Defensa Jurídica del Estado

# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**UNIDAD ADMINISTRATIVA ESPECIAL**
**AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO**
**ENERO DE 2026**

## TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

Alineados con el CONPES 3971/2019 y el Decreto 1008 de 2018 de Política de Gobierno Digital que tiene definido tres habilitadores transversales, dentro de los cuales está el de Seguridad y Privacidad de la Información, que incluye la adopción del Marco de Seguridad y Privacidad de la Información – MSPI del Estado Colombiano, como instrumento para la implementación de los lineamientos de seguridad de la información establecidos para sus procesos, tramites, servicios, sistemas de información, infraestructura y alineados con los requisitos del establecimiento para la estrategia de seguridad digital, de acuerdo con lo establecido en el artículo 5 de la resolución 500 de 2021, se estructura este documento que permite visualizar las actividades para preservar la confidencialidad, integridad y disponibilidad y privacidad de la información en la Agencia Nacional de Defensa Jurídica del Estado.

## 2. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para la vigencia 2026.

## 3. ALCANCE

Este plan va dirigido a todos los procesos de la Agencia Nacional de Defensa Jurídica del Estado, en concordancia con el alcance del Modelo de Seguridad y Privacidad de la Información.

## 4. DEFINICIONES Y ABREVIATURAS

**Acceso a la Información Pública:** Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

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

**Activo de Información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

**Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

**Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

**Ciberespacio:** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

**Confidencialidad:** Es la propiedad que garantiza que la información solo sea accesible para aquellas personas, entidades o procesos que están autorizados a acceder a ella. La confidencialidad protege la información sensible de accesos no autorizados, evitando su divulgación indebida.

**Control:** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

**Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

**Disponibilidad:** Es la propiedad que garantiza que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo necesitan. Esto implica que los sistemas deben estar operativos y accesibles de manera confiable, minimizando tiempos de inactividad o fallos.

**Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

**Integridad:** Es la propiedad que asegura que la información y sus métodos de procesamiento son completos y precisos, es decir, que no han sido alterados de manera no autorizada, ya sea accidental o intencionalmente. La integridad protege contra la modificación o destrucción de la información sin autorización.

**PETI:** Plan Estratégico de Tecnologías de la Información.

**Partes interesadas (Stakeholder):** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

**Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

**Sistema de Gestión de Seguridad de la Información SGSI:** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

**SIGI:** Es el Sistema Integrado de Gestión Institucional, que permite armonizar los procesos en búsqueda de una gestión eficiente, eficaz y trasparente, con el fin de aumentar la satisfacción de los clientes.[1]

**Vulnerabilidad**: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

## 5. RESPONSABILIDADES

El Responsable de Seguridad de la Información o en su ausencia el líder del proceso de Gestión de Tecnologías de la Información es el encargado de dar continuidad a las actividades descritas en este plan.

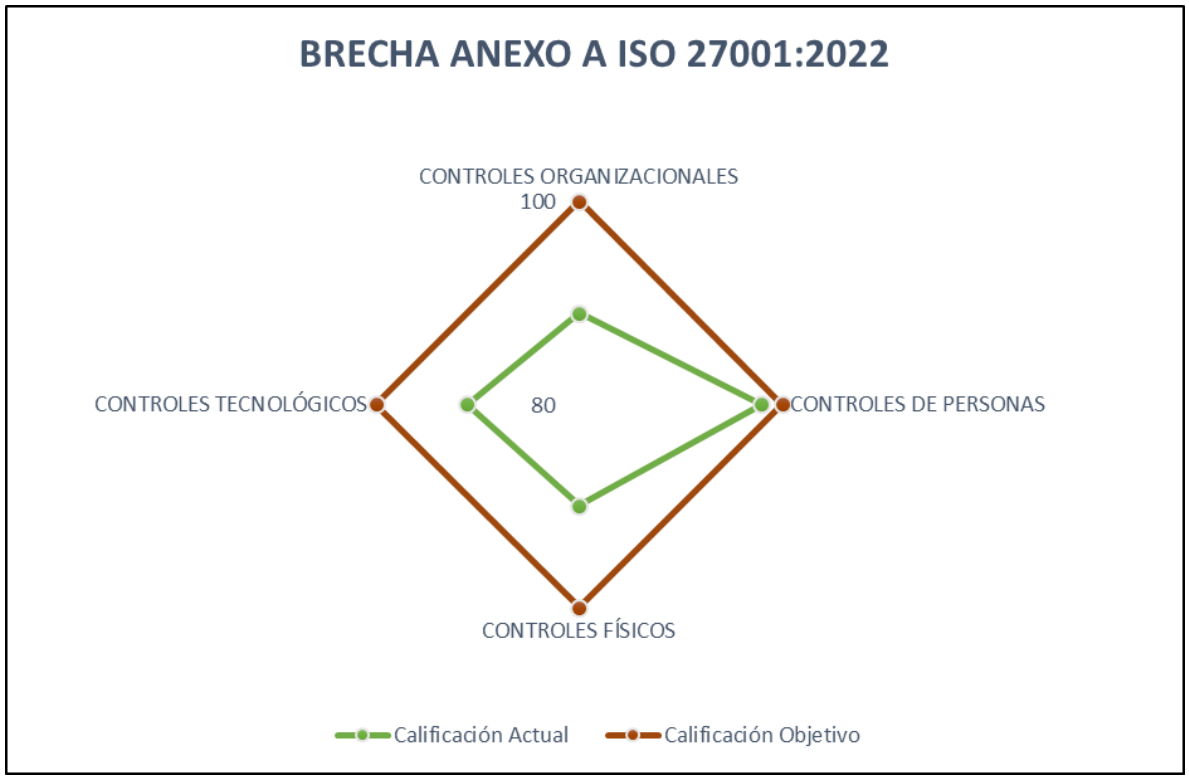
[1] chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://gobiernodigital.mintic.gov.co/692/articles-150517_Modelo_de_Seguridad_Privacidad.pdf

# 6. DESARROLLO

## 6.1 ESTADO ACTUAL DE LA ENTIDAD RESPECTRO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Entidad ha venido fortaleciendo el Modelo de Seguridad y Privacidad de la Información (MSPI) desde el año 2016, abordándolo desde un enfoque técnico y estratégico. En el ámbito técnico, se han adquirido herramientas para el monitoreo y correlación de eventos, así como la contratación de servicios para el análisis de vulnerabilidades, el monitoreo de seguridad y la revisión de marca. Desde el enfoque estratégico, se ha trabajado en la actualización de políticas de seguridad, la documentación procedimental, la verificación de activos y riesgos de seguridad, y la formalización del plan de continuidad del negocio y del plan de recuperación ante desastres (DRP). En agosto de 2025, el MINTIC publicó un nuevo instrumento de evaluación del MSPI alineado con la norma ISO 27001:2022, por lo que el presente autodiagnóstico se realiza utilizando este nuevo instrumento. A partir de este trabajo, se presentan los resultados del estado de implementación del MSPI según los indicadores definidos por MINTIC.

| No. | Evaluación de Efectividad de controles | | | |
|---|---|---|---|---|
| | DOMINIO | Calificación Actual | Calificación Objetivo | Nivel de Madurez |
| A.5 | CONTROLES ORGANIZACIONALES | 89 | 100 | **OPTIMIZADO** |
| A.6 | CONTROLES DE PERSONAS | 98 | 100 | **OPTIMIZADO** |
| A.7 | CONTROLES FÍSICOS | 90 | 100 | **OPTIMIZADO** |
| A.8 | CONTROLES TECNOLÓGICOS | 91 | 100 | **OPTIMIZADO** |
| **PROMEDIO EVALUACIÓN DE CONTROLES** | | **92** | **100** | **OPTIMIZADO** |




De acuerdo con el nuevo instrumento de evaluación del MSPI, las brechas identificadas para alinear el Modelo de Seguridad y Privacidad de la Información con la nueva versión se centran en fortalecer la gobernanza y la operatividad de los controles de seguridad. Entre las acciones previstas se encuentran la elaboración de un Manual de Seguridad, que establezca lineamientos claros para la gestión de la información, y la creación de un documento de contacto con las autoridades pertinentes.

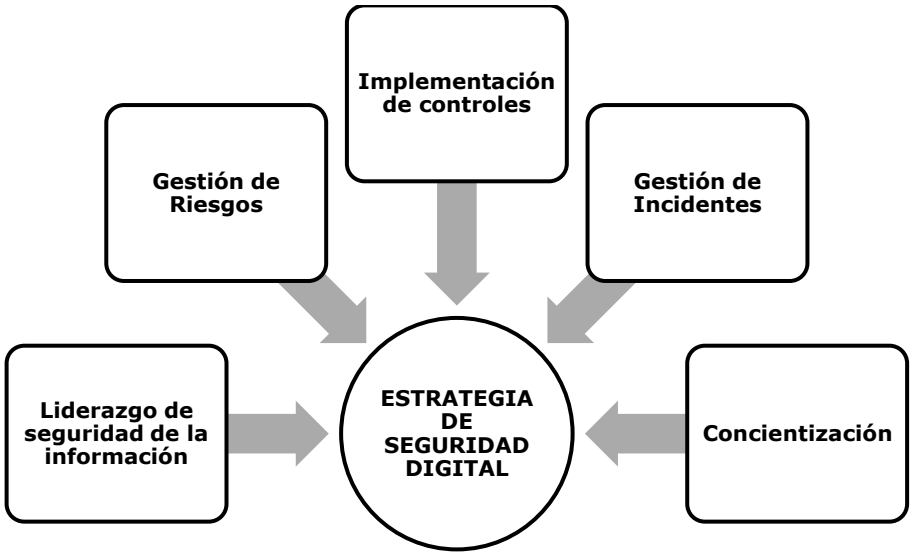
Adicionalmente, se contempla la verificación de los controles relacionados con la gestión de identidades, el seguimiento a los controles asociados con la Continuidad del Negocio, la evaluación de riesgos en protección de datos personales, la implementación de controles contra fuga de información, y la gestión de riesgos asociados a los servicios en la nube.

Estas acciones buscan garantizar que el MSPI esté completamente alineado con el nuevo instrumento de MINTIC y con la norma ISO 27001:2022, fortaleciendo la seguridad, continuidad y cumplimiento normativo de la Entidad.

## 6.2 ESTRATEGIA DE SEGURIDAD DIGITAL

La Agencia establece una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira en torno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes.

Por tal motivo, la Agencia define las siguientes 5 estrategias específicas, que permiten establecer en su conjunto una estrategia general de la seguridad digital:




**6.3**DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECIFICAS (EJES)[2]

| ESTRATEGIA / EJE | DESCRIPCIÓN/OBJETIVO |
|---|---|
| **Liderazgo de seguridad de la información** | Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información. |

[2] PLAN ESTRATÉGICO DE SEGURIDAD DE LA INFORMACIÓN (PESI)-MINTIC

| | |
|---|---|
| **Gestión de riesgos** | Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos. |
| **Concientización** | Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información. |
| **Implementación de controles** | Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos. |
| **Gestión de incidentes** | Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad. |

## **6.4**PORTAFOLIO DE PROYECTOS / ACTIVIDADES

| ESTRATEGIA / EJE | ACTIVIDADES | PRODUCTOS ESPERADOS |
|---|---|---|
| **Liderazgo de seguridad de la información** | **ACTIVIDAD 1**<br>Elaborar, aprobar y publicar el Plan de Seguridad y Privacidad de la Información vigencia 2026. | **ACTIVIDAD 1**<br>Plan de Seguridad y Privacidad de la Información elaborado, aprobado y publicado. |
| | **ACTIVIDAD 2:**<br>Realizar el seguimiento al Plan de Seguridad y Privacidad de la Información. | **ACTIVIDAD 2**<br>Informe sobre la ejecución del Plan de Seguridad y Privacidad de la Información documentado y publicado en DARUMA. |
| | **ACTIVIDAD 3:**<br>Revisar por parte de la Dirección los resultados del Plan del MSPI vigencia 2025. | **ACTIVIDAD 3**<br>Informe de resultados de la vigencia 2025 del MSPI ante el CIGD (Comité de Gestión de Desempeño Institucional. |
| | **ACTIVIDAD 4:**<br>Verificar y actualizar las Políticas de seguridad (Si aplica). | **ACTIVIDAD 4**<br>Manual de Políticas de Seguridad actualizado (si aplica). |
| | **ACTIVIDAD 5:**<br>Aprobar el Autodiagnóstico de Seguridad de la Información por parte del CIGD. | **ACTIVIDAD 5:**<br>Autodiagnóstico de Seguridad de la Información aprobado. |
| | **ACTIVIDAD 6:** | **ACTIVIDAD 6:** |

| | | |
|---|---|---|
| | Elaborar el Manual de Seguridad con los lineamientos para la gestión del MSPI. | Manual de Seguridad de la Información elaborado y formalizado. |
| | **ACTIVIDAD 7:**<br>Elaborar el documento de contactos que permita identificar las autoridades pertinentes en materia de seguridad y protección de la información. | **ACTIVIDAD 7:**<br>Documento elaborado y formalizado. |
| | **ACTIVIDAD 8:**<br>Actualizar los Activos de Información de la ANDJE. | **ACTIVIDAD 8:**<br>Matriz Activos e Información actualizada. |
| **Gestión de riesgos** | **ACTIVIDAD 1**<br>Elaborar, aprobar y publicar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2026. | **ACTIVIDAD 1**<br>Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2026 elaborado, aprobado y publicado. |
| | **ACTIVIDAD 2**<br>Realizar el seguimiento al Plan de Tratamiento de Riesgos de Seguridad (PTRSPI). | **ACTIVIDAD 2**<br>Informe sobre la ejecución del Plan de Riesgos de seguridad. (PTRSPI). |
| | **ACTIVIDAD 3**<br>Verificar el cumplimiento de los controles asociados a los riesgos de Seguridad de la Información en los procesos de la Entidad. | **ACTIVIDAD 3**<br>Publicar informe de seguimiento sobre la aplicación de los controles asociados a los riesgos en la plataforma DARUMA. |
| | **ACTIVIDAD 4**<br>Actualizar e identificar (cuando aplique) riesgos de seguridad de la información, gestión de identidades, continuidad del negocio y datos personales. | **ACTIVIDAD 4**<br>Publicación de riesgos para la vigencia 2026 en la plataforma DARUMA. |
| **Concientización** | **ACTIVIDAD 1**<br>Publicar campañas de sensibilización (Lunes Seguro). | **ACTIVIDAD 1**<br>36 campañas publicadas. |
| | **ACTIVIDAD 2**<br>Realizar Charlas sobre Seguridad de la Información. | **ACTIVIDAD 2**<br>3 charlas gestionadas. |
| | **ACTIVIDAD 3**<br>Desarrollar el Día de la Seguridad. | **ACTIVIDAD 3**<br>Informe sobre las actividades desarrolladas el Día de la Seguridad. |
| | **ACTIVIDAD 4**<br>Realizar la encuesta de apropiación de actividades relacionados con el Plan de Seguridad y Privacidad de la Información. | **ACTIVIDAD 4**<br>Resultado de la encuesta de medición del nivel de apropiación. |
| **Implementación de controles** | **ACTIVIDAD 1**<br>Realizar la contratación de servicios de ciberseguridad y plataforma de ciberseguridad. | **ACTIVIDAD 1**<br>Contratos de servicios de ciberseguridad y plataforma de ciberseguridad debidamente formalizados. |

| | | |
|---|---|---|
| | **ACTIVIDAD 2**<br>Desarrollar controles sobre Fuga de Información_1. | **ACTIVIDAD 2**<br>Informe sobre implementación DLP. |
| | **ACTIVIDAD 3**<br>Desarrollar controles sobre Fuga de Información_2. | **ACTIVIDAD 3**<br>Informe sobre el bloqueo de servicios externos de nube y correos. |
| | **ACTIVIDAD 4**<br>Desarrollar controles sobre controles Fuga de Información_3 | **ACTIVIDAD 4**<br>Informe sobre la activación módulo MTR (Respuesta a Amenazas Gestionada) herramienta Sophos. |
| | **ACTIVIDAD 5**<br>Desarrollar controles sobre Servicios de Nube | **ACTIVIDAD 5**<br>Informe sobre los controles documentados y operativos. |
| **Gestión de incidentes** | **ACTIVIDAD 1**<br>Gestionar los incidentes de seguridad de la información. | **ACTIVIDAD 1**<br>Registro del indicador de incidentes de seguridad en el sistema Daruma. |

### **6.5**DISTRIBUCIÓN PRESUPUESTAL

De acuerdo con la proyección del PAA las siguientes adquisiciones hacen parte de los controles para fortalecer el Modelo de Seguridad y Privacidad de la Información.

| OBJETO | VALOR ESTIMADO EN LA VIGENCIA ACTUAL |
|---|---|
| Profesional especializado apoyo al Oficial de Seguridad de la Agencia para asegurar y mantener el Modelo de Seguridad y Privacidad de la Información. | $132.000.000,00 |
| Contratos Servicios Ciberseguridad y Plataforma Ciberseguridad. | $2181.744.834,69 |
| Renovación del licenciamiento y soporte equipos de seguridad perimetral. | $120.906.894,37 |

Nota: El seguimiento de los proyectos que implican presupuesto es reportado en el seguimiento del plan de implementación y seguimiento del mapa de ruta de los proyectos e iniciativas de tecnología de información -PETI el cual esta soportado en PAA.

## 7. RIESGOS

| CLASIFICACIÓN DEL RIESGO | DESCRIPCIÓN DEL RIESGO | CAUSAS | CONSECUENCIAS | CONTROLES |
|---|---|---|---|---|

| | | | | |
|---|---|---|---|---|
| Estratégico | Incumplimiento de metas propuestas para los planes de acción institucional de TI. | Insuficiente de asignación de tiempos y recursos<br><br>Disminución de presupuesto | Incumplimientos legales y llamados de atención | Planificación y entrega del PAA a Financiera |

## 8. INDICADORES

(A) (Actividades ejecutadas / Actividades programadas) *100

## 9. CRONOGRAMA

| RESULTADO ESPERADO | PESO (%) | RESULTADOS / ENTREGABLES INTERMEDIOS | PESO (%) | RESPONSABLE | EJECUCIÓN | |
|---|---|---|---|---|---|---|
| | | | | | Fecha Inicio | Fecha Final |
| Elaborar, aprobar y publicar el Plan de Seguridad y Privacidad de la Información vigencia 2026. | 4,50% | Plan de Seguridad y Privacidad de la Información elaborado, aprobado y publicado. | 100,00% | Oficial seguridad de la Información | 1-ene-26 | 30-ene-26 |
| Realizar el seguimiento al Plan de Seguridad y Privacidad de la Información. | 5,50% | Informe sobre la ejecución del Plan de Seguridad y Privacidad de la Información documentado y publicado en DARUMA. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Revisar por parte de la Dirección los resultados del Plan del MSPI vigencia 2025. | 2,00% | Informe de resultados de la vigencia 2025 del MSPI ante el CIGD (Comité de Gestión de Desempeño Institucional. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 30-may-26 |
| Verificar y actualizar las Políticas de seguridad (Si aplica) | 4,00% | Manual de Políticas de Seguridad actualizado (si aplica). | 100,00% | Oficial seguridad de la Información | 1-mar-26 | 30-abr-26 |
| Aprobar el Autodiagnóstico de Seguridad de la Información por parte del CIGD. | 4,00% | Autodiagnóstico de Seguridad de la Información aprobado. | 100,00% | Oficial seguridad de la Información | 1-ago-26 | 30-ago-26 |
| Elaborar el Manual de Seguridad con los lineamientos | 6,50% | Manual de Seguridad de la Información | 100,00% | Oficial seguridad de la Información | 1-mar-26 | 30-ago-26 |

| | | | | | | |
|---|---|---|---|---|---|---|
| para la gestión del MSPI. | | elaborado y formalizado. | | | | |
| Elaborar el documento de contactos que permita identificar las autoridades pertinentes en materia de seguridad y protección de la información. | 2,00% | Documento elaborado y formalizado. | 100,00% | Oficial seguridad de la Información | 1-mar-26 | 30-jul-26 |
| Actualizar los Activos de Información de la ANDJE. | 5,50% | Matriz Activos e Información actualizada. | 100,00% | Oficial seguridad de la Información | 1-sep-26 | 30-nov-26 |
| Elaborar, aprobar y publicar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2026. | 4,00% | Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información vigencia 2026 elaborado, aprobado y publicado. | 100,00% | Oficial seguridad de la Información | 1-ene-26 | 30-ene-26 |
| Realizar el seguimiento al Plan de Tratamiento de Riesgos de Seguridad (PTRSPI) | 5,00% | Informe sobre la ejecución del Plan de Riesgos de seguridad. (PTRSPI). | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Verificar el cumplimiento de los controles asociados a los riesgos de Seguridad de la Información en los procesos de la Entidad. | 5,00% | Publicar informe de seguimiento sobre la aplicación de los controles asociados a los riesgos en la plataforma DARUMA. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Actualizar e identificar (cuando aplique) riesgos de seguridad de la información, gestión de identidades, continuidad del | 5,00% | Publicación de riesgos para la vigencia 2026 en la plataforma DARUMA. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 30-may-26 |

| | | | | | | |
|---|---|---|---|---|---|---|
| negocio y datos personales. | | | | | | |
| Publicar campañas de sensibilización (Lunes Seguro). | 5,00% | 36 campañas publicadas. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Realizar Charlas sobre Seguridad de la Información | 4,50% | 3 charlas gestionadas. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Desarrollar el Día de la Seguridad. | 6,50% | Informe sobre las actividades desarrolladas el Día de la Seguridad. | 100,00% | Oficial seguridad de la Información | 1-jul-26 | 30-sep-26 |
| Realizar la encuesta de apropiación de actividades relacionados con el Plan de Seguridad y Privacidad de la Información. | 4,50% | Resultado de la encuesta de medición del nivel de apropiación. | 100,00% | Oficial seguridad de la Información | 1-oct-26 | 31-oct-26 |
| Realizar la contratación de servicios de ciberseguridad y plataforma de ciberseguridad. | 8,00% | Contratos de servicios de ciberseguridad y plataforma de ciberseguridad debidamente formalizados. | 100,00% | Oficial seguridad de la Información | 1-jul-26 | 30-nov-26 |
| Desarrollar controles sobre Fuga de Información_1. | 3,00% | Informe sobre implementación DLP. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Desarrollar controles sobre Fuga de Información_2. | 3,00% | Informe sobre el bloqueo de servicios externos de nube y correos. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Desarrollar controles sobre controles Fuga de Información_3 | 3,00% | Informe sobre la activación módulo MTR (Respuesta a Amenazas Gestionada) herramienta Sophos. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |
| Desarrollar controles sobre Servicios de Nube | 4,00% | Informe sobre los controles documentados y operativos. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Gestionar los incidentes de seguridad de la información. | 5,50% | Registro del indicador de incidentes de seguridad en el sistema Daruma. | 100,00% | Oficial seguridad de la Información | 1-feb-26 | 15-dic-26 |

| Elaboró | Revisó | Aprobó |
|---|---|---|
| **Fredy Zea Rodriguez**<br>Contratista Gestión de Tecnologías de la Información | **Diana Betty Clavijo Vargas**<br>Jefa Gestión de Tecnologías de la Información<br>**Carlos Adolfo Rangel**<br>Gestor Gestión de Tecnologías de la Información | Comité Institucional de Gestión y Desempeño - CIGD |