UNIDAD DE GESTIÓN GENERAL- DIRECCIÓN ADMINISTRATIVA

PROCESO CONCURSO DE MÉRITO ABIERTO No. 002-2025 MDN-UGG-DA

ADENDA No. 1

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

La Directora Administrativa de la Unidad de Gestión General del Ministerio de Defensa Nacional, de conformidad con las facultades delegadas por el Ministro de Defensa Nacional en materia contractual, teniendo en cuenta las observaciones realizadas por los interesados, la verificación por parte del estructurador técnico, y de conformidad con lo señalado en el artículo 2.2.1.1.2.2.1 del Decreto 1082 de 2015, y en atención a la respuesta dada en el formulario de preguntas y respuestas No 2, se permite expedir la presente Adenda con el objeto de:

1. Adicionar el numeral ***1.28 Prevención de Corrupción en la Contratación Pública***, verificación de existencia de situaciones de control (el cual el proponente deberá diligenciar el Anexo 21) del pliego de condiciones, así:

En aplicación a lo establecido en el Art. 2.1.4.3.2.1., del Decreto 1600 de 2024, en concordancia con lo dispuesto en los artículos 260 y 261 del código de comercio, las **personas jurídicas oferentes y/o de los proponentes plurales**, que se presenten **como proponentes** en éste proceso de selección, en el término **máximo de tres (3) días** después del momento en que se cierre definitivamente la presentación de ofertas, deberán poner de presente la existencia o no de situaciones de control de las personas jurídicas que participen y, en particular, si son controlantes, controladas o comparten alguna de estas condiciones con otras personas que se encuentren participando en éste mismo proceso de contratación. Para el caso de los proponentes plurales, deberán indicar si las personas jurídicas que los conforman se encuentran en alguna de las situaciones descritas anteriormente.

En este sentido, los proponentes deberán allegar **por mensaje a través de la plataforma secop II** en el proceso de selección, **certificación suscrita por el representante legal**, en la cual se señale la existencia o no de las citadas situaciones. Lo anterior, en el término **máximo de tres (3) días** después del cierre definitivo parar la presentación de ofertas, conforme al cronograma establecido para el mismo.

2. Modificar el numeral 3.2. ***"REQUISITOS HABILITANTES DEL EQUIPO MÍNIMO DE TRABAJO"***, en el perfil del arquitecto de seguridad, así:

3.2.1.	**CONDICIONES DE EXPERIENCIA DEL PERSONAL ASIGNADO AL CONTRATO** • **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, **electrónico** o afines según el NBC de Ingeniería de Sistemas, Telemática y Afines **y/o de Ingeniería Electrónica, Telecomunicaciones y Afines.** Posgrado en la modalidad de especialización o maestria 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.

3. Modificar en el **ANEXO 2 "ANEXO TÉCNICO" ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS** en el numeral **3.11 CONDICIONES DE EXPERIENCIA DEL PERSONAL ASIGNADO AL CONTRATO** en la descripción del perfil profesional del arquitecto de seguridad, el cual se aportara con la presente adenda.

Los cambios y ajustes adoptados mediante la presente adenda se evidencian en el documento denominado **ANEXO No. 2 "FICHA TECNICA – ADENDA No 1"** y **Anexo 21 "PREVENCIÓN DE CORRUPCIÓN EN LA CONTRATACIÓN PÚBLICA".**

Las demás condiciones no modificadas o aclaradas con la presente adenda conservan plena vigencia.

Bogotá, D.C., 17 de octubre de 2025.

NORA ESPERALDA CARRERO MILLAN
Directora Administrativa

Revisó: Abogado Dirección Administrativa
Elaboró: Nubia Marcela Monsalve Guiza – Abogada contratista Grupo Adquisiciones

ANEXO 2 "ANEXO TÉCNICO – Adenda No. 1"

ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS

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 descrito en el numeral 3.11 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, 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.

MINISTERIO DE DEFENSA NACIONAL
UNIDAD DE GESTION GENERAL
DIRECCION ADMINISTRATIVA
Grupo Adquisiciones

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 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. 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. • **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. 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).

MINISTERIO DE DEFENSA NACIONAL
UNIDAD DE GESTION GENERAL
DIRECCION ADMINISTRATIVA
Grupo Adquisiciones

	• 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. - 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. - 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: • ¿Quién informa a quién? • ¿Con qué frecuencia? • ¿Por qué canal?

MINISTERIO DE DEFENSA NACIONAL
UNIDAD DE GESTION GENERAL
DIRECCION ADMINISTRATIVA
Grupo Adquisiciones

	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 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.
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.

MINISTERIO DE DEFENSA NACIONAL
UNIDAD DE GESTION GENERAL
DIRECCION ADMINISTRATIVA
Grupo Adquisiciones

	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 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.
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, **electrónico** o afines según el NBC de Ingeniería de Sistemas, Telemática y Afines **y/o de Ingeniería Electrónica, Telecomunicaciones 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** 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 Título de posgrado en modalidad de Maestría en Seguridad de Tecnologías de la Información Conocimiento en regulaciones locales como Ley 1581/2012, Decreto 1078/2015 y/o políticas de gobierno digital.

MINISTERIO DE DEFENSA NACIONAL
UNIDAD DE GESTION GENERAL
DIRECCION ADMINISTRATIVA
Grupo Adquisiciones

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).

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.

	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 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 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

MINISTERIO DE DEFENSA NACIONAL
UNIDAD DE GESTION GENERAL
DIRECCION ADMINISTRATIVA
Grupo Adquisiciones

	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 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 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).

Se solicita que la información contenida en el presente Anexo No. 2 "Especificaciones técnicas mínimas exigidas" NO sea modificada por el oferente, ya que estas especificaciones técnicas son exigidas por la Entidad, y por tanto SON DE OBLIGATORIO CUMPLIMIENTO POR LOS OFERENTES, la cuales deberán adjuntar con la oferta.

CONCURSO DE MERITOS ABIERTO No. XXX-2025-MDN-UGG-DA
ANEXO No. 21

PREVENCIÓN DE CORRUPCIÓN EN LA CONTRATACIÓN PÚBLICA. VERIFICACIÓN EXISTENCIA DE SITUACIONES DE CONTROL

_____,identificado con cédula de ciudadanía No_____en calidad de representante legal de_____ identificado con Nit._____en mi calidad representante legal del proponente _____dentro del proceso de CONCURSO DE MERITOS ABIERTO No. XXX-2025-MDN-UGG-DA, suscribo de manera unilateral la presente manifestación y declaro bajo la gravedad del juramento:

Manifiesto que una vez verificada la lista de proponentes que presentaron oferta dentro del presente proceso de selección, he podido constatar que dentro del presente proceso SI ( ) NO ( ) se encuentra participando persona jurídica alguna que ejerza o con la cual me encuentre en situación de control empresarial (controlantes, controladas o con la cual se comparta alguna de estas condiciones con otras personas que se encuentren participando en éste mismo proceso de contratación). **Para el caso de los proponentes plurales, deberán indicar claramente si las personas jurídicas que los conforman se encuentran en alguna de las situaciones descritas anteriormente.**

(En el evento de marcar SI (X) a continuación deberá diligenciar e indicar el nombre de la(s) personas jurídicas que participan en el presente proceso de selección y con las cuales se encuentre en situación de control empresarial (controlantes, controladas o con la cual se comparta alguna de estas condiciones con otras personas que se encuentren participando en éste mismo proceso de contratación).

NOMBRE CONTROLANTE O CONTROLADA: _____

Firma Representante legal del Oferente
Nombre:

Este formato NO lo deben presentar con la oferta, para el efecto los proponentes deberán allegarlo por mensaje a través de la plataforma secop II en el proceso de selección, previo diligenciamiento y suscrito por el representante legal, en la cual se señale la existencia o no de las citadas situaciones, dentro de los tres (3) días siguientes al cierre definitivo parar la presentación de ofertas, conforme al cronograma establecido para el mismo.

MINISTERIO DE DEFENSA NACIONAL
UNIDAD DE GESTION GENERAL
DIRECCION ADMINISTRATIVA
Grupo Adquisiciones

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