PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN- PESI

2026 - 2030

JUSTICIA PENAL MILITAR Y POLICIAL

Oficina de Tecnologías de Información y Comunicaciones

Contenido

1. Introducción

La Unidad Administrativa Especial de la Justicia Penal Militar y Policial (JPMP), en cumplimiento de su función constitucional de administrar justicia de manera autónoma, eficiente y transparente para los integrantes de la Fuerza Pública, reconoce que la información judicial, administrativa y estratégica constituye uno de sus activos más importantes. La disponibilidad, integridad y confidencialidad de dicha información son elementos esenciales para garantizar la continuidad del servicio, la protección de los derechos de los ciudadanos y la confianza en la gestión institucional.

El presente Plan Estratégico de Seguridad de la Información (PESI) surge a partir de un diagnóstico institucional que identificó oportunidades de mejora en las capacidades de seguridad digital, asociadas principalmente a la dependencia de procesos manuales, la necesidad de modernizar componentes tecnológicos y el fortalecimiento de los mecanismos de prevención, detección y respuesta frente a incidentes de seguridad de la información. Estas condiciones evidencian la necesidad de evolucionar hacia un modelo de seguridad más integral, que no se limite al cumplimiento documental, sino que fortalezca la capacidad real de la entidad para prevenir riesgos y responder oportunamente ante eventos que puedan afectar la operación institucional.

Esta necesidad quedó especialmente resaltada tras el incidente de ransomware "Gunra" ocurrido en junio de 2025, el cual puso de manifiesto la importancia de fortalecer las capacidades institucionales de ciberseguridad, continuidad del negocio y recuperación de servicios. Como resultado, se hace necesario adoptar una visión integral que articule la tecnología, los procesos, las personas y los proveedores estratégicos bajo un mismo marco de gestión y protección de la información.

La implementación de este Plan no responde únicamente a una necesidad técnica. También obedece al cumplimiento de las obligaciones legales y de política pública que rigen a las entidades del Estado colombiano en materia de transformación digital, seguridad de la información y gobierno digital. En este sentido, la JPMP debe dar cumplimiento a los lineamientos establecidos en el Plan Nacional de Desarrollo, la Política de Gobierno Digital, el Modelo de Seguridad y Privacidad de la Información (MSPI) y demás disposiciones definidas por el Ministerio de Tecnologías de la Información y las Comunicaciones

(MinTIC), particularmente las establecidas en el Decreto 1078 de 2015 y sus normas complementarias.

Dentro de este marco, el PESI constituye el instrumento de planeación y gobernanza que permite articular las necesidades operativas y misionales de la JPMP con las exigencias normativas en materia de seguridad digital. Su propósito es fortalecer la protección de la información institucional, garantizar la continuidad de los servicios, reducir la exposición a riesgos tecnológicos y promover una cultura organizacional orientada a la seguridad y la gestión responsable de la información.

Para lograrlo, el Plan contempla la adopción gradual de mejores prácticas y estándares internacionales, entre ellos ISO/IEC 27001:2022 y el Marco de Ciberseguridad NIST CSF 2.0, así como la implementación de mecanismos modernos de protección, monitoreo y respuesta frente a amenazas cibernéticas. Estas acciones permitirán que la entidad cuente con controles verificables, procesos más resilientes y capacidades de recuperación acordes con la criticidad de sus funciones misionales.

Finalmente, el documento establece una hoja de ruta de mediano plazo orientada al fortalecimiento progresivo de la seguridad de la información en la entidad. Esta ruta incluye acciones de mejoramiento tecnológico, fortalecimiento de competencias del talento humano, gestión integral de riesgos, fortalecimiento de la ciberseguridad, seguimiento mediante indicadores de desempeño y la consolidación de un modelo de gobernanza que permita asegurar la sostenibilidad de las capacidades implementadas y la protección efectiva de la información institucional frente a un entorno de amenazas en constante evolución.

2. Objetivo general

Implementar y consolidar las estrategias de seguridad y privacidad de la información para la vigencia 2026-2030, garantizando la confidencialidad, integridad y disponibilidad de los activos de información de la Justicia Penal Militar y Policial (JPMP), con el fin de mitigar los riesgos cibernéticos y mantenerlos en niveles aceptables de operación.

2.1. Objetivos específicos

- Detectar y responder a incidentes de seguridad de forma oportuna, reduciendo el tiempo de detección de incidentes críticos de dos semanas a menos de 30 minutos, mediante la puesta en marcha de un centro de monitoreo de seguridad antes de finalizar 2027.
- Fortalecer el gobierno institucional de la seguridad de la información, creando una instancia responsable de seguridad con independencia de la Oficina de Tecnologías, que reporte directamente al Comité Institucional de Gestión y Desempeño y que tenga la facultad de aprobar o rechazar nuevos desarrollos tecnológicos que no incorporen seguridad desde su diseño, conforme al Decreto 338 de 2022.
- Proteger la información judicial durante todo su ciclo de uso, mediante controles de seguridad que actúen en distintos niveles de la infraestructura, evitando que la información probatoria pueda ser alterada o bloqueada por ataques de secuestro de datos, y garantizando que los servicios misionales sigan disponibles incluso ante fallas o desastres.
- Controlar y verificar de forma segura el acceso a la información, implementando un esquema de identidades y accesos basado en verificación permanente, autenticación de doble factor y gestión de cuentas con privilegios, de manera que cada actuación administrativa y judicial quede registrada y se elimine el riesgo de robo o uso indebido de credenciales.

3. Alcance

El alcance del presente Plan Estratégico de Seguridad de la Información (PESI) abarca la totalidad del ecosistema tecnológico, administrativo y judicial de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial (JPMP). Su temática central y campo de aplicación se extienden a la protección integral de los activos de información, la infraestructura de TI, los sistemas críticos (como el SPOA) y las plataformas de servicios digitales, estableciendo un marco de ciberresiliencia basado en la arquitectura de "Confianza Cero" (Zero Trust) y el cumplimiento estricto del Modelo de Seguridad y Privacidad de la Información (MSPI v5.0). El contenido y las directrices de este plan están dirigidos a—y son de obligatorio cumplimiento para—todos los servidores públicos, contratistas, consultores, interventores, proveedores de servicios tecnológicos y cualquier tercero que interactúe, procese o custodie información de la entidad. Esta cobertura transversal asegura que la responsabilidad sobre la

seguridad digital se integre en la cultura organizacional de todas las dependencias, garantizando la soberanía de los datos, el debido proceso y la continuidad ininterrumpida de la administración de justicia militar y policial.

En cuanto a su ciclo de ejecución, la aplicabilidad de este documento inicia con la evaluación exhaustiva del estado de madurez institucional y la valoración dinámica de los riesgos cibernéticos, partiendo del diagnóstico formal de las brechas tecnológicas y administrativas frente a los estándares de la norma ISO/IEC 27001:2022. Una vez establecida esta línea base, el plan continúa con el despliegue operativo de una hoja de ruta estratégica a través de los proyectos de mitigación progresivas, las cuales involucran la modernización defensiva activa (EDR/XDR), la segmentación de redes, la capacitación del talento humano y la gestión segura de la cadena de suministro. Finalmente, el ciclo de aplicación del PESI concluye con la fase de consolidación, medición y auditoría mediante Indicadores Clave de Riesgo (KRIs) y de Desempeño (KPIs), verificando el cumplimiento de las metas de recuperación (RTO/RPO) e inyectando los resultados en el ciclo de mejora continua (PHVA) para garantizar que la inmunidad institucional se adapte proactivamente a las nuevas amenazas hasta el cierre de la vigencia 2030.

4. Marco normativo

Tipo de norma	Número	Año	Descripción - epígrafe
Ley	1273	2009	Tipifica delitos informáticos y otras infracciones relacionadas con sistemas de información y datos (conductas punibles contra sistemas de información).
Ley	1581	2012	Establece el régimen general de protección de datos personales en Colombia.
Ley	1712	2014	Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. Relacionada indirectamente, ya que la gestión de la información pública implica seguridad para garantizar su disponibilidad e integridad.
Directiva Presidencial	003	2021	Establece lineamientos para el uso de servicios en la nube, inteligencia artificial y seguridad digital en entidades públicas.

Tipo de norma	Número	Año	Descripción - epígrafe
Decreto	2609	2012	Establece directrices para la gestión documental en entidades del Estado. Aunque no es exclusivamente de seguridad, incluye aspectos de seguridad y preservación de la información documental.
Decreto	1377	2013	Complementa la Ley 1581 de 2012 en cuanto a la protección de datos personales.
Decreto	886	2014	Reglamenta el Registro Nacional de Bases de Datos (RNBD) administrado por la Superintendencia de Industria y Comercio.
Decreto	1074	2015	Reglamenta parcialmente la Ley 1581 de 2012 en varios aspectos de la protección de datos personales.
Decreto	1078	2015	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones. Proporciona el marco general que incluye aspectos de gobierno y seguridad digitales.
Decreto	620	2020	Establece los lineamientos generales para el uso de Servicios Ciudadanos Digitales, los cuales deben cumplir con principios de seguridad y privacidad.
Decreto	338	2022	Establece lineamientos generales para fortalecer la gobernanza de la seguridad digital en entidades públicas.
Decreto	767	2022	Actualiza la Política de Gobierno Digital, la cual incluye la seguridad y privacidad de la información como uno de sus habilitadores principales. El PESI debe estar articulado con esta política.
Decreto	1389	2022	Se articula con la Resolución 460 de 2022 y el Decreto 767 de 2022. Establece lineamientos generales para la implementación del PNID, relevante para la gobernanza y seguridad de datos.
Resolución	500	2021	Establece los lineamientos y estándares para la estrategia de seguridad digital y adopta el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la política de Gobierno Digital. Es una referencia clave para la formulación del PESI.
Resolución	746	2022	Relacionada con el fortalecimiento y la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).

Tipo de norma	Número	Año	Descripción - epígrafe
Resolución	460	2022	Expide el Plan Nacional de Infraestructura de Datos (PNID) y su Hoja de Ruta. Establece lineamientos y principios para la gobernanza de la infraestructura de datos, incluyendo seguridad y protección de los datos.
Resolución	Resolución 1409 de 2022	2022	Mencionado en contexto de unificar criterios de entrega y tratamiento de datos personales para segundo uso, observando el principio de legalidad en salud.
Resolución	088	2022	Relacionada con la digitalización y automatización de trámites. Debe alinearse con la Política de Gobierno Digital y el MSPI de seguridad y privacidad.
Resolución	2277	2025	Actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI) en Colombia, modificando el Anexo 1 de la Resolución 500 de 2021
CONPES	3854	2016	Política Nacional de Seguridad Digital. Sirve como marco de contexto para la estrategia de seguridad digital del país.
CONPES	3920	2018	Política Nacional de Explotación de Datos (Big Data). Aborda el uso de datos masivos, lo que implica consideraciones importantes sobre seguridad y privacidad.
CONPES	3975	2019	Política nacional para la transformación digital e inteligencia artificial. Cubre temas amplios de transformación digital que requieren la seguridad como un componente necesario.
CONPES	3995	2020	Política Nacional de Confianza y Seguridad Digital de Colombia. Es el marco estratégico fundamental para la seguridad digital del país, orienta las acciones para proteger activos de información, promover un entorno digital seguro y fortalecer la confianza. Define planes de acción estratégicos como el Plan de Gobernanza y Gestión del Riesgo.
CONPES	4144	2025	El presente documento CONPES formula una política nacional de Inteligencia Artificial cuyo objetivo es generar las capacidades para la investigación, desarrollo, adopción y aprovechamiento ético y sostenible de sistemas de IA con

Tipo de norma	Número	Año	Descripción - epígrafe
			el fin de impulsar la transformación social y económica de Colombia
Norma Técnica Internacional	NIST SP 800-39: Managing Information Security Risk	2011	Define la gestión de riesgos en tres niveles (Tier 1: Organización, Tier 2: Procesos de Negocio, Tier 3: Sistemas de Información).
Norma Técnica Internacional	NIST Cybersecurity Framework (CSF) 2.0	2024	se enfoca en Identificar, Proteger, Detectar, Responder y Recuperar. La versión 2.0 añade la función de GOBERNAR (GOVERN), que es donde vive tu estrategia en Ciberseguridad
Norma Técnica Internacional	NIST SP 800-53 Rev. 5: Security and Privacy Controls	2025	Es el catálogo maestro de controles. Con este documento selecciona las contramedidas específicas. Para estrategia, no usas todos; seleccionas una "Línea Base" (Low, Moderate, High) dependiendo de la criticidad de la información.
Norma Técnica Colombiana / Estándar	NTC/ISO 22301	2019	Norma internacional (adoptada como NTC) para Sistemas de Gestión de la Continuidad de Negocio (BCM), fundamental para la elaboración del Plan de Continuidad de Negocio (BCP) y la recuperación ante desastres.
Norma Técnica Internacional	ISO 27000	2022	Familia de estándares internacionales relacionados con la Seguridad de la Información. Mencionada como referencia general para análisis de seguridad y continuidad.
Norma Técnica Colombiana / Estándar	ISO 27001 / NTC/ISO/IEC 27001:2022	2022	Norma internacional (adoptada como NTC) que especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). El MSPI busca alinear y certificar su SGSI con esta norma.
Política	Política General	2024	Política General de Seguridad, Privacidad de la Información y Ciberseguridad - Versión 2

5. Responsables

Cargo / Rol	Responsabilidad en el PESI
Director General	Aprobar el PESI y asegurar la asignación de recursos necesarios para su implementación.

Cargo / Rol	Responsabilidad en el PESI
	Ejercer el patrocinio institucional y promover el fortalecimiento de la seguridad de la información como objetivo estratégico de la entidad.
Comité Institucional de Gestión y Desempeño	Orientar, validar y realizar seguimiento estratégico al cumplimiento del PESI, revisar los avances de implementación y tomar decisiones frente a riesgos y necesidades institucionales que afecten el cumplimiento de los objetivos de seguridad digital.
Secretaria General	Coordinar la articulación institucional requerida para la implementación del PESI, facilitando la gestión administrativa, contractual y del cambio organizacional asociada a los proyectos definidos.
Oficial de Seguridad de la Información - CISO	Liderar la gestión del Sistema de Gestión de Seguridad y Privacidad de la Información, coordinar la implementación del PESI, realizar seguimiento a los riesgos de seguridad, presentar informes a la Alta Dirección y promover la mejora continua del modelo de seguridad.
Jefe Oficina de Tecnologías de Información y las Comunicaciones (CIO)	Dirigir la implementación técnica y tecnológica de los proyectos e iniciativas definidas en el PESI, garantizando la operación, mantenimiento y fortalecimiento de los controles tecnológicos institucionales.
Oficina de Control Interno de Gestión	Realizar la evaluación independiente del cumplimiento de los lineamientos definidos en el PESI, verificando la eficacia de los controles implementados y formulando recomendaciones de mejora.
Oficina Asesora Jurídica	Brindar acompañamiento jurídico en la implementación del PESI, verificar el cumplimiento normativo aplicable y apoyar la gestión de aspectos relacionados con protección de datos personales, contratación y seguridad digital.
Lideres de Proceso	Identificar, valorar y gestionar los riesgos de seguridad de la información asociados a sus procesos, implementar los controles definidos y garantizar el cumplimiento de las políticas institucionales de seguridad y privacidad de la información.
Supervisores de Contratos	Verificar el cumplimiento de los requisitos de seguridad de la información, privacidad y protección de datos establecidos contractualmente para proveedores y terceros.

Cargo / Rol	Responsabilidad en el PESI
Servidores Públicos y Contratistas	Cumplir las políticas, procedimientos y controles de seguridad de la información establecidos por la entidad, participar en las actividades de sensibilización y reportar oportunamente eventos o incidentes de seguridad.

6. Definiciones

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).

Acuerdos de niveles de servicio: Es un acuerdo entre un proveedor de servicios y un cliente. El SLA (en inglés Service Level Agreement) describe el servicio de TI, documenta las metas de niveles de servicio y especifica las responsabilidades del proveedor de servicios de TI y del cliente.

Confidencialidad: Propiedad de la información que pretende garantizar que esta sólo es accedida por personas o sistemas autorizados.

Control: Son todas aquellas políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido
Disponibilidad: Propiedad de la información que pretende garantizar el acceso y uso de la información y los sistemas de tratamiento de esta por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Integridad: Propiedad de la información que pretende mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

Proveedor: Tercero responsable de suministrar bienes o servicios que se requieren para proporcionar servicios de TI, tales como vendedores de productos básicos de hardware y software, redes y comunicaciones y servicios de outsourcing.

Seguridad de la Información: Preservación de la confidencialidad, integridad, y disponibilidad de la información en cualquier medio: impreso o digital.

Tercero: Persona, organización u otra entidad que no forma parte propia de la organización del proveedor de servicios y no es cliente; también denominado subcontratista.

Vulnerabilidad: Es una debilidad de un activo informático, o sistema de información que puede ser explotada por una o más amenazas para causar un daño. Las debilidades pueden aparecer en cualquiera de los elementos de una computadora, tanto en el hardware, el sistema operativo, cómo en el software.

Siglas Institucionales y Gubernamentales, Marcos Normativos y de Gestión, Siglas de Roles y Gobernanza, Técnicas y de Ciberseguridad, Indicadores y Contratos

OTIC: Oficina de Tecnologías de la Información y las Comunicaciones.

MinTIC: Ministerio de Tecnologías de la Información y las Comunicaciones.

ColCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

SIC: Superintendencia de Industria y Comercio.

PESI: Plan Estratégico de Seguridad de la Información.

MSPI: Modelo de Seguridad y Privacidad de la Información.

MTTD: Mide el tiempo promedio que tarda un equipo o sistema de seguridad en identificar que se ha producido una amenaza o una violación.

MIPG: Modelo Integrado de Planeación y Gestión.

PEI: Plan Estratégico Institucional.

SGSPI: Sistema de Gestión de Seguridad y Privacidad de la Información.

ISO/IEC: Organización Internacional de Normalización / Comisión Electrotécnica Internacional (International Organization for Standardization / International Electrotechnical Commission).

NIST: Instituto Nacional de Estándares y Tecnología (National Institute of Standards and Technology).

PHVA: Ciclo de mejora continua: Planificar, Hacer, Verificar, Actuar.

DOFA: Matriz de análisis: Debilidades, Oportunidades, Fortalezas y Amenazas.

CIO: Director de Información / Jefe de la OTIC (Chief Information Officer).

CISO: Oficial de Seguridad de la Información (Chief Information Security Officer).

CSIRT: Equipo de Respuesta a Incidentes de Seguridad Informática (Computer Security Incident Response Team).

RTO: Tiempo Objetivo de Recuperación (Recovery Time Objective).

RPO: Objetivo de Punto de Recuperación (Recovery Point Objective).

MFA: Autenticación Multifactor (Multi-Factor Authentication).

XDR: Detección y Respuesta Extendida (Extended Detection and Response).

EDR: Detección y Respuesta en Endpoints (Endpoint Detection and Response).

NDR: Detección y Respuesta en la Red (Network Detection and Response).

SIEM: Gestión de Eventos e Información de Seguridad (Security Information and Event Management).

DLP: Prevención de Pérdida de Datos (Data Loss Prevention).

WORM: Almacenamiento Inmutable: Escribir una vez, leer muchas (Write Once, Read Many).

VPN: Red Privada Virtual (Virtual Private Network).

KPI: Indicador Clave de Desempeño (Key Performance Indicator).

KRI: Indicador Clave de Riesgo (Key Risk Indicator).

SLA: Acuerdo de Nivel de Servicio (Service Level Agreement).

NDA: Acuerdo de Confidencialidad (Non-Disclosure Agreement).

7. Desarrollo del plan

El presente capítulo desarrolla los componentes estratégicos y operativos del Plan Estratégico de Seguridad de la Información (PESI) de la Justicia Penal Militar y Policial. A partir del diagnóstico institucional del Sistema de Gestión de Seguridad de la Información (SGSI), se identifican las principales brechas, riesgos y oportunidades de mejora que sirven como fundamento para la definición de las estrategias, proyectos y acciones priorizadas para el período 2026-2030.

Con base en este análisis, se presentan las estrategias de seguridad digital, el portafolio de proyectos, la articulación con los riesgos institucionales, la hoja de ruta para su implementación, los recursos requeridos y los mecanismos de seguimiento y medición, con el propósito de fortalecer la protección de la información, la ciberseguridad y la resiliencia digital de la entidad, en concordancia con los lineamientos del MSPI, la Política de Gobierno Digital y los objetivos institucionales

7.1. Diagnóstico del Sistema de Gestión de Seguridad de la Información

El presente compilado del diagnóstico presentado permite ubicar a la entidad para orientar el mapa de ruta, documentando el estado actual de madurez del Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, tomando como línea base el diagnóstico inicial realizado en la vigencia 2024 bajo el marco ISO/IEC 27001:2013, y contrastándolo con la evaluación actual realizada bajo los estándares actualizados de ISO/IEC 27001:2022 y MSPI versión 5.0, tomado primero los tres hallazgos principales.

7.2. Hallazgos principales

La materialización del incidente de ransomware 'Gunra' en junio de 2025 constituyó un punto de inflexión crítico que expuso la brecha existente entre la gestión documental del riesgo y la resiliencia operativa real de la JPMP. Si bien la entidad demostró una capacidad de recuperación técnica superior al promedio sectorial al restablecer el Sistema Misional, el evento evidenció que la resiliencia no se ha abordado desde la planeación integral de la arquitectura institucional. La vulnerabilidad estructural trasciende la simple adopción de controles tecnológicos aislados en la red, revelando la falta de un diseño de plataformas y sistemas dinámicos que sean resilientes por defecto.
Esta debilidad sistémica se extiende a los procesos, la gestión de proveedores y, críticamente, a las personas, evidenciando una carencia institucional de esquemas de redundancia o pares funcionales (respaldo de conocimiento) para el talento humano clave. Más allá de la interrupción operativa, el hallazgo principal reside en una desconexión estratégica: la valoración previa del riesgo como 'Probabilidad Muy Baja' refleja un modelo de gestión estático que ignoró la evolución del panorama de amenazas, contraviniendo el principio de mejora continua de la norma ISO/IEC 27001:2022. Al persistir estas debilidades sistémicas en el diagnóstico de 2026 y carecer de un análisis formal de causa raíz, la institución mantiene una vulnerabilidad latente donde la 'armadura documental' no logra compensar la falta de una verdadera capacidad adaptativa, fragmentando el ciclo PHVA e impidiendo la consolidación de una resiliencia institucional real y holística.

El diagnóstico institucional de 2026 ratifica una asimetría operacional crítica en la JPMP, donde el dominio de controles tecnológicos (39%) presenta un rezago sistémico frente a la robustez administrativa del SGSI. Esta brecha se traduce en una 'invisibilidad táctica' bajo el marco NIST CSF 2.0, evidenciando que las funciones de Protección (48%) y Detección (50%) operan de manera atomizada y reactiva a pesar de la existencia de herramientas perimetrales. La carencia de un 'sistema nervioso digital' basado en la correlación centralizada (SIEM/SOAR) impide la orquestación de una respuesta automatizada, lo que dilata peligrosamente el tiempo de residencia de potenciales amenazas. Al no contar con una trazabilidad técnica integrada, la institución se encuentra en un estado de vulnerabilidad operativa donde la infraestructura es incapaz de identificar movimientos laterales o exfiltraciones silenciosas en tiempo real, comprometiendo

directamente la soberanía del dato judicial y la eficacia de la función misional de justicia ante ataques de alta sofisticación.

Durante la revisión del estado actual de la ciberseguridad para la vigencia 2026, se evidenció una omisión crítica en la planeación presupuestal tecnológica: no se ha documentado ni gestionado el riesgo materializado referente a la no aprobación del presupuesto para la renovación y soporte de la plataforma Trellix (XDR/EDR). En consecuencia, los controles técnicos de protección activa en endpoints, implementados como medida de contención y erradicación tras el incidente de ransomware 'Gunra', han quedado sin respaldo financiero para el 2026, dejando a la entidad operando con un gran riesgo en la cobertura de su herramienta de defensa y visibilidad.

El diagnóstico evidencia un escenario de madurez desequilibrada: la entidad cuenta con fortalezas significativas en la protección de sus instalaciones (Físico) y ha mejorado sus procesos de talento humano (Personas), pero presenta brechas críticas en la implementación de controles tecnológicos y en la formalización de su gobernanza organizacional.

7.3. Índice de Madurez por Dominios (Anexo A - ISO 27001:2022)

Ilustración 1 Gráfico de brechas anexo A ISO 27001:2022 autodiagnóstico JPMP 2026.

Dominio de Control	Calificación	Nivel de Madurez	Interpretación Operativa
Físicos (A.7)	80%	Gestionado	Fortaleza principal. El perímetro y la disposición de activos están controlados.
Personas (A.6)	65%	Gestionado	Avance significativo en revisión de antecedentes y cultura de seguridad base.
Organizacionales (A.5)	46%	Efectivo	Retroceso por falta de evidencia en revisión y aprobación formal de políticas.
Tecnológicos (A.8)	39%	Repetible	Riesgo Crítico. Gestión manual, ausencia de cifrado y monitoreo débil.
PROMEDIO GLOBAL	**57.25%**	**EFECTIVO**	**La entidad depende de la reacción humana más que de la prevención técnica.**

7.4. Cumplimiento ISO 27001:2022 ponderado por categorías

Categoría	Controles Aplicables	Cumplimiento 2024*	Cumplimiento 2025	Delta	Tendencia
Organizacionales	37	48%	45%	-3%	⬇ Deterioro *
Personas	8	58%	65%	+7%	⬆ Mejora
Físicos	14	75%	80%	+5%	⬆ Mejora
Tecnológicos	34	41%	39%	-2%	⬇ Deterioro *

Nota: Los datos del "Cumplimiento 2024" fueron re mapeados de la estructura ISO 27001:2013 (MSPI V4.0) a la taxonomía 2022 (MSPI v5.0) para permitir comparabilidad.

Nota aclaratoria: La disminución en este dominio obedece principalmente a la incorporación de nuevos controles en ISO/IEC 27001:2022 que elevan el nivel de exigencia técnica, particularmente en:

- Gestión de configuración.
- Monitoreo de actividades.
- Enmascaramiento de datos.
- Codificación segura.
- Inteligencia de amenazas.
- Gobierno de servicios en la nube.
- Filtrado web.

los cuales no estaban explícitamente definidos en la versión ISO27001:2013 (MSPI V4.0) y requieren capacidades técnicas y herramientas adicionales para su implementación.

A continuación, se presenta el análisis detallado de cada una de las categorías evaluadas en el marco del MSPI, con el fin de contextualizar los porcentajes de cumplimiento obtenidos y su impacto en el nivel de madurez del SGSI. Este análisis permite identificar fortalezas, brechas y oportunidades de mejora específicas en las categorías: organizacionales, de personas, físicas y tecnológicas, cuyos resultados se resumen en la Tabla.

7.5. Análisis detallado del ciclo PHVA (cláusulas MSPI)

El Modelo de Operación evalúa la gestión estratégica del SGSI. Los resultados indican debilidades en las fases de verificación y mejora continua.

Planificación y liderazgo

- Contexto de la Organización (75%): La entidad tiene claramente identificadas sus partes interesadas, el marco legal (Ley 1581, Ley 1712) y su misión crítica.
- Liderazgo (75%): Existe compromiso de la Alta Dirección, reflejado en la creación del Comité Institucional de Gestión y Desempeño y la aprobación de la Política General V2.
- Planificación (40%): La gestión de riesgos (Cláusula 6) requiere actualización. La matriz actual no refleja dinámicamente los riesgos emergentes de ciberseguridad.

Soporte y operación

- Soporte (40%): Existen recursos asignados, pero la concienciación y la comunicación interna deben pasar de ser teóricas a simulaciones prácticas.
- Operación (40%): El tratamiento de los riesgos no se está ejecutando conforme a lo planeado, evidenciado por la materialización de incidentes técnicos.

Evaluación de desempeño y mejora

- Evaluación y Desempeño (40%): Se carece de un seguimiento adecuado. No se han realizado auditorías internas técnicas rigurosas recientes que midan la eficacia real de los controles.
- Mejora Continua (40%): La gestión de "No conformidades" es reactiva. Se documentan acciones correctivas post-incidente, pero falta gestión preventiva sistemática.

7.6. Perfil de ciberseguridad (alineación NIST CSF)

El cruce de los controles con el Framework de Ciberseguridad del NIST arroja un perfil altamente Reactivo.

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	**Calificación entidad**	**Nivel ideal CSF**
GOBERNAR	50	100
IDENTIFICAR	47	100
PROTEGER	48	100
DETECTAR	50	100
RESPONDER	60	100
RECUPERAR	57	100

Ilustración 2 tabla del modelo de Framework de Ciberseguridad NIST del autodiagnóstico JPMP 2026.

1. Identificar (~50%): Se conoce el entorno y los activos críticos (SPOA, Nodos hiperconvergentes), pero falta evaluación de riesgos en la cadena de suministro de TI.
2. Proteger (~40%) - CRÍTICO: La capacidad para limitar el impacto de un evento es baja. Faltan controles de seguridad de datos (enmascaramiento) y protección de plataformas.
3. Detectar (~40%) - CRÍTICO: "Ceguera operativa". Ausencia de

monitoreo continuo (SIEM/SOC) y análisis de eventos adversos en tiempo real.

4. Responder (60%): Fortaleza. Los planes de comunicación y mitigación se activan correctamente ante la crisis.
5. Recuperar (60%): Existen planes de recuperación y copias de seguridad (backups), aunque requieren pruebas de estrés periódicas (RTO/RPO).
6. Conclusión NIST: La UAE-JPMP tiene buena capacidad para actuar una vez materializado el desastre, pero sus defensas para evitar que el atacante ingrese o se mueva lateralmente son vulnerables.

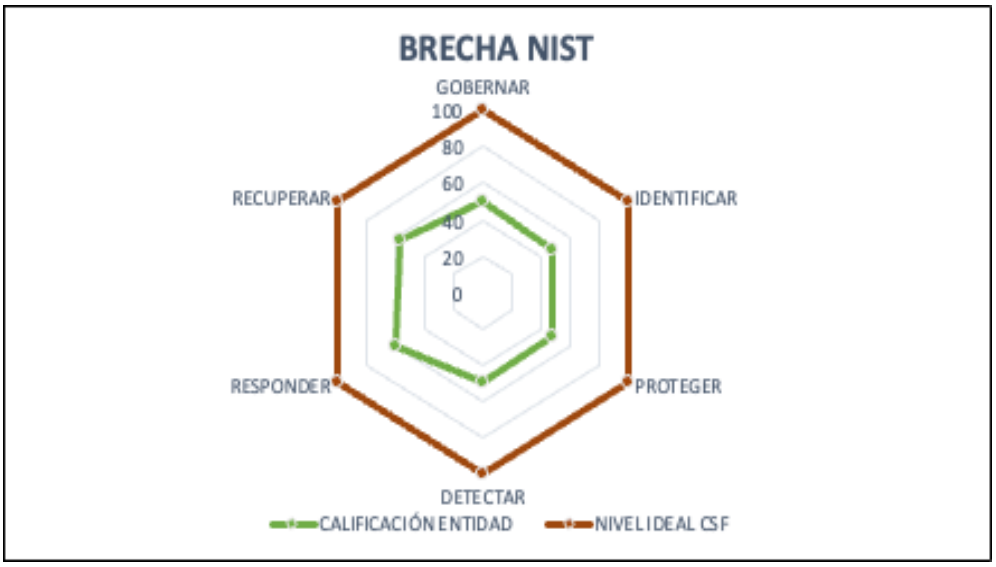

Ilustración 3 Gráfico de Red de brechas NIST del autodiagnóstico JPMP 2026.

7.7. Hallazgos técnicos y brechas de seguridad prioritarias

El análisis detallado de los controles tecnológicos (Dominio A.8) y el incidente de Ransomware "Gunra" (Junio 2025) exponen las siguientes vulnerabilidades críticas:

- A.8.8 Gestión de Vulnerabilidades (Nivel Inicial): El proceso de parchado es esporádico y manual. La falta de escaneos continuos dejó expuesta la vulnerabilidad que fue explotada en el ataque de Ransomware, provocando una indisponibilidad de 2.5 semanas.
- A.8.11 Enmascaramiento de Datos (0% - Inexistente): Las bases de datos de entornos de prueba no cuentan con técnicas de ofuscación. Esto expone datos personales sensibles e información de procesos judiciales, vulnerando la Ley 1581 de 2012 y el

principio de reserva.

- A.8.12 Prevención de Fuga de Datos (DLP) (Bajo Cumplimiento): No existen controles automatizados en los endpoints (estaciones de trabajo) para evitar la extracción de expedientes digitales a través de memorias USB o correos no institucionales.
- A.5.19 Seguridad en Cadena de Suministro de TI: Se identificó una falta de rigurosidad en los anexos técnicos de seguridad y en el derecho a auditar a proveedores de servicios en la nube y desarrolladores externos. (cadena de suministro de TI no se refiere a logística física sino a la dependencia de proveedores de servicios de TI, desarrolladores externos y plataformas en la nube).

7.8. Análisis del contexto presupuestal para la seguridad digital en el sector público.

La inflación representa el desafío más inmediato para la estabilidad macroeconómica en 2026. Tras cerrar 2025 en un 5,10%, el primer bimestre de 2026 ha mostrado una aceleración que sitúa las proyecciones anuales entre el 5,0% y el 7,2%. Este fenómeno se atribuye en gran medida al incremento del salario mínimo del 23,7% decretado para el presente año, una medida que, si bien busca mejorar los ingresos reales, ha generado una presión al alza en los costos de servicios regulados, arriendos y transporte.

La administración central ha tenido que implementar una serie de aplazamientos presupuestales que, de forma acumulada, ascienden a 44 billones de pesos. Estos ajustes no solo responden a la caída de la Ley de Financiamiento, sino también a la suspensión de decretos previos por parte de la Corte Constitucional. Para las entidades públicas, esto se traduce en una rigidez presupuestal extrema, donde el 93% de las apropiaciones se destinan a gastos fijos, servicio de la deuda y transferencias obligatorias, dejando un espacio marginal para la inversión en nuevos proyectos de transformación digital.

En el sector de las Tecnologías de la Información y las Comunicaciones (TIC), la disminución presupuestal es alarmante. El presupuesto del sector para 2026 se ha reducido en un 27% en comparación con 2025, pasando de 2,9 billones de pesos a solo 2,1 billones. Esta contracción obliga a un repriorización de los proyectos, donde las metas de conectividad rural y educación digital deben ejecutarse con una eficiencia operativa mucho mayor según informes de MINTI C y el Senado.

El mayor riesgo para los proyectos de TI en 2026 es el aplazamiento presupuestal por bajo recaudo o compromisos de operación de las entidades.

7.9. Análisis DOFA Estratégico

Para trazar una hoja de ruta que realmente blinde la integridad de la Justicia Penal Militar y Policial hacia el 2030, es vital alejarnos de la conformidad documental y mirar de frente nuestra realidad operativa. Este análisis DOFA no es solo un ejercicio de cumplimiento normativo bajo el MSPI; es el espejo estratégico que nos revela la derivación actual de la entidad: una institución con una envidiable 'armadura' física y normativa, pero con 'músculos' técnicos que requieren un fortalecimiento inmediato tras las lecciones aprendidas del incidente de ransomware 'Gunra'. Al diagnosticar con rigor nuestras debilidades en monitoreo y las amenazas latentes de perjuicio a la prueba digital, abrimos la puerta para capitalizar oportunidades transformadoras como el CONPES 4144, asegurando que la ciberseguridad deje de ser un proceso de soporte para convertirse en el garante soberano de la administración de justicia digital en Colombia.

- **FORTALEZAS (Internas)**

  - Robusta estructura documental: La entidad posee una "armadura" de manuales, resoluciones y políticas aprobadas con un cumplimiento administrativo del 54.7%.
  - Blindaje físico superior: La seguridad perimetral de instalaciones y centros de datos es el dominio más fuerte, calificado entre el 72% y el 80%.
  - Institucionalización del liderazgo: Existe un compromiso real de la Alta Dirección materializado en la creación del Comité Institucional de Gestión y Desempeño.
  - Talento humano con cultura base: Se evidencia un avance en la verificación de antecedentes y programas de concientización inicial (65% de madurez en personas).
  - Claridad en el marco legal: Pleno conocimiento del entorno jurídico sectorial, cumplimiento de la Ley 1581 y alineación con la misión crítica judicial de la entidad.

- **DEBILIDADES (Internas)**

  - Rezago técnico crítico: El dominio de controles tecnológicos (A.8) es el punto más débil con solo 39% de madurez, operando bajo procesos manuales y esporádicos.
  - Bajo registro centralizado: Ausencia de una plataforma centralizada de orquestación (SIEM/SOC) que permita detectar ataques o movimientos laterales en tiempo real.

- Vacío de autoridad técnica (CISO): Falta de designación formal de un Oficial de Seguridad con independencia funcional, lo que genera conflictos de interés con la operación de TI.
- Gestión de riesgos estática: La valoración del riesgo previa al incidente "Gunra" (calificada como "Probabilidad Muy Baja") demuestra un modelo que no se actualiza ante amenazas dinámicas.
- Fragilidad en la clasificación del dato: Inexistencia de criterios CID (Confidencialidad, Integridad, Disponibilidad) granulares, impidiendo proteger con prioridad los expedientes bajo reserva sumarial.

▪ OPORTUNIDADES (Externas)

- Política Nacional de IA (CONPES 4144): Acceso a recursos y marcos nacionales para financiar la automatización de la ciberdefensa mediante algoritmos inteligentes.
- Migración normativa ISO 27001:2022: Ventana de oportunidad para actualizar el SGSI bajo los nuevos controles de ciber-resiliencia antes de octubre de 2025.
- Adopción de Nube Soberana: Posibilidad de transferir riesgos técnicos y mejorar la disponibilidad mediante nubes seguras (Azure/AWS) con soberanía de datos en Colombia.
- Integración con el Sector Defensa: Potenciar la respuesta ante incidentes mediante la coordinación fluida con COLCERT y el Comando Conjunto Cibernético (CCOCI).
- Paradigma Zero Trust (Confianza Cero): Capacidad de blindar los accesos remotos y las identidades privilegiadas siguiendo los lineamientos de NIST SP 800-207.

▪ AMENAZAS (Externas)

- Escalada de Ransomware sectorial: Alta probabilidad de nuevos ataques dirigidos (como el incidente "Gunra" de 2025) diseñados para secuestrar el SPOA y la prueba digital.
- Sofisticación de ataques con IA: Uso de Deepfakes e ingeniería social avanzada para suplantar la identidad de magistrados y fiscales y alterar procesos judiciales.
- Sanciones por brechas de datos: Riesgo legal alto ante la Superintendencia de Industria y Comercio (SIC) por la filtración de datos sensibles de militares, policías y víctimas.
- Obsolescencia de hardware perimetral: Los sistemas de videovigilancia y control de acceso físico están al final de su vida útil y sin soporte vigente del fabricante.

- Vulnerabilidad en la cadena de suministro de TI: Dependencia crítica de proveedores externos de TI que no cuentan con cláusulas de auditoría de seguridad o anexos técnicos rigurosos.
- Nota de Ajuste Técnico: Brecha entre Cumplimiento Normativo y Realidad Operativa (A.7)
- Se ha identificado una inconsistencia crítica entre la valoración del riesgo y el índice de madurez reportado para la Dimensión Física (Control A.7). Mientras que el análisis DOFA institucional categoriza correctamente la "Obsolescencia de hardware perimetral" como una amenaza latente, la calificación de cumplimiento del 80% proyecta una fortaleza que no guarda simetría con la realidad operativa de los sistemas de control de acceso. Esta distorsión se origina en una ponderación que favorece los controles administrativos (políticas y procedimientos) sobre la efectividad técnica del hardware. En consecuencia, la JPMP reconoce que la obsolescencia de los sistemas de autenticación física y mecanismos de cierre compromete la integridad del perímetro judicial, por lo cual se ajusta la visión estratégica para priorizar la modernización tecnológica. Esta corrección es vital para evitar una falsa sensación de seguridad que fragmente el ciclo de mejora continua y para alinear el presupuesto de inversión con la mitigación de vulnerabilidades físicas reales identificadas en el diagnóstico 2026.

7.10. Estrategia de seguridad digital

La Justicia Penal Militar y Policial (JPMP) asume el compromiso de consolidar un ecosistema de seguridad digital resiliente y vanguardista, mediante el despliegue de una arquitectura de gobernanza integral que trasciende el cumplimiento documental para convertirse en un pilar de confianza institucional. Esta estrategia unifica de manera armónica principios, políticas, estándares y procedimientos técnicos, cuyo epicentro es la implementación rigurosa del Modelo de Seguridad y Privacidad de la Información (MSPI) y su plena convergencia con los habilitadores transversales de la Política de Gobierno Digital.

Bajo esta visión, la gestión dinámica de riesgos y la orquestación de la respuesta ante incidentes no operan como procesos aislados, sino como motores de mejora continua que blindan la confidencialidad, integridad y disponibilidad de la información judicial, asegurando así el estricto cumplimiento de la Resolución 500 de 2021 y garantizando

que la transformación digital de la entidad se ejecute sobre una base de soberanía y seguridad jurídica inalienable.

Por tal motivo, LA JUSTICIA PENAL MILITAR Y POLICIAL (JPMP) define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

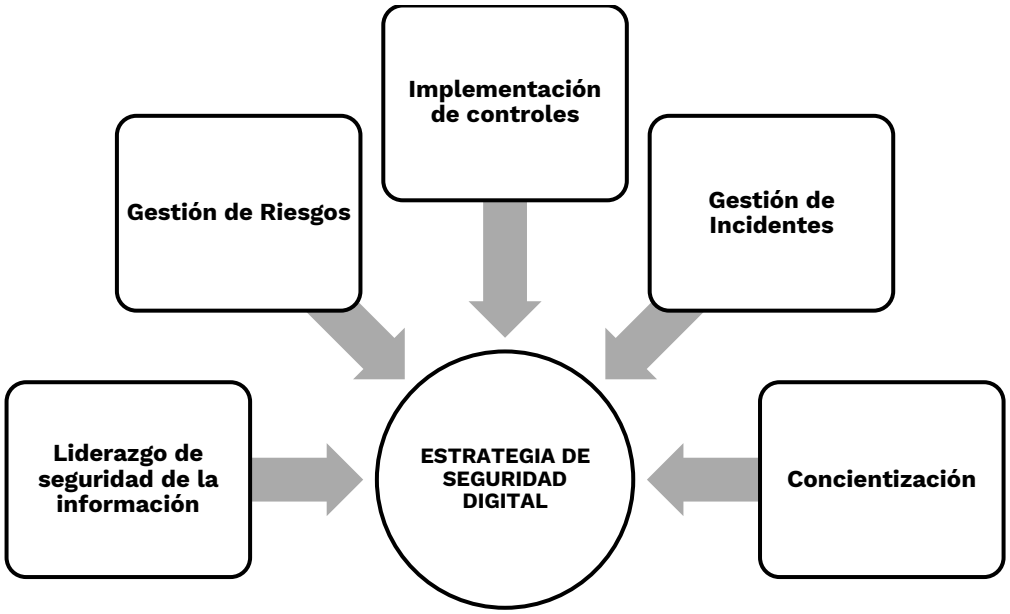

Ilustración 4 conjunto una estrategia general de seguridad digital. MSPI Versión 5 MinTIC 2025.

7.10.1. Descripción de las estrategias específicas.

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

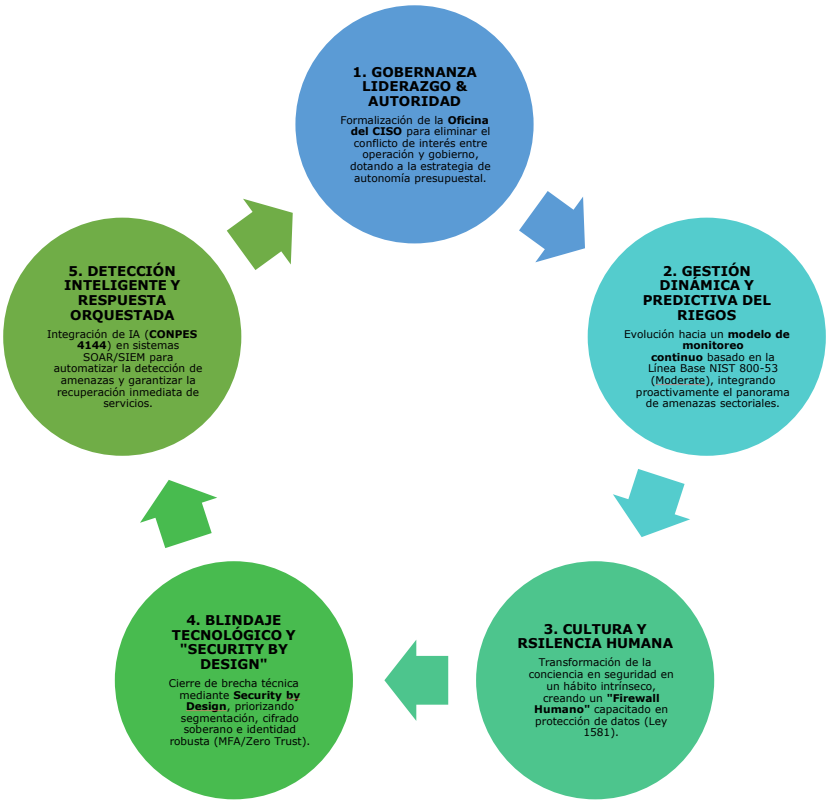

Ilustración 5 Estrategias específicas a implementar. Elaboración propia 2026.

Estrategia	Descripción y enfoque estratégico
Gobernanza, Liderazgo y Autoridad.	Consolidar el Modelo de Seguridad y Privacidad de la Información (MSPI) mediante el compromiso innegociable de la Alta Dirección, materializado en la formalización institucional de la Oficina del CISO (Función GOBERNAR - NIST 2.0). Esta línea busca eliminar la superposición de funciones entre TI y Seguridad, garantizando que el liderazgo de ciberseguridad cuente con la autoridad, autonomía y presupuesto requeridos para supervisar la política general y proteger la soberanía de los activos judiciales, alineándose con la Cláusula 5.3 de ISO 27001:2022.
Gestión Dinámica y Predictiva del Riesgo	Evolucionar de una valoración de riesgos estática y documental a un modelo dinámico de monitoreo continuo. El pilar fundamental será la planificación proactiva que integre el panorama sectorial de amenazas (como el ransomware) y la aplicación rigurosa de controles de la Línea Base NIST 800-53 (Moderate). Se busca reducir el riesgo residual mediante una actualización constante de los vectores de ataque, asegurando que la gestión de riesgos sea el motor del ciclo de mejora continua (PHVA) y no un requisito de cumplimiento pasivo (NIST SP 800-39).

Estrategia	Descripción y enfoque estratégico
Cultura y Resiliencia Humana	Transformar la conciencia en seguridad de una "obligación anual" a un hábito organizacional intrínseco (Higiene Ciber 360°). Mediante programas de capacitación gamificada y transferencia de conocimiento técnico, se fortalecerá el "Músculo de Conciencia" de todo el personal. El objetivo es que cada servidor de la JPMP se convierta en un sensor activo de detección (Human Firewall), apropiando las buenas prácticas de protección de datos personales (Ley 1581) y garantizando la integridad de la prueba digital desde el factor humano.
Blindaje Tecnológico y "Security by Design"	Cerrar la brecha técnica del 39% mediante la implementación prioritaria de controles tecnológicos críticos de la norma ISO 27001:2022 (Cierre de Brecha A.8). Esta línea estratégica prioriza la segmentación de red, el cifrado soberano, la identidad robusta (MFA) y el endurecimiento (Hardening) de sistemas. Se adoptará el principio de "Seguridad desde el Diseño" en cada iniciativa de transformación digital, asegurando que los nuevos sistemas de gestión judicial nazcan protegidos contra la exfiltración de información y el acceso no autorizado.
Detección Inteligente y Respuesta Orquestada	Garantizar una administración de incidentes basada en la orquestación y automatización (SOAR/SIEM), superando la detección reactiva. Bajo la sombrilla del CONPES 4144, se integrarán capacidades de Inteligencia Artificial para la correlación de eventos en tiempo real, permitiendo identificar movimientos laterales y amenazas antes de su materialización. Esta línea institucionaliza el aprendizaje de causa raíz y la formalización de lecciones aprendidas, asegurando que la JPMP opere bajo un estado de vigilancia perpetua y capacidad de recuperación garantizada ante desastres.

7.11. Portafolio de proyectos y actividades

Para cada proyecto específico, Justicia Penal Militar y Policial (JPMP) define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI). Los proyectos deben estar relacionados tanto con el Manual de políticas como con la política de seguridad definida en la entidad, además estos proyectos deben corresponder a la implementación de controles que permita mitigar riesgos de seguridad de la información que la entidad haya identificado. Este mapa de ruta esta alineado a varias iniciativas

que ya se habían programado entre el 2026 al 2023, como gestión vulnerabilidades, solución de Gestión Centralizada y Analítica, reducción verificada de la superficie de ataque, autenticación multifactor (MFA), PAM (Privileged Access Management) para Reducción/Eliminación del riesgo de compromiso por Suplantación/Robo de credenciales esta alineación es fundamental y mandatorio dentro del Plan Estratégico de Seguridad del Información 20226-2030 al tener concentrados el conjunto de actividades requeridas para cumplir con el objetivo principal garantizando la confidencialidad, integridad y disponibilidad de los activos de información.

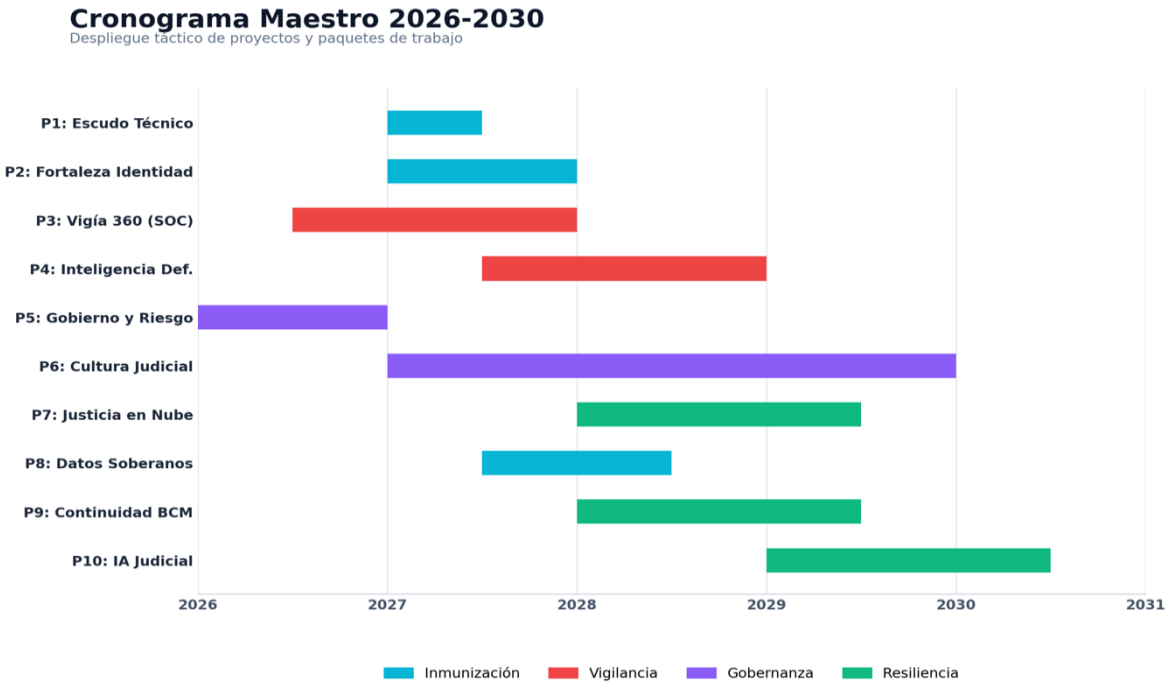

Ilustración 6 Mapa de Ruta Plan Estratégico 2026- 2023. Elaboración propia.

7.11.1. Proyecto 1: Proyecto Escudo Técnico y Blindaje

Alcance Estratégico: Eliminar/Reducir la deuda/brecha técnica y la vulnerabilidad/amenaza estructural a través de soluciones: "Cybersecurity Mesh" – seguridad en arquitectura distribuida:

El objetivo es transitar de una administración basada en el esfuerzo técnico hacia un endurecimiento (Hardening) verificado, elevando las barreras de intrusión para actores malintencionados.

Alcance Técnico:

- Paquete 1.1: Gestión Vulnerabilidades. Despliegue de plataforma para escaneos diarios automatizados y remediación priorizada.
- Paquete 1.2: Endurecimiento superficie de ataque. Implementación de configuraciones seguras basadas en CIS Benchmarks /DISA-STIGs. para el 100% de servidores y estaciones de trabajo
- Paquete 1.3: Gestión de Parchado. Establecimiento de un flujo de trabajo para cerrar vulnerabilidades críticas en menos de 48 horas.
- Paquete 1.4: Inteligencia de Amenazas – caza de amenazas. Implementación de plataforma de inteligencia de amenazas del entorno digital y cacería de amenazas (Threat Hunting).
- Paquete 1.5: Solución de Gestión Centralizada y Analítica: gestión y análisis central de dispositivos de seguridad administrada y visibilidad a través de solución de analítica.

Hito: Reducción verificada de la superficie de ataque en un 80% para Noviembre 2027.

Presupuesto:

Base de Cálculo: Pesos Colombianos (COP) | Referencia: Colombia Compra Eficiente (CCE), juicio de expertos y cotizaciones de nuestra empresa con mayoristas. Se toman 1000 endpoints según estudios previos cargados para la adquisición de herramientas de ciberseguridad.

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado
1.1 Gestión de Vulnerabilidades	Herramientas	Licencia Tenable.ep / Qualys (1.000 activos)	$180.000.000
1.2 Hardening (Endurecimiento superficie de ataque)	Talento Humano	1 Ing. Infraestructura Senior (12 meses)	$144.000.000
1.3 gestión de Parchado	Herramientas	Suscripción Orquestador (Ivanti/Endpoint Central)	$65.000.000
1.4 Inteligencia de Amenazas – caza de amenazas.	Servicios	Suscripción Threat Intelligence / Threat Hunting	$90.000.000
1.5 Solución de Gestión Centralizada y Analítica	Documentación	Consultoría elaboración de Guías Hardening CIS	$45.000.000
TOTAL ESTIMADO P1			**$524.000.000**

7.11.2. Proyecto 2: Proyecto de Fortaleza de Identidad y Acceso Judicial

Alcance Estratégico: Adopción del paradigma Zero Trust (Confianza Cero), SASE - para acceso granular a aplicaciones y recursos donde la identidad es el nuevo perímetro. Busca proteger la legitimidad de las actuaciones judiciales y prevenir la suplantación de funcionarios y de los procesos institucionales.

Alcance Técnico:

- Paquete 2.1: Multifactor de Autenticación con estándar avanzado FIDO2. Mejorar las capacidades de autenticación multifactor robusta para accesos a red y servicios cloud implementando mejores prácticas y capacidades de fabricantes actuales.
- Paquete 2.2: Despliegue de la Gestión de Accesos Privilegiados. Control, gestión y grabación de sesiones para administradores de TI y cuentas de alto privilegio.
- Paquete 2.3: Automatización Gestión de identidad y acceso. Automatización del ciclo de vida del usuario (Onboarding/Offboarding) integrada al Directorio Activo.
- Paquete 2.4: SASE/SE (Borde del Servicio de Acceso Seguro) / ZTNA (acceso Zero Trust a la red). Implementar capacidades de control de acceso a aplicaciones y datos.

Hito: Reducción/Eliminación del riesgo de compromiso por Suplantación/Robo de credenciales en 2027.

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
2.1 MFA / FIDO2 (Multifactor de Autenticación con estándar avanzado FIDO2)	Equipos/Lic.	Tokens físicos (200 und) + Licencia MFA	$110.000.000
2.2 PAM (Gestión de Accesos Privilegiados)	Herramientas	Licencia PAM (50 usuarios administrativos)	$220.000.000

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
2.3 IAM Auto (Gestión de identidad y acceso)	Talento Humano	1 Especialista en Identidad (8 meses)	$96.000.000
2.4 SASE (Borde del Servicio de Acceso Seguro) / ZTNA (acceso Zero Trust a la red)	Herramientas	Licencia ZTNA (Acceso seguro remoto)	$130.000.000
Gobernanza Zero Trust	Documentación	Política Zero Trust y Manual de Identidad	$35.000.000
TOTAL ESTIMADO P2			**$591.000.000**

7.11.3. Proyecto 3: Proyecto de Vigía 360

Alcance Estratégico: Dotar a la entidad de capacidad de detección proactiva. Transforma el monitoreo reactivo en una inteligencia de seguridad centralizada capaz de identificar patrones complejos.
Alcance Técnico:

- Paquete 3.1: SIEM Hybrid (Administración de eventos e información de seguridad). Implementación de un sistema de gestión de eventos con ingesta de logs de aplicaciones core, bases de datos y red.
- Paquete 3.2: 24/7 SOC (Centro de Operaciones de Seguridad) Service 2GEN. Integración con un Centro de Operaciones de Seguridad que utilice cacería de amenazas y para el análisis de comportamiento (UEBA) con inteligencia artificial.
- Paquete 3.3: Respuesta Orquestada (Orquestación, Automatización y Respuesta de Seguridad - SOAR). Automatización de flujos de respuesta ante incidentes detectados a través de Playbooks funcionales con la entidad.

Hito: Reducción del tiempo de detección (Dwell Time) de meses a minutos para finales de 2027.

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
3.1 SIEM Hybrid (Administración de eventos e información de seguridad)	Herramientas	Consumo Cloud (Microsoft Sentinel/Splunk) anual	$320.000.000
3.2 Servicio de SOC (Centro de Operaciones de Seguridad)	Servicios	Tercerización SOC 24/7 (Célula de monitoreo)	$480.000.000
3.3 SOAR (Orquestación, Automatización y Respuesta de Seguridad)	Herramientas	Licencia de Orquestación y Automatización	$150.000.000
Talento Interno Plataforma	Talento Humano	1 Administración de Plataformas de Seguridad	$120.000.000
Procesos - PlayBooks	Documentación	Diseño de Playbooks de Respuesta Institucional	$60.000.000
TOTAL ESTIMADO P3			**$1.130.000.000**

7.11.4. Proyecto 4: Proyecto de Inteligencia Defensiva (EDR/XDR/NDR)

Alcance Estratégico: Evolucionar hacia una defensa basada en comportamiento. Ante amenazas polimórficas y Zero-Day, la red debe tener capacidad de "autodefensa" inteligente.

Alcance Técnico:

- Paquete 4.1: Detección y Respuesta de Endpoint. Sustitución progresiva del antivirus tradicional por soluciones EDR/XDR en el 100% de terminales.
- Paquete 4.2: Cuarentena Automática. Configuración de aislamiento automático de procesos sospechosos basados en indicadores de compromiso (IoC).

- Paquete 4.3: NDR (Detección y Respuesta de Red). detección temprana de amenazas con movimiento lateral en los red y nube.

Hito: Inmunización institucional contra Ransomware moderno para el cierre de 2028

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
4.1 Detección y Respuesta de Endpoint	Herramientas	Licencia EDR/XDR (1.000 puestos)	$240.000.000
4.2 Cuarentena Automática	Talento Humano	1 Ing. Especialista en Respuesta a Incidentes	$132.000.000
4.3 NDR (Detección y Respuesta de Red)	Equipos/Lic.	Sensores de Red (NDR) para Core Data Center	$210.000.000
Estandarización Protocolos de endurecimiento de Punto Final	Documentación	Protocolos de endurecimiento de Punto Final	$30.000.000
TOTAL ESTIMADO P4			**$612.000.000**

7.11.5. Proyecto 5: Proyecto de Gobierno y Riesgo GRC

Alcance Estratégico: Actuar como el "cerebro estratégico" del SGSI. Busca formalizar la toma de decisiones basada en riesgos y garantizar la sostenibilidad del modelo ante cambios presupuestales.

Alcance Técnico:

- Paquete 5.1: Designación del CISO. Nombramiento de un Oficial de Seguridad con independencia jerárquica de TI – Gestión transversal del rol a la JPMP.

- Paquete 5.2: Herramientas GRC (Gobierno, Riesgo y Cumplimiento). Digitalización de la matriz de riesgos institucional y seguimiento automatizado de planes de tratamiento.
- Paquete 5.3: Tableros Dinámicos (Dashboard). Tableros de control con KPI/KRI para la alta dirección y digitalización de evidencia MSPI.

Hito: Designación del CISO en 2026-H2 (Hito no negociable).

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
5.1 Designación CISO	Talento Humano	Honorarios CISO (Nivel Directivo - 12 meses)	$216.000.000
5.2 Herramientas GRC (Gobierno, Riesgo y Cumplimiento)	Herramientas	Licencia Software GRC (Módulos Riesgo/Auditoría)	$160.000.000
5.3 Tableros Dinámicos (Dashboard)	Talento Humano	1 Analista de Riesgos y Cumplimiento	$96.000.000
Actualizar Normatividad (Manual de Políticas)	Documentación	Manual de Políticas SGSI ISO 27001:2022	$55.000.000
TOTAL ESTIMADO P5			**$527.000.000**

7.11.6. Proyecto 6: Proyecto de Cultura Judicial Resiliente

Alcance Estratégico: Fortalecer el cortafuegos humano. Busca mitigar el vector de ataque más utilizado mediante el entrenamiento ético y técnico de los funcionarios.

Alcance Técnico:

- Paquete 6.1: 6.1 Gamificación SAT (Capacitación en concientización sobre seguridad). Plataforma de entrenamiento continuo y obligatorio en ciber higiene.

- Paquete 6.2: Simulación de ataques de Phishing. Campañas trimestrales de ingeniería social con retroalimentación inmediata.
- Paquete 6.3: Talleres funcionarios. Talleres avanzados para magistrados, jueces y fiscales sobre seguridad en dispositivos personales.
- Paquete 6.4: Medición de madurez cultural: Evaluación continua de la cultura de seguridad, alineado a objetivos misionales.

Hito: Reducción del 80% en la tasa de clics en correos maliciosos para 2029.

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
6.1 Gamificación SAT (Capacitación en concientización sobre seguridad)	Herramientas	Licencia Plataforma SAT (Anual)	$75.000.000
6.2 Simulación de ataques de Phishing	Servicios	Campañas trimestrales administradas	$40.000.000
6.3 Talleres funcionarios	Talento Humano	1 Comunicador Especializado en Tecnología	$84.000.000
Campaña	Insumos	Material POP y kits de ciberhigiene	$35.000.000
Medición de madurez cultural	Documentación	Informe de madurez cultural y KPIs	$25.000.000
TOTAL ESTIMADO P6			**$259.000.000**

7.11.7. Proyecto 7: Proyecto de Justicia en la Nube Segura

Alcance Estratégico: Modernizar la infraestructura judicial en entornos Cloud sin perder la soberanía del dato ni el control jerárquico de la información.

Alcance Técnico:

- Paquete 7.1: Implementación de CSPM (Gestión de la Postura de Seguridad en la Nube). Herramientas para el monitoreo de la postura de seguridad en nubes (AWS/Azure/Google).
- Paquete 7.2: WAF (Firewall de Aplicaciones Web) para los Portales. Despliegue de cortafuegos de aplicaciones web para proteger los servicios al ciudadano.
- Paquete 7.3: Servicio de Balanceo de Carga (LB). Mejorar las capacidades de balanceo de aplicaciones/infraestructura/plataforma en NUBE.
- Paquete 7. 4: Gestión de las claves criptográficas para cifrar sus bases de datos. Cifrado nativo de bases de datos con gestión institucional de llaves como BYOK (Bring Your Own Key o "Trae tu propia clave").

Hito: Aseguramiento de la soberanía digital sobre infraestructuras de terceros para 2029.

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
7.1 CSPM (Gestión de la Postura de Seguridad en la Nube)	Herramientas	Licencia Monitoreo Postura Nube (Wiz/Azure)	$120.000.000
7.2 WAF (Firewall de Aplicaciones Web)	Herramientas	Suscripción WAF para portales judiciales	$95.000.000
7.3 Gestión de las claves criptográficas BD.	Equipos/Lic.	Módulo de HSM Cloud / Gestión de Llaves	$110.000.000
Migración	Talento Humano	1 Arquitecto DevSecOps (6 meses)	$90.000.000
Gobernanza Cloud	Documentación	Matriz de Responsabilidad Compartida	$30.000.000
TOTAL ESTIMADO P7			**$445.000.000**

7.11.8. Proyecto 8: Proyecto de Datos Soberanos (DLP/CID)

Alcance Estratégico: Implementar una seguridad centrada en el dato. Busca proteger la reserva legal de los expedientes y cumplir estrictamente con la Ley 1581 (Protección de Datos).

Alcance Técnico:

- Paquete 8.1: Clasificación de Datos con IA. Herramientas de IA para el etiquetado CID automático de expedientes reservados y gobernanza de datos para IA.
- Paquete 8.2: Prevención de Perdida de Datos (DLP)Control de salida de información en puertos USB, correo electrónico y terminales.
- Paquete 8.3: Encriptación de datos Automatizada. Reglas de cifrado automático para cualquier archivo clasificado como "Confidencial".
- Paquete 8.4: Anonimización de datos. Anonimización de datos para pruebas, principalmente para uso de datos en entornos de pruebas.

Hito: Clasificación y protección del 100% de los expedientes reservados en 2028.

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
8.1 Clasificación de Datos con IA	Herramientas	Licencia Microsoft Purview / Varonis	$210.000.000
8.2 Prevención de Perdida de Datos (DLP)	Talento Humano	1 Administrador de Protección de Datos	$108.000.000
8.3 Encriptación de datos Automatizada	Herramientas	Módulo de cifrado de archivos (RMS)	$85.000.000
8.4 Anonimización de datos	Herramientas	Software para enmascaramiento de datos	$130.000.000
Mapeo de Datos	Documentación	Inventario y Taxonomía de Datos Judiciales	$50.000.000
TOTAL ESTIMADO P8			**$583.000.000**

7.11.9. Proyecto 9: Proyecto de Continuidad - Resiliencia cibernética

Alcance Estratégico: Garantizar la supervivencia institucional ante desastres digitales. Actúa como el "seguro de CIBERNETICO" de la JPMP frente a ataques de Secuestro/Denegación/Indisponibilidad/Fuga de datos.

Alcance Técnico:

- Paquete 9.1: WORM (Write Once, Read Many) Infraestructura. Mejora en la gestión de respaldos inmutables protegidos contra borrado lógico accidental o malicioso.
- Paquete 9.2: Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP). Actualización de planes bajo el estándar ISO 22301 y el MSPI.
- Paquete 9.3: Simulacros anuales de caída total (Full Failover Drills). Simulacros anuales de caída total del centro de datos para garantizar indicadores de RTO/RPO/MTPD.

Hito: Validación de recuperación operativa en menos de 12 horas (RTO < 12h) para 2029. (Se puede ajustar según un análisis interno BIA para determinar el RTO real para el 2029 y se toma el valor que se genere del análisis qy).

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
9.1 Infraestructura WORM (Write Once, Read Many	Equipos	Almacenamiento Inmutable (Dell/PureStorage)	$450.000.000
9.2 Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP).	Talento Humano	1 Consultor Continuidad ISO 22301 (6 meses)	$90.000.000
9.3 Drills Failover (Simulacros anuales de caída total)	Servicios	Pruebas de Failover y Estrés de Datos	$80.000.000

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
9.4DRaaS (Recuperación ante Desastres como Servicio)	Herramientas	Suscripción Sitio Alterno de Contingencia	$180.000.000
Actualización del DRP	Documentación	Plan de Recuperación ante Desastres (DRP)	$45.000.000
TOTAL ESTIMADO P9			**$845.000.000**

7.11.10. Proyecto 10: Proyecto de Justicia Aumentada y Ética (IA Segura).

Alcance Estratégico: Adoptar Inteligencia Artificial para la eficiencia judicial bajo un marco ético, de transparencia y de protección de derechos, alineado con el CONPES 4144.

Alcance Técnico:

- Paquete 10.1: entorno Aislado de IA (AI Sandboxing). Creación de entornos seguros para testeo de herramientas de apoyo judicial.
- Paquete 10.2: Anonimización de información IA. Políticas y herramientas para anonimizar datos personales antes de ser procesados por modelos LLM.
- Paquete 10.3: Auditoria de algoritmos. Procesos de auditoría técnica para detectar sesgos algorítmicos que afecten la imparcialidad. (REVISAR VIABILIDAD)

Hito: JPMP reconocida como líder nacional en IA judicial ética y segura al 2030.

Presupuesto:

Paquete de Trabajo	Concepto	Detalle de Recurso	Estimado (Millones COP)
10.1 AI Sandbox	Equipos	Servidor con GPU para entrenamiento local	$280.000.000
10.2 Anonimización de información IA	Talento Humano	1 Científico de Datos (Ingeniero IA)	$144.000.000
10.3 Auditoria de algoritmos	Servicios	Auditoría técnica de algoritmos (Sesgos)	$95.000.000
Ética IA	Documentación	Código de Ética y Políticas de IA JPMP	$40.000.000
Prompts con Filtros de Detención de Perdida	Herramientas	Filtros de privacidad para LLM	$60.000.000
TOTAL ESTIMADO P10			**$619.000.000**

7.12. Matriz de Mitigación de Riesgos

Los 10 proyectos del PESI han sido diseñadas para cubrir la totalidad de los 19 focos de riesgo identificados en el Plan Maestro de Riesgos y el Diagnóstico Integral 2026. A continuación, se presenta la asociación detallada:

No	Escenario de Riesgo Identificado	ID Riesgo Asociado	Proyecto PESI Mitigadora
1	Ingeniería Social y Phishing	SI002	P6: Cultura Judicial Resiliente
2	Suplantación de identidad de funcionarios	SI002	P2: Fortaleza de Identidad (MFA)
3	Robo de credenciales administrativas	SI002	P2: Gestión de Accesos (PAM)

No	Escenario de Riesgo Identificado	ID Riesgo Asociado	Proyecto PESI Mitigadora
4	Accesos no autorizados a bases de datos	SI002	P1: Escudo Técnico (Hardening)
5	Movimientos laterales de atacantes en la red	SI002	P4: Inteligencia Defensiva (NDR)
6	Infección por Ransomware (Caso 'Gunra')	SI002	P4: Inteligencia Defensiva (EDR)
7	Ciberataques dirigidos (APT)	SI002	P3: Vigía 360 (SOC/SIEM)
8	Explotación de vulnerabilidades técnicas	SI002	P1: Gestión de Vulnerabilidades
9	Malware en dispositivos móviles y endpoints	SI002	P4: Inteligencia Defensiva (XDR)
10	Pérdida de integridad en expedientes digitales	IP008 / SI002	P8: Datos Soberanos (Cifrado)
11	Fuga de información sensible (Reserva Sumarial)	SI002	P8: Prevención de Fuga (DLP)
12	Destrucción física de archivos o servidores	GE012	P9: Continuidad (Inmutabilidad)
13	Fuga de conocimiento técnico por salida de personal	GE012	P5: Gobierno y Riesgo GRC
14	Incumplimiento de políticas y normas	IP008 / GE012	P5: Dashboards y Auditoría GRC
15	Indisponibilidad de servicios (SPOA)	GE012 / SI002	P9: Resiliencia (DRP/BCP)
16	Falta de control en infraestructura de nube	SI002	P7: Justicia en la Nube Segura
17	Vulnerabilidades en la cadena de suministro de TI	SI002	P5: Gestión de Proveedores TI
18	Obsolescencia tecnológica no controlada	GE012	P1: Plan de Renovación Técnica
19	Mal uso de IA y falta de ética algorítmica	IP008	P10: Justicia Aumentada y Ética

7.12.1. Análisis detallado por eje táctico

- **Gobernanza, Liderazgo y Autoridad:** Consolidar el Modelo de Seguridad y Privacidad de la Información (MSPI) mediante el compromiso innegociable de la Alta Dirección, materializado en la

formalización institucional de la Oficina del CISO (Función GOBERNAR – NIST 2.0).

- **Gestión Dinámica y Predictiva del Riesgo:** Evolucionar de una valoración de riesgos estática y documental a un modelo dinámico de monitoreo continuo.

- **Cultura y Resiliencia Humana:** Transformar la conciencia en seguridad de una "obligación anual" a un hábito organizacional intrínseco (Higiene Ciber 360°).

- **Blindaje Tecnológico y "Security by Design":** Cerrar la brecha técnica del 39% mediante la implementación prioritaria de controles tecnológicos críticos de la norma ISO 27001:2022 (Cierre de Brecha A.8).

- **Detección Inteligente y Respuesta Orquestada:** Garantizar una administración de incidentes basada en la orquestación y automatización (SOAR/SIEM), superando la detección reactiva. Bajo la sombrilla del CONPES 4144, se integrarán capacidades de Inteligencia Artificial

- **Blindaje Tecnológico y "Security by Design" (Mitiga RS102, RS103, RS104)**

  Impacto en Riesgos: Ataca la causa raíz de la vulnerabilidad estructural (39% de madurez tecnológica).

  Acción: Los proyectos P1, P2 y P8 eliminan la posibilidad de que el malware se propague (Hardening), que las cuentas sean robadas (MFA) y que los datos salgan de la entidad (DLP).

- **Gestión Dinámica y Predictiva del Riesgo (Mitiga RS103)**

Impacto en Riesgos: Reduce el "Dwell Time" o tiempo de residencia de un atacante.

Acción: P3 (Vigía 360) y P4 (Inteligencia Defensiva) proporcionan los "ojos" técnicos para detectar ciberataques que antes pasaban desapercibidos, permitiendo una respuesta inmediata y orquestada.

- **Gobernanza, Liderazgo y Autoridad – Cultura y Resiliencia Humana (Mitiga RS101, RS105)**

Impacto en Riesgos: Fortalece la armadura humana y administrativa.

Acción: P6 (Cultura) actúa sobre el riesgo RS101 (Ingeniería Social), mientras que P5 (GRC) asegura que la fuga de conocimiento (RS105) se mitigue mediante procedimientos operativos documentados y auditables.

- **Detección Inteligente y Respuesta Orquestada (Mitiga RS104 y Riesgos Futuros)**

  Impacto en Riesgos: Garantiza que la entidad sobreviva a la materialización de un desastre.

  Acción: P9 (Resiliencia) asegura la recuperación en menos de 12 horas ante ataques destructivos, y P10 (IA) previene nuevos riesgos derivados de la transformación digital acelerada.

  La articulación estratégica entre el PESI y el Mapa de Riesgos Institucional transforma la seguridad de la JPMP, evolucionando de un enfoque puramente documental a un modelo operativo y dinámico. En este sentido, los recursos asignados a los proyectos 10 cuentan con una trazabilidad directa orientada a la disminución del riesgo residual de los 19 escenarios identificados, impulsando el nivel de madurez del 57.5% actual hacia la meta del 89% proyectada para el año 2030.

7.13. Mapa de Ruta y cronograma de implementación del PESI

El Mapa de Ruta y Cronograma de Implementación del PESI establece la secuencia de ejecución de las estrategias, proyectos y actividades priorizadas para el período 2026-2030, definiendo los principales hitos, responsables y tiempos de desarrollo. Su propósito es orientar la implementación gradual de las capacidades de seguridad de la información, garantizar la articulación entre los proyectos estratégicos y facilitar el seguimiento al cumplimiento de los objetivos, metas e iniciativas definidas en el Plan Estratégico de Seguridad de la Información.

7.13.1. Mapa de Ruta

MAPA DE RUTA — PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN 2026 – 2030																								
PROYECTO / ACTIVIDAD				2026				2027				2028				2029				2030				
				Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
PROYECTO 1 — ESCUDO TÉCNICO Y BLINDAJE																								
P1	1.1 Gestión de Vulnerabilidades	Coord. Plataforma Tecnológica - CISO	31/12/2026				31/12																	
P1	1.1 Gestión de Vulnerabilidades	Coord. Plataforma Tecnológica - CISO	30/06/2027						30/06															
P1	1.2 Hardening (Endurecimiento	Coord. Plataforma Tecnológica - CISO	30/09/2027							30/09														
P1	1.3 Gestión de Parchado	Coord. Plataforma Tecnológica - CISO	31/12/2027								31/12													
P1	1.4 Inteligencia de Amenazas — Caza	Coord. Plataforma Tecnológica - CISO	30/09/2028											30/09										
P1	1.5 Solución de Gestión	Coord. Plataforma Tecnológica - CISO	30/09/2028											30/09										
PROYECTO 2 — FORTALEZA DE IDENTIDAD JUDICIAL																								
P2	2.1 MFA / FIDO2 (Multifactor de	Coord. Plataforma Tecnológica - CISO	30/09/2027							30/09														
P2	2.2 PAM (Gestión de Accesos	Coord. Plataforma Tecnológica - CISO	31/12/2027								31/12													
P2	2.3 IAM Auto (Gestión de	Coord. Plataforma Tecnológica - CISO	30/06/2028										30/06											
P2	2.4 SASE / ZTNA (Acceso Zero Trust a	Coord. Plataforma Tecnológica - CISO	31/12/2029																31/12					
PROYECTO 3 — VIGÍA 360																								
P3	3.1 SIEM Hybrid (Eventos e	Coord. Plataforma Tecnológica - CISO	31/12/2027								31/12													
P3	3.2 Servicio de SOC 2GEN	Coord. Plataforma Tecnológica - CISO	30/06/2028										30/06											
P3	Procesos -	CISO	31/12/2028												31/12									
P3	3.3 SOAR (Orquestación,	Coord. Plataforma Tecnológica - CISO	31/12/2029																31/12					
P3	Talento Interno Plataforma	OTIC	31/12/2029																31/12					
P3	Gobernanza Zero Trust	CISO	30/09/2029															30/09						
PROYECTO 4 — INTELIGENCIA DEFENSIVA																								
P4	4.1 Detección y Respuesta de	Coord. Plataforma Tecnológica - CISO	31/12/2027								31/12													
P4	4.1 Detección y Respuesta de	Coord. Plataforma Tecnológica - CISO	31/12/2028												31/12									
P4	Estandarización Protocolos	CISO	31/12/2028												31/12									
P4	4.2 Cuarentena Automática	Coord. Plataforma Tecnológica - CISO	30/09/2029															30/09						
P4	4.3 NDR (Detección y Respuesta de Red)	Coord. Plataforma Tecnológica - CISO	31/12/2029																31/12					
P4	4.3 NDR (consolidación	Coord. Plataforma Tecnológica - CISO	31/10/2030																					31/1
PROYECTO 5 — GOBIERNO Y RIESGO GRC																								
P5	5.1 Designación CISO	Oficina Asesora de Planeación	31/12/2026				31/12																	
P5	5.1 Designación CISO (ratificación	Oficina Asesora de Planeación	31/12/2030																					31/1
P5	5.2 Herramientas	OTIC - CISO	31/12/2027								31/12													
P5	5.2 Herramientas	OTIC - CISO	31/12/2028												31/12									
P5	Mantenimiento	OTIC - CISO	31/12/2030																					31/1
P5	5.3 Tableros	CISO	31/12/2027								31/12													
P5	Actualizar	CISO	30/09/2028											30/09										
PROYECTO 6 — CULTURA JUDICIAL RESILIENTE																								
P6	6.1 Gamificación SAT	Talento Humano - CISO	31/12/2028												31/12									
P6	6.2 Simulación de ataques de Phishing	Talento Humano - OTIC - CISO	31/10/2028												31/10									
P6	6.2 Simulación de Phishing	Talento Humano - OTIC - CISO	30/09/2029															30/09						
P6	6.3 Talleres funcionarios	Talento Humano - CISO	31/12/2030																					31/1
PROYECTO 7 — JUSTICIA EN LA NUBE SEGURA																								
P7	7.1 CSPM (Postura de Seguridad en la	Coord. Plataforma Tecnológica - CISO	31/12/2028												31/12									
P7	7.2 WAF (Firewall de Aplicaciones Web)	Coord. Plataforma Tecnológica - CISO	31/12/2028												31/12									
P7	7.3 Balanceo de Carga / Encriptación	Coord. Plataforma Tecnológica - CISO	31/12/2028												31/12									
P7	Gobernanza Cloud	CISO	30/06/2029														30/06							
P7	Migración Cloud	Coord. Plataforma Tecnológica - CISO	30/06/2029														30/06							
PROYECTO 8 — DATOS SOBERANOS																								
P8	8.1 Clasificación de	DBA - CISO	31/12/2028												31/12									
P8	Database	DBA - OTIC	31/12/2029																31/12					
P8	8.2 Data Loss Prevention (DLP)	Coord. Plataforma Tecnológica - CISO	31/12/2029																31/12					
P8	8.3 Encriptación de datos Automatizada	DBA - CISO	31/12/2029																31/12					
P8	8.4 Anonimización	DBA - CISO	31/12/2028												31/12									
P8	8.4 Anonimización	DBA - CISO	30/06/2030																					
P8	Mapeo de Datos	DBA - CISO	31/12/2030																					31/1
PROYECTO 9 — CONTINUIDAD - RESILIENCIA CIBERNÉTICA																								
P9	9.1 Infraestructura WORM (Write Once,	Coord. Plataforma Tecnológica - CISO	30/09/2029															30/09						
P9	9.2 BCP y DRP (Continuidad y	Coord. Plataforma Tecnológica - CISO	31/12/2029																31/12					
P9	9.3 Drills Failover (Simulacros de	Coord. Plataforma Tecnológica - CISO	31/12/2029																31/12					
P9	DRaaS (Recuperación ante	Coord. Plataforma Tecnológica - CISO	31/12/2030																					31/1
P9	Actualización del	CISO	30/09/2030																				30/09	
PROYECTO 10 — JUSTICIA AUMENTADA Y ÉTICA																								
P10	10.1 AI Sandbox (Caja de Arena)	Coord. Plataforma Tecnológica - CISO	31/12/2028												31/12									
P10	Ética IA	Control Interno - CISO	31/12/2029																31/12					
P10	10.2 Anonimización	DBA - CISO	31/12/2029																31/12					
P10	10.3 Auditoría de algoritmos	Control Interno - CISO	30/09/2029															30/09						
P10	Prompts Filtros de	DBA - CISO	30/09/2030																				30/09	

7.13.2. Cronograma de Implementación del PESI

Para superar las vulnerabilidades estructurales identificadas, se ha diseñado un portafolio de acciones formuladas bajo estrictos criterios de especificidad técnica. Cada actividad está definida con un alcance unívoco, garantizando que su cumplimiento se mida a través de evidencias inmutables (ej. Logs de sistema, configuraciones activas) y no mediante apreciaciones subjetivas. A continuación, se presenta la matriz operativa del PESI para la presente vigencia:

Acción estratégica	Descripción técnica y entregable	Responsable	Fecha límite de ejecución	Entregable
1. Despliegue de Autenticación Multifactor (MFA)	Configurar y forzar el uso de MFA para el 100% de las cuentas activas (VPN, correo, aplicaciones misionales).	Jefatura OTIC / CISO	31 de diciembre de 2026	Reporte de cobertura del Directorio Activo.
2. Migración/Reactivación de Inteligencia Defensiva	Ejecutar el plan de contingencia para la renovación del licenciamiento EDR/XDR o la migración a herramientas nativas de protección de endpoints.	Jefatura OTIC	30 de mayo de 2028	Consola activa cubriendo los equipos críticos.
3. Simulacros de Recuperación ante Desastres	Realizar pruebas técnicas de restauración desde las copias inmutables (WORM) para el Sistema Misional.	Administrador de TI / CISO	30 de junio de 2029	Acta de cumplimiento de RTO (≤ 4 horas).

Acción estratégica	Descripción técnica y entregable	Responsable	Fecha límite de ejecución	Entregable
4. Modernización de Seguridad Física (A.7)	Publicar los pliegos de condiciones para la actualización del hardware obsoleto de control de acceso físico e integración con CCTV.	Secretaría General / Grupo de Contratos	30 de agosto de 2028	Contrato adjudicado y en ejecución.
5. Estandarización de Seguridad en Cadena de Suministro	Inclusión obligatoria del "Anexo Técnico de Seguridad" en todo nuevo contrato de tecnología y servicios.	Oficina Asesora Jurídica / OTIC	Ejecución Continua	100% de los nuevos contratos con cláusulas A.5.20.

8. Presupuesto

La viabilidad material de las estrategias de ciberresiliencia y la mitigación efectiva de los riesgos documentados en el presente Plan Estratégico de Seguridad de la Información (PESI) dependen ineludiblemente de una asignación presupuestal coherente, sostenida y alineada con la planeación financiera de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial (JPMP).

En este acápite se detallan los recursos financieros requeridos para la ejecución de los diez (10) proyectos estratégicos priorizados para el quinquenio 2026–2030. Los valores aquí referenciados se encuentran debidamente sustentados bajo los siguientes instrumentos de planeación:

- Vigencia 2026: Las asignaciones presupuestales de esta vigencia cuentan con la respectiva viabilidad técnica y se encuentran contempladas dentro del Plan Anual de Adquisiciones (PAA) de la entidad, garantizando la disponibilidad y el flujo de caja necesario para las contrataciones críticas inmediatas (ej. Mitigación de obsolescencia física y recuperación de capacidades EDR/XDR).
- Vigencias 2027–2030: Las proyecciones financieras para estos

años constituyen necesidades estructurales que han sido integradas en el Anteproyecto de Presupuesto institucional y en el Marco de Gasto de Mediano Plazo. Estos valores relacionan componentes tanto de los rubros de Inversión (para adquisición de nuevas capacidades y renovación tecnológica) como de Funcionamiento (para el licenciamiento recurrente, soporte técnico, y mantenimiento de los niveles de servicio – SLA).

A continuación, se presenta la matriz financiera con las cifras completas, expresadas en millones de pesos colombianos (COP), desagregadas por proyecto y vigencia:

Proyectos	Vigencias					
	2026	2027	2028	2029	2030	Total Cuatrienio
1.1 Gestión de Vulnerabilidades	$ 180.000.000					$ 180.000.000
1.2 Hardening (Endurecimiento superficie de ataque)		$ 144.000.000				$ 144.000.000
1.3 gestión de Parchado		$ 65.000.000				$ 65.000.000
1.4 Inteligencia de Amenazas – caza de amenazas.			$ 90.000.000			$ 90.000.000
1.5 Solución de Gestión Centralizada y Analítica			$ 45.000.000			$ 45.000.000
Total 1. Gestión de Vulnerabilidades	**$ 180.000.000**	**$ 209.000.000**	**$ 135.000.000**	**$ 0**	**$ 0**	**$ 524.000.000**
2.1 MFA / FIDO2 (Multifactor de Autenticación con estándar avanzado FIDO2)		$ 110.000.000				$ 110.000.000
2.2 PAM (Gestión de Accesos Privilegiados)		$ 220.000.000				$ 220.000.000
2.3 IAM Auto (La Gestión de identidad y acceso)			$ 96.000.000			$ 96.000.000
2.4 SASE (Borde del Servicio de Acceso Seguro) / ZTNA (acceso Zero Trust a la red)				$ 130.000.000		$ 130.000.000
2.5 Gobernanza Zero Trust				$ 35.000.000		$ 35.000.000
Total 2. Gestión de Identidad y Accesos	**$ 0**	**$ 330.000.000**	**$ 96.000.000**	**$ 165.000.000**	**$ 0**	**$ 591.000.000**
3.1 SIEM Hybrid (Administración de eventos e información de seguridad)		$ 320.000.000				$ 320.000.000
3.2 Servicio de SOC (Centro de Operaciones de Seguridad)			$ 480.000.000			$ 480.000.000
3.3 SOAR (Orquestación, Automatización y Respuesta de Seguridad)				$ 150.000.000		$ 150.000.000
3.4 Talento Interno Plataforma				$ 120.000.000		$ 120.000.000
3.5 Procesos - Playbooks			$ 60.000.000			$ 60.000.000
Total 3. Operaciones de Seguridad (SOC)	**$ 0**	**$ 320.000.000**	**$ 540.000.000**	**$ 270.000.000**	**$ 0**	**$ 1.130.000.000**
4.1 Detección y Respuesta de Endpoint Replacement.			$ 240.000.000			$ 240.000.000
4.2 Cuarentena Automática				$ 132.000.000		$ 132.000.000
4.3 NDR (Detección y Respuesta de Red)				$ 210.000.000		$ 210.000.000

Proyectos	Vigencias					
	2026	2027	2028	2029	2030	Total Cuatrienio
4.4 Estandarización Endurecimiento			$ 30.000.000			$ 30.000.000
Total 4. Detección y Respuesta (Endpoint/Red)	**$ 0**	**$ 0**	**$ 270.000.000**	**$ 342.000.000**	**$ 0**	**$ 612.000.000**
5.1 Designación CISO					$ 216.000.000	$ 216.000.000
5.2 Herramientas GRC					$ 160.000.000	$ 160.000.000
5.3 Tableros Dinámicos (Dashboard)		$ 96.000.000				$ 96.000.000
5.4 Actualizar Normatividad			$ 55.000.000			$ 55.000.000
Total 5. Gobernanza, Riesgo y Cumplimiento (GRC)	**$ 0**	**$ 96.000.000**	**$ 55.000.000**	**$ 0**	**$ 376.000.000**	**$ 527.000.000**
6.1 Gamificación SAT (Capacitación en concientización sobre seguridad)			$ 75.000.000			$ 75.000.000
6.2 Simulación de ataques de Phishing				$ 40.000.000		$ 40.000.000
6.3 Talleres funcionarios					$ 84.000.000	$ 84.000.000
6.4 Campaña					$ 35.000.000	$ 35.000.000
6.5 Medición					$ 25.000.000	$ 25.000.000
Total 6. Concientización y Capacitación	**$ 0**	**$ 0**	**$ 75.000.000**	**$ 40.000.000**	**$ 144.000.000**	**$ 259.000.000**
7.1 CSPM (Gestión de la Postura de Seguridad en la Nube)			$ 120.000.000			$ 120.000.000
7.2 WAF (Firewall de Aplicaciones Web)			$ 95.000.000			$ 95.000.000
7.3 Encriptación			$ 110.000.000			$ 110.000.000
7.4 Migración				$ 90.000.000		$ 90.000.000
7.5 Gobernanza Cloud				$ 30.000.000		$ 30.000.000
Total 7. Seguridad Cloud y Aplicaciones	**$ 0**	**$ 0**	**$ 325.000.000**	**$ 120.000.000**	**$ 0**	**$ 445.000.000**
8.1 Clasificación de Datos con IA			$ 210.000.000			$ 210.000.000
8.2 Data Loss Prevention (DLP)				$ 108.000.000		$ 108.000.000
8.3 Encriptación de datos				$ 85.000.000		$ 85.000.000
8.4 Anonimización de datos					$ 130.000.000	$ 130.000.000
8.5 Mapeo de Datos					$ 50.000.000	$ 50.000.000
Total 8. Seguridad y Privacidad de Datos	**$ 0**	**$ 0**	**$ 210.000.000**	**$ 193.000.000**	**$ 180.000.000**	**$ 583.000.000**
9.1 Infraestructura WORM (Write Once, Read Many				$ 450.000.000		$ 450.000.000
9.2 Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP).				$ 90.000.000		$ 90.000.000
9.3 Drills Failover (Simulacros anuales de caída total)				$ 80.000.000		$ 80.000.000
9.4 DRaaS (Recuperación ante Desastres como Servicio)					$ 180.000.000	$ 180.000.000
9.5 Actualización del DRP					$ 45.000.000	$ 45.000.000
Total 9. Continuidad y Recuperación (BCP/DRP)	**$ 0**	**$ 0**	**$ 0**	**$ 620.000.000**	**$ 225.000.000**	**$ 845.000.000**

Proyectos	Vigencias					
	2026	2027	2028	2029	2030	Total Cuatrienio
10.1 AI Sandbox			$ 280.000.000			$ 280.000.000
10.2 Anonimización de información IA				$ 144.000.000		$ 144.000.000
10.3 Auditoria de algoritmos				$ 95.000.000		$ 95.000.000
10.4 Ética IA				$ 40.000.000		$ 40.000.000
10.5 Prompts Filtros de Detención de Perdida				$ 60.000.000		$ 60.000.000
Total 10. Inteligencia Artificial y Ética	**$ 0**	**$ 0**	**$ 280.000.000**	**$ 339.000.000**	**$ 0**	**$ 619.000.000**
TOTAL GENERAL	**$ 180.000.000**	**$ 955.000.000**	**$ 1.986.000.000**	**$ 2.089.000.000**	**$ 925.000.000**	**$ 6.135.000.000**

Justificación de la Distribución Financiera

- Choque de Inversión Inicial (2026): El presupuesto de la primera vigencia evidencia una carga mayor orientada a estabilizar la infraestructura de protección activa (como la reactivación de licencias de la Proyecto 4) y subsanar las brechas críticas de control de acceso físico evidenciadas en el diagnóstico.

- Ciclos de Renovación Tecnológica (2029 - 2030): Se observan picos de inversión proyectados para los años 2029 y 2030 en proyectos como Almacenamiento Inmutable (Proyecto 2) y Arquitectura de Red (Proyecto 6), obedeciendo a la obsolescencia programada del hardware a adquirir en 2026 y a la necesidad estructural de actualizar los nodos de procesamiento primario del SPOA.

- Sostenibilidad del Modelo (Funcionamiento): Proyectos de naturaleza consultiva u operativa continua, como el CSIRT (Proyecto 5) y las Auditorías (Proyecto 8), reflejan un crecimiento incremental anualizado proyectado bajo el Índice de Precios al Consumidor (IPC), asegurando que el músculo de vigilancia institucional no pierda capacidad adquisitiva frente al mercado laboral y de servicios tecnológicos.

9. Seguimiento y medición del plan

Para garantizar la efectividad y la medición objetiva del Plan Estratégico de Seguridad de la Información (PESI), se validan los indicadores operativos y estratégicos definidos en las matrices de este documento, los cuales actúan como Indicadores Clave de Riesgo

(KRIs) y de Desempeño (KPIs). Se establece expresamente que el cargue, la gestión y el reporte de estos indicadores se realizará de manera exclusiva a través del proceso de Gestión TIC. Esta integración procedimental asegura que la medición del cumplimiento del PESI no sea un esfuerzo aislado, sino que se articule de forma orgánica con el mapa de procesos de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial (JPMP), permitiendo a la Alta Dirección evaluar con datos precisos el avance de los proyectos y el fortalecimiento del ecosistema tecnológico.

Para asegurar una visión unificada de la ciberresiliencia frente a los requerimientos del MSPI v5.0, los indicadores definidos para el seguimiento de este Plan han sido estructurados en coherencia y articulación con el Plan de Seguridad y Privacidad de la Información (PSPI) 2026-2027.

La periodicidad de la medición será de carácter mensual para el seguimiento operativo (a cargo del equipo de la OTIC y el CISO) y de carácter trimestral para la consolidación y presentación de avances estratégicos ante el Comité Institucional de Gestión y Desempeño.

Los responsables directos del cargue de información y validación de evidencias serán los líderes designados para cada proyecto dentro del proceso de Gestión TIC. Asimismo, toda la trazabilidad, incluyendo los soportes, reportes de vulnerabilidades y actas de cumplimiento, deberá registrarse obligatoriamente en la herramienta oficial de gestión y planeación de la entidad (plataforma Daruma o el sistema institucional equivalente), garantizando que el monitoreo sea verificable, oportuno y auditable por los entes de control interno y externo.

9.1. Indicadores

Con el propósito de medir el cumplimiento del Plan Estratégico de Seguridad de la Información (PESI), a continuación, se establecen los indicadores de desempeño y de efectividad de los controles de seguridad. Su cargue, gestión y monitoreo se realizarán de manera centralizada a través del proceso de Gestión TIC:

Nombre del indicador	Objetivo del indicador	Fórmula de cálculo y fuentes de información
Avance del cumplimiento del Plan de Seguridad Información	Mide el cumplimiento del Plan de Seguridad Información.	**Fórmula:** (Número de actividades ejecutadas / Número de actividades planeadas) x 100 **Fuente:** Plan de Seguridad y Privacidad de la Información.
Porcentaje de tratamiento de eventos relacionados en marco de seguridad y privacidad	Verificar la gestión y evolución del modelo de seguridad y privacidad de la información al interior de una entidad.	**Fórmula:** (Número de eventos altos o críticos de seguridad de la información tratados / Número total de eventos de seguridad de la información reportados) x 100. **Fuentes:**
Porcentaje de incidentes de seguridad tratados	Incidentes tratados con soluciones alternas o definitivas.	**Fórmula:** (Incidentes tratados con soluciones alternas o definitivas / Incidentes presentados que afectan la prestación de los servicios y/o el funcionamiento de los sistemas de información críticos registrados en la mesa de ayuda) x 100 **Fuentes:**
Porcentaje de Cumplimiento del Tiempo Objetivo de Recuperación (RTO)	Garantizar la restauración de sistemas críticos en < 12 horas ante contingencia o ciberataques destructivos.	**Fórmula:** (Número de sistemas críticos restaurados en menos de 12 horas / Número total de sistemas críticos afectados por la contingencia) x 100 **Fuentes:** Logs de Consola de Backup (Veeam/Azure), Actas de simulacro de desastre (DR Drill) firmadas, y registros de disponibilidad del SIEM/NMS.
Tasa de Cobertura de Autenticación Multifactor (MFA) en Accesos Críticos	Minimizar riesgos de suplantación de identidad asegurando el principio de Confianza Cero en accesos remotos y sistemas sensibles.	**Fórmula**: (Número de cuentas con acceso crítico que tienen MFA habilitado y activo / Número total de cuentas con acceso crítico) x 100 **Fuentes:** Exportación CSV de la Consola de Identidades (Microsoft Entra ID) y logs de conexión del Firewall/VPN con validación de segundo factor.
Cumplimiento del SLA de Remediación de Vulnerabilidades Críticas	Reducir ventana de exposición tecnológica mitigando vulnerabilidades críticas en un tiempo no mayor a 15 días.	**Fórmula**: (Número de vulnerabilidades críticas remediadas en 15 días o menos / Número total de vulnerabilidades críticas identificadas en el periodo) x 100 **Fuentes:** Reportes técnicos de escáner de vulnerabilidades (Nessus/Tenable), logs de despliegue de parches (WSUS/Endpoint Central) y matriz de excepciones del CISO.
Tiempo Medio de Contención de Incidentes Cibernéticos (MTTC)	Medir la agilidad del equipo de monitoreo para aislar y contener amenazas desde el momento de su detección inicial.	**Fórmula:** (Sumatoria del tiempo total empleado para contener los incidentes / Número total de incidentes de seguridad atendidos). Resultado expresado en horas o minutos.

Nombre del indicador	Objetivo del indicador	Fórmula de cálculo y fuentes de información
		Fuentes: Marcas de tiempo (timestamps) de la consola EDR/SIEM, registros de atención de la Mesa de Ayuda (ITSM) e informes post-incidente (IRCA).
Porcentaje de cumplimiento en la actualización documental del SGSI	Asegurar la transición y actualización de las políticas del SGSI de la norma 2013 a la 2022.	**Fórmula:** (Número de documentos y políticas del SGSI actualizados a la norma 2022 / Número total de documentos del SGSI requeridos para la transición) x 100 **Fuentes:** Actas de aprobación del Comité Institucional de Gestión y Desempeño, repositorio documental de la entidad.
Cobertura de capacitación y sensibilización en Ciberresiliencia	Evaluar el alcance de las campañas de culturización en seguridad de la información para servidores y contratistas.	**Fórmula:** (Número de servidores y contratistas que completaron la capacitación / Número total de servidores y contratistas objetivo de la entidad) x 100 **Fuentes:** Listados de asistencia (físicos/digitales) y reportes de la plataforma de la Escuela de Justicia Penal Militar.
Eficacia en el Tratamiento de Riesgos de Seguridad de la Información	Monitorear el progreso en la implementación de controles para los riesgos calificados como Altos y Críticos.	**Fórmula:** (Número de riesgos Altos y Críticos con controles mitigantes implementados / Número total de riesgos Altos y Críticos identificados) x 100 **Fuentes**: Matriz de riesgos de seguridad de la información institucional y reportes de seguimiento del CISO.
Cobertura de activos críticos bajo escaneo de vulnerabilidades	Garantizar que la totalidad de la infraestructura crítica (SPOA, bases de datos) sea evaluada técnicamente.	**Fórmula:** (Número de activos críticos escaneados en el periodo / Número total de activos críticos registrados en el inventario) x 100 **Fuentes:** Reportes de inventario de activos y logs de ejecución de la herramienta de escaneo (Nessus/Tenable).
Porcentaje de cumplimiento Cronograma Pruebas de Restauración	Asegurar la ejecución periódica de pruebas de restauración para validar la integridad de las copias de seguridad.	**Fórmula:** (Número de pruebas de restauración ejecutadas de acuerdo con el cronograma / Número de pruebas de restauración programadas) x 100 **Fuentes:** Cronograma anual de backups y actas/informes de restauración firmadas por el responsable de infraestructura.
Porcentaje de proveedores críticos con evaluación de seguridad vigente	Controlar el riesgo en la cadena de suministro de TI mediante auditoría de cumplimiento de seguridad a terceros.	**Fórmula:** (Número de proveedores tecnológicos críticos con evaluación o auditoría de seguridad vigente / Número total de proveedores tecnológicos críticos activos) x 100 **Fuentes:** Informes de supervisión de contratos y reportes de auditoría de cumplimiento de seguridad a terceros.

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Instancia de Aprobación**	**Descripción**
1	Xx/xx/2026	Comité Institucional de Gestión y Desempeño	Primer versión del documento.