Agencia Nacional Digital

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL

BOGOTÁ, ENERO DE 2026

CONTENIDO

1. INTRODUCCIÓN

La Corporación Agencia Nacional de Gobierno Digital —AND—, en cumplimiento de su misión como motor de la transformación digital del Estado, reconoce la información como un activo estratégico. Bajo esta premisa, y en concordancia con la Resolución 35 de 2023, el Comité Institucional de Gestión y Desempeño asume la función de asegurar la implementación de directrices en materia de seguridad digital.

Este compromiso se fundamenta en el marco legal vigente, principalmente en el Decreto 1083 de 2015, que rige las Políticas de Gestión y Desempeño Institucional, y el Decreto 1008 de 2018, que establece la seguridad de la información como un principio esencial para generar confianza en el entorno digital mediante la gestión de riesgos y la preservación de la confidencialidad, integridad y disponibilidad.

El presente Plan se articula con el Decreto 767 de 2022, el cual define la Seguridad y Privacidad de la Información como un habilitador transversal. Este enfoque busca que la —AND— desarrolle capacidades robustas en todos sus procesos, servicios e infraestructura. Asimismo, se atiende lo dispuesto en el Decreto 2106 de 2019 y la Resolución 500 de 2021 (actualizada por la Resolución 02277 de 2025), que dictan los lineamientos y estándares para la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).

Como prueba del alto nivel de madurez alcanzado, la —AND— se sometió a un proceso de auditoría externa por parte del ICONTEC en diciembre de 2025. Como resultado, la organización obtuvo la certificación de su Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar internacional ISO/IEC 27001:2022.

Este logro no solo valida el cumplimiento de los requisitos técnicos y legales, sino que ratifica la capacidad institucional para proteger la intimidad y los datos de los ciudadanos, asegurando la mejora continua y la resiliencia ante ciberamenazas.

En consecuencia, el presente Plan de Seguridad y Privacidad de la Información para el periodo vigente tiene como objetivo consolidar los controles establecidos, mantener la certificación obtenida y garantizar que la estrategia de seguridad digital de la —AND— siga siendo un referente de integridad y confianza para el ecosistema de Gobierno Digital en Colombia.

2. OBJETIVO GENERAL

Definir y ejecutar las actividades, roles y responsabilidades necesarios para la operación y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI) durante la vigencia 2026, bajo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), el Departamento Administrativo de la Función Pública y el estándar internacional ISO/IEC 27001:2022. Lo anterior,

con el fin de garantizar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de los activos de información, fortaleciendo la cultura organizacional y el gobierno corporativo para asegurar una atención oportuna y confiable a los grupos de interés de la Corporación Agencia Nacional de Gobierno Digital —AND—.

2.1. OBJETIVOS ESPECIFICOS

- ✓ Asegurar la operación, seguimiento y mejora del Sistema de Gestión de Seguridad de la Información (SGSI) durante la vigencia 2026, garantizando el cumplimiento de los lineamientos del MINTIC y los requisitos de la norma ISO/IEC 27001:2022.
- ✓ Ejecutar el plan de tratamiento derivado de los hallazgos y oportunidades de mejora identificados en la auditoría de certificación de 2025, fortaleciendo la resiliencia institucional frente a nuevas ciberamenazas.
- ✓ Fortalecer el Programa Integral de Protección de Datos Personales mediante la actualización de políticas de tratamiento, asegurando que la recolección, uso y disposición de datos cumpla con los principios de legalidad, transparencia y seguridad digital.
- ✓ Garantizar el ejercicio de los derechos de los titulares de la información, implementando controles técnicos y administrativos que protejan la privacidad desde el diseño y por defecto en todos los proyectos de la AND.
- ✓ Gestionar de forma dinámica el inventario de activos de información y la matriz de riesgos de seguridad digital, aplicando metodologías de valoración que permitan implementar controles proporcionales al impacto y probabilidad de las amenazas.
- ✓ Incrementar la confianza de las partes interesadas mediante el aseguramiento de los activos críticos, garantizando que el entorno digital de la AND sea un espacio seguro para el trámite y servicios ciudadanos.
- ✓ Desarrollar una estrategia integral de comunicación y sensibilización dirigida a empleados de planta y contratistas, que promueva una cultura de "seguridad digital y ciberseguridad" y facilite la adopción de buenas prácticas en el manejo de la información en la AND.

3. ALCANCE

El presente Plan de Seguridad y Privacidad de la Información de la Corporación Agencia Nacional de Gobierno Digital —AND— comprende el conjunto de actividades estratégicas, técnicas y operativas orientadas a la protección de los activos de información. Su implementación se fundamenta en el cumplimiento de la normatividad vigente, el estándar internacional ISO/IEC 27001:2022, el Modelo de Seguridad y Privacidad de la Información (MSPI), la Política de Seguridad Digital y el Programa Integral de Protección de Datos Personales.

4. CONTEXTO NORMATIVO

El presente normograma compila y organiza el marco normativo vigente y aplicable que fundamenta la gestión de la seguridad y privacidad de la información en la Entidad. Este instrumento orientador relaciona las leyes, decretos, resoluciones, circulares, documentos CONPES, lineamientos técnicos y directivas institucionales que establecen los principios, obligaciones y mejores prácticas para la protección de los activos de información, el tratamiento adecuado de datos personales y la gestión integral de riesgos digitales.

- ✓ Ley 1581 de 2012 – Protección de Datos Personales (y proyecto de actualización en trámite 2025).
- ✓ Ley 1712 de 2014 – Transparencia y Derecho de Acceso a la Información Pública.
- ✓ Ley 2088 de 2021 – Régimen del Trabajo en Casa.
- ✓ Ley 1266 de 2008 – Habeas Data financiero.
- ✓ Decreto 1074 de 2015 – Único Reglamentario del Sector Comercio, Industria y Turismo (registro bases de datos).
- ✓ Decreto 1078 de 2015 – Único Reglamentario del Sector TIC.
- ✓ Decreto 1083 de 2015 – Único Reglamentario de Función Pública.
- ✓ Decreto 1377 de 2013 – Reglamenta parcialmente la Ley 1581 de 2012.
- ✓ Decreto 338 de 2022 – Lineamientos para fortalecimiento de gobernanza en seguridad digital.
- ✓ Decreto 2106 de 2019 – Estrategia de seguridad digital.
- ✓ Decreto 612 de 2018 – Integración de planes institucionales y estratégicos.
- ✓ Resolución 500 de 2021 – Lineamientos y estándares para la estrategia de seguridad digital/MSPI.
- ✓ Resolución 460 de 2022 – Plan Nacional de Infraestructura de Datos.
- ✓ Resolución 1519 de 2020 – Estándares para publicar información (acceso, seguridad, datos abiertos).
- ✓ Resolución 1321 de 2020 – Parámetros mínimos para gestión de riesgos tecnológicos (sector salud).
- ✓ Circular Externa 002 de 2024 (SIC) – Tratamiento de datos personales en sistemas de IA.

- ✓ Circular Externa 001 de 2025 (SIC) – Medidas de seguridad de la información y reporte de incidentes.
- ✓ Circulares Superintendencia Financiera 029 de 2014 y 033 de 2020 – Riesgo ciberseguridad, reporte de incidentes.
- ✓ Resolución 02277 de 2025 – Por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- ✓ Modelo de Seguridad y Privacidad de la Información (MSPI) – MinTIC, actualizado 2025.
- ✓ Norma Técnica Colombiana NTC-ISO/IEC 27001:2022 – Gestión de Seguridad de la Información.

- ✓ Modelo Integrado de Planeación y Gestión (MIPG) – Dimensión Seguridad Digital.
- ✓ Guía DAFP: Administración del Riesgo y Diseño de Controles.
- ✓ CONPES 3701 de 2011 – Estrategia Nacional Ciberseguridad y Ciberdefensa.
- ✓ CONPES 3854 de 2016 – Política Nacional de Seguridad Digital.
- ✓ CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital.
- ✓ Directiva Presidencial 03 de 2021 – Lineamientos para uso de nube, IA y seguridad digital.
- ✓ Directiva Presidencial 02 de 2022 – Estrategia para actualización, gestión integral y seguridad digital.

5. MOTIVADORES ESTRATÉGICOS

El Plan de Acción de Seguridad y Privacidad de la Información 2026 se formula en coherencia con el objetivo estratégico institucional orientado a Asegurar la prestación de los Servicios Ciudadanos Digitales Base cumpliendo estándares de seguridad, privacidad, acceso, neutralidad tecnológica y continuidad del servicio. En este marco, el Plan busca fortalecer el Sistema de Gestión de Seguridad y Privacidad de la Información del AND como un componente esencial para la eficiencia institucional, la confianza digital y la consolidación de una cultura organizacional responsable en el tratamiento y protección de la información, siguiendo las buenas prácticas definidas por la norma ISO/IEC 27001:2022.

5.1. Gestión del Riesgo y Continuidad de la Operación

Adoptar este estándar nos permite anticiparnos a las amenazas que pueden poner en riesgo la confidencialidad, integridad y disponibilidad de la información. El principal objetivo es disminuir la probabilidad de incidentes que afecten la operación diaria, asegurando la continuidad del negocio y la capacidad de responder y recuperarse de manera efectiva ante ciberataques o fallas tecnológicas.

5.2. Cumplimiento Normativo y Tranquilidad Legal

La AND desarrolla sus actividades en un entorno regulatorio cada vez más exigente. Implementar ISO 27001:2022 facilita el cumplimiento de normas clave como la Ley 1581 de 2012 sobre protección de datos personales, la Ley 1266 de 2008 de Habeas Data y las circulares vigentes de la Superintendencia de Industria y Comercio (SIC) relacionadas con inteligencia artificial y reporte de incidentes. Esto no solo reduce riesgos legales, sino que también evita sanciones y costos innecesarios.

5.3. Confianza y Valor para las Partes Interesadas

La seguridad de la información es hoy un factor decisivo de confianza. Al estandarizar y fortalecer los procesos de seguridad, la organización demuestra madurez,

responsabilidad y compromiso frente a clientes, proveedores y aliados estratégicos. La protección integral de los datos personales y de la información es un habilitador de confianza que salvaguarda la reputación de la entidad frente a los organismos de control y la ciudadanía y permite construir relaciones comerciales sólidas, basadas en la transparencia y la credibilidad.

5.4. Procesos Más Eficientes y Mejor Gobernanza Digital

En línea con el Modelo Integrado de Planeación y Gestión (MIPG) y el MSPI del MinTIC, la seguridad de la información se concibe como un eje transversal y no como un esfuerzo aislado. Este plan busca optimizar el uso de los recursos tecnológicos mediante la implementación de controles definidos en el Anexo A de la norma, así como la automatización de la supervisión, reduciendo reprocesos y fortaleciendo la toma de decisiones basada en información confiable.

5.5. Cultura de Seguridad y Conciencia Digital

Las personas son el activo más valioso de la AND, pero también el punto más vulnerable frente a los riesgos de seguridad. Por ello, uno de los motivadores estratégicos más importantes es fortalecer la cultura de seguridad de la información, logrando que cada empleado de planta y contratistas entiendan su responsabilidad en la protección de los activos informáticos. Una mayor conciencia reduce significativamente los riesgos asociados a errores humanos y prácticas inseguras.

6. SITUACIÓN ACTUAL

La AND dispone de un Sistema de Gestión de Seguridad Digital estructurado y en fase de implementación continua, cuyo marco de políticas y controles se encuentra alineado con el estándar ISO/IEC 27001:2022; este compromiso con la protección de los activos de información y la mejora continua se evidencia en los resultados del FURAG 2024, donde, frente a un cumplimiento general del 71.3%, la política de Seguridad Digital (P08) alcanzó un destacado 79.8%, desempeño que se ve complementado por la autoevaluación del MSPI (MinTIC) de 2025, la cual arrojó un 86% de efectividad en la implementación de controles, ratificando la solidez institucional en la gestión de riesgos tecnológicos.

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	86	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	95	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	80	100	GESTIONADO
A.8	CONTROLES TECNOLÓGICOS	82	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		86	100	OPTIMIZADO

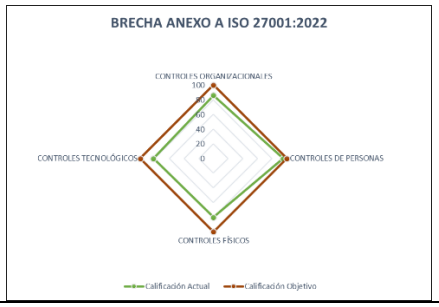

Ilustración 1 Autoevaluación MSPI AND 2025

En este contexto, la AND, a través de la Subdirección de Desarrollo y SCD, ha liderado la gestión de seguridad de la información mediante la coordinación y el monitoreo integral de las acciones de seguridad digital y el cumplimiento de controles, promoviendo así una visión unificada de la seguridad al interior de la entidad; no obstante, se ha identificado la necesidad de fortalecer la articulación técnica con los procesos operativos y misionales, con el propósito de alcanzar una implementación más efectiva y homogénea del Sistema de Gestión de Seguridad Digital y del Programa Integral de Gestión de Datos Personales.

Así mismo con la ejecución de auditorías internas y externas, y la posterior solicitud de certificación ante el ICONTEC en diciembre de 2025, la AND obtuvo con éxito la certificación de su Sistema de Gestión de Seguridad de la Información (SGSI) bajo el estándar internacional ISO/IEC 27001:2022; no obstante, este proceso permitió identificar oportunidades de mejora clave en la efectividad de los controles relacionados con la administración de vulnerabilidades, la trazabilidad de acciones correctivas, la continuidad del negocio y la actualización frente a amenazas emergentes, retos que subrayan la necesidad de consolidar un enfoque de seguridad integral y preventivo que armonice los componentes tecnológicos con los organizacionales.

7. CRONOGRAMA Y EJES ESTRATÉGICOS 2026

El Plan de Implementación de Seguridad y Privacidad de la Información, diseñado para dar cumplimiento al habilitador transversal de la Política de Gobierno Digital, establece un cronograma orientado a la incorporación sistemática de medidas de seguridad en los procesos, proyectos y servicios de la AND. El cual busca fortalecer la confianza ciudadana y garantizar el cumplimiento de los marcos normativos vigentes en seguridad digital y protección de datos, bajo el seguimiento y monitoreo conjunto del Profesional en Seguridad de la Información y la Oficina de Planeación de la entidad.

En este marco, el Plan de Acción 2026 se articula a través de los siguientes ejes estratégicos:

Capacidad de Respuesta y Resiliencia	Fortalecer la infraestructura tecnológica y las capacidades de monitoreo y detección de incidentes, estableciendo Acuerdos de Niveles de Servicio (ANS) que definan tiempos de reacción estandarizados ante eventos de seguridad aplicables a la AND.
Gestión del Riesgo Integrada	Incorporar la gestión del riesgo de seguridad y privacidad en todos los procesos de planeación institucional, garantizando una protección preventiva, alineada con los objetivos de negocio y sostenible en el tiempo.
Cultura y Sensibilización	Fomentar una cultura organizacional de ciberseguridad mediante programas de capacitación y sensibilización que promuevan la corresponsabilidad y el compromiso ético de todos los colaboradores de la entidad.
Liderazgo y Mejora Continua	Potenciar la seguridad digital y la eficacia del SGSI mediante el seguimiento permanente a los hallazgos de auditoría, la trazabilidad rigurosa de los controles y la optimización constante de los procesos internos.
Privacidad Datos personales	Consolidar la protección de datos personales bajo los principios de privacidad desde el diseño y por defecto, asegurando el cumplimiento estricto del Programa Integral de Gestión de Datos Personales

Ilustración 2 Ejes Estratégicos de Seguridad digital

A continuación, se relacionan el cronograma de actividades del Plan de Acción de Seguridad y Privacidad de la Información para el año 2026:

FASE/ETAPA	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
Revisión y actualización de documentación del Sistema de Gestión de Seguridad de la Información.	Actualizar el documento con el resultado de la herramienta de autodiagnóstico, de implementación del MSPI en toda la Entidad	02-02-2026	31-07-2026	Documento autodi MSPI actualizado	Profesional de seguridad de Información
	Actualizar el Plan de Seguridad y Privacidad de la	15-01-2026	31-01-2026	Acta de Aprobación de Plan de Seguridad y	CIGD y Profesional de seguridad

FASE/ETAPA	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
	Información-Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y publicar en el portal WEB.			Privacidad de la Información	de Información
	Actualizar el Plan De Sensibilización De Seguridad y Privacidad de la Información y Datos Personales	02-02-2026	02-03-2026	Documento Plan De Sensibilización De Seguridad y Privacidad de la Información y Datos Personales 2026	Profesional de seguridad de Información
	Actualizar los Documentos del proceso Seguridad y privacidad de la información SYPI, por acción de mejora	15-02-2026	31-07-2026	Listado maestro de documentos de SIGAND	Profesional de seguridad de Información y Planeación AND
Monitoreo, análisis y gestión integral de riesgos de seguridad de la información	Identificar nuevos activos de información por procesos nuevos y/o actualizados	20-02-2026	20-04-2026	Matriz actualizada Identificación y clasificación de activos de información	Profesional de seguridad de Información Líder Proceso
	Actualizar la Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	20-04-2026	29-05-2026	Actualizar la Mapa de Riesgos Sistema Seguridad de la Información	Profesional de seguridad de Información Líder Proceso
	Actualizar el Plan de implementación de controles de seguridad y	05-05-2026	29-05-2026	Documento Plan de implementación de controles de seguridad y	Profesional de seguridad de Información

FASE/ETAPA	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
	privacidad de la información que contenga como mínimo: controles, actividades, fechas, responsable de implementación y Estado de implementación			privacidad de la información	
Protección y gestión de datos personales	Recolectar bases de datos, bases de datos personales de acuerdo con los estándares emitidos por la Superintendencia de Industria y Comercio	10-02-2026	30-03-2026	Matriz de bases de datos personales de para reportar	Oficina Asesora de jurídica
	Registrar y actualizar de las bases de datos Gestión de datos personales ante la Superintendencia de Industria y Comercio	10-02-2026	30-03-2026	Soporte de registro de actualización de las bases de datos personales de para reportar la AND	Oficina Asesora de jurídica
	Aplicar e incluir avisos de la privacidad que contenga el lenguaje mínimo señalado en la ley 1581 de 2012 y decreto 1377 de 2013.	20-02-2026	30-06-2026	Aplicar los Avisos de la privacidad de datos personales para los diferentes aplicativos, formularios y donde requiera a aceptación de tratamiento de datos	Oficina Asesora de jurídica
	Envío del consolidado de activos de	05-05-2026	26-06-2026	Entrega de Matriz actualizada	Profesional de seguridad

FASE/ETAPA	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
	seguridad digital actualizado a la gestión Documental , para el respectivo reporte del índice de información clasificada y reservada y de Publicación de activos de la información AND			Identificación y clasificación de activos de información	de Información Gestión Documental Oficina Asesora de jurídica Profesional de datos personales
	Publicación de índice de información clasificada y reservada	06-07-2026	30-11-2026	Actualizar documento índice de información clasificada y reservada y publicar en el portal https://www.datos.gov.co/	Oficina Asesora de jurídica Profesional de datos personales
Seguimiento Evaluación y mejora continua	Publicación Registro activos de información	06-07-2026	30-11-2026	Actualizar documento Registro activos de información y gestionar la publicación en el portal https://www.datos.gov.co/	Gestión Documental
	Actualizar documentación nueva metodología de gestión de riesgo DAFP	06-07-2026	30-11-2026	Documentos de Seguridad de la información y plan de tratamiento de riesgos.	Planeación AND Profesional de seguridad de Información
	Elaborar los informes de Seguimiento de riesgos de	29-05-2026	31-12-2026	Informe semestral de Riesgos de seguridad de la	Planeación AND Profesional de seguridad

FASE/ETAPA	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
	Seguridad de la Información – Seguridad Digital			Información – Seguridad Digital	de Información
	Actualizar el Informe con la evaluación y medición de la efectividad de la implementación de los controles definidos en el plan de tratamiento de riesgos	30-09-2026	31-12-2026	Documento Reporte anual de matriz de control de controles.	Planeación AND Profesional de seguridad de Información
	Realizar las acciones del Plan de auditorías que evidencia la programación de las auditorias de seguridad y privacidad de la información, con seguimiento de Control Interno	01-03-2026	31-12-2026	Ejecución de Planes de mejora SDI programados	Profesional de seguridad de Información Planeación Control Interno
	Reporte de cumplimento de Plan Sensibilización de Seguridad y Privacidad de la Información y Datos Personales	01-12-2026	31-12-2026	Documento de reporte de la vigencia de cumplimiento de Plan Sensibilización de Seguridad y Privacidad de la Información y Datos Personales	Profesional de seguridad de Información Profesional de Gestión de TI Planeación
	Medir el cumplimiento Plan de Seguridad y Privacidad de la	01-02-2026	31-12-2026	Talero de control y/o cronograma de cumplimiento con el avance Plan de	Profesional de seguridad de Información

FASE/ETAPA	ACTIVIDADES	FECHA DE INICIO	FECHA FIN	META	RESPONSABLE
	Información – Seguridad Digital 2026			Seguridad y Privacidad de la Información – Seguridad Digital 2026	Profesional de Gestión de TI Planeación
	Preparar auditoría interna ISO 27001	01-03-2026	30-06-2026	Dar alcance sobre auditoria interna	Control Interno
	Preparar auditoría de seguimiento ICONTEC ISO 27001:2022	01-02-2026	31-12-2026	Seguimiento planes de acción y cierre, solicitud a ICONTEC	Profesional de seguridad de Información Líder de proceso
	Realizar seguimiento a las oportunidades de mejora producto de revisiones internas y externas a los Procesos	01-02-2026	31-12-2026	Informe de cumplimiento de acciones preventivas y correctivas de los planes de mejora propuestos de seguridad de la información – Seguridad Digital	Profesional de seguridad de Información Planeación Control Interno

Ilustración 3Tabla 3 Plan SYPI Cronograma

8. SEGUIMIENTO Y EVALUACIÓN

Con el fin de garantizar un seguimiento y evaluación al plan de acción, se establece los siguientes indicadores:

- ✓ Porcentaje de participación en inducciones, reinducciones y/o sensibilizaciones en Seguridad Digital
  Fórmula:

  ((Número de colaboradores que participaron en inducciones, reinducciones o sensibilizaciones) / (Número total de empleados)) × 100
  Periodicidad: Anual
  Meta: 50%

Ilustración 4 Fuente: Registros de capacitación anual

- ✓ Porcentaje de Cumplimiento Plan de Acción

Fórmula:

((Numero de actividades del Plan de Acción realizadas en el semestre/ (Número total de actividades planificadas en el semestre)) × 100 Periodicidad: Anual Meta: 90%

Ilustración 5 Registros de Planeación

9. CONTROL DE CAMBIOS

REVISIÓN No.	FECHA	CAMBIOS
1	31-01-2025	Actualización de Documento con actividades para la vigencia 2025 en el cumplimiento de Decreto 612 de 2018 y alineación con la norma ISO 27001:2022
2	30-01-2026	Actualización de Documento con actividades para la vigencia 2026 en el cumplimiento de Decreto 612 de 2018 y alineación con la norma ISO 27001:2022

Digitally signed by ECHAVARRIA POVEDA JULIO ERNESTO

JULIO ERNESTO ECHAVARRIA POVEDA

Subdirector Subdirección de Desarrollo y SCD

Elaboró: Denis Fernando Montealgre Beltran; Profesional de seguridad de la información

Revisó y aprobó: Comité Institucional de Gestión y Desempeño de la Corporación Agencia Nacional de Gobierno Digital del 30 de enero 2026