PARA CONTRATAR BIENES: _____ SERVICIOS: __*X*___ OBRA: _____

DEPENDENCIA SOLICITANTE: *Grupo de Tecnologías de la Información*

1. OBJETO DEL CONTRATO

Contratar la prestación de servicios para realizar las pruebas de vulnerabilidad a los servicios tecnológicos del Archivo General de la Nación.

2. CLASIFICACIÓN EN LA CODIFICACIÓN UNSPSC

El objeto del presente proceso tiene relación con los siguientes códigos de la UNSPSC:

Número	Segmentos	Familias	Clases	*Productos (Opcional)*
1	81 Servicios basados en Ingeniería, Investigación y Tecnología.	11 Servicios Informáticos	18 Servicios de sistemas y administración de componentes de sistemas	8111800 Servicios de sistemas y administración de componentes de sistemas
2	43 Difusión de Tecnologías de Información y Telecomunicaciones.	23 Software	32 Software de seguridad y protección	43233200 Software de seguridad y protección
3	80 Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	10 Servicios de asesoría de gestión	15 Servicios de consultoría de negocios y administración corporativa	80101500 Servicios de consultoría de negocios y administración corporativa
4	80 Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	10 Servicios de asesoría de gestión	16 Gerencia de proyectos	80101600 Gerencia de proyectos

3. ESPECIFICACIONES TÉCNICAS

Las especificaciones técnicas del objeto que se pretende contratar se encuentran relacionadas en el numeral 10 del presente documento.

4. PLAZO DE EJECUCIÓN:

El plazo de ejecución del contrato será de cuatro (4) meses, contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato y sin que se supere la vigencia actual.

5. LUGAR DE EJECUCIÓN

El contrato se ejecutará en la Sede del Archivo General de la Nación, carrera 6 #6 - 91 en la ciudad de Bogotá.

6. OBLIGACIONES A EXIGIR AL CONTRATISTA:

6.1. OBLIGACIONES GENERALES:

1. Responder por sus actuaciones y omisiones derivadas del presente contrato y de la ejecución de este de conformidad con lo establecido en la Ley 80 de 1993.☐
2. Responder por la calidad y cumplimiento del objeto contractual.☐
3. Preparar y presentar los informes sobre las actividades desarrolladas, con la oportunidad y periodicidad requeridas por el supervisor.☐
4. Mantener confidencialidad en el manejo de la información de aquellos eventos que por su naturaleza lo estima la entidad.☐
5. Garantizar la protección de datos y la información entregada por el AGN.☐
6. Responder por la entrega de los documentos producidos en cumplimiento de las obligaciones contractuales.☐
7. Cumplir de manera oportuna con los requisitos exigidos para el trámite de pago.☐
8. Mantener informado al supervisor del contrato sobre el desarrollo de las actividades que afecten el desarrollo del objeto contractual.☐
9. Atender a los requerimientos del supervisor del contrato.☐
10. Entregar los bienes y servicios contratados de manera inmediata y con la disponibilidad requerida por la entidad.☐
11. Desarrollar el contrato acorde con lo establecido en el Artículo 5 de la Ley 80 de 1993.☐
12. Constituir y mantener vigente la Garantía Única que impone la celebración del contrato, en los términos establecidos en el mismo.☐☐
13. Dar cumplimiento a lo establecido en los estudios previos, en el pliego de condiciones y la propuesta presentada los cuales hacen parte integral del contrato.☐☐
14. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones injustificadas.☐☐
15. Ejecutar el objeto del presente contrato, disponiendo de suficiente capacidad técnica y administrativa.☐

16. Acreditar mediante certificación, el Pago de Aportes de Seguridad Social y Aportes Parafiscales, expedida por el Revisor Fiscal de la empresa o el Representante Legal de la misma, en cumplimiento del Artículo 50 de la Ley 789 de 2002, la Ley 828 de 2003 y la Ley 1150 de 2007, del mes correspondiente de la debida ejecución del contrato.☐
17. Desempeñar las demás actividades relacionadas con el objeto Pagar los salarios y prestaciones sociales en forma oportuna a todo el personal que utilice durante la ejecución del Contrato, y en general, dar estricto cumplimiento a la totalidad de obligaciones con el sistema Integral de Seguridad Social y Parafiscales, derivadas de la ejecución☐del mismo☐
18. Adoptar las medidas de seguridad industrial para evitar la ocurrencia de accidentes durante la ejecución del contrato y deberá dotar a su personal de los elementos de seguridad y protección personal adecuados para la labor contratada.☐
19. Actuar con total autonomía técnica y administrativa, en el cumplimiento de las obligaciones que asume con el contrato y, en consecuencia, no contrae relación laboral alguna con el AGN.☐
20. Aplicar buenas prácticas ambientales establecidas en la normativa vigente para el desarrollo del objeto contractual.☐
21. Reportar cualquier emergencia ambiental que pueda generar un impacto ambiental negativo y/o alguna infracción ambiental aplicada por autoridad ambiental en el período de ejecución del contrato.☐
22. Realizar todas las actividades requeridas en el SECOP II para garantizar la oportuna publicación de los documentos del proceso de contratación y la ejecución del respectivo contrato. Dentro de las actividades que se deben realizar se encuentran: aprobación del contrato, cargue de garantías en la plataforma, informes, entre otros.☐
23. Conocer y aplicar todos los lineamientos que sobre el manejo de la plataforma SECOP II emita Colombia Compra Eficiente.☐
24. Respetar, garantizar, promover y no violentar los derechos humanos, especialmente de las mujeres y de las diversidades sexuales.☐
25. ☐Cumplir con las demás obligaciones que se deriven de la naturaleza del objeto del contrato.☐

6.2. OBLIGACIONES ESPECÍFICAS:

1. Presentar, dentro de los cinco (05) días hábiles posteriores a la firma del acta de inicio del contrato, el plan de trabajo con las especificaciones de cada fase, detallando el diseño de la metodología para todos los entregables de los servicios contratados, el cronograma de actividades, los recursos, el personal asignado, el plan de manejo de incidentes derivados de las pruebas y los acompañamientos requeridos, con el propósito de dar cumplimiento de las actividades establecidas en el contrato.
2. Cumplir con los requisitos establecidos y verificar que el personal que va a ejecutar el contrato cumpla con estos y con la dedicación requerida conforme a lo estipulado en los requisitos habilitantes del contrato.

3. Contar con los elementos necesarios (Hardware y Software) requeridos para ejecutar las actividades propias del contrato.
4. Presentar al supervisor del contrato la propiedad o suscripción del licenciamiento de software requerido para la ejecución del contrato.
5. Presentar al supervisor, documentos que acrediten los derechos de uso de cada una de las herramientas que se utilizarán para el desarrollo del objeto contractual.
6. Ejecutar pruebas de Ethical Hacking o Pentesting en la infraestructura tecnológica del Archivo General de la Nación
7. Implementar pruebas de ingeniería social con una muestra estadísticamente representativa de servidores y contratistas de la entidad.
8. Realizar un Re-Test a la infraestructura tecnológica de la entidad para verificar la mitigación de vulnerabilidades identificadas.
9. Entregar y socializar los informes técnicos y gerenciales resultado de la ejecución del contrato, los cuales deberán estar en idioma español, relacionando las evidencias de herramientas técnicas utilizadas, pruebas generadas y resultados obtenidos correspondientes a: • Pruebas de hacking ético • Pruebas de Re-test • Pruebas de ingeniería social.
10. Realizar la socialización y acompañamiento en la aplicación de las recomendaciones a que haya lugar según los resultados del ejercicio de Ethical Hacking.
11. Elaborar el plan para mitigar o remediar las vulnerabilidades, dirigido a cerrar las brechas de seguridad en la infraestructura tecnológica de la Entidad.
12. El contratista deberá suministrar en medio digital los entregables definidos en las Especificaciones Técnicas del Documento Técnico y Especificaciones, el cual hace parte integral de este proceso.
13. Garantizar la logística y recursos necesarios para dar solución a incidentes o eventos que surjan durante la ejecución de las actividades de pruebas y evaluación de vulnerabilidades, ejercicios de Ethical Hacking y actividades de remediación en los términos que se acuerden con el área de Tecnología sin costo adicional para el AGN, limitados a servicios profesionales asociados al objeto del contrato, con el fin de remediar el servicio afectado.
14. Informar al supervisor del contrato cualquier irregularidad que se tenga en el desarrollo del contrato.

7. OBLIGACIONES DEL ARCHIVO GENERAL DE LA NACIÓN:

1. Garantizar al contratista el acceso a las instalaciones del Archivo General de la Nación, cuando así lo requiera para la ejecución del contrato.
2. Informar al contratista sobre los aspectos técnicos que éste requiera para la debida y oportuna ejecución del contrato.
3. Supervisar al contratista en la ejecución idónea y oportuna del objeto contractual.
4. Recibir a satisfacción y verificar la calidad de los bienes y/o servicios que sean entregados por el contratista, cuando estos cumplan con las condiciones establecidas y en especial las especificaciones técnicas contenidas en el documento técnico.
5. Cancelar al contratista la suma establecida en la oportunidad y forma prevista, sujeta a la disponibilidad del PAC.

8. FORMA DE PAGO:

El valor del contrato de que resulte del presente proceso de selección, se pagarán previo giro de PAC por parte del Ministerio de Hacienda y Crédito Público, así:

a) Un primer pago contra el cumplimento del ANÁLISIS DE VULNERABILIDADES Y PRUEBA DE PENTESTING (ítem 1 de la propuesta económica), junto con la entrega completa de los informes técnicos y generales, según lo establecido en el Documento técnico y especificaciones.

b) Un segundo pago contra el cumplimiento de las PRUEBAS DE INGENIERÍA SOCIAL (ítems 3, 4 y 5 de la propuesta económica), junto con la entrega del informe técnico de resultados.

c) Un último pago, de acuerdo con el cumplimiento de las PRUEBAS DE RE-TEST (ítem 2 de la propuesta económica) junto con los informes finales y el recibo de satisfacción por parte del supervisor de la ejecución del contrato.

NOTA 1. En todo caso el pago estará sujeto a la programación, aprobación y giro del Programa Anual Mensualizado de Caja –PAC.

NOTA 2. Para dar cumplimiento al derecho a turno, contemplado en el artículo 19 de la Ley 1150 de 2007, se deberá presentar toda la documentación necesaria para los pagos.

NOTA 3. Si los documentos en mención no se presentan o son devueltos por falta de información o mal diligenciados, la entidad contará hasta con treinta (30) días más para realizar el pago.

NOTA 4. Para efectos de retenciones y contribuciones se aplicarán las que se encuentren vigentes durante la ejecución del contrato, teniendo en cuenta el régimen contributivo que corresponda.

NOTA 5. La entidad no reconocerá pagos sobre pedidos o entregas de elementos o prestación de servicios que no hubieren sido previamente requeridos o autorizados por el supervisor del contrato o quien ejerza su apoyo.

NOTA 6. El contratista deberá acreditar el pago de los aportes establecidos en el Artículo 50 de la ley 789 de 2002 y demás normas que lo modifiquen, reglamentan o complementen, lo cual se hará mediante certificación expedida por el revisor fiscal o el representante legal si no tiene revisor fiscal. Los pagos se realizarán a través de la cuenta de ahorros y/o corriente que disponga el contratista acorde con la certificación expedida por la entidad financiera aportada por el contratista.

9. GARANTÍAS

Acorde con lo establecido en el Decreto 1082 de 2015 y de acuerdo con lo dispuesto en la Ley 1150 de 2007; la entidad, teniendo en cuenta la naturaleza del contrato a celebrar y la forma de pago, solicitará garantías al contratista seleccionado, con el fin de garantizar el cumplimiento y la eficaz ejecución del mismo.

El contratista deberá constituir la garantía dentro de los tres (3) días hábiles siguientes a la fecha de firma del contrato y deberá allegarla por medio de la plataforma SECOP II para ser aprobada por la entidad. La garantía debe cumplir los siguientes amparos:

AMPARO	PORCENTAJE	BASE	VIGENCIA
Calidad del servicio	**(20)%**	Por el cien por ciento (100%) del valor total del contrato.	Vigente a partir del perfeccionamiento del contrato, por el plazo de ejecución y doce (12) meses más, contados a partir de la terminación del contrato.
Cumplimiento del contrato	**(20)%**	Por el cien por ciento (100%) del valor total del contrato.	Vigente a partir del perfeccionamiento del contrato, por el plazo de ejecución y doce (12) meses más, contados a partir de la terminación del contrato.
Pago de salarios Prestaciones Sociales e Indemnizaciones Laborales	**(5)%**	Valor del contrato	Vigente por el plazo de ejecución del contrato y tres (3) años más, contados a partir del perfeccionamiento del contrato.

El hecho de la constitución de estos amparos no exonera al contratista de las responsabilidades legales en relación con los riesgos asegurados. Dentro de los términos estipulados en el contrato, ninguno de los amparos otorgados podrá ser cancelado o modificado sin la autorización expresa de la entidad.

10.ESPECIFICACIONES TÉCNICAS

Ítem.	Descripción de los Bienes y/o servicios Requeridos	Unidad de Medida	Cantidad Requerida
1	Análisis de vulnerabilidades y prueba de Pentesting (Ethical Hacking)	Unidad	1
2	Pruebas de Re-test	Unidad	1
3	Pruebas de ingeniería social tipo Phishing	Unidad	1
4	Pruebas de ingeniería social tipo Baiting	Unidad	1
5	Pruebas de seguridad física	Unidad	1

DETALLAR EL BIEN, Y/O SERVICIO U OBRA QUE SE REQUIERE TENIENDO EN CUENTA LAS CARACTERÍSTICAS TÉCNICAS

La entidad requiere un servicio especializado de pruebas de seguridad informática, con el fin de encontrar y subsanar vulnerabilidades que puedan afectar la información y operación, para ello se requiere que el proveedor realice lo siguiente:

ITEM 1.

NOMBRE DEL PRODUCTO O DEL BIEN	ANÁLISIS DE VULNERABILIDADES Y PRUEBA DE PENTESTING
Unidad de medida	Unidad
Calidad mínima	La entidad requiere un servicio especializado de pruebas de seguridad informática, con el fin de encontrar y subsanar vulnerabilidades que puedan afectar la información y operación, para ello se requiere que el proveedor realice lo siguiente: **FASE I PLANEACIÓN Y DEFINICIÓN DEL ALCANCE** - Entendimiento y levantamiento de la información de procesos, actividades de la entidad, activos de información a sometimiento de las pruebas. - Definición de un plan de trabajo con las especificaciones de cada fase, detallando el diseño de la metodología a implementar para todos los entregables de los servicios contratados, el cronograma de actividades, los recursos, el personal asignado, el plan de manejo de incidentes derivados de las pruebas y los acompañamientos requeridos, con el propósito de dar cumplimiento de las actividades establecidas en el contrato. - Los documentos resultados de esta fase deben estar aprobados por el supervisor del contrato o personal designado por la entidad para proceder con la siguiente fase. Entregable: Plan de trabajo y cronograma. **FASE II PRUEBAS DE ETHICAL HACKING O PENTESTING** - Desarrollar pruebas de vulnerabilidades, Ethical Hacking y Pentesting (pruebas de penetración) sobre redes, firewalls, servidores, bases de datos, sistemas de información y aplicaciones del ARCHIVO GENERAL DE LA NACIÓN, con el fin de establecer el nivel de vulnerabilidad

de la plataforma tecnológica (Hardware y Software) de la entidad.

- Usar las herramientas técnicamente idóneas para la identificación vulnerabilidades. y la ejecución de las pruebas de penetración, que permitan usar como referencia el CVE/MITRE (Common Vulnerabilities and Exposures)/www.mitre.org. Para tal efecto, deberá indicar las herramientas a emplear y acreditar mediante documentación técnica del fabricante o enlaces oficiales, que dichas herramientas cuentan con la capacidad de identificar, clasificar y reportar vulnerabilidades referenciadas en el estándar CVE. Para la generación de las pruebas se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación MITRE (www.mitre.org).
- Las herramientas para realizar las pruebas de vulnerabilidades y de penetración deben ser licenciadas o propiedad del oferente y estar actualizadas a su más reciente versión a la fecha de su utilización, en complemento pueden ser usadas herramientas de uso libre.
- Las pruebas deben realizarse con la aplicación de técnicas de black, gray y white box, según corresponda de acuerdo con el análisis realizado en la primera fase.
- Las pruebas técnicas deben incluir como mínimo un escaneo automatizado de vulnerabilidades, y complementarse con pruebas manuales de validación, evaluación de configuración inseguras, validación de controles de autenticación y autorizaciones, revisión de exposición de servicios, análisis de puertas y servicios activos e identificación de vulnerabilidades conocidas (CVE).
- Los activos de la infraestructura tecnológica a los que se realizarán las pruebas de Ethical Hacking, son los siguientes:

Activos de Información	Cantidad
Servidores Virtuales Windows	63
Servidores Virtuales Linux	55
Servidores Físicos Windows	7
Servidores Físicos Linux	4

Sistema de Virtualización	3
Firewall	1
Micrositios	64
SAN	2
Bases de Datos	10
NAS	2
Sistema de Backup	1

- El desarrollo de Pruebas de Ethical Hacking, debe incluir como mínimo las siguientes actividades:

  - Descubrimiento de contraseñas a Fuerza-Bruta directamente contra servicios y aplicaciones;
  - Cracking de contraseñas sobre cuentas privilegiadas en bases de datos obtenidas por el oferente, directamente de los sistemas objetivo;
  - Secuestro de sesiones;
  - Detección y análisis de errores en aplicaciones o configuraciones débiles que permitan acciones no apropiadas
  - Se deben realizar pruebas desde el exterior de la entidad, a la infraestructura de la red que brinda servicios al público. Debe realizarse al menos una (1) prueba de intrusión.
  - Así mismo, se debe realizar una prueba desde el interior de la entidad, para lo cual, el Oferente adjudicatario debe ser capaz de realizar pruebas de intrusión a la infraestructura tecnológica de ARCHIVO GENERAL DE LA NACIÓN, desde distintos escenarios, hacia su sitio de procesamiento.
  - El contratista deberá ejecutar como mínimo: (i) una (1) prueba de penetración externa sobre la infraestructura perimetral; (ii) una (1) prueba de penetración de aplicaciones web, que incluya los micrositios, priorizando aquellos de mayor criticidad, y (iii) una (1) prueba de penetración interna, orientada a simular un atacante dentro de la red, incluyendo la evaluación de servidores y plataformas de almacenamiento.

    El alcance y la ejecución de estas pruebas se definirán y delimitarán con base en los resultados del análisis de vulnerabilidades; deberán ser concertados con el

	supervisor del contrato o quien este designe, previa evaluación de los riesgos asociados a su ejecución. - Las pruebas de intrusión se deben realizar bajo metodologías reconocidas internacionalmente como lo son: OWASP (para búsqueda de vulnerabilidades en aplicaciones web) y OSSTMM (Metodología Abierta de Testeo de Seguridad). - Las pruebas deben realizarse de manera controlada con el fin de evitar afectación del servicio u operación, no obstante, previamente se debe acordar el proceso de recuperación o remediación con los especialistas en caso de alguna eventualidad desafortunada. - El contratista deberá asegurar la integridad de la infraestructura computacional que ha de ser intervenida durante la ejecución del objeto contractual, así como la integridad, confidencialidad y disponibilidad de la información almacenada y circulante por dicha infraestructura. - En caso de detectar vulnerabilidades de nivel 'Crítico' o 'Alto' (según escala CVSS v3.1) que comprometan la integridad de los datos del Archivo General de la Nación, el contratista deberá reportarlo al Coordinador de GTI en un plazo no mayor a ocho (8) horas hábiles, mediante informe técnico preliminar, sin esperar a la entrega del informe final. Entregable: Certificado de licenciamiento de la herramienta **FASE III ANÁLISIS DE RESULTADOS Y ELABORACIÓN DE INFORMESl** **Informe Técnico:** Entregar un informe detallado del resultado de las pruebas de vulnerabilidad realizadas, que contenga mínimo: - Descripción de la metodología utilizada. - Alcance evaluado. - Desarrollo y resultados generales- - Hallazgos identificados con sus respectivas evidencias. - Nivel de criticidad de las vulnerabilidades (altas, medias y bajas) - Riesgos asociados. - Evaluación de impacto por vulnerabilidad - Referencias y recomendaciones para subsanar cada vulnerabilidad. - Conclusiones

	- Anexo 1: Matriz de vulnerabilidad en formato editable. - Anexo 2: Matriz de riesgos asociados al resultado obtenido. **Hoja de Ruta:** Documento con el plan y hoja de ruta para subsanar los hallazgos encontrados de acuerdo con la priorización. Debe incluir como mínimo: - Listado de vulnerabilidades encontradas. - Clasificación - Descripción de la vulnerabilidad. - Detalle del activo donde fue hallado. - CVE - OWASP - Puerto - Impacto - Descripción del impacto - Criticidad - Acción preventiva - Acción correctiva. - Tipo de Remediación - Referencias. - Proyección de la acción (Largo, mediado o lago plazo) - Priorización. Para el desarrollo de este plan se deben generar mesas de trabajo con los especialistas para acotar actividades de corto, mediano y largo plazo. **Informe Ejecutivo:** Documento con el informe ejecutivo que muestre de manera general las vulnerabilidades, amenazas, recomendaciones y proyección de vulnerabilidad a subsanar por fases, con el fin de presentarlo sin comprometer la seguridad de la infraestructura de TI a la alta dirección de la entidad. En este informe se pueden destacar fortalezas encontradas a las que haya lugar. Entregable: Informe Técnico, Matriz de Vulnerabilidades, Matriz de riesgos, Hoja de Ruta, Informe ejecutivo, plan de remediación.

FASE IV SOCIALIZACIÓN DE HALLAZGOS Y RECOMENDACIONES

Realizar una sesión formal de socialización dirigida al equipo de Tecnologías de la Información, con el propósito de presentar y explicar de manera detallada los informes técnicos entregados.

En esta sesión se deberá:

- ☐ Exponer los hallazgos identificados, clasificados por nivel de criticidad.
- ☐ Explicar los riesgos asociados a cada vulnerabilidad detectada.
- ☐ Presentar las recomendaciones técnicas y administrativas para su mitigación.
- ☐ Priorizar las acciones correctivas conforme al nivel de impacto y probabilidad de ocurrencia.
- ☐ Resolver inquietudes técnicas del equipo de TI del AGN.

La socialización tendrá como objetivo principal facilitar la comprensión de los resultados y apoyar la definición de un plan de acción que permita atender y mitigar el mayor número de vulnerabilidades antes de la ejecución de las pruebas de Re-Test.

Entregables: Presentación, acta de reunión

FASE V ACOMPAÑAMIENTO IMPLEMENTACIÓN DE REMEDIACIONES

El contratista deberá realizar mesas de trabajo con el equipo de especialistas del Archivo General de la Nación (AGN), con el fin de brindar acompañamiento técnico en la implementación de las acciones de remediación priorizadas a corto plazo.

Durante estas sesiones, el contratista deberá:

- ☐ Orientar técnicamente al equipo institucional en la aplicación de las recomendaciones formuladas.
- ☐ Aclarar dudas relacionadas con la mitigación de vulnerabilidades identificadas.
- ☐ Apoyar la validación de configuraciones o ajustes implementados.
- ☐ Emitir recomendaciones adicionales cuando se requiera fortalecer los controles de seguridad.

	El objetivo de este acompañamiento será asegurar la correcta implementación de las acciones correctivas y reducir el nivel de riesgo antes de la ejecución del Re-Test. Entregable: Seguimiento al plan de remedición
Identificación adicional requerida	La información recolectada con ocasión de la ejecución del contrato deberá ser tratada como confidencial y únicamente podrá ser almacenada, consultada, procesada o analizada dentro de la infraestructura y entornos autorizados por el Archivo General de la Nación. En ningún caso podrá ser trasladada, replicada o procesada en entornos externos, salvo autorización previa, expresa y por escrito de la entidad. Todas las pruebas que se realicen en el marco del contrato deberán ejecutarse estrictamente conforme al plan de trabajo, alcance técnico y período de ejecución previamente definidos y aprobados por el Archivo General de la Nación. Cualquier modificación deberá contar con autorización formal de la entidad. La información clasificada como confidencial (Pública clasificada o publica reservada) deberá permanecer cifrada tanto en reposo como en tránsito, utilizando mecanismos criptográficos robustos y acordes con estándares de seguridad reconocidos. El contratista deberá garantizar su adecuada custodia, evitando accesos no autorizados, divulgación, copia o uso indebido. Dicha información únicamente podrá ser compartida con la entidad a través de los canales oficiales y seguros previamente establecidos.

ITEM 2

NOMBRE DEL PRODUCTO O DEL BIEN	RE-TEST
Unidad de medida	Unidad

Calidad mínima	**FASE I RE-TEST Y VALIDACIÓN DE MEDIDAS CORRECTIVAS** - Se debe llevar a cabo como mínimo un RETEST para hacer seguimiento de la disminución del riesgo. - El RETEST se debe llevar a cabo 2 meses después de la entrega de los informes técnicos. - El Re-Test deberá realizarse exclusivamente sobre los activos en los cuales se hayan identificado vulnerabilidades durante la fase inicial de pruebas o sobre aquellos que hayan sido objeto de cambios técnicos posteriores, siempre que dicha modificación sea informada formalmente por el Archivo General de la Nación (AGN). **FASE II ANÁLISIS DE RESULTADOS Y ELABORACIÓN DE INFORMES** **Informe Técnico:** Entregar un informe detallado del resultado de las pruebas de Re-Test realizadas, que contenga mínimo: - Corrección de vulnerabilidades detectadas previamente y las pendientes. - Comparativo de las pruebas iniciales. - Descripción de la metodología utilizada. - Alcance evaluado. - Desarrollo y resultados generales. - Nuevos Hallazgos identificados con sus respectivas evidencias. - Nivel de criticidad de las vulnerabilidades (altas, medias y bajas) - Riesgos asociados. - Evaluación de impacto por vulnerabilidad - Referencias y recomendaciones para subsanar cada vulnerabilidad. - Conclusiones - Anexo 1: Matriz de vulnerabilidad en formato editable actualizada. - Anexo 2: Matriz de riesgos asociados al resultado obtenido Actualizado. **Hoja de Ruta:**

	Actualización del documento del plan de remediación y hoja de ruta, en donde se visualicen las vulnerabilidades pendientes a subsanar. Para la actualización de este plan se debe considerar si se requiere mesas de trabajo con los especialistas para acotar actividades de mediano y largo plazo. **Informe Técnico Final:** Documento que unifique los dos informes técnicos con los resultados de las pruebas de vulnerabilidades iniciales y de Re-test. Este debe relacionar los anexos actualizados: Plan de remediación con la hoja de ruta, matriz de riesgos, matriz de vulnerabilidades. **Informe Ejecutivo Final:** Documento con el informe ejecutivo final que consolide los resultados de las pruebas realizadas y el Re-Test, que muestre de manera general las vulnerabilidades, amenazas, remediaciones, recomendaciones y proyección de vulnerabilidad a subsanar a futuro, con el fin de presentarlo sin comprometer la seguridad de la infraestructura de TI a la alta dirección de la entidad. En este informe se pueden destacar fortalezas encontradas a las que haya lugar. Entregable: Informe Técnico Re-Test, Informe Técnico Final Matriz de Vulnerabilidades actualizada, Matriz de riesgos actualizada, plan de remediación actualizado, Hoja de Ruta actualizada, Informe ejecutivo final. **FASE III SOCIALIZACIÓN DE HALLAZGOS Y RECOMENDACIONES** Realizar una sesión de socialización dirigida al equipo de Tecnologías de la Información, con el propósito de presentar y explicar de manera detallada los informes finales entregados. En esta sesión se deberá: ☐ Exponer los hallazgos remediados. ☐ Los hallazgos que están pendientes de remedición, con su criticidad, riesgos.

	☐ Plan de remediación a mediano y largo plazo. ☐ Explicar los riesgos asociados a cada vulnerabilidad detectada. ☐ Presentar las recomendaciones técnicas y administrativas para su mitigación. ☐ Priorizar las acciones correctivas conforme al nivel de impacto y probabilidad de ocurrencia. ☐ Resolver inquietudes técnicas del equipo de TI del AGN. Entregables: Presentación, acta de reunión.
Identificación adicional requerida	La información recolectada con ocasión de la ejecución del contrato deberá ser tratada como confidencial y únicamente podrá ser almacenada, consultada, procesada o analizada dentro de la infraestructura y entornos autorizados por el Archivo General de la Nación. En ningún caso podrá ser trasladada, replicada o procesada en entornos externos, salvo autorización previa, expresa y por escrito de la entidad. Todas las pruebas que se realicen en el marco del contrato deberán ejecutarse estrictamente conforme al plan de trabajo, alcance técnico y período de ejecución previamente definidos y aprobados por el Archivo General de la Nación. Cualquier modificación deberá contar con autorización formal de la entidad. La información clasificada como confidencial (Pública clasificada o publica reservada) deberá permanecer cifrada tanto en reposo como en tránsito, utilizando mecanismos criptográficos robustos y acordes con estándares de seguridad reconocidos. El contratista deberá garantizar su adecuada custodia, evitando accesos no autorizados, divulgación, copia o uso indebido. Dicha información únicamente podrá ser compartida con la entidad a través de los canales oficiales y seguros previamente establecidos.

ITEM 3

NOMBRE DEL PRODUCTO O DEL BIEN	**PRUEBAS DE INGENIERÍA SOCIAL**
Unidad de medida	Unidad

Calidad mínima	**FASE I PLANEACIÓN Y DEFINICIÓN DEL ALCANCE** - Entendimiento y levantamiento de la información para definir el alcance y usuarios objeto de pruebas. - Definir el un plan de trabajo con las siguientes especificaciones: • Diseño de la metodología a implementar • Cronograma de actividades, recursos y personal asignado. • Plan de manejo de incidentes derivados de las pruebas. • Acompañamientos requeridos por parte del equipo del AGN. • Remediación o actividad para realizar en caso de afectación de servicios u operación. • Definición de técnicas (Phishing, Vishing, Baiting, Smishing, Pretexting) • Identificación de exclusiones. • Anexo 1: Cronograma. • Anexo 2: Matriz de riesgos. - Los documentos resultados de esta fase deben estar aprobados por el supervisor del contrato o personal designado por la entidad para proceder con la siguiente fase. Entregables: Plan de pruebas de ingeniería social, Cronograma, Matriz de riesgos. **FASE II PREPARACIÓN DE LAS PRUEBAS DE INGENIERÍA SOCIAL** Diseño de campañas simuladas para cada uno de los tipos de ataques: - Phishing (Correos Electrónicos Maliciosos): Definir correo y plataforma para la simulación de robo de credenciales. • Alcance: dirigido a 200 funcionarios. • Medición: se debe medir la cantidad de usuarios que accedieron al enlace, suministraron datos y cantidad de reportes del incidente.

	- Baiting (Dispositivos USB o Archivos Maliciosos): pruebas de recorrido para simular escenarios controlados en los que el personal del contratista se presenta como soporte técnico y mediante el uso de dispositivos USB o archivos señuelo, evaluar la reacción de los usuarios frente a intentos de instalación de software o acceso no autorizado a los equipos de cómputo. Estas pruebas deberán ejecutarse bajo un entorno controlado y autorizado por la entidad, con el propósito de identificar vulnerabilidades relacionadas con el acceso a los equipos, la ejecución de archivos no autorizados y el manejo de información confidencial. • Alcance: Las pruebas deberán realizarse a un grupo mínimo de treinta (30) usuarios de la entidad, seleccionados de manera aleatoria o de acuerdo con los perfiles definidos por el AGN. • Medición: indicar el número de usuarios abordados durante la prueba, cantidad de usuarios que permitieron el acceso a sus equipos de cómputo. Número de eventos en los que fue posible intentar o lograr la instalación de software o ejecución de archivos. Casos en los que los usuarios compartieron información o credenciales. Identificación de debilidades en los controles de seguridad y en las prácticas de los usuarios. - Pruebas Físicas: recorridos controlados en las instalaciones de la sede central del AGN, con el fin de identificar posibles vulnerabilidades relacionadas con el acceso no autorizado a información o activos de información. Estas pruebas deberán incluir, entre otras actividades, la verificación de equipos de cómputo desatendidos, la exposición de documentos con información personal, sensible o clasificada en impresoras, escritorios u otros espacios de trabajo, así como intentos controlados de acceso o retiro de equipos sin autorización. • Alcance: Las pruebas estarán dirigidas a todo el personal que labora en la sede central del AGN, incluyendo funcionarios, contratistas y personal de apoyo que tenga acceso a las instalaciones. • Medición: se debe identificar como mínimo: o Número y tipo de vulnerabilidades identificadas.

	o Cantidad de eventos en los que se logró acceder a información o activos sin autorización. o Identificación de debilidades en los controles físicos y en las prácticas de seguridad del personal. o Análisis de riesgos asociados a los hallazgos identificados. - Las pruebas deben incluir una evaluación del nivel de concienciación en ciberseguridad de los funcionarios y contratistas, así como medir la efectividad de políticas, controles y prácticas de seguridad de la información. - Las pruebas deben identificar posibles puntos débiles en la gestión de accesos y manejo de información confidencial. - Las pruebas de ingeniería social y pruebas físicas deberán ejecutarse bajo lineamientos que garanticen la legalidad, el control y la no afectación a la operación de la entidad. En este sentido, se establecen los siguientes lineamientos: • Autorización previa y alcance definido: Las pruebas deberán contar con autorización expresa y por escrito de la entidad, así como con la definición clara del alcance, objetivos, población objetivo y técnicas a emplear, los cuales serán aprobados en la fase de planeación por el supervisor del contrato. • Ejecución controlada y ética: Las actividades deberán desarrollarse bajo principios éticos, sin generar afectaciones reputacionales, legales o laborales a los funcionarios, contratistas o terceros. En ningún caso se permitirá la suplantación de autoridades, entidades externas sensibles o escenarios que puedan generar pánico o desinformación. • Restricciones operativas: No se permitirá la afectación de la operación institucional, ni la interrupción de servicios. No se podrán realizar acciones que comprometan la integridad de las personas, instalaciones o activos físicos. No se permitirá el acceso no autorizado a áreas críticas sin acompañamiento o sin los permisos correspondientes. • Las pruebas deberán ejecutarse en coordinación permanente con la entidad, reportando oportunamente cualquier situación relevante o incidente derivado de su ejecución. • En caso de contemplarse pruebas físicas como intentos de acceso controlado a instalaciones, estas deberán

	realizarse únicamente en los sitios autorizados, en horarios definidos y bajo condiciones previamente concertadas, garantizando en todo momento la seguridad del personal y de las instalaciones. Entregable: Diseño de campañas. **FASE II EJECUCIÓN DE LAS PRUEBAS DE INGENIERÍA SOCIAL** - Realizar pruebas que simulen ataques de diferentes modalidades: • Phishing (Correos Electrónicos Maliciosos) dirigido a 200 funcionarios. Creación de dominios o entornos controlado. • Baiting (Dispositivos USB o Archivos Maliciosos) Pruebas a 30 funcionarios o contratistas. • Pruebas Físicas, las cuales se deben definir en la fase I. - Realizar las pruebas en diferentes momentos y a distintos grupos con el fin de contar con una muestra significativa de usuarios del AGN. **FASE III ANÁLISIS DE RESULTADOS Y ELABORACIÓN DE INFORMES** El contratista deberá realizar el análisis integral de los resultados obtenidos durante la ejecución de las pruebas de ingeniería social y elaborar el informe correspondiente, con el propósito de identificar vulnerabilidades asociadas al factor humano y establecer acciones de mejora para fortalecer la cultura de seguridad de la información en la entidad. - Elaborar el Informe Técnico de Ingeniería Social, el cual deberá contener como mínimo: • Descripción de la metodología aplicada en cada una de las pruebas realizadas. • Análisis de las vulnerabilidades humanas identificadas durante las pruebas. • Estadísticas y métricas de efectividad de cada tipo de prueba realizada. • Nivel de concientización del personal frente a ataques de ingeniería social. • Identificación de fortalezas y debilidades en los comportamientos observados.

	• Tasa de éxito o porcentaje de incidencia en cada una de las modalidades evaluadas (phishing, pruebas físicas, baiting u otras aplicadas). • Análisis de riesgos asociados a los hallazgos identificados. • Recomendaciones de mejora orientadas a fortalecer los controles y la cultura de seguridad de la información. - Diseñar una hoja de ruta de mejora, que incluya estrategias de mitigación, fortalecimiento de controles y acciones de capacitación o sensibilización que la entidad deberá implementar durante la vigencia, con el fin de reducir los riesgos asociados a ataques de ingeniería social. Entregables: - Informe Técnico de Resultados de las Pruebas de Ingeniería Social. - Hoja de ruta o plan de mejora con estrategias de mitigación. **FASE IV SOCIALIZACIÓN DE HALLAZGOS Y RECOMENDACIONES** - Realizar una sesión de socialización de resultados con el equipo de Tecnologías de la Información de la entidad, con el fin de presentar y explicar los resultados del informe de pruebas de ingeniería social. Durante esta sesión se deberán analizar los hallazgos identificados, los riesgos asociados y las recomendaciones planteadas, así como las acciones correctivas y de mejora que deberán implementarse de acuerdo con la hoja de ruta y los planes de mitigación propuestos. - Brindar acompañamiento a la entidad en el proceso de remediación, mediante actividades de sensibilización y asesoría orientadas a fortalecer las prácticas de seguridad de la información y reducir las vulnerabilidades identificadas durante las pruebas realizadas. Entregables: - Presentación de socialización de resultados. - Acta o registro de la sesión realizada con el equipo de TI.

	- Evidencias de las actividades de sensibilización y acompañamiento en la remediación.
Identificación adicional requerida	Todas las pruebas que se realicen en el marco del contrato deberán ejecutarse estrictamente conforme al plan de trabajo, alcance técnico y período de ejecución previamente definidos y aprobados por el Archivo General de la Nación. Cualquier modificación deberá contar con autorización formal de la entidad. La información clasificada como confidencial (Pública clasificada o publica reservada) deberá permanecer cifrada tanto en reposo como en tránsito, utilizando mecanismos criptográficos robustos y acordes con estándares de seguridad reconocidos. El contratista deberá garantizar su adecuada custodia, evitando accesos no autorizados, divulgación, copia o uso indebido. Dicha información únicamente podrá ser compartida con la entidad a través de los canales oficiales y seguros previamente establecidos.

METODOLOGÍA DE DESARROLLO

La metodología de desarrollo tiene como propósito definir el enfoque, las fases, actividades y entregables mediante los cuales se ejecutarán las pruebas de vulnerabilidad, las pruebas de ingeniería social, el proceso de remediación y las actividades de socialización en seguridad de la información en el Archivo General de la Nación.

Esta metodología se desarrollará de manera estructurada por fases, permitiendo garantizar una adecuada planeación, ejecución, análisis de resultados, remediación y fortalecimiento de las capacidades institucionales en materia de ciberseguridad.

FASE	PRODUCTO	CONTENIDO
FASE I Planeación y definición del alcance.	Plan de trabajo y gestión del proyecto	En esta fase se realizará el entendimiento del contexto tecnológico y organizacional de la entidad, así como la definición del alcance técnico de las actividades a ejecutar. Para esta fase se debe tener en cuenta lo descrito en cada uno de los ítems. Durante esta etapa se deberá:

		- Levantar información sobre la infraestructura tecnológica, activos de información y usuarios objeto de pruebas. - Definir el alcance de las pruebas de Ethical Hacking, Re-Test, ingeniería social y actividades de sensibilización. - Elaborar el plan de trabajo del proyecto, incluyendo cronograma, recursos, responsables y ventanas de ejecución. - Establecer la metodología técnica que se utilizará para el desarrollo de cada uno de los componentes del servicio. - Definir el plan de gestión de riesgos asociados a la ejecución de las pruebas e inherentes al proyecto que puedan afectar tanto la ejecución o la calidad de los entregables, esto con el fin de establecer acciones o controles previos a la materialización de los mismos. - Establecer el plan de manejo de incidentes o proceso de remediación en caso de afectación de servicios determinando responsables y canales de comunicación. - Definir el plan de comunicaciones y los mecanismos de coordinación con el equipo de Tecnologías de la Información del AGN. - Incluir los entregables Quincenales que se debe enviar al supervisor, en el cual se evidencie un avance de las actividades desarrolladas, novedades o eventualidades presentadas.
FASE II Ejecución de pruebas de seguridad	Ejecución del análisis de vulnerabilidades, Pentesting, en la plataforma tecnológica de la entidad. Pruebas de ingeniería social.	En esta fase se ejecutarán las actividades técnicas orientadas a identificar vulnerabilidades en la infraestructura tecnológica y en el comportamiento de los usuarios frente a ataques de ingeniería social, cumpliendo con lo establecido en los ítems 1 y 3. *Pruebas de Ethical Hacking o Pentesting* Se realizarán pruebas de análisis de vulnerabilidades y pruebas de penetración sobre los componentes de la infraestructura tecnológica definidos en el alcance, incluyendo servidores, aplicaciones, redes,

		firewalls, sistemas de almacenamiento y servicios expuestos a internet. Las pruebas deberán desarrollarse bajo las especificaciones definidas en el Item 1, teniendo en cuenta las metodologías reconocidas internacionalmente, tales como: ☐ OWASP para pruebas de seguridad en aplicaciones web. ☐ OSSTMM para pruebas de seguridad en infraestructura. ☐ Referencias de vulnerabilidades CVE/MITRE. Las pruebas deberán incluir, como mínimo: ☐ Escaneo automatizado de vulnerabilidades. ☐ Validación manual de hallazgos. ☐ Evaluación de configuraciones inseguras. ☐ Pruebas de autenticación y autorización. ☐ Identificación de puertos y servicios expuestos. ☐ Simulación de ataques internos y externos. *Pruebas de Ingeniería Social* Se ejecutarán campañas controladas para evaluar el nivel de concienciación del personal frente a ataques de ingeniería social. Estas pruebas podrán incluir: ☐ Phishing mediante correos electrónicos simulados. ☐ Baiting mediante dispositivos o archivos señuelo. ☐ Pruebas físicas orientadas a identificar vulnerabilidades en el manejo de información y acceso a equipos.
	Informe Quincenal	Entregar un informe de las actividades realizadas cada 15 días durante el periodo de ejecución del contrato o cuando el supervisor lo requiera, indicando el estado de avance de

		las actividades de acuerdo con lo definido en el plan de trabajo.
FASE III Análisis de resultados y elaboración de informes	Informes Técnicos del análisis de vulnerabilidades, Ethical Hacking e ingeniería social	Una vez finalizadas las pruebas técnicas y de ingeniería social, se realizará el análisis integral de los resultados obtenidos. En esta fase s e deberán elaborar los informes técnicos y ejecutivos, junto con sus anexos de acuerdo con lo especificado en los ítems 1, 2 y 3: *Informe Técnico del análisis de vulnerabilidades, Ethical Hacking* Documento detallado que incluya: ☐ Metodología aplicada. ☐ Alcance evaluado. ☐ Vulnerabilidades identificadas. ☐ Evidencias técnicas. ☐ Nivel de criticidad de los hallazgos. ☐ Evaluación de impacto y riesgos asociados. ☐ Recomendaciones de mitigación. *Matriz de vulnerabilidades* Documento editable con el registro detallado de las vulnerabilidades identificadas, clasificadas por criticidad. *Matriz de riesgos* Documento que permita evaluar el impacto y probabilidad de los riesgos asociados a las vulnerabilidades detectadas. *Hoja de ruta o plan de remediación* Documento que establezca las acciones necesarias para mitigar las vulnerabilidades identificadas, priorizadas en corto, mediano y largo plazo. *Informe Técnico de pruebas de ingeniería social* • Metodología aplicada. • Alcance • Análisis de las vulnerabilidades identificadas. • Análisis de riesgos.

		• Recomendaciones de mejora.
	Informes ejecutivos del análisis de vulnerabilidades y Ethical Hacking	Resumen de los informes técnicos, con clasificación de comportamiento y tipificación de las vulnerabilidades detectadas, donde muestre de manera general las vulnerabilidades, amenazas y recomendaciones, con el fin de presentarlo sin comprometer la seguridad de la infraestructura de TI. Documento dirigido a la alta dirección que resuma los resultados del ejercicio sin comprometer la seguridad de la infraestructura tecnológica.
FASE IV Socialización de resultados y acompañamiento en remediación	Socialización de resultados	En esta fase se realizará la presentación formal de los resultados al equipo de Tecnologías de la Información del AGN. Durante esta etapa se desarrollarán las siguientes actividades: ☐ Socialización de los hallazgos identificados. ☐ Explicación del nivel de criticidad de las vulnerabilidades. ☐ Presentación del plan de remediación. ☐ Priorización de acciones correctivas. ☐ Resolución de inquietudes técnicas del equipo institucional. Para la socialización se deberá tener en cuenta los descrito en cada uno de los ítems.
	Acompañamiento en remediación	Apoyar a la entidad en las actividades de remediación de los hallazgos encontrados con el apoyo de los especialistas de la infraestructura del AGN, quienes aplicarán los cambios y configuraciones con el apoyo del contratista.

FASE V RE-TEST y validación de medidas correctivas	Ejecución de las pruebas de Re- Test	Posteriormente a la implementación de las acciones de remediación priorizadas, se realizará un proceso de Re-Test, con el fin de validar la efectividad de las medidas implementadas. Durante esta fase se verificará: ☐ La mitigación de vulnerabilidades previamente identificadas. ☐ La persistencia de vulnerabilidades no corregidas. ☐ La aparición de nuevos hallazgos derivados de cambios en la infraestructura.
FASE V I Análisis de resultados y elaboración de informes finales	Informe Técnico Re-Test	Entregar un informe técnico con evidencia de corrección de vulnerabilidades detectadas previamente, las pendientes y demás especificidades del ítem 2.
	Informes Técnicos y ejecutivos Finales	Como resultado se generarán los siguientes documentos: ☐ Matriz de vulnerabilidades actualizada. ☐ Plan de remediación actualizado. ☐ Informe técnico final consolidado. ☐ Informe ejecutivo final. Lo documentos deben contener lo descrito en cada uno de los ítems. Informe Técnico Final que concluya todo el proyecto, Actualizando el informe entregado en la Fase I, II y III, junto con sus anexos, con los resultados obtenidos en las diferentes pruebas, verificando si se debe modificar el plan de remediación, la hoja de ruta, los riesgos, recomendaciones y demás capítulos del informe técnico entregado previo a la prueba del Re-Test.
	Informe Ejecutivo Final	Informe gerencial final que resuma el informe técnico Final, incluyendo cada una de las pruebas realizadas en las fases II y III y presente una idea sobre el estado de la

		plataforma posterior a la implementación del plan de remediación.

PERSONAL MINIMO REQUERIDO

Perfil	Formación profesional	Experiencia	Documentación
Gerente de proyecto	Profesional en ingeniería de sistemas, electrónica, telemática, telecomunicaciones o en cualquiera de las ingenierías afines registradas en el SNIES (sistema nacional de información de educación superior)	• Mínimo cuatro (4) años de experiencia profesional, contados a partir de la expedición de la tarjeta profesional. • Mínimo tres (3) años de experiencia especifica en gerencia de proyectos, la cual será verificada mediante certificaciones laborales que acrediten el tiempo y las actividades desarrolladas en los contratos.	· Hoja de vida. · Diploma o acta de grado de la Universidad. · Copia de la matrícula profesional. · Copia de Certificado de Vigencia y Antecedentes Disciplinarios del COPNIA o de la autoridad competente, vigente al cierre del proceso. · Certificado en ISO 27001
Ingeniero	Profesional en ingeniería de sistemas, electrónica, telemática, telecomunicaciones o en cualquiera de las ingenierías afines registradas en el SNIES (sistema nacional de información de educación superior)	• Mínimo cuatro (4) años de experiencia profesional contados a partir de la expedición de la tarjeta profesional • Mínimo tres (3) años de experiencia especifica en ejecución de pruebas de penetración, Ethical Hacking y análisis de vulnerabilidades, la cual será verificada mediante certificaciones laborales que acrediten el tiempo y las actividades desarrolladas en los contratos.	· Hoja de vida. · Diploma o acta de grado de la Universidad · Copia de la matrícula profesional · Copia de Certificado de Vigencia y Antecedentes Disciplinarios del COPNIA o de la autoridad competente, vigente al cierre del proceso. · Certificación CEH (Certified Ethical Hacker). Se aceptará como equivalente o superior a la certificación CEH, las certificaciones OSCP (*Offensive Security Certified Professional*), con el

			fin de asegurar que el profesional cuenta con habilidades prácticas probadas en entornos de explotación controlada.

DEPENDENCIA SOLICITANTE: GRUPO DE TECNOLOGÍAS DE LA INFORMACIÓN

Firma: _____
Nombre: **Jackson Miguel Velandia Bautista**
Cargo: **Coordinador Grupo de Tecnologías de la información**

Proyectó: Katherine Junca Ortiz – contratista Grupo Tecnologías de la Información
Revisó: Lady Alexandra Solano López – contratista Grupo Tecnologías de la Información
Fecha: Abril 2026
Archivado en: Serie contratos – Oficina Asesora Jurídica