ANEXO Núm. 6
ANEXO TÉCNICO SERVICIOS DE SEGURIDAD DE LA INFORMACIÓN

El presente anexo técnico define los requerimientos, especificaciones y justificación técnica para la contratación de servicios y soluciones de seguridad de la información y ciberseguridad, que garanticen la protección de la infraestructura tecnológica, la confidencialidad, integridad y disponibilidad de la información institucional. Este documento se alinea con el Modelo de Seguridad y Privacidad de la Información (MSPI), el MIPG, la Política de Gobierno Digital del MinTIC y estándares internacionales como ISO/IEC 27001 e ISO/IEC 27002, NIST y marcos metodológicos reconocidos (OSSTMM, OWASP, ISSAF).

La AGR administra información pública, reservada y confidencial que requiere mecanismos de protección frente a amenazas internas y externas. Se han identificado riesgos de accesos no autorizados, malware, ransomware, fuga de información e indisponibilidad de servicios. Con base en auditorías internas, evaluaciones de riesgo y controles del MSPI, se establece la necesidad de fortalecer los servicios de seguridad, incorporando mejores prácticas internacionales, controles técnicos y pruebas periódicas.

La Auditoría General de la República requiere atender la prestación de los siguientes servicios profesionales especializados de seguridad de la información:

1. Servicio de análisis, remediación, soporte y pruebas de verificación (retest) de Vulnerabilidades.
2. Servicio de soporte para la remediación y pruebas de verificación (retest) de Hacking Ético.
3. Servicio de Análisis de Código (SAST).
4. Servicio de Pruebas de Ingeniería Social

1. Servicio de análisis, remediación, soporte y pruebas de verificación de Vulnerabilidades

Pruebas tipo caja blanca realizadas para 50 dispositivos con direccionamiento IP privado, dentro de los cuales, 10 servidores cuentan también con direccionamiento público (9 aplicaciones web y 1 portal web), se requiere la prestación del servicio de análisis, remediación, soporte y pruebas de verificación de vulnerabilidades.

A continuación, el detalle del servicio requerido:

- Renovar el soporte y licenciamiento Premium Organization VRx de los 50 dispositivos actuales.
- Realizar las actualizaciones correspondientes que haya tenido el licenciamiento.
- Generar reportes periódicos que permitan visibilizar las vulnerabilidades existentes, su nivel de criticidad e información asociada a las actividades de remediación.
- Permitir la configuración para ejecutar la remediación automática en los 50 dispositivos tipo servidor o estación de trabajo que sean parte del servicio.

- Permitir la revisión de información asociada a la realización de acciones de remediación manual para los demás dispositivos del alcance del servicio. Dicha remediación manual estará a cargo de la AGR.
- Proponer acciones de remediación (automáticas o de ejecución manual) alineadas con estándares internacionales de gestión de riesgos, seguridad informática y mejores prácticas en tecnología, con el fin de asegurar que no se presenten impactos adversos en la disponibilidad de los servicios objeto de la remediación.
- Evitar reporte de vulnerabilidades consideradas falsos positivos.
- Se debe contar con un servicio de soporte vía correo electrónico o telefónico con ANS de atención modalidad 5x8 de manera remota, que permita al Grupo de Gestión TIC realizar las consultas referidas a la remediación automática o a la ejecución de la remediación manual.
- Los plazos de corrección de vulnerabilidades críticas serán definidos de manera conjunta entre el contratista y la AGR, considerando el nivel de riesgo y la complejidad técnica. El contratista continuará realizando el retest y verificación de las acciones de remediación, sin intervenir directamente en los entornos productivos.
- Retest: Nueva verificación para confirmar que las vulnerabilidades se cerraron correctamente esta se debe realizar una vez sea solicitada por el supervisor del contrato.

2. Servicio de soporte para la remediación y pruebas de verificación (retest) de Hacking Ético

A continuación, el detalle del servicio requerido:

El servicio tiene como alcance 10 aplicaciones / direcciones IP públicas, correspondientes a 9 aplicaciones web y portal web.

- Realizar una prueba de hacking Ético de tipo caja negra hasta en 10 aplicaciones / direcciones IP públicas, correspondientes a 9 aplicaciones web y 1 portal web, de acuerdo con lo definido por el supervisor de contrato.
- Las pruebas deben aplicar metodologías de EH como: OSSTMM, ISSAF, OTP (OWASP Testing Project), entre otras, y deben tener cobertura tanto a nivel de sistema operativo como de la funcionalidad que el elemento suple, por ejemplo, webserver o servidor de bases de datos.
- Evitar reporte de vulnerabilidades consideradas falsos positivos.
- Los hallazgos de las vulnerabilidades críticas deben informarse inmediatamente al supervisor del contrato y al Oficial de seguridad de la Información.
- Reporte de hallazgos críticos en menos de 24h.
- Proponer los planes de remediación correspondientes a las vulnerabilidades identificadas en a prueba de verificación de Ethical Hacking, alineados con estándares internacionales de gestión de riesgos, seguridad informática y mejores prácticas en tecnología.

- Los planes de remediación propuestos deben ser revisados en sesiones técnicas, con el equipo que ejecutará por parte de la AGR las acciones de remediación, con el fin de validar la pertinencia del plan propuesto y realizar las aclaraciones a que haya lugar.
- Generar y presentar el correspondiente informe técnico al supervisor del contrato y al oficial de seguridad, con el detalle de las vulnerabilidades detectada o accesos logrados, junto con la evidencia de la metodología utilizada y la explicación pertinente respecto del tipo ataque. Este informe también debe incluir información detalladas para remediar el fallo detectado.
- El proveedor deberá certificar previamente las versiones de las herramientas a utilizar y garantizar su capacidad de análisis en entornos IPv4 e IPv6.
- Realizar para cada elemento escaneado, el registro de vulnerabilidades, nivel de riesgo, criticidad y método de remediación. Consolidar en un mapa de calor de vulnerabilidades. Eliminar vulnerabilidades que puedan ser falsos positivos de manera automatizada.
- Cada informe entregado deberá contener evidencias técnicas verificables (capturas, registros de pruebas, resultados de escaneo) y estar homologado con los formatos internos de la AGR (SGSI, MSPI, MIPG).
- Se debe contar con un servicio de soporte vía correo electrónico o telefónico con ANS de atención modalidad 5x8 de manera remota, que permita al Grupo de Gestión TIC realizar las consultas referidas a la remediación de vulnerabilidades provenientes de las pruebas de Hacking Ético.
- **Retest** enfocado: volver a intentar explotar los hallazgos para confirmar que ya no son explotables.

Nota: El proveedor debe disponer con una bolsa de cincuenta (50) horas de ingeniería, distribuida de la siguiente forma:

- 25 horas para vulnerabilidades.
- 25 horas para hacking ético.

La prestación del servicio deberá llevar un control detallado de la bolsa de horas contratada, reportando indicadores de uso, número de tickets atendidos, tiempos de respuesta y estado de remediación. Para esto, deberá implementar un tablero de control que permita al supervisor del contrato realizar seguimiento en tiempo real al consumo de horas y al avance de las actividades desarrolladas. Este tablero deberá incluir como mínimo: el número total de horas contratadas, las horas ejecutadas, las horas pendientes por ejecutar, el detalle de actividades realizadas y el estado de los entregables asociados. El tablero deberá actualizarse de manera permanente y estar disponible para consulta del supervisor en el formato y medio acordado con la Auditoría General de la República.

El tablero de control deberá permitir al supervisor del contrato y al oficial realizar seguimiento al consumo de horas y al avance de las actividades. Este tablero también deberá incluir indicadores clave de gestión (KPIs), tales como: porcentaje de vulnerabilidades cerradas en los plazos establecidos, tiempos promedio de remediación, cumplimiento de niveles de servicio (ANS) e identificación de falsos

positivos. El tablero deberá actualizarse periódicamente y estar disponible para consulta del supervisor en el formato y medio acordado con la AGR

Para cada requerimiento se convendrá el consumo que este tendrá sobre la bolsa de horas, la cual se consumirá progresivamente hasta su agotamiento o el vencimiento del servicio. La métrica mínima de uso, serán fracciones de ½ hora.

3. Servicio de Análisis de Código

Se requiere la ejecución de pruebas de seguridad durante la etapa de desarrollo tipo estático SAST (Static Application Security Testing), previo a la puesta en producción, con el fin de detectar vulnerabilidades que puedan ser ajustadas o corregidas, reduciendo así el riesgo que puedan ser explotadas por amenazas en los servicios productivos. Esta revisión debe tener cobertura para las 7 aplicaciones in-house con las que cuenta la AGR,

La solución propuesta debe permitir analizar hasta 500.000 líneas de codigo así:

Nombre Aplicación	**Peso Aplicación**	**Escritorio / Web**	**Framework/Compilador/Lenguaje**
Aplicación 1	476 MB	Web	.NET Framework, C#, Visual Studio
Aplicación 2	82,9 MB	Web	.NET Framework, VB, Visual Studio
Aplicación 3	627 MB	Web	.NET Framework, Angular, Visual Studio, Visual Studio Code
Aplicación 4	10,1 MB	Web	.NET Core, C#, Visual Studio
Aplicación 5	85,2 MB	Web	.NET Framework, VB, Visual Studio
Aplicación 6	950 MB	Web	.NET Framework, C#, Visual Studio
Aplicación 7	352 MB	Web	.NET Framework, C#, Visual Studio

Los servicios deben poder ejecutarse, entre otros, para los siguientes lenguajes:

.NET 4.5 y .NET 4.6
.NET Core 6.0
Angular 12.2.16
ASP.NET Web Forms
C# PHP Javascript
Python

- Los servicios deben poder realizar las pruebas correspondientes utilizando Azure DevOps, como herramienta de integración y distribución continua. Como control de bug se utiliza Azure DevOps/TFS.

- Se realizará la revisión de código seguro desde el repositorio definido para tal fin, generando el reporte de vulnerabilidades encontradas, junto con el plan de tratamiento sugerido. Se ejecutará de manera periódica en el evento de adición o modificación de objetos (incremental), o por demanda para un grupo de objetos determinado.
- Se debe contar con una bolsa de veinticinco (25) horas de ingeniería para el acompañamiento técnico al equipo de la AGR, que permita atender inquietudes técnicas sobre el resultado de las pruebas realizadas, los planes de remediación propuestos y el detalle de actividades a ejecutar, entre otros. La métrica mínima de uso, serán fracciones de ½ hora.
- La prestación del servicio deberá llevar un control detallado de la bolsa de horas contratada, reportando indicadores de uso, número de tickets atendidos, tiempos de respuesta y estado de remediación. Para esto, deberá implementar un tablero de control que permita al supervisor del contrato realizar seguimiento en tiempo real al consumo de horas y al avance de las actividades desarrolladas. Este tablero deberá incluir como mínimo: el número total de horas contratadas, las horas ejecutadas, las horas pendientes por ejecutar, el detalle de actividades realizadas y el estado de los entregables asociados. El tablero deberá actualizarse de manera permanente y estar disponible para consulta del supervisor en el formato y medio acordado con la Auditoría General de la República.
- Para cada requerimiento se convendrá el consumo que este tendrá sobre la bolsa de horas, la cual se consumirá progresivamente hasta su agotamiento o el vencimiento del servicio. La métrica mínima de uso, serán fracciones de ½ hora.
- Cada informe entregado deberá contener evidencias técnicas verificables (capturas, registros de pruebas, resultados de escaneo) y estar homologado con los formatos internos de la AGR (SGSI, MSPI, MIPG).
- Los servicios deben eliminar alertas que puedan ser falsos positivos de manera automatizada, evitando ineficiencia y reproceso.
- Validar técnicamente y de forma conjunta los resultados de las pruebas de vulnerabilidad, de forma que el equipo técnico de la AGR participe en la revisión y confirmación de los hallazgos críticos antes de la emisión del informe final.
  No obstante, la responsabilidad del análisis técnico y la emisión de reportes seguirá siendo del contratista.
- Las acciones de remediación se ejecutan por parte del personal de la AGR, de acuerdo al plan detallado propuesto por el contratista para su tratamiento.

4. Servicio de Pruebas de Ingeniería Social

Para las pruebas de ingeniería social se requiere:

- Realizar una prueba de ingeniería social al interior de la AGR, a través del envío hasta a cincuenta (50) funcionarios de un correo tipo phishing.
- Suministrar la infraestructura de TI para la ejecución de la prueba sin generar costos adicionales para la Entidad.

- Registrar la cantidad de personas que accedieron al correo y que accedieron a las solicitudes expresadas en el correo.
- Generar y presentar el correspondiente informe técnico al supervisor del contrato y al oficial de seguridad, con el resultado y análisis del nivel de conciencia de los funcionarios sobre la seguridad de la información. El informe deberá contener, además, las recomendaciones y/o sugerencias que pueda poner en práctica en aras de fortalecer las acciones de los funcionarios para proteger la información.
- Cada informe entregado deberá contener evidencias técnicas verificables (capturas, registros de pruebas, resultados de escaneo) y estar homologado con los formatos internos de la AGR (SGSI, MSPI, MIPG).
- Realizar una presentación de sensibilización para funcionarios y contratistas de la AGR con los resultados de la prueba realizada y las recomendaciones y/o sugerencias que pueda poner en práctica en aras de fortalecer la protección de la información. Duración (1) hora de manera remota.

5.Personal Requerido.

Nombre del rol	Cantidad de personas	Formación académica	Años de experiencia profesional	Experiencia específica	% de participación en el proyecto
Gerente de proyectos	1	Profesional en Ingeniería de sistemas o afines. Con Posgrado en la Modalidad de Especialización, Maestría o Doctorado, en Gestión de Proyectos y/o en Seguridad de la Información o	Mínimo setenta y dos (72) meses de experiencia profesional.	Participación en cuatro (4) proyectos informáticos ejecutados y terminados en los que haya participado en calidad de director o gerente de proyectos.	**100%**

		Ciberseguridad Certificación en SCRUM Máster. Y CISO (Certified Chief Information .Security Officer) Y/o Auditor en Sistemas de Gestión de Seguridad de la Información (ISO 27001:2022) y/o CISM (Certified Information Security Manager – ISACA) y/o CISSP (Certified Information Systems Security Professional – ISC²) y/o ISO/IEC 27001 Lead Implementer o Lead			

		Auditor			
Consultor de Seguridad	1	Profesional en Ingeniería de Sistemas o afines, con posgrado en modalidad de Especialización, Maestría o Doctorado en Seguridad de la Información o Seguridad Informática. Certified Ethical Hacker (CEH)	Mínimo setenta y dos (72) meses de experiencia profesional.	Participación en cuatro (4) proyectos informáticos ejecutados y terminados en los que haya participado realizando ejecución de análisis de vulnerabilidades y pruebas de penetración en diversas tecnologías y plataformas	**100%**

Requisitos del personal y consideraciones

Para el personal anteriormente descrito se requiere al momento de la presentación de la oferta:

Documentos obligatorios por cada profesional propuesto

- Hoja de vida con soportes completos.
- Copia de título profesional o acta de grado.
- Copia de diploma o acta de posgrado (si aplica).
- Copia de matrícula o tarjeta profesional (si la ley lo exige) y certificado vigente.
- Documento de identificación.
- Certificaciones de experiencia laboral relacionadas.
- Carta de compromiso del profesional (según anexo).
- Certificaciones adicionales exigidas en el perfil.

Consideraciones generales del equipo de trabajo

- Ningún profesional podrá ser propuesto en más de una oferta ni para más de un rol dentro de la misma.
- No podrán participar personas que hayan ocupado cargos directivos o de asesoría en la AGR en los últimos dos años, cuando el objeto contractual tenga relación con sus funciones anteriores.
- La experiencia simultánea (trabajos traslapados) solo se contabiliza una vez.
- La AGR podrá solicitar aclaraciones sobre la experiencia, sin que se mejore la oferta.
- El contratista debe garantizar la permanencia y disponibilidad del equipo durante toda la ejecución del contrato. Cualquier cambio de profesional debe justificarse, cumplir iguales o mejores requisitos y contar con aprobación de la supervisión.
- Todo el equipo debe asistir a reuniones presenciales o virtuales cuando lo requiera el supervisor.

Formación académica

- Los títulos deben estar registrados en el **SNIES** y debidamente aprobados por el Ministerio de Educación.
- Títulos extranjeros deben presentarse convalidación del Ministerio de Educación o, en su defecto, diploma, plan de estudios y traducción oficial si aplica.
- No se aceptan cursos, seminarios ni certificaciones que no conduzcan a un título formal.
- Un título solo se reconocerá para una clase de formación, de acuerdo con el núcleo básico de conocimiento del SNIES.
- La formación académica no puede homologarse con experiencia.

Experiencia profesional

- Debe acreditarse mediante certificaciones emitidas por las entidades contratantes, indicando: empresa, nombre del profesional, cargo o rol, actividades realizadas, objeto del contrato, periodo exacto de vinculación.
- La experiencia se computa a partir de la terminación de estudios de pregrado (excepto casos especiales de salud e ingenierías según Ley 1955 de 2019 y COPNIA).
- Para ingenieros en el exterior, se requiere permiso temporal del COPNIA.
- Experiencia traslapada solo se contabiliza una vez.
- No se aceptan experiencias en docencia, asistencia académica, publicaciones o conferencias.
- Certificaciones firmadas por el mismo profesional (autocertificaciones) no serán válidas.

- Si la certificación es expedida por el mismo proponente, debe estar soportada en contrato o acta de junta directiva debidamente firmada y certificada.

PLAZO DE EJECUCIÓN DEL CONTRATO:

El plazo de ejecución del contrato será a partir de la suscripción del Acta de inicio previo cumplimiento de los requisitos de perfeccionamiento y ejecución; sin que exceda el 31 de diciembre de 2025.

Alcance: La suscripción a los servicios asociados a la herramienta de vulnerabilidades y las bolsas de horas tendrá una vigencia técnica de un (1) año. Esta vigencia no implica extensión del plazo contractual, sino la cobertura temporal de los servicios contratados dentro del término de ejecución y liquidación del contrato