



Caja de Sueldos de Retiro
de la Policía Nacional

RESOLUCIÓN Nro.**DEL****"POR LA CUAL SE EXPIDE EL MANUAL DE POLÍTICAS Y ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CAJA DE SUELDOS DE RETIRO DE LA POLICÍA NACIONAL"****EL DIRECTOR GENERAL (E) DE LA CAJA DE SUELDOS DE RETIRO DE LA POLICÍA NACIONAL**

En ejercicio de las facultades legales y en especial, las conferidas en el Decreto 1019 del 1 de abril de 2004, en su artículo 3, numeral 4, y el artículo 21 del Acuerdo 008 de 2001;

CONSIDERANDO:

Que la Ley 23 del 28 de enero de 1982 *"Sobre derechos de autor"*, modificada por la Ley 1915 del 12 de julio de 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."*, establece disposiciones en materia de derecho de autor y derechos conexos.

Que la Ley 527 de 1999 (..) *"Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"*.

Que la Ley 1266 del 31 de diciembre de 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."*, busca respetar y hacer respetar la información contenida en las bases de datos personales.

Que la Ley 1273 del 5 de enero de 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"*, adiciona el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos".

Que la Ley Estatutaria 1581 del 17 de octubre de 2012, *"Por la cual se dictan disposiciones generales para la protección de datos personales"*, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.



Caja de Sueldos de Retiro
de la Policía Nacional

Que mediante la Ley Estatutaria 1712 del 6 de marzo de 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"*, con el fin de regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información, y se establecen los índices de clasificación o excepciones de acceso a la información.

Que el Decreto 1078 de 2015 Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, dispone en el artículo 2.2.9.1.2.1 que la Política de Gobierno Digital será definida por el MinTIC y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC.

Que el artículo 2.2.9.1.2.1 del Decreto 1078 de 2015, dispone que los habilitadores transversales de la Política de Gobierno Digital, corresponde a las capacidades que les permitan ejecutar las Líneas de Acción de la Política de Gobierno Digital y están compuestos por Arquitectura, Cultura y Apropiación, Seguridad y privacidad de la Información y Servicios Ciudadanos Digitales.

Que el Título 9, Políticas y Lineamientos de Tecnologías de la Información, Capítulo 1 del Decreto 1078 de 2015, Subrogado por el artículo 1 del Decreto 767 de 2022, Política de Gobierno Digital, artículo 2.2.9.1.1.2. establece que *"Los sujetos obligados a las disposiciones contenidas en el presente capítulo serán las entidades que conforman la administración pública en los términos del artículo 39 de la Ley 489 de 1998 (...)"*.

Que el Decreto 767 de 2022 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"* dispone al tenor del numeral 3.2 del artículo 2.2.9.1.2.1. que el habilitador transversal de la Política de Gobierno Digital, Seguridad y Privacidad de la Información *"(...) busca que los sujetos obligados desarrollen capacidades a través de la implementación de los lineamientos de seguridad y privacidad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos."*

Que para desarrollar el habilitador transversal de "Seguridad y Privacidad de la Información" el MINTIC expidió la Resolución 00500 de 2021 que establece los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establece los lineamientos y estándares para la estrategia de seguridad digital, a los sujetos obligados señalados en el artículo 2.2.9.1.1.2. del Decreto 1078 de 2015.

Que el artículo 5 de la norma en cita, establece que los sujetos obligados deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital.

Caja de Sueldos de Retiro
de la Policía Nacional

Dicha estrategia debe incluir en el Plan de Seguridad y Privacidad de la Información que se integra al Plan de Acción en los términos artículo 2.2.22.3.14. del capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, o la norma que la modifique, adicione, subrogue o derogue; como el Modelo de Seguridad y Privacidad de la Información – MSPI señalado en el Anexo 1 de la misma resolución, como habilitador de la política de Gobierno Digital, actualizado con la resolución 02277 de 2025.

Que mediante Resolución 001519 del 24 de agosto de 2020 “Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos”, se definen los lineamientos que deben atender los sujetos obligados para cumplir con la publicación y divulgación de la información señalada en la Ley 1712 del 2014, estableciendo los criterios para la estandarización de contenidos e información, accesibilidad web, seguridad digital, datos abiertos y formulario electrónico para Peticiones, Quejas, Reclamos, Sugerencias y Denuncias (PQRSD).

Que la Resolución 746 de 2022 del MinTIC, establece lineamientos adicionales a los establecidos en la Resolución número 500 de 2021, fortaleciendo el Modelo de Seguridad y Privacidad de la Información en los términos de adoptar medidas, al momento de adquirir productos y servicios de Seguridad Digital operados en entornos de nube, que garanticen el cumplimiento de lo dispuesto en la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias, en particular las relativas a la transferencia internacional de datos personales, así como la gestión de la seguridad de la información para las relaciones con los proveedores, determinando e implementando los controles para mitigar los riesgos asociados a la adquisición de productos y servicios de seguridad digital.

Que mediante Resolución 7501 de 2020 la Caja de Sueldos de Retiro de la Policía Nacional - CASUR adopta el Manual de Políticas y Administración de Seguridad de la Información, sin embargo, la entidad en el marco de la evaluación de dicha política y la evolución del marco normativo recomendó articularla teniendo en cuenta la actualización a la versión 2022 de la NTC-ISO/IEC 27001 base para la implementación del SGI, incluyendo buenas prácticas de seguridad digital para el manejo de los sistemas y tecnologías de información en la entidad, medidas de seguridad y privacidad efectivas para garantizar la integridad, confidencialidad, privacidad y disponibilidad de la información, lo que permite prevenir y gestionar riesgos asociados al uso del ciberespacio, la inteligencia artificial y de las herramientas tecnológicas en el cumplimiento de los objetivos de la entidad, integrando los lineamientos del MSPI y las políticas internas del Sistema Integrado de Gestión (SIG).

Que se hace necesario actualizar el **MANUAL DE POLÍTICAS Y ADMINISTRACIÓN DE SEGURIDAD DE LA INFORMACIÓN DE LA CAJA DE SUELDOS DE RETIRO DE LA POLICÍA NACIONAL**, con el fin de alinear con la normativa vigente y los estándares de seguridad actuales. Esta actualización busca mitigar riesgos emergentes y establecer protocolos claros en lo relacionado con compartir, utilizar, recolectar, procesar, intercambiar o consultar información de la entidad. Así como, garantizar el acceso seguro y controlado por parte de los entes de control y terceros vinculados, protegiendo los activos de información independientemente de su soporte, medio, formato o ubicación geográfica.



Caja de Sueldos de Retiro
de la Policía Nacional

En mérito de lo expuesto,

RESUELVE

ARTÍCULO 1. Expedir El Manual de Políticas y Administración de Seguridad de la Información de la Caja de Sueldos de Retiro de la Policía Nacional – CASUR, cuyo texto será el siguiente:

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO Y ALCANCE

Artículo 2. OBJETO. El presente manual tiene por objeto fijar los lineamientos y directrices de la Caja de Sueldos de Retiro de la Policía Nacional que garanticen la confidencialidad, integridad, disponibilidad, privacidad y legalidad de la información de la entidad.

Artículo 3. ALCANCE. El presente manual es aplicable a todos los servidores públicos y dependencias adscritas a la Entidad, bajo el direccionamiento de los subdirectores, jefes de oficinas asesoras, jefe Oficina de Control Interno y Unidad de Control Interno Disciplinario o quien haga sus veces, con el fin de garantizar las directrices definidas para la administración de su información.

Parágrafo. El presente manual deberá ser observado también por el personal de contratistas para el cumplimiento de sus obligaciones contractuales, proveedores y terceros intervinientes en aspectos relacionados con la Caja de Sueldos de Retiro de la Policía Nacional.

CAPÍTULO II
FUNDAMENTO Y PRINCIPIOS

Artículo 4. FUNDAMENTO. El Sistema de Gestión de Seguridad de la Información de la entidad, se fundamenta en el marco legal normativo y demás estándares internacionales en materia de seguridad de la información; incorporando los controles necesarios para contribuir al aseguramiento de la disponibilidad, integridad y confidencialidad de la información de CASUR.

ARTÍCULO 5. PRINCIPIOS. El Manual de políticas y administración de seguridad de la información de la Caja de Sueldos de Retiro de la Policía Nacional, estará enmarcado en los siguientes principios:

- a) **Confidencialidad:** la información es accesible solo para las personas autorizadas a tener acceso a ella. (ISO – International Organization for Standardization).
- b) **Integridad:** propiedad de la información para asegurar que los datos no sean alterados de manera no autorizada y que permanezcan coherentes y correctos a lo largo de su ciclo de vida. (ISO – International Organization for Standardization)



Caja de Sueldos de Retiro
de la Policía Nacional

- c) **Disponibilidad:** propiedad que asegura que la información es accesible y utilizable, cuando se requiera por personas autorizadas. (ISO – International Organization for Standardization)
- d) **Privacidad:** protege los datos personales y garantiza que se cumplan los derechos de privacidad de los individuos en el manejo de su información. (Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales).
- e) **Acceso:** los individuos tienen el derecho de acceder a la información que poseen las entidades públicas y privadas, siempre y cuando no existan restricciones legales o de privacidad. (Ley 1712 de 2014, la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).

TÍTULO II SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

CAPÍTULO I POLÍTICA GENERAL Y OBJETIVOS

Artículo 6. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN. La Caja de Sueldos de Retiro de la Policía Nacional, como entidad del sector defensa comprometida con la protección integral de los derechos de sus afiliados y el cumplimiento de su misión institucional, adopta e implementa el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001 y su anexo A, con el fin de proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y privacidad de la información en todos los niveles organizacionales.

Esta política se constituye en el marco rector del Sistema de Gestión de Seguridad de la Información (SGSI) de CASUR, promoviendo una gestión integral de activos, la identificación de riesgos y la implementación de controles organizacionales, de personas, físicos y tecnológicos que garanticen la prevención, detección y respuesta ante incidentes, así como la continuidad de los procesos misionales, estratégicos y de apoyo de la entidad.

Artículo 7. OBJETIVOS DE LA POLÍTICA GENERAL. El Sistema de Gestión de Seguridad de la Información de la entidad se adoptó mediante Resolución 5572 de 2017, tendrá los siguientes objetivos, los cuales aportan al cumplimiento de la Política General de Seguridad de la Información, así:

- a) Definir y actualizar el marco normativo interno en materia de seguridad y privacidad de la información, incorporando políticas, procedimientos y controles que aseguren la protección efectiva de los activos de información en concordancia con los cambios tecnológicos, normativos y operativos.
- b) Establecer y mantener un enfoque sistemático para la gestión de riesgos de seguridad de la información, evaluando de forma continua las amenazas, vulnerabilidades e impactos que puedan afectar la confidencialidad, integridad, disponibilidad, autenticidad o privacidad de la información.
- c) Prevenir y mitigar los impactos generados por incidentes de seguridad y privacidad de la información, fortaleciendo la capacidad de respuesta



Caja de Sueldos de Retiro
de la Policía Nacional

- institucional mediante procesos estructurados de detección, análisis, contención, recuperación y lecciones aprendidas.
- d) Implementar mecanismos de aseguramiento físico, lógico y organizacional que garanticen la aplicación efectiva de los principios de seguridad en todos los sistemas, plataformas, servicios y canales de comunicación utilizados por la entidad.
 - e) Establecer lineamientos claros para el manejo seguro de la información, tanto en soporte físico como digital, articulando el SGSI con la gestión documental institucional y promoviendo la clasificación, etiquetado, uso, almacenamiento, transmisión y eliminación segura de la información.
 - f) Fortalecer la cultura organizacional en torno a la seguridad de la información, a través de programas permanentes de concientización, capacitación, apropiación y evaluación, dirigidos a todos los grupos de interés internos y externos.
 - g) Cumplir con los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de datos.

CAPÍTULO II POLÍTICAS GENERALES ORGANIZACIONALES

Artículo 8. POLÍTICA DE GESTIÓN DE ACTIVOS DE INFORMACIÓN. La Caja de Sueldos de Retiro de la Policía Nacional, reconoce como activos de información todos los elementos, físicos y/o digitales, generados, almacenados o transformados por sus funcionarios, contratistas o proveedores en desarrollo de sus funciones o servicios contratados.

Los activos de información son de propiedad institucional y deberán utilizarse exclusivamente para fines laborales y misionales. Es importante indicar que CASUR identificará, clasificará y gestionará su inventario de activos conforme a la normatividad vigente y asegurando la protección, disponibilidad, integridad y confidencialidad de la información de la entidad. Dichos aspectos se construirán e impartirán teniendo en cuenta los siguientes criterios:

- a) **Inventario de Activos.** Los activos de CASUR deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. La entidad diseñará una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina.
- b) **Protección.** Con el objetivo de establecer los controles de seguridad físicos y digitales, los dueños de proceso y las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros establecidos.
- c) **Archivos de Gestión.** El Grupo de Información Documental, deberá implementar los controles necesarios para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental y Tablas de Control de Acceso, con el fin



Caja de Sueldos de Retiro
de la Policía Nacional

de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física de la entidad.

- d) **Sistema de gestión de documento electrónico de archivo- SGDEA.** El Grupo de Información Documental, con el apoyo del Grupo de Informática de CASUR, deberán implementar un sistema de gestión documental electrónica y de archivo digital, asegurando la conformación de expedientes electrónicos con características de integridad, disponibilidad y autenticidad de la información. Adicionalmente, para la emisión, recepción y gestión de comunicaciones oficiales, a través de los diversos canales electrónicos y físico, deberá asegurar un adecuado tratamiento archivístico.
- e) **Clasificación de la Información.** El Grupo de Informática en conjunto con el Grupo de Información Documental deberán establecer lineamientos para la clasificación y rotulado (etiquetado) de la información del Instituto, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014 (ley de transparencia y acceso a la información), esta última reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y en el Título 3 de la Parte 8 del Libro 2 del Decreto 1080 de 2015 y demás normativa que reglamente la clasificación de información de las entidades públicas del país.

Artículo 9. POLÍTICA DE CONTROL DE ACCESO. Con el propósito de proteger los activos de información, la Caja de Sueldos de Retiro de la Policía Nacional – CASUR, establecerá controles y procedimientos para el acceso a redes, sistemas de información e infraestructura tecnológica y física, mitigando riesgos de acceso no autorizado. Cada usuario institucional será responsable del uso adecuado de las credenciales asignadas y de la protección de la información a la que acceda. Se deberán implementar mecanismos de autenticación multifactor, administración de privilegios mínimos, control de sesiones y revisiones periódicas de permisos de acceso. Es preciso resaltar que es responsabilidad del Grupo de Informática implementar los mecanismos de asignación de los permisos y el Oficial de Seguridad de la Información garantizar el cumplimiento de dichos controles.

Artículo 10. POLÍTICA DE RELACIONES CON PROVEEDORES. La Caja de Sueldos de Retiro de la Policía Nacional (CASUR) establece las condiciones, responsabilidades y controles necesarios para garantizar la protección de la información institucional involucrada en las relaciones con terceros, contratistas o proveedores, previniendo su interceptación, copia, modificación, divulgación o destrucción no autorizada, así como los riesgos asociados a la adquisición de productos y servicios que puedan comprometer los principios de confidencialidad, integridad, disponibilidad y privacidad de la información.

Esta política aplica a todos los proveedores, contratistas y terceros que, en desarrollo de su relación contractual o comercial con CASUR, requieran acceder a la información institucional o a la infraestructura tecnológica de la Entidad. El Grupo de Gestión Contractual, en coordinación con el Oficial de Seguridad de la Información y la Oficina Asesora Jurídica, deberá establecer, documentar y supervisar las disposiciones necesarias para asegurar que toda información generada, procesada, custodiada, compartida o intercambiada durante la ejecución de contratos sea utilizada exclusivamente dentro del marco de las políticas de seguridad y privacidad de la información de la entidad.

Caja de Sueldos de Retiro
de la Policía Nacional

Asimismo, los supervisores de contratos, convenios o acuerdos serán responsables de verificar el cumplimiento de las políticas y procedimientos de seguridad y privacidad de la información por parte de los proveedores durante todas las fases contractuales: planeación, ejecución, seguimiento y cierre.

Parágrafo. Tratándose de relaciones contractuales de la entidad, estas disposiciones deberán ser incorporadas en los términos, cláusulas, minutas o acuerdos con los que se relacionen estos, a efectos de garantizar su implementación.

Artículo 11. POLÍTICA DE SEGURIDAD EN LA CONTINUIDAD DE LA OPERACIÓN. La Caja de Sueldos de Retiro de la Policía Nacional- CASUR, implementará y mantendrá planes y estrategias que garanticen la continuidad de la operación institucional y la restauración oportuna de los servicios críticos ante la ocurrencia de incidentes, fallas técnicas o desastres que afecten la infraestructura tecnológica o la disponibilidad de la información.

Esta política tiene como propósito asegurar que los aspectos relacionados con la seguridad y la privacidad de la información sean incorporados dentro de los planes de continuidad del negocio y recuperación ante desastres de la Entidad, protegiendo así la confidencialidad, integridad y disponibilidad de los activos de información en escenarios de contingencia.

El Plan de Continuidad Tecnológica de CASUR, incluirá el Análisis de Impacto al Negocio (BIA) y los Planes de Recuperación ante Desastres (DRP), los cuales deberán ser actualizados periódicamente y contener los requisitos mínimos de seguridad, tiempos de recuperación (RTO), puntos de recuperación (RPO) y procedimientos de validación de los servicios tecnológicos esenciales.

Artículo 12. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN. Esta política busca gestionar de manera adecuada los incidentes de seguridad y privacidad de la información y seguridad digital reportado en la entidad, dando cumplimiento al procedimiento establecido para dichos eventos. Lo anterior, aplica para todos los servidores públicos, contratistas o terceros que detecten un evento o incidente relacionado con la seguridad y privacidad de la información y seguridad digital, el cual deben reportar, adecuadamente, teniendo en cuenta el procedimiento establecido en la entidad.

El Oficial de Seguridad y Privacidad de la Información o la dependencia que haga sus veces, promoverá entre los servidores públicos, contratistas y terceros, el reporte y seguimiento de incidentes relacionados con la seguridad y privacidad de la información y seguridad digital. Así mismo, reportará a las autoridades correspondientes para el tratamiento de estos, quienes investigarán y cooperarán en la solución de los incidentes reportados, de acuerdo con el nivel de criticidad.

El Oficial de Seguridad de la Información, comunicara a la Dirección General de la entidad, los incidentes de seguridad de nivel crítico, para que éste en el marco de sus competencias, reporte e instaure las denuncias ante las autoridades pertinentes, tales como, Ministerio de Defensa Nacional, Policía Nacional, Fiscalía y/o entes de control.



Caja de Sueldos de Retiro
de la Policía Nacional

Parágrafo. La Dirección General o quien este delegue, será el único canal de comunicación autorizado para hacer pronunciamientos oficiales ante las entidades externas, medios de comunicación o la ciudadanía.

Artículo 13. POLÍTICA DE CUMPLIMIENTO. Esta política busca evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad y privacidad de la información, y de cualquier requisito de esta índole en la Entidad y asegurar que se revisen y actualicen periódicamente, como mínimo una vez al año o cuando se presente una actualización en la normatividad que afecte la seguridad y privacidad de la información. Esta será aplicada por todas las dependencias de la entidad.

El Oficial de Seguridad de la Información o quien haga de sus veces con apoyo de la Oficina Asesora Jurídica y su personal de apoyo, y la Oficina Asesora de Planeación, velarán por la identificación, documentación, cumplimiento y asesoría de los requisitos legales enmarcados en la seguridad y privacidad de la información y seguridad digital, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional.

CAPÍTULO III
POLÍTICAS GENERALES DE LOS RECURSOS HUMANOS

Artículo 14. POLÍTICA DE SEGURIDAD Y PRIVACIDAD EN EL RECURSO HUMANO. Esta política asegura que tanto los funcionarios como los contratistas comprendan las responsabilidades en los roles que ejercen en la Entidad y tomen conciencia respecto a la implementación de los lineamientos de seguridad y privacidad, con el fin de preservar la disponibilidad, integridad, privacidad y confidencialidad de la información de la entidad.

Para tal el efecto, el Grupo Talento Humano y el Grupo Adquisiciones y Contratos con el apoyo del Oficial de Seguridad de la Información o quien haga sus veces deberán:

- a) Desplegar esfuerzos para generar conciencia y apropiación en los empleados públicos de la entidad y contratistas, sobre sus responsabilidades con el fin de reducir los riesgos, el mal uso de los activos de información, y recursos tecnológicos y así asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información.
- b) Incluir en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y obligaciones, las cuales deberán ser divulgadas a través de los supervisores de los contratos, a proveedores y aquellas personas o terceros que, debido al cumplimiento de sus funciones, obligaciones y las de la entidad, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.
- c) Fomentar la participación de los servidores públicos de la entidad en las convocatorias, charlas o participaciones para el fortalecimiento de capacidades en seguridad digital realizadas por el Gobierno Nacional, organismos y por el Oficial de Seguridad de la Información o quien haga sus veces.

CAJA DE SUELDOS DE RETIRO DE LA POLICIA NACIONAL Fecha de Radicación: 22/12/2025 5:01:22 p. m.
IdControl: 982139
Radicado: 00036-202532794-CASUR
Folios: 9
Anexos: 0
De: ALVARO ANTONIO ARENAS MUÑOZ, DIRECTOR GENERAL (E) ENTIDAD DESCENTRALIZADA ADSCRITA DEL SECTOR DEFENSA
Para: OFICINA PLANEACION PLANEACION, COORDINACION GRUPO
Número Expediente:



Caja de Sueldos de Retiro
de la Policía Nacional

Parágrafo 1. Corresponde a los servidores públicos, sin importar su nivel jerárquico, a los contratistas de la entidad, según el caso, firmar un acuerdo de confidencialidad y no divulgación, según el tipo de vinculación, en lo que respecta a la información de la entidad. Dicho documento original será conservado y archivado en la historia laboral de los servidores públicos y en la carpeta de los procesos contractuales para el caso de los contratistas.

Parágrafo 2. En el caso de persona jurídica proveedora de servicios para la entidad, en la carpeta del contrato deberá reposar el acuerdo de confidencialidad y no divulgación debidamente diligenciada y suscrita por el representante legal.

CAPÍTULO IV

POLÍTICAS GENERALES PARA LA PROTECCIÓN FÍSICA

Artículo 15. POLÍTICA DE SEGURIDAD FÍSICA. La Caja de Sueldos de Retiro de la Policía Nacional, a través del Grupo de Gestión Logística y el Oficial de Seguridad de la Información, deberán adoptar medidas para la protección del perímetro de seguridad de las instalaciones físicas, para controlar el acceso y permanencia del personal tanto de servidores públicos, contratistas o terceros en las oficinas, instalaciones y áreas restringidas, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad, disponibilidad y privacidad de la información de la entidad.

Parágrafo 1. El Grupo de Gestión Logística o la dependencia que haga sus veces, en conjunto con el supervisor de la empresa contratante de vigilancia, deberán garantizar la protección de los datos semiprivados, privados o sensibles recolectados en el área de acceso a las instalaciones de la entidad de los servidores públicos, contratistas y/o visitantes.

Parágrafo 2. Los servidores públicos, contratistas y/o visitantes que se encuentren en las instalaciones físicas de la entidad deben estar debidamente identificados, con un carné, documento o distintivo que acredite el tipo de vinculación, en caso del carné, este debe portarse en un lugar visible y registrar el acceso a las dependencias o áreas que visiten.

Parágrafo 3. Los visitantes que se encuentren en las instalaciones de la entidad, deberán ser registrados por la empresa contratante de vigilancia, y siempre deben ser acompañados por un empleado de la empresa contratante de vigilancia, posteriormente será acompañado por el servidor público o contratista de la entidad debidamente identificado.

CAPÍTULO V

POLÍTICAS GENERALES DE TECNOLOGÍA

Artículo 16. POLÍTICA DE SEGURIDAD DE LAS OPERACIONES. Esta política busca asegurar la operación y administración de los recursos tecnológicos que soportan la operación de la entidad. Para el efecto el Grupo de Informática, velará por la eficiencia de los controles asociados a los recursos tecnológicos protegiendo la confidencialidad, integridad, disponibilidad y privacidad de la información.



Caja de Sueldos de Retiro
de la Policía Nacional

De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la entidad, al igual que desarrollará mecanismos de contingencias y recuperación ante desastres con el fin de propender por la disponibilidad de los servicios de TI en el marco de la operación de la entidad.

El Grupo de Informática deberá realizar y mantener copias de seguridad de la información de la entidad en medio digital, con el objetivo de recuperarla en caso de cualquier tipo de falla. Estas copias se realizarán, de acuerdo con el esquema definido previamente en un procedimiento que enmarque la gestión de las copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la entidad.

El diseño de este procedimiento se hará bajo la responsabilidad del Grupo de Informática, con el apoyo de los líderes de proceso y deberá estar alineado con la gestión documental de la entidad, con el fin de determinar la información a respaldar, la periodicidad, los tiempos de retención, recuperación, restauración y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

Artículo 17. POLÍTICA DE CRIPTOGRAFÍA. La Caja de Sueldos de Retiro de la Policía Nacional, implementará y utilizará herramientas y técnicas criptográficas como mecanismo de protección de la protección de la información, con el fin de garantizar la confidencialidad, integridad, disponibilidad y autenticidad de los activos de información. Estas medidas permitirán asegurar la gestión y transferencia segura de la información.

Artículo 18. POLÍTICA DE SEGURIDAD DE LAS COMUNICACIONES. El Grupo de Informática de CASUR, establecerá los controles para la administración de redes, comunicaciones y transferencia segura de información, con el fin de garantizar la confidencialidad y la integridad de los datos. Es preciso indicar, que toda transmisión de información entre CASUR y terceros deberá realizarse mediante canales cifrados y aprobados por la entidad.

Artículo 19. POLÍTICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS. Esta política tiene como objetivo asegurar que la seguridad digital esté incorporada en todas las etapas del ciclo de vida de los sistemas de información utilizados por CASUR, incluyendo aquellos que operan sobre redes públicas o en entornos tercerizados.

Toda adquisición, implementación o mantenimiento de sistemas deberá contar con la revisión y aval del Grupo de Informática, quien velará porque las soluciones cumplan con los requerimientos de seguridad necesarios para la protección de la información de la entidad, así como con los estándares de desarrollo, pruebas, puesta en producción y mantenimiento. Adicionalmente, el Grupo de Informática garantizará que toda solución tecnológica adquirida cumpla con los criterios de seguridad, mantenimiento, licenciamiento y compatibilidad con la infraestructura tecnológica de la Entidad.

En el marco del Plan Estratégico de Tecnologías de la Información – PETI, el Grupo de Informática es la única dependencia autorizada para adquirir, contratar, avalar y recibir software o soluciones tecnológicas, en atención a los



Caja de Sueldos de Retiro
de la Policía Nacional

requerimientos de las dependencias, asegurando su adecuada implementación, soporte y recuperación ante incidentes o fallos operativos.

Parágrafo. En caso de que alguna dependencia adquiera, desarrolle o realice mantenimientos a sistemas de información dentro del desarrollo misional u operacional de la entidad, deberá cumplir con lo establecido en la presente política.

Artículo 20. POLÍTICA DE SEGURIDAD DIGITAL. Esta política busca establecer un marco de referencia de gestión para iniciar y controlar la implementación de la seguridad digital al interior de la entidad por medio de la definición de roles y responsabilidades en seguridad digital, la separación de deberes, el contacto con las autoridades y grupos de interés y la incorporación de la seguridad digital en la gestión de los proyectos, todo ello alineado con la Política de Gobierno Digital y el Modelo de Seguridad y Privacidad de la Información definido por la entidad, buscando preservar la confidencialidad, integridad, privacidad y disponibilidad de la información.

Aplica a todos los servidores públicos o contratistas que hagan uso de los recursos tecnológicos de la entidad, que tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y, por ende, el cumplimiento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

1. Uso adecuado del correo electrónico institucional. El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los empleados públicos y contratistas de la entidad, cuyo uso es exclusivo para el ejercicio de sus funciones, por lo tanto, se deberán observar las siguientes directrices:

- Es considerado un activo de información y deberá ser inventariado clasificado y protegido conforme a su criticidad.
- Está alineado con los ejes del Modelo de Seguridad y Privacidad de la Información (MSPI), especialmente con la gestión de activos, control de accesos, seguridad en las comunicaciones y cumplimiento normativo.
- Requiere seguridad con doble factor de autenticación, máxime en aquellas circunstancias cuando estando fuera de las instalaciones y por razones del cumplimiento de sus funciones, requieran acceder a este.
- Se rige por los lineamientos de la Política de Gobierno Digital, Ley de Transparencia, Ley de Protección de Datos Personales y el Estatuto Disciplinario aplicable para servidores públicos.
- Cualquier uso indebido, sospecha de suplantación o acceso no autorizado debe reportarse de inmediato al Oficial de Seguridad de la Información o quien haga de sus veces y al Grupo de Informática para adelantar las actuaciones de su competencia.
- Será objeto de seguimiento por parte de los entes de control interno o externo. Tener presente que toda actividad queda registrada y puede ser utilizada como evidencia digital.

2. Corresponde a los funcionarios y contratistas de la Entidad acatar estrictamente las siguientes instrucciones de cara al uso adecuado del correo institucional:



Caja de Sueldos de Retiro
de la Policía Nacional

- a) Es de uso individual, responsable e intransferible.
- b) Debe emplearse únicamente para el desarrollo de las actividades propias del cargo o contrato.
- c) Cada funcionario es responsable conforme al usuario asignado, por la seguridad, confidencialidad y contenido de los mensajes enviados o recibidos.
- d) Los correos electrónicos de las dependencias y/o procesos, deben administrarse de forma segura, por ello, los mensajes de datos enviados y recibidos deben organizarse y conservarse de acuerdo con las tablas de retención documental y las políticas de archivo institucional.
- e) El usuario y contraseña son de carácter confidencial, por ello, deben ser renovados periódicamente y cumplir con criterios de robustez (caracteres y alfanumérica) y doble factor de autenticación.
- f) Abstenerse de enviar, reenviar o difundir mensajes de datos con contenidos que promuevan cadenas, que no estén relacionados con las funciones o actividades de la Entidad.
- g) Abstenerse de registrar o usar el correo electrónico institucional para uso meramente personal, familiar, así como, para afiliaciones, suscripciones a páginas web no autorizadas.
- h) Abstenerse de usar su cuenta institucional para registrarse en redes o medios sociales, indistintamente su naturaleza.
- i) Abstenerse de solicitar o compartir información reservada sin autorización expresa de la Entidad.
- j) Abstenerse de usarlo para fines personales, comerciales o ajenos a la Entidad.

3. Uso adecuado de Internet. La Caja de Sueldos de Retiro de la Policía Nacional (CASUR) provee el servicio de Internet como un recurso institucional destinado exclusivamente al desarrollo de funciones laborales, contractuales y misionales. Su uso estará restringido a actividades que estén directamente relacionadas con las funciones asignadas, de acuerdo con el rol del usuario, su jerarquía, y las autorizaciones formales emitidas por su jefe inmediato o supervisor al Oficial de Seguridad de la Información o quien haga de sus veces y activación por parte del Grupo de Informática de la entidad.

El uso adecuado de Internet deberá efectuarse de manera ética, responsable y segura, cumpliendo con los principios de confidencialidad, integridad, disponibilidad, legalidad y uso aceptable establecidos en el marco del Sistema de Gestión de Seguridad de la Información – SGSI, la Política de Seguridad de la Información, las normas legales vigentes.

El Grupo de Informática en coordinación con el Oficial de Seguridad de la Información o quien haga de sus veces, establecerán y gestionarán políticas de navegación basadas en categorías, horarios y niveles de usuario, determinados según criterios de necesidad, función y jerarquía. La entidad se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la entidad. Adicionalmente, se implementarán controles técnicos para la restricción y monitoreo del acceso, conforme a la capacidad tecnológica de la entidad.

Será responsabilidad de todos los funcionarios, contratistas o terceros que utilicen este servicio:



Caja de Sueldos de Retiro
de la Policía Nacional

- a) Utilizar el servicio de Internet únicamente para fines institucionales y en función de las tareas autorizadas, de acuerdo con su perfil de cargo y las instrucciones de su superior o supervisor.
 - b) Abstenerse de acceder, enviar, descargar o visualizar contenido ofensivo, discriminatorio, obsceno, ilegal, violento, injurioso o que atente contra la moral, la buena imagen institucional, los derechos de autor o los valores éticos de la Entidad.
 - c) No acceder a páginas web, aplicaciones o plataformas no autorizadas por el Grupo de Informática.
 - d) No enviar ni descargar software, archivos o contenidos de origen desconocido, no verificado o que puedan representar un riesgo para la seguridad digital de la entidad.
 - e) Abstenerse de propagar de manera intencional o negligente virus, malware, spyware, troyanos u otro tipo de código malicioso.
 - f) No utilizar herramientas, configuraciones o técnicas para eludir los controles de acceso o los filtros de navegación implementados por la Entidad.
 - g) Mantener una conducta proactiva en la detección y reporte de usos indebidos del servicio o intentos de acceso no autorizados.
4. Uso de los recursos tecnológicos institucionales: Los recursos tecnológicos asignados por la Caja de Sueldos de Retiro de la Policía Nacional (CASUR) son herramientas institucionales destinadas exclusivamente al cumplimiento de funciones propias del cargo o del contrato suscrito.

El Grupo de Informática, en coordinación con el Oficial de Seguridad de la Información o quien haga sus veces, establecerá los lineamientos y controles para garantizar el uso adecuado de los recursos tecnológicos, incluyendo computadores, portátiles, dispositivos móviles, periféricos, redes, software, herramientas colaborativas, medios de almacenamiento y plataformas digitales.

Todo funcionario, contratista o tercero autorizado deberá observar las siguientes disposiciones:

- a) Los bienes de cómputo asignados serán de uso exclusivo del funcionario o contratista y no podrán ser utilizados para fines personales ni por terceros no autorizados.
- b) Solo se permitirá el uso de software licenciado por la Entidad o de aquel expresamente aprobado por el Grupo de Informática.
- c) Toda la información institucional debe almacenarse exclusivamente en los repositorios oficiales habilitados por CASUR. Al finalizar el vínculo contractual o laboral, la información debe ser entregada al supervisor en dichos repositorios o carpetas compartidas.
- d) Se encuentra prohibido el almacenamiento de archivos personales (videos, música, imágenes) en los discos duros institucionales o carpetas compartidas, especialmente si vulneran derechos de autor o afectan la capacidad operativa.
- e) Es obligatorio utilizar las herramientas tecnológicas institucionales para la gestión de la información digital, evitando el uso de plataformas externas no autorizadas.
- f) Se prohíbe ingerir alimentos o bebidas en las áreas donde se encuentren elementos tecnológicos o documentos físicos que puedan verse comprometidos.

Caja de Sueldos de Retiro
de la Policía Nacional

- g) Las únicas personas autorizadas para modificar, reparar o manipular físicamente los recursos tecnológicos son las designadas por el Grupo de Informática.
- h) El uso de medios de almacenamiento externos (USB, discos externos, CD, etc.) serán autorizados mediante el procedimiento establecido por el Oficial de Seguridad de la Información o quien haga sus veces, y será habilitado, monitoreado y restringido por el Grupo de Informática para prevenir fugas de información y/o instalación de software no licenciado, propagación de virus o malware.
- i) El traslado físico de los recursos tecnológicos deberá ser realizado exclusivamente por el Grupo de Informática conforme al procedimiento de inventario institucional.
- j) Toda pérdida, daño o deterioro de equipos deberá ser reportado inmediatamente al Grupo de Informática. Si el equipo es propiedad de la entidad, también se notificará al Grupo de Almacén y Suministros para su trámite conforme a los procedimientos internos.
- k) La pérdida de información será considerada un incidente de seguridad y deberá reportarse de forma detallada al Oficial de Seguridad de la Información y el Grupo de Informática.
- l) Cualquier evento que comprometa la confidencialidad, integridad, disponibilidad o privacidad de la información deberá ser reportado de manera inmediata al Grupo de Informática y al Oficial de Seguridad de la Información o quien haga de sus veces, conforme al procedimiento de gestión de incidentes.
- m) El Grupo de Informática es la única dependencia autorizada para administrar, instalar o distribuir software institucional. Está prohibida su copia, cesión o uso con fines personales.
- n) Todo acceso a la red institucional mediante equipos no institucionales debe ser informado y controlado por el Grupo de Informática, bajo políticas de seguridad definidas.
- o) La conexión a la red Wi-Fi institucional deberá realizarse únicamente a través de los SSID definidos por el Grupo de Informática, mediante autenticación con usuario y contraseña institucional.
- p) La red Wi-Fi para visitantes será administrada por el Grupo de Informática, quien cambiará las credenciales periódicamente para garantizar la seguridad.
- q) El acceso a la red Wi-Fi por parte de equipos personales de funcionarios o contratistas estará condicionado a la validación de seguridad previa y a la capacidad técnica disponible.
- r) Los equipos de cómputo deberán permanecer apagados al final de la jornada laboral o cuando no estén en uso, salvo autorización para acceso remoto o labores programadas.
- s) Toda herramienta corporativa instalada en dispositivos personales será gestionada por el Grupo de Informática, quien garantizará la protección de la información institucional, conforme a las políticas vigentes y los principios de confidencialidad, integridad, disponibilidad y privacidad.
- t) Toda solicitud de acceso remoto mediante Red Privada Virtual (VPN) deberá realizarse conforme a los procedimientos establecidos por la entidad, previa autorización formal del jefe inmediato o supervisor responsable la subdirección u oficina asesora solicitante. Para el caso de VPN permanentes, con una duración no mayor a tres (3) meses, estas deberán ser aprobadas por el director general, con visto bueno del Oficial de Seguridad de la Información. En el caso de VPN temporales, requeridas para el desarrollo de comisiones o actividades específicas con duración



Caja de Sueldos de Retiro
de la Policía Nacional

inferior a quince (15) días, la aprobación corresponderá al Oficial de Seguridad de la Información. En ambos casos, la habilitación técnica del acceso será realizada únicamente por el Grupo de Informática, conforme a las validaciones de seguridad establecidas.

5. Uso de los sistemas o herramientas de información. Todo funcionario, contratista o tercero vinculado a la Caja de Sueldos de Retiro de la Policía Nacional - CASUR será responsable de la protección, custodia y uso adecuado de sus credenciales de acceso a los sistemas de información y recursos tecnológicos institucionales, conforme a los lineamientos establecidos en la Política de Control de Acceso y la normativa vigente sobre seguridad digital, para lo cual se dictan las siguientes directrices:

- a) Las credenciales de acceso (usuario y contraseña) asignadas para ingresar a los sistemas, redes, servicios y plataformas tecnológicas de CASUR son de uso estrictamente personal e intransferible. Está prohibido compartirlas, divulgarlas o usarlas en nombre de otra persona.
- b) Todos los usuarios deberán cambiar su contraseña periódicamente, siguiendo los parámetros definidos por el Grupo de Informática en cuanto a frecuencia, complejidad y robustez.
- c) Cada usuario será responsable de toda acción, registro, modificación o acceso realizado con su cuenta, siendo su deber reportar de forma inmediata cualquier sospecha de uso no autorizado o suplantación al Oficial de Seguridad de la Información o quien haga sus veces y al Grupo de Informática.
- d) En caso de ausencia laboral temporal o prolongada, deberá solicitarse el bloqueo preventivo de la cuenta de usuario ante el Grupo de Informática, a través de la cuenta de correo institucional o gestor de documental de la entidad. Esta medida aplica tanto para funcionarios como para contratistas, y su solicitud será responsabilidad del jefe inmediato o supervisor.
- e) El Grupo de Talento Humano deberá informar de forma oportuna cualquier novedad laboral (retiro, traslado, incapacidad prolongada, comisión) de los funcionarios que implique suspensión de accesos. Igualmente, el Grupo de Adquisiciones y Contratos deberán reportar las novedades contractuales que requieran suspensión o modificación de accesos a recursos tecnológicos.
- f) Al momento de finalizar el vínculo laboral o contractual, todos los privilegios, cuentas y accesos tecnológicos deberán ser suspendidos de forma inmediata. La información asociada será resguardada en los repositorios institucionales conforme a los procedimientos de custodia y conservación definidos por la Entidad.
- g) El jefe inmediato o supervisor del usuario retirado será responsable de garantizar la custodia de la información institucional, así como la cesión de derechos de uso y propiedad intelectual, en concordancia con la legislación vigente y las cláusulas contractuales aplicables.
- h) El retiro del personal deberá gestionarse conforme al procedimiento de paz y salvo institucional, en el cual se dejará constancia del cierre de accesos tecnológicos y la entrega de la información pertinente.
- i) La solicitud de acceso se realizará a través del formato de gestión de usuarios será de uso obligatorio para todos los servidores públicos y contratistas de la Caja de Sueldos de Retiro de la Policía Nacional - CASUR. Este deberá ser diligenciado para los trámites de activación, desactivación o actualización de cuentas de usuario, tanto al inicio como al término de



Caja de Sueldos de Retiro
de la Policía Nacional

la vinculación, o ante cualquier novedad administrativa que implique cambios en los privilegios de acceso. La autorización de dichos trámites corresponderá al Oficial de Seguridad de la Información, quien autorizará y validará la pertinencia de los accesos solicitados. Una vez el formato haya sido firmado y autorizado por el Oficial de Seguridad de la Información o quien haga sus veces, será remitido a través de la herramienta de gestión de activos y servicios de TI (GLPI), el Grupo de Informática será el encargado de realizar la activación, inactivación o modificación técnica de los accesos.

Artículo 21. POLÍTICA PARA EL USO RESPONSABLE DE LA INTELIGENCIA ARTIFICIAL. La Caja de Sueldos de Retiro de la Policía Nacional, promoverá el uso responsable, ético, transparente y seguro de tecnologías basadas en Inteligencia Artificial (IA) en el desarrollo de sus funciones misionales, científicas, técnicas y administrativas exclusivamente como fuente de consulta y no como gestor de la actividad misional. Esta política busca garantizar que la implementación de soluciones de IA respete los derechos fundamentales, la protección de datos personales, la seguridad de la información y los principios de equidad, no discriminación.

Parágrafo 1. Toda iniciativa, proyecto o sistema que utilice algoritmos de IA deberá ser evaluado previamente por Grupo de Informática en coordinación con el Oficial de Seguridad de la Información o quien haga sus veces y la Oficina Asesora Jurídica y las áreas funcionales involucradas, para verificar su alineación con los principios institucionales, la normativa vigente y los estándares internacionales en ética digital.

Parágrafo 2. Corresponde a la entidad asegurar que los sistemas de IA utilizados o desarrollados por la entidad cuenten con mecanismos de trazabilidad, supervisión humana, gestión de riesgos y documentación técnica que permita explicar sus decisiones y resultados.

Parágrafo 3. Se prohíbe el uso de herramientas de IA que comprometan la confidencialidad, integridad o disponibilidad de la información institucional, que generen sesgos injustificados, o que no cuenten con licenciamiento, validación técnica o respaldo legal por las dependencias correspondientes.

Parágrafo 4. La capacitación del talento humano en el uso ético y seguro de la IA será promovida como parte de la cultura institucional de innovación y transformación digital dentro de la entidad.

TÍTULO III
DISPOSICIONES FINALES

Artículo 22. DESIGNACIÓN DEL OFICIAL DE SEGURIDAD DE LA INFORMACIÓN. El director general de la Caja de Sueldos de Retiro de la Policía Nacional - CASUR designará el funcionario y asignará las funciones que ejercerá el Oficial de Seguridad de la Información, en los términos definidos en la presente resolución.

Artículo 23. REVISIÓN Y ACTUALIZACIÓN. El Oficial de Seguridad de la Información o quien haga de sus veces, como responsable del Sistema de Gestión de Seguridad de la Información, será el encargado de revisar,

CAJA DE SUELDOS DE RETIRO DE LA POLICIA NACIONAL Fecha de Radicación: 22/12/2025 5:01:22 p. m.
IdControl: 982139
Radicado: 00036-202532794-CASUR
Folios: 9
Anexos: 0
De: ALVARO ANTONIO ARENAS MUÑOZ, DIRECTOR GENERAL (E) ENTIDAD DESCENTRALIZADA ADSCRITA DEL SECTOR DEFENSA
Para: OFICINA PLANEACION PLANEACION, COORDINACION GRUPO
Número Expediente:



Caja de Sueldos de Retiro
de la Policía Nacional

implementar los controles que contribuyan a la aplicación de las mejores prácticas de seguridad de la información y proponer las actualizaciones al presente manual.

Artículo 24. PUBLICIDAD. La presente resolución deberá ser publicada en la pagina web de la entidad.

Artículo 25. VIGENCIA. La presente Resolución rige a partir de la fecha de su publicación y deroga las demás disposiciones que le sean contrarias, en especial la Resolución 7501 de 2020.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C.

Coronel (RP) ALVARO ANTONIO ARENAS MUÑOZ

Director General (E) Caja de Sueldos de Retiro de la Policía Nacional

Elaboró: OPS Ronald Ricardo Ruiz Velásquez - OAD
OPS William Jerez Beltrán - OAD
Revisó: OPS Julián Andrés Medina - OAP
PD. Bibiana León Beltrán - OAP
Claudia Cecilia Chauta Rodríguez - OAJ
Aprobó: César Ovidio Castro Guerrero - OAP
Fecha de elaboración: 19/12/2025