Plan de Seguridad y Privacidad de la Información 2024

JUSTICIA PENAL MILITAR Y POLICIAL

Oficina de Tecnologías de la Información y de las comunicaciones

Abril 2024

Contenido

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información se diseñó con el objetivo de proteger y garantizar la integridad, confidencialidad y disponibilidad de la información, teniendo en cuenta las mejores prácticas y estándares de seguridad en el entorno digital y físico. En este sentido, se tomó en cuenta los lineamientos y recomendaciones del Manual de Política de Gobierno Digital y del Modelo de Privacidad y Seguridad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones[1]

El plan se basa en el ciclo PHVA (Planificar-Hacer-Verificar-Actuar) para garantizar la continuidad del plan y asegurar que las medidas implementadas sean eficaces[2]. Entre las actividades del plan, se encuentra la identificación de los activos de información y los riesgos asociados, la implementación de controles de seguridad para mitigar posibles afectaciones y la gestión de la continuidad tecnológica para garantizar la disponibilidad de la información en caso de eventos imprevistos.

El propósito del Plan de Seguridad y Privacidad de la Información es crear un entorno de uso confiable y seguro para los usuarios de la información, tanto en el ámbito digital como físico.

Este plan se define teniendo en cuenta el contexto, las necesidades de la organización, las buenas prácticas y la normatividad vigente como: la NTC (Norma Técnica Colombiana) ISO 27001:2022, ISO 27701:2020, ISO 22301:2019, Lineamientos Para La Elaboración del Plan de Seguridad de la Información (PESI) y el Decreto 767 de 2022 "Por el cual se establecen los lineamientos generales de la política de Gobierno Digital" y se subroga "el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones", la Resolución 1519 de 2020 "Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos" y la Resolución 500 de 2021 "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" dentro del cual se establecen para las entidades del estado los Habilitadores Transversales: Seguridad de la Información, Arquitectura de TI y Servicios Ciudadanos Digitales, y los Lineamientos para la Elaboración del Plan de Seguridad y Privacidad de la Información del MINTIC.

[1] https://gobiernodigital.mintic.gov.co/portal/Manual-de-Gobierno-Digital/
[2] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

2. OBJETIVO GENERAL

Asegurar la integridad, confidencialidad, disponibilidad y privacidad de la información institucional mediante la definición e implementación de las acciones necesarias que permitan aumentar el nivel de madurez de seguridad y privacidad de la información en la Justicia Penal Militar y Policial, teniendo en cuenta las estrategias de Gobierno Digital, el MIPG, los requerimientos de la Entidad, las disposiciones legales y las buenas prácticas vigentes en la materia.

2.1 Objetivos específicos

1. Identificar y evaluar los riesgos de seguridad y privacidad de la información.
2. Establecer políticas y procedimientos de seguridad de la información.
3. Implementar tecnologías de seguridad adecuadas.
4. Capacitar al personal en prácticas de seguridad y privacidad de la información.
5. Realizar revisiones periódicas de los controles de seguridad y privacidad implementados.

3. ALCANCE

El alcance del presente documento abarca los siguientes temas: Marco Normativo, Responsables, Definiciones, Desarrollo del Plan, Presupuesto, Seguimiento y Medición del Plan e Indicadores. En cuanto a los procesos se cubren los siguientes procesos (Actualizar del 1 al 6 y Realizar desde ceros del 7 al 11):

1. Direccionamiento estratégico a cargo del Jefe Oficina Asesora de Planeación.
2. El Mapa Judicial a cargo del Director General y Jefe Oficina Asesora de Planeación.
3. Gestión TIC a cargo del Jefe Oficina de las Tics.
4. Fortalecimiento de las capacidades de la Jurisdicción Penal Militar y Policial a cargo del Director General.
5. Selección e Incorporación a cargo de la Dirección General/ Secretaria General,
6. Gestión Jurídica a cargo de la oficina jurídica.
7. Gestión Documental a cargo del Coordinador Grupo Administrativo,
8. Control Disciplinario a cargo de la Secretaria General,
9. Adquisición de Bienes y Servicios a cargo de la Secretaria General,
10. Gestión de la Formación del Talento Humano a cargo del Director de la Escuela de JPMP,
11. Control Interno a cargo del líder de la oficina.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

Este Plan aplica a toda la Justicia Penal Militar y Policial, jueces, fiscales, judicantes, tribunal y fiscalía; asimismo, está dirigida a los servidores públicos, funcionarios, contratistas, personal de apoyo, policía judicial en encargo, y terceros de LA JPMP, sus grupos de valor e interés y la ciudadanía en general respecto a la seguridad de la información, en cumplimiento de las disposiciones legales vigentes.

4. MARCO NORMATIVO

El marco normativo que se debe tener en cuenta para el Plan de seguridad se lista a continuación:

Tipo de norma	Número	Año	Descripción - epígrafe
Ley	2294	2023	Plan nacional de Desarrollo 2022-2026 "Colombia, Potencia Mundial de la Vida"
Ley	1915	2018	Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta ley a los intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor.
Ley	1712	2014	Regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantías del derecho y las excepciones a la publicidad de la información. Toda persona puede conocer sobre la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. El acceso a la información solamente podrá ser restringido excepcionalmente.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

Tipo de norma	Número	Año	Descripción - epígrafe
Ley	1581	2012	Por la cual se dictan disposiciones generales para la protección de datos. Esta ley busca proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o supresión por parte de entidades de naturaleza pública y privada, sin embargo, a los datos financieros se les continúa aplicando la Ley 1266 de 2008, excepto los principios.
Ley	1273	2009	Artículo 1°. Adicionase el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos", del siguiente tenor: CAPÍTULO PRIMERO de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos y CAPÍTULO SEGUNDO de los atentados informáticos y otras infracciones.
Ley	1266	2008	Artículo 1°. Objeto. La presente Ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos, y los demás derechos, libertades y garantías constitucionales relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la Constitución Política, así como el derecho a la información establecido en el artículo 20 de la Constitución Política, particularmente en relación con la información financiera y crediticia, comercial, de servicios y la proveniente de terceros países.
Ley	1221	2008	ARTÍCULO 3o. política pública de fomento al teletrabajo. Parágrafo 1o. Teletrabajo para población vulnerable.
Ley	527	1999	reglamentación del Uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y entidades de certificación

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

Tipo de norma	Número	Año	Descripción - epígrafe
Decreto	767	2022	Establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual propende por la transformación digital pública. Con esta política pública se busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública y el Estado en general, a través del uso y aprovechamiento de las TIC. Hace parte del Modelo Integrado de Planeación y Gestión - MIPG y se integra con las políticas de Gestión y Desempeño Institucional.
Decreto	612	2018	Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año.
Decreto	415	2016	Lineamientos para el fortalecimiento institucional y ejecución de los planes, programas y proyectos de tecnologías y sistemas de información en la respectiva entidad.
Decreto	1078	2015	Artículo 2.2.9.1.2.1. Componentes. Los fundamentos de la estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda de Gobierno En Línea. 4. Seguridad y privacidad de la Información.
Decreto	2573	2014	Artículo 5. Componentes. Los fundamentos de la estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda de Gobierno En Línea. 4. Seguridad y privacidad de la Información.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

Tipo de norma	Número	Año	Descripción - epígrafe
Decreto	886	2014	Que el artículo 25 de la Ley 1581 de 2012 crea el Registro Nacional de Bases de Datos, el cual se define como el directorio público de las bases de datos personales sujetas a Tratamiento que operan en el país, administrado por la Superintendencia de Industria y Comercio y de libre consulta para los ciudadanos. Gobierno Nacional reglamentará la información mínima que debe contener el registro, así como los términos y condiciones de inscripción a los que estarán sujetos los responsables del Tratamiento.
Decreto	1377	2013	Artículo 1°. Objeto. El presente Decreto tiene como objeto reglamentar parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Resolución	500	2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
Resolución	1519	2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos, materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
Conpes	3995	2020	El objetivo es aumentar la generación de valor social y económico a través de la transformación digital del sector público y del sector privado, para que Colombia pueda aprovechar las oportunidades y enfrentar los retos relacionados con la 4RI. Dicha política, además de ser el marco para temas digitales en el país, establece dentro de sus acciones, la formulación de una política pública sobre ciberseguridad para mejorar las capacidades del país al respecto.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

Tipo de norma	Número	Año	Descripción - epígrafe
ISO	31000	2018	**Establecer el contexto:** Identificar y comprender el entorno en el que opera la organización, incluyendo su misión, objetivos, partes interesadas relevantes y el alcance de la gestión del riesgo. **Identificar los riesgos:** Identificar los riesgos potenciales que podrían afectar a la organización en la consecución de sus objetivos. Esto implica analizar tanto los riesgos internos como los externos, teniendo en cuenta los diferentes contextos operativos. **Analizar y evaluar los riesgos:** Evaluar la probabilidad de ocurrencia y el impacto de los riesgos identificados. Realizar un análisis de riesgos para determinar su nivel de prioridad y establecer criterios para la toma de decisiones. **Tratar los riesgos:** Desarrollar e implementar estrategias y planes de acción para tratar los riesgos identificados. Esto puede implicar la mitigación de los riesgos, la transferencia de los riesgos a terceros, la aceptación de los riesgos o la implementación de medidas de contingencia. **Comunicación y consulta:** Establecer canales de comunicación efectivos para compartir información sobre los riesgos y consultar con las partes interesadas relevantes. La comunicación clara y transparente ayuda a mejorar la comprensión y apoyo a la gestión del riesgo en toda la organización. **Monitoreo y revisión:** Establecer un proceso continuo de monitoreo y revisión de los riesgos y las medidas de gestión implementadas. Esto permite asegurar que las estrategias de gestión del riesgo sean efectivas y se ajusten a los cambios en el entorno operativo.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

Tipo de norma	Número	Año	Descripción - epígrafe
ISO/IEC	27001		Seleccionar e implementar los controles de seguridad de la información que sean relevantes y necesarios para abordar los riesgos identificados en el contexto de la organización. Esto implica realizar una evaluación de riesgos, identificar los controles adecuados y establecer un plan de implementación.

5. RESPONSABLES

1. Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones: Es responsable de la gestión del plan de seguridad de la información y de asesorar al Director General en la formulación, actualización e implementación.
2. Coordinador del Grupo de Plataforma Tecnológica: Apoya el plan en lo relacionado con las funciones de la Plataforma Tecnológica de LA UNIDAD.
3. Coordinador del Grupo de Redes y Telecomunicaciones: Apoya el plan en lo relacionado con las funciones de Redes y Comunicaciones de la UNIDAD.
4. Coordinador del Grupo de Sistemas de Información: Apoya el plan en lo relacionado con los Sistemas de Información de LA UNIDAD.

6. DEFINICIONES

Para una mejor comprensión del presente documento se toman como referencia los presentes términos y definiciones establecidos en la Norma ISO 27000:

- **Aceptación del riesgo**: Decisión informada de asumir un riesgo concreto.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos relacionado con el tratamiento de datos. El activo representa los datos que tienen valor para los procesos de la entidad, pueden ser un documento físico, un archivo guardado en un servidor, un aplicativo o cualquier elemento que permita almacenar información calificada o reservada de la SNS.
- **Amenaza**: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o activo de información.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

- **Análisis de riesgos**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.
- **Análisis de riesgos cualitativo**: Análisis de riesgos en el que se usa algún tipo de escalas de valoración para situar la criticidad del impacto y la probabilidad de ocurrencia.
- **Análisis de riesgos cuantitativo**: Análisis de riesgos en función de las pérdidas financieras que causaría el impacto.
- **Autenticación:** Provisión de una garantía de que una característica afirmada por una entidad es correcta.
- **Autenticidad**: Propiedad de que una entidad es lo que afirma ser.
- **CID:** Acrónimo español de confidencialidad, integridad y disponibilidad, las dimensiones básicas de la seguridad de la información.
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

  La información debe ser accedida solo por aquellas personas que lo requieran como una necesidad legítima para la realización de sus funciones. La revelación no autorizada de la información calificada de acuerdo con un nivel de confidencialidad alta implica un grave impacto en la Superintendencia Nacional de Salud, en términos económicos, de su imagen y ante sus clientes.
- **Controles Preventivos:** actúan sobre la causa de los riesgos, con el fin de disminuir su probabilidad de ocurrencia y constituyen la primera línea de defensa contra ellos; también actúan para disminuir la acción de los agentes generadores de los riesgos.
- **Controles Detectivos:** se diseñan para descubrir un evento, irregularidad o un resultado no previsto; alertan sobre la presencia de los riesgos y permiten tomar medidas inmediatas; pueden ser manuales o computarizados. Generalmente, sirven para supervisar la ejecución del proceso y se usan para verificar la eficacia de los controles preventivos. Ofrecen la segunda barrera de seguridad frente a los riesgos, pueden informar y registrar la ocurrencia de los hechos no deseados, accionar alarmas, bloquear la operación de un sistema, monitorear, o alertar a los servidores públicos.
- **CIO:** En CIO (Chief Information Officer) de una empresa es la persona que tiene el cargo de director de IT (director de Tecnologías de la Información). Un CIO es un ejecutivo responsable del desarrollo,

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

implementación y operación de la política de tecnología de la información de una empresa. EL director de IT supervisa toda la infraestructura de los sistemas de información dentro de la organización y es responsable de establecer los estándares de información para facilitar el control de la gestión de todos los recursos corporativos.

- **Controles de Protección:** se aplican para neutralizar los efectos de los eventos no deseables y el alcance de los daños que pueden producir con el fin de minimizarlos o eliminarlos; estos pueden ser Activos, cuando requieren para su funcionamiento de la actuación del servidor público, bien en su activación o en su operación o Pasivos, si no la requieren. Son más costosos que los preventivos y requieren refuerzo en capacitación.
- **Controles Correctivos:** permiten el restablecimiento de la actividad después de ser detectado un evento no deseable y la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan y permiten mejorar las deficiencias; por lo general actúan con los controles detectivos, implican reprocesos y son más costosos porque actúan cuando ya se han presentado hechos que implican pérdidas para la entidad. La mayoría son de tipo administrativo y requieren políticas o procedimientos para su ejecución
- **Control disuasivo**: Control que reduce la posibilidad de materialización de una amenaza, p. ej., por medio de avisos o de medidas que llevan al atacante a desistir de su intención.
- **Declaración de aplicabilidad**: Documento que enumera los controles aplicados por el SSI -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.
- **Desastre**: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una durante el tiempo suficiente como para verse la misma afectada de manera significativa.
- **Directiva o directriz**: Una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.
- **Disponibilidad:** Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

- **Estimación de riesgos**: Proceso de comparar los resultados del análisis de riesgos con los criterios de riesgo para determinar si el riesgo y/o su magnitud es aceptable o tolerable.
- **Evaluación de riesgos**: Proceso global de identificación, análisis y estimación de riesgos.
- **Gestión de claves**: Controles referidos a la gestión de claves criptográficas.
- **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.
- **Gestión de riesgos**: Actividades coordinadas para dirigir y controlar una con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- **Identificación de riesgos**: Proceso de encontrar, reconocer y describir riesgos.
- **IEC:** También conocida por su sigla en inglés IEC (International Electrotechnical Commission), es una organización de normalización en los campos: eléctrico, electrónico y tecnologías relacionadas.
- **Impacto:** El coste para la empresa de un incidente -de la escala que sea-, que puede o no ser medido en términos estrictamente financieros -p. ej., pérdida de reputación, implicaciones legales, etc.
- **Incidente de seguridad de la información**: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Integridad**: Propiedad de la información relativa a su exactitud y completitud.
- **Inventario de activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SSI, que tengan valor para y necesiten, por tanto, ser protegidos de potenciales riesgos.
- **ISO/IEC 27001**: Norma que establece los requisitos para un sistema de gestión de la seguridad de la información (SSI). Primera publicación en 2005; segunda edición en 2022. Es la norma en base a la cual se certifican los SSI a nivel mundial.
- **No conformidad**: Incumplimiento de un requisito.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

- **No repudio**: Según [CCN-STIC-405:2006]: El no repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Según [OSI ISO-7498-2]: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).
- **MSPI:** Modelo de Seguridad y Privacidad de Información
- **Objetivo de seguridad de la información**: Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad determinada.
- **Parte interesada:** Persona u área que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de continuidad del negocio**: Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Recursos de tratamiento de información**: Cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizadas para su alojamiento.
- **Seguridad de la información**: Preservación de la confidencialidad, integridad y disponibilidad de la información.
- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.
- **Trazabilidad**: Según [CESID:1997]: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

7. DESARROLLO DEL PLAN

7.1 Mapa de ruta

A continuación, se describen las acciones a desarrollar durante la vigencia 2024:

No	Actividad	Inicio	Fin	Responsable	Producto
1. Nivel de madurez del MSPI					
1.1	Revisión y actualización del Análisis del nivel de madurez actual del MSPI de Unidad	Junio	Julio	Líderes de los procesos de Direccionamiento estratégico Jefe Oficina Asesora de Planeación, el Mapa Judicial, Director General y Jefe Oficina Asesora de Planeación, gestión TIC Jefe Oficina de las Tics, Fortalecimiento de las capacidades de la Jurisdicción Penal Militar y Policial Director General, Selección e Incorporación Dirección General / Secretaria General	Instrumento de Evaluación del MSPI actualizado y ampliado a once (11) procesos, Documento del Resultado de análisis de brechas
1.2	Actualización de la metodología de gestión integrada de riesgos de seguridad de la información	Julio	Agosto	Oficina Asesora de Planeación, Oficina de Control Interno de Gestión y Oficina de Tecnologías de la información y las Comunicaciones	Documento de metodología de gestión integrada de riesgos de seguridad de la información de la Unidad actualizada Informe de evaluación de riesgos de seguridad de la información
2. Sistema de gestión de seguridad y privacidad de la información					
2.1	Diligenciamiento de la herramienta "Instrumento Evaluación MSPI" para determinar el estado del SGSI al final del ejercicio en que se entrega el sistema	Noviembre	Diciembre	Todas las áreas y acompañamiento de Oficina de Tecnologías de la información y las Comunicaciones	Instrumento Evaluación MSPI, diligenciado en la etapa final del SGSI

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

No	Actividad	Inicio	Fin	Responsable	Producto
2.2	*Aplicación de la metodología de gestión del riesgo de seguridad y privacidad de la información y riesgos de ciberseguridad de la Unidad*	*Noviembre*	*Diciembre*	*Oficina de Tecnologías de la información y las Comunicaciones*	*Resultado de la identificación, clasificación y valoración de activos de información para los once (11) incluyendo adicionalmente Gestión Documental Coordinador Grupo Administrativo, Control Disciplinario Secretaria General, Adquisición de Bienes y Servicios Secretaria General, Gestión de la Formación del Talento Humano Director de la Escuela de JPMP, Control interno líder de la oficina.* *Plan de seguridad de la información.*
3. Concienciación y Sensibilización en Seguridad y Privacidad de la Información					
3.1	Definición del Plan de Concienciación en Seguridad y Privacidad	Septiembre	Octubre	Oficina de Tecnologías de la Información y las Comunicaciones	Documento con el informe de resultados del plan de comunicación, sensibilización y capacitación

8. PRESUPUESTO

Los recursos para este plan provienen del Proyecto de Inversión ***"Fortalecimiento de las capacidades administrativas, de gestión y de infraestructura tecnológica de la Justicia Penal Militar y Policial"***, en lo que respecta a la actividad establecida para la vigencia 2024 en el componente de Tecnología, así:

Detalle	2024
Desarrollar e implementar el modelo de seguridad y privacidad de la información (MSPI)	$350.000.000

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

9. SEGUIMIENTO Y MEDICIÓN DEL PLAN

9.1 Indicadores

Los indicadores del Plan son medidas o métricas que permiten evaluar y monitorear el desempeño del plan y los controles implementados para proteger la información, a continuación, se presentan los contemplados para el presente plan:

1. Índice de incidentes de seguridad: Mide la cantidad y la gravedad de los incidentes de seguridad de la información, como violaciones de datos, intrusiones o ataques informáticos. Puede incluir la frecuencia de los incidentes, el tiempo de respuesta para abordarlos y su impacto en la organización.
2. Índice de cumplimiento: Evalúa el grado en que la organización cumple con los requisitos de seguridad de la información establecidos por normas, leyes o regulaciones específicas. Puede medir el cumplimiento de políticas, controles, auditorías o evaluaciones internas y externas.
3. Tiempo de recuperación de incidentes: Mide el tiempo necesario para recuperarse de un incidente de seguridad de la información. Este indicador puede medir el tiempo desde la detección hasta la resolución completa del incidente, incluyendo la restauración de servicios, la reparación de sistemas afectados y la mitigación de riesgos.
4. Índice de conciencia y capacitación: Evalúa el nivel de conocimiento y comprensión de los empleados sobre las prácticas de seguridad de la información. Puede incluir la participación en programas de capacitación, el resultado de pruebas de conocimiento o encuestas de percepción de seguridad.
5. Índice de disponibilidad de servicios: Mide la disponibilidad y el rendimiento de los servicios de información críticos para la organización. Puede incluir el tiempo de inactividad planificado y no planificado, la capacidad de recuperación ante desastres y el cumplimiento de los acuerdos de nivel de servicio (SLA).
6. Cumplimiento del plan de seguridad y privacidad de la información: Mide las actividades planeadas comparadas con las actividades ejecutadas del plan.

Indicador	Fórmula de cálculo
Índice de incidentes de seguridad	Número de incidentes / período de tiempo

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023

Indicador	Fórmula de cálculo
Índice de cumplimiento	(Cumplimiento alcanzado / Cumplimiento objetivo) x 100%
Tiempo de recuperación de incidentes	Tiempo total de recuperación de incidentes
Índice de conciencia y capacitación	(Número de funcionarios capacitados / Total de funcionarios) x 100%
Índice de disponibilidad de servicios	(Tiempo de disponibilidad / Tiempo total) x 100%
Cumplimiento del plan	(Actividades ejecutadas/actividades programadas) x 100%

CONTROL DE CAMBIOS			
Versión	**Fecha**	**Instancia de Aprobación**	**Descripción**
01	29/08/2023	Comité Institucional de Gestión y Desempeño.	Formulación y Aprobación del Plan de Seguridad y Privacidad de la Información 2023. Sesión 06 de 2022
02	29/04/2024	Comité Institucional de Gestión y Desempeño.	Actualización del Plan de Seguridad y Privacidad de la Información 2024.

Unidad Administrativa Especial de la Justicia Penal Militar y Policial
Carrera 46 No. 20 C - 01 (Puente Aranda)
Cantón Militar Occidental "Coronel Francisco José de Caldas", Bogotá D.C., Colombia
PBX (57-601) 5169563 Ext. 1023