



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

1. INTRODUCCIÓN:

La **JUSTICIA PENAL MILITAR Y POLICIAL (JPMP)** reconoce la importancia de gestionar la seguridad de la información de manera efectiva. Por lo tanto, se ha comprometido con la implementación del "Modelo de Seguridad y Privacidad de la Información", teniendo en cuenta la resolución 000009 de 2024 donde se establece su misión: *"La Justicia Penal Militar y Policial tiene como misión investigar y juzgar las conductas punibles cometidas por los miembros de la Fuerza Pública en servicio activo y en relación con el mismo servicio, con autonomía, independencia, transparencia, legitimidad y efectividad, apoyada en la organización, funcionamiento y administración de procesos oportunos, con un talento humano íntegro"* y el objetivo estratégico 10. que establece: " 10.

Implementar sistemas de información, herramientas logísticas y tecnológicas que simplifiquen y agilicen los procesos en el marco de una cultura digital.", por lo anterior, en el presente documento definirá la Política de Seguridad de la Información de la Entidad con el fin de establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos en estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad sobre el manejo de los activos de información de la Entidad.

Lo anterior responde al cumplimiento del Decreto 767 del 2022 del Ministerio TIC respecto a la actualización Política Colombiana de Gobierno Digital, donde la seguridad digital es un componente importante de la misma y establece en el portal del MINTIC que requiere el apoyo de todas las áreas de las entidades.

2. PROPÓSITO DE LA POLÍTICA:

La Política de Seguridad de la Información de la Entidad busca establecer un entorno de confianza en el ejercicio de sus responsabilidades hacia el Estado y los ciudadanos. Este compromiso se realiza en estricto cumplimiento de las leyes y en alineación con los objetivos estratégicos de la entidad en relación con la cadena de valor, la implementación de sistemas de información, así como las redes, herramientas logísticas y tecnológicas que simplifiquen y agilicen los procesos, dentro del marco de un gobierno digital.

3. ALCANCE:

Aplica a todas las actuaciones administrativas y procesos que adelante 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 al uso de activos de información de la



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

Entidad en cumplimiento de las disposiciones legales vigentes.

3.1. Objetivos Específicos

- a) Gestionar los activos de seguridad de la información de la JPMP en cuanto a su identificación, clasificación y protección para preservar su confidencialidad, integridad y disponibilidad.
- b) Sensibilizar al personal para lograr servidores públicos competentes y comprometidos con una cultura de seguridad de la información reflejada en la aceptación y aplicación de las directrices de seguridad establecidas por la entidad.
- c) Mantener en constante mejora y evaluación el Sistema de Seguridad de la Información, aplicando las acciones consideradas para el sostenimiento de este.
- d) Afrontar las amenazas y ataques digitales (cibernéticos) de los que es objeto la infraestructura de la JPMP, mediante la correcta gestión de eventos e incidentes de seguridad de la información y ciberseguridad.

4. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, persona) que tenga valor para la organización (ISO/IEC 27000).

Activos de información: Se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal (MINTIC. 2016. Modelo de Seguridad y Privacidad de la Información).

Propietario de la Información: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

Usuario: Persona natural o jurídica, pública o privada que, en los términos y circunstancias previstos en la Ley 1266 de 2008, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

usuario y fuente, y asumirá los deberes y responsabilidades de ambos.

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro de la dependencia donde ellos se aplican.

Seguridad de la información: Es el conjunto de medidas asumidas por la Entidad con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información de LA JPMP. Se desarrolla partir de los siguientes criterios:

- a) Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
- b) Integridad: Propiedad de salvaguardar la exactitud y estado completo de



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

los activos.

- c) Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

Ciberdelito/Delito cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

Ciberdelincuente: Persona o software que ejerce el ciberdelito.

Firewall: Un firewall es una aplicación de seguridad diseñada para bloquear las conexiones en determinados puertos del sistema, independientemente de si el tráfico es benigno o maligno. Un firewall debería formar parte de una estrategia de seguridad estándar de múltiples niveles.

IPS: En seguridad de la información se utiliza un IPS, o sistema de prevención de intrusiones. Proporciona políticas y reglas para el tráfico de red junto con un sistema de detección de intrusiones para alertar a los administradores del sistema o de la red sobre tráfico sospechoso, pero permite al administrador proporcionar la acción al recibir la alerta.

IDS: Un sistema de detección de intrusos (IDS) inspecciona toda la actividad de la red entrante y saliente e identifica patrones sospechosos que pueden indicar un ataque a la red o al sistema por parte de alguien que intenta ingresar o comprometer un sistema.

Antivirus: Antivirus es una categoría de software de seguridad que protege un equipo de virus, normalmente a través de la detección en tiempo real y también mediante análisis del sistema, que pone en cuarentena y elimina los virus. El antivirus debe ser parte de una estrategia de seguridad estándar de múltiples niveles.

WAF: Un firewall de aplicaciones web (WAF) es una solución de seguridad que filtra, rastrea y bloquea el tráfico del Protocolo de transferencia de hipertexto (HTTP) para proteger aplicaciones y servidores. Aplica un conjunto de reglas en la conversación entre una aplicación web e Internet, separando el tráfico benigno del malicioso y evitando que posibles amenazas a la seguridad se infiltren en el sistema.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

Antispam: Antispam es un producto, herramienta, servicio o mejor práctica que detiene el spam o correo no deseado antes de que se convierta en una molestia para los usuarios. El antispam debe ser parte de una estrategia de seguridad multinivel.

5. DOCUMENTACIÓN DE REFERENCIA

- a) MSPI - Documento maestro del Modelo de Seguridad y Privacidad de la Información - Versión 4 - octubre 2021.
- b) MSPI - Guía 2 - Política General MSPI v1.
- c) Manual de Seguridad y Privacidad de la Información.
- d) ISO/IEC 27001:2013/2022.

6. MARCO NORMATIVO

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
Constitución Política de Colombia		1991	<p><i>"Artículo 15: Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas.</i></p> <p><i>En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.</i></p> <p><i>La correspondencia y demás formas de comunicación privada son inviolables. Sólo pueden ser interceptadas o registradas mediante orden judicial, en los casos y con las formalidades que establezca la ley.</i></p> <p><i>Para efectos tributarios o judiciales y para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados, en los términos que señale la ley.</i></p>
Ley	527	1999	<p><i>"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del</i></p>



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
			<i>comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones."</i>
Ley	594	2000	<i>"Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones."</i>
Ley	1266	2008	<i>"Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"</i> .
Ley	1273	2009	<i>"Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado 'de la protección de la información y de los datos'- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones."</i>
Ley	1581	2012	<i>"Por la cual se dictan disposiciones generales para la protección de datos personales"</i> .
Ley	1712	2014	<i>"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"</i> .
Ley	1765	2015	<i>"Por la cual se reestructura la Justicia Penal Militar y Policial, se establecen requisitos para el desempeño de sus cargos, se implementa su Fiscalía General Penal Militar y Policial, se organiza su cuerpo técnico de investigación, se señalan disposiciones sobre competencia para el tránsito al sistema penal acusatorio y para garantizar su plena operatividad en la Jurisdicción Especializada y se dictan otras disposiciones", especialmente el numeral 3° del artículo 48 y numeral 1° del artículo 54 que establece como función de LA JPMP la implementación de las políticas de la Entidad.</i>



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
Ley	1915	2018	"Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos".
Ley	1952	2019	"Por medio de la cual se expide el Código General Disciplinario, se derogan la Ley 734 de 2002 y algunas disposiciones de la Ley 1474 de 2011, relacionadas con el derecho disciplinario." Art. 38 #25.
Decreto	235	2010	"por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas"
Decreto	19	2012	"Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública"
Decreto	1377	2013	"Por el cual se reglamenta parcialmente la Ley 1581 de 2012"
Decreto	415	2016	"Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones."
Decreto	1008	2018	"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"
Decreto	1747	2000	"Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con las entidades de certificación, los certificados y las firmas digitales."



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
Decreto	312	2021	"Por el cual se fija la estructura interna de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial", especialmente el numeral 3° del artículo 5° y numeral 1° del artículo 7° que establece como función de LA JPMP la implementación de las políticas de la Entidad.
Resolución	000084	2021	"Por la cual se adopta el Manual Específico de Funciones y Competencias para los empleos que conforman la planta de personal de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial"
Decreto	767	2022	Ministerio TIC respecto a la actualización Política Colombiana de Gobierno Digital, donde la seguridad digital es un componente importante de la misma.
ISO	ISO 31000	2018	Gestión del Riesgo. "Este documento proporciona directrices para gestionar el riesgo al que se enfrentan las organizaciones. La aplicación de estas directrices puede adaptarse a cualquier organización y a su contexto."
ISO	ISO/IEC 27001.	2022	"Requisitos del sistema de gestión de seguridad de la información."
ISO	ISO/IEC 27002.	2022	"Buenas prácticas para gestión de la seguridad de la información".

7. POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La JPMP asume el compromiso de implementar y mantener el Sistema de Gestión de Seguridad y Privacidad de la Información, destacando la importancia de una gestión adecuada de la información y el fortalecimiento de la confianza en el cumplimiento del deber institucional, cuyo objetivo es la formulación, adopción, implementación, y seguimiento de las políticas, regulaciones, planes, programas y proyectos de la Entidad.

Esta política aplica a toda la entidad, sus servidores y funcionarios públicos, contratistas y terceros, buscando la protección de los activos de seguridad de la información, a través del cumplimiento de los requisitos legales e institucionales, así como la generación e implementación de lineamientos para el óptimo



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

tratamiento de la información y complementado con el diseño de controles, identificación y gestión de riesgos.

La Política General de Seguridad y privacidad de la Información estará determinada por las siguientes premisas:

- a) Contar con plataformas apropiadas que protejan los mecanismos de procesamiento, almacenamiento y comunicación donde están contenidos y soportados todos los servicios, registro, validación y realización de trámites JPMP.
- b) Fortalecer la cultura y competencias de los empleados públicos, contratistas, terceros, proveedores de la entidad respecto a la gestión de Seguridad de la Información.
- c) Implementar y mantener actualizada una metodología de gestión de riesgos de seguridad de la información como herramienta para actuar proactivamente ante la presencia de situaciones que puedan afectar la disponibilidad, confidencialidad e integridad de la información de la JPMP de acuerdo con los lineamientos establecidos en la regulación legal vigente, normas y buenas prácticas nacionales e internacionales para la correcta gestión de riesgos.

Como complemento a esta política y para brindar orientación y soporte la JPMP generará un conjunto de políticas suplementarias para la seguridad de la información, las cuales serán aprobadas, publicadas y socializadas a las partes interesadas.

8. POLÍTICAS DE CIBERSEGURIDAD

Las políticas de ciberseguridad son el conjunto de principios, normas, directrices y procedimientos diseñados para gestionar y mitigar los riesgos asociados a la seguridad de la información y las tecnologías de la información en un entorno digital. Esta política tiene como objetivo establecer un marco estructurado que guíe la toma de decisiones y las acciones para proteger los activos digitales, prevenir ataques cibernéticos, y asegurar la confidencialidad, integridad y disponibilidad de la información crítica de la organización. Incluye medidas para proteger sistemas informáticos, redes, datos sensibles y otros recursos digitales, así como para responder eficientemente a incidentes de ciberseguridad. La política de ciberseguridad es esencial para garantizar la resiliencia de la entidad frente a las amenazas digitales en constante evolución y para cumplir con los estándares y regulaciones de seguridad de la información.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

8.1. Principios de la Ciberseguridad

Con el fin de dar cumplimiento al marco normativo, regulatorio y a los objetivos misionales, de la JPMP considera los siguientes principios de la Ciberseguridad para preservar la información y correcto funcionamiento de la plataforma tecnológica para que no se afecten los procesos de la Entidad:

- a) **Mínimo privilegio:** Son todos aquellos privilegios que tienen los sistemas y aplicaciones que se encuentran interconectados pero que solo deben tener los usuarios, configuración y conexión de red necesarios para que funcionen de acuerdo con lo requerido por el proceso.
- b) **Mínima superficie de exposición:** Deben diseñarse las tareas o actividades a realizar en cada uno de los procesos de la JPMP, de tal forma que no queden o se habiliten canales, privilegios, direcciones IP, usuarios, publicación puertos que faciliten a un ciberdelincuente acceder a los sistemas, producto de estas debilidades de configuración en la red y plataforma tecnológica.
- c) **Defensa en profundidad:** Debe existir seguridad por niveles o anillos, es decir, que la arquitectura de red o controles de ciberseguridad que se implementen, tales como: firewall, IPS, IDS, Antivirus, WAF, antispam, entre otros, deben configurarse en diferentes zonas de red. Así como usar diferentes dispositivos para dificultar el trabajo de un ciberdelincuente, obstaculizando su paso por las diferentes capas y evitando que cumpla con su objetivo.

9. MANUAL DE SEGURIDAD DE LA INFORMACIÓN

La JPMP determina la información como un activo de alta importancia para la Entidad, el cual permite el desarrollo continuo de la misión y el cumplimiento del objetivo de esta, generando la necesidad de implementar reglas y medidas que permitan identificar los riesgos y proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información, razón por la cual la JPMP establece el Manual del sistema de gestión de seguridad y privacidad de la información, el cual debe ser adoptado por los servidores públicos, contratistas, terceros y proveedores que presten sus servicios o tengan algún tipo de relación con la entidad; estas políticas se encuentran enfocadas al cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013/2020.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

Todos los empleados públicos, contratistas y terceros que conforman las diferentes áreas de la Entidad deberán clasificar la información que tengan bajo su custodia en alguna de las categorías establecidas.

Toda la información catalogada por las áreas como crítica debe contar con copias de respaldo para garantizar su seguridad.

El acceso a los diferentes equipos informáticos y sistemas de información debe hacerse a través de los mecanismos de autenticación establecidos de acuerdo con los niveles de seguridad.

El acceso no autorizado a los sistemas de información y uso indebido de los recursos informáticos de la entidad está prohibido.

10. ROLES Y RESPONSABILIDADES

Los servidores, funcionarios y terceros de la JPMP como parte activa de la Gestión de Seguridad de la Información y ciberseguridad, deben conocer y dar cumplimiento a las responsabilidades y funciones establecidas para tal fin.

Por tanto, la Justicia Penal Militar y Policial a través de la Oficina de Tecnologías de la Información y de las Comunicaciones estará a cargo de liderar el diseño, implementación, puesta en funcionamiento, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información de la Entidad, por lo que a continuación detallará las responsabilidades frente a la Política, así:

- a) **Dirección General:** Es responsable de velar que se cumpla el Gobierno Digital en la política de seguridad digital y suministrar los recursos necesarios para el desarrollo del Sistema de Gestión integrado de Seguridad de la información.
- b) **Comité de desempeño y gestión institucional:** Es responsable de asegurar la implementación y desarrollo de las políticas de seguridad de la información y del modelo de seguridad y privacidad de la información, hacer seguimiento al plan de gobierno y seguridad digitales, entre otros.
- c) **Líder del Sistema de Gestión de Seguridad de la Información:** Oficial u oficina TIC a cargo de la integración entre los aspectos estratégicos y tácticos que se presenten en el SGSI.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

d) **Propietario o titular de la Información:** Es el funcionario responsable de los procesos dentro de la entidad, y por tanto de la información generada y utilizada en dichos procesos. Como tal tiene la responsabilidad de cumplir con las siguientes obligaciones:

- i. Garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifiquen adecuadamente.
- ii. Definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre la materia.
- iii. Clasificar y documentar la información de acuerdo con el grado de sensibilidad y criticidad de esta.
- iv. Mantener actualizada la clasificación de la información.
- v. Definir la asignación de usuario y los permisos de acceso a la información, de acuerdo con sus funciones y competencias.

e) **Custodio de la Información:** Es el que tiene la responsabilidad de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido.

f) **Usuario de la Información:** Son todos los funcionarios incluidos los del Tribunal Superior Militar y Policial, Fiscal General Penal Militar y Policial, Policía judicial, personal de apoyo, judicantes, proveedores, contratistas y terceros, que, con la debida autorización del propietario de la información, pueden consultar, ingresar, modificar o borrar en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la entidad.

g) **Oficina de Tecnologías de la Información y las Comunicaciones:**

Es responsable junto con el responsable o área encargada de la seguridad de la información de asesorar al Director General en la formulación, actualización e implementación de la Política de Seguridad de la Información y apoyar el desarrollo de las siguientes funciones:

- i. Revisar y proponer la Política de Seguridad de la Información para aprobación del Director General, así como las funciones generales en materia de seguridad Informática.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

- ii. Apoyar el establecimiento e implementación de una metodología de análisis, evaluación y gestión de riesgos de activos informáticos.
- iii. Monitorear y evaluar los cambios significativos en los riesgos que afectan a los activos informáticos frente a las amenazas más importantes de acuerdo con los criterios y niveles para la aceptación de riesgos a los que se ven abocados los activos informáticos de la Entidad.
- iv. Apoyar la revisión y actualización periódica de la Política de Seguridad de la Información, teniendo como marco los siguientes aspectos:
 - Identificación y documentación de nuevos riesgos que afecten los activos informáticos, provenientes de amenazas internas y externas.
 - Evaluación de los incidentes relativos a la seguridad informática en la Entidad, producto del monitoreo y análisis de estos.
 - Recopilación de iniciativas provenientes de las dependencias de la Justicia Penal Militar y Policial, con el fin de mejorar la seguridad de la información.
 - Evaluación de los avances tecnológicos relacionados con la seguridad informática y la viabilidad de implementación en la Justicia Penal Militar y Policial, con el fin de mejorar la seguridad de la información.
 - Evaluación de los avances tecnológicos relacionados con la seguridad informática y la viabilidad de implementación en la Justicia Penal Militar y Policial, con el fin de mejorar la seguridad de la información.
- v. Gestionar la implementación, operación, seguimiento, revisión, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información de la Entidad, así como los objetivos y planes que se formulen dentro de este ámbito.
- vi. Formular soluciones tecnológicas para incrementar la seguridad informática, de acuerdo con las competencias y responsabilidades identificadas en la Entidad.
- vii. Formular metodologías y procesos específicos relativos a la seguridad informática.
- viii. Apoyar el desarrollo de la cultura organizacional en aspectos de seguridad informática como parte del proceso de planificación de la información.
- ix. Apoyar la formulación y seguimiento de planes de divulgación de la importancia de cumplir los objetivos de seguridad de la información.
- x. Evaluar y coordinar la implementación de controles específicos de seguridad informática para nuevos sistemas o servicios.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

- xi. Apoyar la difusión de la seguridad de la información dentro de la Entidad.
- xii. Apoyar los planes de recuperación y continuidad de servicios informáticos de la Entidad.
- xiii. Apoyar las acciones tendientes a impulsar la implementación y cumplimiento de la Política de Seguridad de la Información.
- xiv. Apoyar la realización de las funciones relativas a la seguridad informática de la Entidad, lo cual incluye lo relacionado con la supervisión de todos los aspectos inherentes a los temas tratados en la Política de Seguridad de la Información.
- xv. Identificar y gestionar los requerimientos de seguridad informática para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Entidad.
- xvi. Gestionar con el Coordinador de sistemas de información, que las tareas de desarrollo y mantenimiento de sistemas de información sigan una metodología apropiada de ciclo de vida y que contemple las medidas de seguridad en todas sus fases.
- xvii. Gestionar con el Coordinador de Redes y Comunicaciones, que las tareas de conectividad implementadas sigan una metodología apropiada de ciclo de vida y que contemple las medidas de seguridad en todas sus fases.
- xviii. Ejecutar los requerimientos de seguridad informática establecidos para la operación, administración y comunicación de los sistemas de información y de los recursos de tecnología de la Entidad.
- xix. Coordinar, planear y promover todas aquellas actividades que tengan como fin el mantener la disponibilidad, confidencialidad e integridad de todos los activos informáticos de la Entidad, lo cual incluye la supervisión de todos los aspectos inherentes a los temas tratados en la presente Política.
- xx. Adelantar los procesos de selección de herramientas y proveedores en materia de seguridad informática.
- xxi. Definir la estructura de restricciones y excepciones de acceso a la información de todo el personal, de acuerdo con las pautas de la política de seguridad y a las necesidades de acceso de los usuarios en conformidad con las funciones que desempeñan.
- xxii. Identificar los activos informáticos más críticos de la Entidad.
- xxiii. Promover la difusión y actualización permanente de la Política de Seguridad de la Información de la institución, debido al comportamiento cambiante de la tecnología que trae consigo nuevos riesgos y amenazas.
- xxiv. Promover la aplicación de auditorías enfocadas a la seguridad de la información.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

- h) **Coordinador, oficial u oficina TIC de la seguridad de la información:** Se encarga de coordinar la ejecución de las actividades derivadas de la planeación, implementación, revisión y mantenimiento del SGSI.
- i) **Oficina Asesora de Planeación:** La Oficina asesora de planeación, en coordinación con el Líder del Sistema de Gestión de Seguridad de la Información, estará encargada de la gestión documental del SGSI perteneciente al sistema integrado de gestión de la JPMP.
- j) **Grupo de Talento Humano:** En cumplimiento a la Política de Seguridad de la Información debe asesorar al Director General en:
 - i. El reporte de las novedades administrativas del personal de la Entidad a la OTIC: Vacaciones, permisos, retiros, traslados, comisiones, para que se tomen las acciones necesarias sobre los controles de seguridad de la información.
 - ii. Firmar el acuerdo de confidencialidad con todo el personal que ingresa a la Entidad, respecto del cumplimiento de la Política de Seguridad de la Información.
- k) **Oficina de Control Interno:** Es la encargada de realizar revisiones regulares de la eficacia del SGSI que incluyen el cumplimiento de la política y objetivos del SGSI y la revisión de los controles de seguridad.

En cumplimiento de la Política de Seguridad de la Información, se debe encargar de asesorar al Director General en:

 - i. Realizar auditorías periódicas sobre la operación de los sistemas de información por parte de los usuarios y el uso adecuado de los recursos informáticos de la Entidad.
 - ii. Informar sobre el cumplimiento por parte de los usuarios de la normatividad, la reglamentación y las medidas de seguridad de la información establecidas por esta Política, así como de las buenas prácticas, procedimientos e instructivos que de ella surjan.
- l) **Oficina Asesora Jurídica:** En cumplimiento de la Política General de Seguridad y privacidad de la Información, se debe encargar de asesorar al Director General en:



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

- i. Asesorará en materia legal sobre los cambios o ajustes que se deban realizar a las Políticas de Seguridad de la Información de la Entidad.
- ii. Verificará el cumplimiento de la presente Política en la gestión de todos los procesos, acuerdos, convenios u otra documentación de la Entidad, con sus funcionarios y con terceros.

m) Grupo de contratos:

- i. Verificar e implementar las medidas de seguridad de la información en la gestión con los proveedores y contratistas de la entidad, a través de obligaciones específicas de cumplimiento de la política de seguridad de la información y el acuerdo de confidencialidad.
- ii. Procurar la protección de la seguridad de la información de todos los activos de la información que puedan verse involucrados en los procesos contractuales o contratos.

11. DIFUSIÓN, REVISIÓN, CUMPLIMIENTO Y VIGENCIA

11.1. Difusión

La JPMP comunicará a través del Grupo de Comunicaciones todas las políticas, procedimientos u otros documentos generados en el marco del Sistema de Gestión de Seguridad de la Información a través de los siguientes canales de comunicación: correo electrónico, intranet, comunicaciones impresas, charlas y/o capacitaciones.

La Escuela de Justicia Penal Militar y Policial será responsable de incorporar la aplicación de la política de seguridad de la información en el plan de capacitación institucional y velar por la correcta inducción y reinducción de los funcionarios en materia de seguridad.

El Grupo de Contratos será la responsable de incorporar dentro de los procesos, la cláusula de cumplimiento de las Políticas de Seguridad de la Información, la cual debe ser entregada para su consentimiento y firma de esta.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

La Oficina de Tecnologías de la Información y las Comunicaciones será la responsable de la existencia permanente y el cumplimiento de un plan formal de difusión, capacitación y sensibilización de la seguridad de la información.

La Oficina de Tecnologías de la Información y las Comunicaciones debe velar por la ejecución del plan de difusión y el cumplimiento de sus objetivos con la Escuela de la Unidad, así como la existencia de un plan de comunicaciones que lo complemente.

11.2. Revisión

La Política General de Seguridad y Privacidad de la Información será revisada y evaluada en su cumplimiento mínimo una vez (1) al año o cuando requiera modificaciones con el objetivo de mantenerla actualizada, este proceso será liderado por la OTIC, revisado por la oficina de planeación, y aprobado por el responsable o área encargada de la seguridad de la información, considerando los siguientes aspectos:

- a) Condiciones contractuales, regulatorias y legales.
- b) Cambios en ámbito organizacional o técnico.
- c) Disponibilidad de recursos.
- d) Retroalimentación de las partes interesadas.
- e) Resultados de las revisiones efectuadas por terceras partes.
- f) Estados de acciones preventivas y correctivas.
- g) Alertas ante amenazas y vulnerabilidades.
- h) Información relacionada a incidentes de seguridad.
- i) Medición de los indicadores del Sistema de Gestión de Seguridad de la Información.

11.3. Cumplimiento.

El cumplimiento de la Política General de Seguridad y privacidad de la Información es obligatorio a todo nivel, por lo tanto, debe ser cumplida por todos los servidores públicos, funcionarios, contratistas, terceros y proveedores que interactúen con los activos de información y con la información para el desempeño de sus funciones de acuerdo con los roles y responsabilidades.



UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

Política General de Seguridad, Privacidad de la Información y Ciberseguridad

El incumplimiento de las políticas de seguridad y Privacidad de la Información traerá consigo, las consecuencias legales o disciplinarias que apliquen de acuerdo con la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., 29 de abril de 2024

CONTROL DE CAMBIOS			
Versión	Fecha	Instancia de Aprobación	Descripción
01	19/07/2022	Sesión 04 Comité Institucional de Gestión y Desempeño	Elaboración de la política V1
02	29/04/2024	Comité Institucional de Gestión y Desempeño – Sesión 5 de 2024	Actualización de la política V2, se actualiza el alcance, se adiciona definiciones, se incluyen las normas ISO y ciberseguridad, y se suprimen políticas detalladas que se tramitarán de acuerdo con los tratamientos que se realicen, o a los planes de acción que se definan en la vigencia 2024 hasta la 2026.