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

Los bienes y/o servicios a adquirir a través del proceso de selección deberán cumplir con las siguientes especificaciones técnicas mínimas:

<table>
<tr><td colspan="2">Para el desarrollo del objeto a contratar el oferente puede ser las personas jurídicas legalmente constituidas que, de conformidad con su objeto social o actividades registradas, se encuentren facultadas para prestar servicios de formación, capacitación y/o certificación técnica relacionados con el objeto del proceso, y que acrediten el cumplimiento de los requisitos jurídicos, técnicos y de experiencia establecidos por la Entidad.</td></tr>
<tr><th>ÍTEM</th><th>DESCRIPCIÓN</th></tr>
<tr><td>1. Generalidades</td><td>1. TIPO DE FORMACIÓN: Curso de formación en Transformación Digital del sector defensa – ciberseguridad y ciberdefensa para operaciones en el ciberespacio, desarrollado en modalidad virtual y estructurado sobre las normas técnicas que establezcan los lineamientos para la realización de operación de ciberseguridad y ciberdefensa, sistemas de gestión de la seguridad de la información, ciberseguridad y gestión de incidentes, para fortalecer las capacidades del personal y garantizar el cumplimiento de las regulaciones sectoriales y de las mejores prácticas internacionales para el sector defensa.

2. MODALIDAD DE LA PRESTACIÓN DEL SERVICIO: El Ministerio de Defensa Nacional requiere que el proveedor tenga la capacidad académica, logística y organizacional para realizar un curso de formación:

▪ Modalidad: La entidad prestadora del servicio deberá disponer de los medios requeridos para la realización del curso de formación en modalidad virtual asincrónica, con el cumplimiento de los requisitos emitidos para tal modalidad. El Curso de formación incluirá seis (6) conferencias sincrónicas, cada una de una (1) hora académica, dictadas en tiempo real por los docentes designados y grabadas para consulta posterior de los participantes.

▪ Laboratorio: El Curso de formación deberá contener como mínimo veinticuatro (24) horas de ejercicios prácticos, del total de las 120 horas académicas, concentradas en el módulo de Estándares técnicos y distribuidas, según acuerdo con la supervisión del contrato, entre las normas ISO/IEC 27001:2022 Lead Auditor, ISO/IEC 27032:2023, ISO/IEC 27005:2022 e ISO/IEC 27035-1 y -2:2023, desarrollados en laboratorios virtuales o entornos simulados accesibles de forma remota desde</td></tr>
</table>

	la plataforma de aprendizaje. Entre las partes se podrá pactar un mayor número de horas de laboratorio. ▪ Idioma: El lenguaje oficial para impartir el Curso de formación es el idioma español. ▪ **Plataforma tecnológica:** Se deberá disponer de manera permanente de una plataforma de aprendizaje virtual (LMS) provista por el contratista, disponible las veinticuatro (24) horas del día, la cual debe contar con todos los elementos técnicos, tecnológicos y logísticos de calidad y con un ambiente académico apropiado para la realización del curso de formación, así como con soporte técnico y mesa de ayuda durante toda la ejecución del contrato. La plataforma, sus licencias, la capacidad de almacenamiento, la herramienta de videoconferencia y la conectividad requerida serán suministradas, administradas y sostenidas por el contratista, a su costo y riesgo, sin que el Ministerio de Defensa Nacional deba aportar infraestructura tecnológica alguna. El contratista deberá garantizar la conexión simultánea de la totalidad de los participantes, la grabación de las conferencias sincrónicas y el registro de trazabilidad de accesos y avance académico para efectos de supervisión. El contratista con la presentación de la oferta presentará al MDN la propuesta de plataforma tecnológica que cumple con los requisitos exigidos para la ejecución del presente contrato. ▪ **Sesiones teóricas:** Facilitar y poner a disposición de cada participante los contenidos audiovisuales asincrónicos, el aula virtual, el tablero digital, la herramienta de videoconferencia para el desarrollo de las conferencias sincrónicas y los demás elementos o materiales que sean necesarios para el desarrollo de las sesiones teóricas. ▪ **Sesiones prácticas:** Contar con entornos de aprendizaje virtuales para la realización de las actividades de práctica de auditoría, los cuales deben disponer de laboratorios remotos con las características técnicas mínimas para el desarrollo de los ejercicios. **3. ELEMENTOS PARA LOS BENEFICIARIOS:** La entidad prestadora del servicio debe entregar a cada uno de los participantes, los siguientes elementos: • Información acerca del curso de formación. • Presentaciones de las clases. • Información adicional de consulta.

	• Material de lectura y práctica para las sesiones de clase, en formato digital descargable, incluidas las normas técnicas requeridas para el desarrollo de las actividades. • Credenciales de acceso individuales a la plataforma de aprendizaje y a los laboratorios virtuales propuestos para la ejecución de los ejercicios prácticos. Esta información deberá entregarse en formato digital a cada uno de los participantes, junto con una copia en medio magnético para el supervisor del objeto contractual.
2. Aspectos Funcionales y de Coordinación	El futuro contratista deberá garantizar el cumplimiento de: • Suministrar elementos básicos para el desarrollo de las actividades académicas. • Los talleres y demás materiales que se requieran para el debido desarrollo de las clases serán suministrados en formato digital a cada uno de los participantes. • Mesa de ayuda y soporte técnico permanente para los participantes durante el desarrollo de las jornadas académicas. • La disponibilidad permanente de los contenidos asincrónicos en la plataforma durante toda la ejecución del contrato y por un término mínimo de tres (3) meses posteriores a su finalización. • Un coordinador académico con disponibilidad de tiempo permanente, encargado de solucionar los aspectos educativos, logísticos y técnicos en los tiempos previstos en la presente ficha técnica, quien tendrá comunicación directa con el supervisor del contrato. • Las conferencias sincrónicas se programarán en jornada laboral, entre las 08:00 y las 12:00 o entre las 13:00 y las 17:00, de lunes a viernes, previa concertación con el supervisor del contrato. Los contenidos asincrónicos estarán disponibles de manera permanente para consulta de los participantes. • Flexibilidad en el cambio de horarios que por caso fortuito o fuerza mayor impida el desarrollo de las jornadas programadas, previa coordinación con el supervisor del contrato. • Entregar al supervisor del contrato, en medio físico o digital con firma electrónica verificable, las certificaciones originales de la asistencia al curso de formación contratado de cada uno de los participantes que aprueben la capacitación. **PERFIL** • Funcionarios de la Fuerza Pública (EJC-ARC-FAC-PONAL), del Ministerio de Defensa o entidades descentralizadas. • Que no se encuentren pendientes de retiro del servicio activo.

	• Que laboren o se encuentren proyectados para laborar en áreas relacionadas con tecnología, ciberseguridad y/o ciberdefensa se encuentre proyectado para laborar en áreas relacionadas con Tecnología, Ciberseguridad y/o Ciberdefensa de las Fuerzas Militares, Policía Nacional, Unidad de Gestión General y entidades descentralizadas del sector defensa. **INTENSIDAD HORARIA MÍNIMA REQUERIDA** • 120 horas académicas, distribuidas entre los módulos señalados en el numeral 3. Aspectos Técnicos Específicos. • Plazo de ejecución de un (1) mes y medio, mediante contenidos asincrónicos disponibles en la plataforma de aprendizaje y seis (6) conferencias sincrónicas de una (1) hora académica cada una. Las sesiones sincrónicas y asincrónicas se desarrollarán en un único bloque para la totalidad de los participantes, sin conformación de grupos, para un total de hasta 100 participantes. **NÚMERO Y TAMAÑO DE LOS GRUPOS** • No se requiere la conformación de grupos: las sesiones sincrónicas y asincrónicas se desarrollarán con la totalidad de los participantes en un mismo bloque. El contratista deberá garantizar que la plataforma soporte la conexión simultánea de hasta 100 participantes y su capacidad logística y de manejo de audiencia, para dar cumplimiento en óptimas condiciones. • El curso de formación se ofertará para un total de hasta 100 participantes en un único grupo.	
3. Aspectos Técnicos Específicos	**CONTENIDOS ESPECÍFICOS DEL CURSO DE FORMACIÓN EN *TRANSFORMACIÓN DIGITAL DEL SECTOR DEFENSA – CIBERSEGURIDAD Y CIBERDEFENSA* PARA OPERACIONES EN EL CIBERESPACIO.** Se requiere que el personal beneficiario se capacite y se apropie de los seis (6) módulos relacionados a continuación:	
	Tema 1. Transformación digital en las operaciones del sector defensa – contexto: conceptos, habilitadores tecnológicos y efectos de la transformación digital en las operaciones militares y policiales; gobierno y transformación digital del Estado y su aplicación al sector defensa; casos de uso.	12 horas

	Tema 2. Ciberseguridad y ciberdefensa: respeto de las normas en las operaciones en el ciberespacio: marco jurídico nacional e internacional aplicable a las operaciones en el ciberespacio, derecho internacional humanitario, política nacional de ciberseguridad y ciberdefensa, y límites legales de la respuesta ante incidentes cibernéticos.	12 horas
	Tema 3. Infraestructuras críticas cibernéticas: identificación, clasificación y priorización de las infraestructuras críticas cibernéticas nacionales; análisis de interdependencias, protección de tecnologías de operación (OT/ICS) y planes de continuidad y resiliencia.	12 horas
	Tema 4. Inteligencia artificial aplicada a operaciones de defensa nacional: fundamentos y tipologías de sistemas de inteligencia artificial; casos de uso en apoyo a la toma de decisiones, analítica de datos e inteligencia operacional; gestión de los riesgos asociados a los sistemas de IA y marcos de referencia aplicables; y consideraciones éticas, jurídicas y de control humano en el empleo de la inteligencia artificial en el sector defensa.	12 horas
	Tema 5. Estándares técnicos: implementación, auditoría y gestión de la seguridad de la información conforme a las normas ISO/IEC aplicables al sector defensa. Este módulo comprende las siguientes normas y contenidos y concentra las veinticuatro (24) horas de laboratorio del curso: • ***ISO/IEC 27001:2022*** – Lead Auditor: introducción, principios y conceptos de sistemas de gestión de la seguridad de la información; estructura de la norma; implementación y verificación de los controles técnicos del Anexo A y de su guía ISO/IEC 27002:2022; gestión de un programa de auditoría; y simulaciones de auditoría y evaluaciones de seguridad en las que los participantes identificarán hallazgos y formularán planes de acción. Incluye doce (12) horas de laboratorio. • ***ISO/IEC 27032:2023***: ciberseguridad en el contexto de la defensa, gestión de incidentes y estrategias de protección frente a amenazas cibernéticas; procedimientos de detección, respuesta y recuperación; e intercambio de	60 horas

	información para anticipar posibles ataques. Incluye tres (3) horas de laboratorio. • ***ISO/IEC 27005:2022***: metodologías y herramientas para la gestión de riesgos; identificación, clasificación y evaluación de los riesgos y de los activos relevantes, determinando las amenazas y vulnerabilidades. Incluye tres (3) horas de laboratorio. • ***ISO/IEC 27035-1:2023 e ISO/IEC 27035-2:2023***: gestión de incidentes de seguridad de la información; detección, clasificación y evaluación de incidentes, contención y mitigación, y definición de roles y responsabilidades dentro del equipo de respuesta. Incluye tres (3) horas de laboratorio. Se deberá certificar a los beneficiarios en cada una de las temáticas.	
	Tema 6. Marco de Ciberseguridad del NIST (NIST CSF) v2.0: directrices para gestionar los riesgos de seguridad cibernética. Conocer el marco de referencia en ciberseguridad CSF 2.0 como complemento documental para los procesos de certificación de la norma ISO/IEC 27001. • Conocer la importancia de la gobernanza para establecer la postura de ciberseguridad de las organizaciones.	12 horas
4. Certificaciones	• Se debe otorgar a los participantes un certificado de aprobación por cada uno de los seis (6) módulos que integran el curso y un certificado general de aprobación del curso de formación, en el cual se evidencie que los participantes cumplieron con los objetivos académicos establecidos en el Curso de formación . • La entidad prestadora del servicio deberá hacer entrega al Ministerio de Defensa Nacional de las copias de los diplomas y/o certificados entregados a los participantes que hayan completado como mínimo el 80% de las actividades y contenidos del curso, verificado mediante los reportes de avance y trazabilidad de la plataforma de aprendizaje y que hayan cumplido con los requisitos contemplados para la aprobación del curso de formación.	
5. Informes de Ejecución	• El contratista deberá entregar un informe que resuma lo realizado, que incluya los reportes de avance y trazabilidad de la plataforma por participante, los listados de asistencia a las conferencias sincrónicas, copias de los certificados entregados a los	

	participantes, las memorias, presentaciones y encuestas de satisfacción. • La entidad prestadora del servicio deberá dar cumplimiento a la normatividad vigente y aplicable para la realización del curso de formación requerido, la emisión de todos los certificados y los demás aspectos aplicables.
6. Idoneidad de los Docentes	La habilitación técnica del curso de formación recae íntegramente en el equipo de docentes, cuya idoneidad deberá acreditarse documentalmente con la oferta. Para el cumplimiento del presente objeto contractual se requiere personal que esté capacitado, certificado y con experiencia, el cual deberá cumplir con los siguientes requisitos: • Título universitario en áreas afines, como: Ingeniería en Sistemas, Informática, Telecomunicaciones, Seguridad de la Información o Ciberseguridad, Administración con énfasis en Gestión de Riesgos o Auditoría o Derecho con especialización en protección de datos, ciberseguridad, ciberdefensa nacional, tecnologías o seguridad informática. • Estudios de posgrado, especialización o maestría o doctorado en: tecnologías y servicios de la sociedad de la información, ciberseguridad, ciberdefensa, seguridad de la información, gestión de riesgos tecnológicos o auditoría de tecnologías de la información. • Para los módulos de Transformación digital, Ciberseguridad y ciberdefensa – normas en el ciberespacio, Infraestructuras críticas cibernéticas e Inteligencia artificial aplicada a operaciones de defensa nacional, el docente asignado deberá acreditar título profesional y posgrado en derecho, ciberseguridad, ciberdefensa, políticas públicas o tecnologías de la información, y experiencia certificada de mínimo cinco (5) años en asesoría, docencia o gestión en dichas materias en el sector público o de Defensa. • A cada uno de los profesionales asignados a las sesiones técnicas de normas ISO se le exigirá estar certificado como mínimo en una (1) de las siguientes: i) para las sesiones de ISO: Auditor Interno ISO/IEC 27001:2022; Auditor Líder ISO/IEC 27001:2022; o auditor en entornos tecnológicos, ciberdefensa, seguridad de la información, gestión de riesgos tecnológicos o auditoría de tecnologías de la información, siempre que la certificación se encuentre vigente; y contar con más de tres (3) años de experiencia en el sector; ii) para las demás sesiones tener mínimo de 3 años de experiencia docente en inteligencia artificial, ciberseguridad, ciberdefensa, gobierno digital y contar con más de tres (3) años de experiencia en el sector.

	• Cada uno de los profesionales que sean asignados para realizar el curso de formación podrá acreditar, como certificaciones complementarias que no sustituyen el requisito de certificación mínima antes señalado, entre otras: CISM (Certified Information Security Manager) – Enfoque en gestión de seguridad de la información, CISSP (Certified Information Systems Security Professional) – Seguridad avanzada y buenas prácticas, CISA (Certified Information Systems Auditor) – Enfoque en auditoría de TI y SGSI o ISO 22301:2019 Auditor o Implementador – para gestión de continuidad del negocio, Auditor de entornos tecnológicos, doctorado en tecnologías o máster en ciberseguridad, ciberdefensa, seguridad de la información, gestión de riesgos tecnológicos o auditoría de entornos tecnológicos o de tecnologías de la información. Los títulos de posgrado mencionados en este literal se acreditan como formación académica y podrán aportarse también para el requisito de posgrado previsto anteriormente. • Experiencia específica: cada profesional asignado a las sesiones técnicas de normas ISO/IEC deberá acreditar experiencia en auditoría o implementación de ISO/IEC 27001 y al menos una (1) participación en ISO/IEC 27001:2022, en calidad de auditor interno, auditor líder o implementador, indistintamente o ser docente de ciberseguridad y ciberdefensa, o de inteligencia artificial, . Esta experiencia podrá acreditarse mediante certificación del contratante o empleador o mediante constancia suscrita por el representante legal del oferente, en la que se indique el rol desempeñado y la versión de la norma. Para las demás sesiones podrá acreditar experiencia específica a través de certificaciones en cursos, clases, consultorías, de transformación digital del sector público. • Deberá contar con la tarjeta profesional vigente en caso de que su profesión lo exija. • El personal que sea designado para realizar el curso de formación deberá contar con vinculación comercial, civil o laboral con la entidad prestadora del servicio y se deberá aportar certificado de existencia y representación legal de la empresa en el que figure su actividad comercial. • Los docentes asignados deberán acogerse a la propuesta aprobada y desarrollar los temas específicos a tratar dentro de cada módulo, la programación en horas por cada tema a tratar en la capacitación durante los días concertados con la Entidad, detallando las actividades que se realizarán en cada sesión. • Garantizar el desarrollo del curso de formación en caso de ausencia del docente designado inicialmente, por otro docente que cumpla con los mismos requisitos exigidos. • Contar con el equipo de apoyo que garantice la logística para el desarrollo y la calidad de la transferencia de conocimiento.

	• El contratista deberá allegar junto con la presentación de la oferta, las hojas de vida del personal docente designado para la ejecución del presente objeto contractual.

Elaboro: TC. Correa Luz - CSIRT
VoBo: TC. Barragán Diana - Coordinadora Grupo de Educación DDFP
Revisado: OPS. Dayra Moreno - Asesora Contractual DDFP