1. DEPENDENCIA SOLICITANTE

DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES - DEL MINISTERIO DE DEFENSA NACIONAL- OFICINA DE RESPUESTA A INCIDENTES CIBERNÉTICOS CSIRT

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

De conformidad con el artículo 5° del Decreto No. 1874 de diciembre 30 de 2021 *"Por el cual se modifica la estructura del Ministerio de Defensa Nacional, se crean nuevas dependencias, funciones y se dictan otras disposiciones"*, se creó la Oficina de Respuesta a Incidentes Cibernéticos – (CSIRT por sus siglas en inglés) adscrita a la Unidad de Gestión General, con subordinación del Despacho del señor Ministro de Defensa, entre las funciones a cumplir se encuentran las establecidas en el artículo 5, de las cuales se detallan las siguientes: *"(...) 2. "Coordinar las capacidades de ciberseguridad y ciberdefensa con la Dirección de Seguridad Nacional y los organismos del Sector Defensa y otros sectores"; (...) 4. "Generar e implementar los protocolos, lineamientos, guías, estándares, buenas prácticas y recomendaciones de ciberseguridad y ciberdefensa para el Sector Defensa y hacer su seguimiento, medición, análisis y evaluación."; 5. "Definir acciones, servicios de prevención, concientización y sensibilización ante amenazas cibernéticas y dar respuesta frente a incidentes en esta materia en el Sector Defensa"; (...) 7. "Formular e implementar planes, programas, proyectos y acciones que permitan generar y producir conocimiento relativo a la ciberseguridad y ciberdefensa para el Sector Defensa"; 8. "Generar cultura en el Sector Defensa para crear, conservar, compartir, difundir, reconocer y valorar el conocimiento relativo a la ciberseguridad y ciberdefensa y utilizar herramientas para su apropiación, seguimiento, medición, análisis y evaluación"; (...) 10. "Gestionar y establecer mecanismos de prevención y control a los incidentes cibernéticos que puedan ocurrir en Ministerio de Defensa Nacional y servir de punto focal especializado del Sector Defensa."; (...) 12. "Informar a los miembros del ecosistema cibernético del Sector Defensa acerca de las nuevas vulnerabilidades, advertencias y descubrimientos que afecten la seguridad cibernética"; (...)13. "Coordinar con la Dirección de Seguridad Nacional y organismos del Sector, la respuesta a incidentes cibernéticos de seguridad y defensa e implementar la infraestructura necesaria y hacer seguimiento a la gestión relacionada con el riesgo en estas materias"*, entre otras funciones.

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) publicó el Decreto 338 del 08 de marzo de 2022, por el cual se establecen "(...) *lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones* (...)". Es así como este Decreto reglamentó parcialmente los artículos 64 de la Ley 1437 de 2011, 147 de la Ley 1955 de 2019 y 230 de la Ley 1450 de 2011, modificado por el

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

artículo 148 de la Ley 1955 de 2019, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la· gestión de riesgos y la respuesta a incidentes de seguridad digital. En el mencionado Decreto, el artículo 2.2.21.1.1.4. estableció que las autoridades deberán adoptar medidas técnicas, humanas y administrativas para garantizar la gobernanza de la seguridad digital, la gestión de riesgos de seguridad digital, la identificación y reporte de infraestructuras críticas cibernéticas y servicios esenciales y la gestión y respuesta a incidentes de seguridad digital.

En la sección 5 *"Modelo Nacional de Atención y Gestión de Incidentes"* del Decreto 338 de 2022, se define que, el CSIRT Defensa, entre otras instancias nacionales, son las responsables para la atención y gestión de incidentes de seguridad digital. Así mismo, en la misma sección, en el artículo 2.2.21.1.5.5 *"Cooperación y coordinación de los CSIRT sectoriales"*, se consagra que el MinTIC con los CSIRT sectoriales establecerá dentro de los doce (12) meses siguiente a la expedición del presente decreto, un protocolo que incorpore los lineamientos y estándares de gestión de incidentes de seguridad digital nacional, que determine los roles, responsabilidades, mecanismos de coordinación, canales de comunicación y tiempos de respuesta que deberán cumplir cada uno de los equipos. Que el numeral 2.2.21.1.5.10 *"intercambio y reporte de información"* establece que los CSIRTs deberán priorizar acciones para facilitar el intercambio de información entre estos, así como con otras partes interesadas sobre amenazas, vulnerabilidades e incidentes, con el fin de desarrollar capacidades de análisis y prevención de incidentes cibernéticos.

Actualmente, la entidad cuenta con mecanismos de respaldo de información (backups) y controles de seguridad perimetral. Sin embargo, estos son insuficientes y no constituyen un plan de recuperación. Razón por la cual se requiere adelantar el presente proceso de selección con la finalidad de solventar dichas limitaciones, las cuales principalmente son:

(i) Inexistencia de un Plan Formal: No existe un Plan de Recuperación ante Desastres (DRP) documentado, estructurado y socializado. Las acciones de recuperación dependen del conocimiento individual del personal técnico, lo que genera incertidumbre, inconsistencia y falta de garantías en la respuesta.

(ii) Tiempos de Recuperación Indefinidos: Al no tener un plan, no se han definido ni medido los Objetivos de Tiempo de Recuperación (RTO) ni los Objetivos de Punto de Recuperación (RPO). Hoy, si falla un servidor crítico o se materializa un ciberataque destructivo (como un ransomware), no se puede garantizar en cuánto tiempo se restablecerá el servicio ni cuánta información se perderá, lo que podría afectar gravemente los sistemas misionales del Ministerio.

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

(iii) Procedimientos No Validados: Los respaldos de información existen, pero no se cuenta con protocolos probados y validados periódicamente que aseguren que dichos respaldos son funcionales y que el proceso de restauración se puede ejecutar de manera exitosa bajo un escenario de crisis.

Es relevante destacar que, si bien el CSIRT Defensa cumple un papel fundamental como ente de coordinación de incidentes a nivel sectorial, su capacidad para ejercer una supervisión efectiva se enfrenta a un desafío considerable: la diversidad de la infraestructura tecnológica y los sistemas de información administrados por la UGG. Esta heterogeneidad dificulta la estandarización de los controles, complica el seguimiento de potenciales incidentes en un perímetro lógico tan variado y limita la capacidad de generar alertas tempranas de manera unificada.

Esta falta de una capacidad de respuesta homogénea y predecible ante un incidente mayor subraya la necesidad crítica de diseñar un Plan de Recuperación ante Desastres (DRP) que estandarice los protocolos de actuación en todo el ecosistema tecnológico de la Unidad.

Que en consonancia con lo expuesto, teniendo en cuenta que La Unidad de Gestión General del Ministerio de Defensa Nacional administra procesos misionales críticos que dependen de la disponibilidad y continuidad de sus sistemas de información y ante el incremento exponencial y la sofisticación de las ciberamenazas a nivel global y sectorial, se ha identificado una brecha crítica entre las capacidades de prevención existentes estándar y la capacidad de respuesta y recuperación de la entidad ante un desastre tecnológico.

Actualmente, la entidad no cuenta con un DRP documentado, validado ni alineado con los estándares internacionales y sectoriales vigentes como la **ISO/IEC 27001 y Control A17** – *Gestión de la Seguridad de la Información*: Este estándar incluye controles específicos para la continuidad del negocio (Control A17), que exige redundancia en infraestructura TIC y continuidad en la seguridad de la información, elementos clave para un DRP efectivo y la **ISO/IEC 27031** – *Guía para la continuidad de las TIC*: Este estándar complementa la ISO 27001 y proporciona directrices específicas para la preparación de las tecnologías de la información y comunicaciones ante interrupciones lo cual representa una vulnerabilidad en términos de disponibilidad, tiempo de respuesta ante fallos e integridad operativa de los servicios TIC críticos.

En virtud de lo expuesto, resulta necesaria el diseño de este plan, el cual permitirá:

- Reducir el tiempo de inactividad y mitigar el impacto de incidentes tecnológicos sobre los procesos misionales.

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

- Fortalecer la resiliencia operativa y cibernética mediante protocolos claros, asignación de roles y validación periódica.
- Cumplir con obligaciones normativas y sectoriales, como el MSPI (Modelo de Seguridad y Privacidad de la Información) del MinTIC, las directrices del Ministerio de Defensa y los requisitos de auditoría.
- Establecer un marco técnico para la respuesta y recuperación, asegurando la continuidad de la operación institucional bajo escenarios adversos.

El DRP será una herramienta fundamental para garantizar la disponibilidad de los servicios tecnológicos, la protección de los activos de información y la respuesta articulada ante incidentes mayores o desastres tecnológicos.

Soportado en lo anterior y teniendo en cuenta que la Dirección Tecnologías de Información y Comunicaciones (TICS), estableció un modelo para la gestión automatizada e integrada de controles de seguridad informática, cuyo modelo en referencia se encuentra soportado en una arquitectura de ciberseguridad y lo conforman 11 áreas funcionales de Tics que se encargan de organizar y gestionar la seguridad digital en donde se desarrolla análisis de vulnerabilidades en la infraestructura y se cumple con lo requerido acuerdo a lo recomendado por Icontec en concordancia con la Norma Técnica Colombiana NTC-ISO/IEC 27001:2022, estas áreas funcionales se describen a continuación:

AREAS FUNCIONALES ARQUITECTURA DE CIBERSEGURIDAD
1. Administración de sistemas: proporciona la administración segura de la infraestructura de la Dirección TICS y los sistemas de seguridad, y protege a los canales de administración del sistema.
2. Seguridad de red: proporciona la seguridad de las redes, sus servicios, y el acceso a ellos a través de Internet y dispositivos conectados internamente.
3. Seguridad de aplicaciones: proporciona seguridad de las aplicaciones empresariales utilizando tecnologías de seguridad que sean apropiados y adaptados para la protección de esas aplicaciones y sus comunicaciones.
4. Punto final, servidor y dispositivo de seguridad: se prevé la protección de puntos finales, servidores y dispositivos que acceden a datos de la empresa, y los protege de compromiso.
5. Identidad, autenticación y administración de acceso: proporciona para la identificación, autenticación y control de acceso en todo el ciclo de vida de identidad, incluyendo el aprovisionamiento, la recertificación, y des aprovisionamiento.
6. Protección de Datos y Criptografía: prevé la protección de los datos almacenados en la Dirección TICS y el uso de tecnologías criptográficas para llevar a cabo esa protección, así como para apoyar otras operaciones tales como la autenticación, no repudio, y la integridad de los datos.

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

7. Monitoreo, la vulnerabilidad y la administración de revisiones: permite la supervisión regular de la infraestructura de seguridad, la exploración y el análisis de vulnerabilidades en la infraestructura, y la gestión de parches y soluciones temporales para hacer frente a esas vulnerabilidades.
8. Alta disponibilidad, recuperación de desastres y protección física: se prevé la protección de la disponibilidad en la Dirección TICS, incluyendo la realización de sistemas de alta disponibilidad, se recuperan de desastres, y físicamente protección de las instalaciones, las personas, los sistemas y los datos.
9. Respuesta a Incidentes: proporciona para la investigación, la respuesta y la recuperación de los incidentes que se identifican a través del monitoreo de la Dirección TICS.
10. Gestión de Activos: se prevé la contabilización de los activos de la Dirección TICS, información del activo, sus ciclos de vida, cambios.
11. Política, Auditoría, E-Discovery y Formación: prevé la supervisión de la política de controles de auditoría y de su eficacia, el apoyo a las actividades de e-discovery legales, y la formación del personal en las políticas y prácticas de seguridad adecuadas.

Mediante una iniciativa del Ministerio de Defensa que logró un mayor fortalecimiento a mediano y largo plazo de las capacidades en materia de tecnologías de la información y las comunicaciones, resultó de vital importancia la integración de capacidades operacionales, usos de tecnologías y servicios entre la oficina CSIRT y la Dirección de TICS, que si bien cumple un papel fundamental como ente de coordinación de incidentes a nivel sectorial y nacional, su capacidad para garantizar una respuesta homogénea se enfrenta a un desafío considerable: la diversidad de la infraestructura tecnológica y los sistemas de información administrados por la Dirección de Tecnologías de la Información y las Comunicaciones. Esta heterogeneidad dificulta la estandarización de los protocolos de actuación, complica el seguimiento de incidentes en un perímetro lógico tan variado y limita la capacidad de asegurar tiempos de recuperación predecibles.

.

Aunque en años anteriores no se había considerado indispensable contar con un Plan de Recuperación ante Desastres (DRP) debido a que la dependencia tecnológica era menor y los mecanismos básicos de respaldo resultaban suficientes, las condiciones actuales del Ministerio evidencian una necesidad urgente. Hoy, la operación institucional depende en gran medida de sistemas críticos de información y comunicaciones, y lo que se tiene implementado solo permite atender incidentes menores, sin garantizar la continuidad en casos de mayor impacto. La creciente frecuencia de ciberataques, las exigencias normativas vigentes y los riesgos identificados en auditorías internas hacen que esta contratación sea prioritaria, no solo para dar cumplimiento a la regulación, sino para proteger la misión institucional y asegurar la prestación continua de los servicios del Ministerio.

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)

De conformidad con el acta de sesión extraordinaria No. A20250808000273 de fecha 5 de agosto de 2025, el comité CITI aprobó la totalidad del proyecto aquí solicitado.

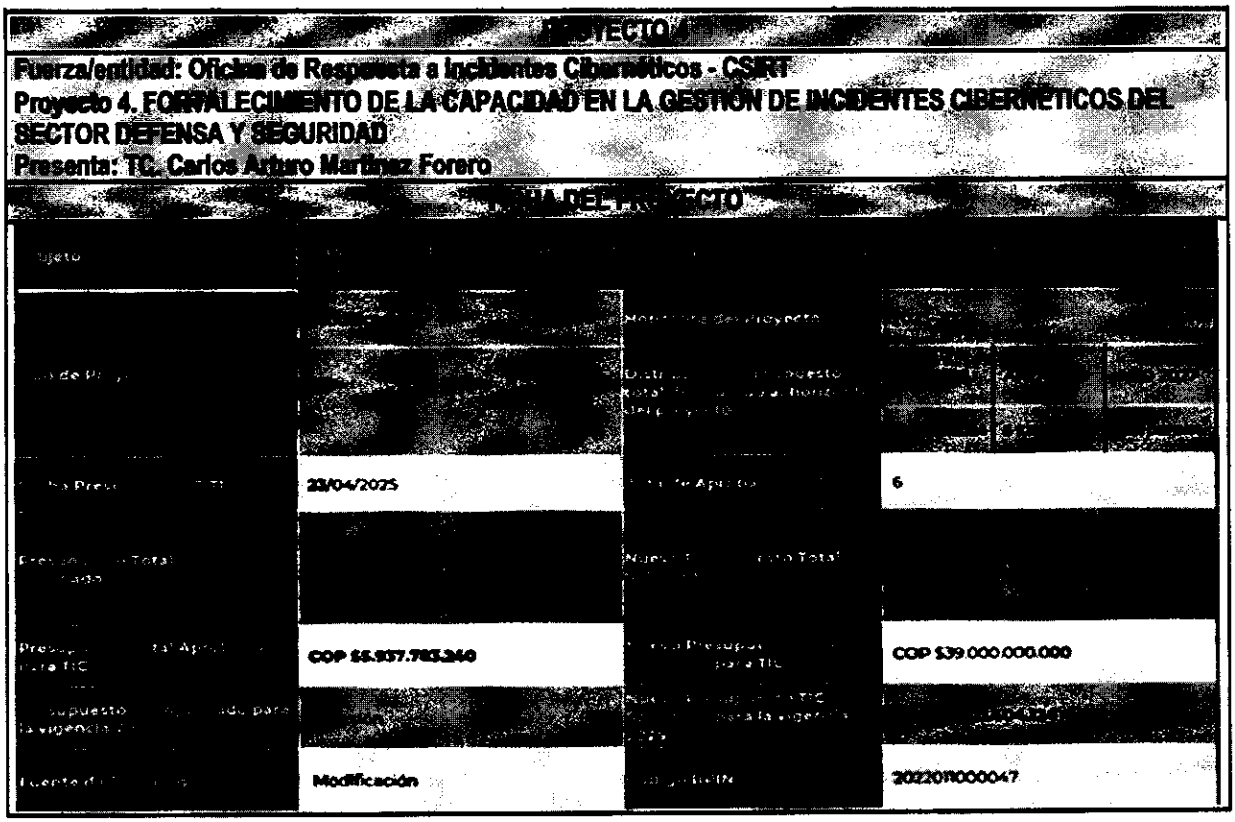
Defensa	FORMATO	Página 1 de 13
		Código: DP-F-011
	ACTA REUNION DE TRABAJO	Versión: 6
		Vigente a partir de: 27 de junio de 2024

Firmado digitalmente

Acta No.	A20250808000273				
Tema	14 Sesión Extraordinaria Comité de Integración de TIC del Sector Defensa				
Fecha	05 agosto de 2025	Hora inicial	10:00 horas	Hora final	12:00 horas
Lugar	Sesión Virtual – Microsoft Teams				

Participantes	
Ingeniero Mauricio Andrés Téllez Garcés	Director de Tecnologías de la Información y las Comunicaciones –TICS MDN - Presidente del Comité
CR. Rafael Enrique Niño Zea	Jefe Departamento Conjunto de Comunicaciones - CGDJ6 - CGFM
CR. Nelson Alexander Tapia Flórez	Comandante del Comando Conjunto Cibernético CCOCI
CR. Mery Cecilia Meléndez Quintero	Jefe Tecnologías Información y Comunicaciones- FAC
CF. Jose Francisco Avila Ruiz	Delegado Director Tecnologías de Información y Comunicaciones – ARC
MY. Héctor Adolfo Blanco Castro	Delegado Jefe Departamento de Comunicaciones CEDE6 – EJC
TC. Carlos Arturo Martinez Forero	Delegado Jefe (e) Oficina de Respuesta a Incidentes Cibernéticos – CSIRT MDN
TC. Andrés Felipe Campos Villamil	Delegado Jefe Oficina de Telemática - PONAL
IJ. Luis Alberto Pacheco Yépez	Delegado Directora (e) Contratación Estatal - MDN
ST. Bayron Blanquicet	Delegado Directora de Planeación y Presupuesto – MDN
Lyda Baron Bareño	Coordinadora Grupo Gobierno Digital - MDN - Secretario técnico Comité
SV. Leydi Viviana Martinez Ramirez	Grupo Gobierno Digital - MDN
SI. Carlos Velasquez	Grupo Gobierno Digital - MDN
Invitados	
N/A	N/A
Ausencias	
BG. Rafael Hernando Jiménez Jiménez	Jefe Departamento de Comunicaciones CEDE6 – EJC - Delegó
CN. Wilbhart Alejandro Castro Celis	Director Tecnologías de Información y Comunicaciones – ARC - Delegó
TC. Luz Esperanza Correa Cruz	Jefe (e) Oficina de Respuesta a Incidentes Cibernéticos – CSIRT MDN - Delegó

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



3. OBJETO A CONTRATAR

DISEÑAR UN PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) QUE GARANTICE LA CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA NACIONAL.

3.1. ALCANCE DEL OBJETO:

El presente servicio tiene por objeto **diseñar un Plan de Recuperación ante Desastres (Disaster Recovery Plan – DRP)** para la **Unidad de Gestión General del Ministerio de Defensa Nacional**, con el fin de garantizar la continuidad operativa de los servicios de Tecnologías de la Información y las Comunicaciones (TIC) frente a eventos disruptivos que puedan afectar la infraestructura tecnológica, los sistemas de información o los servicios críticos asociados.

El alcance del servicio incluye, pero no se limita a:

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

1. **Diagnóstico y levantamiento de información** sobre la infraestructura tecnológica actual, aplicaciones críticas, procesos de negocio soportados por TIC, y riesgos asociados a desastres naturales, fallas técnicas, ciberataques u otras contingencias.
2. **Identificación y clasificación de activos de TI críticos**, líneas de comunicación, dependencias funcionales y puntos únicos de falla, con enfoque en la misión institucional de la Unidad de Gestión General.
3. **Análisis de impacto en el negocio (Business Impact Analysis – BIA)** y evaluación de riesgos (Risk Assessment) para definir los niveles de criticidad de los servicios, así como los tiempos máximos tolerables de interrupción (RTO) y los puntos de recuperación de datos (RPO).
4. **Diseño integral del Plan de Recuperación ante Desastres (DRP)**, que incluya estrategias de respaldo, recuperación y continuidad de servicios, definición de roles y responsabilidades, procedimientos técnicos y administrativos, plan de comunicaciones y matrices de decisiones.
5. **Definición de pruebas de validación del DRP**, incluyendo recomendaciones para la ejecución periódica de simulacros, ajustes posteriores y mejora continua del plan.
6. **Entrega de documentos formales**, incluyendo el DRP completo, anexos técnicos, formatos de control y manuales operativos que faciliten su implementación por parte del personal responsable.
7. **Realización de pruebas** con el equipo técnico designado por la Unidad de Gestión General, con el objetivo de asegurar la apropiación del plan y su capacidad de ejecución ante una contingencia real.

El diseño del DRP deberá cumplir con estándares internacionales de continuidad de negocio y recuperación ante desastres, tales como **ISO 22301**, **ISO/IEC 27031**, **NIST SP 800-34**, entre otros, así como observar el marco normativo y de seguridad de la información aplicable al sector defensa en Colombia.

4. VALOR ESTIMADO DEL CONTRATO Y LA JUSTIFICACIÓN DEL MISMO.

El valor estimado para el presente proceso es hasta por la suma de **TRESCIENTOS CINCUENTA Y CINCO MILLONES SESENTA Y SEIS MIL SEISCIENTOS SESENTA Y SEIS PESOS CON SESENTA Y SIETE CENTAVOS ($355.066.666,67),** incluido Iva y demás impuestos, tasas, retenciones, contribuciones, costos directos, e indirectos a que hubiere lugar.

El presupuesto se encuentra respaldado por el Certificado de Disponibilidad Presupuestal No 44325 del 13 de agosto de 2025

La justificación del valor del contrato y el procedimiento para establecer el presupuesto oficial del proceso de selección se encuentra descrito en el documento denominado: "ANÁLISIS DEL SECTOR Y ESTUDIOS DE MERCADO - PROCESOS DE SELECCIÓN".

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

numeral 6.1.3. CONCLUSIÓN ANÁLISIS DEL VALOR ESTIMADO DEL CONTRATO

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 (Cuando Aplique)

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 vigentes y se evidenció que **NO** existe alguno que pueda estar relacionado directamente con los bienes objeto del presente proceso

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:

A continuación, se describen los requerimientos o necesidades, que hace parte integral del alcance del presente proceso, y que son de obligatorio cumplimiento, de acuerdo con las prioridades de la Oficina de Respuesta a Incidentes Cibernéticos CSIRT; el contratista debe desarrollar en su totalidad dentro del marco del objeto contractual.	
DISEÑAR UN PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) QUE GARANTICE LA CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA NACIONAL.	
1. ASPECTOS GENERALES	
1.1	A continuación, se describen los aspectos generales que el contratista debe cumplir en desarrollo de las actividades tendientes a realizar: 1. El objetivo del proceso es desarrollar, formular o actualizar e implementar un Plan tecnológico de Recuperación ante Desastres (DRP) robusto y eficiente que garantice la continuidad de las operaciones críticas tecnológicas de la UGG que administra la DTICS, para minimizar el impacto de posibles interrupciones por desastres tecnológicos y apuntar a la construcción de una resiliencia cibernética constituida para el sector. 2. Se deberá tener un grupo especializado descrito en el numeral 3.11 requerido para la Entidad y desarrollar el contenido de la

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

	especificación técnica, con el liderazgo de un equipo transversal o Gerente del proyecto. 3. El desarrollo del DRP deberá estar fundamentado en los lineamientos sectoriales de continuidad de negocio existentes dentro del sector de Defensa del Estado colombiano, alineándolos con las políticas sectoriales y definiciones de MinTIC. 4. Crear un cronograma detallado de las actividades del proyecto, incluyendo la secuencia, la duración estimada, las dependencias y los hitos. Identificando y asignando los roles y responsabilidades a los miembros del equipo, cronograma que deberá entregarse al supervisor del contrato dentro de los cinco (05) días hábiles siguientes al perfeccionamiento de este. 5. Durante la realización del proyecto, el contratista deberá mantener todos los aspectos de seguridad de los equipos, sistemas, activos informáticos, siempre que haya modificaciones y/o actualizaciones que puedan afectar la configuración existente, siendo este aspecto responsabilidad del contratista por los cambios realizados. 6. El contratista deberá alinearse a las políticas de seguridad de las Entidades, así como el modelo MSPI del Ministerio de las Telecomunicaciones de Colombia – MinTIC. 7. Obtener con la oportunidad debida, las licencias, autorizaciones y permisos a que hubiere lugar para el cumplimiento de todas las obligaciones que le corresponden en los términos del presente contrato. 8. Mantener durante el plazo de ejecución del contrato los precios ofertados. 9. El contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato. 10. El contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de este contrato. 11. Si el oferente llegase a ajustar o a realizar algún cambio sobre la plataforma tecnológica de la UGG deberá mantener todos los aspectos de seguridad de los equipos siempre que haya modificaciones y/o actualizaciones que puedan afectar la configuración existente, siendo este aspecto responsabilidad del oferente, por los cambios realizados.
2.	Fases y desarrollo del DRP

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

2.1	**LEVANTAMIENTO DE INFORMACIÓN** Recopilar, analizar y organizar toda la información necesaria sobre procesos, sistemas, activos y dependencias tecnológicas de la entidad (UGG), como base para la construcción del DRP, en donde se realizará las siguientes actividades: 1. Identificar a todas las personas, grupos de interés que participaran directa o indirectamente en la construcción del DRP con el conocimiento del negocio. 2. Definir los resultados y beneficios que se esperan obtener con la implementación del DRP (por ejemplo, reducción del tiempo de inactividad, minimización de la pérdida de datos, mejora de la resiliencia operativa). 3. Alinear los objetivos del proyecto con las metas y prioridades estratégicas de las entidades del sector defensa definidas en este proceso. 4. Definir estrategias para gestionar las relaciones con las diferentes partes interesadas. 5. Definir plan de proyecto para la gestión del alcance, el tiempo, costos, la calidad, los recursos humanos, las comunicaciones y los riesgos entre otros. 6. Identificar y clasificar según su criticidad a todos los procesos esenciales del negocio, la dependencia e interconexión vitales para la operación. 7. Identificar los recursos de TI necesarios para cada proceso crítico según la misionalidad de la Unidad de Gestión General del Ministerio de Defensa Nacional 8. Definir metodología de recopilación de datos que será empleada para la ejecución del objeto contractual (entrevistas, cuestionarios, análisis documental, sesiones de trabajo). 9. Registrar servicios o recursos contratados a terceros (proveedores de nube, telecomunicaciones, etc.). 10. Generar el Inventario y clasificar los activos de TI críticos y que serán parte del plan DRP: • **Hardware** (servidores, estaciones, dispositivos de red, etc.). • **Software** (sistemas operativos, aplicaciones críticas, bases de datos). • **Redes** (topología, enlaces, proveedores). • **Datos** (bases de datos, volúmenes de datos, clasificaciones) Y de más activos que puedan ser clasificados como críticos para el Ministerio de Defensa Nacional. 11. Analizar el contexto organizacional y el análisis de los factores internos y externos que pueden influir en la continuidad del negocio.

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

	12. Analizar el liderazgo y compromiso para obtener el apoyo de la alta dirección del área encargada del DRP para garantizar la asignación de recursos y la alineación con los objetivos organizacionales. 13. Realizar el análisis de la arquitectura tecnológica y de seguridad actual (hardware, software, redes, etc.) de las tecnologías de la Información y comunicaciones. Entregables: Los documentos entregables deberán estar en formato digital en original y copia editable. - Matriz de procesos y activos críticos. - Mapa preliminar de dependencias tecnológicas. - Informe de hallazgos y brechas identificadas.
2.2	**ANÁLISIS DEL NEGOCIO (BIA)** Realizar un Análisis de Impacto al Negocio (BIA) para identificar procesos críticos, tiempos de recuperación requeridos y posibles consecuencias de la interrupción de servicios TIC en la operación de la UGG que contenga las siguientes actividades: 1. La definición del Alcance del BIA, la cual debe contemplar la Identificación de procesos, servicios y áreas que serán evaluados 2. Alinear el alcance con los objetivos estratégicos de la entidad y la misión de la UGG. 3. Elaborar cuestionarios, plantillas y guías de entrevistas para recopilar información clave y socializarlo con el supervisor del contrato mínimo tres (3) días hábiles antes de su aplicación. 4. Realizar sesiones de entrevistas con líderes de procesos, áreas críticas y responsables de TI. 5. Aplicar cuestionarios para documentar: • Procesos críticos y dependencias. • Recursos necesarios (personas, infraestructura, tecnología, proveedores). • Impactos ante la interrupción (operativo, financiero, legal, reputacional). • Tiempos máximos de tolerancia a la interrupción. 6. Priorizar los procesos según su criticidad para la entidad e identificar relaciones de dependencia entre procesos y servicios TIC. 7. Determinar, por cada proceso y sistema crítico: • **RTO** (Recovery Time Objective): Tiempo máximo tolerado para reanudar la operación. • **RPO** (Recovery Point Objective): Cantidad máxima de datos que se pueden perder.

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

	• **WRT** (Work Recovery Time): Tiempo adicional para restaurar la funcionalidad tras la recuperación técnica. • **MTD** (Maximum Tolerable Downtime): Tiempo máximo total de interrupción aceptable para el negocio. 8. Evaluar y cuantificar: • Impacto financiero (pérdidas económicas, multas, contratos afectados). • Impacto operativo (interrupción de servicios, tiempos de espera, afectación a usuarios). • Impacto legal y regulatorio (incumplimientos normativos, sanciones). • Impacto reputacional (imagen, confianza de los usuarios). 9. Crear tablas consolidadas que muestren: • Procesos críticos, prioridades, dependencias. • RTO, RPO, MTD, WRT por cada proceso/sistema. • Clasificación de impactos (alto, medio, bajo). 10. Redactar el informe completo con: • Metodología utilizada. • Resultados por proceso. • Recomendaciones. • Incluir anexos: cuestionarios aplicados, matrices de resultados y gráficos. Entregables: - Informe de Análisis de Impacto al Negocio (BIA). - Matriz de procesos críticos y tiempos de recuperación (RTO, RPO, MTD, WRT). - Matriz de impactos clasificados.
2.3	**ANÁLISIS DE RIESGOS TI** Identificar, analizar y evaluar los riesgos que puedan afectar la continuidad de los servicios tecnológicos y los procesos críticos de la Unidad de Gestión General del Ministerio de Defensa Nacional, estableciendo las bases para definir estrategias de mitigación y recuperación. 1. Definición del Alcance y Metodología del Análisis de Riesgos 2. Establecer el marco de análisis (procesos TIC críticos, sistemas, infraestructura, personal, proveedores). 3. Definir la metodología a utilizar (ej. ISO 27005, ISO 31000, NIST SP 800-30, MAGERIT). 4. Acordar escalas de impacto y probabilidad (bajo, medio, alto) con el supervisor del contrato.

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

5. Revisar los activos TIC identificados en el inventario (hardware, software, datos, redes, servicios) validando su importancia para la continuidad del negocio y clasificar los activos según su criticidad
6. Determinar las amenazas que pueden afectar la continuidad, como:
   - Amenazas naturales (inundaciones, incendios, terremotos).
   - Fallos tecnológicos (caídas de servidores, pérdida de datos, errores de configuración).
   - Ciberamenazas (ataques DDoS, ransomware, accesos no autorizados, etc).
   - Errores humanos.
   - Factores externos (fallo de servicios de terceros, proveedores críticos).
   - Identificar vulnerabilidades existentes (brechas de seguridad, falta de redundancia, errores de configuración, etc).
7. Calcular el nivel de riesgo de cada combinación amenaza–vulnerabilidad–activo.
8. Clasificar riesgos según matriz de criticidad (alto, medio, bajo).
9. Análisis de Brechas (Gap Analysis) comparando el estado actual frente a estándares y mejores prácticas (ISO 22301, ISO 27001, MSPI-MinTIC, NIST), Identificando diferencias, deficiencias o carencias en los controles implementados.
10. Establecer el nivel de riesgo que persiste después de aplicar los controles existentes e identificar riesgos inaceptables que requieren mitigación adicional.
11. Definir qué riesgos deben abordarse prioritariamente en el DRP y establecer planes de tratamiento para mitigarlos.
12. Elaborar una matriz de riesgos en donde se consolide la información que incluya:
    - Activo afectado
    - Amenaza/vulnerabilidad.
    - Nivel de riesgo.
    - Controles existentes.
    - Controles adicionales recomendados.
13. Redactar el informe completo de análisis de riesgos:
    - Metodología utilizada.
    - Matriz de riesgos.
    - Recomendaciones.
    - Brechas encontradas

Entregables:

- Matriz de riesgos tecnológicos (amenazas, vulnerabilidades, activos afectados, nivel de riesgo, controles).
- Informe de análisis de riesgos y brechas.

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

	- Hoja de ruta preliminar para mitigación de riesgos. - Documentación de metodología aplicada y anexos.
2.4	**ESTRATEGIAS DE RECUPERACIÓN** Definir las estrategias más adecuadas y viables para restablecer los servicios TIC críticos de la Unidad de Gestión General del Ministerio de Defensa Nacional en caso de una interrupción, alineadas con la criticidad de los procesos y los requerimientos de recuperación establecidos en el BIA que contenga los siguientes puntos: 1. Analizar resultados del BIA (procesos críticos, RTO, RPO, MTD, WRT). 2. Revisar la matriz de riesgos TI y vulnerabilidades identificadas. 3. Validar información sobre capacidades actuales y limitaciones de la infraestructura. 4. Definir opciones técnicas y logísticas para la recuperación de los servicios TIC, tales como: • Recuperación en sitio alterno (activo, pasivo, cálido o frío). • Recuperación en la nube (IaaS, PaaS, SaaS). • Alta disponibilidad y soluciones de tolerancia a fallos. • Backups y esquemas de respaldo/restore. • Procesos manuales de respaldo temporal (cuando aplique). 5. Evaluar la capacidad actual de la entidad para soportar las estrategias propuestas. 6. Identificar necesidades adicionales: hardware, software, redes, servicios de terceros. 7. Estimar los costos asociados a cada opción de recuperación junto con la identificación de recursos humanos, tecnológicos y logísticos requeridos. 8. Asignar estrategias específicas a cada sistema, servicio o proceso clave. 9. Ordenar las estrategias según criticidad y tiempos de recuperación definidos. 10. Incorporar ajustes según retroalimentación técnica. 11. Redactar el Documento de Estrategias de Recuperación que incluya: • Alternativas evaluadas. • Estrategias seleccionadas y su justificación. • Costos estimados y recursos requeridos. • Cronograma de implementación preliminar. Entregables: - Documento de Estrategias de Recuperación (por sistema crítico). - Matriz de alternativas evaluadas con análisis costo-beneficio.

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

	- Hoja de ruta preliminar para la implementación. - Acta de validación de estrategias por la entidad.
2.5	**DESARROLLO DEL PLAN DE COMUNICACIÓN DE CRISIS (PCC)** Diseñar e implementar un Plan de Comunicación de Crisis (PCC) que establezca los protocolos, roles, canales, mensajes y tiempos para informar oportunamente a las partes interesadas internas y externas durante una contingencia que afecte los servicios TIC. El cual se realizarán las siguientes actividades: 1. Determinar qué tipos de incidentes o desastres activarán el PCC. 2. Identificar los procesos y sistemas críticos cuya interrupción requiere comunicación inmediata. 3. Elaborar una matriz de interesados: • Internos (directivos, colaboradores, equipos técnicos, usuarios finales). • Externos (proveedores, clientes, entidades reguladoras, medios de comunicación, terceros críticos). 4. Crear directorio actualizado de contactos de emergencia. 5. Asignar responsables para: • Vocería oficial. • Redacción de mensajes. • Canales digitales (correo, página web, redes sociales). • Contacto directo con autoridades y medios. 6. Establecer métodos de comunicación redundantes para garantizar el acceso en situaciones de emergencia 7. Identificar y validar los canales formales y alternativos, por ejemplo: • Correo institucional. • Mensajes de texto/SMS. • Llamadas telefónicas directas. • Plataforma de mensajería (WhatsApp, Teams, etc.). • Publicación en intranet o sitio web 8. Asegurar que el Plan de Comunicación de Crisis esté alineado e integrado con: • DRP (Plan de Recuperación ante Desastres). • Plan de Continuidad del Negocio (BCP). • Plan de Gestión de Incidentes. 9. Establecer cuándo y cómo se debe informar durante: • Detección de la crisis. • Activación del DRP. • Progreso de recuperación. • Finalización y retorno a la normalidad 10. Diagramar el proceso de comunicación:

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

	• ¿Quién informa a quién? • ¿Con qué frecuencia? • ¿Por qué canal? 11. Definir tiempos de respuesta y niveles de aprobación. 12. Redactar el documento final incluyendo: • Objetivos y alcance. • Roles y responsabilidades. • Canales y protocolos. • Plantillas de mensajes. • Flujos de comunicación. • Directorio de contactos clave. Entregables: - Documento del Plan de Comunicación de Crisis. - Matriz de partes interesadas (Stakeholders). - Directorio de contactos de emergencia. - Flujogramas de comunicación. - Plantillas de mensajes tipo. - Revisión y validación del PCC por la entidad.
2.6	Desarrollo del DRP Elaborar, documentar y estructurar el Plan de Recuperación ante Desastres (DRP) de la Unidad de Gestión General del Ministerio de Defensa, con procedimientos claros, roles definidos y recursos asignados para garantizar la recuperación oportuna de los servicios TIC críticos y que contenga lo siguiente: 1. Establecer el índice y los capítulos del documento final (alineado a estándares como ISO 22301, NIST SP 800-34, DRI). 2. Redactar la política de recuperación ante desastres definiendo los objetivos generales y específicos del DRP, alineados al BIA y análisis de riesgos. 3. Redactar procedimientos paso a paso para la recuperación de cada sistema, servicio o proceso crítico incluyendo instrucciones claras sobre: • Activación del DRP. • Comunicación inicial de la crisis. • Recuperación técnica de cada servicio (servidores, aplicaciones, redes, bases de datos, etc.). • Validación y verificación de la restauración. • Retorno a la normalidad. • Documentar los flujos de actividades y diagramas de procesos

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

4. Establecer el Comité de Recuperación ante Desastres y los equipos de respuesta (líderes, técnicos, comunicaciones, logística), junto con la definición de funciones específicas de cada rol.
5. Identificar los recursos tecnológicos, humanos y logísticos requeridos para activar el DRP, estableciendo la disponibilidad y ubicación de recursos críticos (servidores, respaldos, enlaces alternos, etc.).
6. Definir la arquitectura de seguridad para operativizar el DRP.
7. Definir protocolos de comunicación internos y externos durante una contingencia, estableciendo canales de comunicación alternativos.
8. Incluir protocolos de gestión de incidentes, gestión de cambios y continuidad de servicios.
9. Incorporar políticas de seguridad de la información y sanitización de datos post-evento.
10. Diseñar formularios y registros necesarios para la ejecución del DRP:
    - Registro de incidentes.
    - Listas de verificación (checklists) para la recuperación.
    - Formatos de seguimiento y control.
11. Validar internamente el contenido del DRP junto con el supervisor del contrato y realizar ajustes según revisiones técnicas y de estilo.
12. Entregar borrador para revisión por parte de la UGG
13. Consolidar el documento definitivo:

- En formato digital (Word, PDF, editable).
- Se deberá entregar un libro con capítulos de cada tema requerido en la ficha técnica, con un mínimo de 120 páginas, la medida del libro es de 17,5 x 25, libros en tapa dura, impresa en cote de 150 gr. plastificada en brillantes a 4x4 tintas, en bond de 90gra a 4x4 tintas. Páginas, letra Arial 10, de contenido de acuerdo con la concertación de la estructuración entre el consultor y las Entidades corregido y ajustado, diagramado e impreso, en forma física y digital en una USB, con la corrección de estilo para que este pueda ser editado en caso de ser necesario, referente a los temas de estudio relacionado en esta especificación técnica
- Asegurar cumplimiento de normas APA y requisitos editoriales (diseño, diagramación, estilo).

Entregables:

- Documento completo del DRP, estructurado, revisado y aprobado
- Procedimientos de recuperación detallados por sistema crítico
- Matriz de roles y responsabilidades.
- Plan de comunicación de crisis.
- Formatos, anexos y flujogramas de recuperación.
- Borrador revisado por la entidad y versión final validada.

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

2.7	**VALIDACIÓN Y PRUEBAS DEL DRP** Verificar que el DRP sea funcional, completo y efectivo para garantizar la continuidad operativa ante una interrupción, mediante simulaciones controladas y pruebas estructuradas, asegurando que los equipos sepan cómo actuar y que los procedimientos sean adecuados, para lo cual se deberá realizar las siguientes actividades: 1. Definir el tipo de pruebas a realizar: • Pruebas de escritorio (TableTop). • Pruebas técnicas unitarias (por sistema crítico). • Simulacros integrados (opcional según madurez). 2. Establecer objetivos de cada prueba (ej. validar tiempos de respuesta, comunicación, ejecución de pasos técnicos). 3. Seleccionar participantes clave como líderes de recuperación, responsables de TI, personal de comunicaciones, seguridad y apoyo operativo. 4. Asignar roles para ejecución, observación y evaluación. 5. Diseñar escenarios realistas y alineados a riesgos identificados (ej. falla de servidor de base de datos, ciberataque, corte de energía en CPD). 6. Crear documentos guía para los participantes: • Instrucciones detalladas de prueba. • Formatos de observaciones. • Plantillas para evaluación de desempeño. 7. Definir métricas de éxito: cumplimiento de RTO/RPO, activación efectiva del plan, errores detectados, tiempos de reacción 8. Realizar la prueba TableTop: • Simulación teórica en sala de crisis • Evaluación del tiempo de reacción, coordinación, toma de decisiones 9. Ejecutar pruebas unitarias de recuperación en donde se tenga en cuenta simulación técnica por sistema crítico (restauración de respaldos, recuperación de base de datos, failover de servidores, etc.). 10. Comparar resultados frente a los objetivos definidos. 11. Identificar deficiencias, retrasos, fallas técnicas o errores en la ejecución. 12. Consolidar toda la información en un informe: • Descripción del escenario y participantes. • Resultados observados por sistema/proceso. • Brechas identificadas. • Recomendaciones de mejora.

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

	Entregables: - Plan de pruebas documentado (tipos, cronograma, escenarios, objetivos). - Escenarios de simulación y guías para participantes - Registro de resultados y formatos de observación. - Informe de validación del DRP (con hallazgos, recomendaciones, mejoras). - Versión final del DRP ajustado. - Acta de validación aprobada por la Unidad de Gestión General del Ministerio de Defensa Nacional
3	**CONDICIONES PARA EL PERSONAL QUE DESARROLLARÁ EL OBJETO CONTRACTUAL POR PARTE DEL CONTRATISTA**
3.1	El contratista deberá garantizar la continuidad del desarrollo o ejecución de cada una de las actividades objeto del contrato, para lo cual, de ser necesario debe prever el reemplazo del personal que se encuentra adelantando las actividades cuando así se requiera, por uno igual o de superior experiencia, entregando la hoja de vida de la persona reemplazante al supervisor del contrato dentro de los (3) días hábiles previos a la materialización del reemplazo, lo anterior para la validación y aprobación del perfil y la experiencia técnica de los ingenieros que fueron requeridos.
3.2	El contratista debe desarrollar las actividades objeto del contrato en horario laboral y en días y horas no hábiles o en fines de semana o días festivos, tanto en horario diurno como nocturno, es decir 7x24.
3.3	Al personal asignado para el desarrollo del proyecto por parte del contratista, se le realizará un estudio de seguridad para lo cual se debe aportar la siguiente documentación en un término no mayor a quince (15) días calendarios a partir de la aprobación de la garantía de cumplimiento: a. Copia cédula de ciudadanía b. Copia libreta militar (para quien aplique) c. Referencias laborales. Una carta de referencia laboral relacionada con el cargo a desempeñar. d. Copia de los diplomas de estudios acreditados – Actas de Grado e. Copia de la tarjeta profesional. f. Antecedentes judiciales (vigencia no mayor a treinta (30) días. g. Antecedentes disciplinarios procuraduría (vigencia no mayor a treinta (30) días. h. Boletín de responsabilidades fiscales contraloría (vigencia no mayor a treinta (30) días. i. Referencias personales. Dos cartas con referencias personales

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

	j. Diligenciamiento del formato Estudio de Seguridad Personal MDN, el cual será aportado al contratista al momento de aprobación de la garantía.
3.4	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 de gestión técnica, 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.
3.5	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.
3.6	El contratista asumirá todos los costos o gastos asociados al desplazamiento de su personal a los sitios de trabajo del Ministerio de Defensa Nacional.
3.7	El contratista debe garantizar que el personal que realice las actividades en desarrollo del objeto contractual sea especializado en cada uno de los productos o sistemas o herramientas descritas en el presente documento.
3.8	Todo el personal requerido para la ejecución del contrato debe tener disponibilidad de tiempo para la atención y solución de los requerimientos en el marco del objeto contractual, efectuados por parte de la Dirección de Tecnologías de la Información y las Comunicaciones, en el momento que se le requiera. Será de la autonomía y responsabilidad del contratista la vinculación, organización, orientación y control del personal a su cargo, comprometiéndose a cumplir con las normas de seguridad existentes en el Ministerio de Defensa Nacional. Cabe anotar que la Unidad de Gestión General del Ministerio de Defensa Nacional no adquiere ninguna relación contractual, civil o laboral con los trabajadores del contratista.
3.9	La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto dentro de los (3) días hábiles siguientes a la solicitud, Esta exigencia no dará derecho al contratista para elevar ningún reclamo contra la Entidad contratante.
3.10	La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que el supervisor haya fijado.

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

3.11	**CONDICIONES DE EXPERIENCIA DEL PERSONAL ASIGNADO AL CONTRATO** **Gerente de proyectos:** El profesional requerido deberá liderar y coordinar la identificación, planificación, implementación, y la ejecución de estrategias de recuperación ante desastres que puedan vulnerar la infraestructura tecnológica de la Entidad, garantizando la continuidad operativa de la UGG. **Perfil Profesional:** Ingeniero de sistemas o afines Posgrado en la modalidad de Maestría en Gerencia de Proyectos **Experiencia Mínima** Experiencia Profesional no menor a diez (10) años a partir de la expedición de la tarjeta profesional. Experiencia específica como gerente de proyectos en al menos un (1) proyecto de tecnología que corresponda a proyectos de arquitectura de seguridad. **Arquitecto de seguridad** El profesional requerido deberá identificar y/o diseñar/implementar la arquitectura de seguridad de la Entidad que garantice la protección integral de la operación frente a amenazas internas o externas en cumplimiento de las normas estatales e institucionales, mediante la definición de controles de seguridad, evaluación de vulnerabilidades, cumplimiento normativo, y la validación técnica de simulacros. **Perfil Profesional:** Ingeniero de sistemas o afines según el NBC de *Ingeniería de Sistemas, Telemática y Afines*. Posgrado en la modalidad de especialización o maestría en Seguridad de la Información **Experiencia mínima** Experiencia profesional no menor a diez (10) años a partir de la expedición de la tarjeta profesional. Experiencia específica como arquitecto de seguridad en por lo menos un (1) proyectos relacionados con las tecnologías de la información. **Consultor Senior BCP/DRP**

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

El profesional requerido deberá diseñar y/o implementar y/o mejorar el Sistema de Gestión de continuidad del negocio y recuperación ante desastres (BCP/DRP), asegurando la operatividad de la tecnología en el cumplimiento de la misión de la Entidad.

Perfil Profesional:
Ingeniero de sistemas o ingeniero industrial, ingeniero administrativo, seguridad informática o áreas afines
Conocimiento en regulaciones locales como Ley 1581/2012, Decreto 1078/2015 y/o políticas de gobierno digital.

Experiencia:
Experiencia profesional mínima de diez (10) años a partir de la expedición de la tarjeta profesional.
Experiencia específica como especialista en seguridad de la información y/o continuidad del negocio en al menos un (1) proyecto relacionado con planes de continuidad (BCP) o recuperación ante desastres (DRP).

Consultor gestión del cambio

Deberá garantizar y facilitar la adopción efectiva de los cambios o estructuras implementadas en la operación de la UGG

Perfil Profesional:
Profesional en Comunicación Social o Corporativa.

Experiencia Mínima
Experiencia profesional mínimo de diez años (10) a partir de la obtención del título profesional, de los cuales al menos seis (6) años deben estar relacionados con formulación e implementación de proyectos de gestión del cambio y cultura organizacional preferiblemente en entornos de tecnología, habiendo participado como profesional, consultor, líder o asesor en dichos proyectos; incluyendo al menos un (1) proyecto relacionado con arquitectura de seguridad en el rol de experto en gestión del cambio, o transformación digital o modernización administrativa o rediseño institucional.

Mecanismo de acreditación:

Título profesional expedido por una universidad reconocida en Colombia o en el exterior (si es extranjero, debe estar convalidado por el Ministerio de Educación Nacional).

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

Tarjeta profesional o matrícula (si aplica, ej. ingenieros de sistemas, industriales, administrativos) expedida por el Consejo Profesional Nacional de Ingeniería (COPNIA) u otra entidad competente.

Acta de grado puede admitirse cuando el título aún no ha sido expedido.

Documento requerido:

Copia del diploma y/o acta de grado.

Copia de la matrícula profesional (si es exigida por la ley para la disciplina).

Requisito: Ley 1581 de 2012 (protección de datos personales), Decreto 1078 de 2015 (sector TIC) y/o políticas de gobierno digital.

Mecanismo de acreditación:

Certificados de educación:

Cursos, diplomados o especializaciones en protección de datos, seguridad informática, gobierno digital, gestión TIC, etc.

Deben estar expedidos por universidades, entidades acreditadas (ICONTEC, ESAP, MinTIC, SENA, etc.) o plataformas reconocidas con validez oficial.

Experiencia laboral certificada:

Certificados laborales donde se especifique el cargo, funciones y periodo trabajado, indicando que el profesional desempeñó tareas relacionadas con la aplicación de la Ley 1581/2012, el Decreto 1078/2015 o las políticas de gobierno digital.

Producción académica o técnica (opcional, si el pliego lo admite):

Publicaciones, consultorías o informes en los que el candidato haya trabajado directamente sobre dichas regulaciones.

CO-SC6710-1

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

	Documentos requeridos: Certificados de cursos o diplomados con intensidad horaria. Certificados laborales con funciones explícitas relacionadas con protección de datos o gobierno digital. En caso de publicaciones, constancias de la institución o copia del documento Para acreditar la idoneidad del personal aportado, se deben anexar los siguientes requisitos dentro de los cinco (5) días hábiles posteriores a la suscripción del acta de inicio: • La hoja de vida del personal propuesto • Fotocopias de los diplomas o actas de grado, • Soporte de la experiencia • Carta de compromiso. **Gerente de proyectos** **Arquitecto de seguridad** **Consultor Senior BCP/DRP** **Consultor gestión del cambio**
3.12	Para acreditar la experiencia del personal, se debe anexar certificación que reúna los siguientes requisitos: • Ser expedidas por el contratante. En caso de ser expedida por una entidad pública o privada, la certificación deberá estar suscrita por el funcionario de la Entidad, competente para emitirla. • Señalar el objeto del contrato, • Indicar fecha de inicio y terminación del contrato, • Indicar el cargo ocupado dentro del contrato, • Indicar nombre, dirección y teléfono del contratante. Las certificaciones que acrediten la experiencia del personal propuesto se considerarán expedidas bajo gravedad de juramento
3.13	Respecto de las certificaciones de experiencia laboral, el oferente debe contemplar para cada una la siguiente información: a. Nombre de la empresa que recibió los servicios y en la cual el experto propuesto prestó sus servicios. b. Nombre del proyecto ejecutado. c. Perfiles o cargos desempeñados.

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

	d. Fechas de inicio y terminación del contrato. e. Actividades ejecutadas. f. Teléfono y correo de contacto.
3.14	Para su evaluación por parte de la supervisión, las certificaciones de experiencia requeridas deben ser entregadas por parte del contratista a más tardar dentro de los ocho (08) días calendario siguiente a la fecha de suscripción del Acta de Inicio al supervisor del contrato o a la persona que este designe para tal fin.
3.15	Para el personal al que se le exige título profesional o título de tecnólogo o título de técnico, la experiencia se computará a partir de la fecha de expedición de la tarjeta o matricula profesional. En consecuencia, para este aspecto el contratista debe suministrar copia de la tarjeta o matricula profesional.
4	**RIESGOS PROFESIONALES**
4.1	El contratista cumplirá todas las normas de seguridad industrial en la prestación del servicio y garantizará los cuidados y precauciones necesarias para el desarrollo de este.
4.2	El contratista deberá entregar al supervisor el certificado del curso virtual de 50 horas sobre seguridad y salud en el trabajo (Art. 2.2.4.6.35 del Decreto 1072 de 2015), el cual deberá permanecer vigente durante el plazo de ejecución del contrato.
5	**CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN INSTITUCIONAL**
5.1	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, que garantizará 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 y la Oficina de Respuesta a Incidentes informáticos CSIRT del MDN ponga a su disposición. Dicho documento deberá suscribirse 5 días posteriores a la firma el acta de inicio.
5.2	De igual manera, Documento del Plan de Recuperación ante Desastres (DRP): Plan completo con los procedimientos, roles y recursos, hoja de ruta y plan de implementación del DRP, Plan de Comunicación de Crisisel diseño, las pruebas y sus resultados, las políticas y los procesos en la actualización de la solución serán considerados por el contratista como información confidencial propiedad del Ministerio de Defensa Nacional – Unidad Gestión

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

	su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida.
5.3	Durante la actualización y asistencia técnica de las soluciones, el contratista se compromete a no hacer uso indebido de las herramientas utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.
5.4	De acuerdo con el Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de las Telecomunicaciones de Colombia – MinTic y la Directiva de seguridad de la información del sector Defensa y en pro de su cumplimiento todos los equipos Laptop y/o equipos de escritorio, así como equipos de conectividad y seguridad utilizados por el personal para el desarrollo de esta especificación técnica, al finalizar se les deberá realizar procedimiento de borrado seguro y/o sanitización de datos para los discos duros que conlleven a la eliminación de la data recopilada y analizada de cada una de las Entidades, el software utilizado para el borrado seguro debe estar debidamente licenciado y no puede ser de código abierto. Además, debe generar un certificado auditable que garantice que el borrado de los datos ha sido irreversible, el cual podrá ser presentado ante auditorías sobre el tratamiento de la información (debe cumplir con las normas nacionales e internacionales aplicables a la eliminación segura de información sensible descritas en las condiciones técnicas exigidas en las licencias de acceso a nube requeridas para las 4 entidades).

7. CRITERIOS Y DOCUMENTOS TÉCNICOS MÍNIMOS HABILITANTES (Cuando Aplique)

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 de selección.

Los bienes y/o servicios que hacen parte del objeto a contratar cuentan con los siguientes códigos en la Clasificación de Bienes y Servicios:

Clasificación UNSPSC

CÓDIGO UNSPSC	SEGMENTO	FAMILIA	CLASE
80101600	**80** Servicios de Gestión, Servicios	**10**	**16** Gerencia de Proyectos

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

	Profesionales de Empresa y Servicios Administrativos	Servicios de asesoría de gestión	
80101500	**80** Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	**10** Servicios de asesoría de gestión	**15** Servicios de consultoría de negocios y administración corporativa
81112000	**81** Servicios basados en ingeniería, investigación y Tecnología	**11** Servicios informáticos	**20** Servicios de Datos
81111900	**81** Servicios basados en ingeniería, investigación y Tecnología	**11** Servicios informáticos	**19** Sistemas de Recuperación de información

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 la presentación por parte del proponente de máximo dos (2) contratos relacionados(s) en el RUP que individualmente esté clasificado en la totalidad de los siguientes códigos UNSPSC:

CÓDIGO UNSPSC	SEGMENTO	FAMILIA	CLASE
80101600	**80** Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	**10** Servicios de asesoría de gestión	**16** Gerencia de Proyectos
80101500	**80** Servicios de Gestión, Servicios	**10**	**15** Servicios de consultoría de

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

	Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	Servicios de asesoría de gestión	Servicios de consultoría de negocios y administración corporativa
81112000 Servicios de Datos	**81** Servicios basados en ingeniería, investigación y Tecnología	**11** Servicios informáticos	**20** Servicios de Datos
81111900	**81** Servicios basados en ingeniería, investigación y Tecnología	**11** Servicios informáticos	**19** Sistemas de Recuperación de información

El proponente acreditará su experiencia bajo las siguientes condiciones:

A. Certificaciones: los contratos deben haber sido ejecutados y terminados en un ciento por ciento (100%) a la fecha de cierre del proceso de contratación.

B. Los contratos a presentar como experiencia debe tener como objeto y/o actividades específicas de diseño y/o implementación y/o diagnóstico y/o análisis de arquitectura de seguridad en entornos TI. Al menos uno (1) de los (2) contratos exigidos en la experiencia habilitante general deberá acreditar experiencia específica en materia de tecnologías emergentes, inteligencia artificial o Política de Gobierno Digital.

C. La sumatoria de los contratos aportados debe ser igual al 100% del valor del presupuesto oficial, equivalente en SLMMLV, de conformidad con el Registro Único de Proponentes – RUP

D. Para efectos de la verificación y evaluación de la experiencia exigida en el presente proceso de selección, únicamente se aceptarán certificaciones que acrediten la ejecución directa de los contratos por parte del proponente.
En consecuencia, no se aceptarán certificaciones derivadas de contratos en los que el proponente haya participado en calidad de subcontratista, ni aquellas en las que no se evidencie de forma clara y verificable que el proponente fue el contratista principal y ejecutó directamente el objeto contractual. Las certificaciones deberán indicar de manera expresa el objeto del contrato, el alcance de las actividades desarrolladas, el porcentaje de ejecución (cuando aplique), la fecha de inicio y finalización, y el cumplimiento a satisfacción.

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

7.2.1. CRITERIOS DIFERENCIALES PARA EMPRENDIMIENTOS Y EMPRESAS DE MUJERES EN EL SISTEMA DE COMPRAS PÚBLICAS (DECRETO 1860 DE 2021).

De conformidad con lo establecido en el Decreto 1082 de 2015, artículos 2.2.1.2.4.2.15 y 2.2.1.2.4.2.18. **Criterios diferenciales para Mipyme en el sistema de compras públicas,** que expresan: *"En los procesos de licitación pública, selección abreviada de menor cuantía y concurso de méritos, así como en los procesos competitivos que adelanten las Entidades Estatales no sometidas al Estatuto General de Contratación de la Administración Pública, las Entidades incluirán condiciones habilitantes para incentivar los emprendimientos y empresas de mujeres con domicilio en el territorio nacional."*, por ello, tratándose de proponentes que acrediten la calidad de MIPYME o EMPRENDIMIENTO Y EMPRESAS DE MUJERES con domicilio en el territorio nacional, podrá acreditar con su propuesta máximo tres (3) certificaciones de contratos ejecutados y terminados, que consten en el RUP, bajo las mismas condiciones de la experiencia habilitante exigida.

NOTA 1: Tratándose de proponente plurales, el criterio diferencial solo se aplicará si por lo menos uno de los integrantes acredita que es emprendimiento y empresa de mujeres, bajo los criterios dispuestos en el artículo 3 del Decreto 1860 de 2021 y tiene una participación igual o superior al diez por ciento 10%.

NOTA 2: Tratándose de proponente plurales, el criterio diferencial solo se aplicará si por lo menos uno de los integrantes acredita la calidad de MYPIME y tiene una participación igual o superior al diez por ciento 10%.

7.2.2. ACREDITACIÓN DE LA EXPERIENCIA:

El proponente acreditará la experiencia requerida para este proceso de selección a través de cualquiera de las siguientes formas: a) mediante el diligenciamiento del Anexo No. 4 "CERTIFICACIONES DE EXPERIENCIA HABILITANTE DEL PROPONENTE" del pliego de condiciones, y con el lleno de los requisitos antes exigidos, o, b) 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 No. 4 , y con el lleno de los requisitos antes exigidos.

7.2.2.1. ACREDITACION DE EXPERIENCIA DEL PROPONENTE A TRAVES DE CONTRATOS SUSCRITOS CON ENTIDADES ESTATALES.

En el caso en que, de la información aportada no sea posible extractar la totalidad de la información requerida, el proponente deberá adjuntar adicionalmente a la certificación, uno o algunos de los documentos que se establecen a continuación en

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

- Acta de Liquidación Debidamente diligenciada y suscrita por todas las partes involucradas, en la cual conste la información requerida, que no se acredite con el certificado del RUP.
- Acta de Entrega o de Recibo Definitivo Debidamente diligenciada y suscrita por todas las partes involucradas, en las cuales conste la información requerida, que no se acredite con el certificado del RUP.
- Acta de Terminación Debidamente diligenciada y suscrita por todas las partes involucradas, en las cuales conste la información requerida, que no se acredite con el certificado del RUP.

7.2.2.2. ACREDITACION DE EXPERIENCIA DEL PROPONENTE A TRAVES DE CONTRATOS SUSCRITOS CON PARTICULARES.

El proponente deberá aportar los documentos que se describen a continuación:

I. Certificado de Existencia y Representación Legal de la persona contratante; la fecha de expedición del certificado debe ser no mayor a treinta (30) días anteriores a la fecha de cierre del presente proceso; en el caso de acreditar Experiencia obtenida en el Extranjero, deberá aportar los documentos que acrediten la existencia y representación legal, legalizados a más tardar dentro de los tres (3) meses anteriores a la fecha de cierre del presente proceso de selección, de conformidad con el presente documento (personas naturales y jurídicas extranjeras sin domicilio o sucursal en Colombia). La certificación aportada debe contener los datos requeridos en el presente documento, que no se acrediten con el certificado del RUP.

II. Igualmente, para que el contrato sea validado para efectos de acreditación de experiencia, además de la certificación, se debe anexar el contrato de la empresa con el cliente que soporta dicha experiencia y facturación de la ejecución del contrato suscrita por revisor fiscal y/o contador con sus respectivos soportes (cédula de ciudadanía, Tarjeta Profesional y antecedentes profesionales vigentes).

NOTA 1: Para efectos de acreditación de experiencia no se aceptarán documentos diferentes a los señalados en numerales que anteceden esta nota. En caso de existir discrepancias entre dos (2) o más de los documentos aportados por el proponente para acreditación de experiencia, se tendrá en cuenta el orden de prevalencia establecido anteriormente, para efectos de la evaluación.

NOTA 2: Las personas que objeten la experiencia de algún otro oferente, deberán aportar los documentos que prueben sus afirmaciones; por lo tanto, no es procedente efectuar manifestaciones temerarias respecto de los documentos aportados por los demás oferentes, sin contar con medios de prueba que acrediten tales manifestaciones. Cabe agregar, que la entidad propende por garantizar el principio constitucional de la buena fe.

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

NOTA 3. Para efectos de acreditación de experiencia entre particulares no se aceptarán documentos diferentes a los señalados en el presente numeral.

NOTA 4: Para efectos de la verificación de la Experiencia del Proponente, se procederá a sumar los SMMLV obtenidos en este aspecto de cada uno de los contratos que se pretenden hacer valer como experiencia registrada en el RUP, debiendo cumplir con los salarios exigidos.

NOTA 5: En caso de que el proponente se presente en Consorcio o Unión temporal para efectos de la verificación de la Experiencia del Proponente, se procederá a sumar los SMMLV de conformidad con el porcentaje de participación de los contratos aportados y registrados en el RUP, cuya sumatoria será un monto igual o superior al presupuesto oficial del presente proceso de contratación.

NOTA 6: La condición de emprendimiento y empresa de mujeres deberá acreditarse aportando la documentación que evidencie el cumplimiento de alguna de las condiciones establecidas en el Decreto 1082 de 2015 y el Decreto 1860 de 2021, así como lo exigido en el Pliego de Condiciones.

NOTA 7: La condición de MIPYME, deberá acreditarse aportando la documentación que evidencie el cumplimiento de alguna de las condiciones establecidas en el Decreto 1082 de 2015 y el Decreto 1860 de 2021, así como lo exigido en el Pliego de Condiciones

7.3. DOCUMENTOS Y VERIFICACIONES TÉCNICOS ADICIONALES (Cuando Aplique)

N/A

8. CRITERIOS TÉCNICOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE.

De conformidad con lo establecido en el numeral 4 del artículo 5 de la Ley 80 de 1993, que expresamente indica:

> *"ARTÍCULO 5o. DE LA SELECCIÓN OBJETIVA. Es objetiva la selección en la cual la escogencia se haga al ofrecimiento más favorable a la entidad y a los fines que ella busca, sin tener en consideración factores de afecto o de interés y, en general, cualquier clase de motivación subjetiva. En consecuencia, los factores de escogencia y calificación que establezcan las entidades en los pliegos de condiciones o sus equivalentes, tendrán en cuenta los siguientes criterios:*
> *(...) 4. 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*

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

conformidad con las condiciones que señale el reglamento, se podrán utilizar criterios de experiencia específica del oferente y del 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."

Se han establecido los criterios técnicos para la selección de la oferta mas favorable para la entidad de acuerdo con los siguientes criterios:

1. VERIFICACIÓN DEL CUMPLIMIENTO DE CRITERIOS DE CALIFICACION

El Comité Evaluador verificará el cumplimiento de los requisitos mínimos exigidos a los proponentes, con el fin de determinar cuáles de las ofertas son HÁBILES o NO HABILES y en tal caso, continuará en el proceso de calificación así.

FACTORES	CUMPLIMIENTO
Capacidad Jurídica	HÁBIL O NO HÁBIL
Capacidad Financiera y Organizacional	HÁBIL O NO HÁBIL
Experiencia	HÁBIL O NO HÁBIL
Capacidad Técnica	HÁBIL O NO HÁBIL

Una vez se determine las propuestas hábiles, se procederá a calificarlas de conformidad con los siguientes criterios de CALIFICACIÓN, sobre un total máximo de 100 puntos:

CRITERIOS DE CALIFICACIÓN	**PUTAJE**
Experiencia Específica Adicional del proponente	30 puntos
Formación académica y experiencia adicional del equipo Mínimo Requerido	58.5 Puntos
Estímulo a la Industria Nacional	10 Puntos
Personal con Discapacidad	1 Punto
Emprendimiento y Empresas de Mujeres	0.25 puntos
Mipymes domiciliadas en Colombia	0.25 puntos
Total	**100 puntos**

8.1. Experiencia específica adicional del proponente (30 puntos)

Este criterio evalúa la experiencia relevante adicional del proponente en proyectos similares al objeto de esta contratación. Se otorgará hasta un máximo de treinta (30) puntos con base en el número de contratos similares adicionales ejecutados por el proponente, más allá del mínimo exigido para habilitación. El puntaje se asignará de forma progresiva según la cantidad de contratos adicionales debidamente certificados, conforme a la siguiente escala:

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

Contratos similares adicionales (por encima del mínimo requerido)	Puntaje otorgado
0 – Cumple con los 2 o 3 contratos mínimos exigidos de acuerdo a la calidad acreditada (sin contratos adicionales)	0 puntos
1 contrato adicional similar ejecutado	10 puntos
2 contratos adicionales similares ejecutados	20 puntos
3 o más contratos adicionales similares ejecutados	30 puntos (puntaje máximo)

Todos los contratos deberán estar debidamente certificados por la entidad contratante, acreditando su correcta ejecución (100% del objeto contractual) en los últimos tres (3) años de acuerdo con los requisitos del pliego.

Solo se computarán para puntaje aquellos contratos que cumplan con las condiciones mínimas de experiencia habilitante; aclarando que, los contratos presentados en cumplimiento del requisito mínimo de experiencia no reciben puntaje, únicamente sirven para habilitación.

El proponente obtendrá el puntaje máximo de este criterio (30 puntos) si acredita tres (3) o más contratos adicionales de naturaleza similar, ejecutados satisfactoriamente.

8.2. FORMACIÓN ACADÉMICA Y EXPERIENCIA ADICIONAL DEL EQUIPO MÍNIMO REQUERIDO (58,5 PUNTOS)

Este criterio evalúa y califica equipo mínimo propuesto, con un puntaje total de 58,5 puntos distribuidos entre los perfiles clave requeridos. Los perfiles considerados y sus puntajes máximos son:

- Gerente de Proyectos – hasta 15 puntos.
- Arquitecto de Seguridad – hasta 15 puntos.
- Consultor Senior BCP/DRP – hasta 15 puntos.
- Consultor de Gestión del Cambio – hasta 13,5 puntos.

Cada perfil se calificará de manera independiente, más allá de los requisitos mínimos exigidos para el cargo. A continuación, se detallan las escalas de puntaje progresivo para la experiencia de cada perfil, basadas en el grado en que el candidato propuesto supera las condiciones mínimas de formación, años de experiencia, proyectos similares y certificaciones pertinentes:

8.2.1. GERENTE DE PROYECTOS (MÁXIMO 15 PUNTOS):

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

Este perfil será evaluado teniendo en cuenta la experiencia mínima habilitante y se otorgará puntaje por certificados relacionados con la gestión de proyectos, metodologías ágiles y arquitectura empresarial así:

Puntaje del Gerente de Proyectos (Puntaje máx. 15 puntos)	
Certificaciones de conocimiento (Puntaje máx. 7 puntos)	
Profesional que presente uno (1) de los siguientes certificados vigente: PMP – Proyect Management Professional o Scrum Master o TOGAF	3 puntos
Profesional que presente dos (2) de los siguientes certificados vigentes: PMP – Proyect Management Professional o Scrum Master o TOGAF	5 puntos
Profesional que presente los tres (3) de los siguientes certificados vigente: PMP – Proyect Management Professional o Scrum Master o TOGAF	7 puntos
Experiencia Específica Adicional (Puntaje máx. 8 puntos)	
Experiencia como gerente de proyectos en dos (2) proyectos de tecnología	4 puntos
Experiencia como gerente de proyectos en tres (3) o más proyectos de tecnología	8 puntos

Acreditación: El proponente deberá anexar con los documentos mínimos requeridos para el cargo de gerente de proyecto, los certificados de conocimiento vigentes y experiencia adicional.

8.2.2. ARQUITECTO DE SEGURIDAD (MÁXIMO 15 PUNTOS):

Este perfil será evaluado teniendo en cuenta la experiencia mínima habilitante y se otorgará puntaje por certificados relacionados seguridad de la información así:

Puntaje del Arquitecto de Seguridad (Puntaje máx. 15 puntos)	
Certificaciones de Conocimiento (Puntaje máx. 7 puntos)	
Profesional que presente dos (2) de los siguientes certificados vigente: TOGAF Certified, 27001/2022, Certificado CISSP, Certificado CISA, Certificado COBIT 2019	3 puntos
Profesional que presente tres (3) de los siguientes certificados vigente: TOGAF Certified, 27001/2022, Certificado CISSP, Certificado CISA, Certificado COBIT 2019	5 puntos
Profesional que presente todos los siguientes certificados vigente: TOGAF Certified, 27001/2022, Certificado CISSP, Certificado CISA, Certificado COBIT 2019	7 puntos
Experiencia Específica Adicional (Puntaje máx. 8 puntos)	

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

Puntaje del Arquitecto de Seguridad (Puntaje máx. 15 puntos)	
Certificaciones de Conocimiento (Puntaje máx. 7 puntos)	
Experiencia específica como arquitecto de seguridad en dos (2) proyectos relacionados con las tecnologías de la información	4 puntos
Experiencia específica como arquitecto de seguridad en tres (3) o más proyectos relacionados con las tecnologías de la información	8 puntos

Acreditación: El proponente deberá anexar con los documentos mínimos requeridos para el cargo de Arquitecto de seguridad, los certificados de conocimiento vigentes y experiencia adicional.

8.2.3. CONSULTOR SENIOR BCP/DRP (MÁXIMO 15 PUNTOS):

Este perfil será evaluado teniendo en cuenta la experiencia mínima habilitante y se otorgará puntaje por certificados relacionados con continuidad de negocio y recuperación ante desastres (BCP/DRP) así:

Puntaje del Consultor Senior BCP/DRP (Puntaje máx. 15 puntos)	
Certificaciones de Conocimiento (Puntaje máx. 7 puntos)	
Profesional que presente uno (1) de los siguientes certificados vigentes: Certificación en riesgo corporativo y/o gestión de crisis, normas ISO 22301 (Gestión de Continuidad del negocio) e ISO/IEC 27001 (Gestión de seguridad de la Información)	3 puntos
Profesional que presente dos (2) de los siguientes certificados vigentes: Certificación en riesgo corporativo y/o gestión de crisis, normas ISO 22301 (Gestión de Continuidad del negocio) e ISO/IEC 27001 (Gestión de seguridad de la Información)	5 puntos
Profesional que presente todos de los siguientes certificados vigentes: Certificación en riesgo corporativo y/o gestión de crisis, normas ISO 22301 (Gestión de Continuidad del negocio) e ISO/IEC 27001 (Gestión de seguridad de la Información).	7 puntos (puntaje máximo)
Experiencia Específica Adicional (Puntaje máx. 8 puntos)	
Experiencia específica como especialista en seguridad de la información y/o continuidad del negocio en dos (2) proyectos relacionado con planes de continuidad (BCP) o recuperación ante desastres (DRP)	4 Puntos
Experiencia específica como especialista en seguridad de la información y/o continuidad del negocio en tres (3) o más proyectos relacionado con planes de continuidad (BCP) o recuperación ante desastres (DRP)	8 Puntos

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

Acreditación: El proponente deberá anexar con los documentos mínimos requeridos para el cargo de Consultor Senior BCP/DRP, los certificados de conocimientos vigentes y experiencia adicional.

8.2.4. CONSULTOR DE GESTIÓN DEL CAMBIO (MÁXIMO 13,5 PUNTOS):

Se evalúa la experiencia del profesional en liderar procesos de gestión del cambio y cultura organizacional en proyectos tecnológicos, así como sus certificaciones especializadas en gestión del cambio. La asignación de puntaje seguirá esta escala:

Puntaje del Consultor de Gestión del Cambio (Puntaje máx. 13,5 puntos)	
Certificaciones de Conocimiento (Puntaje máx. 6 puntos)	
Profesional que presente uno (1) de los siguientes certificados: HCMP (Human Change Management Professional), certificación en el estándar HCMBOK (Human Change Management Body of Knowledge), certificación Management 3.0, y certificación como Agile Coach Professional	3 puntos
Profesional que presente tres (3) de los siguientes certificados: HCMP (Human Change Management Professional), certificación en el estándar HCMBOK (Human Change Management Body of Knowledge), certificación Management 3.0, y certificación como Agile Coach Professional	4 puntos
Profesional que presente todos los siguientes certificados: HCMP (Human Change Management Professional), certificación en el estándar HCMBOK (Human Change Management Body of Knowledge), certificación Management 3.0, y certificación como Agile Coach Professional	6 puntos (puntaje máximo)
Experiencia Específica Adicional (Puntaje máx. 7,5 puntos)	
Experiencia Específica como líder, o asesor en formulación e implementación de proyectos de gestión del cambio y cultura organizacional en entornos de tecnología de 7 a 10 años	5 Puntos
Experiencia Específica como líder, o asesor en formulación e implementación de proyectos de gestión del cambio y cultura organizacional en entornos de tecnología de más de 10 años	7,5 Puntos

Acreditación: El proponente deberá anexar con los documentos mínimos requeridos para el cargo de Consultor Senior BCP/DRP, los certificados de conocimiento vigentes experiencia adicional.

8.2.5.NOTAS APLICABLES A LA ASIGNACIÓN DE PUNTAJE Y PERFILES REQUERIDOS:

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

NOTA 1. La experiencia acreditada como Requisito Habilitante para cada perfil, NO SERÁ TENIDA EN CUENTA PARA LA ASIGNACIÓN DE PUNTAJE EN ESTA ETAPA.

NOTA 2. El puntaje máximo por experiencia adicional del Equipo de Trabajo es de TREINTA (30) PUNTOS. La acreditación de experiencia adicional a la solicitada NO GENERA PUNTAJE ADICIONAL.

NOTA 3. Si el proponente no presenta los documentos necesarios y completos para la asignación de puntaje, éste se calificará con cero (0,00) puntos.

NOTA 4. En caso de requerirse subsanación a alguno de los perfiles detallados en el Equipo Mínimo Habilitante, no se asignará puntaje en el presente componente, por tal razón dicho perfil no se tendrá en cuenta para la evaluación de la experiencia y obtendrá cero (0,00) puntos.

8.3. ESTÍMULO A LA INDUSTRIA NACIONAL (10 PUNTOS)

Con sujeción a lo dispuesto en la Ley 816 de 2003, se otorgará tratamiento de bienes y servicios nacionales a aquellos bienes y servicios originarios de los países con los que Colombia ha negociado trato nacional en materia de compras estatales y de aquellos países en los cuales a las ofertas de bienes y servicios colombianos se les conceda el mismo tratamiento otorgado a sus bienes y servicios nacionales.

Teniendo en cuenta que el contrato producto del presente proceso tiene implícita la prestación de servicios por parte del contratista, la entidad procedió a revisar el porcentaje de participación de los bienes en el presupuesto del proceso de contratación, así como la existencia de los bienes en el Registro de Productores de Bienes Nacionales, en los términos del Decreto 2680 de 2009 o las normas que lo modifiquen, aclaren, adicionen o sustituyan, encontrando que dicho porcentajes no es relevante teniendo en cuenta que la mayor parte de las inversiones para el desarrollo de las actividades, no son de origen nacional, por lo anterior se otorgará puntaje al proponente que vincule empleados o contratistas por prestación de servicios colombianos, en una proporción igual o superior al sesenta (60%) porciento del total de empleados y contratistas asociados al cumplimiento del contrato.

En el caso de Proponentes Plurales cualquiera de sus integrantes podrá vincular el **sesenta por ciento (60%)** del personal requerido para el cumplimiento del contrato.

Razón por la cual, el puntaje se otorgará en función de:

1. Servicios nacionales o con trato nacional o reciprocidad.
2. Incorporación de componente nacional en servicios extranjeros.

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

La entidad en ningún caso otorgará simultáneamente el puntaje por ambos aspectos

Los puntajes para estimular a la industria nacional se relacionan en la siguiente tabla:

Concepto	Puntaje
Promoción de Servicios Nacionales o con Trato Nacional	10,00
Incorporación de componente nacional en servicios extranjeros	5,00

8.3.1. PROMOCIÓN DE SERVICIOS NACIONALES O CON TRATO NACIONAL

En los contratos que deban cumplirse en Colombia, el servicio es nacional cuando además de ofertarse por una **persona natural colombiana** o por **un residente en Colombia**, por una **persona jurídica constituida de conformidad con la legislación colombiana** o por un **Proponente Plural conformado por estos** o por estos y un extranjero con Trato Nacional:

1. Usa el o los bienes nacionales relevantes definidos por la Entidad Estatal para el desarrollo de la obra, o
2. Vincula el porcentaje mínimo de personal colombiano, según corresponda.

Debido a la especialidad del contrato, en este Proceso de Contratación para el otorgamiento de puntaje **no habrá bienes nacionales relevantes** y, por tanto, se otorgará el puntaje de apoyo a la industria nacional a los Proponentes que se comprometan a vincular durante el desarrollo del objeto contractual un porcentaje de empleados o contratistas por prestación de servicios colombianos, de **al menos el sesenta por ciento (60%) del personal requerido para el cumplimiento del contrato**.

En el caso de Proponentes Plurales, todos, varios o cualquiera de sus integrantes podrá vincular un porcentaje de empleados o contratistas por prestación de servicios colombianos, de al menos el **sesenta por ciento (60%)** del personal requerido para el cumplimiento del contrato.

Además de la incorporación del porcentaje de personal colombiano requerido para la ejecución del contrato, tratándose de Proponentes Plurales, su composición deberá estar acorde con lo exigido por la noción de Servicios Nacionales prevista en el artículo 2.2.1.1.1.3.1 del Decreto 1082 de 2015, de lo que dependerá la franja del puntaje aplicable en lo referente al apoyo de la industria nacional.

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

A tales efectos en la siguiente tabla se indican las posibles composiciones de Proponentes Plurales, la regla de origen que les aplica en virtud de dicha conformación, así como la franja de puntaje correspondiente:

No.	Composición del componente plural	Regla de origen aplicable	Puntajes aplicables
1	Únicamente integrantes colombianos	Decreto 1082 de 2015	Promoción de Servicios Nacionales o con Trato Nacional
2	Colombianos en asocio con extranjeros con trato nacional	Decreto 1082 de 2015	Promoción de Servicios Nacionales o con Trato Nacional
3	Únicamente integrado por extranjeros con trato nacional	La regla de origen del país con el que se tenga el acuerdo comercial o la del Decreto 1082 de 2015. Si el proponente plural no especifica a cuál regla se acoge, se aplicará la del Decreto 1082 de 2015	Promoción de Servicios Nacionales o con Trato Nacional
4	Proponente plural en el que al menos uno de los integrantes es extranjero sin trato nacional	No aplica la regla de origen del Decreto 1082 de 2015, ni la de los países de origen	Incorporación de componente nacional en servicios extranjeros

La entidad asignará hasta **DIEZ (10,00) PUNTOS** a la oferta de: i) Servicios Nacionales o ii) Contrato Nacional.
Para que el proponente obtenga puntaje por Servicios Nacionales debe presentar:

1. **Persona natural colombiana**: La cédula de ciudadanía del proponente.
2. **Persona natural extranjera residente en Colombia**: La visa de residencia que le permita la ejecución del objeto contractual de conformidad con la ley.
3. **Persona jurídica constituida en Colombia**: El certificado de existencia y representación legal emitido por las Cámaras de Comercio.

Para que el proponente extranjero obtenga puntaje por trato nacional debe acreditar que los servicios son originarios de los Estados mencionados en la sección de acuerdos comerciales aplicables al presente proceso de contratación, información que se acreditará con los documentos que aporte el proponente extranjero para acreditar su domicilio.

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

Para asignar el puntaje por Servicios Nacionales o por Trato Nacional el proponente nacional o extranjero con trato nacional deben presentar el **ANEXO PROMOCIÓN DE SERVICIOS NACIONALES O CON TRATO NACIONAL**, junto al anexo debe presentar los documentos señalados en esta sección.

El proponente podrá subsanar la falta de presentación de la cédula de ciudadanía, la falta de certificado de existencia y representación legal para acreditar el requisito habilitante de capacidad jurídica; **no obstante, no podrá subsanar esta circunstancia para la asignación del puntaje por Servicios Nacionales o con Trato Nacional**.

La entidad asignará **DIEZ (10,00) PUNTOS** a un proponente plural cuando todos sus integrantes cumplan con las anteriores condiciones. Cuando uno de sus integrantes no cumpla con las condiciones descritas no obtendrá puntaje por Servicios Nacionales o Trato Nacional.

NOTA 1. ANEXO PROMOCIÓN DE SERVICIOS NACIONALES O CON TRATO NACIONAL Es necesario para la acreditación de la oferta realizada, por lo tanto, se deberá presentar toda la documentación de manera simultánea con la propuesta, de lo contrario, no será tenido en cuenta para el otorgamiento de puntaje.

NOTA 2. En el caso de consorcios, uniones temporales o cualquier figura asociativa, cada uno de sus integrantes deberá demostrar estar cubierto por el acuerdo comercial que pretenda acreditar y que el mismo se encuentre vigente con Colombia (Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación) para la obtención del puntaje y tratamiento como nacional. En todo caso, la inexistencia del acuerdo o certificación mencionados no restringe la participación de sociedades o personas extranjeras, ni constituye causal de rechazo de su propuesta

8.3.1.1. INCORPORACIÓN DE COMPONENTE NACIONAL EN SERVICIOS EXTRANJEROS

La entidad asignará **CINCO (5,00) PUNTOS** a los proponentes extranjeros sin derecho a Trato Nacional que incorporen a la ejecución del contrato **más del 70% del personal calificado de origen colombiano**.

Por otro lado, el Proponente que ofrezca personal colombiano con títulos académicos otorgados en el exterior deberá acreditar la convalidación de estos títulos en Colombia ante el Ministerio de Educación Nacional para la ejecución del contrato. En este sentido, para acreditar los títulos académicos otorgados en el exterior se requiere presentar la Resolución expedida por el Ministerio de Educación Nacional que convalida el título obtenido en el exterior.

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

Por personal calificado se entiende aquel que requiere de un título universitario otorgado por una institución de educación superior, conforme a la Ley 749 de 2002, para ejercer determinada profesión.

Para recibir el puntaje por incorporación de componente colombiano, el representante legal o apoderado del proponente debe diligenciar el **ANEXO INCORPORACIÓN DE COMPONENTE NACIONAL EN SERVICIOS EXTRANJEROS** en el cual manifieste bajo la gravedad de juramento el porcentaje de personal ofrecido y su compromiso de vincularlo en caso de resultar adjudicatario del proceso.

La entidad únicamente otorgará el puntaje por promoción de la incorporación de componente nacional cuando el proponente que presente el **ANEXO INCORPORACIÓN DE COMPONENTE NACIONAL EN SERVICIOS EXTRANJEROS** no haya recibido puntaje alguno por promoción de Servicios Nacionales o con Trato Nacional.

ACREDITACIÓN INCENTIVO COMPONENTE COLOMBIANO PROPONENTE EXTRANJERO SIN TRATO NACIONAL

La Entidad Estatal asignará **CINCO (5) PUNTOS** a los proponentes extranjeros sin derecho a Trato Nacional o a Proponentes Plurales en los que al menos uno de sus integrantes sea un extranjero sin derecho a Trato Nacional, que incorporen a la ejecución del contrato más del **noventa por ciento (90%) del personal técnico, operativo y profesional de origen colombiano**.

La Entidad Estatal únicamente debe ser aportado por los proponentes extranjeros sin derecho a trato nacional que opten por incorporar personal calificado colombiano. En el evento que un proponente nacional o extranjero con trato nacional lo presente, no será una razón para no otorgar el puntaje de promoción de servicios nacionales o con trato nacional.

Los proponentes plurales conformados por integrantes nacionales o extranjeros con derecho a trato nacional e integrantes extranjeros sin derecho a trato nacional podrán optar por la Incorporación de componente nacional en servicios extranjeros de acuerdo con las reglas definidas en este numeral.

En caso de no efectuar ningún ofrecimiento, el puntaje por este factor será de cero (0).

NOTA 1. Si el **ANEXO APOYO A LA INDUSTRIA NACIONAL ACREDITACIÓN INCENTIVO COMPONENTE COLOMBIANO PROPONENTE EXTRANJERO SIN TRATO NACIONAL** no es debidamente diligenciado de conformidad con los términos del presente numeral, dará lugar a que la propuesta obtenga **cero (0) puntos** de calificación por este concepto.

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

8.3.1.2. ACREDITACIÓN DE LA RECIPROCIDAD – PROTECCIÓN A LA INDUSTRIA NACIONAL

De conformidad con lo señalado en el artículo 2.2.1.2.4.1.3 del Decreto 1082 de 2015, en relación con la existencia de trato nacional, la Secretaría Distrital de Movilidad concederá trato nacional a:

1) Los oferentes bienes y servicios provenientes de Estados con los cuales Colombia tenga Acuerdos Comerciales, en los términos establecidos en tales Acuerdos Comerciales;
2) A los bienes y servicios provenientes de Estados con los cuales no exista un Acuerdo Comercial pero respecto de los cuales el Gobierno nacional haya certificado que los oferentes de servicios nacionales gozan de trato nacional, con base en la revisión y comparación de la normativa en materia de compras y contratación pública de dicho Estado; y
3) A los servicios prestados por oferentes miembros de la Comunidad Andina de Naciones teniendo en cuenta la regulación exterior andina aplicable a la materia.

El Ministerio de Relaciones Exteriores debe expedir el certificado por medio del cual se acredite la situación mencionada en el literal 2) anterior en relación con un Estado en particular, lo cual no es requerido para acreditar las situaciones a las que se refieren los literales 1) y 2) anteriores. Para constatar que los oferentes y servicios nacionales gozan de trato nacional en un Estado, el Ministerio de Relaciones Exteriores debe revisar y comparar la normativa en materia de compras y contratación pública del respectivo Estado para lo cual puede solicitar el apoyo técnico del Ministerio de Comercio, Industria y Turismo y de Colombia Compra Eficiente, dentro de sus competencias legales.

Los certificados para acreditar la condición a la que se refiere el literal 2) anterior deben ser publicados en la forma y oportunidad que para el efecto disponga Colombia Compra Eficiente. La vigencia de los certificados será de dos (2) años contados a partir de la fecha de su expedición, sin perjuicio de que el Ministerio de Comercio, Industria y Turismo o Colombia Compra Eficiente soliciten al Ministerio de Relaciones Exteriores su revisión con ocasión de la expedición de nueva normativa en el Estado sobre el cual se expide el certificado. Colombia Compra Eficiente puede determinar vía circular la forma como el Ministerio de Relaciones Exteriores debe constatar que los oferentes de Servicios nacionales gozan de trato nacional y de revisar y comparar la normativa en materia de compras y contratación pública para la expedición del certificado.

NOTA. El proponente que ofrezca bienes o servicios de origen extranjero y que pretenda la aplicación de trato nacional o reciprocidad, deberá acreditar la condición correspondiente, incluyendo en la propuesta la certificación expedida por el Ministerio de Relaciones Exteriores. La omisión de la Certificación del Ministerio de Relaciones

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

Exteriores por parte del proponente, hará que el factor de Protección a la Industria Nacional sea calificado con **cero (0,00) puntos**.

En todo caso, la inexistencia del acuerdo o certificación mencionados no restringe la participación de sociedades o personas extranjeras, ni constituye causal de rechazo de su propuesta.

8.3.1.3. INCENTIVO A LA INCORPORACIÓN DE COMPONENTE COLOMBIANO

Para la aplicación de este criterio se tendrá en cuenta lo dispuesto por el segundo inciso del artículo 2° de la Ley 816/03: A los proponentes de origen extranjero que ofrezcan determinado porcentaje de componente colombiano incorporado, referido a la totalidad del personal calificado del contrato, se les otorgará puntaje de conformidad con la tabla de componente nacional que se establece más adelante para la evaluación correspondiente.

Por personal calificado se entiende por aquel personal que requiere de un título universitario otorgado por una institución de educación superior, conforme a la Ley 749 de 2002, para ejercer determinada profesión.

Para estos efectos, los proponentes extranjeros que no hayan acreditado reciprocidad deberán señalar en el anexo correspondiente, el porcentaje ofrecido de componente nacional incorporado, referido a la totalidad del personal calificado que empleará para la ejecución del contrato.

8.4. ACREDITACIÓN DE PERSONAL CON DISCAPACIDAD (1 PUNTO)

Conforme a lo establecido en el Decreto 392 de 2018, para incentivar el sistema de preferencias a favor de las personas con discapacidad, las entidades estatales deberán otorgar el uno por ciento (1%) del total de los puntos establecidos en el pliego de condiciones electrónico y anexo complementario, a los proponentes que acrediten la vinculación de trabajadores con discapacidad en su planta de personal, de acuerdo con los siguientes requisitos:

1. El proponente deberá diligenciar el formato – VINCULACIÓN DE PERSONAS CON DISCAPACIDAD suscrito por la persona natural, el representante legal o el revisor fiscal, según corresponda, en el cual certifique el número total de empleados vinculados a la planta de personal del proponente o de sus integrantes a la fecha de cierre del proceso de selección.
2. Adicionalmente, deberá 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 presente proceso de selección

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

Verificados los anteriores requisitos, se asignará el 1,00%, a quienes acrediten el número mínimo de trabajadores con discapacidad, señalados a continuación:

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

Para los proponentes plurales, la entidad tendrá en cuenta la planta de personal del integrante del proponente plural que aporte como mínimo el 40% de la experiencia requerida para el proceso de contratación. De conformidad con lo anterior, es pertinente aclarar que la entidad validará el 40% en SMLMV. Adicionalmente, deberá suscribir el formato - VINCULACIÓN DE PERSONAS CON DISCAPACIDAD, suscrito por la persona natural o el representante legal de la persona jurídica que aporte como mínimo el 40% de la experiencia requerida para el proceso de contratación.
NOTA 1: Si el formato VINCULACIÓN DE PERSONAS CON DISCAPACIDAD no es diligenciado en su totalidad de conformidad con los términos del presente numeral, dará lugar a que la propuesta obtenga **cero (0,00)** puntos de calificación por este concepto.

8.5. EMPRENDIMIENTO Y EMPRESAS DE MUJERES (0,25 PUNTOS)

La entidad asignará un puntaje de 0,25 PUNTOS, al proponente que acredite la calidad de emprendimiento y empresa de mujeres con domicilio en el territorio nacional, de conformidad con lo previsto 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.

Se deberá diligenciar el formato – ACREDITACIÓN DE EMPRENDIMIIENTOS Y EMPRESA DE MUJERES y aportar la documentación requerida por la norma antes referida.

Tratándose de proponentes plurales este puntaje solo se otorgará si por lo menos uno de los integrantes acredita la calidad de emprendimiento y empresa de mujeres y tiene una participación igual o superior al 10% en el consorcio o unión temporal.

NOTA: La asignación de este puntaje no excluye la aplicación del puntaje para MIPYME.

8.6. MIPYME DOMICILIADAS EN COLOMBIA (0,25 PUNTOS)

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

La entidad asignará un puntaje de 0,25 PUNTOS, al proponente que acredite la calidad de MIPYME domiciliada en Colombia, de conformidad con el tamaño empresarial previsto en el artículo 2.2.1.13.2.2. del Decreto 1074 de 2015.

Se deberá diligenciar el Formato ACREDITACIÓN DE MIPYME y aportar la documentación requerida por la norma antes referida.

Tratándose de proponentes plurales este puntaje solo se otorgará si por lo menos uno de los integrantes acredita la calidad de MIPYME y tiene una participación igual o superior al 10%.

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, 2.2.1.1.2.1.1 y 2.2.1.1.2.1.3. 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:

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

N°	CLASE	FUENTE	ETAPA	TIPO	DESCRIPCIÓN (que puede pasar y, como puede ocurrir)	CONSECUENCIA DE LA OCURRENCIA DEL EVENTO	PROBABILIDAD	IMPACTO	VALORACION DEL RIESGO	CATEGORIA	¿A QUIEN SE LE ASIGNA?	TRATAMIENTO/ CONTROLES A SER IMPLEMENTADOS	IMPACTO DESPUES DEL TRATAMIENTO				¿AFECTA LA EJECUCION DEL CONTRATO?	PERSONA RESPONSABLE POR IMPLEMENTAR EL	FECHA ESTIMADA EN QUE INICIA EL TRATAMIENTO	FECHA ESTIMADA EN QUE SE COMPLETA EL TRATAMIENTO	MONITOREO Y REVISION	
													PROBABILIDAD	IMPACTO	VALORACION DEL RIESGO	CATEGORIA					¿COMO SE REALIZA EL MONITOREO?	PERIDIOCIDAD ¿Cuándo?
1	Especifico	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 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 posibilidad de que no se obtenga el objeto contractual debido a entregas inadecuadas, lo cual puede generar demoras en los tiempos de ejecución, afectaciones la calidad de los productos recibidos.	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, 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 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	Especifico	externo	Ejecución	operacional	Acceso o divulgación no autorizada que permite la utilización indebida de la información o del servicio	fuga y perdida de la informaci ón	probable (2)	mayor (4	Riesgo alto	Alto	Contratista	Exigir al contratista la suscripción del formato compromiso de confidencialida d de la información.	alta (4)	Moderado (3)	3	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 periódicos del supervisor sobre el cumplimiento del contrato

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

10. LUGAR Y PLAZO DE EJECUCIÓN

El plazo para ejecutar el contrato resultante del proceso será desde la firma del Acta de Inicio, previa expedición del registro presupuestal y aprobación de la(s) garantía(s) que debe tomar el contratista y hasta el 31 de diciembre de 2025.

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, edificio fortaleza.

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, una vez se encuentre aprobado el P.A.C., (Programa Anual Mensualizado de Caja) por parte del Ministerio de Hacienda y Crédito Público de la siguiente manera:

Un pago correspondiente al 100% del valor total a la entrega de la totalidad de los documentos indicados en el Anexo Técnico por parte del contratista a nombre del MINISTERIO DE DEFENSA NACIONAL – UNIDAD DE GESTIÓN GENERAL y del acta de recibo a satisfacción emitida por el supervisor del contrato.

Lo anterior será dentro de los treinta (30) días siguientes a la radicación en el Grupo Financiero 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

La(s) factura(s) deberá(n) ser presentada(s) al vencimiento del período facturado.

Si la (s) factura (s) no ha (n) sido correctamente elaborada(s) o no se acompañan los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte el último de los documentos y/o se presenten en debida forma. Las demoras que se presenten por estos conceptos serán responsabilidad del contratista y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza.

De conformidad con lo establecido en la Directiva Presidencial No. 09 del 17 de Septiembre de 2020 *"Lineamientos para el pago a los proveedores del Estado"*, **en**

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

caso que el proveedor que resulte contratista dentro del presente proceso de selección esté obligado a facturar electrónicamente, deberá presentar la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados, conforme con las disposiciones señaladas en el Decreto 358 del 5 de marzo de 2020, en concordancia, con lo dispuesto en la Resolución No. 000042 del 5 de mayo de 2020 y las normas que las modifiquen o sustituyan. Así mismo, el Contratista deberá haber efectuado el proceso de **Validación de la factura electrónica** en el Sistema SECOP II, de conformidad con lo señalado sobre el particular por Colombia Compra Eficiente.

Dichos pagos serán consignados en la cuenta bancaria que el contratista acredite como propia.

Para la realización de los pagos derivados del presente contrato, EL CONTRATISTA deberá entregar al supervisor del contrato el soporte que acredite que se encuentra al día en el pago de los aportes al Sistema de Seguridad Social Integral (salud, pensión y riesgos laborales) y aportes parafiscales, según corresponda, tanto de sus trabajadores y contratistas, mediante certificación expedida por el revisor fiscal o el representante legal según corresponda, de conformidad con la normatividad vigente.

conformidad con lo establecido en el parágrafo 2 del artículo 519 del Estatuto Tributario modificado por el artículo 8 del Decreto legislativo 0175 de 14 de febrero de 2025 "*Por el cual se adoptan medidas tributarias destinadas a atender los gastos del Presupuesto General de la Nación necesarios para hacer frente al estado de conmoción interior decretado en la región del Catatumbo, el área metropolitana de Cúcuta y los municipios de Rio de Oro y González del departamento del Cesar*", aplicable sobre los instrumentos públicos y documentos privados cuya cuantía sea superior a 6.000 Unidad de Valor Tributario -UVT, deberá presentar la el soporte de pago del impuesto, de acuerdo con lo estipulado por la DIAN. (documento DIAN No. 100208192-224 - Concepto General sobre el impuesto de timbre nacional)

12. PLAN DE COMPRAS

Certificado de Disponibilidad Presupuestal CDP No. 44325 del 13/08/2025

13. VIGENCIA FUTURAS (CUANDO APLIQUE)

N/A

14. DOCUMENTOS ANEXOS

- Cotizaciones
- Certificado de Disponibilidad Presupuestal - CDP.
- Concepto Técnico CITI

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

- Análisis del Sector y Estudios de Mercado
- Ficha Técnica

15. OFERTA ECONÓMICA

DESCRIPCION	V/r UNIT	VALOR IVA	VALOR TOTAL
DISEÑAR UN PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) QUE GARANTICE LA CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA NACIONAL.	298.375.350,00	56.691.316,67	355.066.666,67
TOTAL		-	**355.066.666,67**

Bogotá, 12 de septiembre de 2025

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

TC. LUZ ESPERANZA CORREA CRUZ
Jefe Oficina de Respuesta Incidentes Cibernéticos CSIRT - Defensa

Elaboró:
ASD Luis Felipe Martinez

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

FICHA TÉCNICA

Las siguientes son las especificaciones técnicas mínimas que deben cumplir los oferentes, teniendo en cuenta que tendrá que cubrir la totalidad de los servicios y requerimientos técnicos mínimo, así:

A continuación, se describen los requerimientos o necesidades, que hace parte integral del alcance del presente proceso, y que son de obligatorio cumplimiento, de acuerdo con las prioridades de la Oficina de Respuesta a Incidentes Cibernéticos CSIRT; el contratista debe desarrollar en su totalidad dentro del marco del objeto contractual.	
DISEÑAR UN PLAN DE RECUPERACIÓN ANTE DESASTRES (DRP) QUE GARANTICE LA CONTINUIDAD DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DE LA UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA NACIONAL.	
1. ASPECTOS GENERALES	
1.1	A continuación, se describen los aspectos generales que el contratista debe cumplir en desarrollo de las actividades tendientes a realizar 1. El objetivo del proceso es desarrollar, formular o actualizar e implementar un Plan tecnológico de Recuperación ante Desastres (DRP) robusto y eficiente que garantice la continuidad de las operaciones críticas tecnológicas de la UGG que administra la DTICS, para minimizar el impacto de posibles interrupciones por desastres tecnológicos y apuntar a la construcción de una resiliencia cibernética constituida para el sector. 2. Se deberá tener un grupo especializado requerido para la Entidad y desarrollar el contenido de la especificación técnica, con el liderazgo de un equipo transversal o Gerente del proyecto. 3. El desarrollo del DRP deberá estar fundamentado en los lineamientos sectoriales de continuidad de negocio existentes dentro del sector de Defensa del Estado colombiano, alineándolos con las políticas sectoriales y definiciones de MinTIC. 4. Crear un cronograma detallado de las actividades del proyecto, incluyendo la secuencia, la duración estimada, las dependencias y los hitos. Identificando y asignando los roles y responsabilidades a los miembros del equipo, dentro de los cinco (05) días hábiles siguientes al perfeccionamiento de este. 5. Durante la realización del proyecto, el contratista deberá mantener todos los aspectos de seguridad de los equipos, sistemas, activos informáticos, siempre que haya modificaciones y/o actualizaciones que puedan afectar la configuración existente, siendo este aspecto responsabilidad del contratista por los cambios realizados. 6. El contratista deberá alinearse a las políticas de seguridad de las Entidades, así como el modelo MSPI del Ministerio de las Telecomunicaciones de Colombia – MinTIC. 7. Obtener con la oportunidad debida, las licencias, autorizaciones y permisos a que hubiere lugar para el cumplimiento de todas las obligaciones que le corresponden en los términos del presente contrato. 8. Mantener durante el plazo d ejecución del contrato los precios ofertados. 9. El contratista deberá cumplir todas las normas de seguridad industrial en la ejecución del contrato. 10. El contratista deberá asumir la responsabilidad en el manejo del personal empleado, así como la seguridad y responsabilidad de los elementos y materiales que se requieran para el desarrollo de este contrato. 11. Si el oferente llegase a ajustar o a realizar algún cambio sobre la plataforma tecnológica de la UGG deberá mantener todos los aspectos de seguridad de los

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

	equipos siempre que haya modificaciones y/o actualizaciones que puedan afectar la configuración existente, siendo este aspecto responsabilidad del oferente, por los cambios realizados.
2.	Fases y desarrollo del DRP
2.1	Levantamiento de información Recopilar, analizar y organizar toda la información necesaria sobre procesos, sistemas, activos y dependencias tecnológicas de la entidad (UGG), como base para la construcción del DRP, en donde se realizará las siguientes actividades: 1. Identificar a todas las personas, grupos de interés que participaran directa o indirectamente en la construcción del DRP con el conocimiento del negocio. 2. Definir los resultados y beneficios que se esperan obtener con la implementación del DRP (por ejemplo, reducción del tiempo de inactividad, minimización de la pérdida de datos, mejora de la resiliencia operativa). 3. Alinear los objetivos del proyecto con las metas y prioridades estratégicas de las entidades del sector defensa definidas en este proceso 4. Definir estrategias para gestionar las relaciones con las diferentes partes interesadas. 5. Definir plan de proyecto para la gestión del alcance, el tiempo, costos, la calidad, los recursos humanos, las comunicaciones y los riesgos entre otros. 6. Identificar y clasificar según su criticidad a todos los procesos esenciales del negocio, la dependencia e interconexión vitales para la operación 7. Identificar los recursos de TI necesarios para cada proceso crítico según la misionalidad de la Unidad de Gestión General del Ministerio de Defensa Nacional 8. Definir metodología de recopilación (entrevistas, cuestionarios, análisis documental, sesiones de trabajo). 9. Registrar servicios o recursos contratados a terceros (proveedores de nube, telecomunicaciones, etc.). 10. Generar el Inventario y clasificar los activos de TI críticos y que serán parte del plan DRP: • Hardware (servidores, estaciones, dispositivos de red, etc.). • Software (sistemas operativos, aplicaciones críticas, bases de datos). • Redes (topología, enlaces, proveedores). • Datos (bases de datos, volúmenes de datos, clasificaciones) Y de más activos que puedan ser clasificados como críticos para el Ministerio de Defensa Nacional. 11. Analizar el contexto organizacional y el análisis de los factores internos y externos que pueden influir en la continuidad del negocio. 12. Analizar el liderazgo y compromiso para obtener el apoyo de la alta dirección del área encargada del DRP para garantizar la asignación de recursos y la alineación con los objetivos organizacionales. 13. Realizar el análisis de la arquitectura tecnológica y de seguridad actual (hardware, software, redes, etc.) de las tecnologías de la Información y comunicaciones. Entregables: - Matriz de procesos y activos críticos. - Mapa preliminar de dependencias tecnológicas. - Informe de hallazgos y brechas identificadas.

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

2.2	Análisis del Negocio (BIA) Realizar un Análisis de Impacto al Negocio (BIA) para identificar procesos críticos, tiempos de recuperación requeridos y posibles consecuencias de la interrupción de servicios TIC en la operación de la UGG que contenga las siguientes actividades: 1. La definición del Alcance del BIA debe contemplar la Identificación de procesos, servicios y áreas que serán evaluados 2. Alinear el alcance con los objetivos estratégicos de la entidad y la misión de la UGG. 3. Elaborar cuestionarios, plantillas y guías de entrevistas para recopilar información clave y socializarlo con el supervisor del contrato antes de su aplicación 4. Realizar sesiones de entrevistas con líderes de procesos, áreas críticas y responsables de TI. 5. Aplicar cuestionarios para documentar: • Procesos críticos y dependencias. • Recursos necesarios (personas, infraestructura, tecnología, proveedores). • Impactos ante la interrupción (operativo, financiero, legal, reputacional). • Tiempos máximos de tolerancia a la interrupción. 6. Priorizar los procesos según su criticidad para la entidad e identificar relaciones de dependencia entre procesos y servicios TIC. 7. Determinar, por cada proceso y sistema crítico: • **RTO** (Recovery Time Objective): Tiempo máximo tolerado para reanudar la operación. • **RPO** (Recovery Point Objective): Cantidad máxima de datos que se pueden perder. • **WRT** (Work Recovery Time): Tiempo adicional para restaurar la funcionalidad tras la recuperación técnica. • **MTD** (Maximum Tolerable Downtime): Tiempo máximo total de interrupción aceptable para el negocio. 8. Evaluar y cuantificar: • Impacto financiero (pérdidas económicas, multas, contratos afectados). • Impacto operativo (interrupción de servicios, tiempos de espera, afectación a usuarios). • Impacto legal y regulatorio (incumplimientos normativos, sanciones). • Impacto reputacional (imagen, confianza de los usuarios). 9. Crear tablas consolidadas que muestren: • Procesos críticos, prioridades, dependencias. • RTO, RPO, MTD, WRT por cada proceso/sistema. • Clasificación de impactos (alto, medio, bajo). 10. Redactar el informe completo con: • Metodología utilizada. • Resultados por proceso. • Recomendaciones. • Incluir anexos: cuestionarios aplicados, matrices de resultados y gráficos. Entregables: - Informe de Análisis de Impacto al Negocio (BIA). - Matriz de procesos críticos y tiempos de recuperación (RTO, RPO, MTD, WRT). - Matriz de impactos clasificados.

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

2.3	Análisis de Riesgos TI Identificar, analizar y evaluar los riesgos que puedan afectar la continuidad de los servicios tecnológicos y los procesos críticos de la Unidad de Gestión General del Ministerio de Defensa Nacional, estableciendo las bases para definir estrategias de mitigación y recuperación. 1. Definición del Alcance y Metodología del Análisis de Riesgos 2. Establecer el marco de análisis (procesos TIC críticos, sistemas, infraestructura, personal, proveedores). 3. Definir la metodología a utilizar (ej. ISO 27005, ISO 31000, NIST SP 800-30, MAGERIT). 4. Acordar escalas de impacto y probabilidad (bajo, medio, alto) con el supervisor del contrato. 5. Revisar los activos TIC identificados en el inventario (hardware, software, datos, redes, servicios) validando su importancia para la continuidad del negocio y clasificar los activos según su criticidad 6. Determinar las amenazas que pueden afectar la continuidad, como: • Amenazas naturales (inundaciones, incendios, terremotos). • Fallos tecnológicos (caídas de servidores, pérdida de datos, errores de configuración). • Ciberamenazas (ataques DDoS, ransomware, accesos no autorizados, etc). • Errores humanos. • Factores externos (fallo de servicios de terceros, proveedores críticos). • Identificar vulnerabilidades existentes (brechas de seguridad, falta de redundancia, errores de configuración, etc). 7. Calcular el nivel de riesgo de cada combinación amenaza–vulnerabilidad–activo. 8. Clasificar riesgos según matriz de criticidad (alto, medio, bajo). 9. Análisis de Brechas (Gap Analysis) comparando el estado actual frente a estándares y mejores prácticas (ISO 22301, ISO 27001, MSPI-MinTIC, NIST), Identificando diferencias, deficiencias o carencias en los controles implementados. 10. Establecer el nivel de riesgo que persiste después de aplicar los controles existentes e identificar riesgos inaceptables que requieren mitigación adicional. 11. Definir qué riesgos deben abordarse prioritariamente en el DRP y establecer planes de tratamiento para mitigarlos. 12. Elaborar una matriz de riesgos en donde se consolide la información que incluya: • Activo afectado • Amenaza/vulnerabilidad. • Nivel de riesgo. • Controles existentes. • Controles adicionales recomendados. 13. Redactar el informe completo de análisis de riesgos: • Metodología utilizada. • Matriz de riesgos. • Recomendaciones. • Brechas encontradas Entregables: - Matriz de riesgos tecnológicos (amenazas, vulnerabilidades, activos afectados, nivel de riesgo, controles).

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

	- Informe de análisis de riesgos y brechas. - Hoja de ruta preliminar para mitigación de riesgos. - Documentación de metodología aplicada y anexos.
2.4	Estrategias de Recuperación Definir las estrategias más adecuadas y viables para restablecer los servicios TIC críticos de la Unidad de Gestión General del Ministerio de Defensa Nacional en caso de una interrupción, alineadas con la criticidad de los procesos y los requerimientos de recuperación establecidos en el BIA que contenga los siguientes puntos: 1. Analizar resultados del BIA (procesos críticos, RTO, RPO, MTD, WRT). 2. Analizar la arquitectura de seguridad de la UGG. 3. Revisar la matriz de riesgos TI y vulnerabilidades identificadas. 4. Validar información sobre capacidades actuales y limitaciones de la infraestructura. 5. Definir opciones técnicas y logísticas para la recuperación de los servicios TIC, tales como: • Recuperación en sitio alterno (activo, pasivo, cálido o frío). • Recuperación en la nube (IaaS, PaaS, SaaS). • Alta disponibilidad y soluciones de tolerancia a fallos. • Backups y esquemas de respaldo/restore. • Procesos manuales de respaldo temporal (cuando aplique). 6. Evaluar la capacidad actual de la entidad para soportar las estrategias propuestas. 7. Identificar necesidades adicionales: hardware, software, redes, servicios de terceros. 8. Estimar los costos asociados a cada opción de recuperación junto con la identificación de recursos humanos, tecnológicos y logísticos requeridos. 9. Asignar estrategias específicas a cada sistema, servicio o proceso clave. 10. Ordenar las estrategias según criticidad y tiempos de recuperación definidos. 11. Incorporar ajustes según retroalimentación técnica. 12. Redactar el Documento de Estrategias de Recuperación que incluya: • Alternativas evaluadas. • Estrategias seleccionadas y su justificación. • Costos estimados y recursos requeridos. • Cronograma de implementación preliminar. Entregables: - Documento de Estrategias de Recuperación (por sistema crítico). - Matriz de alternativas evaluadas con análisis costo-beneficio. - Hoja de ruta preliminar para la implementación. - Acta de validación de estrategias por la entidad.
2.5	Desarrollo del Plan de Comunicación de Crisis (PCC) Diseñar e implementar un Plan de Comunicación de Crisis (PCC) que establezca los protocolos, roles, canales, mensajes y tiempos para informar oportunamente a las partes interesadas internas y externas durante una contingencia que afecte los servicios TIC. El cual se realizarán las siguientes actividades: 1. Determinar qué tipos de incidentes o desastres activarán el PCC.

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

2. Identificar los procesos y sistemas críticos cuya interrupción requiere comunicación inmediata.
3. Elaborar una matriz de interesados:
   - Internos (directivos, colaboradores, equipos técnicos, usuarios finales).
   - Externos (proveedores, clientes, entidades reguladoras, medios de comunicación, terceros críticos).
4. Crear directorio actualizado de contactos de emergencia.
5. Asignar responsables para:
   - Vocería oficial.
   - Redacción de mensajes.
   - Canales digitales (correo, página web, redes sociales).
   - Contacto directo con autoridades y medios.
6. Establecer métodos de comunicación redundantes para garantizar el acceso en situaciones de emergencia
7. Identificar y validar los canales formales y alternativos, por ejemplo:
   - Correo institucional.
   - Mensajes de texto/SMS.
   - Llamadas telefónicas directas.
   - Plataforma de mensajería (WhatsApp, Teams, etc.).
   - Publicación en intranet o sitio web
8. Asegurar que el Plan de Comunicación de Crisis esté alineado e integrado con:
   - DRP (Plan de Recuperación ante Desastres).
   - Plan de Continuidad del Negocio (BCP).
   - Plan de Gestión de Incidentes.
9. Establecer cuándo y cómo se debe informar durante:
   - Detección de la crisis.
   - Activación del DRP.
   - Progreso de recuperación.
   - Finalización y retorno a la normalidad
10. Diagramar el proceso de comunicación:
    - ¿Quién informa a quién?
    - ¿Con qué frecuencia?
    - ¿Por qué canal?
11. Definir tiempos de respuesta y niveles de aprobación.
12. Redactar el documento final incluyendo:
    - Objetivos y alcance.
    - Roles y responsabilidades.
    - Canales y protocolos.
    - Plantillas de mensajes.
    - Flujos de comunicación.
    - Directorio de contactos clave.

Entregables:

- Documento del Plan de Comunicación de Crisis.
- Matriz de partes interesadas (Stakeholders).
- Directorio de contactos de emergencia.
- Flujogramas de comunicación.
- Plantillas de mensajes tipo.

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

	- Revisión y validación del PCC por la entidad.
2.6	Desarrollo del DRP Elaborar, documentar y estructurar el Plan de Recuperación ante Desastres (DRP) de la Unidad de Gestión General del Ministerio de Defensa, con procedimientos claros, roles definidos y recursos asignados para garantizar la recuperación oportuna de los servicios TIC críticos y que contenga lo siguiente: 1. Establecer el índice y los capítulos del documento final (alineado a estándares como ISO 22301, NIST SP 800-34, DRI). 2. Redactar la política de recuperación ante desastres definiendo los objetivos generales y específicos del DRP, alineados al BIA y análisis de riesgos. 3. Redactar procedimientos paso a paso para la recuperación de cada sistema, servicio o proceso crítico incluyendo instrucciones claras sobre: • Activación del DRP. • Comunicación inicial de la crisis. • Recuperación técnica de cada servicio (servidores, aplicaciones, redes, bases de datos, etc.). • Validación y verificación de la restauración. • Retorno a la normalidad. • Documentar los flujos de actividades y diagramas de procesos 4. Establecer el Comité de Recuperación ante Desastres y los equipos de respuesta (líderes, técnicos, comunicaciones, logística), junto con la definición de funciones específicas de cada rol. 5. Identificar los recursos tecnológicos, humanos y logísticos requeridos para activar el DRP, estableciendo la disponibilidad y ubicación de recursos críticos (servidores, respaldos, enlaces alternos, etc.). 6. Definir la arquitectura de seguridad para operativizar el DRP. 7. Definir protocolos de comunicación internos y externos durante una contingencia, estableciendo canales de comunicación alternativos. 8. Incluir protocolos de gestión de incidentes, gestión de cambios y continuidad de servicios. 9. Incorporar políticas de seguridad de la información y sanitización de datos post-evento. 10. Diseñar formularios y registros necesarios para la ejecución del DRP: • Registro de incidentes. • Listas de verificación (checklists) para la recuperación. • Formatos de seguimiento y control. 11. Validar internamente el contenido del DRP junto con el supervisor del contrato y realizar ajustes según revisiones técnicas y de estilo. 12. Entregar borrador para revisión por parte de la UGG 13. Consolidar el documento definitivo: • En formato digital (Word, PDF, editable). • Se deberá entregar un libro con capítulos de cada tema requerido en la ficha técnica, con un mínimo de 120 páginas, la medida del libro es de 17,5 x 25, libros en tapa dura, impresa en cote de 150 gr. plastificada en brillantes a 4x4 tintas, en bond de 90gra a 4x4 tintas. Páginas, letra Arial 10, de contenido de acuerdo con la concertación de la estructuración entre el consultor y las Entidades corregido y ajustado, diagramado e impreso, en forma física y digital en una USB, con la corrección de estilo para que este

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

	pueda ser editado en caso de ser necesario, referente a los temas de estudio relacionado en esta especificación técnica • Asegurar cumplimiento de normas APA y requisitos editoriales (diseño, diagramación, estilo). Entregables: - Documento completo del DRP, estructurado, revisado y aprobado - Procedimientos de recuperación detallados por sistema crítico - Matriz de roles y responsabilidades. - Plan de comunicación de crisis. - Formatos, anexos y flujogramas de recuperación. - Borrador revisado por la entidad y versión final validada.
2.7	Validación y Pruebas del DRP Verificar que el DRP sea funcional, completo y efectivo para garantizar la continuidad operativa ante una interrupción, mediante simulaciones controladas y pruebas estructuradas, asegurando que los equipos sepan cómo actuar y que los procedimientos sean adecuados, para lo cual se deberá realizar las siguientes actividades: 1. Definir el tipo de pruebas a realizar: • Pruebas de escritorio (TableTop). • Pruebas técnicas unitarias (por sistema crítico). • Simulacros integrados (opcional según madurez). 2. Establecer objetivos de cada prueba (ej. validar tiempos de respuesta, comunicación, ejecución de pasos técnicos). 3. Seleccionar participantes clave como líderes de recuperación, responsables de TI, personal de comunicaciones, seguridad y apoyo operativo. 4. Asignar roles para ejecución, observación y evaluación. 5. Diseñar escenarios realistas y alineados a riesgos identificados (ej. falla de servidor de base de datos, ciberataque, corte de energía en CPD). 6. Crear documentos guía para los participantes: • Instrucciones detalladas de prueba. • Formatos de observaciones. • Plantillas para evaluación de desempeño. 7. Definir métricas de éxito: cumplimiento de RTO/RPO, activación efectiva del plan, errores detectados, tiempos de reacción 8. Realizar la prueba TableTop: • Simulación teórica en sala de crisis • Evaluación del tiempo de reacción, coordinación, toma de decisiones 9. Ejecutar pruebas unitarias de recuperación en donde se tenga en cuenta simulación técnica por sistema crítico (restauración de respaldos, recuperación de base de datos, failover de servidores, etc.). 10. Comparar resultados frente a los objetivos definidos. 11. Identificar deficiencias, retrasos, fallas técnicas o errores en la ejecución. 12. Consolidar toda la información en un informe: • Descripción del escenario y participantes. • Resultados observados por sistema/proceso.

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

	• Brechas identificadas. • Recomendaciones de mejora. Entregables: - Plan de pruebas documentado (tipos, cronograma, escenarios, objetivos). - Escenarios de simulación y guías para participantes - Registro de resultados y formatos de observación. - Informe de validación del DRP (con hallazgos, recomendaciones, mejoras). - Versión final del DRP ajustado. - Versión final de la arquitectura de seguridad. - Acta de validación aprobada por la Unidad de Gestión General del Ministerio de Defensa Nacional
3	**CONDICIONES PARA EL PERSONAL QUE DESARROLLARÁ EL OBJETO CONTRACTUAL POR PARTE DEL CONTRATISTA**
3.1	El contratista deberá garantizar la continuidad del desarrollo o ejecución de cada una de las actividades objeto del contrato, para lo cual, de ser necesario debe prever el reemplazo del personal que se encuentra adelantando las actividades cuando así se requiera, por uno igual o de superior experiencia, entregando la hoja de vida de la persona reemplazante al supervisor del contrato para la aprobación de la experiencia técnica de los ingenieros que fueron requeridos.
3.2	El contratista debe desarrollar las actividades objeto del contrato en horario laboral y en días y horas no hábiles o en fines de semana o días festivos, tanto en horario diurno como nocturno, es decir 7x24.
3.3	Al personal asignado para el desarrollo del proyecto por parte del contratista, se le realizará un estudio de seguridad para lo cual se debe aportar la siguiente documentación en un término no mayor de 15 días calendarios a partir de la aprobación de la garantía de cumplimiento: a. Copia cedula de ciudadanía b. Copia libreta militar (para quien aplique) 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
3.4	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 de gestión técnica, 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.
3.5	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

3.6	El contratista asumirá todos los costos o gastos asociados al desplazamiento de su personal a los sitios de trabajo del Ministerio de Defensa Nacional.
3.7	El contratista debe garantizar que el personal que realice las actividades en desarrollo del objeto contractual sea especializado en cada uno de los productos o sistemas o herramientas descritas en el presente documento.
3.8	Todo el personal requerido para la ejecución del contrato debe tener disponibilidad de tiempo para la atención y solución de los requerimientos en el marco del objeto contractual, efectuados por parte de la Dirección de Tecnologías de la Información y las Comunicaciones, en el momento que se le requiera. Será de la autonomía y responsabilidad del contratista la vinculación, organización, orientación y control del personal a su cargo, comprometiéndose a cumplir con las normas de seguridad existentes en el Ministerio de Defensa Nacional. Cabe anotar que la Unidad de Gestión General del Ministerio de Defensa Nacional no adquiere ninguna relación contractual, civil o laboral con los trabajadores del contratista.
3.9	La Entidad se reserva el derecho de exigir al contratista, previo escrito emitido por el competente contractual y el supervisor designado, el reemplazo de cualquier persona vinculada al proyecto, Esta exigencia no dará derecho al contratista para elevar ningún reclamo contra la Entidad contratante.
3.10	La supervisión podrá solicitar al contratista en cualquier momento, información sobre la nómina del personal y cumplimiento de aportes al sistema de seguridad social del personal contratado por prestación de servicios. El contratista atenderá esta solicitud con el detalle requerido y en el plazo razonable que el supervisor haya fijado.
3.11	CONDICIONES DE EXPERIENCIA DEL PERSONAL ASIGNADO AL CONTRATO **Gerente de proyectos:** El profesional requerido deberá liderar y coordinar la identificación, planificación, implementación, y la ejecución de estrategias de recuperación ante desastres que puedan vulnerar la infraestructura tecnológica de la Entidad, garantizando la continuidad operativa de la UGG. **Perfil Profesional:** Ingeniero de sistemas o afines Posgrado en la modalidad de Maestría en Gerencia de Proyectos **Experiencia Mínima** Experiencia Profesional de 10 años a partir de la expedición de la tarjeta profesional. Experiencia específica como gerente de proyectos en al menos un (1) proyecto de tecnología que corresponda a proyectos de arquitectura de seguridad. **Arquitecto de seguridad** El profesional requerido deberá identificar y/o diseñar/implementar la arquitectura de seguridad de la Entidad que garantice la protección integral de la operación frente a amenazas internas o externas en cumplimiento de las normas estatales e institucionales, mediante la definición de controles de seguridad, evaluación de vulnerabilidades, cumplimiento normativo, y la validación técnica de simulacros. **Perfil Profesional:** Ingeniero de sistemas o carrera afín Posgrado en la modalidad de especialización o maestría en Seguridad de la Información

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

Experiencia mínima
Experiencia profesional no menor a diez (10) años a partir de la expedición de la tarjeta profesional.
Experiencia específica como arquitecto de seguridad en por lo menos un (1) proyectos relacionados con las tecnologías de la información.

Consultor Senior BCP/DRP

El profesional deberá diseñar y/o implementar y/o mejorar el Sistema de Gestión de continuidad del negocio y recuperación ante desastres (BCP/DRP), asegurando la operatividad de la tecnología en el cumplimiento de la misión de la Entidad.

Perfil Profesional:
Ingeniero de sistemas o ingeniero industrial, ingeniero administrativo, seguridad informática o áreas afines
Conocimiento en regulaciones locales como Ley 1581/2012, Decreto 1078/2015 y/o políticas de gobierno digital.

Experiencia:
Experiencia profesional mínima de diez (10) años a partir de la expedición de la tarjeta profesional.
Experiencia específica como especialista en seguridad de la información y/o continuidad del negocio en al menos un (1) proyecto relacionado con planes de continuidad (BCP) o recuperación ante desastres (DRP).

Consultor gestión del cambio

Deberá garantizar y facilitar la adopción efectiva de los cambios o estructuras implementadas en la operación de la UGG

Perfil Profesional:
Profesional en Comunicación Social o Corporativa.

Experiencia Mínima
Experiencia profesional mínimo de diez años (10) a partir de la obtención del título profesional, de los cuales al menos seis (6) años deben estar relacionados con formulación e implementación de proyectos de gestión del cambio y cultura organizacional preferiblemente en entornos de tecnología, habiendo participado como profesional, consultor, líder o asesor en dichos proyectos; incluyendo al menos un (1) proyecto relacionado con arquitectura de seguridad en el rol de experto en gestión del cambio, o transformación digital o modernización administrativa o rediseño institucional

Para acreditar la idoneidad del personal aportado, se deben anexar los siguientes requisitos:
- La hoja de vida del personal propuesto
- Fotocopias de los diplomas o actas de grado,
- Soporte de la experiencia
- Carta de compromiso.

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

	NOTA 1. El proponente deberá aportar en su propuesta, como requisito mínimo habilitante los documentos antes mencionados, en relación con los siguientes cargos o profesionales que integran el PERSONAL MINIMO a saber: **Gerente de proyectos** **Arquitecto de seguridad** **Consultor Senior BCP/DRP** **Consultor gestión del cambio**
3.12	Para acreditar la experiencia del personal, se debe anexar certificación que reúna los siguientes requisitos: • Ser expedidas por el contratante. En caso de ser expedida por una entidad pública o privada, la certificación deberá estar suscrita por el funcionario de la Entidad, competente para emitirla. • Señalar el objeto del contrato, • Indicar fecha de inicio y terminación del contrato, • Indicar el cargo ocupado dentro del contrato, • Indicar nombre, dirección y teléfono del contratante. Las certificaciones que acrediten la experiencia del personal propuesto se considerarán expedidas bajo gravedad de juramento
3.13	Respecto de las certificaciones de experiencia laboral, el contratista debe contemplar para cada una la siguiente información: a. Nombre de la empresa que recibió los servicios y en la cual el experto propuesto prestó sus servicios. b. Nombre del proyecto ejecutado. c. Perfiles o cargos desempeñados. d. Fechas de inicio y terminación del contrato. e. Actividades ejecutadas. f. Teléfono y correo de contacto.
3.14	Para su evaluación por parte de la supervisión, las certificaciones de experiencia requeridas deben ser entregadas por parte del contratista a más tardar dentro de los ocho (08) días calendario siguiente a la fecha de suscripción del Acta de Inicio al supervisor del contrato o a la persona que este designe para tal fin.
3.15	Para el personal al que se le exige título profesional o título de tecnólogo o título de técnico, la experiencia se computará a partir de la fecha de expedición de la tarjeta o matricula profesional. En consecuencia, para este aspecto el contratista debe suministrar copia de la tarjeta o matricula profesional.
4	**RIESGOS PROFESIONALES**
4.1	El contratista cumplirá todas las normas de seguridad industrial en la prestación del servicio y garantizará los cuidados y precauciones necesarias para el desarrollo de este.
4.2	El contratista deberá entregar el certificado del curso virtual de 50 horas sobre seguridad y salud en el trabajo (Art. 2.2.4.6.35 del Decreto 1072 de 2015), el cual deberá permanecer vigente durante el plazo de ejecución del contrato.
5	**CONFIDENCIALIDAD E INTEGRIDAD DE LA INFORMACIÓN INSTITUCIONAL**
5.1	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, deberá garantizar 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

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

	durante la ejecución del contrato, así como de los elementos que para su ejecución la Unidad de Gestión General y Oficina de Respuesta a Incidentes informáticos del MDN ponga a su disposición. Dicho documento deberá suscribirse 5 días posterior a la firma el acta de inicio.
5.2	De igual manera, Documento del Plan de Recuperación ante Desastres (DRP): Plan completo con los procedimientos, roles y recursos, hoja de ruta y plan de implementación del DRP, Plan de Comunicación de Crisis el diseño, las pruebas y sus resultados, las políticas y los procesos en la actualización de la solución serán considerados por el contratista como información confidencial propiedad del Ministerio de Defensa Nacional – Unidad Gestión General, en tal virtud, adoptará todas las medidas necesarias para impedir su duplicación, sustracción, divulgación, alteración, ocultamiento o utilización indebida.
5.3	Durante la actualización y asistencia técnica de las soluciones, el contratista se compromete a no hacer uso indebido de las herramientas utilizadas en desarrollo del objeto contractual, ni duplicar, sustraer, divulgar o alterar información a la cual pueda tener acceso a través de ellas.
5.4	De acuerdo con el Modelo de Seguridad y Privacidad de la Información – MSPI del Ministerio de las Telecomunicaciones de Colombia – MinTic y la Directiva de seguridad de la información del sector Defensa y en pro de su cumplimiento todos los equipos Laptop y/o equipos de escritorio, así como equipos de conectividad y seguridad utilizados por el personal para el desarrollo de esta especificación técnica, al finalizar se les deberá realizar procedimiento de borrado seguro y/o sanitización de datos para los discos duros que conlleven a la eliminación de la data recopilada y analizada de cada una de las Entidades, el software utilizado para el borrado seguro debe estar debidamente licenciado y no puede ser de código abierto. Además, debe generar un certificado auditable que garantice que el borrado de los datos ha sido irreversible, el cual podrá ser presentado ante auditorías sobre el tratamiento de la información (debe debe cumplir con las normas nacionales e internacionales aplicables a la eliminación segura de información sensible descritas en las condiciones técnicas exigidas en las licencias de acceso a nube requeridas para las 4 entidades).
6	CONDICIONES DE EXPERIENCIA DEL PROPONENTE
6.1	Para garantizar la idoneidad y capacidad técnica de los oferentes, cada firma deberá presentar mínimo 2 certificaciones que cumplan con los siguientes criterios: - El proponente deberá acreditar la ejecución satisfactoria de al menos un (1) contrato cuyo valor sea igual o superior al 100 % del presupuesto oficial. Esto asegura que la empresa haya gestionado previamente proyectos de magnitud económica similar, con todos los retos operativos y financieros que ello conlleva. - Los contratos a presentar como experiencia debe tener como objeto y/o actividades específicas de diseño y/o implementación y/o diagnóstico y/o análisis de arquitectura de seguridad en entornos TI.

Clasificación UNSPSC

CÓDIGO UNSPSC	SEGMENTO	FAMILIA	CLASE
80101600 Gerencia de proyectos	**80** Servicios de Gestión, Servicios Profesionales de	**10** Servicios de asesoría de gestión	**16** Gerencia de Proyectos

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

	Empresa y Servicios Administrativos		
80101500 Servicios de consultoría de negocios y administración corporativa	**80** Servicios de Gestión, Servicios Profesionales de Empresa y Servicios Administrativos	**10** Servicios de asesoría de gestión	**15** Servicios de consultoría de negocios y administración corporativa
81161500 Servicios de Administración de Acceso	**81** Servicios basados en ingeniería, investigación y Tecnología	**16** Entrega de servicios de tecnología de información	**15** Servicios de Administración de Acceso
8111900 Servicios de Administración de Acceso	**81** Servicios basados en ingeniería, investigación y Tecnología	**11** Servicios informáticos	**19** Sistemas de Recuperación de información

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