REPÚBLICA DE HONDURAS

ADMINISTRACIÓN ADUANERA DE HONDURAS

(ADUANAS)

TERMINOS DE REFERENCIA

PARA LA CONTRATACIÓN DE FIRMA AUDITORA

GOBIERNO DE LA REPÚBLICA DE HONDURAS

ADUANAS Administración Aduanera de Honduras

SERVICIOS DE AUDITORÍA FORENSE AL SISTEMA AUTOMATIZADO DE RENTAS ADUANERAS DE HONDURAS (SARAH) CORRESPONDIENTE AL PERÍODO COMPRENDIDO ENTRE ENERO DE 2024 Y ENERO DE 2026

TEGUCIGALPA M.D.C, FRANCISCO MORAZÁN

AGOSTO 2026

ADMINISTRACIÓN ADUANERA DE HONDURAS
ADUANAS
Gerencia
GERENCIA NACIONAL ADMINISTRATIVA Y FINANCIERA
REPÚBLICA DE HONDURAS

TÉRMINOS DE REFERENCIA
PARA LA CONTRATACIÓN DE FIRMA AUDITORA
AUDITORÍA FORENSE AL SISTEMA AUTOMATIZADO DE RENTAS ADUANERAS DE HONDURAS (SARAH)
CORRESPONDIENTE AL PERÍODO COMPRENDIDO ENTRE ENERO DE 2024 Y ENERO DE 2026

I. ANTECEDENTES

La Administración Aduanera de Honduras (AAH), en el marco de sus atribuciones legales, tiene la responsabilidad de administrar, controlar y fiscalizar las operaciones de comercio exterior, así como garantizar la correcta aplicación de la legislación aduanera y la recaudación de los tributos asociados a las operaciones de importación y exportación. Para el cumplimiento de estas funciones, la institución ha impulsado un proceso continuo de modernización tecnológica orientado a fortalecer la eficiencia operativa, la transparencia institucional y la facilitación del comercio. Como parte de este proceso de modernización, la Administración Aduanera implementó el Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH), plataforma informática que constituye el núcleo de los procesos operativos aduaneros del país y mediante la cual se administran las declaraciones aduaneras, la determinación y recaudación de tributos, el control de mercancías, la gestión de los diferentes regímenes aduaneros y la interoperabilidad con instituciones nacionales e internacionales relacionadas con el comercio exterior.

Durante los años de operación del sistema SARAH, la plataforma ha experimentado múltiples procesos de evolución tecnológica, incorporación de nuevos módulos funcionales, adecuaciones derivadas de reformas legales, integración con servicios electrónicos de otras entidades gubernamentales y mejoras orientadas a responder a las crecientes necesidades del comercio internacional y de la Administración Aduanera. Estas modificaciones han incrementado la complejidad técnica del sistema, así como el volumen de información crítica que administra y procesa diariamente.

Paralelamente, el entorno internacional en materia de ciberseguridad y protección de infraestructuras críticas ha evolucionado significativamente, incrementándose los riesgos asociados a amenazas cibernéticas, accesos no autorizados, manipulación de información, fraude informático, alteración de registros electrónicos y otras actividades que pueden comprometer la integridad y confiabilidad de los sistemas de información gubernamentales. Organismos internacionales como la Organización Mundial de Aduanas (OMA), la Organización Internacional de Normalización (ISO), el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST) e INTERPOL han recomendado el fortalecimiento de los mecanismos de auditoría, monitoreo y análisis forense como parte de las estrategias de gestión de riesgos tecnológicos y protección de infraestructuras críticas.

En este contexto, la Administración Aduanera de Honduras ha venido fortaleciendo su modelo de gobernanza tecnológica mediante la implementación de controles de seguridad de la información, mecanismos de trazabilidad de operaciones, políticas de gestión de riesgos, monitoreo de eventos de seguridad y procesos de mejora continua sobre sus plataformas tecnológicas. No obstante, considerando la criticidad del sistema SARAH para la recaudación

tributaria, la facilitación del comercio exterior y la seguridad nacional resulta necesario complementar dichos mecanismos mediante una evaluación especializada que permita verificar la integridad de la información, la consistencia de las transacciones registradas, la efectividad de los controles implementados y la adecuada preservación de la evidencia digital.

Asimismo, la creciente relevancia que ha adquirido la evidencia digital dentro de los procesos administrativos, disciplinarios y judiciales exige la aplicación de metodologías especializadas de auditoría forense informática que permitan identificar, recolectar, preservar, analizar y documentar evidencia electrónica conforme a estándares internacionalmente aceptados, garantizando su autenticidad, integridad y cadena de custodia.

En virtud de lo anterior, y considerando la importancia estratégica del Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH) para la gestión institucional y la protección de los recursos fiscales del Estado, la Administración Aduanera estima procedente la contratación de una auditoría forense informática especializada que permita obtener una evaluación técnica independiente sobre la integridad del sistema, fortalecer los mecanismos de control institucional y contribuir al mejoramiento continuo de la seguridad, transparencia y confiabilidad de las operaciones aduaneras.

II. JUSTIFICACIÓN

La Administración Aduanera de Honduras (AAH), gestiona y controla las operaciones vinculadas al comercio exterior a través del Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH), el cual constituye la principal plataforma tecnológica para la automatización y administración de los procesos aduaneros del país. Mediante este sistema se registran, procesan y controlan las declaraciones de importación y exportación, la liquidación y recaudación de tributos aduaneros, el control y seguimiento de mercancías, la administración de regímenes aduaneros especiales, así como la interoperabilidad con otras instituciones gubernamentales vinculadas a la gestión fiscal, comercial y de seguridad nacional.

El sistema SARAH procesa un volumen significativo de operaciones relacionadas con el comercio internacional, integrando información de carácter tributario, financiero, comercial y logístico, lo que lo convierte en un activo estratégico para el funcionamiento del sistema aduanero y para la adecuada recaudación de ingresos fiscales del Estado de Honduras. En consecuencia, la disponibilidad, integridad, confidencialidad y trazabilidad de la información gestionada por este sistema resultan elementos fundamentales para garantizar la transparencia de las operaciones aduaneras, la correcta determinación de obligaciones tributarias y el cumplimiento de la normativa vigente en materia de comercio exterior.

Asimismo, debido a la naturaleza sensible de la información procesada y al impacto económico que las operaciones aduaneras tienen en la recaudación fiscal, el sistema SARAH representa un componente crítico dentro de la infraestructura tecnológica del Estado. Cualquier alteración indebida de registros electrónicos, modificación no autorizada de declaraciones, manipulación de valores declarados o aranceles, eliminación de registros de auditoría o accesos indebidos al sistema podría generar impactos significativos en la recaudación tributaria, facilitar esquemas de defraudación aduanera o comprometer la confiabilidad institucional de la administración aduanera.

En este contexto, y considerando la necesidad de fortalecer los mecanismos de control institucional y garantizar la transparencia en la gestión de las operaciones aduaneras, se hace necesario llevar a cabo una auditoría forense informática especializada al Sistema SARAH. Esta auditoría permitirá evaluar la integridad de la información almacenada en el sistema, analizar la trazabilidad de las transacciones registradas, identificar posibles irregularidades o vulnerabilidades en los controles de seguridad informática y preservar evidencia digital conforme a estándares técnicos internacionalmente reconocidos, que pueda ser utilizada en eventuales procesos administrativos, disciplinarios o judiciales.

La realización de esta auditoría constituye, por tanto, una medida técnica y preventiva orientada a fortalecer la gobernanza institucional, garantizar la confiabilidad de los sistemas de información aduaneros y proteger los recursos económicos del Estado de Honduras derivados de las operaciones de comercio exterior.

El Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH) fue implementado con el propósito de modernizar y automatizar la gestión de las operaciones aduaneras en Honduras, constituyéndose en la plataforma tecnológica central mediante la cual la Administración Aduanera registra, procesa y controla las actividades vinculadas al comercio exterior. Este sistema permite gestionar de manera integrada múltiples procesos operativos y administrativos, contribuyendo a mejorar la eficiencia institucional, fortalecer los mecanismos de control y facilitar el cumplimiento de las obligaciones tributarias derivadas de las operaciones de importación y exportación. A través del sistema SARAH se desarrollan, entre otras, las siguientes funciones fundamentales:

- Registro y procesamiento de declaraciones de importación y exportación.
- Determinación, liquidación y recaudación de tributos aduaneros y otros gravámenes aplicables al comercio exterior.
- Control, seguimiento y trazabilidad de las mercancías que ingresan o salen del territorio nacional.
- Administración y control de los diferentes regímenes aduaneros especiales.
- Interoperabilidad e intercambio de información con otras instituciones del Estado vinculadas al comercio exterior, la recaudación tributaria y la seguridad nacional.

En virtud de su carácter transaccional y del volumen de operaciones que procesa, el sistema SARAH administra información de naturaleza tributaria, financiera, comercial y logística de alta relevancia para el Estado de Honduras. En consecuencia, la integridad, confiabilidad y trazabilidad de los registros electrónicos contenidos en dicho sistema resultan esenciales para garantizar la correcta determinación de los tributos aduaneros, el adecuado control del comercio exterior y la transparencia en la gestión institucional.

Bajo este contexto, cualquier manipulación indebida de registros, alteración de valores declarados, modificación no autorizada de aranceles, eliminación o alteración de registros de auditoría (logs), o accesos no autorizados al sistema podría generar impactos significativos en la recaudación tributaria del Estado, así como facilitar la implementación de esquemas de defraudación aduanera, evasión fiscal o prácticas de corrupción administrativa. Estas situaciones podrían además comprometer la credibilidad institucional de la Administración Aduanera de

Honduras y debilitar los mecanismos de control del comercio internacional.

Adicionalmente, debe considerarse que la evidencia digital contenida en los sistemas informáticos posee un carácter altamente volátil, lo que significa que puede ser modificada, sobrescrita o eliminada si no se aplican procedimientos técnicos adecuados para su preservación. Por tal razón, la identificación, recolección, análisis y conservación de este tipo de información requiere la aplicación de metodologías especializadas de auditoría forense informática que garanticen la integridad, autenticidad y trazabilidad de la evidencia digital, permitiendo su eventual utilización en procesos administrativos, disciplinarios o judiciales.

Considerando la criticidad del sistema SARAH dentro de la gestión aduanera del país, se hace necesario llevar a cabo una Auditoría Forense al Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH), con el propósito de analizar la integridad de la información almacenada, identificar posibles irregularidades o vulnerabilidades en el funcionamiento del sistema, reconstruir eventos o transacciones relevantes y determinar eventuales responsabilidades administrativas, civiles o penales derivadas de los hallazgos que pudieran detectarse. Asimismo, la realización de esta auditoría permitirá fortalecer los mecanismos de control interno, mejorar los niveles de seguridad de la información y contribuir al fortalecimiento de la transparencia y la rendición de cuentas en la gestión de la Administración Aduanera de Honduras.

III. OBJETIVO GENERAL Y ESPECIFICO DE LA AUDITORÍA

1. Objetivo General

Realizar una auditoría forense al Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH) con el propósito de evaluar la integridad, confiabilidad y trazabilidad de la información procesada y almacenada en dicho sistema, mediante la aplicación de técnicas especializadas de auditoría e investigación informática. Esta auditoría tiene como finalidad identificar posibles alteraciones indebidas de registros, accesos no autorizados, manipulaciones de datos o cualquier otra irregularidad que pudiera haber afectado el funcionamiento del sistema o la correcta gestión de las operaciones aduaneras.

Asimismo, el proceso de auditoría debe permitir analizar la seguridad del sistema, examinar la consistencia de las transacciones registradas, reconstruir eventos relevantes y preservar evidencia digital conforme a estándares técnicos internacionalmente reconocidos. Todo ello con el objetivo de generar información técnica confiable que contribuya a determinar eventuales responsabilidades administrativas, civiles o penales, así como a fortalecer los mecanismos de control institucional, la transparencia en la gestión aduanera y la protección de los recursos fiscales del Estado de Honduras.

2. Objetivos Específicos

Evaluar la integridad, consistencia y trazabilidad de la información almacenada en el Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH), verificando que los registros electrónicos correspondan fielmente a las operaciones realizadas y que no hayan sido objeto de modificaciones indebidas.

ADMINISTRACIÓN ADUANERA DE HONDURAS ADUANAS Gerencia GERENCIA NACIONAL ADMINISTRATIVA Y FINANCIERA REPÚBLICA DE HONDURAS

Analizar los registros de auditoría del sistema (logs), las transacciones registradas y los metadatos asociados, con el propósito de identificar actividades inusuales, patrones anómalos o eventos que puedan indicar manipulación de información o uso indebido del sistema.

Identificar accesos no autorizados o indebidos al sistema, así como la existencia de privilegios excesivos, uso compartido de credenciales o utilización inapropiada de cuentas de usuario que pudieran comprometer la seguridad y la confiabilidad de la información.

Verificar la integridad de las declaraciones aduaneras procesadas en el sistema, determinando si existieron modificaciones indebidas en valores declarados, tributos liquidados, clasificación arancelaria, aplicación de regímenes aduaneros o cualquier otro elemento que incida en la determinación de obligaciones tributarias. Evaluar la efectividad de los controles de seguridad informática implementados en el sistema, incluyendo mecanismos de autenticación, control de accesos, monitoreo de actividades, registro de eventos y protección de la integridad de la información.

Identificar vulnerabilidades técnicas o debilidades en la arquitectura del sistema, en la gestión de usuarios o en los mecanismos de control que pudieran haber sido explotadas para alterar registros, manipular transacciones o acceder de forma indebida a la información.

Cuantificar el posible impacto económico derivado de irregularidades detectadas, estimando el efecto que dichas irregularidades pudieran haber tenido en la recaudación de tributos aduaneros o en el control del comercio exterior.

Recolectar, preservar y documentar evidencia digital conforme a metodologías de auditoría forense informática y procedimientos de cadena de custodia, garantizando la integridad, autenticidad y trazabilidad de la información obtenida durante el proceso de auditoría.

Formular recomendaciones técnicas, administrativas y de control interno orientadas a fortalecer la seguridad del sistema, mejorar los mecanismos de monitoreo y prevenir la ocurrencia de irregularidades en la gestión del Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH).

IV. ALCANCE DE LA AUDITORÍA

La auditoría forense debe comprender el análisis técnico, funcional y de seguridad del Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH) en el período entre **enero de 2024 y enero de 2026,** con el propósito de evaluar la integridad, confiabilidad y trazabilidad de la información procesada en dicho sistema, así como identificar posibles irregularidades, vulnerabilidades o debilidades en los mecanismos de control implementados.

El análisis debe abarcar el periodo comprendido entre enero de 2024 y enero de 2026, considerando todas aquellas operaciones, registros electrónicos, configuraciones del sistema y actividades de usuarios que hayan sido registradas o ejecutadas durante dicho intervalo de tiempo.

La auditoría debe incluir la revisión y evaluación de los siguientes componentes:

INFRAESTRUCTURA TECNOLÓGICA

Se debe realizar una revisión técnica de la infraestructura tecnológica que soporta el funcionamiento del sistema SARAH, con el objetivo de evaluar la seguridad, disponibilidad y confiabilidad de los recursos tecnológicos utilizados. El análisis debe comprender, entre otros aspectos:

- Servidores del sistema, incluyendo servidores de aplicaciones, bases de datos y servidores asociados al funcionamiento del sistema.
- Infraestructura de red, considerando la arquitectura de comunicaciones, segmentación de red, dispositivos de seguridad y mecanismos de control de acceso a la red.
- Sistemas de almacenamiento de información, incluyendo repositorios de datos, unidades de almacenamiento y mecanismos de gestión de información.
- Sistemas de respaldo y recuperación de información, verificando la existencia, periodicidad y confiabilidad de los procesos de respaldo (backup) y recuperación ante incidentes o pérdida de datos.

BASES DE DATOS

Se debe realizar un análisis detallado de la estructura, arquitectura y funcionamiento de las bases de datos utilizadas por el sistema SARAH, con el propósito de verificar la integridad y consistencia de la información almacenada.

Este análisis debe incluir:

- Evaluación de la estructura y arquitectura de las bases de datos, incluyendo tablas, relaciones y mecanismos de control de integridad.
- Verificación de la integridad y consistencia de los registros almacenados, mediante técnicas de análisis de datos y validación de transacciones.
- Análisis de modificaciones realizadas en datos críticos, tales como valores declarados, tributos liquidados, clasificaciones arancelarias y demás registros relevantes para la determinación de obligaciones aduaneras.

TRANSACCIONES ADUANERAS

La auditoría forense debe comprender el análisis detallado de las transacciones registradas en el Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH) relacionadas con las operaciones de comercio exterior, con el propósito de verificar la integridad, consistencia y trazabilidad de la información registrada en el sistema durante el período objeto de revisión.

Dicho análisis debe permitir identificar posibles irregularidades, inconsistencias o modificaciones indebidas en los registros electrónicos que puedan afectar la correcta determinación de las obligaciones tributarias aduaneras o el adecuado control de las operaciones de importación y exportación. Asimismo, se debe evaluar si los procesos automatizados del sistema se ejecutan conforme a la normativa aduanera vigente y a los procedimientos institucionales establecidos.

En este sentido, la auditoría deberá examinar de manera integral los distintos componentes que intervienen en el registro y procesamiento de las operaciones aduaneras, considerando tanto las transacciones originales como las modificaciones posteriores que pudieran haberse realizado sobre los registros del sistema.

Entre los aspectos a evaluar se deberán incluir, como mínimo, los siguientes:

- Declaraciones de importación y exportación registradas en el sistema, verificando la integridad de los datos consignados, la correspondencia entre los registros electrónicos y la documentación de respaldo, así como la consistencia de la información declarada en relación con las operaciones de comercio exterior realizadas.
- Procesos de determinación, liquidación y pago de tributos aduaneros, incluyendo la correcta aplicación de aranceles, impuestos, tasas y demás gravámenes asociados a las operaciones de comercio exterior, con el fin de identificar posibles inconsistencias, errores de cálculo o alteraciones indebidas en los montos determinados.
- Registro y control de modificaciones efectuadas en las transacciones aduaneras, incluyendo cambios en valores declarados, clasificación arancelaria, cantidades, origen de mercancías, aplicación de exoneraciones, regímenes aduaneros especiales o cualquier otro dato relevante para la determinación de los tributos o el control de las mercancías.
- Historial de cambios o trazabilidad de las operaciones, verificando la existencia de registros que permitan identificar qué usuario realizó modificaciones en el sistema, en qué momento fueron efectuadas y bajo qué condiciones se autorizaron dichos cambios.
- Análisis de patrones de comportamiento en las transacciones registradas, con el fin de identificar operaciones atípicas, modificaciones recurrentes o cualquier otro indicio que pudiera evidenciar posibles irregularidades o debilidades en los controles del sistema.

El análisis de estas transacciones debe permitir determinar si los registros almacenados en el sistema SARAH reflejan de manera fiel y transparente las operaciones aduaneras realizadas, así como identificar posibles manipulaciones, inconsistencias o debilidades en los mecanismos de control que pudieran haber afectado la correcta gestión del comercio exterior y la recaudación de los tributos correspondientes.

GESTIÓN DE USUARIOS Y ACCESOS

Se deben analizar los mecanismos de gestión de usuarios y control de accesos al sistema, con el objetivo de

determinar si los privilegios y permisos asignados se encuentran debidamente controlados y alineados con los principios de seguridad informática.

Este análisis debe incluir:

- Administración de usuarios del sistema, incluyendo creación, modificación y eliminación de cuentas.
- Asignación de roles y niveles de privilegios, verificando la correcta segregación de funciones.
- Mecanismos de autenticación y control de accesos, así como posibles accesos indebidos o utilización inapropiada de cuentas de usuario.

REGISTROS DE AUDITORÍA DEL SISTEMA

Se debe realizar un análisis exhaustivo de los registros de auditoría (logs) generados por el sistema SARAH, con el propósito de identificar actividades irregulares, accesos indebidos o modificaciones no autorizadas de información. El análisis debe comprender:

- Registros de acceso al sistema, incluyendo autenticaciones exitosas y fallidas.
- Registros de modificación, actualización o eliminación de datos dentro del sistema.
- Eventos de seguridad informática, tales como intentos de acceso no autorizados, cambios en configuraciones del sistema o alteraciones de registros.

PRESERVACIÓN DE EVIDENCIA DIGITAL

Durante el desarrollo de la auditoría se deben aplicar procedimientos especializados para la identificación, recolección, preservación y análisis de evidencia digital, con el fin de garantizar su integridad y trazabilidad.
Entre las actividades previstas se debe incluir:

- Captura forense de servidores, bases de datos o repositorios de información, cuando sea necesario para el análisis técnico.
- Análisis de metadatos y registros electrónicos asociados a las transacciones del sistema.
- Reconstrucción cronológica de eventos y actividades realizadas dentro del sistema.
- Aplicación de procedimientos de cadena de custodia, garantizando la preservación y autenticidad de la evidencia digital obtenida.

EVALUACIÓN DE CONTROLES DE SEGURIDAD

Se debe evaluar la efectividad de los controles de seguridad informática implementados en el sistema SARAH, con

el propósito de identificar posibles vulnerabilidades o debilidades que puedan comprometer la integridad de la información o la confiabilidad del sistema.

Esta evaluación debe incluir:

- Controles de integridad y protección de datos, incluyendo mecanismos que permitan detectar modificaciones no autorizadas.
- Sistemas de monitoreo y supervisión del sistema, orientados a detectar actividades irregulares.
- Gestión de vulnerabilidades y actualización de sistemas, evaluando la existencia de procedimientos para la identificación y mitigación de riesgos tecnológicos.

V. MARCO LEGAL Y NORMATIVO

La ejecución de la presente auditoría forense se debe desarrollar en estricto apego al marco jurídico y normativo vigente en la República de Honduras, así como a los principios y buenas prácticas internacionalmente reconocidos en materia de auditoría, control interno, seguridad de la información e investigación forense digital.

En el ámbito nacional, la auditoría debe considerar como referencia, entre otras, las disposiciones establecidas en los siguientes instrumentos legales y normativos:

- Ley Aduanera de Honduras, que regula el régimen jurídico aplicable al control, fiscalización y administración de las operaciones de comercio exterior, así como las facultades de la autoridad aduanera para la determinación y recaudación de los tributos aduaneros, como ser CAUCA, RECAUCA, Código Tributario, y demás normativa aduanera aplicable.
- Código Tributario, que establece los principios, normas y procedimientos aplicables a la administración, fiscalización y control de las obligaciones tributarias, incluyendo las disposiciones relacionadas con la determinación de responsabilidades administrativas y sanciones por infracciones tributarias.
- Ley de Transparencia y Acceso a la Información Pública, que promueve la rendición de cuentas, la transparencia en la gestión pública y el acceso a la información generada por las instituciones del Estado.
- Ley de Administración Pública, que regula la organización, funcionamiento y responsabilidad de las instituciones del sector público, así como los principios de legalidad, eficiencia y control en la gestión administrativa.
- Ley Especial Contra el Lavado de Activos, en lo relativo a la prevención, detección e investigación de operaciones financieras o comerciales que puedan estar vinculadas a actividades ilícitas, incluyendo aquellas relacionadas con el comercio exterior.

- Normativa de control interno aplicable a las instituciones públicas, particularmente las disposiciones y lineamientos orientados al fortalecimiento de los mecanismos de control, supervisión y gestión de riesgos dentro de la administración pública.

Adicionalmente, la auditoría debe tomar en consideración las normas técnicas y estándares internacionales aplicables a la auditoría de sistemas de información, seguridad informática e investigación forense digital, con el propósito de garantizar que los procedimientos utilizados cumplan con criterios reconocidos de rigor técnico, confiabilidad y validez probatoria.

En este sentido, la auditoría se debe alinear con buenas prácticas internacionales tales como:

- ISO/IEC 27001 – Sistemas de Gestión de Seguridad de la Información, que establece los requisitos para la implementación, mantenimiento y mejora continua de los controles destinados a proteger la confidencialidad, integridad y disponibilidad de la información.
- COBIT (Control Objectives for Information and Related Technologies), marco de referencia internacional para la gobernanza y gestión de tecnologías de información, ampliamente utilizado para evaluar la eficacia de los controles y procesos relacionados con los sistemas informáticos.
- ISACA – Normas y buenas prácticas de auditoría de sistemas de información, que proporcionan lineamientos metodológicos para la evaluación, control y aseguramiento de la confiabilidad de los sistemas tecnológicos.
- Buenas prácticas de informática forense y manejo de evidencia digital, orientadas a la correcta identificación, recolección, preservación, análisis y documentación de evidencia electrónica, garantizando su integridad, autenticidad y admisibilidad en eventuales procesos administrativos o judiciales.

La aplicación de este marco normativo y técnico permitirá asegurar que la auditoría forense se realice bajo criterios de legalidad, objetividad, rigurosidad técnica y validez probatoria, contribuyendo a fortalecer la transparencia, la rendición de cuentas y la confiabilidad de los sistemas de información utilizados por la Administración Aduanera de Honduras.

VI. METODOLOGÍA DE LA AUDITORÍA

La auditoría forense al Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH) se desarrollará mediante una metodología estructurada y sistemática, basada en buenas prácticas internacionales de auditoría de sistemas de información, seguridad informática e investigación forense digital.

La aplicación de la metodología se realizará **exclusivamente sobre la información, registros y transacciones correspondientes al período de auditoría comprendido entre enero de 2024 y enero de 2026**, conforme al alcance definido en los presentes Términos de Referencia.

ADMINISTRACIÓN ADUANERA DE HONDURAS ADUANAS Gerencia GERENCIA NACIONAL ADMINISTRATIVA Y FINANCIERA REPÚBLICA DE HONDURAS

La metodología tiene como objetivo asegurar un proceso ordenado, trazable y técnicamente riguroso, que permita planificar, recolectar, analizar y documentar evidencia digital, garantizando su integridad, autenticidad, trazabilidad y validez técnica.

La metodología se organizará en las siguientes fases: planificación, recolección de evidencia, análisis técnico, determinación de hallazgos y elaboración de informes.

Las actividades mínimas por fase y los requisitos operativos para su ejecución se detallan en la Sección VII 'Actividades o tareas a realizar' y forman parte integral de los presentes Términos de Referencia.

VII. ACTIVIDADES O TAREAS A REALIZAR

Todas las actividades descritas en esta sección se ejecutarán con base en la información correspondiente **al período de auditoría comprendido entre enero de 2024 y enero de 2026,** sin perjuicio de que se utilice información histórica previa únicamente como referencia técnica cuando sea estrictamente necesario.

Las actividades que ejecutará la firma auditora se estructuran conforme a las fases metodológicas descritas anteriormente y constituyen el desarrollo operativo de la auditoría forense.

1. Actividades de la Fase de Planificación de la Auditoría

- Revisión documental del sistema SARAH, incluyendo manuales técnicos, arquitectura tecnológica, diagramas de procesos, políticas de seguridad informática y documentación operativa.
- Identificación y análisis de riesgos asociados al sistema, considerando riesgos tecnológicos, operativos, de control interno y de integridad de la información.
- Definición del alcance y enfoque de la auditoría, estableciendo los componentes, procesos y registros que serán objeto de análisis.
- Elaboración del Plan de Auditoría, que incluirá la metodología de trabajo, los procedimientos técnicos a aplicar, el cronograma de actividades y los recursos requeridos.

2. Actividades de la Fase de Recolección de Evidencia

- Captura forense de información digital, incluyendo registros de servidores, bases de datos, sistemas de almacenamiento y otros componentes relevantes del sistema.
- Revisión y extracción de información de las bases de datos para el análisis de registros relacionados con las operaciones aduaneras.
- Obtención y análisis de registros del sistema (logs), incluyendo registros de acceso, modificaciones de datos y eventos de seguridad.

- Preservación de la evidencia digital mediante la aplicación de procedimientos de cadena de custodia que garanticen su autenticidad y trazabilidad.

3. Actividades de la Fase de Análisis Técnico

- Análisis de transacciones registradas en el sistema, incluyendo declaraciones aduaneras, liquidación de tributos y modificaciones efectuadas en registros operativos.
- Identificación de patrones anómalos o comportamientos atípicos mediante técnicas de análisis de datos, correlación de eventos y revisión de registros históricos.
- Evaluación de los controles de seguridad informática, incluyendo mecanismos de autenticación, control de accesos, monitoreo del sistema y registros de auditoría.
- Análisis de la integridad de los datos, con el fin de identificar posibles alteraciones o inconsistencias en la información almacenada.

4. Actividades de la Fase de Determinación de Hallazgos

- Documentación técnica de irregularidades, vulnerabilidades o debilidades detectadas, incluyendo la evidencia que respalde cada hallazgo.
- Análisis de las causas y condiciones que permitieron la ocurrencia de las irregularidades, considerando aspectos tecnológicos, administrativos y de control interno.
- Identificación de posibles responsables, cuando la evidencia técnica permita establecer la participación de usuarios o administradores del sistema. La identificación es técnica y basada en trazabilidad, sin calificación jurídica.
- Estimación del impacto económico potencial derivado de las irregularidades detectadas, especialmente aquellas que puedan haber afectado la recaudación de tributos aduaneros.

5. Actividades de la Fase de Elaboración de Informes

- Elaboración del informe preliminar de auditoría, presentando los principales hallazgos identificados.
- Desarrollo del proceso de validación o retroalimentación institucional, cuando sea necesario para aclarar aspectos técnicos de los hallazgos.
- Elaboración y presentación del informe final de auditoría forense, que incluirá los hallazgos confirmados, la evidencia técnica recopilada, el análisis de impactos, la determinación de responsabilidades cuando corresponda y las recomendaciones para fortalecer los controles y la seguridad del sistema.

VIII. PRODUCTOS ESPERADOS

Todos los productos de la auditoría forense deberán elaborarse **con base en el análisis de la información correspondiente al período comprendido entre enero de 2024 y enero de 2026**, conforme al alcance y objetivos establecidos en los presentes Términos de Referencia.

Como resultado del proceso de auditoría forense al Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH), el equipo auditor deberá generar una serie de productos técnicos y documentales que permitan evidenciar el desarrollo de las actividades realizadas, los resultados obtenidos durante el proceso de análisis y las conclusiones derivadas de la investigación. Estos productos deberán elaborarse conforme a estándares técnicos de auditoría e investigación forense informática, garantizando la claridad, trazabilidad y respaldo documental de los hallazgos identificados.

Los principales productos esperados de la auditoría son los siguientes:

1. **Plan de Auditoría Forense**

Documento que establecerá el enfoque metodológico, alcance, procedimientos técnicos y cronograma de trabajo de la auditoría. Este plan deberá incluir, entre otros aspectos:

- Objetivos y alcance de la auditoría.
- Metodología y técnicas de auditoría forense a utilizar.
- Identificación de riesgos asociados al sistema.
- Actividades y procedimientos de auditoría a ejecutar.
- Cronograma de trabajo y recursos requeridos.

Este documento servirá como guía para la ejecución ordenada y sistemática del proceso de auditoría.

2. **Informe de Diagnóstico Inicial**

Documento que presentará los resultados de la evaluación preliminar del sistema SARAH, incluyendo una descripción general de la arquitectura tecnológica, los procesos operativos asociados al sistema y los principales riesgos identificados durante la fase inicial de la auditoría.

Este informe deberá incluir, entre otros elementos:

- Descripción general del entorno tecnológico del sistema.
- Identificación de componentes críticos del sistema.

- Evaluación preliminar de los controles de seguridad existentes.
- Identificación inicial de riesgos o vulnerabilidades potenciales.

El diagnóstico inicial permitirá orientar las actividades de análisis técnico que se desarrollarán en las fases posteriores de la auditoría.

3. Informe de Hallazgos Preliminares

Documento que presentará los hallazgos iniciales derivados del análisis técnico realizado durante el proceso de auditoría, incluyendo posibles irregularidades, vulnerabilidades o debilidades identificadas en el sistema.

Este informe deberá contener:

- Descripción detallada de los hallazgos preliminares.
- Evidencia técnica que respalde cada hallazgo.
- Análisis inicial de las causas o condiciones que permitieron la ocurrencia de las irregularidades detectadas.
- Evaluación preliminar de los posibles impactos operativos o financieros.

Este informe permitirá a la institución conocer de manera anticipada los principales resultados del proceso de auditoría y facilitar la validación técnica de los hallazgos identificados.

4. Informe Final de Auditoría Forense

Documento técnico que consolidará los resultados finales de la auditoría forense, incluyendo el análisis integral de la información recopilada, la descripción de los hallazgos confirmados y las conclusiones derivadas del proceso de investigación.

El informe final deberá incluir, entre otros elementos:

- Descripción del alcance y metodología aplicada durante la auditoría.
- Presentación detallada de los hallazgos confirmados.
- Evidencia técnica que respalde las conclusiones de la auditoría.
- Determinación de posibles irregularidades o vulnerabilidades detectadas.
- Estimación del impacto económico potencial derivado de las irregularidades identificadas.
- Identificación de posibles responsabilidades técnicas o administrativas cuando la evidencia lo permita.

ADMINISTRACIÓN ADUANERA DE HONDURAS ADUANAS Gerencia GERENCIA NACIONAL ADMINISTRATIVA Y FINANCIERA REPÚBLICA DE HONDURAS

- Recomendaciones orientadas al fortalecimiento de los controles de seguridad y la gobernanza del sistema.

Este documento constituirá el principal producto técnico de la auditoría y servirá como base para la adopción de medidas correctivas o para la eventual remisión de información a las instancias administrativas o judiciales competentes.

5. **Anexos Técnicos con Evidencia Digital Documentada**

Juntamente con el informe final, se deberán presentar anexos técnicos que contengan la documentación detallada de la evidencia digital recopilada durante el proceso de auditoría.

Estos anexos podrán incluir, entre otros:

- Registros de auditoría (logs) analizados.
- Extractos de bases de datos relevantes para la investigación.
- Registros de transacciones evaluadas.
- Resultados de análisis técnicos o herramientas de auditoría utilizadas.
- Documentación de la cadena de custodia de la evidencia digital.

Los anexos técnicos deberán garantizar la trazabilidad, integridad y autenticidad de la evidencia digital, asegurando su posible utilización en procesos administrativos, disciplinarios o judiciales cuando corresponda.
Cada producto será revisado y aprobado formalmente por la contraparte técnica en un plazo definido en el contrato.

Tabla Formal de Productos – Hitos – Pagos

N.º	Producto / Entregable	Hito de Cumplimiento	Contenido mínimo del producto (según TDR)	Condición de Pago	Entrega en días calendario a partir de la Orden de Inicio
1	**Plan de Auditoría Forense**	Aprobación formal del Plan por la entidad contratante	Enfoque metodológico, alcance, técnicas de auditoría forense, identificación de riesgos, actividades a ejecutar, cronograma y recursos	Pago del 10% contra entrega y aprobación del Plan de Auditoría Forense	10 días
2	**Informe de Diagnóstico Inicial**	Aprobación del Informe de Diagnóstico Inicial	Evaluación preliminar del sistema SARAH, descripción del entorno tecnológico,	Pago del 20% contra entrega y aprobación del	30 días

			componentes críticos, controles de seguridad y riesgos iniciales	Informe de Diagnóstico Inicial	
3	**Informe de Hallazgos Preliminares**	Aprobación del Informe de Hallazgos Preliminares	Hallazgos iniciales, evidencia técnica de respaldo, análisis preliminar de causas y evaluación inicial de impactos	Pago 20% contra entrega y aprobación del Informe de Hallazgos Preliminares	90 días
4	**Informe Final de Auditoría Forense**	Aprobación del Informe Final	Hallazgos confirmados, evidencia técnica consolidada, análisis integral, estimación de impacto económico, responsabilidades y recomendaciones	Pago 35% contra entrega y aprobación del Informe Final de Auditoría Forense	150 días
5	**Anexos Técnicos con Evidencia Digital Documentada**	Aprobación de anexos y cierre técnico de la consultoría	Logs analizados, extractos de bases de datos, registros de transacciones, resultados de análisis técnicos y documentación de cadena de custodia	**Pago final** 15% contra aprobación de anexos y conformidad de cierre del contrato	180 días

Los productos, hitos y pagos establecidos en la presente sección corresponden al desarrollo de la auditoría forense del sistema SARAH dentro del período de auditoría definido en los presentes Términos de Referencia.

Forma de Pago

Los pagos se efectuarán bajo la modalidad de **contrato a suma global**, exclusivamente contra la entrega y aprobación de los productos establecidos en los presentes Términos de Referencia.

La aprobación de cada producto constituirá el **hito contractual** que habilita el pago correspondiente. No se realizarán pagos por concepto de tiempo trabajado, dedicación horaria o actividades no asociadas a productos aprobados.

NOTA:

La firma podrá gozar de un anticipo del 20% del monto total del contrato, mediante la presentación de una garantía bancaria de anticipo por el 100% del valor anticipado y el cual será amortizado en los porcentajes de cada pago, descrito en la tabla anterior.

La firma consultora residente en Honduras recibirá su pago mediante transferencia bancaria electrónica a través

del Sistema Nacional de Pagos de Honduras por medio del Sistema de Administración Financiera Integrada (SIAFI). La Firma Consultora deberá proporcionar copia del registro del beneficiario.

Los pagos de los productos o informes objeto de la auditoria, se efectuarán contra la presentación original de los entregables (productos ADUANAS se reserva el derecho de revisa el Producto (Entregable) en tiempo máximo de 10 días hábiles. A más tardar al día 10 deberá aprobar o comentar el producto presentado. El pago se realizará contra aceptación a satisfacción del producto. Asimismo, la Firma Auditora deberá presentar recibos originales apegados al Régimen de Facturación, Acuerdo No. 189-2014.

En caso de no presentar la constancia que acredite que está sujeto a pagos a cuenta, se aplicará el Art. No. 50 de la Ley del Impuesto Sobre la Renta, "Las Personas Jurídicas de Derecho Público y Derecho Privado, que efectúen pagos o constituyan créditos a favor de personas naturales o jurídicas residentes en Honduras, no exoneradas del Impuesto Sobre la Renta, deberán retener y enterar al fisco el doce punto cinco por ciento (12.5%) del monto de los pagos o créditos que efectúen por concepto de honorarios profesionales".

A la firma consultora no residente en Honduras, se le retendrá el 25% de impuesto sobre la renta (ISR).

Decreto No. 62-2026, Capítulo III. Ejecución Presupuestaria de los Ingresos del Presupuesto general de ingresos y egresos de la República y sus disposiciones generales ejercicio Fiscal vigente. Artículo 106: En todo contrato financiado con fondos externos, la suspensión o cancelación del préstamo o donación, dará lugar a la rescisión o resolución del contrato, sin más obligación por parte del Estado. Igual medida se aplicará en los casos previstos en el Artículo 39, párrafo primero de la Ley Orgánica del Presupuesto. Lo dispuesto en este Artículo debe consignarse obligatoriamente en los pliegos de condiciones, términos de referencia y Contrato.

IX. CALIFICACIONES Y EXPERIENCIA DE LA FIRMA CONSULTORA

La firma consultora deberá acreditar experiencia comprobada de al menos cinco auditorías forenses informáticas o investigaciones técnicas en sistemas tributarios, aduaneros, financieros o recaudatorios y que disponga de herramientas especializadas para análisis forense de base de datos, correlación de logs de auditoría y preservación de evidencia digital, auditorías de sistemas de información, investigaciones de incidentes tecnológicos, análisis de evidencia digital, gestión de riesgos tecnológicos, control interno, seguridad de la información y evaluación de plataformas tecnológicas de misión crítica. Asimismo, deberá demostrar capacidad técnica para identificar, preservar, analizar y documentar evidencia digital conforme a estándares y metodologías internacionalmente reconocidas.

1. PERFIL DE LA FIRMA CONSULTORA

1.1 Experiencia General

La firma consultora deberá acreditar una experiencia mínima de diez (10) años en la prestación de servicios profesionales relacionados con auditorias forenses informáticas, tecnologías de información y seguridad de la

información.

Deberá demostrar experiencia en la ejecución de proyectos relacionados con:

- Auditorías forenses informáticas y análisis de evidencia digital.
- Auditorías de sistemas de información y tecnologías de información.
- Evaluación de controles generales de TI y controles automatizados de aplicación.
- Gestión de riesgos tecnológicos y evaluación de controles internos.
- Investigaciones de incidentes de seguridad de la información y ciberseguridad.
- Análisis de trazabilidad de registros electrónicos, transacciones, bitácoras (logs) y eventos de sistemas.
- Revisión de bases de datos, integridad de información y mecanismos de auditoría.
- Evaluación de plataformas tecnológicas de alta criticidad institucional.
- Evaluación de mecanismos de autenticación, autorización, segregación de funciones y gestión de privilegios.

1.2 Experiencia Específica

La firma consultora deberá acreditar la ejecución satisfactoria de al menos cinco (5) proyectos de auditoría forense informática, auditoría de sistemas críticos o investigaciones técnicas especializadas durante los últimos diez (10) años.

Los proyectos acreditados deberán haber contemplado uno o varios de los siguientes componentes:

- Análisis forense de sistemas de información.
- Investigación de incidentes de seguridad o presuntos actos irregulares en sistemas informáticos.
- Revisión de trazabilidad de operaciones y transacciones electrónicas.
- Reconstrucción cronológica de eventos mediante análisis de registros electrónicos.
- Análisis de bases de datos y correlación de información proveniente de múltiples fuentes.
- Evaluación de integridad, disponibilidad y confidencialidad de la información.
- Identificación de accesos indebidos, modificaciones no autorizadas o alteraciones de datos.
- Evaluación de controles de seguridad lógica, segregación de funciones y administración de privilegios.
- Revisión de bitácoras de auditoría, logs de aplicaciones, bases de datos, servidores, dispositivos de seguridad y sistemas operativos.
- Análisis de vulnerabilidades y debilidades de control que pudieran facilitar la ocurrencia de eventos irregulares.

Evidenciar experiencia en la elaboración de productos similares a los requeridos en la presente consultoría, incluyendo:

- Planes de auditoría forense.
- Planes de preservación y manejo de evidencia digital.

ADMINISTRACIÓN ADUANERA DE HONDURAS ADUANAS Gerencia GERENCIA NACIONAL ADMINISTRATIVA Y FINANCIERA REPÚBLICA DE HONDURAS

- Informes técnicos de análisis forense.
- Informes de hallazgos.
- Informes periciales o informes con potencial valor probatorio.
- Informes finales sustentados con evidencia digital verificable y documentada.

La firma deberá demostrar conocimiento y aplicación de estándares y marcos de referencia internacionalmente reconocidos, tales como:

- ISO/IEC 27001.
- ISO/IEC 27002.
- ISO/IEC 27037 (Identificación, recolección, adquisición y preservación de evidencia digital).
- ISO/IEC 27041.
- ISO/IEC 27042.
- ISO/IEC 27043.
- NIST Cybersecurity Framework.
- NIST SP 800-61.
- COBIT.
- ISACA IT Assurance Framework (ITAF).
- Guías de buenas prácticas de informática forense reconocidas internacionalmente.

2. PERSONAL CLAVE MÍNIMO REQUERIDO

La firma consultora deberá disponer, como mínimo, del siguiente equipo profesional clave, el cual deberá participar directamente en la ejecución de la consultoría.

Todo el personal clave deberá acreditar experiencia específica mediante hojas de vida y constancias de participación en proyectos similares.

Se valorará especialmente la posesión de certificaciones internacionales vigentes.

a. Líder del Proyecto de la Auditoría Forense

Será responsable de la dirección integral de la consultoría, la supervisión metodológica, la validación de resultados y la presentación de informes.

Perfil profesional:

- Título universitario en Ingeniería en Sistemas, Informática, Ciencias de la Computación, Auditoría, Ingeniería Industrial o carreras afines.
- Experiencia profesional mínima de diez (10) años.

- Experiencia mínima de cinco (5) años liderando auditorías de sistemas, auditorías forenses informáticas o investigaciones tecnológicas.
- Participación comprobada en al menos cinco (5) proyectos similares.
- Experiencia en sistemas críticos del sector público o privado.
- Deseable certificación CISA, CISM, CRISC, CISSP, CGEIT o equivalente.

b. Especialista en Auditoría de Sistemas de Información

Responsable de evaluar controles tecnológicos, procesos automatizados y mecanismos de auditoría.

Perfil profesional:

- Formación universitaria en tecnologías de información, auditoría informática o áreas afines.
- Experiencia mínima de cinco (5) años en auditoría de sistemas.
- Experiencia en evaluación de controles generales de TI y controles automatizados.
- Experiencia en sistemas tributarios, aduaneros, financieros o gubernamentales.
- Deseable certificación CISA o equivalente.

c. Especialista en Informática Forense

Responsable de la identificación, recolección, preservación, análisis y documentación de evidencia digital.
Perfil profesional:

- Formación universitaria en informática, sistemas o carreras afines.
- Experiencia mínima de cinco (5) años en informática forense.
- Experiencia comprobada en investigaciones forenses digitales.
- Experiencia en aplicación de cadena de custodia y preservación de evidencia digital.
- Conocimiento de herramientas especializadas de análisis forense.
- Deseable certificación CHFI, GCFA, GCFE, EnCE, CFCE o equivalente.

d. Especialista en Seguridad de la Información y Ciberseguridad

Responsable de evaluar la arquitectura de seguridad, controles de acceso, gestión de privilegios y eventos de seguridad.

ADMINISTRACIÓN ADUANERA DE HONDURAS ADUANAS Gerencia GERENCIA NACIONAL ADMINISTRATIVA Y FINANCIERA REPÚBLICA DE HONDURAS

Perfil profesional:

- Formación universitaria en informática, sistemas, telecomunicaciones o carreras afines.
- Experiencia mínima de cinco (5) años en seguridad de la información.
- Experiencia en gestión de vulnerabilidades, análisis de riesgos y monitoreo de eventos.
- Experiencia en sistemas críticos y entornos transaccionales.
- Deseable certificación CISSP, CISM, CEH, CompTIA Security+ o equivalente.

e. Especialista en Bases de Datos y Analítica Forense de Datos

- Responsable del análisis técnico de bases de datos, validación de integridad y reconstrucción de transacciones.

Perfil profesional:

- Formación universitaria en informática, sistemas, ingeniería o carreras afines.
- Experiencia mínima de cinco (5) años en administración o análisis de bases de datos.
- Experiencia en análisis masivo de datos, minería de datos y correlación de eventos.
- Experiencia en revisión de transacciones electrónicas complejas y trazabilidad de registros.
- Conocimiento de bases de datos relacionales y no relacionales.

f. especialista Legal o Perito en Evidencia Digital

- Responsable de asesorar sobre aspectos de admisibilidad, integridad y valor probatorio de la evidencia digital obtenida durante la auditoría.

Perfil profesional:

- Profesional del Derecho con especialización o experiencia en delitos informáticos, evidencia digital o peritaje tecnológico.
- Experiencia en procedimientos administrativos, judiciales o investigaciones especiales relacionadas con tecnología.

Disposiciones Complementarias

El personal clave será responsable directo de la elaboración, revisión y validación técnica de los productos entregables.

La sustitución de personal clave requerirá autorización previa y por escrito de la entidad contratante. El profesional sustituto deberá acreditar calificaciones, experiencia y certificaciones iguales o superiores a las exigidas para el perfil reemplazado.

La entidad contratante podrá solicitar entrevistas técnicas al personal clave propuesto y verificar la autenticidad de las certificaciones, credenciales profesionales y experiencias acreditadas.

X. MECANISMO / CRITERIO DE EVALUACIÓN TÉCNICA

El proceso de evaluación se llevará a cabo en dos etapas sucesivas e independientes: a) Evaluación Técnica, y b) Evaluación de Precio, las cuales serán posteriormente combinadas para determinar la propuesta mejor calificada.

a) Evaluación Técnica

La Propuesta Técnica de cada firma consultora será evaluada exclusivamente con base en su conformidad con los presentes Términos de Referencia, aplicando los criterios y subcriterios de evaluación definidos en este apartado. Esta evaluación será realizada por el Comité de Evaluación designado por la Entidad Contratante.

La Propuesta Técnica tendrá una ponderación del ochenta por ciento (80%) del puntaje total y será calificada sobre una base de 100 puntos, considerando, entre otros aspectos, la experiencia específica de la firma, la calidad del enfoque técnico, la metodología y el plan de trabajo propuestos, así como las calificaciones y competencias del personal profesional clave.

Las propuestas técnicas que no alcancen el puntaje técnico mínimo establecido de 70% o que no cumplan con los requisitos esenciales de los Términos de Referencia no serán consideradas para la siguiente etapa del proceso.

CRITERIOS DE EVALUACIÓN TÉCNICA

PUNTAJE TOTAL: 100 PUNTOS

No.	Criterio	Puntaje Máximo
1	Experiencia específica de la Firma Consultora	10
2	Calidad del Enfoque Técnico, Metodología y Plan de Trabajo	20
3	Calificaciones del Personal Profesional Clave y Competencia para el Trabajo	70
	TOTAL	100

1. EXPERIENCIA ESPECÍFICA DE LA FIRMA CONSULTORA
Puntaje máximo: 10 puntos

No.	Criterio/Subcriterio	Pts.	Puntaje

ADMINISTRACIÓN ADUANERA DE HONDURAS ADUANAS Gerencia GERENCIA NACIONAL ADMINISTRATIVA Y FINANCIERA REPÚBLICA DE HONDURAS

			Máximo
1.	**Experiencia Específica de la Firma Consultora**		**10**
1.1	***La firma consultora deberá acreditar la ejecución satisfactoria de al menos cinco (5) proyectos de auditoría forense informática, auditoría de sistemas críticos o investigaciones técnicas especializadas durante los últimos diez (10) años.*** *Los proyectos acreditados deberán haber contemplado uno o varios de los siguientes componentes: Análisis forense de sistemas de información, Investigación de incidentes de seguridad o presuntos actos irregulares en sistemas informáticos, Revisión de trazabilidad de operaciones y transacciones electrónicas, Reconstrucción cronológica de eventos mediante análisis de registros electrónicos, Análisis de bases de datos y correlación de información proveniente de múltiples fuentes, Evaluación de integridad, disponibilidad y confidencialidad de la información, Identificación de accesos indebidos, modificaciones no autorizadas o alteraciones de datos, Evaluación de controles de seguridad lógica, segregación de funciones y administración de privilegios, Revisión de bitácoras de auditoría, logs de aplicaciones, bases de datos, servidores, dispositivos de seguridad y sistemas operativos, Análisis de vulnerabilidades y debilidades de control que pudieran facilitar la ocurrencia de eventos irregulares.*		**4**
1.1.1	Menos de cinco (5) proyectos	2	
1.1.2	Cinco (5) proyectos	3	
1.1.3	Más de cinco (5) proyectos	4	
1.2	**Evidenciar experiencia en la elaboración de productos similares a los requeridos en la presente consultoría, incluyendo: Planes de auditoría forense, Planes de preservación y manejo de evidencia digital, Informes técnicos de análisis forense, Informes de hallazgos, Informes periciales o informes con potencial valor probatorio, Informes finales sustentados con evidencia digital verificable y documentada.**		**3**
1.2.1	Evidencia alguno de los aspectos	1	
1.2.2	Evidencia la mayoría de los aspectos	2	
1.2.3	Evidencia todos los aspectos o más	3	
1.3	**La firma deberá demostrar conocimiento y aplicación de estándares y marcos de referencia internacionalmente reconocidos, tales como: ISO/IEC 27001, ISO/IEC 27002, ISO/IEC 27037 (Identificación, recolección, adquisición y preservación de evidencia digital), ISO/IEC 27041, ISO/IEC 27042, ISO/IEC 27043, NIST Cybersecurity Framework, NIST SP 800-61, COBIT, ISACA IT Assurance Framework (ITAF), Guías de buenas prácticas de informática forense reconocidas internacionalmente.**		**3**
1.3.1	Evidencia alguno de los estándares	1	
1.3.2	Evidencia la mayoría de los estándares	2	
1.3.3	Evidencia todos los estándares o más	3	

2. CALIDAD DEL ENFOQUE TÉCNICO, METODOLOGÍA Y PLAN DE TRABAJO

Puntaje máximo total: 20 puntos

No.	Criterio/ Subcriterio	Pts.	Puntaje Máximo
2.	**Calidad del enfoque técnico, metodología y plan de trabajo**		**20**
2.1	**Enfoque Técnico y Metodología**		**10**
2.1.1	**Coherencia y solidez del enfoque técnico y la metodología propuesta para alcanzar los objetivos y productos de la consultoría**		**10**
2.1.1.1	Muy sólida y detallada	10	
2.1.1.2	Adecuada	8	
2.1.1.3	General	7	
2.1.1.4	Insuficiente	0	
2.2	**Plan de Trabajo**		**10**
2.2.1	**Plan de trabajo estructurado por fases, actividades, cronograma, hitos y entregables, con secuencia lógica y coherente con los objetivos**		**10**
2.2.1.1	Completo y consistente	10	
2.2.1.2	Completo con menor detalle	8	
2.2.1.3	Parcial	7	
2.2.1.4	Insuficiente	0	

3. PERSONAL PROFESIONAL CLAVE Y COMPETENCIA PARA EL TRABAJO

Puntaje máximo: 70 puntos

Personal Clave	Puntos
a. Líder del Proyecto de la Auditoría Forense	15
b. Especialista en Auditoría de Sistemas de Información	10
c. Especialista en Informática Forense	15
d. Especialista en Seguridad de la Información y Ciberseguridad	10
e. Especialista en Bases de Datos y Analítica Forense de Datos	10
f. Especialista Legal o Perito en Evidencia Digital	10

Total	70

3.A - Líder de Proyecto de la Auditoría Forense - 15 puntos

No.	Criterio/ Subcriterio	Pts.	Puntaje Máximo
3.A	Líder del Proyecto de la Auditoría Forense		15
3.A.1	Título universitario en Ingeniería en Sistemas, Informática, Ciencias de la Computación, Auditoría, Ingeniería Industrial o carreras afines		Cumple/No cumple
3.A.2	Experiencia profesional mínima de diez (10) años.	0 ó 3	3
3.A.3	Experiencia mínima de cinco (5) años liderando auditorías de sistemas, auditorías forenses informáticas o investigaciones tecnológicas.	0 ó 3	3
3.A.4	Participación comprobada en al menos cinco (5) proyectos similares.	0 ó 3	3
3.A.5	Experiencia en sistemas críticos del sector público o privado.	0 ó 3	3
3.A.6	Deseable certificación CISA, CISM, CRISC, CISSP, CGEIT o equivalente.	0 ó 3	3

3.B - Especialista en Auditoría de Sistemas de Información- 10 puntos

No.	Criterio/ Subcriterio	Pts.	Puntaje Máximo
3.B	Especialista en Auditoría de Sistemas de Información		10
3.B.1	Formación universitaria en tecnologías de información, auditoría informática o áreas afines.		Cumple/No cumple
3.B.2	Experiencia mínima de cinco (5) años en auditoría de sistemas	0 ó 3	3
3.B.3	Experiencia en evaluación de controles generales de TI y controles automatizados.	0 ó 3	3
3.B.4	Experiencia en sistemas tributarios, aduaneros, financieros o gubernamentales.	0 ó 2	2
3.B.5	Deseable certificación CISA o equivalente	0 ó 2	2

3.C - Especialista en Informática Forense -15 puntos

No.	Criterio/ Subcriterio	Pts.	Puntaje Máximo
3.C	Especialista en Informática Forense		15
3.C.1	Formación universitaria en informática, sistemas o carreras afines.		Cumple/No cumple
3.C.2	Experiencia mínima de cinco (5) años en informática forense.	0 ó 3	3
3.C.3	Experiencia comprobada en investigaciones forenses digitales	0 ó 3	3
3.C.4	Experiencia en aplicación de cadena de custodia y preservación de evidencia digital.	0 ó 3	3
3.C.5	Conocimiento de herramientas especializadas de análisis forense.	0 ó 3	3
3.C.6	Deseable certificación CHFI, GCFA, GCFE, EnCE, CFCE o equivalente.	0 ó 3	3

3.D Especialista en Seguridad de la Información y Ciberseguridad - 10 puntos

No.	Criterio/ Subcriterio	Pts.	Puntaje Máximo
3.D.	Especialista en Seguridad de la Información y Ciberseguridad		10
3.D.1	Formación universitaria en informática, sistemas, telecomunicaciones o carreras afines.		Cumple/No cumple
3.D.2	Experiencia mínima de cinco (5) años en seguridad de la información	0 ó 3	3
3.D.3	Experiencia en gestión de vulnerabilidades, análisis de riesgos y monitoreo de eventos	0 ó 2	2
3.D.4	Experiencia en sistemas críticos y entornos transaccionales	0 ó 3	3
3.D.5	Deseable certificación CISSP, CISM, CEH, CompTIA Security+ o equivalente.	0 ó 2	2

3.E - Especialista en Bases de Datos y Analítica Forense de Datos - 10 puntos

No.	Criterio/ Subcriterio	Pts.	Puntaje Máximo
3.E.	Especialista en Bases de Datos y Analítica Forense de Datos		10
3.E.1	Formación universitaria en informática, sistemas, ingeniería o carreras afines.		Cumple/No cumple
3.E.2	Experiencia mínima de cinco (5) años en administración o análisis de bases de datos.	0 ó 3	3

ADMINISTRACIÓN ADUANERA DE HONDURAS ADUANAS Gerencia Operacional Administrativa y Financiera REPÚBLICA DE HONDURAS

3.E.3	**Experiencia en análisis masivo de datos, minería de datos y correlación de eventos.**	**0 ó 2**	**2**
3.E.4	**Experiencia en revisión de transacciones electrónicas complejas y trazabilidad de registros.**	**0 ó 3**	**3**
3.E.5	**Conocimiento de bases de datos relacionales y no relacionales.**	**0 ó 2**	**2**

3.F - Especialista Legal o Perito en Evidencia Digital - 10 puntos

No.	Criterio/ Subcriterio	Pts.	Puntaje Máximo
3.F.	**Especialista Legal o Perito en Evidencia Digital**		**10**
3.F.1	**Profesional del Derecho con especialización o experiencia en delitos informáticos, evidencia digital o peritaje tecnológico**	**0 ó 5**	**5**
3.F.2	**Experiencia en procedimientos administrativos, judiciales o investigaciones especiales relacionadas con tecnología**	**0 ó 5**	**5**

PUNTAJE MÍNIMO PARA CALIFICAR

Condición	Umbral
Puntaje técnico mínimo para calificar	**70/100 puntos o 70% del puntaje**

b) Evaluación de Precio

Una vez concluida la Evaluación Técnica, únicamente se procederá a la apertura y evaluación de las Propuestas de Precio correspondientes a aquellas firmas que hayan alcanzado el puntaje técnico mínimo requerido.

c) Evaluación Combinada y Selección

El puntaje final de cada propuesta se obtendrá mediante la combinación ponderada del puntaje técnico (80%) y el puntaje de precio (20%).

La firma consultora que obtenga el mayor puntaje combinado será considerada como la propuesta mejor calificada y será recomendada para iniciar el proceso de negociación del contrato.

XI. RECURSOS Y FACILIDADES A SER PROVISTOS POR LA ENTIDAD CONTRATANTE

La entidad contratante designará una contraparte técnica institucional responsable de la coordinación y validación de los productos.

Asimismo, facilitará al consultor el acceso oportuno a la información, sistemas y registros necesarios para la ejecución de la auditoría, referidos principalmente al período comprendido entre enero de 2024 y enero de 2026, bajo estrictos controles de confidencialidad y seguridad.
El consultor deberá aplicar procedimientos de preservación de evidencia digital y mantener la cadena de custodia correspondiente.

XII. COORDINACIÓN Y SUPERVISIÓN

La firma consultora coordinará sus actividades con la Gerencia Nacional de Tecnología (GNT), la cual será responsable de la aprobación de cada uno de los productos para efectos de pago.

XIII. DURACIÓN DE LA AUDITORÍA

La auditoría forense al Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH) tendrá un **plazo máximo de ejecución de hasta seis (6) meses calendario**, contados a partir de la fecha de inicio formal de las actividades de auditoría, establecida mediante la correspondiente Orden de Inicio.

Dentro de este plazo máximo, la firma consultora deberá ejecutar de manera progresiva todas las fases establecidas en la metodología de la auditoría, incluyendo la planificación, recolección de información y evidencia digital, análisis técnico, determinación de hallazgos y elaboración de los informes correspondientes, asegurando la **entrega y aprobación de la totalidad de los productos definidos en los presentes Términos de Referencia**.

El cronograma detallado de actividades y entregables será propuesto por la firma consultora en el Plan de Auditoría Forense y deberá ser aprobado por la entidad contratante, constituyendo el instrumento de referencia para el seguimiento de la ejecución contractual.

Cualquier modificación al plazo de ejecución únicamente podrá realizarse de manera excepcional, cuando exista una **modificación formal del alcance de la consultoría**, debidamente justificada y aprobada por la entidad contratante conforme a las disposiciones contractuales aplicables.

El plazo establecido permitirá realizar un análisis exhaustivo y técnicamente riguroso del sistema SARAH, garantizando la adecuada identificación de posibles irregularidades, la correcta preservación de la evidencia digital y la emisión de conclusiones sustentadas en criterios técnicos sólidos.

XIV. CONFIDENCIALIDAD Y MANEJO DE INFORMACIÓN

Toda la información recopilada, analizada o generada durante el desarrollo de la auditoría forense deberá ser tratada bajo estrictos protocolos de confidencialidad, seguridad de la información y manejo responsable de datos, considerando la naturaleza sensible de la información procesada por el Sistema Automatizado de Rentas Aduaneras de Honduras (SARAH).

El equipo auditor estará obligado a proteger la confidencialidad, integridad y disponibilidad de la información a la que tenga acceso durante la ejecución de la auditoría, evitando cualquier uso indebido, divulgación no autorizada o manipulación de los datos obtenidos. Esta obligación será aplicable tanto a la información digital como a la documentación física o electrónica generada durante el proceso de auditoría.

En particular, deberán adoptarse medidas técnicas y administrativas orientadas a:

- Garantizar la protección de datos sensibles, incluyendo información tributaria, comercial, financiera y operativa relacionada con las operaciones de comercio exterior.
- Resguardar adecuadamente la información institucional y los registros contenidos en el sistema SARAH, evitando su alteración, pérdida o acceso no autorizado.
- Preservar la integridad de la evidencia digital, mediante la aplicación de procedimientos técnicos adecuados para su identificación, recolección, almacenamiento y análisis.
- Mantener la cadena de custodia de la evidencia digital, documentando de manera detallada el proceso de obtención, traslado, almacenamiento y análisis de la información utilizada durante la auditoría.
- Limitar el acceso a la información recopilada únicamente al personal autorizado, que participe directamente en las actividades de auditoría.

Asimismo, toda la información obtenida durante la auditoría deberá ser utilizada exclusivamente para los fines establecidos en los presentes Términos de Referencia, y no podrá ser divulgada a terceros sin la debida autorización de la autoridad competente, salvo en los casos en que dicha información deba ser remitida a las instancias administrativas, de control o judiciales correspondientes.

El cumplimiento de estos principios permitirá garantizar que el proceso de auditoría se realice bajo criterios de confidencialidad, integridad, legalidad y rigor técnico, asegurando la protección de la información institucional y la validez de la evidencia digital que pudiera derivarse del proceso de auditoría forense.

Las obligaciones de confidencialidad, preservación de evidencia digital y mantenimiento de la cadena de custodia serán aplicables a toda la información correspondiente al **período de auditoría definido en los presentes Términos de Referencia**, así como a cualquier información complementaria a la que se tenga acceso durante la ejecución de la consultoría.