La Unidad Administrativa Especial de la Justicia Penal Militar y Policial (UAE-JPMP), como encargada de la organización, funcionamiento y administración de la Jurisdicción Especializada, entendiendo la importancia de la adecuada gestión de la seguridad de la información se ha comprometido con la implementación del *"Modelo de Seguridad y Privacidad de la Información*", por lo cual 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 él Estado y los ciudadanos en estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad[1] sobre el manejo de los activos de información de la Entidad.

1. OBJETIVO

Proporcionar las herramientas organizacionales, estratégicas y reglamentarias para la protección de los activos de información de la Entidad en su creación, difusión, modificación, almacenamiento, preservación y eliminación, contra el uso indebido de estos cuyo propósito es mantener un nivel de exposición que permita responder por la confidencialidad, integridad y disponibilidad acorde con las necesidades de los distintos grupos de valor y de interés contribuyendo con el incremento de la transparencia de la Gestión Pública..

2. ALCANCE

Aplica a todas las actuaciones administrativas y procesos que adelante la Justicia Penal Militar y Policial; asimismo, está dirigida a los servidores públicos, funcionarios, contratista y terceros de la Entidad, sus grupos de valor e interés y la ciudadanía en general respecto al uso de activos de información de la Entidad en cumplimiento de las disposiciones legales vigentes.

3. DEFINICIONES

Activo: Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) 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).

[1] Resolución No. 000010 del 07 de enero de 2022 ""Por la cual se adopta la Misión, Visión y Objetivos Estratégicos de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial"

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 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, 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 del a dependencia donde ellos se aplican.

Seguridad de la información: conjunto de medidas asumidas por la Entidad con el fin de proteger la confidencialidad, integridad y disponibilidad de los activos de información de la UAE-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 los activos.
c) **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

4. MARCO NORMATIVO

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
Constitución Política de Colombia		1991	*"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.* *En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución.* *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.*

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
			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.
Ley	1266	2008	*"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".*
Ley	1273	2009	*"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."*
Ley	1581	2012	*"Por la cual se dictan disposiciones generales para la protección de datos personales".*
Ley	1712	2014	*"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".*
Ley	1765	2015	*"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 UAE - JPMP la implementación de las políticas de la Entidad.
Decreto	235	2010	*"por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas"*
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*

TIPO DE NORMA	NÚMERO	AÑO	Descripción - Epígrafe
			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	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 UAE – 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"*

5. PRINCIPIOS Y LINEAMIENTOS DE IMPLEMENTACIÓN

La Política de Seguridad de la Información constituye la declaración general que representa la posición de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial con respecto a la protección de los activos de la Entidad, por lo cual atenderá los siguientes principios:

- Minimizar el riesgo de los procesos misionales de la Entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de los funcionarios, contratistas y terceros.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información (SGSI).
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Jurisdicción Especializada.
- Garantizar la continuidad del servicio frente a incidentes.

Asimismo, los lineamientos a partir de los cuales la Entidad asegurará la correcta implementación son:

- Definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros

alineados a las necesidades de la Jurisdicción Especializada, y a los requerimientos regulatorios que le aplican a su naturaleza.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

- Protegerá la información generada, procesada, transmitida o resguardada por los procesos y activos de información que hacen parte de estos, con el fin de minimizar impactos financieros, operativos o legales debido a su uso incorrecto, a partir de la aplicación controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- Protegerá su información de las amenazas originadas por parte del personal.

- Protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- Controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- Implementará control de acceso a la información, sistemas y recursos de red.

- Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- Garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- Garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basado en el impacto que pueden generar los eventos.

- Garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

Así las cosas, el incumplimiento a la Política de Seguridad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno Nacional

6. POLITICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

Teniendo en cuenta que, junto con el recurso humano, la información generada por la Unidad Administrativa Especial de la Justicia Penal Militar y Policial y la tecnología informática que la soporta, se han convertido en elementos indispensables para el funcionamiento de la Entidad, es necesario protegerlos contra las amenazas que puedan atentar contra los objetivos misionales, especialmente la relativa a garantizar el acceso a una justicia penal militar y policial oportuna y eficaz

En ese sentido, la implementación de la Política de Seguridad de la Información implica la armonización y adopción de otras que implementen los controles las cuales hacen parte del Sistema de Seguridad de la Información (SGSI) cuya verificación estará integrado por un Comité que se creará mediante el correspondiente acto administrativo.

La Políticas para la implementación de los controles de seguridad de la información:

6.1. Gestión de activos

6.1.1. Identificación de activos

6.1.1.1. Definición

Se realizará periódicamente una identificación y actualización de los activos de información.

6.1.1.2. Parámetros de implementación

I. La identificación de activos de información estará a cargo de los líderes de los procesos definidos en la Entidad.

II. El registro de activos de información deberá ser consignada en la Matriz de Activos de Información formato que reposa en el sistema SGI.

6.1.2. Clasificación de activos

6.1.2.1. Definición

Se determinará la clasificación de los activos de información de acuerdo con la criticidad, sensibilidad y reserva de esta.

6.1.2.2. Parámetros de implementación

I. En la implementación de esta política debe tenerse en cuenta las normas vigentes que regulen la materia y los siguientes parámetros:

El inventario de activos de la información deberá especificar para cada activo: i) información básica del activo (nombre, observaciones, proceso), ii) nivel de clasificación de las propiedades de información según los criterios de privacidad, integridad y disponibilidad, iii) información relacionada con su ubicación física y/o electrónica, iv) Su propietario y custodio, v) los usuarios y su derecho de acceso.

II. Las propiedades de la información se clasificarán según los siguientes criterios:

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA RESERVADA	**ALTA (A)**	**ALTA (1)**
INFORMACIÓN PUBLICA CLASIFICADA	**MEDIA (M)**	**MEDIA (2)**
INFORMACIÓN PÚBLICA	**BAJA (B)**	**BAJA (3)**
NO CLASIFICADA	**NO CLASIFICADA**	**NO CLASIFICADA**

III. Las propiedades de la información se clasificarán según los siguientes niveles:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

6.1.3. Etiquetado de la información

6.1.3.1. Definición

La Entidad desarrollará un conjunto de procedimientos de etiquetado de la información, los cuales deberán especificar la clasificación dada a cada activo de información.

6.1.3.2. Parámetros de implementación

I. Se deberán etiquetar los activos de información según su esquema de clasificación en confidencialidad, integridad y disponibilidad
II. Si un activo de información en formato impreso no se encuentra etiquetado deberá ser tratado en todos sus niveles como NO CLASIFICADA

6.1.4. Devolución de los activos

6.1.4.1. Definición

Todos los empleados y usuarios de partes externas deberán hacer entrega de los activos de información que se encontraren a su cargo al terminar su empleo, contrato o acuerdo.

6.1.4.2. Parámetros de implementación

I. Los activos de información como bases de datos, archivos de datos, contratos, documentaciones de sistemas, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes, contratos, hardware, equipos periféricos, impresoras, medios extraíbles, equipos de conexión y comunicaciones y cualquier otro que se encuentre en el inventario de Activos de Información y que se encuentre en propiedad de un usuario o en custodia del mismo deberá ser devuelto a la UAESPJPMP terminadas sus labores, en el caso de equipos de tecnología deberá tener el visto bueno de la Oficina de Tecnologías de la Información y las Comunicaciones de su correcto funcionamiento e integridad y de la Grupo Administrativo de la Dirección Ejecutiva.

6.1.5. Gestión de medios removibles

6.1.5.1. Definición

La Entidad permitirá el uso de medios removibles que hayan sido entregados a los funcionarios por parte de la OTIC, y siempre y cuando la información guarde relación directa con las funciones a su cargo y observando las políticas de seguridad y privacidad de la información.

6.1.5.2. Parámetros de implementación

I. Los medios removibles no podrán ser utilizados en ningún caso para guardar información que contenga datos peligrosos para la integridad, disponibilidad o privacidad de la información de la Entidad como archivos multimedia que no guarden relación directa con las funciones de su cargo.

II. En caso de perdida, daño o robo se deberá informar a la Entidad del tipo de activo de información que contenía el medio removible y sí se puede presentar un incidente de seguridad que deba ser reportado.

III. En ningún caso los medios extraíbles deberán ser vendidos, prestados, compartidos o utilizados en actividades externas a las directamente relacionadas con las funciones del cargo.

6.1.6. Disposición de los activos

6.1.6.1. Definición

La Entidad mantendrá en conservación de los activos de información según los lineamientos de ley y los tiempos de retención establecidos en las tablas de retención documental

6.1.6.2. Parámetros de implementación

I. La OTIC como custodia de la información digital debe mantener copias de respaldo de la información contenida en sus sistemas de información, bases de datos y repositorios de datos

II. Se deben hacer pruebas de respaldo periódicas y verificación de la integridad de estas al menos dos veces al mes para los activos de información digital que sean clasificados en la categoría ALTA, una vez al mes para los activos de categoría MEDIA y una vez cada dos meses para los activos de categoría BAJA.

III. La OTIC deberá mantener la documentación actualizada de la manera en la que se realizan los respaldos de la información, se hace su verificación y se hace la respectiva recuperación

IV. Los dispositivos móviles y medios extraíbles podrán ser reutilizados y asignados a nuevos usuarios una vez se haya realizado una copia y borrado seguro de la información contenida en el dispositivo siempre y cuando contenga información cuya clasificación haya sido categorizada como ALTA.

6.1.7. Dispositivos móviles

6.1.7.1. Definición

Los funcionarios de la UAESPJPMP que requieran en desarrollo de sus funciones el uso equipos portátiles y/o dispositivos móviles que sean de propiedad de la entidad, deberán cumplir con los lineamientos de seguridad establecidos por parte de la Oficina de Tecnologías de la Información y de las Comunicaciones.

6.1.7.2. Parámetros de implementación

I. Es permitido el uso del correo institucional en los dispositivos móviles personales de los funcionarios, quienes deberán hacer un uso adecuado del servicio y manteniendo los principios de confidencialidad de la información

II. En caso de pérdida o robo del equipo móvil en donde se encuentren activos de información de la Entidad, se deberá informar de manera formal a la OTIC para evaluar sí se presenta un incidente de seguridad de la información.

III. El uso de dispositivos móviles de la Entidad es para el desarrollo exclusivo de las funciones del cargo

IV. Los usuarios que tengan dispositivos móviles de la Entidad deberán mantenerlos libres de programas maliciosos y del cualquier programa que no sea necesario para el desarrollo de sus funciones

6.2. Control de acceso

6.2.1. Control de acceso con usuario y contraseña

6.2.1.1. Definición

Se protegerá el acceso a los equipos de cómputo, sistemas de información, sistemas de comunicación e infraestructura tecnológica a través de contraseñas o cualquier otro mecanismo de autenticación que permita la autenticación de los usuarios.

6.2.1.2. Parámetros de implementación

I. Se deben incluir en los sistemas de información mecanismos como: tokens, ID'S, doble factor de autenticación, huellas dactilares o cualquier mecanismo que permita obtener de forma inequívoca la identidad de los usuarios.

II. El uso de las credenciales de acceso es personal e intransferible y es responsabilidad de los usuarios, y terceros mantener en secreto las mismas e informar de su pérdida o revelación a la OTIC, quien deberá asignar nuevas credenciales e informar al usuario para su cambio inmediato.

III. Las operaciones, transacciones, mensajes, procesos y demás actividades realizadas y obtenidas con la identidad de los usuarios son su responsabilidad siempre y cuando no se demuestre que han sido obtenidas por medio abusivo o vulnerando los controles tecnológicos que tiene la Entidad.

6.2.2. Suministro del control de acceso

6.2.2.1. Definición

Las credenciales de acceso a los sistemas tecnológicos serán suministradas una vez se cuente con las autorizaciones necesarias por parte de la Entidad

6.2.2.2. Parámetros de implementación

I. Las credenciales serán suministradas por la OTIC, previo diligenciamiento de las autorizaciones de su jefe inmediato y del Grupo de Personal.

II. Se deberá contactar al usuario personalmente haciendo entrega de las credenciales de acceso al usuario, que corresponden a una identificación de usuario y una contraseña, token o mecanismo definido por la OTIC.

III. El usuario deberá hacer cambio inmediato de la contraseña al momento de su recepción inicial.

IV. En caso de personal externo la autorización deberá ser realizada por el supervisor del contrato o convenio siempre y cuando este se encuentre vigente, especificando la fecha de caducidad de estas. De la misma forma en caso de presentarse prorrogas el supervisor del contrato o convenio deberá informar la OTIC la nueva fecha de caducidad de las credenciales adjuntando el respectivo formato y especificando los accesos requeridos.

6.2.3. Gestión de contraseñas

6.2.3.1. Definición

Las contraseñas deberán tener una complejidad alta determinada por cada sistema de información y deberá ser cambiada mínimo cada sesenta (60) días. Las credenciales de usuario que no hayan sido usadas por un periodo de noventa (90) días deben ser inhabilitadas y reportadas al Grupo de Talento Humano para su conservación o eliminación definitiva.

6.2.3.2. Parámetros de implementación

I. Los sistemas cuyo acceso este protegido a través del uso de credenciales, nombre de usuario y contraseña deben proveer los mecanismos necesarios para su cambio y recuperación en casos de olvido

II. La complejidad de las contraseñas será definida para cada sistema de información por la Oficina de Tecnologías de la Información y las Comunicaciones

III. El uso de las contraseñas es personal e intransferible, los usuarios son responsables del uso de estas y se prohíbe compartirlas a través de cualquier medio

6.2.4. Perímetros de seguridad

6.2.4.1. Definición Es responsabilidad de la OTIC velar por el adecuado uso de las conexiones autorizadas e impedir accesos no autorizados a las redes de comunicación.

6.2.4.2. Parámetros de implementación

I. La Oficina de Tecnologías de la Información y Comunicaciones deberá monitorear las conexiones con terceros hacia la red interna y velar por que se dé el uso que ha sido establecido en los acuerdos o condiciones contractuales establecidas.

II. Las conexiones y el uso de activos de información que dé manera directa o indirecta transfieran la responsabilidad de la información a un tercero y que sean necesarias en el marco de la ejecución de contratos deberán incluir los acuerdos para cumplir las políticas de seguridad de la información establecidas por la UAESPJPM.

6.2.5. Áreas de carga

6.2.5.1. Definición La entidad dispondrá de áreas de carga segura para el despacho y recibo de paquetes físicos, impidiendo su apertura, pérdida de confidencialidad o integridad por parte de personal no autorizado.

6.2.5.2. Parámetros de implementación

I. La apertura de paquetes físicos que contengan activos de información deberá hacerse únicamente por personal de la Unidad, debidamente autorizado o personal externo de mensajería que haya sido designado para esta actividad

II. La manipulación de activos de información en las áreas administrativas y despachos de la Justicia Especial estará a cargo de los jefes, coordinadores, fiscales, jueces y magistrados, quienes velarán por la custodia de los activos de información en los lugares y espacios de trabajo previstos

6.3. No repudio

6.3.1. Trazabilidad

6.3.1.1. Definición

La OTIC, deberá proveer los mecanismos técnicos para que las operaciones digitales que generen transformen, transporten o almacenen activos de información dejen trazas digitales para su seguimiento y auditoría.

6.3.1.2. Parámetros de implementación

I. Los sistemas de información misionales o de apoyo que generen, transformen, almacenen, procesen o transmitan activos de información con criticidad alta deben generar rastros que permitan identificar el autor, la fecha y hora y el tipo de operación del evento realizado.

II. Los sistemas de transmisión de información y de telecomunicaciones deberán mantener un registro de los eventos de tráfico de la información, así como de los eventos anómalos presentados para su posterior revisión y auditoría

6.3.2. Retención

6.3.2.1. Definición

La Entidad mantendrá un registro histórico de los activos de información y de las acciones realizadas por los usuarios por periodos que se ajusten a los tiempos determinados por las tablas de retención documental de la Entidad.

6.3.2.2. Parámetros de implementación

I. La Oficina de Tecnologías de la Información y las Comunicaciones, a través de sus coordinaciones, conservará los activos de información digital de acuerdo con las tablas de retención adoptadas por la Entidad manteniendo su integridad, confidencialidad y disponibilidad, hasta su disposición final, eliminación conservación definitiva o destrucción

II. La Secretaría General a través del Grupo Administrativo conservara los activos de información en medios físicos de acuerdo con las tablas de retención documental adoptadas por la Entidad manteniendo su integridad, confidencialidad y disponibilidad, hasta su disposición final, eliminación conservación definitiva o destrucción

III. Los activos de información de registros de auditoría de las acciones realizadas a través de los sistemas de información, medios de comunicación digital, sistemas de transmisión de datos o telecomunicaciones deberán conservarse de acuerdo con las tablas de retención documental y es deber de la Oficina de Tecnologías de la Información y las Comunicaciones mantener su integridad, confidencialidad y disponibilidad

IV. La información correspondiente a activos de vigilancia externa, sistemas de grabación de video en áreas comunes, ingreso de personal, vehículos u objetos será conservada por Grupo Administrativo quien conservará los activos de información en medios físicos de acuerdo con las tablas de retención documental adoptadas por la Entidad manteniendo su integridad, confidencialidad y disponibilidad, hasta su disposición final, eliminación conservación definitiva o destrucción

6.3.3. Auditoría

6.3.3.1. Definición

La Entidad revisará periódicamente las trazas de auditoría de los sistemas de información y comunicaciones para poder establecer la completitud y

corrección de los eventos o las anomalías presentadas en el procesamiento o la transmisión

6.3.3.2. Parámetros de implementación

I. La Oficina de Tecnologías de la Información deberá con una periodicidad de una vez cada tres (3) meses realizar una verificación de que las trazas de auditoría de los sistemas de información y los sistemas de comunicaciones registren de forma correcta los accesos y operaciones que se den como parte de las acciones realizadas

II. Los registros de auditoría que se soliciten por parte de autoridades internas o externas como parte de procesos disciplinarios o penales deben ser recolectadas por la Oficina de Tecnologías de la Información a través de las coordinaciones y equipo técnico especializado, estos registros de auditoría en ningún caso pueden revelar información intrínseca de los casos ni información sujeta a reserva procesal y se dará solo en los casos en los que sea solicitada por autoridad competente en el marco del proceso investigativo.

6.3.4. Intercambio electrónico de información

6.3.4.1. Definición

Los intercambios electrónicos de información que se den en el ámbito de la colaboración interinstitucional o con otras entidades deberán incluir características de no repudio, integridad y confidencialidad

6.3.4.2. Parámetros de implementación

I. En los casos enmarcados en colaboración interinstitucional y que prevean recepción de información, estará cubierta bajo los principios de privacidad y no repudio, los mensajes electrónicos y demás trazas de información se consideran fiables y los autores o transmisores originales tendrán responsabilidad en el contenido de estos y esta responsabilidad no podrá ser trasladada a la Entidad receptora

II. Los mensajes electrónicos generados en la Entidad en el marco de la colaboración interinstitucional estarán estará cubierta bajo los principios de privacidad y no repudio, los mensajes electrónicos y demás trazas de información se consideran fiables y los autores o transmisores originales tendrán responsabilidad en el contenido de estos y esta responsabilidad no podrá ser trasladada a la Entidad receptora

6.4. Privacidad y confidencialidad

Las políticas sobre el tratamiento y protección de datos personales en cumplimiento de la regulación y con el respeto de los derechos de los titulares de la información se adopta en la Política de Tratamiento de Datos Personales, la cual es de obligatoria aplicación en todas las actividades que involucren el tratamiento de dicha información.

6.5. Integridad

6.5.1. Definición de la Política

La información contenida en los activos de la Entidad debe seguir el principio de integridad, los funcionarios, contratistas y terceros deben velar que la información se mantenga fiel a su sentido original, sin modificaciones ni alteraciones, sin importar sí se encuentra en medios físicos, electrónicos o haya sido transmitida verbalmente

6.5.2. Parámetros de implementación

6.5.2.1. En el caso de vínculos contractuales debe establecerse a través de una Cláusula de Integridad de la Información los compromisos de administración y manejo integro e integral de la información interna

6.5.2.2. La política de integridad deberá ser conocida por los funcionarios, contratistas y terceros que produzcan, transporten, almacenen o entreguen información en activos de información de la Entidad.

6.6. Disponibilidad del servicio e información

6.6.1. Definición

La entidad debe contar con un plan de continuidad de negocio que asegure y permita reestablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y los procesos misionales de la Entidad ante la ocurrencia de un incidente de seguridad de la información a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones.

6.6.2. Niveles de disponibilidad

6.6.2.1. Definición

Los acuerdos, contratos, convenios y demás compromisos que involucren la administración, producción, transmisión, almacenamiento, publicación

o transformación de activos de información deben conocer y aplicar la política de disponibilidad de la información

6.6.2.2. Parámetros de implementación

I. Los sistemas de información o transmisión de datos que traten con activos de información deben contemplar cláusulas que indiquen los acuerdos de niveles de servicio (ANS), en donde se especifiquen los términos y tiempos máximos de indisponibilidad de los mismos, los tiempos de recuperación aceptables, es responsabilidad de la supervisión de los contratos hacer cumplir estos acuerdos e informar a la Oficina de Tecnologías de la Información y las Comunicaciones y al Grupo de Contratos los eventos que los afecten

II. Los sistemas de información y comunicación catalogados con el nivel de criticidad ALTO deberán contar con sistemas de respaldo y contingencia que garanticen que la disponibilidad sea aceptada por la Entidad y la Oficina TIC deberá revisar periódicamente que se encuentre dentro de los niveles aceptables por la Entidad

III. En casos en que la disponibilidad de la Información sea afectada a activos críticos de la Entidad por incidentes de seguridad de la información se deberá seguir la ruta de atención definida en el Plan de Tratamiento de Incidentes de Seguridad Digital

6.6.3. Planes de recuperación

6.6.3.1. Definición de la Política

La Entidad deberá contar con un plan de recuperación de sus activos de información

6.6.3.2. Parámetros de implementación

I. Los activos de información categorizados con criticidad ALTA deben incluir un plan de recuperación de desastres de acuerdo con los niveles de servicio definidos, tiempo y punto de recuperación objetivo (RTO y RPO) acordado con los dueños del activo

II. Los planes de recuperación de desastres deben ser conocidos por la Entidad y deben ser actualizados y comunicados de forma periódica a todos los grupos objetivo, dueños de activos de información y funcionarios

III. Una vez concluida la ejecución del plan de recuperación de desastres la Oficina de Tecnologías de la Información deberá presentar un informe escrito en donde se detallen los controles vulnerados, los activos de información comprometidos, su estado final en caso de existir perdidas

6.6.4. Interrupciones

6.6.4.1. Definición de la Política

Las interrupciones a los servicios de información y comunicaciones deben ser planeadas, aprobadas y comunicadas a la Entidad, la ciudadanía, los líderes de procesos y grupos de interés de manera anticipada

6.6.4.2. Parámetros de implementación

I. Las interrupciones que se presenten en virtud de ventanas de mantenimiento, actualización, revisión o reemplazo, deben ser comunicadas a los grupos de interés con al menos 24 horas de anticipación y en todo caso se debe procurar por no inferir en el normal desarrollo de las actividades misionales de la Entidad, en casos en que las actividades se deban realizar en horario de jornada laboral corriente se debe contar con la autorización de los lideres de los procesos o dueños de los activos de información

II. En los casos en que las interrupciones de den en virtud de fallas o defectos en los activos, la Oficina de Tecnologías de la Información y las Comunicaciones deben comunicar a los lideres de proceso y dueños de los activos las novedades presentadas y activar los planes de recuperación de manera inmediata

III. En los casos en que las interrupciones se den en virtud de incidentes de seguridad la Oficina de Tecnologías de la Información y las Comunicaciones deben activa el Plan de Tratamiento de Incidentes de Seguridad Digital e informar al Comité de Seguridad de manera inmediata

6.6.5. Acuerdos de niveles de servicio

6.6.5.1. Definición de la política

En los casos en los que la disponibilidad de los activos de información se vea afectada, se deben respetar los acuerdos de niveles de servicio e informar a proveedores, contratistas y terceros

6.6.5.2. Parámetros de implementación

I. La Oficina de Tecnologías de la Información y las Comunicaciones, velara por el cumplimiento de los acuerdos de niveles de servicio ANS, definidos para los activos de información y en los eventos de indisponibilidad llevara un registro de las fechas y horas y de interrupción y restablecimiento, las causas técnicas o fallos humanos de la indisponibilidad y en los casos en los que haya lugar aplicara las cláusulas sancionatorias y demás instrumentos de control previstos en los acuerdos y contratos

II. Los contratos interadministrativos que celebre la Entidad deberán contemplar acuerdos de niveles de servicio de disponibilidad de los servicios,

plataformas y sistemas de información que sean utilizados para el desarrollo de los procesos internos

6.6.6. Segregación de ambientes

6.6.6.1. Política

Los sistemas de información adquiridos, desarrollados o implementados deberán contar con ambientes tecnológicos para el desarrollo, las pruebas y la puesta en producción.

6.6.6.2. Parámetros de implementación

I. Los sistemas de información que sean implementados para el apoyo, control o seguimiento de los procesos misionales, estratégicos o de apoyo deberán contar con ambientes tecnológicos separados independientes para las labores de desarrollo de software, pruebas de calidad y ambiente productivo

II. Los repositorios de información, bases de datos, sistemas de archivos y demás contenedores de datos deberán segregarse de forma que no se comparta información entre los ambientes tecnológicos

III. Los datos utilizados para el desarrollo y las pruebas deben observar los principios de confidencialidad consignados en la presente política y no podrán ser usados datos personales o de casos reales para impartir capacitaciones o hacer pruebas del software

6.6.7. Gestión de cambios

6.6.7.1. Política

Los cambios en los sistemas de información, modelos de transmisión y en general la operación tecnológica que afecte los procesos misionales, de apoyo o estratégicos deberá ser concertada, probada y aprobada por los dueños de los activos de información

6.6.7.2. Parámetros de implementación

I. Las solicitudes de cambios en los códigos fuentes, modelos de operación, configuración de los sistemas de información o telecomunicaciones que afecten la operación de los procesos de la Entidad deberá ser solicitados y aprobados por los dueños de activos de información, los lideres de los procesos, deberán estar documentados, así como sus pruebas de funcionamiento

II. La puesta en producción de los cambios a los activos de información deberá ser aprobada por los dueños de los activos y los lideres de proceso, su puesta en funcionamiento deberá ser coordinada con el Grupo de Sistemas de

Información y el Grupo de Plataforma Tecnológica de la Oficina de Tecnologías de la Información y las Comunicaciones en un horario acordado y que minimice el impacto sobre la operación de la Entidad

III. La Oficina de Tecnologías de la Información y las Comunicaciones deberá en todos los casos mantener un control de las versiones de los códigos fuentes y demás artefactos tecnológicos que permitan reversar los cambios realizados y volver a un estado estable de operación

IV. Los lideres de los procesos y dueños de los activos de información deben mantener informada a la Oficina de Tecnologías de la Información y las Comunicaciones sobre la correcta operación de los activos de información después de la realización de cambios, en caso de presentarse fallas informarlas a través de los canales de ayuda y soporte técnico

6.7. Gestión de incidentes de seguridad de la información

Todos los usuarios de la UAEJPMP deben reportar cualquier incidente de seguridad que detecten, mediante oficio, correo electrónico, telefónicamente o a través de la Mesa de Ayuda, dirigiéndose al Equipo de Seguridad Informática de la Oficina de Tecnologías de la Información y las Comunicaciones y según lo establecido en el Plan de Tratamiento de Incidentes de Seguridad Digital.

6.8. Capacitación y sensibilización en seguridad de la información

La Entidad en cabeza la Oficina de Tecnologías de la Información y las Comunicaciones diseñara, implementara, evaluara, actualizará y mantendrá disponible, material de capacitación sobre la Política de Seguridad de la Información y su aplicación, esta deberá ser difundida y conocida por todos los funcionarios, terceros y grupos de interés.

7. POLÍTICAS RELACIONADAS PARA LA IMPLEMETACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

7.1. Uso aceptable de los servicios informáticos

7.1.1. Correo electrónico institucional

7.1.1.1. Política

Todo servidor o funcionario de la Entidad que posea un usuario o una cuenta de red puede contar con servicio de correo electrónico institucional suministrado por la Entidad

7.1.1.2. Parámetros de implementación

I. La dirección de correo electrónico institucional deberá crearse de la siguiente manera: nombre.apellido@justiciamilitar.gov.co

En donde "nombre. Apellido" corresponde al nombre y apellido del titular de la cuenta y justiciamilitar.gov.co, es el dominio registrado por la UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL

II. En caso de que por necesidades del servicio se deba crear una cuenta institucional se debe establecer su responsable y crearse de la siguiente manera: nombre despacho@justiciamilitar.gov.co.

III. Los mensajes de correo pueden considerarse como elementos probatorios de acuerdo con la Ley 527/99 por medio de la cual se define y reglamenta el uso de mensajes de datos, del Comercio Electrónico y firmas digitales.

IV. El servidor o funcionario de la Entidad deberá diligenciar el formato correspondiente, definido en el SGI, para que le sea asignada una cuenta de correo electrónico institucional, en el cual se compromete a mantener la confidencialidad de su contraseña de acceso la cual es personal e intransferible

V. El usuario debe enviar y recibir la información de la Entidad inherente al desarrollo de su labor a través de la cuenta de correo electrónico institucional que le fue asignada y no a través de cuentas de correo personales, públicas o comerciales. Así mismo debe incluir en todos los mensajes la información correspondiente al nombre, cargo, área, secciona/, dependencia, grupo y teléfono

VI. Es responsabilidad del usuario leer, depurar y respaldar el contenido de su respectivo buzón de correo, dado que éste tiene capacidad limitada de almacenamiento.

VII. Todas las personas que tengan acceso al servicio de correo electrónico institucional de la Entidad deben estar identificadas plenamente como: Servidores Públicos de la Justicia Penal Militar y Policial, Contratistas autorizados, judicantes, estudiantes en pasantías y funcionarios de otras entidades autorizados por Ley, por convenio, contrato u orden de servicio. Por lo tanto, no se permite el acceso al servicio de correo sin la previa solicitud emitida por los responsables de los convenios, supervisores de los contratos,

prestaciones del servicio y/o jefes de las dependencias donde laboran dichas personas.

VIII. La responsabilidad del contenido de los mensajes de correo será del usuario remitente

IX. La información de carácter confidencial que se transmita a través del servicio de correo electrónico debe ser emitida con los medios de seguridad que disponga

X. No se debe utilizar ningún tipo de procedimiento o herramienta que permita ocultar o tergiversar el nombre del remitente

XI. No se debe utilizar ningún tipo de procedimiento o herramienta que afecte el normal desempeño de otras máquinas, tal como el uso del servicio de correo electrónico institucional para el envío de software malicioso (virus, troyanos, etc.) y el envío de mensajes con información no solicitada, a todos los usuarios de la red (spam)

XII. No suplantar la cuenta de correo electrónico de otro usuario.

XIII. No se debe transmitir información que se considere de uso exclusivo y/o confidencial sin la autorización del responsable de la información y con los mecanismos adecuados para su transmisión

7.1.2. Uso de las conexiones de red e Internet provistos por la Entidad

7.1.2.1. Política

Todo usuario con acceso a Internet tiene un perfil que determina los sitios a los cuales pueden servir como apoyo a la gestión que realiza en la entidad.

7.1.2.2. Parámetros de implementación

I. Se autoriza el uso de los recursos informáticos para capacitación a distancia y debidamente autorizado por el Jefe inmediato

II. Se prohíbe descargar e instalar software que no esté debidamente licenciado y sin autorización de la Oficina de Informática.

III. La Entidad se reserva el derecho de restringir el acceso a sitios no seguros y que no sean necesarios para apoyar el desarrollo de las actividades labórales

IV. La Entidad, en cabeza de la Oficina de Tecnologías de la Información y las Comunicaciones, se reserva el derecho de monitorear, restringir, bloquear y analizar permanentemente el uso de los servicios informáticos de la Entidad, mediante herramientas técnicas adquiridas para tal fin.

V. La Oficina TIC es la responsable de monitorear el acceso lógico y físico a las redes a través del Grupo de comunicaciones: Conectividad 'a la red local (LAN) con nodos alámbricos e inalámbricos Acceso a Internet, Acceso a

Servicio ofrecidos por la OTIC, siendo éstos: Correo electrónico. Sistemas administrativos, misionales, estratégicos y de apoyo.

VI. Se prohíbe instalar servicios WEB, FTP, DHCP, DNS de correo o configurar una dirección IP no autorizada en los dispositivos conectados en red

VII. Se prohíbe realizar la instalación de equipos a la red institucional sin ser autorizado por la Oficina de Informática.

8. RESPONSABILIDADES Y FUNCIONES

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

Por tanto, la Unidad Administrativa Especial de la Justicia Penal Militar y Policial a través de la Oficina Asesora de Tecnologías de la Información 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:

8.1. PROPIETARIOS DE LA INFORMACIÓN:

Como partes designadas de la Entidad, en un cargo, proceso, o grupo de trabajo tienen las siguientes responsabilidades:

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

8.2. USUARIOS DE LOS ACTIVOS INFORMÁTICOS

Los cargos de nivel directivo o cuyos servidores de la Entidad que tengan a su cargo personal, entre los que se encuentran: Director General, Subdirector, Secretario General, Director de la Escuela de la JPMP, el Presidente del Tribunal Superior Militar y Policial, Fiscal General Penal Militar y Policial, Jefes de Oficina, Jueces, Fiscales, entre otros. Razón por la cual tienen la responsabilidad de conocer, divulgar, cumplir y hacer cumplir la presente Política.

8.3. LA OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Es responsable de asesorar al Director Ejecutivo en el establecimiento de una Política de Seguridad de la Información y apoyar el desarrollo de las siguientes funciones:

a. Revisar y proponer la Política de Seguridad de la Información para aprobación del Director Ejecutivo, así como las funciones generales en materia de seguridad Informática.
b. Apoyar el establecimiento e implementación de una metodología de análisis, evaluación y gestión de riesgos de activos informáticos.
c. 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.
d. 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 Unidad Administrativa Especial 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 Unidad Administrativa Especial de la Justicia Penal Militar y Policial, con el fin de mejorar la seguridad de la información.

e. Apoyar 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.
f. Formular soluciones tecnológicas para incrementar la seguridad informática, de acuerdo con las competencias y responsabilidades identificadas en la Entidad.
g. Formular metodologías y procesos específicos relativos a la seguridad informática.
h. Apoyar el desarrollo de la cultura organizacional en aspectos de seguridad informática como parte del proceso de planificación de la información.
i. Apoyar la formulación y seguimiento de planes de divulgación de la importancia de cumplir los objetivos de seguridad de la información.
j. Evaluar y coordinar la implementación de controles específicos de seguridad informática para nuevos sistemas o servicios.
k. Apoyar la difusión de la seguridad de la información dentro de la Entidad.
l. Apoyar los planes de recuperación y continuidad de servicios informáticos de la Entidad.
m. Apoyar las acciones tendientes a impulsar la implementación y cumplimiento de la Política de Seguridad de la Información.
n. 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.
o. Identificar y gestionar los requerimientos de seguridad informática para la operación, administración y comunicación de los sistemas y recursos de tecnología de la Entidad.
p. Realizar las tareas de desarrollo y mantenimiento de sistemas de información, siguiendo una metodología apropiada de ciclo de vida y que contemple las medidas de seguridad en todas sus fases.
q. 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.
r. 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.
s. Adelantar los procesos de selección de herramientas y proveedores en materia de seguridad informática.
t. 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.

u. Identificar los activos informáticos más críticos de la institución.
v. 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.
w. Promover la aplicación de auditorías enfocadas a la seguridad de la información.

8.4. LA OFICINA DE ADMINISTRACIÓN DE PERSONAL

En cumplimiento a la Política de Seguridad de la Información debe asesorar al Director Ejecutivo en:

a. Reportar las novedades de personal a la oficina de TIC: Vacaciones, permisos, retiros, traslados, comisiones, para que se tomen las acciones necesarias sobre los Sistemas de Información misional y de apoyo.
b. Notificar a todo el personal que ingresa a la Institución, de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información.

8.5. LA OFICINA ASESORA JURÍDICA

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

a. Asesorará en materia legal sobre los cambios o ajustes que se deban realizar a las Políticas de Seguridad de la Información de la Entidad.

b. Verificará el cumplimiento de la presente Política en la gestión de todos los contratos, acuerdos, convenios u otra documentación de la Entidad, con sus empleados y con terceros.

8.6. LA OFICINA DE CONTROL INTERNO DE GESTIÓN

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

a. 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.

b. 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.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., el 19 de julio de 2022

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