1. DEPENDENCIA SOLICITANTE

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - DEL MINISTERIO DE DEFENSA NACIONAL.

2. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON LA CONTRATACIÓN

De conformidad con el Decreto 1874 de 2021, la Dirección de Tecnologías de la Información y Comunicaciones del Ministerio de Defensa Nacional tiene la responsabilidad de velar por los recursos tecnológicos y contribuir con el óptimo desempeño en la prestación de los servicios informáticos requeridos para apoyar el cumplimiento misional.

En el año 2015 la Oficina Asesora de Sistemas, hoy Dirección de Tecnologías de la Información y las Comunicaciones TICs, ha realizado procesos de contratación para que la Unidad de Gestión General del Ministerio de Defensa se certifique en dos procesos: el proceso TIC´S y el proceso de seguridad y defensa en la norma ISO 27001:2013.

La Dirección requiere actualizar los procedimientos a la nueva versión de la norma ISO 27001:2022, la Unidad de Gestión General del Ministerio por lo que pretende realizar este proceso de contratación para asegurar que los cambios efectuados en la norma ISO queden alineados y se pueda continuar con la certificación, manteniendo la disponibilidad, integridad y confidencialidad de la información, que es el activo más valioso de la organización.

La certificación en la norma ISO 27001:2022 es fundamental para cualquier organización que desee asegurar la protección de sus activos de información, para lo cual se deben tener en cuenta algunas razones clave para obtener esta certificación a saber:

1. **Mejora de la seguridad de la información**: La norma ISO 27001 proporciona un marco estructurado para gestionar la seguridad de la información, ayudando a identificar y mitigar riesgos, y asegurando la confidencialidad, integridad y disponibilidad de los datos.
2. **Cumplimiento legal y regulatorio**: La certificación ayuda a cumplir con las leyes y regulaciones relacionadas con la protección de datos y la privacidad, evitando sanciones y multas.
3. **Confianza y reputación**: Obtener la certificación ISO 27001 demuestra a clientes, socios y otras partes interesadas que la organización toma en serio la seguridad de la información, lo que puede mejorar la confianza y la reputación.
4. **Ventaja competitiva**: La certificación puede diferenciar a la organización de sus competidores, mostrando un compromiso con las mejores prácticas en seguridad de la información.
5. **Mejora continua**: La norma ISO 27001 fomenta la mejora continua de los procesos de seguridad de la información, asegurando que la organización se mantenga al día con las amenazas y vulnerabilidades emergentes.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

2.1 VERIFICACION DE LA APROBACION DE LA NECESIDAD EN EL CITI (CUANDO APLIQUE)

No Aplica

3. OBJETO POR CONTRATAR

ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA A LA NUEVA VERSIÓN DE LA NORMA ISO 27001:2022.

ALCANCE DEL OBJETO

Para realizar la actualización del sistema de gestión de seguridad de la información se requiere realizar las siguientes fases:

1) **Levantamiento:** Esta fase implica la recopilación y revisión de la información existente para entender cómo se encuentra la Unidad de Gestión General y qué necesidades tiene para realizar la actualización.

2) **Actualización de los procedimientos:** En esta fase se revisan y actualizan los procedimientos existentes para que cumplan con los requerimientos exigidos en la norma vigente 27001:2022.

3) **Implementación:** Finalmente, se lleva a cabo la implementación de los cambios necesarios para asegurar que los procedimientos y controles estén alineados con la nueva versión de la norma.

4. VALOR ESTIMADO DEL CONTRATO Y LA JUSTIFICACIÓN DE ESTE.

EL valor de presupuesto oficial corresponde a la suma **DOSCIENTOS NOVENTA Y NUEVE MILLONES NOVECIENTOS SETENTA Y NUEVE MIL CIENTO SESENTA Y SIETE PESOS MCTE ($299.979.167,00),** incluido IVA y demás impuestos, tasas, contribuciones, costos directos e indirectos, a que hubiere lugar.

5. ANÁLISIS TÉCNICO DEL SECTOR

Ver documento Análisis del Sector y estudios de mercado, numeral 2.

5.1 VERIFICACION SOBRE LA EXISTENCIA Y APLICACIÓN DE ACUERDOS MARCOS

En cumplimiento del artículo 2.2.1.2.1.2.9. Del Decreto 1082 de 2015, se verificó en la página web de "COLOMBIA COMPRA EFICIENTE" los acuerdos marco vigente y se evidenció que **NO** existe acuerdo marco que puede estar relacionado directamente con los bienes objeto del presente proceso.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

6. CARACTERÍSTICAS Y/O ESPECIFICACIONES TÉCNICAS DE LOS BIENES Y/O SERVICIOS A CONTRATAR Y/O OBLIGACIONES CONTRACTUALES:

El contratista debe garantizar la prestación del servicio objeto del proceso de selección, dando cumplimiento a las especificaciones técnicas indicadas a continuación:

[redacted]	
1.1.1	Revisar los 14 numerales existentes de la versión 27001:2013 para verificar el estado de la información, para la transición a la nueva versión 27001:2022 de acuerdo como lo exige la norma. (entregar informe técnico de la revisión efectuada).
1.1.2	Revisar los 114 controles existentes de la versión 27001:2013 para verificar el estado de la información, para realizar la transición a la nueva versión 27001:2022 de acuerdo como lo exige la norma. (entregar informe técnico de la revisión efectuada).
1.1.3	Revisar el levantamiento de activos, (identificación, valoración y clasificación) de los mismos para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe de la revisión efectuada.)
1.1.4	Revisar el levantamiento de riesgos (Identificación, análisis de riesgos, evaluación de riesgos, tratamiento, revisión, monitoreo y comunicación) de los mismos para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe de la revisión efectuada.)
1.1.5	Revisar las escalas de impacto y niveles de clasificación de la información para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe de la revisión efectuada.)
1.1.6	Revisar la política general de seguridad de la información que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe de la revisión efectuada).
1.1.7	Revisar las partes interesadas del SGSI con sus respectivas necesidades y expectativas para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe de la revisión efectuada).
1.1.8	Revisar la Declaración de aplicabilidad para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe de la revisión efectuada).
1.1.9	Revisar el análisis de brechas de seguridad GAP existente para que cumpla los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe de la revisión efectuada).
1.1.10	Revisar los indicadores del SGSI para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe de la revisión efectuada).
1.1.11	Revisar los objetivos del SGSI para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe de la revisión efectuada)
1.1.12	Revisar el autodiagnóstico del SGSI para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe de la revisión efectuada)
[redacted]	
1.2.1.	Revisión y actualización de los procedimientos existentes que se requieran para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe de cada uno de los procedimientos mencionados actualizados a la nueva norma ISO 27001:2022) así: Procedimiento gestión de usuarios y contraseñas. Procedimiento acciones correctivas y preventivas.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

OBJETO ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA A LA NUEVA VERSIÓN DE LA NORMA ISO 27001:2022	
	Procedimiento Auditorías Internas. Procedimiento revisión por la alta dirección. Procedimiento Gestión de Incidentes de Seguridad. Procedimiento Seguridad de los medios e información en tránsito. Procedimiento identificación de requisitos legales. Procedimiento gestión de vulnerabilidades. Procedimiento segregación de roles. Procedimiento de activos y riesgos. Procedimiento Acceso Áreas Seguras Data Center. Procedimiento Gestión Copias de Respaldo. Procedimiento Control de cambios TI. Procedimiento etiquetado de la información. Procedimiento gestión de medios removibles y solicitud servicios mesa de ayuda – TICS.
1.2.2	Si durante la verificación de los procedimientos existentes se identifican necesidades adicionales, se crearán nuevos procedimientos conforme a lo requerido en la nueva versión ISO 27001:2022.
[illegible]	[illegible]
1.3.1	Alinear los 14 numerales existentes de la versión 27001:2013 a los 4 numerales de la nueva versión 27001:2022 de acuerdo como lo exige la norma. (entregar informe técnico donde se evidencie el cambio de los numerales de la versión 27001:2013 a la nueva versión 27001:2022). -Controles Organizacionales -Controles de personas -Controles físicos -Controles tecnológicos
1.3.2	Alinear los 114 controles existentes de la versión 27001:2013 a los 93 controles de la nueva versión 27001:2022 de acuerdo como lo exige la norma. (entregar informe técnico donde se evidencie el cambio de los controles de la versión 27001:2013 a la nueva versión 27001:2022). -Controles Organizacionales: Con un total de 37 controles enfocados principalmente en la seguridad de la información administrativa de la organización. -Controles de personas: Con un total de 8 controles enfocados en la seguridad de la información en el capital humano. -Controles físicos: Con un total 14 controles enfocados principalmente en la seguridad de las instalaciones físicas. -Controles tecnológicos: Con un total de 34 controles enfocados en la seguridad informática de los sistemas de información de la organización.
1.3.3	actualización al levantamiento de activos, (identificación, valoración y clasificación) de los mismos para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe.)
1.3.4	actualización al levantamiento de riesgos (Identificación, análisis de riesgos, evaluación de riesgos, tratamiento, revisión, monitoreo y comunicación) de los mismos para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe.)
1.3.5	actualización de las escalas de impacto y niveles de clasificación de la información para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe.)
1.3.6	actualizar la política general de seguridad de la información que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar Manual de Seguridad de la Información actualizada a la nueva versión ISO27001:2022).

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

OBJETO: ACTUALIZACION DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) PARA LA UNIDAD DE GESTION GENERAL DEL MINISTERIO DE DEFENSA A LA NUEVA VERSION DE LA NORMA ISO 27001:2022	
1.3.7	actualizar partes interesadas del SGSI con sus respectivas necesidades y expectativas para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar informe partes interesadas actualizada a la nueva versión ISO27001:2022).
1.3.8	actualizar la Declaración de aplicabilidad para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe comparativo (versión ISO27001:2013 a la versión ISO27001:2022).
1.3.9	actualización del análisis de brechas de seguridad GAP existente para que cumpla los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe del análisis de brechas de seguridad GAP análisis versión ISO27001:2013 a la versión ISO27001:2022).
1.3.10	actualización que los indicadores del SGSI para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar un informe de los indicadores del muestreo de las evidencias tomadas de los indicadores definidos). ▪ Al menos cuatro (4) indicadores para la medición del SGSI y cuatro (4) para la medición específica de los principales controles de seguridad tecnológica, procedimental y/o del talento humano.
1.3.11	actualización del autodiagnóstico al SGSI para que cumplan los requerimientos exigidos en la norma vigente 27001:2022. (entregar la matriz del autodiagnóstico de la norma vigente 27001:2022
1.3.12	Validar los resultados obtenidos en las fases anteriores y generar los planes de acción necesarios para mejorar el Sistema de Gestión de Seguridad de la Información implementado. (entregar el informe final de la auditoría realizada donde se evidencie los hallazgos, oportunidades de mejora, buenas prácticas entre otras).
[illegible] CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN [illegible]	
2.1	Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista debe garantizar la integridad y confidencialidad de la información institucional a la cual llegue a tener acceso directamente o por intermedio de terceros, para lo cual el contratista suscribe el respectivo compromiso de confidencialidad que hará parte integral del presente contrato.
2.2	De igual manera, el desarrollo de las pruebas y sus resultados serán considerados por el contratista como información confidencial propiedad del Ministerio de Defensa Nacional, en tal virtud, adoptará todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida, asimismo, suscribirá el formato de confidencialidad de la información.
2.3	Durante el desarrollo de las actividades el contratista se compromete a no hacer uso indebido de las herramientas utilizadas para el cumplimiento del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.
[illegible]	
3.1	Para el desarrollo del contrato se propone un equipo de trabajo mínimo, el cual debe cumplir con toda la estructura necesaria para garantizar el desarrollo del contrato. El proponente deberá disponer de todos los profesionales necesarios para la ejecución del contrato.

PERFIL	CANTIDAD	DEDICACIÓN
GERENTE DE PROYECTO	1	50%
CONSULTORES DE SEGURIDAD DE LA INFORMACION	2	100%

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

[illegible]	[illegible] SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN [illegible] UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA A LA NUEVA [illegible] ISO 27001: 2022
	Todo el personal relacionado deberá ser tenido en cuenta por el proponente para la valoración de su propuesta económica. Los profesionales exigidos, deben cumplir y adjuntar como mínimo con los requisitos de calidad, experiencia y documentos solicitados, teniendo en cuenta lo siguiente: 1) **GERENTE DE PROYECTO.** **Formación Académica:** • Título Profesional en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Software o Ingeniería en Telecomunicaciones o Ingeniería Telemática, • Título de Posgrado en modalidad de especialización en Gerencia de Proyectos o Administración de Negocios o Gerencia de Tecnología. **Experiencia:** mínimo diez (10) años de experiencia general, contados a partir de la fecha de expedición de la matricula profesional y hasta la fecha de cierre del presente proceso de selección. **Documentos Adicionales**, aportar las siguientes certificaciones: • Certificación PMP • Auditor Líder ISO 27001:2022 2) **CONSULTOR DE SEGURIDAD DE LA INFORMACIÓN.** **Formación Académica:** • Título profesional en Ingeniería de Sistemas o Ingeniería Informática o Ingeniería de Software o Ingeniería en Telecomunicaciones o Ingeniería Telemática. • Título de Posgrado en modalidad de especialización en Seguridad Informática o Seguridad de la información. **Experiencia:** mínimo cinco (5) años de experiencia general, contados a partir de la fecha de expedición de la matricula profesional y hasta la fecha de cierre del presente proceso de selección. **Documentos Adicionales,** aportar las siguientes certificaciones: • Auditor Líder ISO 27001:2022 • Gestor de Ciberseguridad ISO 27032:2023
3.2	Respecto de las certificaciones de experiencia laboral, el proponente debe contemplar para cada uno la siguiente información: 1.NOMBRE O RAZÓN SOCIAL DEL CONTRATISTA A QUIEN SE CERTIFICA 2. FECHA DE EXPEDICIÓN DE LA CERTIFICACIÓN 3. NOMBRE O RAZÓN SOCIAL DEL CONTRATANTE O DE QUIEN CERTIFICA 4. FECHA DE SUSCRIPCIÓN DEL CONTRATO QUE SE CERTIFICA 5. OBJETO DEL CONTRATO QUE SE CERTIFICA 6. PORCENTAJE DE EJECUCIÓN DEL CONTRATO 7. ACTIVIDADES DEL CONTRATO QUE SE CERTIFICA

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

OBJETO: ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA NACIONAL VERSIÓN DE LA NORMA ISO 27001:2022	
	8. NOMBRE Y/O RAZÓN SOCIAL DE QUIEN EXPIDE LA CERTIFICACIÓN 9. FECHA DE INICIO DEL CONTRATO QUE SE CERTIFICA (Mes/Año) 10. FECHA TERMINACIÓN DEL CONTRATO QUE SE CERTIFICA (Mes/Año) 11. DURACIÓN EN MESES DEL CONTRATO 12. VALOR DEL CONTRATO QUE SE CERTIFICA (indicar el valor de las adiciones si las hubo) 13. PORCENTAJE DE PARTICIPACIÓN DEL PROPONENTE (en caso de que haya sido ejecutado en Unión temporal o consorcio) 14. NÚMERO TELEFÓNICO Y CORREO ELECTRÓNICO DE LA PERSONA NATURAL O JURÍDICA A LA CUAL LE PRESTÓ LOS SERVICIOS, DONDE SE PUEDA VERIFICAR LA INFORMACIÓN (en el caso en que esta información no se encuentre en la certificación y la misma pueda ser consultada en herramientas y/o plataformas de datos abiertos del estado colombiano, páginas web, sistema electrónico de compras públicas, se entenderá como cumplido este requisito).Ó Mediante el acta de liquidación del (los) contrato (s) que se certifiquen
[illegible]	[illegible]
4.1	El contratista entregará un plan de trabajo detallado, el cual debe contener las fechas de ejecución de cada fase. Este cronograma deberá ser acordado y presentado en un plazo máximo de tres (03) días hábiles una vez firmada del acta de inicio, aprobada por el supervisor del contrato.
4.2	El contratista realizará las actividades descritas en el presente documento en el sitio de las instalaciones de la Dirección de Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa Nacional, garantizando la continuidad del desarrollo o ejecución de cada una de las actividades objeto del contrato; las labores se realizarán en el horario de 08:00 a 17:00 horas, de lunes a viernes.
4.3	El contratista en el caso que requiera efectuar el reemplazo del personal autorizado para la ejecución del contrato, por alguien con igual o mayor experiencia, el cual deberá aportar la documentación para aprobación del supervisor.
4.4	Al personal asignado para el desarrollo del proyecto por parte del contratista, se le realizara un estudio de seguridad para lo cual se debe aportar la siguiente documentación en un término no mayor de 5 días calendarios a partir de la firma del acta de inicio: a. Copia cedula de ciudadanía b. Copia libreta militar c. Referencias laborales d. Copia de los diplomas estudios – Actas de Grado e. Copia de la tarjeta profesional. f. Antecedentes judiciales g. Antecedentes disciplinarios procuraduría h. Boletín de responsabilidades fiscales contraloría i. Referencias personales j. Diligenciamiento del formato Estudio de Seguridad Personal MDN
4.5	El contratista debe garantizar que los expertos tengan su propio equipo de cómputo, así como los demás recursos necesarios para cumplir con su trabajo (equipos, internet, herramientas y software licenciado que requiera para prestar los servicios derivados del objeto del contrato.). De requerirse, el equipo de cómputo debe someterse al proceso de sanitización establecido por el Ministerio de Defensa Nacional - MDN donde será analizado y verificado durante el ingreso y salida de las instalaciones pertenecientes al MDN, con el fin de garantizar la seguridad de la información de la entidad.
4.6	El personal que conforme el equipo de trabajo del contratista debe brindar un trato formal y respetuoso a los usuarios del Ministerio de Defensa Nacional, acatando fielmente los procedimientos que se establezcan para la prestación de los servicios.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

OBJETO: CONTRATACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN [illegible] GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA A LA NUEVA VERSIÓN DE LA NORMA ISO 27001:2022	
4.7	El contratista asumirá todos los costos o gastos asociados al desplazamiento de su personal a los sitios de trabajo del Ministerio de Defensa Nacional.
4.8	El contratista debe garantizar para cada integrante del equipo de trabajo que asigne al desarrollo del objeto contractual, efectúe las actividades de manera presencial en el sitio de las instalaciones de la Dirección de Tecnologías de la Información y las Comunicaciones.
4.9	Dada la naturaleza de las actividades a realizar en desarrollo del objeto contractual, el contratista se debe comprometer bajo acuerdo de confidencialidad suscrito con el MDN, garantizando la integridad y confidencialidad de la información institucional, que la información suministrada no pueda ser divulgada en forma parcial o total a terceros, ni utilizada con propósitos distintos al desarrollo del contrato. Así mismo, El contratista deberá asegurar el cuidado, la confidencialidad y la correcta utilización de la información entregada y generada durante la ejecución del contrato, así como de los elementos que para su ejecución la Unidad de Gestión General del MDN ponga a su disposición. El citado documento deberá suscribirse una vez se firme el acta de inicio.

7. CRITERIOS Y DOCUMENTOS TÉCNICOS MÍNIMOS HABILITANTES.

7.1. CERTIFICADO DE INSCRIPCIÓN, RENOVACIÓN Y ACTUALIZACIÓN EN EL REGISTRO ÚNICO DE PROPONENTES.

En el Registro Único de Proponentes expedido por la respectiva Cámara de Comercio en Colombia, el cual deberá tener una fecha de expedición no mayor a treinta (30) días calendarios anteriores a la fecha de presentación de la propuesta y encontrarse en firme a la fecha de cierre del proceso.

7.2. EXPERIENCIA HABILITANTE EXIGIDA PARA EL PROCESO DE SELECCIÓN Y FORMA DE ACREDITARLA

La experiencia es un requisito habilitante, por lo tanto, los oferentes deberán tenerla inscrita en el RUP, usando los códigos del Clasificador de Bienes y Servicios en el tercer nivel de conformidad con el artículo 2.2.1.1.1.5.2 del Decreto 1082 de 2015.

Se verificará como requisito habilitante máximo tres (3) contrato (s) relacionado (s) en el RUP esté clasificado en al menos un (1) de los siguientes códigos UNSPSC:

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE
80101500 Servicios de auditoría de TI	**80** Servicios de Gestion, Servicios Profesionales de Empresa y Servicios Administrativos	**10** Servicios de Asesoría de gestión	**15** Servicios de consultoría de negocios y administración corporativa
81102700 Servicios de diseño e ingeniería de sistemas instrumentados de control	**81** Servicios basados en Ingenieria, investigación y tecnología	**10** Servicios profesionales de ingeniería y arquitectura	**00** Servicios de diseño e ingeniería de sistemas instrumentados de control
81111800	**81**	**11**	**18**

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

Servicios de consultoría en seguridad informática	Servicios basados en Ingeniería, investigación y tecnología	Servicios Informáticos	Servicios de sistemas y administración de componentes de sistemas

Nota 1: Los consecutivos del reporte de los contratos ejecutados para acreditar la experiencia habilitante general pueden ser los mismos de la experiencia habilitante específica.

7.3 EXPERIENCIA HABILITANTE ESPECÍFICA EXIGIDA PARA EL PROCESO DE SELECCIÓN Y FORMA DE ACREDITARLA:

Los proponentes deberán acreditar la experiencia específica requerida para este proceso de selección a través de CUALQUIERA de las siguientes formas:

A. Certificaciones: **máximo tres (3) contratos** que hayan sido ejecutados en un cien por ciento (100%) a la fecha de cierre del proceso de contratación.

B. Que el (los) contrato(s) haya(n) sido ejecutado(s) durante los últimos tres (3) años anteriores a la fecha de cierre del proceso de selección.

C. Acreditar que el Objeto del (los) contrato (s) ejecutado (s) sea igual o similar al objeto de la presente contratación, entiéndase por similar que el objeto del contrato contemple actividades de: **Implementación ó auditoría ó evaluación ó Actualización de Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001:2022.**

Sin embargo, no será obligatorio que el objeto de cada uno de los contratos y de cada una de las certificaciones con los cuales se acredita la experiencia contenga todas las actividades de manera conjunta, por lo que las actividades pueden ser acreditadas de manera independiente, en máximo tres (3) contratos.

D. La sumatoria de la cuantía del (los) contrato(s) ejecutados deberá(n) ser igual o mayor al 100% del valor del presupuesto oficial, asignado al proceso de contratación, expresado en S.M.L.M.V.

Los proponentes obligados a estar inscritos en el RUP deben tener allí registrados los contratos con que pretender acreditar la experiencia específica.

El (los) contrato(s) que el proponente acredite como experiencia debe(n) identificarse claramente en el RUP, por lo tanto, deberá indicar en el cuestionario del proceso del SECOP II, el (los) número (s) del consecutivo del reporte del contrato ejecutado con el (los) cual (es) está acreditando la experiencia requerida, siempre y cuando contengan la totalidad de los siguientes datos:

1. NOMBRE O RAZÓN SOCIAL DEL CONTRATISTA A QUIEN SE CERTIFICA
2. FECHA DE EXPEDICIÓN DE LA CERTIFICACIÓN
3. NOMBRE O RAZÓN SOCIAL DEL CONTRATANTE O DE QUIEN CERTIFICA
4. FECHA DE SUSCRIPCIÓN DEL CONTRATO QUE SE CERTIFICA
5. OBJETO DEL CONTRATO QUE SE CERTIFICA
6. PORCENTAJE DE EJECUCIÓN DEL CONTRATO

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

7. ACTIVIDADES DEL CONTRATO QUE SE CERTIFICA
8. NOMBRE Y/O RAZÓN SOCIAL DE QUIEN EXPIDE LA CERTIFICACIÓN
9. FECHA DE INICIO DEL CONTRATO QUE SE CERTIFICA (Mes/Año)
10. FECHA TERMINACIÓN DEL CONTRATO QUE SE CERTIFICA (Mes/Año)
11. DURACIÓN EN MESES DEL CONTRATO
12. VALOR DEL CONTRATO QUE SE CERTIFICA (indicar el valor de las adiciones si las hubo)
13. PORCENTAJE DE PARTICIPACIÓN DEL PROPONENTE (en caso de que haya sido ejecutado en Unión temporal o consorcio)
14. NÚMERO TELEFÓNICO Y CORREO ELECTRÓNICO DE LA PERSONA NATURAL O JURÍDICA A LA CUAL LE PRESTÓ LOS SERVICIOS, DONDE SE PUEDA VERIFICAR LA INFORMACIÓN (en el caso en que esta información no se encuentre en la certificación y la misma pueda ser consultada en herramientas y/o plataformas de datos abiertos del estado colombiano, páginas web, sistema electrónico de compras públicas, se entenderá como cumplido este requisito).Ó Mediante el acta de liquidación del (los) contrato (s) que se certifiquen.

Los consecutivos del reporte de los contratos ejecutados para acreditar la experiencia habilitante general pueden ser los mismos de la experiencia habilitante especifica.

7.4 CRITERIOS DIFERENCIALES PARA MIPYME EN EL SISTEMA DE COMPRAS PÚBLICAS

En aplicación a los artículos 2.2.1.2.4.2.15. y 2.2.1.2.4.2.18 del decreto 1082 de 2015, adicionados por el Decreto 1860 de 2021, el Ministerio incluye para el presente proceso como "*Criterios diferenciales para emprendimientos y empresas de mujeres en el sistema de compras públicas*" y "*Criterios diferenciales para Mipyme en el sistema de compras públicas*", se establece como condición habilitante diferencial para las Mipyme domiciliadas en Colombia y emprendimientos y empresas de mujeres, el aspecto relacionado con la experiencia, literal A de la siguiente manera:

CERTIFICACIONES: Máximo cuatro (4) contratos que hayan sido ejecutados en un 100%.

Los proponentes deberán acreditar la experiencia específica requerida para este proceso de selección a través de CUALQUIERA de las siguientes formas:

a) Mediante la presentación de certificaciones suscritas por la persona natural o jurídica **contratante**, siempre y cuando contengan la totalidad de datos solicitados en el Anexo, y con el lleno de los requisitos antes exigidos, o;
b) Mediante el acta de liquidación del (los) contrato (s) que se certifiquen.

7.5 DOCUMENTOS Y VERIFICACIONES TÉCNICOS ADICIONALES

El Oferente deberá presentar copia de la certificación emitida por una entidad certificadora acreditada o su representante en Colombia en la que conste que el oferente se encuentra certificado en la norma ISO 27001:2022 Sistema de Gestión de Seguridad de la Información (SGSI).

El proponente deberá aportar la certificación en original o copia autentica debidamente apostilladas y traducidas de conformidad con la normatividad legal vigente.

Sistema de Gestión y Desempeño Institucional
IQNet
Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

8. CRITERIOS TÉCNICOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE.

De conformidad con lo establecido en la Ley 1150 de 2007, artículo 5 numeral 4 el cual establece: *"En los procesos para la selección de consultores se hará uso de factores de calificación destinados a valorar los aspectos técnicos de la oferta o proyecto. De conformidad con las condiciones que señale el reglamento, se podrán utilizar* ***criterios de experiencia específica del oferente y el equipo de trabajo****, en el campo de que se trate. En ningún caso se podrá incluir el precio, como factor de escogencia para la selección de consultores (...)".*

8.1 PONDERACIÓN TECNICA (Máximo 100 puntos)

Para efectos de la evaluación de los factores de escogencia se considerarán únicamente las propuestas hábiles, es decir, aquellas que cumplan la totalidad de los requisitos habilitantes para la participación en el proceso.

8.1.1 OFRECIMIENTO ADICIONAL POR PARTE DEL OFERENTE PARA OBTENER PONDERACIÓN TÉCNICA (Máximo 60 puntos)

Los oferentes que efectúen los ofrecimientos señalados a continuación, para lo cual se diligenciará el **Anexo No. 4** "OFRECIMIENTO ADICIONAL POR PARTE DEL OFERENTE PARA OBTENER LA PONDERACIÓN TÉCNICA" del presente pliego, se les asignará el puntaje indicado así:

Se asignará un máximo de **sesenta (60) puntos** al proponente que ofrezca, como valor agregado, la realización de las actividades adicionales establecidas en los FACTORES DE PONDERACIÓN TÉCNICA.

En documento independiente debidamente suscrito, el oferente garantizará el cumplimiento del aspecto de ponderación técnica adicional y se asignarán puntos al oferente que oferte adicionalmente a lo mínimo habilitante requerido, así:

OFRECIMIENTO ADICIONAL POR PARTE DEL OFERENTE	PUNTOS
El proponente que ofrezca el curso y el baucher para certificarse como Certified Ethical Hacker (CEH-EC-Council) última versión, por una institución acreditada, para tres (03) funcionarios de TIC´S.	30
El proponente que ofrezca el curso y el baucher para certificarse como CHFI Computer Hacking Forensic Investigator (EC-Council) última versión, por una institución acreditada, para tres (03) funcionarios de TIC´S.	20
El proponente que realice tres (3) campañas de sensibilización al personal de la Unidad de Gestión General del Ministerio de Defensa UGG sobre el SGSI. (infografías, videos cortos, trivias interactivas, simulacros de incidentes, juegos interactivos) (entregar evaluaciones de efectividad de las sensibilizaciones).	10

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

8.1.2 FORMACIÓN ACADÉMICA Y EXPERIENCIA ADICIONAL DEL PERSONAL MÍNIMO REQUERIDO (MÁXIMO 40 PUNTOS)

Se otorgará un puntaje máximo de **cuarenta (40) puntos** al proponente que ofrezca:

EXPERIENCIA Y FORMACION ACADEMICA ADICIONAL DEL PERSONAL MINIMO REQUERIDO	PUNTOS
Si el profesional propuesto como **Gerente de Proyecto** acredita, experiencia adicional a la mínima requerida, de 5 años con relación Gestión de Proyectos en Tecnologías	14
Si el profesional propuesto como **Consultor de Seguridad de la Información** acredita, experiencia adicional a la mínima requerida, de 5 años de experiencia sobre consultoría de seguridad de la información o continuidad del negocio.	14
Si el profesional propuesto como **Gerente de Proyecto** acredita, además, una en Maestría en administración de Negocios.	8
Si el profesional propuesto como **Consultor de Seguridad de la Información** acredita, además, una en Maestría en seguridad de la información o seguridad informática o ciberseguridad.	4

NOTA 1: Sobre los aspectos y/o documentos señalados para la asignación del puntaje técnico, el Ministerio **NO REALIZARÁ ningún tipo de requerimiento, teniendo en cuenta que los mismos constituyen factor de escogencia de las ofertas.**

NOTA 2: En caso de no ofertar los aspectos técnicos objeto de ponderación de la oferta se le asignará cero (0) puntos y la misma **no constituye factor excluyente**.

NOTA 3: Para efectos de la ponderación técnica el oferente deberá indicar el **FACTOR ADICIONAL que ofrece** en el presente Anexo No. 4 "OFRECIMIENTO ADICIONAL POR PARTE DEL OFERENTE PARA OBTENER LA PONDERACIÓN TÉCNICA".

8.2. APOYO A LA INDUSTRIA NACIONAL (20%)

La Industria Nacional será efectuado ***después de la sumatoria del puntaje técnico*** de la siguiente forma:

Para estimular la industria colombiana cuando los proponentes oferten bienes o servicios nacionales	**20%**
Tratándose de bienes o servicios extranjeros, la entidad contratante establecerá un puntaje, para incentivar la incorporación de componente colombiano de bienes y servicios profesionales, técnicos y operativos.	**10%**
NOTA: Si una vez efectuada la calificación correspondiente, la oferta de un proponente extranjero se encuentra en igualdad de condiciones con la de un proponente nacional, se adjudicará al nacional. (Art. 2 Ley 816 de 2003).	

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

8.3. PUNTAJE ADICIONAL EMPRENDIMIENTO Y EMPRESAS DE MUJERES (0,25 % DEL PUNTAJE TOTAL TÉCNICO)

Se otorgará un puntaje adicional de cero puntos veinticinco por ciento (0.25%) del valor total del puntaje técnico de los puntos establecidos en los pliegos de condiciones o documentos equivalentes, a lo establecido en el artículo 2.2.1.2.4.2.14. del Decreto 1082 de 2015, adicionado por el artículo 3 del Decreto 1860 de 2021 y demás normas concordantes y complementarias, emprendimientos y empresas de mujeres. El oferente deberá diligenciar los emprendimientos y empresas de mujeres de conformidad con lo establecido en el artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015, adicionado por el artículo 3 del Decreto 1860 de 2021.

8.4. PUNTAJE ADICIONAL MIPYMES (0,25 % DEL PUNTAJE TOTAL TÉCNICO)

La Entidad otorgará un puntaje adicional de cero puntos veinticinco por ciento (0.25%) del valor total del puntaje técnico de los puntos establecidos en los pliegos de condiciones o documentos equivalentes, a los proponentes que acrediten la calidad de Mipyme conforme a lo establecido en el numeral para la capacidad jurídica del pliego de condiciones.

Tratándose de proponentes plurales, los criterios diferenciales y los puntajes adicionales solo se aplicarán si por lo menos uno de los integrantes acredita que es emprendimiento y empresa de mujeres bajo los criterios dispuestos en el artículo precedente y que tiene una participación igual o superior al diez por ciento (10%) en el consorcio o la unión temporal.

8.5. PUNTAJE ADICIONAL INCENTIVO PARA VINCULACIÓN LABORAL DE PERSONAS CON DISCAPACIDAD (1,00 % DEL PUNTAJE TOTAL TÉCNICO)

En virtud de lo previsto en el Artículo 2.2.1.2.4.2.6 del Decreto 1082 de 2015, en el presente proceso con el fin de incentivar el sistema de preferencias a favor de las personas con discapacidad, la entidad otorgará el uno por ciento (1%) del total de los puntos establecidos, esto es 1 punto, a los proponentes que acrediten la vinculación de trabajadores con discapacidad en su planta de personal, de acuerdo con los siguientes requisitos[1]:

> *"(...) 1. La persona natural, el representante legal de la persona jurídica o el revisor fiscal, según corresponda certificará el número total de trabajadores vinculados a la planta de personal del proponente o sus integrantes a la fecha de cierre del proceso de selección.*
>
> *2. Acreditar el número mínimo de personas con discapacidad en su planta de personal, de conformidad con lo señalado en el certificado expedido por el Ministerio de Trabajo, el cual deberá estar vigente a la fecha de cierre del proceso de selección.*
>
> *Verificados los anteriores requisitos, se asignará el 1%, a quienes acrediten el número mínimo de trabajadores con discapacidad, señalados a continuación:*

Número total de trabajadores de la planta de personal del proponente	Número mínimo de trabajadores con discapacidad exigido

[1] Tomado de: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=77653

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

Entre 1 y 30	1
Entre 31 y 100	2
Entre 101 y 150	3
Entre 151 y 200	4
Más de 200	5

Tabla No. 4. Profesionales Vinculados con discapacidad Fuente: Decreto 1082 de 2015 (...)".

Nota 1: Para efectos de lo señalado en el presente artículo. si la oferta es presentada por un consorcio, unión temporal o promesa de sociedad futura, se tendrá en cuenta la planta de personal del integrante del oferente plural que aporte como mínimo el cuarenta por ciento (40%) de la experiencia requerida para la respectiva contratación.

Nota 2: Para la obtención del puntaje por este factor, el oferente deberá presentar junto con la propuesta, los documentos requisito establecidos en el numeral 1 y 2 del Art. 2.2.1.2.4.2.6 del Decreto No. 392 de 2018.

8.7. FOMENTO A LA EJECUCIÓN DE CONTRATOS ESTALES POR PARTE DE LA POBLACIÓN EN POBREZA EXTREMA, DESPLAZADOS POR LA VIOLENCIA, PERSONAS EN PROCESO DE REINTEGRACIÓN O REINCORPORACIÓN.

Con respecto al artículo 2.2.1.2.4.2.16. "*Fomento a la ejecución de contratos estatales por parte de población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional*" del decreto 1860 de 2021, esta Dirección se permite informar que para el desarrollo y ejecución de la prestación del servicio de actualización de la Norma ISO 27001.2022 para la Unidad de Gestión General del Ministerio de Defensa Nacional, se requiere de talento humano especializado con el conocimiento y experiencia en materia de sistemas de gestión en normas ISO 27001.

Igualmente, se incurre en alto riesgo de que el proceso se declare desierto, al exigir a los oferentes el cumplimiento de esta directriz y ellos no cuenten con el talento humano, de las condiciones que trata el decreto 1860 de 2021, con la suficiente experiencia en materia de seguridad informática y análisis de vulnerabilidades y hacking ético.

8.6. REQUISITOS PONDERABLES

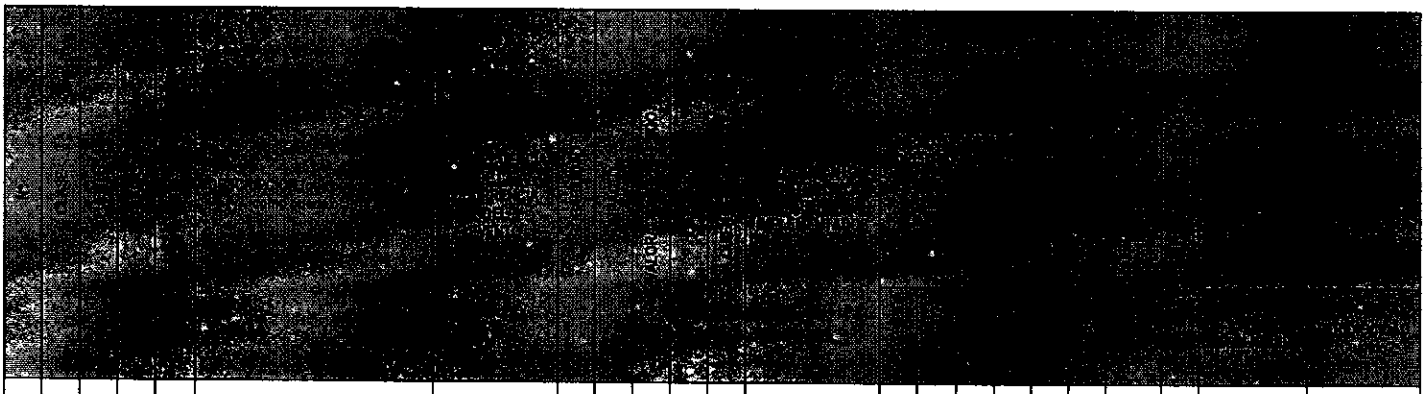
Experiencia adicional del oferente	60 puntos
Formación académica y experiencia adicional del Personal	40 puntos
Apoyo a la Industria Nacional	20%
Emprendimiento y empresas de mujeres	0,25 %
Mipymes	0,25%

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

vinculación laboral de personas con discapacidad	1%
PUNTAJE TOTAL TÉCNICO	**100 PUNTOS**

9. ANÁLISIS DE RIESGO Y LA FORMA DE MITIGARLO

De acuerdo con lo establecido por el artículo 4º de la Ley 1150 de 2007, los artículos 2.2.1.1.1.6.3, . del Decreto 1082 de 2015, la Dirección de Tecnologías de la Información y comunicaciones ha tipificado, estimado y asignado provisionalmente los siguientes riesgos previsibles involucrados en la presente contratación, de conformidad con la siguiente matriz y aplicación de la siguiente tabla:



1	Específico	Externo	Ejecución	operacional	Inadecuados procesos, procedimientos, parámetros, sistemas de información y tecnológicos, equipos humanos o técnicos	Posibilidad de no obtención del objeto del contrato	Improbable (3)	Menor (2)	5	Riesgo Medio	Contratista	Exigir al contratista los más altos estándares de cumplimiento y calidad de los bienes y servicios objetos del contrato.	Improbable (2)	Menor (2)	4	Riesgo bajo	Si	Contratista	Desde la suscripción y publicación del contrato, emisión del certificado de registro presupuestal y aprobación de las garantías.	Hasta la terminación del contrato.	Seguimiento y validación del cumplimiento de las obligaciones y comunicación periódica con el contratista revisando este riesgo	En los informes mensuales del supervisor sobre el cumplimiento del contrato.
2	General	Externo	Ejecución	Operacional	Riesgos asociados a la operatividad del contrato, tales como la no obtención del objeto del contrato como consecuencia de la existencia de inadecuados en la entrega de los elementos que generen demoras en las entregas, y calidad en los productos.	Inadecuados procesos	improbable(3)	Menor(3)	6	Riesgo Alto	Contratista	Exigir al contratista los más altos estándares de cumplimiento y calidad de los bienes y servicios objeto del contrato	Improbable (2)	Menor (2)	4	Riesgo bajo	Si	Contratista	Desde la suscripción y publicación del contrato,	Hasta la terminación del contrato.	Seguimiento y validación del cumplimiento de las obligaciones y comunicación periódica con el contratista, revisando ese riesgo.	En los informes mensuales del supervisor sobre el cumplimiento del contrato.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

3	Específico	externo	Ejecución	operacional	Acceso o divulgación no autorizada que permita la utilización indebida de la información o del servicio	Posibilidad de no obtención del objeto del contrato	Improbable (2)	Menor (2)	Riesgo bajo	Alto	Contratista	Exigir al contratista los más altos estándares de cumplimiento y calidad de los bienes y servicios objeto del contrato	Insignificante (1)	Menor (2)	3	Riesgo bajo	Si	Contratista	Desde la suscripción y publicación del contrato,	Hasta la terminación del	Seguimiento y validación del cumplimiento de las obligaciones y comunicación periódica con el contratista revisando este riesgo	En los informes periódicos del supervisor sobre el cumplimiento del contrato

10. LUGAR Y PLAZO DE EJECUCIÓN

El plazo para ejecutar el contrato resultante del proceso será **hasta el 15 de noviembre de 2025** a partir de la suscripción del Acta de Inicio, previa expedición del registro presupuestal y aprobación de la(s) garantía(s) que debe tomar el contratista.

El lugar de ejecución será en el Complejo Militar CAN ubicado en la Carrera 54 No. 26-25 de la ciudad de Bogotá D.C.

11. FORMA DE PAGO

Marca con una X:

A) Mensual _____, bimensual____ __trimestral_____, semestral _____.
B) Por servicio o producto entregado _____.
C) Un único pago al finalizar el contrato _X___.

El valor del contrato, se pagará, por intermedio de la Dirección de Finanzas de este Ministerio, al CONTRATISTA, en **UN ÚNICO PAGO** correspondiente al 100% del valor total del contrato **a la entrega de los informes recibidos a satisfacción al supervisor del contrato**, una vez se encuentre aprobado el P.A.C., (Programa Anual Mensualizado de Caja), por parte del Ministerio de Hacienda y Crédito Público, de acuerdo con el valor ofertado por el contratista, dentro de los treinta (30) días hábiles siguientes a la radicación en la Dirección de Finanzas de este Ministerio de los documentos requeridos para pago: Factura en caso de ser aplicable; certificado de cumplimiento a satisfacción suscrito por el supervisor designado y los demás trámites administrativos a que haya lugar.

12. PLAN DE COMPRAS

Certificado de disponibilidad Presupuestal CDP No. 28725 del 20-03-2025

13. VIGENCIA FUTURAS (CUANDO APLIQUE)

No aplica

DOCUMENTOS ANEXOS

- Cotizaciones

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial

- CDP
- ANALISIS DEL SECTOR Y ESTUDIOS DE MERCADO

14. OFERTA ECONÓMICA

DESCRIPCIÓN	CANTIDAD	UNIDAD	VALOR TOPE INCLUIDO IVA
ACTUALIZACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA A LA NUEVA VERSIÓN DE LA NORMA ISO 27001:2022	1	UN	$299.979.167,00

Bogotá, 09 de julio de 2025

MAURICIO ANDRES TELLEZ GARCES
Director de Tecnologías de la Información y las Comunicaciones

Revisó. Ing. Martha Lucia Sanchez Niño
Elaboró: IT. Yersonpp Daniel Quintero Zipa

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial