Agencia Nacional Digital

PROPUESTA TÉCNICA - RED EMPRESARIAL

AGENCIA NACIONAL DIGITAL - AND

DIRIGIDO A: ColCERT

BOGOTÁ D.C., ENERO DE 2026

CONTENIDO

Control de revisiones 3
1. NOMBRE DEL PROYECTO 4
2. PARTICIPANTES 4
3. INTERLOCUCIÓN PARA LA FORMULACIÓN DEL PROYECTO 4
4. CONFIDENCIALIDAD 4
5. OBJETIVOS 5
5.1 Objetivo general 5
5.2 Objetivos Específicos 5
6. JUSTIFICACIÓN 6
7. DESCRIPCIÓN GENERAL DE LA SOLUCIÓN 7
8. ALCANCE DE LA PROPUESTA 8
9. TIEMPO Y FASES DEL PROYECTO 13
10. METODOLOGÍA DE EJECUCIÓN 14
11. ENTREGABLES 15
12. CRONOGRAMA 17
13. COSTOS DEL PROYECTO 17
14. RIESGOS 18
15. Exclusiones del Proyecto 21
16. Condiciones para el Desarrollo del Proyecto 23
17. Acuerdo de niveles de servicio ANS 25
18. Cierre del Proyecto 26

Control de revisiones

Descripción	Responsable	Subdirección	Fecha
Revisión Técnica	Julio Echavarría	Desarrollo y SCD	28/01/2026
Revisión Financiera	Diana Moya	Financiera y Administrativa	28/01/2026
Revisión Comercial	Víctor Botero	Soluciones y Servicios	28/01/2026
Revisión Jurídica	Paula Ricaurte	Jurídica	28/01/2026

Tabla 1 Control de revisiones

1. NOMBRE DEL PROYECTO

Implementación del modelo Ciberseguridad 360 para el fortalecimiento de las capacidades institucionales de ColCERT.

2. PARTICIPANTES

Entidad contratante:

ColCERT, en su calidad de entidad responsable de la supervisión, coordinación y validación de los entregables del proyecto, conforme a lo establecido en el Anexo Técnico.

Entidad contratista:

Agencia Nacional Digital – AND, a través de la Subdirección de Desarrollo y Servicios Ciudadanos Digitales.

3. INTERLOCUCIÓN PARA LA FORMULACIÓN DEL PROYECTO

Por parte de ColCERT, la interlocución para la formulación, coordinación y validación del proyecto estará a cargo del equipo designado por la entidad, responsable de definir los lineamientos, requerimientos y prioridades institucionales, así como de realizar la revisión y validación de los entregables, conforme a lo establecido en el Anexo Técnico.

Por parte de la Agencia Nacional Digital – AND, la interlocución se realizará a través de la Subdirección de Desarrollo y Servicios Ciudadanos Digitales, como área responsable de la estructuración técnica de la propuesta, la coordinación de la ejecución del proyecto y la articulación con el equipo designado por ColCERT.

4. CONFIDENCIALIDAD

La Agencia Nacional Digital – AND se compromete a mantener la confidencialidad de toda la información, documentación, datos y contenidos a los que tenga acceso con ocasión de la formulación y ejecución del proyecto, suministrados por

ColCERT, independientemente de su formato o medio, y a utilizarlos exclusivamente para los fines relacionados con el cumplimiento de las obligaciones contractuales.

De igual forma, ColCERT se compromete a mantener la confidencialidad de la información técnica, metodológica, documental o estratégica suministrada por la Agencia Nacional Digital – AND, que haya sido identificada como confidencial o que, por su naturaleza, deba ser tratada como tal, y a no divulgarla ni utilizarla para fines distintos a los relacionados con la ejecución del proyecto, salvo autorización previa y expresa de AND o requerimiento legal de autoridad competente.

Las partes adoptarán las medidas necesarias para evitar la divulgación, reproducción o uso no autorizado de la información confidencial. Las obligaciones aquí establecidas se mantendrán durante la vigencia del contrato y por el término que este disponga, aun después de su terminación, sin perjuicio del cumplimiento de las disposiciones legales aplicables en materia de protección de datos personales, seguridad de la información y reserva legal.

5. OBJETIVOS

5.1 Objetivo general

Contribuir al ecosistema de las capacidades institucionales de ColCERT en materia de seguridad digital, a través de la habilitación de componentes técnicos y la ejecución de procesos de formación especializada del talento humano, conforme a lo establecido en el Anexo Técnico, con el fin de apoyar la gestión de riesgos cibernéticos y la protección de los activos digitales bajo su responsabilidad institucional.

5.2 Objetivos Específicos

1. Implementar prácticas avanzadas para la protección, prevención y respuesta ante incidentes de ciberseguridad, garantizando el cumplimiento de políticas y lineamientos nacionales.

2. Optimizar el monitoreo y la administración de sistemas de información, incorporando tecnologías de predicción de demanda que faciliten la toma de decisiones y la resiliencia institucional.
3. Fortalecer las competencias técnicas y operativas de entidades frente a los riegos durante los procesos electorales en materia de seguridad digital.
4. Desarrollar y consolidar capacidades técnicas básicas y/o avanzadas en las entidades beneficiarias, mediante programas de formación certificados y actividades prácticas que eleven la preparación frente a riesgos y amenazas digitales.
5. Garantizar la trazabilidad, seguimiento y certificación de los procesos de formación y simulación, mediante la generación de informes estructurados y la retroalimentación continua de los participantes y aliados estratégicos.

6. JUSTIFICACIÓN

La presente propuesta se fundamenta en la necesidad identificada por ColCERT de fortalecer sus capacidades institucionales en materia de seguridad digital, en un contexto caracterizado por el incremento y sofisticación de las amenazas cibernéticas, la creciente dependencia de los servicios digitales y las obligaciones normativas aplicables a las entidades del sector público colombiano. De acuerdo con los análisis y lineamientos definidos por la entidad, resulta prioritario adoptar un enfoque estructurado que permita mejorar la gestión de riesgos cibernéticos y apoyar la protección de los activos digitales bajo su responsabilidad institucional.

Como respuesta a este contexto, el Ministerio de Tecnologías de la Información y las Comunicaciones definió la iniciativa Ciberseguridad 360, concebida para abordar de manera sistemática los desafíos históricos en materia de protección digital. Esta iniciativa se sustenta en una estrategia multidimensional que articula el fortalecimiento de capacidades técnicas mediante la capacitación especializada del talento humano y la actualización e integración de infraestructuras tecnológicas avanzadas, orientadas a optimizar la resiliencia institucional y apoyar la protección eficiente de los activos críticos frente a amenazas cibernéticas emergentes.

En el marco de la iniciativa Ciberseguridad 360, se establecen dos componentes fundamentales. El componente técnico se orienta a fortalecer la infraestructura tecnológica que soporta los servicios asociados al portafolio de ColCERT, contribuyendo a ampliar sus capacidades operativas para anticipar riesgos y

mejorar la eficiencia en la gestión de incidentes de seguridad digital, conforme a los alcances definidos en el Anexo Técnico. De manera complementaria, el componente de formación de talento humano especializado busca desarrollar procesos de formación práctica y certificable, orientados al fortalecimiento de competencias técnicas y a la consolidación de una cultura institucional resiliente y sostenible en ciberseguridad, en respuesta a la demanda creciente de capacidades especializadas en esta materia.

En este contexto, la contratación de la Agencia Nacional Digital – AND se orienta a la implementación del modelo Ciberseguridad 360, de conformidad con los componentes, actividades y alcances establecidos en el Anexo Técnico. La ejecución del proyecto permitirá habilitar las capacidades técnicas y formativas previstas, mediante la configuración y puesta en operación de las herramientas tecnológicas definidas, la ejecución de los procesos de formación correspondientes y el acompañamiento técnico durante el periodo contractual, sin que ello implique la sustitución de las funciones misionales de ColCERT ni la asunción de responsabilidades que excedan el alcance del contrato.

Adicionalmente, el proyecto se encuentra alineado con los lineamientos de la Estrategia Nacional de Seguridad Digital, particularmente en lo relacionado con el fortalecimiento de capacidades institucionales, la gestión de riesgos cibernéticos, el uso eficiente de herramientas tecnológicas y la mejora continua de los procesos asociados a la seguridad digital. La implementación del modelo Ciberseguridad 360 contribuirá a que ColCERT avance en el fortalecimiento de su madurez institucional en esta materia, en coherencia con sus prioridades y capacidades internas.

En consecuencia, la presente propuesta responde a una necesidad real, actual y verificable de ColCERT, y se orienta a apoyar el cumplimiento de sus objetivos institucionales mediante la implementación de una estrategia integral de seguridad digital, ejecutada bajo un marco contractual claro, delimitado y alineado con el Anexo Técnico aprobado.

7. DESCRIPCIÓN GENERAL DE LA SOLUCIÓN

La solución adopta un enfoque estructurado, progresivo y controlado, que articula dos componentes estratégicos: 1)un componente técnico y 2) un componente uso y apropiación a través de la formación de capacidades especializadas, todo ello orientado al fortalecimiento de las capacidades institucionales de ColCERT, en materia de seguridad digital, sin sustituir sus funciones misionales ni asumir responsabilidades que excedan el alcance contractual.

El componente técnico se orienta al licenciamiento, configuración de las herramientas tecnológicas con el propósito de apoyar los procesos de monitoreo, análisis, gestión y mitigación de riesgos cibernéticos, contribuyendo al fortalecimiento de la capacidad operativa de ColCERT durante el periodo de ejecución del proyecto.

El componente de Uso y Apropiación contempla la ejecución de programas de formación en ciberseguridad, dirigidos a los públicos definidos por ColCERT, conforme a las rutas de formación, contenidos, modalidades, cronogramas y metas establecidas en el Anexo Técnico. Dichos programas están orientados al fortalecimiento de competencias técnicas especializadas y a la apropiación de buenas prácticas en seguridad digital.

Adicionalmente, la solución incorpora de manera transversal actividades de comunicación, seguimiento, control conforme las metodologías consideradas como parte de las buenas prácticas en la administración de proyectos. Estas actividades permiten verificar el avance de la ejecución, asegurar la calidad y oportunidad de los entregables, y garantizar la trazabilidad y transparencia.

8. ALCANCE DE LA PROPUESTA

El alcance de la propuesta se consolida en la siguiente matriz:

Componente	Elemento del alcance	Descripción del alcance
Componente Técnico de Seguridad Digital	Fortalecimiento de la Infraestructura Tecnológica	Configuración y habilitación de las siguientes herramientas: Gestión temprana de vulnerabilidades (Tenable One): Permite visibilidad integral de activos, configuraciones inseguras y puntos críticos; su renovación fortalece la postura de seguridad del Estado y reduce brechas explotables. • Detección y respuesta ante amenazas (Trellix): Plataforma que identifica comportamientos anómalos, bloquea malware avanzado y contiene ataques; clave para mantener la continuidad operativa y apoyar entidades sin tecnología propia. • Protección DNS (Cisco Umbrella): Actúa como defensa temprana bloqueando conexiones maliciosas, reduciendo phishing y exfiltración de

Componente	Elemento del alcance	Descripción del alcance
		datos; esencial en contextos de alto tráfico como procesos electorales. • Mitigación de ataques DDoS (Cloudflare): Proporciona protección contra denegación de servicio y mejora la estabilidad y rendimiento de servicios críticos durante picos de consultas. • Plataforma de comunicaciones (Mailchimp): Facilita envío masivo y segmentado de alertas, boletines y mensajes institucionales confiables; crucial para contrarrestar desinformación. • Laboratorio de simulación y pruebas (VMware ESXi/vCenter): Permite ejecutar análisis, ejercicios y pruebas sin comprometer producción; su renovación garantiza continuidad y preparación técnica. • Capacidad forense digital (MAGNET AXIOM Cyber + Torre Forense): Habilita adquisición remota de evidencia, análisis profundo y generación de reportes con cadena de custodia; fundamental en incidentes durante procesos electorales. • Videowall del Centro de Operaciones: Es vital para la visualización situacional y coordinación con el PMU Cyber Electoral; requiere soporte y mantenimiento para garantizar operación continua. • Servicio MDR con CrowdStrike: Proporciona monitoreo continuo 24/7, caza de amenazas y contención inmediata; reduce significativamente los tiempos de detección (MTTD) y respuesta (MTTR), fortaleciendo la defensa estatal.
Componente Técnico de Seguridad Digital	Plataforma de vigilancia y monitoreo continuo (MDR)	Implementar una plataforma integral de detección y respuesta 24/7, capaz de cubrir 2000 activos de TI. • Integrar las fuentes de telemetría: EDR/XDR, DNS seguro, análisis de vulnerabilidades, infraestructura crítica, flujos de red e indicadores de compromiso. • Desplegar completamente la solución MDR: instalación de agentes, reglas, tableros de monitoreo y afinamiento inicial. • Garantizar soporte 24/7, gestión de escalamiento, coordinación con SOC. • Documentar cada incidente desde la detección hasta el cierre y asegurar que toda la información pertenezca al Ministerio TIC.

Componente	Elemento del alcance	Descripción del alcance
		• Entregar informes por entidad, incluyendo análisis, resultados, recomendaciones y reportes forenses cuando corresponda. • Definir y activar estrategias de contingencia y continuidad operativa.
Componente Técnico de Seguridad Digital	Informes estratégicos, métricas y evaluación	Elaborar informes mensuales, trimestrales y de cierre que integren: o Métricas de desempeño. o Indicadores estratégicos. o Análisis de vulnerabilidades e incidentes. o Uso del MDR. o Avances de formación y resultados de las herramientas de gamificación. • Incluir retroalimentación estructurada, análisis de impacto, riesgos y acciones adelantadas con el ColCERT. • Entregar la totalidad de la información generada y recolectada, asegurando que permanezca bajo propiedad exclusiva del Ministerio TIC.
Componente Uso y Apropiación Fortalecimiento en capacidades digitales	Formación Especializada	Programas de capacitación y actualización en seguridad digital. ➢ Desarrollo de habilidades especializadas para prevenir y responder a incidentes. ➢ Impulso al aprendizaje organizativo como medio para fortalecer la democracia. ➢ Plataforma de formación avanzada basada en IA y algoritmos propietarios, para personalizar el aprendizaje y predecir tendencias formativas. ➢ Solución parametrizable, escalable y 100% web, accesible sin instalación desde cualquier navegador. ➢ Incluye retos técnicos en áreas como criptografía, forense, explotación web, pentesting y reversing. ➢ Ofrece formatos de competencia: individual, por equipos, por niveles, tiempo limitado o ranking abierto. ➢ Posee gamificación completa: puntuación automática, rankings, insignias y progresión por niveles. ➢ Puede integrarse con procesos formativos previos y funcionar como herramienta de evaluación post-entrenamiento. ➢ Genera métricas detalladas: análisis por participante, tipo de reto y tiempos de resolución.

Componente	Elemento del alcance	Descripción del alcance
		➢ Incluye administración integral de usuarios, con autenticación segura y mecanismos de recuperación de credenciales. ➢ Provee registro de auditoría exportable, con datos como ID, IP, fechas, horas y eventos. ➢ Garantiza compatibilidad con múltiples dispositivos, sistemas operativos y navegadores. ➢ Gestión centralizada de inscripciones mediante formulario único nacional, con reportes quincenales y apoyo en certificación. ➢ Permite talleres prácticos y laboratorios de simulación durante el proyecto. ➢ Programas de formación de mínimo 40 horas asíncronas impartidos por personal docente especializado, para workshop y webinars entregando certificados a quienes culminen cada nivel y garantizando al menos una clasesincrónica obligatoria, grabada y disponible para consulta posterior. ➢ Enfoque práctico y aplicado, evitando contenidos puramente teóricos mediante ejercicios, laboratorios y competencias simuladas. ➢ Estrategia de formación alineada con los objetivos del plan sectorial TIC. ➢ Actividades clave: talleres, clases sincrónicas, difusión segmentada, integración institucional, monitoreo y retroalimentación continua. Clasificada ➢ Meta de formación: capacitar a 4.000 usuarios en competencias básicas y especializadas (Curso especialista en ciberseguridad, CTF, ciudadanía, profesionales y funcionarios). ➢ Toda comunicación cumple lineamientos de imagen institucional del MinTIC y ColCERT. ➢ Mecanismos rigurosos de seguimiento y mejora continua, con informes periódicos e indicadores de impacto.
Componente Uso y Apropiación Fortalecimiento en capacidades digitales	Programas de formación	Diseñar y ejecutar programas de formación alineados con la Estrategia Nacional de Seguridad Digital, con módulos prácticos • Garantizar disponibilidad en una plataforma web interactiva, funcional durante toda la vigencia contractual. Clasificada • Realizar actividades de difusión y publicidad respetando el manual de identidad del MinTIC. • Entregar certificados digitales y

Componente	Elemento del alcance	Descripción del alcance
		mantener actualizados los registros de beneficiarios conforme a las políticas de datos personales. • Incluir entrenamientos especializados para el personal del Centro de Operaciones del ColCERT. • Alertar al Ministerio sobre amenazas emergentes que puedan afectar la continuidad del servicio formativo.
Componente Transversal	Producción de piezas comunicativas e institucionales	Diseñar piezas de comunicación alineadas con los lineamientos de imagen y accesibilidad del MinTIC y el ColCERT. • Apoyar las actividades del proyecto: formación, campañas de ciberseguridad, notificaciones y mensajes institucionales. • Validar contenido técnico y narrativo en coordinación con el área de comunicaciones. • Incorporar estas piezas en la plataforma de formación y en las estrategias de comunicación para situaciones de riesgo o eventos críticos.
Componente Transversal	Plan de trabajo del proyecto	Documento que consolida el alcance, cronograma, actividades y mecanismos de seguimiento para la ejecución del proyecto, conforme al Anexo Técnico y validado con ColCERT.
Componente Transversal	Esquema de seguimiento y control	Definición de los mecanismos de coordinación, seguimiento y reporte para el control de la ejecución del proyecto.
Componente Transversal	Informes de avance	Informes periódicos que consolidan el avance de la ejecución del proyecto, de acuerdo con los mecanismos de seguimiento establecidos. Métricas de desempeño. Indicadores estratégicos. Análisis de vulnerabilidades e incidentes. Uso del MDR. Avances de resultados de la herramienta de gamificación.
Componente Transversal	Reportes de seguimiento y control	Reportes de métricas y control que permiten verificar el cumplimiento de las actividades previstas durante la ejecución del proyecto.

9. TIEMPO Y FASES DEL PROYECTO

El proyecto se desarrollará de manera estructurada a través de las siguientes fases, iniciando el 01 de febrero del 2026 al 31 de diciembre del 2026 con el fin de garantizar una ejecución ordenada, controlada y alineada con los objetivos definidos:

Fase	Nombre de la fase	Propósito	Actividades principales
Fase 1	Planeación y alistamiento operativo	Establecer las condiciones técnicas, operativas y metodológicas necesarias para la correcta ejecución del proyecto, conforme al Anexo Técnico.	Validación del alcance, cronograma y actividades del proyecto. Definición del plan de trabajo y mecanismos de seguimiento. Alistamiento técnico y operativo de los componentes del proyecto. Articulación inicial con el equipo designado por COLCERT.
Fase 2	Implementación del componente técnico de seguridad digital	Configurar, habilitar y poner en operación las capacidades técnicas del modelo Ciberseguridad 360 definidas en el Anexo Técnico.	Configuración y habilitación de las herramientas tecnológicas previstas. Puesta en operación de las capacidades técnicas de monitoreo y gestión de riesgos. Validación técnica y funcional de los componentes implementados. Acompañamiento técnico durante la ejecución.
Fase 3	Ejecución del componente de uso, apropiación y fortalecimiento de capacidades	Desarrollar las actividades orientadas al uso efectivo, la apropiación y el fortalecimiento de capacidades en seguridad digital, conforme al Anexo Técnico.	Ejecución de actividades de sensibilización. Ejecución de procesos de formación práctica y certificable. Desarrollo y uso de contenidos, laboratorios y competencias prácticas (CTF).
Fase 4	Seguimiento, control y acompañamiento transversal	Realizar el seguimiento y control de la ejecución del proyecto, verificando el avance de las actividades definidas.	Seguimiento a indicadores y métricas del proyecto. Generación de informes periódicos de avance. Acompañamiento técnico y formativo. Ajustes operativos permitidos conforme al Anexo Técnico.
Fase 5	Cierre del proyecto	Formalizar la finalización del proyecto mediante la validación de la ejecución y el cumplimiento de las	Consolidación de resultados de la ejecución. Validación técnica y administrativa con COLCERT. Entrega de reconocimientos según

Fase	Nombre de la fase	Propósito	Actividades principales
		obligaciones contractuales.	el Anexo Técnico. Formalización del cierre del proyecto.

10. METODOLOGÍA DE EJECUCIÓN

La ejecución del proyecto se desarrollará mediante una metodología estructurada, progresiva y orientada a la correcta implementación del modelo Ciberseguridad 360, garantizando el cumplimiento del alcance, las fases y las actividades definidas en el Anexo Técnico.

La metodología se fundamenta en un enfoque por fases y componentes, que permite una ejecución ordenada y controlada del proyecto, articulando el componente técnico de seguridad digital y el componente de uso, apropiación y fortalecimiento de capacidades en seguridad digital. Cada fase se desarrolla bajo criterios de coordinación, trazabilidad y control, facilitando la supervisión y el seguimiento por parte de ColCERT.

En la fase de planeación y alistamiento operativo, se validan el alcance, el cronograma y las actividades del proyecto, y se establecen los mecanismos de coordinación y seguimiento necesarios para su ejecución. Esta fase permite asegurar las condiciones técnicas y operativas requeridas, sin modificar los lineamientos definidos en el Anexo Técnico.

Durante la implementación del componente técnico, la metodología contempla la configuración, habilitación y puesta en operación de las capacidades técnicas previstas, de acuerdo con los parámetros y condiciones establecidos en el Anexo Técnico. Estas actividades se desarrollan bajo criterios de validación técnica y funcional, asegurando la correcta operación de los componentes durante el periodo de ejecución contractual.

De manera complementaria, la ejecución del componente de uso, apropiación y fortalecimiento de capacidades se orienta al desarrollo de actividades de sensibilización, formación práctica y certificable, y ejercicios técnicos, conforme a los públicos, contenidos y modalidades definidos por ColCERT. Este enfoque busca promover el uso efectivo de las capacidades implementadas y la apropiación de buenas prácticas en seguridad digital.

La metodología incorpora de forma transversal actividades de seguimiento, control y acompañamiento, orientadas a verificar el avance de la ejecución, identificar oportunidades de ajuste operativo y asegurar la alineación permanente con el Anexo Técnico. Dicho seguimiento se soporta en la generación periódica de información de avance y en espacios de coordinación con ColCERT.

Finalmente, la metodología contempla una fase de cierre, orientada a la validación de la ejecución del proyecto, la consolidación de los resultados alcanzados y la formalización del cierre contractual, garantizando el cumplimiento integral de las actividades previstas.

11. ENTREGABLES

A continuación, se indican los entregables generales y específicos que deben ser contemplados durante la planeación y ejecución del proyecto por parte del aliado.

El proyecto consolida los siguientes entregables estratégicos diseñados para fortalecer la seguridad digital del Estado:

Componente	Entregable	Descripción del entregable
Componente1: Técnico de Seguridad Digital	Licenciamiento, despliegue y operación de soluciones tecnológicas	Garantizar que las herramientas, plataformas y soluciones de ciberseguridad ofrecidas en la presente propuesta estén debidamente licenciadas, activas y documentadas durante un mínimo de 12 meses.
		Asegurar la entrega oportuna de licencias antes del vencimiento de las existentes, sin generar interrupciones de operación.
		Incluir tecnologías esenciales como Tenable One, Trellix, Cisco Umbrella, Cloudflare, VMware ESXi/vCenter, MDR, Magnet AXIOM Cyber, Mailchimp, Kiteworks y otras soluciones complementarias.
		Activar la membresía FIRST como mecanismo de cooperación internacional en ciberseguridad.
		Desarrollar y entregar un plan completo de soporte, mantenimiento, actualizaciones, escalamiento y evidencia documental.
		Ejecutar transferencia de conocimiento para cada herramienta, impartida por personal certificado, con materiales, prácticas guiadas y evidencias formativas
Componente2: Uso, Apropiación y Fortalecimiento de Capacidades	Plataforma tecnológica de formación configurada y habilitada	Evidencia de la configuración, parametrización y habilitación de la plataforma tecnológica de formación para la ejecución de las actividades de sensibilización, formación práctica, competencias técnicas y gestión de evidencias, conforme a lo establecido en el Anexo Técnico,
Componente2: Uso, Apropiación y Fortalecimiento de Capacidades	Ejecución de actividades de uso y apropiación	Evidencias de la ejecución de actividades de sensibilización, formación práctica, ejercicios técnicos y competencias definidas en el Anexo Técnico.
Componente2: Uso, Apropiación y Fortalecimiento de Capacidades	Registros y métricas de participación	Registros de participación, asistencia y uso de las actividades desarrolladas, conforme a los públicos y metas definidas por ColCERT.
Transversal	Informes de avance	Informes periódicos que consolidan el avance de la ejecución del proyecto, de acuerdo con los mecanismos de seguimiento establecidos.
Transversal	Reportes de seguimiento y control	Reportes de métricas y control que permiten verificar el cumplimiento de las actividades previstas durante la ejecución del proyecto.
Transversal	Informe final del proyecto	Documento consolidado que presenta el desarrollo del proyecto, las actividades ejecutadas y los resultados obtenidos, conforme al alcance definido.
Transversal	Acta de cierre del proyecto	Documento mediante el cual ColCERT valida la finalización de la ejecución del proyecto y el cumplimiento de las obligaciones contractuales.

12. CRONOGRAMA

El cronograma será desarrollado según la etapa de planeación en conjunto con los entregables de esta etapa.

Componente 1: Técnico de seguridad digital

Componente 2: Formación de talento humano especializado

13. COSTOS DEL PROYECTO

El valor total estimado del proyecto asciende a **CINCO MIL NOVECIENTOS MILLONES DE PESOS M/CTE ($5.900.000.000)**, cifra que cubre de manera integral los componentes del proyecto.

Los costos del proyecto se discriminan de la siguiente manera:

No.	COMPONENTE	VALOR TOTAL INCLUIDO IVA
1	TECNICO DE SEGURIDAD DIGITAL	$ 3.800.000.000
2	FORMACIÓN DE TALENTO HUMANO ESPECIALIZADO	$ 2.100.000.000
TOTAL PROYECTO INCLUIDO IVA		$ 5.900.000.000

El valor total del proyecto incluye el Impuesto al Valor Agregado (IVA) y el costo de las pólizas de seguro requeridas para la ejecución del mismo. Esto significa que el monto acordado cubre no solo los costos directos del proyecto, sino también los impuestos y seguros asociados, proporcionando una visión clara y completa del costo total.

Nota1: Es de anotar que el proyecto ha sido estructurado bajo un enfoque integral de ejecución, en el cual los componentes definidos se conciben como partes articuladas de una única solución de fortalecimiento institucional. Este enfoque permite una gestión coordinada de los recursos técnicos, operativos y financieros, facilitando la optimización del uso del presupuesto global del proyecto y la adecuada priorización de actividades entre componentes, de acuerdo con las necesidades reales de la Entidad y los objetivos estratégicos establecidos. En este sentido, la ejecución del proyecto contempla la posibilidad de realizar ajustes

operativos y técnicos internos que contribuyan al cumplimiento del alcance integral, sin afectar el valor total estimado del proyecto ni los resultados esperados.

Nota2: El detalle de los costos proyectados de las líneas del proyecto se encuentran en el anexo "Detalle propuesta económica AND" la cual hace parte del presente anexo

14. RIESGOS

La presente matriz de riesgos identifica, clasifica y asigna las posibles contingencias que pueden afectar el desarrollo del proceso contractual, abarcando tanto la etapa precontractual como la fase de ejecución. Su propósito es anticipar eventos que puedan impactar el alcance, los costos, los tiempos y la calidad del contrato, permitiendo establecer medidas de prevención, mitigación y control acordes con la naturaleza del proyecto. Este instrumento facilita la toma de decisiones informada, promueve la adecuada distribución de responsabilidades entre las partes y contribuye a garantizar la continuidad, eficiencia y transparencia en la gestión contractual.

ETAPA PRECONTRACTUAL							
Clasificación	Riesgo	Causa	Responsable	Tipo	Controles	Impacto	Evaluación
Operativo	Definición incompleta o ambigua del alcance del convenio	Levantamiento insuficiente de requerimientos técnicos y operativos	AND - ColCERT	Operativo / Técnico	Revisión técnica interáreas, validación con ColCERT, mesas de trabajo previas	Alto	Alto
Operativo	Desalineación entre los componentes del convenio	Falta de articulación entre equipos técnicos, jurídicos y financieros	AND – PMO	Operativo / Contractual	Revisión cruzada de documentos, comité de aprobación	Alto	Alto

ETAPA PRECONTRACTUAL							
Clasificación	Riesgo	Causa	Responsable	Tipo	Controles	Impacto	Evaluación
Operativo	Retrasos en la aprobación del proceso contractual	Dependencias administrativas o jurídicas externas	AND - ColCERT	Operativo / Administrativo	Anexo técnico, propuesta económica, matriz de riesgos	Moderado	Extremo
Operativo	Definición inadecuada de roles y responsabilidades	Ambigüedad en la gobernanza del convenio	AND - ColCERT	Operativo	Matriz RACI, modelo de gobierno del proyecto	Moderado	Moderado
Técnico	Requisitos técnicos insuficientes	Falta de estandarización técnica	AND - ColCERT	Técnico	Definición de requisitos mínimos y estándares técnicos Anexo y criterios de aceptación	Moderado	Moderado
Seguridad de la información	Cláusulas insuficientes de seguridad	Omisión de obligaciones específicas	AND - ColCERT	Seguridad de la información	Inclusión de cláusulas de confidencialidad y protección de datos.	Alto	Alto

Técnicos

ID	Riesgo identificado	Descripción del riesgo	Probabilidad	Impacto	Estrategia de mitigación
R1	Retrasos en la articulación institucional	Posibles demoras en la coordinación, validación o aprobación de actividades por parte de los actores designados por COLCERT.	Media	Media	Definición temprana de canales de comunicación, cronograma acordado y espacios periódicos de seguimiento.

ID	Riesgo identificado	Descripción del riesgo	Probabilidad	Impacto	Estrategia de mitigación
R2	Disponibilidad limitada de información	Restricciones en el acceso oportuno a información técnica o insumos requeridos para la ejecución de las actividades definidas en el Anexo Técnico.	Media	Media	Coordinación previa con COLCERT para definir responsables, tiempos y condiciones de acceso a la información.
R3	Baja participación en actividades de uso y apropiación	Niveles de participación inferiores a los esperados en actividades de sensibilización, formación o ejercicios prácticos.	Media	Media	Coordinación con COLCERT para la convocatoria, comunicación oportuna y seguimiento a la participación.
R4	Cambios en prioridades institucionales	Ajustes en prioridades, agendas o necesidades institucionales de COLCERT que puedan afectar la planeación inicial del proyecto.	Baja	Media	Mecanismos de seguimiento y ajuste operativo dentro del alcance definido en el Anexo Técnico.
R5	Dependencia de terceros tecnológicos	Dependencia de plataformas, herramientas o servicios de terceros previstos en el Anexo Técnico para la ejecución de actividades.	Baja	Alta	Gestión preventiva de accesos, validación técnica temprana y creación de planes contingentes operativos.
R6	Limitaciones en capacidades técnicas del personal	Diferencias en los niveles de conocimiento técnico de los participantes que pueden afectar el ritmo de las actividades de uso y apropiación.	Media	Baja	Desarrollo de actividades de sensibilización y formación de acuerdo con los públicos definidos.
R7	Cambios normativos o lineamientos externos	Limitación en nuevos lineamientos normativos o disposiciones que puedan incidir en la	Baja	Media	Seguimiento normativo y ajuste de actividades conforme a lineamientos de COLCERT y el Anexo Técnico.

ID	Riesgo identificado	Descripción del riesgo	Probabilidad	Impacto	Estrategia de mitigación
		ejecución del proyecto durante su vigencia.			
R8	Riesgos asociados a la gestión de la información	Posible exposición no autorizada de información o insuficiencia en la gestión de actividades técnicas o formativas.	Baja	Alta	Aplicación de cláusulas de confidencialidad y adopción de medidas de seguridad en la ejecución.
R9	Riesgos de cronograma	Retrasos en la ejecución de actividades por causas externas o contractuales.	Media	Media	Seguimiento permanente al cronograma y ajustes operativos acordados con COLCERT.

15. Exclusiones del Proyecto

El proyecto no contempla, de manera expresa, las siguientes actividades, servicios o responsabilidades, las cuales se entienden excluidas del alcance contractual:

- Formulación de políticas públicas, lineamientos estratégicos o marcos normativos en materia de seguridad digital o ciberseguridad, los cuales son competencia de las entidades rectoras y de ColCERT.
- Administración, operación permanente o soporte misional continuo de la infraestructura tecnológica, plataformas, sistemas de información o servicios de ColCERT, una vez finalizado el periodo de ejecución contractual.
- Garantía de resultados específicos relacionados con la eliminación de riesgos cibernéticos, la prevención total de incidentes de seguridad digital o el aseguramiento absoluto de los activos digitales de la entidad.
- Adquisición, renovación o ampliación de infraestructura tecnológica no prevista expresamente en el Anexo Técnico, incluyendo, entre otros, hardware, equipos de red, dispositivos de seguridad perimetral, enlaces de conectividad o centros de datos.

- Prestación de servicios de mesa de ayuda institucional, soporte 24/7 permanente o atención de incidentes fuera del alcance y periodo definidos en el Anexo Técnico.

- El proyecto no contempla la adquisición, licenciamiento permanente, cesión, transferencia de propiedad intelectual ni titularidad sobre la plataforma tecnológica de formación a favor de ColCERT. La participación de la Agencia Nacional Digital – AND se limita a la configuración, parametrización, habilitación y uso de la plataforma durante el periodo de ejecución del proyecto, exclusivamente para la realización de las actividades de sensibilización, formación práctica, competencias técnicas y gestión de evidencias, conforme a lo establecido en el Anexo Técnico.

- Desarrollo de campañas de comunicación masivas o de alcance nacional, distintas a las acciones de comunicación y divulgación expresamente definidas y aprobadas por ColCERT en el marco del proyecto.

- Certificación profesional, acreditación oficial o expedición de títulos académicos, distintos de los certificados de participación o constancias asociadas a las actividades de uso, apropiación y fortalecimiento de capacidades previstas en el proyecto.

- Evaluaciones de madurez institucional, gestión de indicadores, acuerdos de niveles de servicio (ANS), auditorías de seguridad, certificaciones normativas o procesos de cumplimiento no contemplados expresamente en el Anexo Técnico.

- Asunción de responsabilidades relacionadas con procesos electorales, transparencia electoral o protección de infraestructuras críticas nacionales, más allá del alcance de apoyo técnico y fortalecimiento de capacidades definido contractualmente.

- Transferencia de propiedad intelectual, licenciamiento permanente o cesión de derechos sobre herramientas, metodologías, contenidos o desarrollos no pactados expresamente en el contrato.

16. Condiciones para el Desarrollo del Proyecto

El desarrollo del proyecto se realizará bajo las siguientes condiciones, las cuales constituyen el marco operativo y contractual para la correcta ejecución de las actividades previstas:

Articulación institucional:

La ejecución del proyecto se desarrollará en coordinación permanente con el equipo designado por ColCERT, quien actuará como instancia de interlocución, validación y supervisión de las actividades, conforme a lo establecido en el Anexo Técnico.

Disponibilidad de información e insumos:

ColCERT deberá garantizar la disponibilidad oportuna de la información, accesos, insumos técnicos y definiciones necesarias para la ejecución de las actividades del proyecto, en los términos y condiciones acordados, sin que ello implique la transferencia de responsabilidades misionales.

Alcance y ajustes operativos:

Las actividades se ejecutarán estrictamente dentro del alcance definido en el Anexo Técnico. Cualquier ajuste operativo requerido durante la ejecución deberá realizarse de común acuerdo entre las partes, sin que ello implique ampliación del alcance contractual ni modificación de los objetivos del proyecto.

Cronograma y coordinación:

El desarrollo del proyecto se sujetará al cronograma acordado entre las partes. Los ajustes al cronograma derivados de causas justificadas deberán ser coordinados y validados con ColCERT, manteniendo la coherencia con las fases definidas.

Recursos humanos y técnicos:

La Agencia Nacional Digital – AND dispondrá del equipo humano y los recursos técnicos necesarios para la ejecución del proyecto, conforme a lo definido en el Anexo Técnico y a las condiciones contractuales establecidas.

Participación de los públicos definidos:

La ejecución de las actividades de uso, apropiación y fortalecimiento de capacidades estará condicionada a la participación de los públicos definidos por ColCERT, así como a los mecanismos de convocatoria y comunicación que esta entidad determine.

Cumplimiento normativo:

El proyecto se ejecutará en cumplimiento del marco normativo aplicable, incluyendo las disposiciones relacionadas con seguridad de la información, protección de datos personales y confidencialidad, sin perjuicio de las obligaciones contractuales asumidas.

Seguimiento y control:

Durante la ejecución del proyecto se realizarán actividades de seguimiento y control, orientadas a verificar el avance de las actividades y la alineación con el Anexo Técnico, mediante los mecanismos de coordinación definidos entre las partes.

Limitaciones de responsabilidad:

La responsabilidad de la Agencia Nacional Digital – AND se circunscribe a la ejecución de las actividades definidas contractualmente, sin asumir obligaciones relacionadas con la operación misional permanente, la garantía de resultados específicos o la gestión integral de incidentes de seguridad digital.

Adecuaciones físicas y locativas:

El desarrollo del proyecto no contempla la ejecución de adecuaciones físicas, obras civiles, modificaciones locativas ni intervenciones sobre la infraestructura física de ColCERT. En caso de que para la ejecución de alguna actividad se requiera el uso de espacios físicos, estos deberán encontrarse previamente habilitados por ColCERT y cumplir con las condiciones necesarias para su utilización, sin que ello implique responsabilidades adicionales para la Agencia Nacional Digital – AND.

17. Acuerdo de niveles de servicio ANS

Entrega y activación de cada licencia hasta 15 días calendario antes del vencimiento previo o dentro del plazo acordado para nuevas adquisiciones; documentación en orden (derecho de uso, versión y soporte vigente). Buenas prácticas exigen plazos claros y remedios ante demoras.

El cumplimiento de los niveles de servicio asociados al licenciamiento objeto del presente Acuerdo de Niveles de Servicio (ANS) se encuentra condicionado a la disponibilidad de las condiciones técnicas, administrativas y legales necesarias para su correcta habilitación, configuración y uso. En consecuencia, la Agencia Nacional Digital – AND no será responsable por retrasos, limitaciones o afectaciones en la prestación del servicio cuando estos se deriven de eventos constitutivos de fuerza mayor, caso fortuito o hechos atribuibles a terceros, ajenos a su ámbito de control.

Para efectos del presente ANS, se consideran hechos exógenos, entre otros, la indisponibilidad o restricción de plataformas, infraestructuras o servicios administrados por terceros; la falta de provisión oportuna de información, accesos, ambientes o insumos requeridos por parte de la Entidad; cambios normativos o decisiones administrativas que afecten el uso del licenciamiento; así como cualquier circunstancia imprevisible o irresistible que impida la habilitación o utilización normal de las licencias.

En estos eventos, la AND informará a la Entidad sobre la situación presentada y las acciones de mitigación que, de manera razonable, puedan adoptarse, sin que ello genere la imposición de sanciones, penalidades o afectaciones contractuales, siempre que se acredite la debida diligencia en la gestión del licenciamiento conforme a los términos acordados.

18. Cierre del Proyecto

El cierre del proyecto se realizará una vez culminadas las actividades previstas en el alcance y las fases definidas, y tendrá como finalidad verificar y formalizar la correcta ejecución del proyecto, de conformidad con lo establecido en el Anexo Técnico y en el contrato suscrito entre las partes.

Durante esta etapa, la Agencia Nacional Digital – AND consolidará la información correspondiente a la ejecución del proyecto, incluyendo los informes finales, las evidencias de las actividades desarrolladas y los resultados alcanzados, los cuales serán presentados a ColCERT para su revisión y validación.

El cierre del proyecto se formalizará mediante la suscripción del acta de cierre, en la cual ColCERT dejará constancia de la culminación de las actividades contractuales, la aceptación de los resultados de la ejecución y el cumplimiento de las obligaciones a cargo de la AND, sin perjuicio de las responsabilidades que, por su naturaleza, deban mantenerse vigentes con posterioridad al cierre.

Con la formalización del cierre del proyecto se dará por finalizada la ejecución contractual, sin que ello implique la continuidad automática de servicios, la operación misional permanente de capacidades técnicas o formativas, ni la asunción de nuevas obligaciones por parte de la Agencia Nacional Digital – AND, distintas a las expresamente pactadas en el contrato.