



UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

**Oficial de Seguridad de la Información
Comité Ejecutivo de Dirección Institucional**

PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN – PESI (2026-2028)

Fecha de aprobación (30/ 09/ 2026)

TABLA DE CONTENIDO

I. PRESENTACIÓN	4
II. OBJETIVOS DEL PLAN	5
2.1. Objetivo General	5
2.2. Objetivos Específicos	5
III. ALCANCE.	5
IV. VIGENCIAS	6
V. DIAGNÓSTICO Y LÍNEA BASE	7
5.1 Estado Actual por Dimensiones de Control (ISO 27001:2022)	7
5.2. Madurez del Ciclo de Gestión del MSPI (PHVA)	8
5.2.1 Brechas Críticas Identificadas en el Ciclo de Gestión	8
5.3. Alineación con el Framework NIST CSF	8
5.4. Fortalezas Institucionales	9
5.5. Debilidades y Brechas Prioritarias	9
5.6. Articulación Estratégica y Operativa PESI - PETI (2026-2028)	10
VI. 11	
6.1. Ejes de Acción	12
Eje 1. Liderazgo de Seguridad de la Información y Gobernanza	12
Eje. 2. Gestión Integral de Riesgos y Ciberresiliencia	13
Eje 3. Implementación de Controles, Resiliencia y Continuidad	13
Eje 4. Gestión de Incidentes, Ciberdefensa y Aseguramiento Técnico	13
Eje 5. Concientización, Cultura Digital y Factor Humano	14
6.2. Líneas Operativas	14
6.2.1 Líneas Operativas del Eje 1: Liderazgo de Seguridad de la Información y Gobernanza	14
Línea Operativa 1.1. Actualización y armonización del marco normativo interno	15
Línea Operativa 1.2. Monitoreo, autodiagnóstico y evaluación del cumplimiento	15
Línea Operativa 1.3. Rendición de cuentas e informes de desempeño ante la Alta Dirección	15
6.2.2 Líneas Operativas del Eje 2: Gestión Integral de Riesgos y Ciberresiliencia	15
Línea Operativa 2.1. Automatización de la matriz institucional de riesgos y clasificación de activos	15
Línea Operativa 2.2. Ejecución de los Planes de Tratamiento de Riesgos (PTR) y controles técnicos	15
Línea Operativa 2.3. Valoración del riesgo residual y evaluación de cambios tecnológicos	15
6.2.3 Líneas Operativas del Eje 3: Implementación de Controles, Resiliencia y Continuidad	16
Línea Operativa 3.1. Actualización del Análisis de Impacto del Negocio (BIA)	16

Línea Operativa 3.2. Gestión de la infraestructura de almacenamiento y respaldos	16
Línea Operativa 3.3. Simulacros DRP/BCP y custodia de fondos documentales territoriales	16
6.2.4 Líneas Operativas del Eje 4: Gestión de Incidentes, Ciberdefensa y Aseguramiento Técnico	16
Línea Operativa 4.1. Despliegue de capacidades de ciberdefensa perimetral e interna	16
Línea Operativa 4.2. Estandarización de la asistencia técnica remota segura	16
Línea Operativa 4.3. Correlación de eventos, atención de incidentes y reporte a autoridades	17
6.2.5 Líneas Operativas del Eje 5: Concientización, Cultura Digital y Factor Humano	17
Línea Operativa 5.1. Ejecución del Plan Institucional de Capacitación en Seguridad y Privacidad y Reserva	17
Línea Operativa 5.2. Simulacros de ingeniería social y evaluación del factor humano	17
6.3. Metas Plurianuales / Anuales	17
6.3.1. Desglose de Compromisos Anuales de Ejecución	19
6.4. Matriz programática del plan	20
VII. 20	
7.1. Proyección de Presupuesto Financiero (2026-2028)	21
7.2. Asignación y Necesidades de Talento Humano	23
7.3. Soporte Tecnológico y Logística Operativa	24
VIII. NORMATIVIDAD	24
IX. REFERENCIAS	25
X. TÉRMINOS Y DEFINICIONES	25
XI. ANEXOS	30
XII. CONTROL DE CAMBIOS	30
XIII. BLOQUE DE FORMALIZACIÓN Y FIRMAS	31
Anexo 1. Matriz Programática del PESI 2026-2028. UBPD	31

I. PRESENTACIÓN

La Unidad de Búsqueda de Personas dadas por Desaparecidas (UBPD) rige su mandato humanitario y extrajudicial bajo el marco jurídico establecido por el Acto Legislativo 01 de 2017, el Decreto Ley 589 de 2017 y las Sentencias C-067 y C-080 de 2018 de la Corte Constitucional. En este contexto, la entidad tiene el compromiso ineludible de salvaguardar la reserva de la información que reciba, recaude, procese o genere, tanto en su desarrollo misional como en sus procesos estratégicos y de apoyo.

Para dar cumplimiento a este mandato frente a las actuales exigencias tecnológicas, se formula el Plan Estratégico de Seguridad de la Información (PESI) para la vigencia 2026-2028. Este plan, debidamente alineado con el Plan de Acción Institucional (PAI), define la hoja de ruta para orientar los esfuerzos de la entidad hacia la protección de sus activos, incrementando los niveles de confidencialidad, integridad y disponibilidad de la información.

Este instrumento adopta los habilitadores de la Política de Gobierno Digital, el Marco de Referencia de Arquitectura TI (MRAE) y el Modelo de Seguridad y Privacidad de la Información (MSPI). Asimismo, materializa las directrices del Modelo Integrado de Planeación y Gestión (MIPG) mediante una gobernanza transversal liderada por el Comité Ejecutivo de Dirección Institucional (CEDI), con el acompañamiento técnico del Grupo Interno de Trabajo Gestión Tecnológica (GITGT), la Secretaría General y la Oficina Asesora de Planeación (OAP).

La alineación de esta estrategia tecnológica con los objetivos institucionales asegura que la tecnología facilite la comunicación electrónica segura con la ciudadanía, organizaciones y entidades públicas. A su vez, garantiza que la infraestructura técnica de la entidad se consolide como un componente esencial para la protección integral de los datos aportados por quienes buscan a sus seres queridos. De esta manera, se salvaguarda la memoria histórica y se reafirma el compromiso de la UBPD de administrar sus ecosistemas digitales con estricto rigor institucional y sentido humanitario.

Finalmente, en cumplimiento de los lineamientos de planeación, la formulación y ejecución de este plan mitiga de manera directa los riesgos reputacionales, estratégicos de planeación, financieros y de gestión de la UBPD. Sin la implementación coordinada de controles para la salvaguarda de los datos y los mecanismos aquí descritos, la entidad se expone a incidentes críticos, tales como ataques de día cero, denegación de servicio, manipulación no autorizada (SQL Injection), secuestro de datos (ransomware) a la infraestructura tecnológica y exfiltración de bases de datos altamente sensibles.

La materialización de estos riesgos a través de diferentes vectores de ataque no solo paralizaría el cumplimiento misional, sino que generaría sanciones jurídicas por el incumplimiento de los principios rectores de la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, ocasionando un daño irreparable en la confianza ciudadana y afectando la viabilidad operativa de su mandato constitucional.

II. OBJETIVOS DEL PLAN

2.1. Objetivo General

Incrementar la madurez del Sistema de Seguridad y Privacidad de la Información de la UBPD durante el periodo 2026-2028, mediante la ejecución de las líneas operativas organizacionales, humanas, físicas y tecnológicas definidas en este plan, con el fin de lograr la optimización progresiva del sistema, cerrar las brechas identificadas y asegurar la protección integral del ciclo de vida de la información en la UBPD.

2.2. Objetivos Específicos

- Verificar la eficacia técnica y administrativa del Sistema de Seguridad y Privacidad de la Información a través de ejercicios de autodiagnóstico y monitoreo de controles, asegurando la generación de planes de mejora verificables por la Alta Dirección.
- Mitigar la exposición de los activos de información institucionales mediante la ejecución sistemática de los planes de tratamiento de riesgos, manteniendo las amenazas físicas, operativas y digitales en niveles aceptables.
- Asegurar la resiliencia institucional y la continuidad operativa de la entidad frente a eventos disruptivos, estandarizando y comprobando periódicamente los mecanismos de respaldo tecnológico y la protección de los archivos físicos.
- Robustecer las capacidades de prevención y respuesta ante incidentes, implementando controles de acceso y esquemas de seguridad física y lógica que salvaguarden transversalmente las instalaciones y la infraestructura de la UBPD.
- Ejecutar los ciclos de capacitación y simulacros controlados, con el propósito de reducir cuantitativamente las vulnerabilidades asociadas a la interacción del factor humano con los documentos físicos, testimonios y ecosistemas digitales administrados por la entidad.

III. ALCANCE.

El alcance del presente Plan Estratégico es de carácter transversal y delimita las fronteras institucionales, operativas y técnicas para la implementación de las capacidades de seguridad de la información, estructurándose bajo las siguientes dimensiones:

- **Responsabilidad de Ejecución:** La implementación técnica, seguimiento y cumplimiento de las metas programáticas definidas en este plan recaen sobre los roles y procesos líderes asignados, en cabeza del Comité Ejecutivo de Dirección Institucional (CEDI), el Oficial de Seguridad de la Información (OSI) y el Grupo Interno de Trabajo Gestión Tecnológica (GITGT).
- **Cobertura de Impacto y Aplicación de Controles:** Las medidas preventivas, herramientas de seguridad, controles físicos y ciclos formativos que se desplieguen como resultado de este plan, amparan e impactan la gestión de la totalidad de los servidores públicos, contratistas, pasantes, proveedores, aliados estratégicos y terceros que accedan, administren, custodien o interactúen con los activos de información de la UBPD.
- **Cobertura de Procesos y Ciclo de Vida:** Comprende la salvaguarda de la información en todos los procesos institucionales (estratégicos, misionales, de apoyo, y de evaluación

y control). El plan cubre la totalidad del ciclo de vida de la información: desde su recolección y captura en territorio, hasta su procesamiento, uso, almacenamiento, intercambio, preservación definitiva o disposición en el archivo general e histórico de la entidad.

- **Cobertura Operativa y Territorial:** Abarca todos los escenarios de actuación de la UBPD, incluyendo las instalaciones físicas del nivel central, las sedes de los Grupos Internos de Trabajo Territoriales (GITT), las modalidades de trabajo fuera de sede y los despliegues u operaciones humanitarias en campo.
- **Cobertura Técnica y Física:** Aplica de manera integral sobre todos los activos de información, independientemente de su soporte. Incluye expedientes y archivos físicos, así como la totalidad de la infraestructura tecnológica, bases de datos, sistemas de información, redes corporativas y servicios alojados en la nube.

IV. VIGENCIAS

El presente Plan Estratégico de Seguridad de la Información (PESI) es un instrumento de nivel programático con un horizonte temporal plurianual correspondiente al trienio 2026-2028, articulado transversalmente con el Plan Estratégico de Tecnologías de la Información (PETI) y el Marco Estratégico – 2024 – 2028 de la UBPD.

El plan rige e inicia su ejecución oficial a partir de la fecha de su aprobación formal por parte del Comité Ejecutivo de Dirección Institucional (CEDI), y mantendrá su vigencia hasta el 31 de diciembre de 2028, fecha en la que perderá su validez o será sustituido por el instrumento que actualice la planeación estratégica de la entidad.

Periodicidad y Mecanismo de Revisión: El Oficial de Seguridad de la Información (OSI), en articulación con el Grupo Interno de Trabajo Gestión Tecnológica (GITGT) y la Oficina Asesora de Planeación (OAP), liderará un ejercicio de revisión y seguimiento formal al plan durante el último trimestre de cada vigencia anual.

Causales de Ajuste o Actualización: El plan será objeto de modificación ordinaria o extraordinaria frente a cualquiera de las siguientes circunstancias:

- Cambios significativos en la matriz de riesgos institucionales o en el perfil de exposición de los activos de información.
- Actualizaciones normativas emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) o variaciones en el marco legal vigente.
- Modificaciones en la estructura organizacional, los procesos o el modelo de operación de la UBPD.
- Resultados de autodiagnósticos, evaluaciones de desempeño o planes de mejoramiento del Sistema de Seguridad de la Información.

Toda modificación o actualización requerirá la validación previa del OSI, y la aprobación formal del Comité Ejecutivo de Dirección Institucional (CEDI) previo a su adopción e implementación.

V. DIAGNÓSTICO Y LÍNEA BASE

La Unidad de Búsqueda de Personas dadas por Desaparecidas (UBPD) cuenta con un nivel de implementación base en sus controles de operabilidad, alcanzando una calificación promedio del **86%** en la evaluación del Anexo A de la norma ISO 27001:2022. Sin embargo, la ejecución global del ciclo de gestión del Modelo de Seguridad y Privacidad de la Información (MSPI) registra un avance del **70,4%**, lo que evidencia una brecha entre la existencia de controles técnicos operativos y la formalización de su ciclo de mejora continua.

El principal reto programático para el periodo 2026-2028 consiste en cerrar las brechas del ciclo PHVA y transformar los controles existentes en capacidades medibles, verificables y automatizadas, asegurando la protección integral del ciclo de vida de la información sensible (documental, testimonial y digital) custodiada en el ejercicio del mandato humanitario. Este diagnóstico toma como insumo oficial el *Autodiagnóstico UBPD 2026*, consolidado por la Oficina Asesora de Planeación (OAP).

5.1 Estado Actual por Dimensiones de Control (ISO 27001:2022)

Para diagnosticar la madurez de la seguridad de la información en la UBPD, se evaluaron los cuatro dominios de control establecidos en el Anexo A de la norma ISO 27001:2022, comparando la situación operativa frente a las exigencias de gestión del MSPI. La escala de valoración del instrumento institucional establece que el rango entre 80% y 99% corresponde al nivel **Gestionado**, mientras que la denominación de **Optimizado** exige el cumplimiento del 100%. A continuación, se presenta la consolidación del diagnóstico por dimensiones y la brecha general frente al modelo de gestión.

Tabla 1. Resultado de la evaluación de controles por dimensiones (ISO 27001:2022 Anexo A vs. Cláusulas MSPI)

Dimensión Evaluada (Anexo A)	Resultado Actual	Meta	Estado de Madurez y Diagnóstico
Controles Organizacionales (A.5)	82%	100%	Gestionado. Marcos y directrices vigentes; pendiente la automatización de flujos de revisión y actualización de procedimientos.
Controles de Personas (A.6)	83%	100%	Gestionado. Fortalezas en acuerdos de confidencialidad y selección; brechas en la articulación de acuerdos de nivel de servicio y régimen disciplinario.
Controles Físicos (A.7)	91%	100%	Gestionado Alto. Adecuada protección en la sede central; requiere homologar controles de acceso y custodia de archivos en sedes territoriales (GITT).
Controles Tecnológicos (A.8)	88%	100%	Gestionado Alto. Herramientas base desplegadas; riesgos focalizados en continuidad de servicios, respaldos periódicos y desarrollo seguro.
Promedio Anexo A (ISO 27001)	86%	100%	Base sólida de controles implementados, aún no optimizada.
Cláusulas MSPI / PHVA	70,4%	100%	Brecha estructural en tratamiento formal de riesgos, medición de desempeño, revisión por la dirección y mejora continua.

5.2. Madurez del Ciclo de Gestión del MSPI (PHVA)

El análisis del Modelo de Seguridad y Privacidad de la Información (MSPI) mediante el ciclo Planear-Hacer-Verificar-Actuar (PHVA) revela que, si bien la entidad cuenta con una fase de planificación desarrollada, existe un rezago acentuado en la ejecución de la evaluación del desempeño y la mejora continua. La siguiente tabla detalla la distribución del porcentaje de avance en cada fase del ciclo, identificando los puntos porcentuales (pp) requeridos para alcanzar el nivel objetivo.

Tabla 2. Nivel de avance y brechas por componentes del ciclo de gestión PHVA del MSPI

Componente PHVA	Avance Actual	Esperado	Brecha (pp)
Planificación	46,8%	56,0%	9,2 pp
Implementación	9,6%	16,0%	6,4 pp
Evaluación del Desempeño	8,4%	14,0%	5,6 pp
Mejora Continua	5,6%	14,0%	8,4 pp
Total Consolidado MSPI	70,4%	100,0%	29,6 pp

5.2.1 Brechas Críticas Identificadas en el Ciclo de Gestión

- **Tratamiento de Riesgos (Cláusula 8.3 - 0%):** Inexistencia de planes de tratamiento formalmente aprobados con asignación explícita de responsable, cronograma y presupuesto.
- **Mejora Continua (Cláusula 10.1 - 0%):** Ausencia de un procedimiento estandarizado para la gestión sistemática de no conformidades y acciones correctivas del sistema.
- **Comunicación e Intercambio (Cláusula 7.4 - 20%):** Necesidad de formalizar protocolos de transferencia segura de información física y digital con actores externos y aliados estratégicos.
- **Revisión por la Dirección (Cláusula 9.3 - 20%):** Falta de institucionalización de rendiciones de cuentas periódicas sobre el desempeño de la seguridad de la información ante el CEDI.
- **Componentes en Madurez Parcial (60%):** El alcance del sistema (4.3), la matriz de roles y responsabilidades (5.3), la metodología de gestión de riesgos (6.1) y los indicadores de gestión (9.1) requieren actualización para reflejar el modelo de operación actual.

5.3. Alineación con el Framework NIST CSF

Como complemento a la norma ISO 27001, la UBPD evalúa la madurez de sus capacidades técnicas a través del *National Institute of Standards and Technology Cybersecurity Framework* (NIST CSF). Este enfoque permite medir la capacidad institucional en las seis funciones fundamentales de ciberseguridad y determinar las prioridades de intervención para mitigar amenazas sobre la infraestructura y los ecosistemas de datos de la entidad.

Tabla 3. Nivel de madurez y priorización por funciones del Framework NIST CSF

Función NIST CSF	Resultado	Prioridad de Intervención	Diagnóstico de Capacidad
Gobernar (GV)	82%	Media	Existencia de políticas generales; requiere fortalecer la articulación interinstitucional.
Identificar (ID)	76%	Alta	Necesidad de afinar el inventario de activos de información y la valoración de riesgos por proceso.
Proteger (PR)	83%	Alta	Adecuados controles de acceso; requiere reforzar la protección de archivos físicos y cifrado.
Detectar (DE)	70%	Muy Alta	Punto crítico. Ausencia de un esquema centralizado de monitoreo continuo y correlación de eventos.
Responder (RS)	80%	Alta	Existen guías de atención de incidentes; requiere entrenamiento práctico y pruebas forenses.
Recuperar (RC)	80%	Alta	Planes BCP/DRP formulados; pendiente la ejecución periódica de pruebas de conmutación.

5.4. Fortalezas Institucionales

- **Gobernanza e Institucionalidad:** Contexto estratégico definido, política marco de seguridad de la información (GTI-PC-001) promulgada y respaldo formal del Comité Ejecutivo de Dirección Institucional (CEDI).
- **Factor Humano:** Procesos estructurados de verificación de antecedentes, acuerdos de confidencialidad en la vinculación y jornadas periódicas de sensibilización al personal.
- **Protección Física y Documental:** Esquemas de control de acceso a instalaciones centrales, definición de áreas de seguridad, políticas de escritorio limpio y procedimientos de destrucción segura de medios físicos.
- **Infraestructura Tecnológica:** Despliegue de protección en endpoints, esquemas de autenticación centralizada, protección contra código malicioso, segregación de redes y gestión de copias de respaldo.
- **Capacidad de Respuesta y Recuperación:** Existencia de procedimiento formal para atención de incidentes, formatos para preservación de evidencia digital, operación del Network Operations Center (NOC) y servicios de respaldo en la nube.
- **Gestión de Activos:** La UBPD dispone de un inventario general de activos de información y una matriz de riesgos consolidada como base para la toma de decisiones.

5.5. Debilidades y Brechas Prioritarias

Para garantizar que el plan atienda las causas raíz del nivel de exposición institucional, se priorizan las siguientes brechas operativas y de gestión:

1. **Gestión Deficitaria del Tratamiento de Riesgos:** Existencia de riesgos altos y extremos en la matriz institucional que carecen de planes de tratamiento aprobados, responsables asignados, presupuesto ejecutado y mecanismos de verificación de eficacia.

2. **Incompletitud en las Pruebas de Continuidad Operativa:** El Grupo Interno de Trabajo Gestión Tecnológica (GITGT) requiere actualizar el Análisis de Impacto del Negocio (BIA) para dimensionar los impactos de interrupción sobre la operación misional, así como estructurar y ejecutar las pruebas anuales de conmutación del Plan de Recuperación ante Desastres (DRP).
3. **Descentralización del Monitoreo y Detección:** Falta de un esquema unificado para la correlación de eventos de seguridad (SIEM/SOC) que permita detectar oportunamente intrusiones, desviaciones o accesos no autorizados sobre la infraestructura física y lógica.
4. **Heterogeneidad de Controles en Territorio:** Brechas de infraestructura, custodia documental y seguridad física en las sedes de los Grupos Internos de Trabajo Territoriales (GITT) en comparación con el nivel central.
5. **Formalización del Ciclo PHVA:** Falta de un mecanismo sistemático para el reporte de indicadores de desempeño, la ejecución de autodiagnósticos periódicos y la formalización de planes de mejoramiento presentados ante la Alta Dirección.

5.6. Articulación Estratégica y Operativa PESI - PETI (2026-2028)

Para asegurar la coherencia institucional y responder a la necesidad de unificar la visión tecnológica bajo un único ecosistema seguro y resiliente, el Plan Estratégico de Seguridad y Privacidad de la Información (PESI) se articula directamente con el Plan Estratégico de Tecnologías de la Información (PETI 2026-2028 / GTI-PL-001 V3).

Al estructurar esta alineación, la UBPD asegura que cada inversión en hardware, licenciamiento en la nube o canales de conectividad gestionados por el Grupo Interno de Trabajo de Gestión Tecnológica (GITGT) incorpore la seguridad digital *"desde el diseño y por defecto"*. Este enfoque preventivo y coordinado permite que la modernización de los sistemas informáticos avance a la par del robustecimiento de los controles lógicos, blindando la infraestructura crítica frente a incidentes que puedan comprometer la confidencialidad de los datos de las víctimas y la estricta reserva legal que rige el mandato humanitario de búsqueda.

Desde el punto de vista operativo y normativo, esta sinergia metodológica da cumplimiento exacto a la Cláusula 8.1 (*Planificación y Control Operacional*) de la norma ISO 27001:2022 y a los lineamientos del MSPI del MinTIC, la cual exige que la entidad planifique, implemente y controle los procesos necesarios para cumplir con los requisitos de seguridad de la información. La Unidad opera este mandato enlazando de forma directa las salvaguardas del PESI con el portafolio de proyectos, los catálogos técnicos del PETI y las instancias de gobernanza formalizadas en la Resolución 297 de 2026, articulándose en cada uno de los 5 ejes estratégicos:

- **Alineación con la Estrategia 1 (Gobernanza y Alineación Estratégica):** Se integra directamente con el dominio de *Gobierno de TI* del PETI y con la aplicación de la Resolución 297 de 2026, la cual establece los roles, comités de dirección y niveles de autoridad para la toma de decisiones tecnológicas en la Unidad. Encuentra su viabilidad técnica en el Catálogo de Sistemas de Información (Anexo GTI-FT-042) mediante el uso de la suite corporativa **QuickDataERP**, plataforma encargada del inventario institucional y la clasificación estricta de los activos de información de acuerdo con su nivel de criticidad frente a la tríada de seguridad (confidencialidad, integridad y disponibilidad).

- **Alineación con la Estrategia 2 (Gestión Integral de Riesgos y Prevención de Amenazas):** El requerimiento del PESI de transitar hacia una Matriz de Riesgos Automatizada se viabiliza a través del dominio de *Estrategia de TI* y los hitos lógicos definidos en la Hoja de Ruta de Proyectos de TI del PETI. Esta directriz se apalanca en la ejecución del proyecto "**Herramientas especializadas con controles tecnológicos de Seguridad Digital (Forti-SIEM, DLP, NAC Heimcore, FortiMail, análisis PaaS y SOC como servicio)**", interconectando los sensores perimetrales con el Catálogo de Componentes de Información para actualizar dinámicamente la exposición al riesgo técnico sin depender de procesos manuales estáticos, complementado con la solución **TeamPass** para la administración centralizada y almacenamiento seguro de credenciales.
- **Alineación con la Estrategia 3 (Resiliencia y Continuidad Operativa):** Se fundamenta directamente en el dominio de *Infraestructura de TI* del PETI, alineándose de manera estricta con los diagramas de flujo de Conectividad Internet y WAN y los esquemas de la Proyección DRP (modelo Activo-CPP / Activo-CAL en Kubernetes). La obligatoriedad de respaldar y salvaguardar los datos misionales (SIM, SIDOBU, Gestionemos) encuentra su soporte técnico en la iniciativa estratégica de **Hiperconvergencia (Soportes, Actualizaciones, Licenciamientos Veeam y Continuidad)** descrita en el portafolio del GITGT, la cual utiliza los recursos del Catálogo de Elementos de Infraestructura (Anexo) para garantizar el cumplimiento estricto de los objetivos de tiempo de recuperación (RTO) y punto de recuperación (RPO) ante contingencias ambientales o fallas críticas.
- **Alineación con la Estrategia 4 (Ciberdefensa y Aseguramiento Técnico de la Infraestructura):** Su correspondencia operativa está fijada en el dominio de *Seguridad de la Información* del PETI y responde lógicamente a los flujos técnicos modelados en la Ilustración 14 (*Arquitectura de Seguridad*). El despliegue de agentes EDR/XDR (FortiClient), WAF Cloud, FortiSOAR y la adquisición de la solución licenciada corporativa para la asistencia técnica remota segura con cifrado de extremo a extremo y autenticación multifactor (MFA), se viabilizan presupuestalmente mediante el proyecto "**Conectividad y Mesa de Ayuda**", operando bajo la plataforma de software corporativo **Aranda SAS** (módulo de mesa de servicio e inventario lógicos) registrada en el Catálogo de Servicios de TI (Anexo GTI-FT-047).
- **Alineación con la Estrategia 5 (Cultura Digital y Apropiación del Factor Humano):** Se mapea transversalmente con el dominio de *Uso y Apropiación de TI* del PETI y los compromisos normativos evaluados a través del Formulario Único de Reporte de Avances de la Gestión (FURAG). Las campañas trimestrales de *phishing* ético y las jornadas de capacitación en reserva legal para el personal del nivel central y territorial (GITT) se soportan tecnológicamente en la plataforma **Moodle (Sistema de Gestión de Aprendizaje)**, la cual se encuentra plenamente integrada en la infraestructura del GITGT y se articula estratégicamente con las directrices de la Estrategia de Comunicación del PETI.

VI. EJES DE ACCIÓN, LÍNEAS OPERATIVAS Y FORMULACIÓN DE METAS

La Unidad de Búsqueda de Personas dadas por Desaparecidas (UBPD) establece la estrategia general del Plan Estratégico de Seguridad y Privacidad de la Información (PESI 2026-2028) como

un esquema integral, resiliente y adaptado al carácter **humanitario y extrajudicial** de su mandato. Esta estrategia articula los principios, políticas, procedimientos, guías, manuales y formatos institucionales bajo el liderazgo y supervisión del Oficial de Seguridad de la Información (OSI) en coordinación con el Grupo Interno de Trabajo Gestión Tecnológica (GITGT), garantizando la consolidación del Modelo de Seguridad y Privacidad de la Información (MSPI) y su engranaje directo con el Plan Estratégico de Tecnologías de la Información (PETI 2026-2028 / GTI-PL-001 V3).

A fin de asegurar la máxima confidencialidad, integridad y disponibilidad sobre la información de víctimas, aportantes, personas buscadoras, expedientes de investigación y registros administrativos, la UBPD adopta las mejores prácticas de la norma ISO/IEC 27001:2022 y las directrices del MinTIC. Tomando como base la Política de Seguridad de la Información (**GTI-PC-001**) y el Manual de Seguridad de la Información (**GTI-MN-002**), el PESI protege transversalmente los procesos misionales de investigación humanitaria, así como los procesos estratégicos, de soporte (administrativo, financiero, documental, jurídico, contractual y de talento humano) y de evaluación y control, tanto en la sede central como en las 33 sedes de los Grupos Internos de Trabajo Territoriales (GITT) y despliegues en campo.

El Plan se estructura en los siguientes cinco (5) Ejes de Acción:

Figura 1. Ejes de acción. PESI, 2026 – 2028. UBPD



6.1. Ejes de Acción

Eje 1. Liderazgo de Seguridad de la Información y Gobernanza

Este eje define la articulación normativa y la toma de decisiones para blindar la reserva legal y la confianza institucional que sustenta la búsqueda humanitaria y extrajudicial.

Para la ejecución efectiva del PESI, este eje orienta la participación técnica y administrativa en la actualización de los marcos normativos internos. Su propósito central comprende la revisión integral de la política GTI-PC-001 para adaptar las directrices institucionales a las realidades operativas de la UBPD. Asimismo, establece un modelo de supervisión continua mediante ciclos anuales de autodiagnóstico y evaluación de cumplimiento de los controles ISO 27001:2022 e indicadores del MinTIC (FURAG), sometiendo los resultados a la revisión formal del Comité

Ejecutivo de Dirección Institucional (CEDI/CIGD) para respaldar tanto el desarrollo misional como la gestión transparente de los procesos de soporte administrativo.

Eje. 2. Gestión Integral de Riesgos y Ciberresiliencia

Como pilar preventivo del PESI, este eje transforma la *Matriz Institucional de Riesgos de la UBPD*, en su componente de Seguridad y Privacidad de la Información, articulado al Sistema Integrado de Gestión (SIG) y al Modelo Estándar de Control Interno (MECI), en un instrumento dinámico, proactivo y automatizado, conforme al artículo 6 de la Resolución 500 de 2021 y la Resolución 02277 de 2025 del MinTIC.

Bajo este marco, la entidad clasifica y protege los activos críticos registrados en *QuickDataERP*, abarcando de manera transversal los procesos estratégicos, misionales, de apoyo y de evaluación, desde los módulos del Sistema de Información Misional (SIM) hasta las plataformas de gestión administrativa, contractual y presupuestal (*Gestionemos*, *Tramitemos*) en el Nivel Central y en las sedes de los GITT.

Así mediante el despliegue del Plan de Tratamiento de Riesgos (PTR) y la integración de módulos de observabilidad y herramientas técnicas especializadas (NCM, IPAM, SRM, SEM, Forti-SIEM, DLP, NAC y *TeamPass*), la UBPD neutraliza las exposiciones valoradas en nivel "Extremo" o "Alto" que puedan comprometer la reserva legal de las víctimas o la estabilidad operativa de la institución, garantizando la evaluación semestral del riesgo residual conforme a los estándares de la norma ISO/IEC 27001:2022.

Eje 3. Implementación de Controles, Resiliencia y Continuidad

Este eje tiene como propósito garantizar la ininterrupción del mandato humanitario y de los procesos de soporte administrativo ante contingencias tecnológicas, desastres físicos o ciberataques.

Mediante la articulación del Plan de Continuidad del Negocio (BCP) y el Plan de Recuperación ante Desastres (DRP) bajo el estándar ISO/IEC 27001:2022, la UBPD define técnicamente las métricas de tiempo de recuperación (RTO) y punto de recuperación (RPO) para salvaguardar las bases de datos misionales, el Sistema de Gestión Documental (*SIDOB*) y los expedientes físicos custodiados en el Nivel Central y en las sedes territoriales (GITT).

Esta resiliencia se soporta en una arquitectura hiperconvergente con respaldos Veeam, monitoreo en nube e híbrido (SAM, DPA, SRM) y un esquema *DRP Activo-CPP / Activo-CAL Automático-Asistido* en Kubernetes con replicación geográfica cifrada, cuya efectividad se valida mediante simulacros periódicos de conmutación reportados ante el Comité Ejecutivo de Dirección Institucional (CEDI).

Eje 4. Gestión de Incidentes, Ciberdefensa y Aseguramiento Técnico

Esta eje se orienta al blindaje físico, perimetral y lógico de la infraestructura institucional que soporta la captación de información en campo, los datos testimoniales, las herramientas de analítica avanzada, los modelos de inteligencia artificial y los cruces masivos de bases de datos

requeridos para la investigación humanitaria y extrajudicial, así como la operación de los sistemas administrativos y de soporte.

Mediante un esquema de ciberdefensa proactiva y aseguramiento técnico perimetral en el Nivel Central y en las 33 sedes de los GITT, la UBPD previene, detecta y reacciona ante amenazas avanzadas como el secuestro de información (*Ransomware*) o la exfiltración de datos. Para ello, despliega agentes FortiClient EDR/XDR, interconexión SD-WAN, WAF Cloud, FortiSOAR, autenticación multifactor (MFA) y monitoreo de tráfico de red (NPM, NTA).

Asimismo, estandariza el soporte remoto seguro con cifrado de extremo a extremo canalizado en la plataforma *Aranda* SAS y la analítica centralizada de registros (*logs* con SEM y LA), garantizando la generación de evidencias técnicas para el reporte obligatorio de incidentes ante el ColCERT, el cumplimiento de los ANS y la protección integral de la reserva legal de la información.

Eje 5. Concientización, Cultura Digital y Factor Humano

Este eje se orienta a fortalecer las capacidades de la organización desde el comportamiento de las personas, consolidando el "firewall humano" de la entidad y promoviendo la responsabilidad ética, legal y operativa de servidores públicos, contratistas y pasantes como primeros custodios de la información de las víctimas y de los recursos institucionales. Bajo los lineamientos de la norma ISO/IEC 27001:2022, la Resolución 02277 de 2025 y las directrices de Gobierno Digital del MinTIC, la UBPD implementa un Plan Institucional de Capacitación a través del entorno virtual de aprendizaje *Moodle* (LMS), abarcando contenidos en ciberseguridad, reserva legal, hábitos digitales seguros y gestión responsable de archivos confidenciales físicos y digitales. Asimismo, la estrategia aplica evaluaciones diagnósticas y ejecuta simulacros periódicos de ingeniería social (*phishing* ético) y ejercicios de fuga de información, permitiendo medir, evaluar y reducir de manera sistemática la vulnerabilidad del factor humano en los procesos del Nivel Central y en las sedes territoriales (GITT).

6.2. Líneas Operativas

Las líneas operativas constituyen los frentes específicos de trabajo en los que se despliegan las capacidades técnicas, administrativas y operativas de los procesos intervinientes en la UBPD. Estas líneas operativizan las salvaguardas del Modelo de Seguridad y Privacidad de la Información (MSPI) sobre el ciclo de vida de la información, abarcando desde las actividades de investigación humanitaria y extrajudicial en territorio hasta los procesos de soporte administrativo, financiero, jurídico, contractual y de gestión documental.

A través de catorce (14) líneas operativas, articuladas con los cuatro dominios de control normados por la ISO/IEC 27001:2022 (Organizacionales, de Personas, Físicos y Tecnológicos), la entidad materializa el cumplimiento de sus cinco ejes estratégicos.

6.2.1 Líneas Operativas del Eje 1: Liderazgo de Seguridad de la Información y Gobernanza

Línea Operativa 1.1. Actualización y armonización del marco normativo interno

Revisión, ajuste y formalización periódica de la Política General de Seguridad de la Información (**GTI-PC-001**) y del Manual del MSPI (**GTI-MN-002**). Adapta las reglas institucionales de reserva legal, confidencialidad y uso de activos bajo la articulación del OSI, el OPD (privacidad desde el diseño) y la STIH (reserva extrajudicial del SIM) ante el CEDI.

Línea Operativa 1.2. Monitoreo, autodiagnóstico y evaluación del cumplimiento

Ejecución de ciclos anuales de autodiagnóstico sobre los controles de la norma ISO/IEC 27001:2022 y evaluación de los indicadores de la Política de Gobierno Digital registrados en el FURAG del MinTIC.

Además estructura planes de mejoramiento técnico liderados por el OSI y el OPD sin interferir con la evaluación independiente de Control Interno

Línea Operativa 1.3. Rendición de cuentas e informes de desempeño ante la Alta Dirección

Consolidación de reportes ejecutivos, indicadores del SSPI y estado de excepciones críticas para ser presentados por el OSI, el OPD y la STIH ante el Comité Ejecutivo de Dirección Institucional (CEDI / CIGD), garantizando la toma de decisiones basadas en evidencia y el blindaje institucional de la reserva legal.

6.2.2 Líneas Operativas del Eje 2: Gestión Integral de Riesgos y Ciberresiliencia

Línea Operativa 2.1. Automatización de la matriz institucional de riesgos y clasificación de activos

Integración de la Matriz Institucional de Riesgos de Seguridad de la Información, articulada al Sistema Integrado de Gestión (SIG) y al MEC, con el inventario de activos información. Clasifica y valora dinámicamente la criticidad de los activos pertenecientes al Sistema de Información Misional (SIM), *Gestionemos*, *Tramitemos*, *SIDOB* y repositorios de datos, requiriendo el aval de la STIH sobre activos misionales y del OPD sobre bases con datos personales sensibles.

Línea Operativa 2.2. Ejecución de los Planes de Tratamiento de Riesgos (PTR) y controles técnicos

Formulación, asignación presupuestal y despliegue de salvaguardas técnicas definidas en el Anexo 1, nos permite fortalecer la UBPD de acuerdo con los lineamientos establecidos en la Resolución 500 de 2021 y la Resolución 02277 de 2025 del MinTIC. Incorporando plataformas de monitoreo (NCM, IPAM, SRM, SEM, Forti-SIEM, DLP, NAC y SOC como servicio) y la herramienta *TeamPass* para la administración centralizada y almacenamiento cifrado de credenciales institucionales, así como los protocolos de la STIH para la recepción segura de medios externos de víctimas, aportantes y esquemas BYOD en campo

Línea Operativa 2.3. Valoración del riesgo residual y evaluación de cambios tecnológicos

Evaluación semestral de la efectividad de los controles y revaloración del riesgo residual ante la adopción de nuevas plataformas, modelos de analítica, inteligencia artificial o despliegues operacionales en territorio.

6.2.3 Líneas Operativas del Eje 3: Implementación de Controles, Resiliencia y Continuidad

Línea Operativa 3.1. Actualización del Análisis de Impacto del Negocio (BIA)

Evaluación periódica de los procesos misionales, estratégicos, de soporte y de evaluación del Modelo Operativo de Procesos (MOP). Establece los Objetivos de Tiempo de Recuperación (RTO) y Punto de Recuperación (RPO) tolerables para garantizar la ininterrupción de la investigación de campo y la gestión administrativa.

Línea Operativa 3.2. Gestión de la infraestructura de almacenamiento y respaldos

Operación y monitoreo continuo de servidores, bases de datos y repositorios de información a través de soluciones híbridas y en la nube (SAM, DPA, SRM, respaldos Veeam e infraestructura hiperconvergente). Garantiza la disponibilidad e integridad del Sistema de Gestión Documental (SIDOBU), del Archivo Misional para la Búsqueda y de las bases de datos de la entidad.

Línea Operativa 3.3. Simulacros DRP/BCP y custodia de fondos documentales territoriales

Ejecución anual de pruebas de conmutación sobre la arquitectura DRP Activo-CPP / Activo-CAL Automático-Asistido en Kubernetes con replicación geográfica cifrada. Incluye la estandarización y auditoría de protocolos de custodia física para archivos en papel y medios magnéticos en las 33 sedes de los GITT.

6.2.4 Líneas Operativas del Eje 4: Gestión de Incidentes, Ciberdefensa y Aseguramiento Técnico

Línea Operativa 4.1. Despliegue de capacidades de ciberdefensa perimetral e interna

Implementación y mantenimiento de agentes FortiClient EDR/XDR, interconexión SD-WAN para las 33 sedes territoriales, WAF Cloud, FortiSOAR, autenticación multifactor (MFA) y herramientas de supervisión de tráfico (NPM, NTA). Protege la captación de información en campo, los modelos de analítica de datos e IA y las plataformas administrativas frente a *ransomware* y ciberamenazas.

Línea Operativa 4.2. Estandarización de la asistencia técnica remota segura

Operación de soluciones licenciadas de soporte remoto con cifrado de punto a punto, autenticación multifactor y registro de auditoría canalizado mediante la mesa de servicio Aranda SAS. Elimina el uso de software no autorizado en equipos corporativos y territoriales.

Línea Operativa 4.3. Correlación de eventos, atención de incidentes y reporte a autoridades

Centralización y análisis de registros (*logs* mediante SEM y LA) para la detección temprana de anomalías. Asegura la gestión de incidentes bajo Acuerdos de Nivel de Servicio (ANS), la preservación de evidencia digital y el reporte obligatorio de eventos críticos ante el ColCERT.

6.2.5 Líneas Operativas del Eje 5: Concientización, Cultura Digital y Factor Humano

Línea Operativa 5.1. Ejecución del Plan Institucional de Capacitación en Seguridad y Privacidad y Reserva

Formación continua para servidores públicos, contratistas y pasantes del Nivel Central y territorial a través del entorno virtual *Moodle* (LMS). Desarrolla competencias sobre manejo de información reservada, deberes ético-legales, protección de datos de víctimas, hábitos digitales seguros, uso seguro de IA.

Línea Operativa 5.2. Simulacros de ingeniería social y evaluación del factor humano

Realización periódica de ejercicios controlados de *phishing* ético y pruebas de simulación de fuga de información. Mide y reduce de manera sistemática la tasa de vulnerabilidad del personal ante técnicas de manipulación digital.

6.3. Metas Plurianuales / Anuales

Las metas plurianuales y anuales constituyen los compromisos cuantitativos y cualitativos de gestión que la Unidad de Búsqueda de Personas dadas por Desaparecidas (UBPD) se obliga a alcanzar durante el trienio 2026-2028. Estos compromisos garantizan la evolución progresiva del Sistema de Seguridad y Privacidad de la Información (SSPI), elevando el nivel de madurez del 70,4% al 100% en el ciclo PHVA del MSPI y optimizando los controles del Anexo A de la norma ISO/IEC 27001:2022.

La distribución temporal fija hitos de cumplimiento desde la aprobación del plan (1 de octubre de 2026) hasta el 31 de diciembre de 2028, alineando la asignación presupuestal y operativa del Grupo Interno de Trabajo Gestión Tecnológica (GITGT), la Oficialía de Seguridad de la Información (OSI), el Oficial de Protección de Datos Personales (OPD) y la Subdirección Técnica de Investigación Humanitaria (STIH):

Tabla 4. Compromisos Cuantitativos de Gestión: Metas Plurianuales y Anuales. PESI (2026-2028)

Eje estratégico	Meta plurianual 2026–2028	Meta anual 2026 T4	Meta anual 2027	Meta anual 2028	Indicadores y fórmulas
Eje 1: Gobernanza y liderazgo	Formalizar el 100% de los dos documentos normativos programados, ejecutar 3 autodiagnósticos MSPI/ISO 27001	Actualizar, aprobar y publicar la Política GTI-PC-001 V4 y el Manual GTI-MN-002 V3; ejecutar 1	Verificar la vigencia del marco normativo; ejecutar 1 autodiagnóstico y presentar 2 informes semestrales de desempeño y	Evaluar y actualizar el marco normativo si procede; ejecutar 1 autodiagnóstico de cierre y	Documentos formalizados = documentos aprobados y publicados / 2 × 100. Autodiagnósticos = ejecutados / 3

Eje estratégico	Meta plurianual 2026–2028	Meta anual 2026 T4	Meta anual 2027	Meta anual 2028	Indicadores y fórmulas
	y presentar 5 informes de desempeño al CEDI en el trienio.	autodiagnóstico MSPI y presentar 1 informe al CEDI.	excepciones al CEDI.	presentar 2 informes de gestión al CEDI.	$\times 100$. Informes CEDI = presentados / 5 $\times 100$.
Eje 2: Gestión integral de riesgos	Ejecutar y verificar el 100% de las acciones de los PTR aprobados para riesgos altos y extremos, clasificar el 100% de activos del alcance, integrar la matriz con SIG/MECI en 2027 y aplicar AIA ex ante al 100% de proyectos de IA que lleguen a producción.	Clasificar el 100% de los activos misionales y de soporte del alcance en QuickDataERP y desplegar TeamPass y el SOC como servicio. Aplicar AIA ex ante a los proyectos de IA que entren en producción.	Ejecutar y verificar los controles de los PTR programados, integrar la matriz automatizada con SIG/MECI a diciembre de 2027, documentar 2 evaluaciones formales de riesgo residual y mantener revisiones trimestrales de umbrales.	Mantener operativa la matriz integrada, verificar el cumplimiento de los PTR y efectuar AIA ex ante en el 100% de los proyectos de IA antes de su producción. Mantener las revisiones trimestrales y las evaluaciones semestrales de riesgo residual.	$PTR = \text{acciones ejecutadas y verificadas} / \text{acciones programadas en los PTR} \times 100$. $\text{Activos} = \text{activos clasificados} / \text{activos identificados en el alcance} \times 100$. $AIA = \text{proyectos evaluados antes de producción} / \text{proyectos que llegan a producción} \times 100$.
Eje 3: Resiliencia y continuidad	Actualizar el BIA sobre el 100% de los procesos del MOP, ejecutar 54 pruebas de restauración, 5 simulacros DRP y auditar las 33 sedes GITT.	Aprobar el BIA con RTO/RPO; realizar 6 pruebas de restauración y 1 simulacro DRP. Tramitar la actualización del BCP, cuya publicación está programada para junio de 2027.	Publicar el BCP; realizar 24 pruebas de restauración y 2 simulacros DRP; auditar al menos 17 de las 33 sedes GITT (más del 50%).	Realizar 24 pruebas de restauración y 2 simulacros DRP; culminar la auditoría acumulada de las 33 sedes GITT.	$BIA = \text{procesos cubiertos} / \text{procesos del MOP} \times 100$. $\text{Restauración} = \text{pruebas exitosas} / \text{pruebas programadas} \times 100$. $DRP = \text{simulacros exitosos} / \text{simulacros programados} \times 100$. $\text{Custodia} = \text{sedes auditadas} / 33 \times 100$.
Eje 4: Ciberdefensa y aseguramiento	Alcanzar el 100% de cobertura EDR/XDR en los equipos del alcance y SD-WAN en las 33 sedes programadas; cerrar el 100% de los incidentes dentro del ANS; habilitar	Desplegar agentes EDR/XDR en el 100% de equipos del alcance, activar soporte remoto cifrado con MFA en Aranda SAS y monitoreo SOC/SIEM permanente.	Operar SD-WAN en las 33 sedes, habilitar Sandbox para IA y cerrar el 100% de los incidentes dentro del ANS. Reportar los eventos críticos a ColCERT y las brechas de datos personales a la SIC, por conducto	Mantener cobertura de ciberdefensa, cerrar el 100% de los incidentes dentro del ANS y verificar la aplicación del protocolo BYOD y el borrado seguro al cierre de las	$EDR = \text{equipos protegidos} / \text{equipos del alcance} \times 100$. $SD-WAN = \text{sedes conectadas} / 33 \times 100$. $ANS = \text{incidentes cerrados dentro del ANS} / \text{incidentes}$

Eje estratégico	Meta plurianual 2026–2028	Meta anual 2026 T4	Meta anual 2027	Meta anual 2028	Indicadores y fórmulas
	entornos Sandbox y aplicar el protocolo BYOD.		del OPD, cuando corresponda.	comisiones que utilicen dispositivos personales.	registrados $\times$ 100. BYOD = comisiones verificadas / comisiones con BYOD $\times$ 100.
Eje 5: Factor humano y cultura	Configurar el entorno virtual institucional sin costo de licenciamiento, certificar al menos al 85% del personal activo en 2028, ejecutar 9 simulacros de phishing y alcanzar una vulnerabilidad inferior al 10%.	Diseñar el curso de reserva legal, ciberseguridad e IA responsable, y ejecutar 1 simulacro de phishing ético en T4.	Configurar Moodle Open Source o aulas de MS Teams/SharePoint, hacer pruebas piloto y ejecutar 4 simulacros trimestrales de phishing.	Poner en marcha la formación, certificar al menos al 85% del personal activo, ejecutar 4 simulacros y mantener la vulnerabilidad ante phishing $<$ 10%.	Formación = personas certificadas / personal activo $\times$ 100. Phishing = participantes únicos que interactúan con el señuelo / participantes únicos del simulacro $\times$ 100. Simulacros ejecutados = realizados / 9 $\times$ 100.

6.3.1. Desglose de Compromisos Anuales de Ejecución

1. Vigencia 2026 (1 de octubre a 31 de diciembre - Corto Plazo):

- Formalizar la actualización de la Política GTI-PC-001 y el Manual GTI-MN-002 adaptando las reglas de reserva legal del SIM (Decreto Ley 589 de 2017) y protección de datos (Ley 1581 de 2012) antes del 30 de noviembre de 2026.
- Completar la carga e inventario del 100% de activos de información en *QuickDataERP* al 30 de noviembre de 2026.
- Publicar el estudio BIA actualizado con la matriz RTO/RPO aprobada por CEDI al 15 de diciembre de 2026.
- Desplegar agentes FortiClient EDR/XDR en el 100% de equipos corporativos al 31 de diciembre de 2026.
- Diseñar los contenidos pedagógicos y la estructura técnica del curso institucional de reserva legal, ciberseguridad e IA responsable al 15 de diciembre de 2026.

2. Vigencia 2027 (1 de enero a 31 de diciembre - Mediano Plazo):

- Desplegar y poner en operación los módulos de observabilidad técnica (Forti-SIEM, DLP, NAC) y el protocolo STIH para la recepción segura de medios externos en comisiones de campo al 30 de noviembre de 2027.
- Habilitar entornos *Sandbox* lógicamente aislados para pruebas de modelos de Inteligencia Artificial misional al 31 de marzo de 2027.
- Auditar e inspeccionar el protocolo de custodia física y ambiental en el 50% de las sedes territoriales GITT (17 sedes) al 30 de junio de 2027.

- Instalar y configurar la plataforma *Moodle Open Source* en servidores de la UBPD o habilitar la estructura de aulas en la suite corporativa (MS Teams / SharePoint) al 30 de noviembre de 2027.
 - Ejecutar 4 campañas trimestrales de *phishing* ético y 2 simulacros de conmutación DRP (30 de mayo y 30 de noviembre de 2027).
3. **Vigencia 2028 (1 de enero a 31 de diciembre - Largo Plazo):**
- Consolidar la automatización en tiempo real de la Matriz Institucional de Riesgos GSI-MT-004 en el SIG/MECI mediante paneles de control (Dashboards).
 - Culminar las auditorías de custodia física y ambiental en el 100% de las sedes de los GITT (33 sedes) al 30 de junio de 2028.
 - Ejecutar el 100% de las Evaluaciones de Impacto Algorítmico (AIA ex-ante) sobre desarrollos o contrataciones de IA misional.
 - **Lanzar formalmente el entorno virtual de formación (Moodle Open Source / MS Teams) con el curso obligatorio de reserva legal, ciberseguridad e IA al 15 de diciembre de 2028**, logrando la certificación de al menos el 85% del personal activo de la UBPD (planta y contratistas) en articulación con las jornadas presenciales de socialización.
 - Certificar la contención de la tasa de vulnerabilidad por engaño digital por debajo del 10% al 30 de diciembre de 2028.

6.4. Matriz programática del plan

La Matriz Programática constituye el instrumento de planificación operacional que despliega las acciones concretas para materializar las catorce (14) líneas operativas del plan. Define la distribución de responsabilidades institucionales y organiza la ejecución en un horizonte temporal estructurado en: **Corto Plazo (Año 1 / 2026)** para acciones de formalización, diseño e implementación prioritaria; **Mediano Plazo (Año 2 / 2027)** para la consolidación, integración de herramientas y auditorías territoriales; **Largo Plazo (Año 3 / 2028)** para la optimización, maduración y evaluación integral del modelo; y **Acciones Continuas (Transversales 2026-2028)** para actividades de monitoreo, operación permanente, capacitación y rendición de cuentas.

En el Anexo 1 se encuentra la Matriz Programática del PESI.

VII. RECURSOS Y PROYECCIÓN PRESUPUESTAL

La viabilidad, sostenibilidad financiera y eficiencia operacional del Plan Estratégico de Seguridad y Privacidad de la Información (PESI 2026-2028) se fundamentan en una estricta alineación con el Plan Estratégico de Tecnologías de la Información (PETI / GTI-PL-001 V3), el Plan de Acción Institucional (PAI) y el Presupuesto Anual de la UBPD.

7.1. Proyección de Presupuesto Financiero (2026-2028)

La estimación de los recursos financieros requeridos para la ejecución de las catorce (14) líneas operativas del PESI se proyecta en millones de pesos y se desglosa entre **Gastos de Inversión** (adquisición, fortalecimiento y despliegue de capacidades tecnológicas y proyectos PAI) y

Gastos de Funcionamiento / Operación (sostenimiento de licencias corporativas, servicios administrados de ciberseguridad, enlaces de conectividad y soporte técnico).

El Plan Estratégico de Seguridad y Privacidad de la Información (PESI) contempla un monto total estimado de **cinco mil treinta millones de pesos colombianos (\$5.030 Millones COP)** para su ejecución en el trienio 2026-2028. Esta asignación financiera se distribuye en **\$620 Millones COP** para la vigencia de inicio 2026 (correspondiente al cuarto trimestre), **\$2.230 Millones COP** para la vigencia 2027 y **\$2.180 Millones COP** para la vigencia 2028, financiados a través de los rubros de inversión y funcionamiento articulados con el PETI y el PAI. El 64,6% del presupuesto asignado (\$3.250 Millones COP) se concentra en las capacidades operativas de ciberdefensa, conectividad cifrada, alta disponibilidad e infraestructura hiperconvergente (Ejes 3 y 4), garantizando la continuidad del mandato humanitario de búsqueda y la protección de los datos de las víctimas en el marco de la confidencialidad que involucra el carácter extrajudicial de la UBPD.

Tabla 5. Proyección Presupuestal Plurianual Estimada por Eje Estratégico en Pesos Colombianos (2026-2028)

(Cifras expresadas en millones de pesos colombianos - \$ COP)

Eje estratégico	Componente tecnológico y operativo	Tipo de presupuestos	2026 T4	2027	2028	Total (millones COP)	Articulación PETI / PAI y referencias normativas
Eje 1: Gobernanza y liderazgo	Asesoría técnica, actualización de la Política GTI-PC-001 V4 y el Manual GTI-MN-002 V3, 3 autodiagnósticos MSPI/ISO 27001 y 5 informes al CEDI (1 en 2026 y 2 en cada año siguiente).	Inversión / funcionamiento	\$50	\$120	\$130	\$300	Fortalecimiento institucional y PAI. Referencia institucional a la Resolución 297/2026 según el PESI; MSPI (Resolución MinTIC 500/2021, actualizada por la 2277/2025) y FURAG de Función Pública.
Eje 2: Gestión integral de riesgos	QuickDataERP y matriz de riesgos integrada al SIG/MECI en 2027; formulación y ejecución de PTR, herramientas NCM, IPAM, SEM, Forti-SIEM, DLP, NAC y TeamPass; integración técnica inicial con el SOC y evaluaciones AIA ex ante. La operación recurrente del SOC	Inversión / funcionamiento	\$180	\$650	\$500	\$1.330	Proyecto de inversión TI y PETI. Gestión de riesgos conforme al artículo 6 de la Resolución MinTIC 500/2021, con el MSPI actualizado por la Resolución 2277/2025; Ley 1581/2012.

Eje estratégico	Componente tecnológico y operativo	Tipo de presupuesto	2026 T4	2027	2028	Total (millones COP)	Articulación PETI / PAI y referencias normativas
	se registra en el eje 4.						
Eje 3: Resiliencia y continuidad	Actualización del BIA y BCP; hiperconvergencia, Veeam Backup y monitoreo SAM/DPA; 54 pruebas de restauración (6/24/24), 5 simulacros DRP (1/2/2) y auditoría de custodia en 33 sedes GITT (al menos 17 en 2027 y 33 acumuladas en 2028).	Inversión / funcionamiento	\$120	\$550	\$580	\$1.250	Infraestructura TI y continuidad en PETI, con Secretaría General para custodia física. Decreto Ley 589/2017, Ley 594/2000 y referencia técnica ISO 22301.
Eje 4: Ciberdefensa y aseguramiento	Agentes FortiClient EDR/XDR, red SD-WAN en 33 sedes, WAF Cloud y FortiSOAR; SOC 24/7 como servicio operativo, respuesta a incidentes, soporte remoto cifrado con MFA (Aranda SAS), NPM/NTA, Sandbox para IA y aplicación de BYOD.	Funcionamiento	\$250	\$850	\$900	\$2.000	Servicios gestionados de redes y telecomunicaciones. MSPI de la Resolución MinTIC 500/2021 actualizado por la 2277/2025; procedimientos aplicables de reporte de incidentes a ColCERT y de protección de datos personales ante la SIC.
Eje 5: Factor humano y cultura	Diseño pedagógico; Moodle Open Source en infraestructura propia o aulas MS Teams/SharePoint sin costo adicional de licencias; 9 simulacros de phishing (1/4/4), socialización y	Inversión / funcionamiento	\$20	\$60	\$70	\$150	Plan Institucional de Capacitación, OACP y Gestión Humana. Capacitación anual prevista en la Resolución MinTIC 500/2021 (art.

Eje estratégico	Componente tecnológico y operativo	Tipo de presupuesto	2026 T4	2027	2028	Total (millones COP)	Articulación PETI / PAI y referencias normativas
	certificación de al menos el 85% del personal activo en 2028.						5, numeral 4), Decreto 1083/2015 y directrices de austeridad aplicables.
TOTAL PROYECTO	PESI 2026–2028	Inversión y funcionamiento	\$620	\$2.230	\$2.180	\$5.030	Proyección plurianual articulada con el PETI y el PAI.

Notas a la Proyección Presupuestal

1. **Programación:** los montos son estimaciones para cada vigencia y requieren incorporación al presupuesto anual. La aprobación del PESI no equivale a apropiación de recursos.
2. **Ajuste por Periodo de Ejecución 2026 (T4):** El presupuesto asignado a la vigencia 2026 contempla el inicio oficial a partir del 1 de octubre de 2026, concentrando los recursos en la formalización de políticas, el inicio de operaciones del SOC como servicio, el despliegue inicial de agentes EDR/XDR y la actualización del estudio BIA.
3. **Ahorro Presupuestal en el Eje 5 (Factor Humano):** La decisión de emplear **Moodle Open Source (Software Libre)** instalado en servidores propios de la UBPD o de estructurar aulas en la suite corporativa (Microsoft Teams / SharePoint) genera un ahorro de software proyectado superior a **\$300.000.000 COP** durante el trienio, reduciendo el gasto del Eje 5 únicamente al diseño pedagógico, material educativo y apoyo logístico para las jornadas presenciales y virtuales de socialización.
4. **Carga Operativa en Gastos de Funcionamiento:** Los Ejes 3 y 4 representan el 64,6% del presupuesto total del plan (\$3.250.000.000 COP) debido al costo recurrente de los contratos administrados de telecomunicaciones (SD-WAN para las 33 sedes), la renovación de suscripciones de ciberdefensa (EDR/XDR, WAF Cloud, FortiSOAR), el almacenamiento en nube e hiperconvergencia y los servicios 24/7 del SOC.

7.2. Asignación y Necesidades de Talento Humano

La ejecución y supervisión continua del Sistema de Seguridad de la Información (SSI) se apoya en la estructura organizacional y en las instancias de gobernanza formalizadas por la UBPD, distribuyendo las responsabilidades de implementación, apoyo y cumplimiento sin generar ampliaciones no financiadas de la plantilla de personal:

- **Liderazgo Estratégico y Gobernanza (Alta Dirección y OSI):** Liderado por la Dirección General, el Comité Ejecutivo de Dirección Institucional (CEDI), la Oficina Asesora de Planeación (OAP) y el Oficial de Seguridad de la Información (OSI), responsables de la rendición de cuentas, la asignación de recursos y la toma de decisiones sobre excepciones y riesgos críticos.
- **Gobernanza de Privacidad y Datos Personales (OPD):** El Oficial de Protección de Datos Personales brinda acompañamiento transversal para garantizar el cumplimiento de la Ley 1581 de 2012, avalar procesos de anonimización (IAH-GU-020), evaluar el impacto en privacidad de modelos de IA y gestionar el reporte formal de brechas ante la SIC.
- **Operación Técnica y Ciberdefensa (GITGT):** El equipo de ingenieros, administradores de red, administradores de sistemas y analistas de ciberseguridad del Grupo Interno de Trabajo Gestión Tecnológica (GITGT), complementado con el servicio de Centro de Operaciones de Seguridad (SOC como servicio) y la Mesa de Servicio *Aranda SAS*.
- **Protección y Metodología Misional (STIH):** Los profesionales técnicos y metodológicos de la Subdirección Técnica de Investigación Humanitaria encargados de la custodia del

SIM, la definición de lineamientos para medios externos en campo (BYOD) y la Evaluación de Impacto Algorítmico (AIA ex-ante) en desarrollos de IA.

- **Gestión del Conocimiento y Formación (PIC / PAE):** Las brechas de competencia especializada en ciberseguridad y forensia digital del personal de TI se gestionan a través de los Proyectos de Aprendizaje en Equipo (formatos GTH-FT-099) y el Plan Institucional de Capacitaciones liderado por la Subdirección de Gestión Humana.

7.3. Soporte Tecnológico y Logística Operativa

La sostenibilidad logística del PESI reposa sobre el parque tecnológico institucional y los contratos marco de tecnología administrados por la Secretaría General y el GITGT. La infraestructura tecnológica que soporta la operativización de las salvaguardas comprende:

- **Ciberdefensa y Capa Perimetral:** Despliegue de la red SD-WAN interconectando las 33 sedes territoriales (GITT) con el Nivel Central, agentes FortiClient EDR/XDR en la totalidad del parque informático, reglas activas de WAF Cloud, plataforma de orquestación FortiSOAR y monitoreo de tráfico con herramientas NPM y NTA.
- **Observabilidad e Identidades:** Arquitectura de gestión de identidades con Autenticación Multifactor (MFA), administración cifrada de credenciales en *TeamPass*, módulos de inspección de red (NCM, IPAM, SEM) e integración con el SIEM/SOC.
- **Continuidad, Almacenamiento y Resiliencia:** Solución de respaldos cifrados bajo el esquema 3-2-1 con Veeam Backup, arquitectura hiperconvergente en sitio alternativo (ODATA-CAL en Kubernetes), herramientas de analítica de almacenamiento (SAM, DPA, SRM) y bóvedas de seguridad física para expedientes documentales en sedes territoriales.
- **Operación de Soporte y Gestión de Incidentes:** Mesa de ayuda corporativa basada en *Aranda SAS* (módulos de incidentes, inventario y soporte remoto cifrado p2p) y canalización obligatoria del **Formato GTI-FT-006** para el registro, escalamiento y reporte de eventos de ciberseguridad ante el OSI y el ColCERT.
- **Ecosistema de Formación Eficiente:** Instancia propia de *Moodle Open Source* o canales virtuales estructurados en la suite Microsoft Teams / SharePoint para la difusión de cursos interactivos de reserva legal y hábitos digitales seguros, eliminando sobre costos de licenciamiento e-learning con terceros.

VIII. NORMATIVIDAD

Para la consulta y aplicación del marco normativo externo e interno que rige las actuaciones institucionales de este documento, remítase obligatoriamente al repositorio central del Normograma UBPD a través del siguiente enlace oficial:

<https://intranet.unidadbusqueda.gov.co/mop/> (Instrumentos del MOP/ Normograma)

IX. REFERENCIAS (Si aplica)

Listado formal de aquellos documentos técnicos, metodológicos, científicos, doctrinales o estándares nacionales e internacionales (ej. guías técnicas del DAFP, lineamientos del Ministerio del Trabajo, manuales de la Cruz Roja Internacional, normas ISO, etc.) que sirvieron de soporte conceptual, base científica o insumo técnico para la elaboración del documento.

No debe confundirse con las leyes (Normatividad). Las referencias garantizan la trazabilidad y el rigor metodológico del contenido del documento. Si un documento no requirió bibliografía o soportes externos para su redacción, se consignará obligatoriamente la frase: "No aplica para este documento".

X. TÉRMINOS Y DEFINICIONES

Acción sin Daño: Principio rector humanitario de la UBPD que orienta la implementación de controles de seguridad digital, física y humana para asegurar que el tratamiento, procesamiento o eventual exposición de datos jamás genere revictimización, vulneración de la privacidad o riesgos a la vida e integridad de las víctimas, aportantes y personas buscadoras.

Activo de Información: Cualquier dato, expediente físico, base de datos, sistema informático, infraestructura tecnológica, soporte documental, persona o servicio que tenga valor para la Entidad y requiera protección en términos de confidencialidad, integridad y disponibilidad.

AIA (Evaluación de Impacto Algorítmico / AIA ex-ante): Mecanismo de análisis preventivo y técnico ejecutado antes del desarrollo, adquisición o puesta en producción de sistemas de Inteligencia Artificial o analítica avanzada, orientado a identificar y mitigar riesgos sobre la privacidad, brechas de reserva legal y sesgos algorítmicos.

ANS (Acuerdo de Niveles de Servicio / SLA): Compromiso formal entre la Entidad y un proveedor interno o externo de tecnologías que define los parámetros esperados del servicio, tales como disponibilidad, tiempos de respuesta y tiempos de solución frente a incidentes.

Aranda SAS: Plataforma de software corporativo adoptada por la UBPD para la gestión centralizada de la Mesa de Servicios de TI, inventario lógico, registro de tickets de soporte y canalización de la asistencia técnica remota segura con cifrado p2p y MFA.

BCP (Plan de Continuidad del Negocio): Conjunto estructurado de estrategias, protocolos y procedimientos institucionales que garantizan la reanudación y continuidad de los procesos misionales y administrativos críticos ante eventos disruptivos o desastres.

BIA (Análisis de Impacto del Negocio): Estudio técnico y operativo mediante el cual la UBPD evalúa los impactos de interrupción sobre los procesos del Modelo Operativo de Procesos (MOP) para calcular y formalizar los tiempos objetivos de recuperación (RTO y RPO).

BYOD (Bring Your Own Device): Esquema regulado que normatividad el uso seguro de dispositivos móviles o equipos personales de contratistas durante comisiones de campo o trabajo fuera de sede, exigiendo la conexión cifrada, la prohibición de sincronización en nubes personales y el borrado seguro tras la transferencia oficial.

CEDI (Comité Ejecutivo de Dirección Institucional): Máxima instancia de gobernanza de la UBPD encargada de revisar el desempeño del SSPI, aprobar políticas generales, autorizar

excepciones de alto riesgo, decidir sobre solicitudes de borrado crítico y priorizar los recursos presupuestales.

Ciberresiliencia: Capacidad estratégica, tecnológica y humana de la UBPD para anticipar, resistir, responder, recuperarse y adaptarse velozmente ante ciberataques, incidentes de seguridad o fallas de infraestructura, garantizando la ininterrupción del mandato humanitario.

CoICERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia, instancia nacional encargada de la coordinación de ciberseguridad a la cual la UBPD debe notificar obligatoriamente los incidentes tecnológicos críticos en menos de dos (2) horas.

Confidencialidad: Propiedad que garantiza que los activos de información de la Entidad no sean divulgados ni hechos accesibles a personas, procesos o entidades no autorizadas.

Dashboard (Panel de Control de Riesgos): Herramienta de visualización técnica automatizada que interconecta los sensores perimetrales (NCM, IPAM, SEM) y el catálogo de activos en *QuickDataERP* para actualizar dinámicamente el nivel de exposición al riesgo técnico.

DLP (Data Loss Prevention / Prevención de Pérdida de Datos): Conjunto de herramientas y reglas de ciberseguridad configuradas para monitorear, detectar y bloquear la transmisión o exfiltración no autorizada de información confidencial fuera de la red institucional.

DRP (Disaster Recovery Plan / Plan de Recuperación ante Desastres): Conjunto de estrategias, políticas y procedimientos técnicos de contingencia diseñados para restaurar la infraestructura tecnológica, redes, servidores y bases de datos institucionales en un sitio alternativo (como la arquitectura ODATA-CAL en Kubernetes) tras la ocurrencia de un evento disruptivo, desastre natural o ciberataque

EDR/XDR (FortiClient Endpoint Detection and Response): Solución avanzada de protección instalada en las estaciones de trabajo y servidores de la UBPD para el monitoreo en tiempo real, detección proactiva y contención automática de *malware* o *ransomware*.

FortiSOAR / WAF Cloud: Plataforma de orquestación, automatización y respuesta de seguridad (SOAR) y cortafuegos de aplicaciones en la nube desplegados para la defensa perimetral e inspección de tráfico de la UBPD.

Forti-SIEM: Sistema de gestión de información y eventos de seguridad encargado de centralizar, correlacionar y analizar en tiempo real los registros (*logs*) de auditoría provenientes de toda la infraestructura tecnológica.

FURAG (Formulario Único de Reporte de Avance de la Gestión): Instrumento de evaluación del DAFP y MinTIC que mide el grado de avance y madurez en la implementación de las políticas del MIPG, incluyendo el Modelo de Seguridad y Privacidad de la Información (MSPI).

GITT (Grupo Interno de Trabajo Territorial): Unidades descentralizadas de la UBPD presentes en 33 sedes del territorio nacional encargadas del despliegue directo de la investigación humanitaria y de la custodia física y digital de expedientes.

GITGT (Grupo Interno de Trabajo Gestión Tecnológica): Dependencia encargada de la administración, soporte, infraestructura de red, ciberdefensa, desarrollo seguro y continuidad del ecosistema tecnológico institucional.

Integridad: Propiedad de salvaguardar la exactitud, completitud y estado no alterado de los datos, expedientes y bases de datos institucionales.

Inteligencia Artificial (IA): Tecnología analítica y algorítmica utilizada como herramienta de soporte en la investigación humanitaria, regulada en la UBPD bajo supervisión humana permanente, prohibición de uso de plataformas públicas no autorizadas y evaluación de sesgos (*Data Fairness*).

IPAM (IP Address Management): Módulo técnico especializado de administración encargado de la planificación, rastreo y gestión automatizada de las direcciones IP en la red institucional.

MFA (Autenticación Multifactor): Control lógico de seguridad que exige la presentación de dos o más mecanismos de verificación independientes para otorgar acceso a los correos corporativos, VPN, nubes y sistemas sensibles.

Moodle Open Source: Plataforma de gestión de aprendizaje (LMS) de software libre desplegada en servidores propios de la UBPD para impartir capacitaciones interactivas sobre ciberseguridad, reserva legal y protección de datos sin generar costos de licenciamiento SaaS.

MOP (Modelo Operativo de Procesos): Estructura organizacional por procesos (estratégicos, misionales, de apoyo y de evaluación) sobre la cual se despliega el alcance del Sistema de Seguridad y Privacidad de la Información.

MSPI (Modelo de Seguridad y Privacidad de la Información): Marco de referencia del MinTIC que adapta la norma ISO/IEC 27001 para la gestión pública, articulando la ciberseguridad, la privacidad de datos y la continuidad operacional.

NAC (Network Access Control): Solución de control de acceso a la red que autentica, autoriza y evalúa la postura de seguridad de los dispositivos informáticos antes de permitir su conexión a la infraestructura de la UBPD.

NCM (Network Configuration Manager): Módulo de gestión y auditoría automatizada de configuraciones para equipos de red y telecomunicaciones en la infraestructura institucional.

ODATA-CAL en Kubernetes (Arquitectura): Esquema técnico de alta disponibilidad y recuperación ante desastres (DRP) desplegado sobre la plataforma de orquestación de contenedores Kubernetes. Opera bajo un modelo de conmutación y replicación geográfica cifrada entre el Centro Principal de Procesamiento (CPP) y el Centro Alterno (CAL / ODATA), permitiendo la conmutación automática o asistida de los sistemas misionales (como el SIM y SIDOBU) para garantizar la continuidad operativa ante contingencias o fallas en la sede principal.

OPD (Oficial de Protección de Datos Personales): Rol institucional encargado de velar por el cumplimiento del régimen de protección de datos (Ley 1581 de 2012), asesorar en privacidad desde el diseño, avalar procesos de anonimización y reportar brechas ante la SIC.

OSI (Oficial de Seguridad de la Información): Rol estratégico responsable de coordinar la gobernanza de ciberseguridad, monitorear el SSPI, evaluar excepciones técnicas, gestionar la matriz de riesgos y rendir cuentas semestralmente ante el CEDI.

PAI (Plan de Acción Institucional): Instrumento de planeación anual de la UBPD con el cual se alinean las metas, actividades y presupuestos de inversión del PESI.

PESI (Plan Estratégico de Seguridad de la Información): Instrumento de planificación plurianual (2026-2028) que define las líneas operativas, metas cuantificables, responsabilidades e inversiones para elevar la madurez del SSPI de la UBPD.

PETI (Plan Estratégico de Tecnologías de la Información): Hoja de ruta tecnológica institucional con la cual se articula el PESI para garantizar la financiación e implementación de proyectos de infraestructura, conectividad y sistemas.

Phishing Ético: Campañas simuladas de ingeniería social ejecutadas periódicamente para medir, evaluar y reducir la tasa de vulnerabilidad del factor humano ante técnicas de engaño digital.

PTR (Plan de Tratamiento de Riesgos): Documento formalmente aprobado que especifica las acciones, salvaguardas tecnológicas, responsables y cronogramas destinados a mitigar o neutralizar los riesgos con nivel Alto o Extremo.

QuickDataERP: Sistema de información corporativo adoptado por la UBPD para el registro, inventario unificado y clasificación estricta de los activos de información conforme a su nivel de criticidad.

Reserva Legal y Extrajudicial: Calidad jurídica especial que ampara la totalidad de la información recopilada o generada en la investigación de personas desaparecidas (Decreto Ley 589 de 2017), proscribiendo su uso con fines punitivos o judiciales.

RPO (Recovery Point Objective / Objetivo de Punto de Recuperación): Límite máximo de pérdida de datos tolerable medido en tiempo que la Entidad acepta asumir tras un incidente antes de afectar la continuidad de sus operaciones.

RTO (Recovery Time Objective / Objetivo de Tiempo de Recuperación): Período máximo de tiempo permitido para la restauración total de un proceso, sistema informático o servicio tecnológico tras una interrupción o desastre.

Sandbox (Entorno Controlado): Segmento de red o entorno de prueba lógicamente aislado diseñado para ejecutar código, experimentar con algoritmos de IA o analizar archivos sospechosos sin poner en riesgo la plataforma de producción del SIM.

SD-WAN (Software-Defined Wide Area Network): Arquitectura de red privada sobre internet que interconecta de forma cifrada y optimizada la sede central de la UBPD con las 33 sedes territoriales (GITT).

SEM (Security Event Manager): Módulo de análisis y monitoreo en tiempo real de eventos de seguridad que facilita la identificación temprana de comportamientos anómalos en los componentes de TI.

SIC (Superintendencia de Industria y Comercio): Autoridad nacional de protección de datos personales ante la cual el OPD debe notificar formalmente cualquier brecha o incidente que comprometa datos personales sensibles.

SIDOBU (Sistema de Gestión Documental): Plataforma institucional encargada del flujo, archivo, conservación y gestión electrónica de los documentos administrativos de la UBPD.

SIEM (Security Information and Event Management / Gestión de Información y Eventos de Seguridad): Sistema centralizado de tecnología encargado de recolectar, centralizar, correlacionar y analizar en tiempo real los registros de auditoría (*logs*) y eventos generados por los diversos componentes de la infraestructura tecnológica de la UBPD (servidores, redes, bases de datos y cortafuegos), facilitando la identificación proactiva de anomalías, la atención de incidentes y el cumplimiento de reportes legales.

SIM (Sistema de Información Misional): Plataforma informática central que almacena, analiza y gestiona los datos, expedientes y testimonios de la investigación humanitaria y extrajudicial para la búsqueda de personas dadas por desaparecidas.

SOC (Security Operations Center / Centro de Operaciones de Seguridad): Unidad técnica o servicio especializado de ciberseguridad (operado como servicio administrado 24/7 en la UBPD) encargado del monitoreo continuo, detección, análisis, correlación de eventos e intervención inmediata ante incidentes que amenacen la infraestructura tecnológica, redes y activos de información institucionales.

SRM (Storage Resource Monitor): Herramienta tecnológica de analítica orientada al monitoreo, gestión de capacidad y evaluación de salud sobre el almacenamiento hiperconvergente e infraestructura de datos.

SSPI (Sistema de Seguridad y Privacidad de la Información): Componente del sistema integrado de gestión de la UBPD encargado de establecer, operar, evaluar y mejorar continuamente los controles de confidencialidad, integridad y disponibilidad bajo la norma ISO 27001:2022.

STIH (Subdirección Técnica de Investigación Humanitaria): Dependencia misional responsable de la custodia del SIM, la autorización exclusiva de excepciones sobre datos de búsqueda, la validación de impacto algorítmico y los protocolos de campo.

TeamPass: Plataforma tecnológica corporativa de código abierto adoptada por la UBPD para la administración centralizada, gestión de accesos con privilegios y almacenamiento

altamente cifrado de contraseñas y credenciales institucionales, garantizando el control de acceso y la trazabilidad sobre los sistemas de la entidad

Veeam Backup: Solución especializada de copias de seguridad cifradas que opera bajo la regla 3-2-1 para garantizar la restauración de servidores, hiperconvergencia y bases de datos institucionales.

XI. ANEXOS

Anexo No. 1: Matriz Programática PESI 2026 – 2028.

Anexo No. 2: Declaración de Aplicabilidad del Anexo A (ISO/IEC 27001:2022). UBPD *Statement of Applicability* (SoA) del SSPI
https://docs.google.com/spreadsheets/d/137jUm_G24LnAlMZ7q0c-YCiCxOLkdW3g/edit?usp=drive_link&ouid=118226198084974995805&rtpof=true&sd=true

XII. CONTROL DE CAMBIOS

VERSIÓN	FECHA	DETALLE DE LOS CAMBIOS EFECTUADOS
Versión 01	30/09/2026	Dando cumplimiento a los lineamientos del MinTIC, se construye el Plan Estratégico de seguridad y privacidad de la Información, el cual se articula con el PETI, PAA y la estrategia de seguridad digital, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta todos los procesos de la UBPD.

XIII. BLOQUE DE FORMALIZACIÓN Y FIRMAS

ELABORÓ:	REVISÓ:	APROBÓ:
01/09/2026 Juan Gabriel Prieto Otavo Experto Técnico	18/09/2026 Andrea Del Pilar Acero Alvarez Oficial de Seguridad de la Información	30/09/2026 Andrea Del Pilar Acero Alvarez Oficial de Seguridad de la Información Miembros del Comité Ejecutivo Directivo Institucional

Anexo 1. Matriz Programática del PESI 2026-2028. UBPD

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 1: Gobernanza L1.1. Actualización marco normativo interno	1. Revisar y ajustar técnicamente las políticas GTI-PC-001 V4 y GTI-MN-002 V3 incorporando privacidad desde el diseño y reserva del SIM. 2. Realizar mesas de trabajo de alineación normativa con STIH, OPD, OAJ y Secretaría General frente a Res. 297/2026 y Res. 500/2021. 3. Tramitar la aprobación formal ante el CEDI y gestionar su publicación en el aplicativo del SIG. 4. Verificar la vigencia de ambos documentos en 2027 y evaluarlos y actualizarlos, si procede, en 2028.	Política GTI-PC-001 V4 y Manual GTI-MN-002 V3 actualizados y formalizados institucional mente. Revisiones de vigencia documentadas en 2027 y 2028.	Alineación de la gobernanza con ISO 27001:2022 y el marco legal del mandato humanitario.	- Tipo: Producto. - Fórmula: Documentos formalizados = (política y manual actualizados, aprobados y publicados / 2 documentos programados) × 100. - Revisiones de vigencia: 1 en 2027 y 1 en 2028. - Línea Base: Política desactualizada (V1 de 2021). - Periodicidad: Anual (Trim).	Líder: OSI / OAP Interviene: OPD, STIH, GITGT, Sec. General	Corto Plazo (2026) - Inicio: 01/10/2026. - Mesas de trabajo: 31/10/2026. - Aprobación CEDI: 30/11/2026. - Fin / Publicación en SIG: 15/12/2026. - Revisión de vigencia: T4 de 2027 y T4 de 2028.	- Documento de política aprobado por CEDI y radicado formalmente en el SIG. - Registro de publicación de la versión actualizada en el aplicativo del SIG. - Actas o registros de las revisiones anuales y nuevas versiones, cuando proceda.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 1: Gobernanza L1.2. Monitoreo y autodiagnósticos MSPI	1. Diseñar y aplicar el instrumento anual de autodiagnóstico sobre controles ISO/IEC 27001:2022 y la Ley 1581 de 2012. 2. Recopilar y consolidar las evidencias para el reporte de indicadores en la plataforma FURAG del MinTIC. 3. Formular e ingresar en el SIG los planes de mejoramiento técnico derivados del análisis de control interno y autodiagnóstico.	Informes anuales de evaluación de control, autodiagnóstico y madurez del MSPI bajo ISO 27001.	Cierre sostenido de brechas operativas y elevación de la madurez del SSPI.	• Tipo: Gestión. • Fórmula: Autodiagnósticos ejecutados = (autodiagnósticos MSPI/ISO 27001 formalizados / autodiagnósticos programados en el periodo) x 100. Total trienal: 3. • Línea Base: Ciclos ejecutados anualmente de forma intermitente (70,4% MSPI). • Periodicidad: Anual (T4).	Líder: OSI / OAP Interviene: OPD, STIH, Líderes de Proceso	Ejecución Continua (2026-2028) • Inicio ciclo 2026: 01/10/2026. • Cierre Ciclo 2026: 30/12/2026. • Cierre Ciclo 2027: 30/12/2027. • Fin Plan: 30/12/2028.	• Informes institucionales de autodiagnóstico MSPI/ISO 27001 formalizados. • Constancia de reporte del FURAG ante MinTIC. • Planes de mejoramiento formalizados con código de seguimiento en el SIG.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 1: Gobernanza L1.3. Rendición de cuentas ante Alta Dirección	1. Consolidar semestralmente el tablero de control de métricas, incidentes y riesgo residual del SSPI. 2. Elaborar informes ejecutivos sobre el estado de excepciones del SIM autorizadas por la STIH y solicitudes de Habeas Data tramitadas con el OPD. 3. Sustentar los avances y solicitar decisiones estratégicas ante el Comité Ejecutivo de Dirección Institucional (CEDI).	Informe ejecutivo de desempeño del SSPI presentado e ingresado al orden del día del CEDI.	Toma de decisiones estratégica informada y respaldo institucional a la reserva legal.	• Tipo: Resultado. • Fórmula: Informes al CEDI = (informes presentados con acta / informes programados en el periodo) × 100. Total trienal: 5. • Línea Base: 20% (Cláusula 9.3 / Revisión informal). • Periodicidad: Un informe en T4 de 2026; semestral en 2027 y 2028.	Líder: OSI / OAP Interviene: OPD, STIH, OAJ, GITGT	Ejecución Continua (2026-2028) • Inicio: 01/10/2026. • Informe Cierre 2026: 15/12/2026. • Informes 2027-2028: 30/06 y 15/12 de cada año. • Total trienal: 5 informes (1 en 2026, 2 en 2027 y 2 en 2028).	• Actas firmadas de las sesiones del CEDI. • Tablero de control de indicadores y documento del informe semestral. • Conceptos técnicos suscritos sobre excepciones o solicitudes de borrado crítico.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 2: Riesgos L2.1. Matriz automatizada y activos	1. Recolectar y actualizar la información de activos de información en la plataforma QuickDataERP. 2. Clasificar la criticidad de los activos pertenecientes al SIM, SIDOBU, Gestionemos y Tramitemos, obteniendo los avales de la STIH y del OPD. 3. Articular técnicamente los riesgos de activos con la Matriz Institucional GSI-MT-004 en el SIG/MECI.	Inventario de activos clasificado en ERP y Matriz de Riesgos de Seguridad actualizada y automatizada.	Visibilidad automática y monitoreo en tiempo real del riesgo técnico sobre activos misionales y de soporte.	• Tipo: Producto. • Fórmula: Clasificación de activos = (activos misionales y de soporte clasificados y validados / total de activos identificados en QuickDataERP) x 100. • Automatización SIG/MECI: matriz integrada y aprobada al 30/12/2027. • Línea Base: Cálculo estático y manual de la matriz institucional de riesgos (76% NIST ID). • Periodicidad: Anual.	Líder: GITGT / OSI Interviene: OPD, STIH, OAP, Custodios	Corto a Mediano Plazo (2026-2027) • Inicio: 01/10/2026. • Hito Clasificación ERP: 30/11/2026. • Fin / Automatización SIG: 30/12/2027. • Integración de la matriz automatizada con SIG/MECI: 30/12/2027.	• Reporte exportado del Formato GSI-FT-003 desde QuickDataERP. • Matriz GSI-MT-004 aprobada en el SIG.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 2: Riesgos L2.2. Ejecución de PTR, visibilidad y Dashboards	1. Formular y asignar presupuesto a los Planes de Tratamiento de Riesgos (PTR) para salvaguardas de la Res. 500/2021 y Res. 02277/2025. 2. Adquirir e interconectar módulos de visibilidad (NCM, IPAM, SEM, Forti-SIEM, DLP, NAC, TeamPass, SOC) con el catálogo de activos. 3. Desplegar un Panel de Control (Dashboard) de riesgos con actualización dinámica de vulnerabilidades y formalizar el protocolo STIH de medios de aportantes.	Módulos de visibilidad configurados, Dashboard de riesgos en línea y protocolo operativo de campo en ejecución.	Ejecución y verificación del 100% de las acciones de los PTR aprobados para riesgos altos y extremos, con valoración posterior del riesgo residual.	- Tipo: Resultado. - Fórmula: Cumplimiento de PTR = (acciones ejecutadas y verificadas de los PTR aprobados para riesgos altos y extremos / total de acciones programadas en esos PTR) x 100. - Línea Base: 0% (Cláusula 8.3 / Sin visibilidad integrada). - Periodicidad: Semestral.	Líder: GITGT Interviene: OSI, STIH, OPD, Contratación	Corto a Mediano Plazo (2026-2027) - Inicio: 01/10/2026. - Puesta en marcha TeamPass y SOC: 15/12/2026. - Instalación NCM/IPAM/SEM: 30/11/2027. - Fin / Dashboard de Riesgos integrado: 30/12/2027.	- Panel de Control (Dashboard) de riesgos operativo y visualizable. - Documento de PTR firmado y verificado. - Informes de soporte de herramientas visibilidad (NCM, IPAM, Forti-SIEM, SOC). - Protocolo STIH para medios externos.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 2: Riesgos L2.3. Riesgo residual e Impacto en IA (AIA)	1. Realizar el monitoreo y ajuste trimestral de los umbrales de riesgos técnicos en el Tablero de Control (Dashboard). 2. Diseñar la metodología y ejecutar Evaluaciones de Impacto Algorítmico (AIA ex-ante) previo a proyectos de analítica o IA misional. 3. Auditar la calidad y representatividad de datos de entrenamiento (Data Fairness) para prevenir sesgos y proteger la reserva legal. 4. Documentar dos evaluaciones formales de riesgo residual cada año desde 2027, además de las cuatro revisiones trimestrales de umbrales.	Tablero de control (Dashboard) de umbrales actualizado y Evaluaciones de Impacto Algorítmico (AIA ex-ante) aprobadas.	Despliegue seguro y ético de modelos algorítmicos sin fuga de información sensible ni sesgos.	• Tipo: Gestión / Producto. • Fórmula: $AIA_{ex\ ante} = \frac{\text{proyectos de IA evaluados antes de producción}}{\text{proyectos de IA que llegan a producción}} \times 100$. Si no hubo proyectos en el periodo, registrar N. A. • Riesgo residual: 2 evaluaciones formales al año desde 2027; umbrales: 4 revisiones al año. • Línea Base: 0% (Sin evaluaciones algorítmicas). • Periodicidad: Trimestral / Semestral.	Líder: OSI / OPD Interviene: STIH, GITGT	Ejecución Continua (2026-2028) • Inicio: 01/10/2026. • Ajuste trimestral umbrales: Cierre T1, T2, T3, T4. • Evaluaciones AIA: Previo a la puesta en producción de cada proyecto de IA. • Evaluaciones formales de riesgo residual: 30/06 y 15/12 de 2027 y 2028. • AIA ex ante: antes de la puesta en producción de cada proyecto de IA desde 2026.	• Visualización y actas de revisión del Tablero de Control (Dashboard) de umbrales. • Informes de revaloración de riesgo residual en el SIG. • Formato de Evaluación AIA ex-ante firmado por OSI, OPD y STIH. • Dos informes anuales formales de evaluación del riesgo residual desde 2027.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 3: Resiliencia L3.1. Actualización del BIA y BCP	1. Levantar la información operativa y evaluar los impactos de interrupción sobre todos los procesos del Modelo Operativo (MOP). 2. Definir técnicamente los parámetros RTO/RPO y actualizar el documento formal del Plan de Continuidad del Negocio (BCP). 3. Presentar el estudio BIA y el BCP actualizado para su aprobación en el CEDI.	Estudio BIA institucional y documento del Plan de Continuidad del Negocio (BCP) actualizado y publicado.	Tolerancias de interrupción del negocio formalizadas y resiliencia operativa garantizada ante contingencias.	- Tipo: Producto. - Fórmula: Cobertura del BIA = (procesos del MOP incluidos en el BIA aprobado / total de procesos del MOP) × 100. BCP actualizado y publicado: 1 documento a junio de 2027. - Línea Base: BCP parcial o desactualizado. - Periodicidad: BIANUAL.	Líder: GITGT Interviene: OAP, STIH, Sec. General, Gest. Administrativa	Corto a Mediano Plazo (2026-2027) - Inicio: 01/10/2026. - Aprobación BIA en CEDI: 15/12/2026. - Fin / Publicación Documento BCP: 30/06/2027.	- Documento del Análisis de Impacto del Negocio (BIA) en el SIG. - Documento del Plan de Continuidad del Negocio (BCP) actualizado y aprobado por CEDI.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 3: Resiliencia L3.2. Almacenamiento, respaldos y anonimización	1. Administrar la infraestructura hiperconvergente y ejecutar copias de seguridad cifradas bajo el esquema 3-2-1 con Veeam en nube segura. 2. Monitorear el rendimiento de servidores y bases de datos (SAM, DPA, SRM) para asegurar el SIM, SIDOBU y Archivo Misional. 3. Realizar pruebas técnicas continuas de restauración de respaldos en la nube (6 en T4 de 2026, 24 en 2027 y 24 en 2028 (54 en total; 2 al mes)) y aplicar anonimización (IAH-GU-020).	Servicio técnico de restauración y copias de seguridad estandarizado con reportes de restauración mensuales.	Disponibilidad, integridad y confidencialidad ininterrumpida de la memoria histórica y bases misionales.	• Tipo: Gestión / Resultado. • Fórmula: Restauraciones exitosas = (pruebas de restauración exitosas / pruebas programadas) × 100. - Programación: 6 en 2026, 24 en 2027 y 24 en 2028, para 54. • Línea Base: Respaldos periódicos sin pruebas sistemáticas de restauración (88% ISO A.8). • Periodicidad: Mensual (2 pruebas al mes).	Líder: GITGT Interviene: STIH, OPD, Gest. Administrativa	Ejecución Continua (2026-2028) • Inicio: 01/10/2026. • Verificación mensual (2 pruebas): Cierre de cada mes. • Fin Plan: 30/12/2028. • Total programado: 6 pruebas en T4 de 2026, 24 en 2027 y 24 en 2028 (54).	• Reportes mensuales de restauración exitosa firmados por soporte técnico. • Logs y reportes automáticos exportados de la consola Veeam. • Certificados de anonimización aplicados (IAH-GU-020).

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 3: Resiliencia L3.3. Pruebas DRP y custodia física GITT	1. Planificar y ejecutar 5 simulacros DRP: 1 en 2026, 2 en 2027 y 2 en 2028 sobre la arquitectura DRP 2. Actualizar y estandarizar el protocolo de custodia física y ambiental para archivos de papel y medios magnéticos en sedes territoriales. 3. Realizar auditorías e inspecciones a las condiciones de custodia física y seguridad en las 33 sedes de los GITT.	Informes y planes correctivos de resiliencia derivados de simulacros DRP e inspecciones a GITT.	Ciberresiliencia comprobada ante desastres y conservación de los fondos documentales territoriales.	- Tipo: Resultado. - Fórmula: Simulacros DRP exitosos = (simulacros exitosos / simulacros programados) × 100; total: 5. - Cobertura GITT = (sedes auditadas / 33 sedes) × 100; mínimo 17 en 2027 y 33 acumuladas en 2028. - Línea Base: No se realizaban simulacros formales de DRP para alta prioridad. - Periodicidad: DRP: 1 en 2026 y semestral en 2027-2028; GITT: anual.	Líder: GITGT / OSI Interviene: STIH, Sec. General, OAP, GITT	Mediano a Largo Plazo (2026-2028) - Inicio: 01/10/2026. - Prueba DRP 2026: 30/11/2026. - Pruebas DRP 2027-2028: 30/05 y 30/11 de cada año. - Auditoría GITT (100% sedes): 30/11/2028. - Auditorías GITT: al menos 17 de 33 sedes en 2027 y las 33 acumuladas al 30/11/2028.	- Evidencia documental y reporte técnico del resultado del simulacro DRP (GTI-PL-002). - Listas de chequeo e informes de inspección física aplicados a las 33 sedes GITT.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 4: Ciberdefensa L4.1. Ciberdefensa y entornos Sandbox	1. Desplegar y mantener la red SD-WAN (33 sedes), agentes FortiClient EDR/XDR, WAF Cloud, FortiSOAR y MFA. 2. Monitorear el tráfico de red mediante herramientas NPM y NTA para prevenir ransomware y exfiltración. 3. Configurar y habilitar entornos Sandbox lógicamente aislados para pruebas de modelos de IA misional.	Capacidades de monitoreo y respuesta activa desplegadas en terminales, red y entornos Sandbox.	Protección perimetral e interna eficaz contra ciberataques avanzados y fugas de información.	• Tipo: Producto / Resultado. • Fórmula: Cobertura EDR/XDR = (equipos del alcance con agente activo / equipos del alcance) × 100. Cobertura SD-WAN = (sedes conectadas y verificadas / 33 sedes programadas) × 100. • Línea Base: Protección antivirus convencional de carácter reactivo (70% NIST DE). • Periodicidad: Trimestral.	Líder: GITGT Interviene: STIH, Proveedores Ciberseguridad	Corto a Mediano Plazo (2026-2027) • Inicio: 01/10/2026. • Fin / Despliegue 100% EDR: 30/12/2026. • Habilitación Sandboxes IA: 31/03/2027.	• Certificación del 100% de despliegue de los agentes en consola FortiSOAR/EDR. • Reportes de consolas centrales (SD-WAN, WAF Cloud). • Acta de entrega técnica de entornos Sandbox para IA.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 4: Ciberdefensa L4.2. Soporte remoto y protocolo BYOD	1. Implementar y configurar la solución corporativa licenciada para soporte remoto cifrado p2p con MFA integrada en Aranda SAS. 2. Reglamentar y desplegar el protocolo BYOD para dispositivos móviles en comisiones de campo bajo pautas de la STIH. 3. Auditar y aplicar el borrado seguro de datos locales en equipos personales tras la sincronización en nube institucional.	Solución corporativa de gestión de soporte remoto cifrado activa y reglamentación BYOD.	Erradicación del uso de software de soporte no autorizado y control riguroso sobre datos en movilidad. Aplicación del protocolo BYOD y borrado seguro verificado al cierre de cada comisión que utilice dispositivos personales.	• Tipo: Gestión. • Fórmula: Soporte remoto autorizado = (sesiones atendidas con la solución corporativa y MFA / total de sesiones de soporte remoto) × 100. • Línea Base: Uso informal de software de soporte remoto no corporativo o no autorizado. • Periodicidad: Semestral.	Líder: GITGT Interviene: STIH, OSI, Usuarios en Campo	Corto Plazo y Operación Continua • Inicio: 01/10/2026. • Fin / Puesta en marcha herramienta: 30/11/2026. • Auditoría BYOD: Al cierre de cada comisión.	• Reporte automático de auditoría y grabación de las sesiones generado por Aranda SAS. • Formatos de constancia de borrado seguro firmados tras comisiones en campo.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 4: Ciberdefensa L4.3. Protocolo de incidentes y reportes (ColCERT/SIC)	1. Implementar la Guía de Gestión de Incidentes de SI y centralizar logs (SEM/LA) mediante monitoreo 24/7 en SOC/SIEM. 2. Documentar obligatoriamente todo evento o anomalía en el Formato GTI-FT-006 (Reporte de eventos e incidentes al OSI) y atender bajo ANS. 3. Reportar los eventos críticos al ColCERT y comunicar a la SIC, por conducto del OPD, las brechas de datos personales cuando corresponda.	Guía de gestión de incidentes operando, Formato GTI-FT-006 implementado y radicados oficiales enviados.	Detección temprana, contención inmediata de ciberataques y pleno cumplimiento del régimen legal.	- Tipo: Resultado. - Fórmula: Incidentes dentro del ANS = (incidentes cerrados dentro del ANS / total de incidentes registrados) × 100. Reportes externos: casos comunicados oportunamente / casos que cumplen los supuestos de reporte. - Línea Base: Monitoreo descentralizado o sin correlación automática (< 2h reporte). - Periodicidad: Continuo (24/7).	Líder: GITGT / OSI Interviene: OPD, STIH	Ejecución Continua (2026-2028) - Inicio: 01/10/2026. - Monitoreo SOC/SIEM: 24/7 permanente. - Reporte ColCERT / Formato GTI-FT-006: < 2 horas tras detección. - Fin Plan: 30/12/2028.	- Formatos oficiales GTI-FT-006 diligenciados de reporte de eventos e incidentes al OSI. - Registros de cierre de incidentes en Aranda SAS (GTI-FT-008). - Oficios y radicados oficiales de notificación al ColCERT y a la SIC.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 5: Factor Humano L5.1. Capacitación, Moodle Open Source / Teams y Socialización	1. Diseñar los contenidos pedagógicos sobre reserva extrajudicial, Ley 1581/2012, ciberseguridad e IA responsable (2026). 2. Desplegar la instancia Moodle Open Source (sin costo de licenciamiento) en infraestructura propia o estructurar aulas virtuales en la suite de Microsoft Teams / SharePoint (2027). 3. Ejecutar jornadas presenciales/virtuales de socialización de Seguridad Digital y certificar al menos el 85% del personal activo en el entorno virtual (2028).	Estructura pedagógica diseñada (2026), entorno virtual configurado sin costo de software (2027) y personal capacitado/certificado (2028).	Certificación de al menos 85% del personal activo en 2028 y sensibilización activa y reducción sostenida de vulnerabilidad es asociadas al factor humano sin generar sobrecostos presupuestales.	• Tipo: Producto / Resultado. • Fórmula: Cobertura de formación 2028 = (personas del personal activo certificadas en el entorno virtual / total del personal activo) × 100. Meta: al menos 85%. • Línea Base: Charlas informales periódicas sin trazabilidad ni control formal (83% ISO A.6). • Periodicidad: Anual.	Líder: GITGT / OSI Interviene: OAP, Talento Humano, OPD, STIH, OACP	Ejecución Plurianual (2026-2028) • Inicio: 01/10/2026. • Diseño pedagógico: 15/12/2026. • Configuración Moodle OS / Teams: 30/11/2027. • Jornadas y Cierre 85% capacitado: 30/11/2028. • Fin Plan: 30/12/2028.	• Repositorio y cursos configurados en la instancia Moodle Open Source o canal corporativo de Teams. • Listados institucionales de asistencia DPE-FT-002 y certificados de jornadas de socialización. • Reportes exportados de completitud del entorno virtual.

Eje y línea operativa	Actividades operativas	Producto entregable	Resultado esperado	Indicador, fórmula, línea base y periodicidad	Responsables	Cronograma e hitos	Evidencias de cumplimiento
Eje 5: Factor Humano L5.2. Simulacros de phishing y evaluación	1. Diseñar y lanzar 9 campañas en el trienio: 1 en T4 de 2026 y 4 anuales en 2027 y 2028 de simulación de ingeniería social (phishing ético) y pruebas de fuga de información. 2. Evaluar el cumplimiento de la norma de reporte de incidentes a la Mesa de Servicio en menos de 2 horas (aplicando la excepción de campo). 3. Desarrollar talleres de retroalimentación pedagógica dirigidos a los procesos con mayor tasa de vulnerabilidad.	Reportes técnicos de métricas de vulnerabilidad del factor humano y estadísticas de clics.	Tasa de vulnerabilidad del personal ante técnicas de engaño digital reducida a niveles < 10%.	- Tipo: Resultado. - Fórmula: Vulnerabilidad ante phishing = (participantes únicos que interactúan con el señuelo / participantes únicos del simulacro) × 100. Meta 2028: < 10%. - Campañas ejecutadas: 1 + 4 + 4 = 9. - Línea Base: Inexistencia de pruebas controladas de phishing de forma masiva. - Periodicidad: Una prueba en T4 de 2026; cuatro por año en 2027 y 2028.	Líder: GITGT / OSI Interviene: OPD, STIH	Ejecución Continua (2026-2028) - Inicio: 01/10/2026. - Primer Simulacro (T4 2026): 15/11/2026. - Pruebas 2027-2028: Marzo, Junio, Septiembre y Diciembre de cada año. - Fin Plan: 30/12/2028. - Total trienal: 9 simulacros (1 + 4 + 4).	- Reportes consolidados con estadísticas de clics, tasa de caída y reportes realizados. - Métrica de tickets reportados a la Mesa de Servicio notificando sospecha de engaño.