Fecha de la Reunión

DÍA	MES	AÑO
23	09	2025

1. INFORMACIÓN GENERAL

NÚMERO DE CONTRATO	325-2025
TIPO DE CONTRATO	PRESTACIÓN DE SERVICIOS
VALOR DE CONTRATO	$29.750.400
FECHA DE INICIACIÓN	23 septiembre de 2025
PLAZO DE EJECUCIÓN	Dos (2) meses
FECHA DE TERMINACIÓN	15 diciembre de 2025
SUPERVISOR ETITC	Ing. ANGELA A. PULIDO R.

2. PARTICIPANTES

2.1 ASISTENTES	2.2 AUSENTES
ALEXANDER BRICEÑO GODOY (OBIKA S.A.S.) CHRISTIAN FABIAN RUBIANO (OBIKA S.A.S.) DIANA PILAR PINZON (OBIKA S.A.S.) Ing. ANGELA A. PULIDO R. (GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ETITC)	

2.3 INVITADOS
N/A

2.4 OBSERVACIONES
El supervisor del contrato verifica el total cumplimiento de documentación en SECOP contrato 325-2025

Hora de Inicio	**04:00**	**p.m.**	**OBSERVACIONES:**

3. DESARROLLO DE LA REUNIÓN

3.1 PRINCIPALES DISCUSIONES Y CONCLUSIONES (Describir las obligaciones generales y específicas del contratista y demás ítems que considere relevantes para la supervisión)

Se hace presentación formal del equipo que forma parte de OBIKA S.A.S., así mismo como el profesional de seguridad de la información de la Escuela Tecnológica Instituto Técnico Central.

En base al objeto del presente contrato: “PRESTACIÓN DE SERVICIO ESPECIALIZADO PARA REALIZAR EL ANÁLISIS DE VULNERABILIDADES CAJA BLANCA (WHITE BOX) Y PRUEBAS DE INTRUSIÓN (ETHICAL HACKING) FÍSICAS Y LÓGICAS A LOS SISTEMAS DE INFORMACIÓN DE LA ESCUELA TECNOLÓGICA INSTITUTO TÉCNICO CENTRAL Y SUS SEDES.”

A continuación, se mencionan las obligaciones contractuales así:

Fase 1: Preparación y Validación Técnica

1. Definición del alcance técnico del servicio

El análisis debe realizarse bajo la modalidad "White Box" 15 puntos externos, es decir, con información previa sobre la infraestructura interna del Instituto. Evaluación técnica de los activos expuestos a internet con su respectivo plan de remediación, incluyendo:

• Servidores web
• Aplicaciones web institucionales
• Dispositivos de red con acceso público
• IPs y dominios autorizados para la prueba
• Simulación de ataques externos controlados para identificar vulnerabilidades explotables.
• No se permite la ejecución de pruebas destructivas ni la interrupción de los servicios

- https://siac.itc.edu.co/
- https://mantum.etitc.edu.co/mantum/publico/
- https://itc.gnosoft.com.co/inicioV2/index.jsp

- https://academusoft.etitc.edu.co/itec/hermesoft/portalIG/home_1/publicacion/publicado/index.htm
- https://permanencia.itc.edu.co
- https://bolsadeempleo.itc.edu.co/
- https://www.emitc.co/radio/
- https://intranet.etitc.edu.co/
- https://ninos.itc.edu.co/
- https://etitc.edu.co/es/
- https://kawak.com.co/itc/
- https://mesadeayuda.etitc.edu.co/
- https://revistas.itc.edu.co/index.php/letras
- https://campusvirtualedigital.etitc.edu.co/
- https://www.etitc.edu.co/es/page/informativo

2. Definición de puntos internos de prueba White Box

Se requiere análisis de vulnerabilidad interno de White Box a (3) Puntos Internos:
- Red Local (1 Punto) Administrativa Sede Principal
- Académica (1 Punto) Sede Principal
- Académica (1 Punto) Sede Tintal

3. Definición de la Metodología

La metodología empleada deberá estar basada en estándares reconocidos internacionalmente, tales como:
• OWASP Top 10
• NIST SP 800-115
• MITRE ATT&CK
• OSSTMM o similar

4. Selección de Herramientas

Las herramientas utilizadas deben ser reconocidas en el sector de ciberseguridad, tales como:
• Nmap, Nessus, Burp Suite, Nikto, Acunetix, entre otras.

El uso de herramientas debe cumplir con criterios de legalidad y estar autorizado por licencias cuando aplique. Se deben registrar y documentar las herramientas utilizadas y su configuración durante el proceso

Fase 2: Ejecución del Análisis y Pruebas

Objetivo: Realizar pruebas prácticas, identificar vulnerabilidades, validar la remediación y socializar resultados.

1. **Ejecución de pruebas de Ethical Hacking internas y externas**

   •Escaneo y análisis de vulnerabilidades White Box en la infraestructura definida.
   • Simulación de ataques externos controlados

2. **Aplicación de ejercicio de ingeniería social**
   Se debe de realizar un (1) ejercicio de ingeniería social, el cual se desplegará mediante campañas diferenciadas por áreas del mapa de procesos. Cada campaña incluirá el diseño, adquisición de dominio, despliegue y análisis de resultados. La muestra total será de 250 usuarios (funcionarios, docentes y estudiantes), distribuidos proporcionalmente por área, de acuerdo con las directrices definidas por la entidad.

3. **Entrega de Informe técnico**
   El proveedor deberá entregar un informe técnico que incluya como mínimo:

   Resumen ejecutivo de los hallazgos.
   • Listado de vulnerabilidades encontradas, con:
   - Descripción
   - Nivel de criticidad (bajo, medio, alto, crítico)
   - Evidencias técnicas
   - Recomendaciones específicas de remediación.
   - Mapa de riesgos técnicos y análisis de impacto.
   - Recomendaciones de mejora priorizadas.
   - Anexos técnicos (registros, pruebas, escaneos, logs).

4. **Informe de Remediación**

Documentación de acciones correctivas implementadas por la entidad.

El alcance del informe de remediación comprende la documentación de hallazgos y las recomendaciones de acciones correctivas derivadas de las pruebas realizadas. La implementación de dichas acciones será responsabilidad de la entidad. No obstante, el proveedor brindará asesoría y acompañamiento experto para orientar la priorización y aplicación de las medidas sugeridas, sin sustituir la gestión interna de la ETITC.

5. Retesting (después de 8 días hábiles)

Un (1) RETESTING que contenga:

• Validación de cierre de vulnerabilidades previamente detectadas.
• Entrega de Informe de Retesting.

*S*e debe aplicar una metodología sistemática de identificación, validación, clasificación y reporte de vulnerabilidades.

6. Reunión de socialización de resultados
• Se debe realizar una reunión (presencial o virtual) para la presentación de resultados al equipo técnico y directivo del Instituto.
• El proveedor debe explicar los hallazgos, resolver dudas y apoyar la comprensión técnica del informe entregado.

Confidencialidad

Se debe firmar un Acuerdo de Confidencialidad (NDA) para proteger la información evaluada.
El proveedor se compromete a no almacenar, divulgar ni utilizar con fines distintos los datos, configuraciones, accesos o información sensible a la que tenga acceso durante el proceso.
Estas actividades deben ser ejecutadas con recursos tecnológicos y humanos certificados. Las herramientas tecnológicas utilizadas deben ser aprobadas por el supervisor del contrato, en caso de requerirse licenciamiento de uso el contratista deberá contar con dicho licenciamiento.
La Escuela Tecnológica Instituto Técnico Central – ETITC, en su compromiso con el fortalecimiento institucional y la mejora continua de la calidad en la prestación de sus servicios, ha consolidado una estructura organizativa que le permite avanzar en el cumplimiento de su misión. En este contexto, la Oficina Asesora de Planeación desempeña un papel estratégico como responsable del diseño, seguimiento y evaluación de planes, programas y proyectos, garantizando la adecuada aplicación de normas y procedimientos vigentes, en concordancia con el Plan de Desarrollo Institucional y los lineamientos del Gobierno Nacional.
Como parte del Sistema Interno de Aseguramiento de la Calidad, la ETITC ha implementado el Modelo Integrado de Planeación y Gestión (MIPG), articulando principios de equidad, inclusión, sostenibilidad y responsabilidad ambiental. En esta lógica, el aseguramiento de la calidad institucional incorpora elementos claves como el registro calificado, la acreditación de alta calidad, la autoevaluación permanente y la integración de sistemas de gestión, incluyendo el Sistema de Gestión de Seguridad de la Información (SGSI).
En coherencia con este compromiso, la institución se encuentra certificada en la norma ISO/IEC 27001:2022, “Seguridad de la Información, Ciberseguridad y Protección de la Privacidad”, la cual establece los requisitos para implementar, mantener y mejorar un sistema de gestión de la seguridad de la información. Esta norma fue actualizada a nivel internacional el 25 de octubre de 2022 y, en atención a sus lineamientos, la ETITC expidió el Acuerdo No. 012 del 26 de julio de 2024, mediante el cual se aprueba la nueva Política de Seguridad de la Información, ajustada

al Modelo de Seguridad y Privacidad de la Información del Gobierno Digital.

Obligaciones Generales del Contratista:

1. Responder por sus actuaciones y omisiones derivadas de la celebración del contrato y de la ejecución de este, de conformidad con lo establecido en las Leyes.
2. Cumplir con las obligaciones en los sistemas de seguridad social conforme al artículo 23 de la Ley 1150 de 2007 y el artículo 50 de la Ley 789 de 2002 o las normas legales que lo modifiquen, adicionen o complemente.
3. Mantener indemne a la ETITC de cualquier reclamación proveniente de terceros que tenga como causa sus actuaciones en el desarrollo y ejecución del contrato.
4. No acceder a peticiones o amenazas de grupos que actúen por fuera de la Ley con el fin de obligarlos a hacer u omitir algún acto o hecho.
5. Velar por la adecuada y racional utilización de los recursos de la ETITC y demás equipos y elementos que sean destinados para el cumplimiento de sus actividades contractuales.
6. Reportar oportunamente las anomalías en el desarrollo del objeto contractual y proponer alternativas de solución.
7. Dar aplicación al principio de debida diligencia y, en consecuencia, revisar, estudiar y analizar la información existente, a fin de construir un concepto respecto a la ejecución del contrato.
8. Poner a disposición de la ejecución del contrato toda su idoneidad y experiencia, a fin de ejecutar las actividades con los más altos estándares de calidad y eficiencia, para lo cual proporcionará la asistencia y acompañamiento técnico, jurídico y financiero a que haya lugar.
9. Prestar la asesoría y asistencia técnica necesaria para la ejecución de las actividades del objeto del contrato.
10. Desarrollar las actividades administrativas, técnicas, jurídicas y financieras que permitan el cumplimiento del objeto del contrato.
11. Adelantar bajo su exclusivo riesgo y responsabilidad, los trámites contractuales a que haya lugar para adelantar los procesos de selección y contratación de las personas naturales o jurídicas para ejecutar el objeto del contrato, cuando haya lugar a ello.
12. Adelantar todos los trámites necesarios para entregar los bienes y servicios del contrato señaladas en la propuesta, de acuerdo con las especificaciones técnicas, establecidas por la ETITC; para tal efecto se suscribirá la respectiva acta de entrega a satisfacción del contratante.
13. Manejar de manera centralizada y segura, todos los documentos relacionados con los aspectos jurídicos, financieros y administrativos que se generen en desarrollo del contrato, sujetándose en lo pertinente a las normas de retención documental vigentes aplicables.
14. Suscribir junto con la ETITC las actas de iniciación, entrega y liquidación del contrato.
15. Garantizar que el personal del contratista que se encuentre en las instalaciones de la ETITC permanezca identificado y carnetizado.
16. Guardar estricta reserva sobre toda la información y documentos que tenga acceso, maneje en desarrollo de su actividad o que llegue a conocer en desarrollo del contrato y que no tenga carácter de pública. En consecuencia, se obliga a no divulgar por ningún medio dicha información o documentos a terceros, sin la previa autorización escrita de la ETITC.

17. Mantener correctamente actualizados cada uno de los sistemas de información que maneje en desarrollo de su actividad.
18. El adjudicatario del contrato deberá aportar la Certificación Bancaria como requisito indispensable para la celebración del contrato y expedición del correspondiente Registro Presupuestal.
19. Aplicar los procedimientos establecidos para el manejo seguro de residuos ordinarios y peligrosos respetando los principios de separación en la fuente, que se han adoptado en la entidad.
20. Hacer un uso eficiente de los recursos a su cargo y poner en práctica estrategias de ahorro y uso eficiente de agua potable, energía eléctrica y papel de impresión, así como propender en la disminución en la generación de residuos.
21. Realizar sus actividades propendiendo por el cuidado del ambiente y la prevención de la contaminación.

Obligaciones Específicas del Contratista:

1. Plan de trabajo y metodología

Elaborar y presentar, en un plazo no mayor a diez (10) días hábiles siguientes a la suscripción del contrato, el plan de trabajo del objeto contractual, bajo lineamientos metodológicos reconocidos (PMI, OWASP, OSSTMM, WSTG, NIST u otros aplicables).

- El plan deberá incluir: etapas de ejecución de las pruebas, cronograma detallado, técnicas y herramientas a utilizar, equipo de trabajo por parte del contratista y de la ETITC, canales de comunicación y plan de contingencia.
- Dicho plan será coordinado con la Entidad y aprobado por el supervisor del contrato.

2. Ejecución de pruebas

• Realizar pruebas de análisis de vulnerabilidades caja blanca (White Box) y de intrusión (penetration testing) internas y externas, tanto físicas como lógicas, dentro de las franjas horarias autorizadas por la Entidad, asegurando que las actividades no afecten la continuidad de los servicios críticos.

• Garantizar que las pruebas se ejecuten con software, hardware y recurso humano idóneo dispuesto por el contratista.

3. CONFIDENCIALIDAD Y AUTORIZACIÓN

• Suscribir y cumplir estrictamente el acuerdo de autorización de pruebas y explotación de vulnerabilidades con la ETITC.

• Mantener confidencialidad absoluta sobre la información, hallazgos, accesos y resultados obtenidos durante la ejecución del contrato.

4. INFORMES Y ENTREGABLES

• Entregar los documentos establecidos en el anexo técnico, organizados de forma clara, verificable y completa:

- Resumen ejecutivo (fecha y hora de ejecución de los escaneos).
- Informe técnico White Box interno.
- Informe técnico Gray Box externo sobre las redes.
- Matriz de vulnerabilidades priorizadas por nivel de criticidad (CVE, OWASP u otros estándares).

- Informe de remediación con plan de mitigación sugerido.
- Informe de Retesting, realizado dentro de los quince (15) días calendario posteriores a la entrega del informe de remediación.

- Los informes deberán incluir conclusiones, evidencias de hallazgos, resultados técnicos, y recomendaciones de mejora.

5. SOCIALIZACIÓN Y COMUNICACIÓN

- Exponer los resultados a nivel técnico y gerencial, en al menos dos jornadas:
  a) Una técnica, dirigida a los equipos de TI y seguridad de la información.
  b) Una ejecutiva, dirigida a la alta dirección, con enfoque en riesgos e impacto estratégico.
- Atender reuniones de seguimiento convocadas por la Entidad, levantando las respectivas actas.
- Garantizar canales de comunicación disponibles durante la vigencia del contrato (línea telefónica, correo electrónico, chat, mesa de ayuda u otros).

6. CUMPLIMIENTO NORMATIVO Y SEGURIDAD

- Cumplir con la normativa aplicable en Colombia en materia de seguridad de la información y protección de datos personales (Ley 1581 de 2012 y sus decretos reglamentarios).
- Garantizar el correcto uso de accesos y credenciales proporcionados por la Entidad (VPN, usuarios de prueba, contraseñas, etc.).
- Definir y aplicar un plan de contingencia que minimice el impacto de las pruebas sobre los sistemas de información de la ETITC.

7. GESTIÓN DE HALLAZGOS CRÍTICOS

- Informar de manera inmediata al supervisor del contrato sobre las vulnerabilidades de alto impacto o críticas que se identifiquen, que pongan en riesgo la seguridad de la información o la operación institucional, recomendando acciones de mitigación inmediatas.

8. GESTIÓN DE PERSONAL

- Informar a la Entidad, en un plazo no mayor a veinticuatro (24) horas hábiles, sobre la ausencia definitiva de algún profesional del equipo asignado y presentar candidatos en iguales o mejores condiciones. La aprobación del nuevo profesional estará sujeta a la validación del supervisor del contrato.

9. CIERRE DEL CONTRATO

- Elaborar el acta de cierre contractual una vez se hayan entregado y aceptado a satisfacción todos los entregables.
- Presentar la documentación de soporte de actividades, registros de asistencia, actas de reuniones, reportes de ejecución y demás documentos conforme a los lineamientos de la Entidad.

Obligaciones contractuales asociadas a los Sistemas de Gestión Integrados:

1. Atender los lineamientos y políticas generales, así como dar cumplimiento a los procesos, procedimientos, manuales, lineamientos y demás documentos del Sistema de Gestión

Integrado definidos por la ETITC que se relacionen con el objeto del contrato.
2. Asistir y participar en las reuniones y actividades programadas en el marco del Sistema de Gestión Integrado; así como sugerir medidas que contribuyan a su mantenimiento y mejora, cuando sea conveniente.
3. Garantizar y generar los soportes que evidencien el cumplimiento de requisitos legales asociados a la ejecución del contrato, en el marco del Sistema de Gestión Integrado.

Sistema de Gestión de Seguridad y Salud en el Trabajo:

1. De acuerdo documento interno de la entidad. MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL TRABAJO Y AMBIENTAL PARA CONTRATISTAS, SUBCONTRATISTAS Y PROVEDORES SSTMA-01 https://www.etitc.edu.co/archives/calidad/SST-MA-01.pdf
2. Reportar oportunamente cualquier acto, condición insegura o accidente que observen o tengan.
3. Utilizar los elementos de Protección Personal que la ETITC le ha asignado y mantenerlos adecuadamente dándole el uso debido.
4. Participar en proceso de inducción y así conocer el plan de emergencias y casos de actuación en caso de emergencia.

Sistema de Gestión Ambiental:

1. Revisar las obligaciones y especificaciones técnicas aplicables contenidas en el MANUAL DEL SISTEMA DE GESTION DE SEGURIDAD Y SALUD EN EL TRABAJO Y AMBIENTAL PARA CONTRATISTAS, SUBCONTRATISTAS Y PROVEDORES.
2. El CONTRATISTA es responsable de las obligaciones establecidas para el desarrollo de la Gestión Ambiental, por lo que deben implementar dentro de sus actividades las medidas de prevención, control, mitigación, compensación o corrección de aquellos impactos que se puedan generar en el desarrollo de su actividad.
3. Remitir a la entidad las evidencias sobre la gestión ambiental que adelanta el proyecto, obra o actividad para mitigar y controlar sus impactos ambientales en el marco del objeto contractual.
4. Remitir a la entidad el análisis de ciclo de vida del bien o servicio a suministrar identificando los impactos ambientales en cada etapa: extracción de materia prima, producción, distribución, uso, consumo y disposición final o final de la actividad.

6.6 Sistema de Gestión de Seguridad de la Información:

1. Conocer y aplicar los lineamientos establecidos en la Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad de la Información de la ETITC.

2. Mantener la integridad, reserva, responsabilidad y confidencialidad de la información que conozca con ocasión del acceso a los activos de información (documentos, bases de datos, sistemas de información, material físico y digital), que la entidad le proporcione en el ejercicio de sus obligaciones contractuales, de conformidad con la normativa vigente que incluye Derechos de Autor, Protección de datos personales y Transparencia y Acceso a la Información Pública.

3. Respetar la confidencialidad de la información entregada por otras fuentes en la ETITC, en el ejercicio de sus obligaciones contractuales.

a) Abstenerse de revelar y divulgar la información clasificada, reservada, confidencial y/o con datos personales sensibles, privados, que utilice la ETITC, en el ejercicio de sus obligaciones contractuales, ni dentro de los dos años siguientes a la finalización de estas, sin previo consentimiento por escrito en la ETITC, siendo consciente de las penas, multas y sanciones derivadas del incumplimiento, al igual de las demás acciones que puedan llegar a derivarse de éste.
b) Con la firma del contrato autorizo a la Escuela Tecnológica Instituto Técnico Central para realizar la recolección y tratamiento de mis datos personales de conformidad al cumplimiento de la Ley 1581 de 2012 o Ley de Protección de Datos Personales, la cual se encuentra publicado en el sitio web. https://www.etitc.edu.co/es/page/nosotros&seguridad-portal

En caso donde los Contratistas vinculados a los procesos de Gestión de Informática y Telecomunicaciones y del Sistema de Gestión de Seguridad de la Información se debe tener en cuenta las siguientes obligaciones:

1. Reportar los incidentes de seguridad que se presenten en los activos y/o servicios afectados de manera inmediata al área del Sistema de Gestión de Seguridad de la Información a través del correo institucional (mesadeayuda@itc.edu.co).

2. Entregar informes de implementación y de soporte, utilizando las técnicas y metodología de anonimización de acuerdo con el GSI-MA-02.

3. Suscribir el Acuerdo de Confidencialidad DNS como una buena práctica para garantizar la Confidencialidad de la Información.

Cuando se requiera la ETITC, solicitará la participación de auditoría para gestionar los riesgos de seguridad asociados con el uso de productos o servicios prestados a la entidad.

OBLIGACIONES DE LA ETITC: Además de las obligaciones y estipulaciones señaladas en las Leyes 80 de 1993 y 1150 de 2007, así como las que se deriven del Decreto 1082 de 2015, LA ETITC se obliga a:

1. Expedir el Registro Presupuestal del contrato.
2. Efectuar los pagos estipulados en el contrato en la forma y oportunidad previstas en el mismo.
3. Designar el supervisor para vigilar el cumplimiento del objeto contractual dentro del término de ejecución y demás condiciones establecidas.
4. Prestar toda la colaboración necesaria para la debida ejecución del contrato.
5. Suministrar al CONTRATISTA la información requerida para el desarrollo del objeto contractual.
6. Vigilar el cumplimiento de todas y cada una de las obligaciones que se deriven del presente contrato.
7. Exigir a EL CONTRATISTA la ejecución idónea y oportuna de las obligaciones del presente contrato.

8. Efectuar la supervisión y seguimiento del presente contrato.

4. ANEXOS

Dando cumplimiento al objetivo, se da por terminada la sesión.

Hora de finalización	**5:00**	**p.m.**	**Observaciones**

En Constancia firman:

Ing. ANGELA A. PULIDO R. GESTIÓN DE SEGURIDAD DE LAINFORMACIÓN ETITC	ALEXANDER BRICEÑO GODOY (OBIKA S.A.S.)
SUPERVISOR DEL CONTRATO	**CONTRATISTA**