOMPAÑAMIENTO, ACTUALIZACIÓN, Y MEJORA CONTINUA DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN DEL MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE DE CONFORMIDAD CON EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA POLÍTICA DE GOBIERNO DIGITAL**. Proceso de Selección Abreviada de Menor Cuantía Nro. SAMC-003-2021**

DESCRIPCIÓN GENERAL:

Este servicio debe contener como mínimo las siguientes fases las cuales deberán desarrollarse en paralelo acorde con el plan de pagos:

- **FASE 1:**

Análisis GAP de conformidad o cumplimiento con las normas ISO/IEC 27001:2013 e ISO 27032 y lo dispuesto por MinTIC mediante el MSPI (Resolución 500 de marzo 10 de 2021, ANEXO 1 Modelo de Seguridad y Privacidad de la Información - Documento Maestro del Modelo de Seguridad y Privacidad de la Información Versión 4 del 22 de febrero de 2021), Directiva Presidencial No. 03 de 15 de marzo de 2021 sobre lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos.

- **FASE 2:**

Desarrollo del marco documental de gobierno digital en Sistemas de Información, Seguridad de la Información y Ciberseguridad.

Levantamiento, actualización e implementación del SGSI

- **FASE 3:**

Pruebas Técnicas de Ciberseguridad: Ethical Hacking, Análisis de Vulnerabilidades y Revisión de Código

- **FASE 4:**

Capacitación a funcionarios del Ministerio de Ambiente.

Planificar y ejecutar el acompañamiento para evidenciar el cumplimiento de los controles al nivel de madurez y brecha de acuerdo con la herramienta de Evaluación MSPI en las siguientes entidades adscritas al Ministerio: ANLA, IDEAM y Parques Nacionales.

FASES	REQUERIMIENTOS TÉCNICOS
FASE 1: Análisis de brecha	Debe incluir: • Análisis del recurso humano existente para soportar las actividades relacionadas con seguridad, incluyendo sesiones de trabajo para lograr un entendimiento preliminar de los procesos del negocio. • Evaluación del hardware, software y comunicaciones con que cuenta el MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE • Evaluación de los sistemas de información actuales. • Análisis de las políticas, procesos y procedimientos y demás documentación relacionada con el SGSI. • Análisis de brechas de seguridad informática de acuerdo a los requerimientos de seguridad exigidos por los marcos de control y buenas prácticas ISO 27001:2013 e ISO 27032:2012. • Generación ROAD MAP del MSPI y de Ciberseguridad para la Entidad y matriz de madurez de controles implementados en el Ministerio actualmente.
FASE 2: Levantamiento, actualización implementación	Debe incluir: Levantamiento, actualización e implementación del Marco Documental de la Entidad, alineado con: MSPI, Resolución 500/2021 de MINTIC, e ISO 27001:2013, MIPG y Sistema Integrado de Gestión del Ministerio. La documentación mínima requerida contiene los siguientes aspectos: • Gestión de riesgos • Plan de seguridad de la información • Compromiso de la alta gerencia • Políticas de seguridad. • Estructura organizacional • Gestión de activos y clasificación de la información • Gestión de incidentes de seguridad de la información. • Seguridad relacionada con los recursos humanos. • Políticas de Continuidad de negocio. • Cumplimiento y conformidad con la legislación vigente. • Control de acceso físico y lógico • Adquisición, desarrollo y mantenimiento de sistemas de información • Gestión de operaciones y comunicaciones (incluye gestión de servicios en la nube). • Criptografía • Integridad de datos y confidencialidad. • Seguridad física y del entorno de los servicios centrales. (Centros de cómputo y oficinas) Entregables fases 1 y 2:

	– Metodología de administración de riesgos ajustada a las necesidades de la entidad, de acuerdo con las normas ISO 31000, ISO 27005 recientes y en concordancia con la metodología de Riesgos del DAFP y sus anexos sobre lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas. – Gestión de Activos – Levantamiento de Procedimientos – Análisis de Riesgos – Plan de Tratamiento de Riesgos (PTR) – Resultados de las entrevistas de análisis de riesgos – Mapa de riesgos. – Modelo del SGSI / Políticas del SGSI / Construcción de Controles del SGSI.
FASE 3: **Pruebas de ciberseguridad ethical hacking, análisis de vulnerabilidades y revisión de código**	Contratar como servicio pruebas técnicas de Ciberseguridad: Ethical Hacking, Análisis de Vulnerabilidades y Revisión de Código, sobre la arquitectura tecnológica perteneciente a MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE. A continuación, se describen las especificaciones requeridas: **ENTREGABLES de las pruebas Técnicas de Ciberseguridad** **Fases 3:** • Generar informe detallado con los resultados obtenidos (Informe Técnico). • Generar Informe ejecutivo a alto nivel (Informe Ejecutivo). • Generar plan de remediaciones de los hallazgos encontrados. • Generar Informe ejecutivo a alto nivel con los resultados obtenidos en el Re-Test (Informe Ejecutivo Re- Test) **ETHICAL HACKING Y ANÁLISIS DE VULNERABILIDADES** ● **ALCANCE:** 200 activos de información pertenecientes al Ministerio, Incluye Re-TEST ● **LEVANTAMIENTO DE INFORMACIÓN:** Realización de test de intrusión tanto externo como interno, tales pruebas deben ser en modalidad Blackbox. ● **ACTIVIDADES:** Verificación de la efectividad de los controles establecidos a nivel externo e interno, sometiéndose a prueba con técnicas diseñadas para vulnerar la seguridad. Análisis estático y dinámico de código en donde se espera la inspección

directa de la fuente u objeto codificado que describe el sistema con respecto a la semántica del código.

El proveedor deberá utilizar herramientas licenciadas y avaladas por la Common Weakness Enumeration (CWE) y Common Vulnerabilities and Exposures (CVE), para el proceso de gestión de vulnerabilidades. Determinar los falsos positivos y los falsos negativos. Atacar los objetivos seleccionados, utilizando las vulnerabilidades descubiertas. Probar la existencia real de las vulnerabilidades encontradas para determinar el impacto de estas. El proveedor debe implementar una herramienta licenciada para la explotación de vulnerabilidades.

El proveedor debe simular todos los ataques que sean convenientes según el tipo de objetivo a probar, en coordinación con el supervisor designado para el contrato. Entre ellos se mencionan algunos de los más importantes (lista de referencia, no limitativa):

- · Enumeración de la red
- · Reconocimiento de la red
- · Enumeración y explotación de Wi-Fi
- · Enumeración y explotación de Bluetooth
- · Cross Site script
- · Ataques al Browser
- · Keylogger
- · Cracking de contraseñas
- · Sniffing.
- · Ataques de denegación de servicio.
- · Identificación de vulnerabilidades de perímetro.
- · Identificación de las debilidades de la arquitectura, revisión de las zonas de la red y criterios de conformación.
    - · Ataques man-in-the-middle
    - · Re-direccionamiento IP
    - · Comprobación de la seguridad de los equipos de los proveedores de comunicaciones
    - · SQL Injection
    - · Ataque de fuerza bruta
    - · Buffer Overflow
    - · MAC Spoofing
    - · DNS Spoofing
    - · DHCP Spoofing
    - · VLAN Hopping
    - · Secuestro de sesiones

● **METODOLOGÍA:** La metodología requerida a utilizar contempla los pasos y actividades necesarias para efectuar las pruebas de vulnerabilidad y ethical hacking, como metodología base se debe utilizar el marco de referencia OSSTMM (*Open*

	Source Security Testing Methodology Manual), OWASP *(Open Web Apllication Security Project*), CEH (*Certified Ethical Hacking*) y OSCP (*Offensive Security Certified Professional*), todas en su última versión de las cuales se deriva las siguientes actividades. ● **HERRAMIENTAS:** El proveedor deberá demostrar que por lo menos una de las herramientas utilizadas para el ejercicio de las pruebas técnicas de seguridad, es licenciada. El proveedor deberá demostrar que por lo menos una de las herramientas utilizadas para el ejercicio de auditoría de código fuente, es licenciada. ● **REVISIÓN DE CÓDIGO ESTÁTICO Y DINÁMICO:** 1 aplicación de la Entidad, hasta con 500.000 Línea de código, Incluye Re-TEST ● **LEVANTAMIENTO DE INFORMACIÓN:** Realizar la evaluación del entorno de seguridad que soporta las funciones asociadas a las aplicaciones, perteneciente a la Entidad, incluyendo la inspección o análisis estático de código fuente y pruebas dinámicas sobre el front end de la aplicación. ● **ACTIVIDADES**: La lista de comprobación para código contendrá varias verificaciones incluyendo entre otras: Evaluar características del código que puedan conducir a ataques como: • Errores de inyección, SQL, LDAP y Xpath, entre otros. • Desbordamiento de buffer • Almacenamiento cifrado inseguro • Comunicaciones inseguras • Manejo inadecuado de errores de sesión interrumpidas • Lenguaje de comandos entre distintos sitios (XSS) • Control de acceso inapropiado • Falsificación de solicitudes entre distintos sitios (CSRF) • Autenticación y administración **ANÁLISIS DE SOFTWARE DE CÓDIGO FUENTE: Capacidades mínimas:** Analítica de software en nube Tener un conjunto de analizadores propios para: - Análisis estático - Métricas - Detección de código duplicado Tener motores de análisis de código multi tecnología, capaz de escanear: Objective-C, Android, Java, JSP, JavaScript, PHP, C, C++, ABAP, COBOL, RPG, JCL, Natural, PL/SQL, FORMS, Transact-SQL, SQL, Informix, Visual Basic, PowerScript, C#, ASP.NET o VB.NET, con sus cerca de 3.000 reglas, y demás tecnologías que interoperan en nube u on-premise y sus terceros.

	Mutado de defectos (“Defects Mute”), para evitar falsos positivos o excepciones a reglas Rule Developer & Rule API. Para el desarrollo de reglas personalizadas. Detección de código duplicado. Obtención de más de 60 métricas de software: número de violaciones, complejidad, actualización, volumetría Obtención de indicadores de software, necesarios para el gobierno y la gestión de la cartera de aplicaciones software: - Riesgo —Asociado a la estructura del código—; - Índice Global del software; - Esfuerzo de reparación de defectos (“Effort to Target”); - Deuda técnica. Visualización, a través de cuadros de mandos, de los resultados obtenidos. Análisis What-If. Que permita: a) El esfuerzo que se necesita para alcanzar el nivel de calidad que necesitan las aplicaciones, o b) Cuál sería la calidad de las aplicaciones si se invierte un esfuerzo determinado para mejorarla. Plan de acción, incluyendo propuestas de modificaciones, para reducir el esfuerzo del mantenimiento del software y, por consiguiente, su TCO, con la opción de exportar este plan a una herramienta de gestión de incidencias, como por ejemplo Atlassian JIRA. Verificación de la ejecución de los planes de acción (Remediation Process) mostrando el grado de cumplimiento de los planes guardados. Guardar el histórico de resultados de los análisis. Comparar de resultados con otras aplicaciones (Rankings) Generar informes automáticos a niveles ejecutivo y detallado. Tener vista “cruzada” (“Crossings”), mediante la cual se puede seleccionar dos grupos diferentes de portafolios y mostrar el indicador o la métrica seleccionados de entre la agregación de todas las carteras de esos grupos. Gestionar la actividad de los proveedores que han hecho las aplicaciones analizadas. Posibilidad de configurar el logo del usuario en los cuadros de mando o en los informes.

	Agregación de la información en portafolios basados en una o más características definibles por el usuario, tales como proveedor, área funcional o departamento al que pertenece la aplicación, tecnología, arquitectura. Tener vistas de la información a nivel aplicación o portafolio. que proporcione los indicadores y métricas agregadas, para seguir las medidas y análisis de un portafolio completo. Sobre estas vistas, se puede seleccionar los datos de las aplicaciones en los portafolios que se necesita agregar, en base a criterios definibles por el usuario (filtros). Tener visibles cuadrantes de decisión, para obtener de forma rápida el estado de salud de todos nuestros desarrollos, o un “application ranking” que permite ver todas sus aplicaciones desde distintas perspectivas. Posibilidad de enriquecer los resultados y reglas con notas del usuario. Tener la utilidad completa para la Gestión y personalización de modelos software, que permita dar soporte y gestionar modelos reconocidos por la industria o elaborados por clientes, con capacidad de versionado para facilitar la medición de distintos tipos de aplicaciones. Categorización de las reglas y métricas aplicadas. Tener utilidad para la gestión de cuentas y usuarios, que soporta personalizaciones a nivel de roles y permisos. Autenticación delegada por ejemplo, si la organización utiliza LDAP para gestionar todas sus cuentas y usuarios, o se dispone de un sistema de SSO (‘Single Sign On’) dentro de su red interna, puede delegar su autenticación mediante un servidor de un tercero. Soporte a operaciones masivas (‘bulk’). Implementar la inspección continua del código, con capacidades de integración (RESTfull API) en su proceso de desarrollo (ALM) y de DevOps, permitiendo automatizar y conocer en todo momento, el estado de la calidad y seguridad de las aplicaciones. Dispone de integraciones con JIRA, Jenkins, IBM UrbanCode, CloudBees. Estar alineado con estándares de la industria, tales como OWASP, CWE, WASC, PCI, MISRA, CERTC, ISO/IEC 25000, ó ISO/IEC 9126.

FASE 4: CAPACITACIÓN Y EVALUACIÓN	● **CAPACITACIÓN.** En esta fase se requieren los siguientes ítems: • Seminario de Ciberseguridad, Delitos Informáticos y Privacidad de la Información en el sector público, hasta 80 funcionarios, con duración de 8 horas. • Dos (2) cupos para funcionarios del Ministerio en Curso certificado que permita obtener a los asistentes la certificación como Auditor Líder e ISO 27001:2013. • Dos (2) ejercicios de simulación de incidentes de seguridad al interior de la entidad los cuales deberán ser programados y aprobados con el supervisor. ● **EVALUACIÓN:** De acuerdo con los compromisos establecidos en las mesas sectoriales, se hace necesario: Planificar y ejecutar el acompañamiento al cumplimiento de los controles para identificar el nivel de madurez y brecha de acuerdo con la herramienta de Evaluación MSPI en las siguientes entidades adscritas al Ministerio: ANLA, IDEAM y Parques Nacionales. Generar informe detallado a los controles descritos en la herramienta de autodiagnóstico dispuesta por Mintic para verificar el estado actual, brecha, recomendaciones de mejora y madurez.

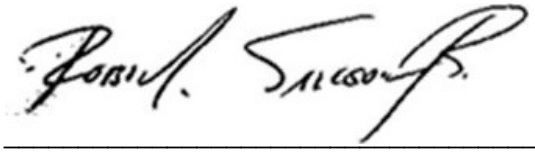
Nota. Con la suscripción del presente anexo se aceptan todas las condiciones allí contenidas.

PROPONENTE: IDENTIAN SAS
NIT: 900.678.711-3

Declaro bajo mi responsabilidad y comprometiendo la responsabilidad institucional de la persona jurídica que represento, que **ACEPTO Y CUMPLO** en su totalidad con las especificaciones técnicas, criterios de sostenibilidad ambiental y de verificación y de obligatorio cumplimiento descritas en el presente **ANEXO TECNICO**.

MANIFIESTO BAJO LA GRAVEDAD DE JURAMENTO, QUE CONOZCO Y ACEPTO LAS ESPECIFICACIONES TÉCNICAS SOLICITADAS POR EL MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Cordialmente,



ROBIN JOSE SALCEDO BUELVAS
CC 77.090.560 Valledupar
Representante Legal IDENTIAN SAS NIT 900.678.711-3
Dirección: Carrera 80b # 24a-40 Piso 1 - Teléfonos: 7042400. / 300 688 1950