



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

(MSPI) MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD (SEGURIDAD DIGITAL)

ELABORÓ	REVISÓ	APROBÓ
Nombre: Mauricio Ruiz Castaño Cargo: Líder Gestor SGSI y Ciberseguridad Fecha: 18/May/2021	Nombre: Paola Inés Arellana Cargo: Líder Mejora Continua Fecha: 18/May/2021 Nombre: Ronald Mauricio Cely Espitia Cargo: Gerente Oficial de Seguridad de la Información y Ciberseguridad Fecha: 18/May/2021	Nombre: Comité Institucional de Gestión y Desempeño – Versión 5 Fecha: 26/Ene/2021 Nombre: Secretaría General – Clara Isabel Vega Rivera. – Versión 6 Fecha: 18/May/2021

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

8 POLÍTICAS ESPECÍFICAS (MSPI) PARA LA GESTIÓN DE CIBER-SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

8.1 POLÍTICA DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

8.1.1 INTRODUCCIÓN

El artículo 15 de la Constitución Política de Colombia, explica la protección de datos personales como el derecho de toda persona para conocer, actualizar, rectificar y/o cancelar la información y datos personales que de ella se hayan recolectado y/o se traten en bases de datos públicas o privadas.

Así mismos, mediante la Ley 1581 del 17 de octubre de 2012, el Congreso de la República reglamentó el ya mencionado derecho al establecer las Disposiciones Generales para la Protección de Datos Personales en Colombia, igualmente reglamentada por los Decretos 1377 de 2013 y 886 de 2014 (hoy incorporados en el Decreto único 1074 de 2015), entre otros.

En cumplimiento e implementación de las anteriores disposiciones Servicios Postales Nacionales, consecuente con la responsabilidad que les asiste en materia de Tratamiento de Datos Personales y Políticas De Tratamiento De Datos Personales, garantiza el derecho constitucional que tienen todas las personas a conocer, actualizar, rectificar, suprimir y revocar la autorización respecto a las informaciones que hayan recogido sobre ellas en las bases de datos que la entidad ha recopilado para las finalidades previstas en la Ley y las autorizaciones respectivas, las cuales han sido tratadas conforme a lo establecido por el régimen nacional de protección de datos personales.

Para el correcto cumplimiento y ejecución de todo lo precedente Servicios Postales Nacionales ha elaborado a través del presente documento la Política Para El Tratamiento De Datos Personales, es válido resaltar que el presente documento es de carácter obligatorio para todas las personas naturales o jurídicas que hagan tratamiento de los datos personales registrados en las bases de datos de la Entidad, para así dar cumplimiento a los lineamientos legales.

Así las cosas, Servicios Postales Nacionales le comunica a todos los interesados, que los datos personales que obtenga en virtud de las transacciones, negociaciones, contrataciones, y demás circunstancias que se soliciten o celebren con la entidad, serán tratados conforme a los principios y deberes definidos en la ley 1581 de 2012 y demás normas que traten y regulen esta materia.

Para todos los fines pertinentes, de Servicios Postales Nacionales S.A. Servicios Postales Nacionales S.A., identificado con el número de Nit. 900062917. Cuyos datos de contacto son: Dirección: Diagonal 25G # 95A - 55 Bogotá (Cundinamarca). Teléfono: (571) 4722005, sitio Web: WWW.4-72.COM.CO, correo electrónico habeasdata@4-72.com.co

8.1.2 DESTINATARIOS

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

El presente documento contiene la política de tratamiento de datos personales de la entidad Servicios Postales Nacionales, se aplicará a todas las bases de datos tanto físicas como digitales, que contengan datos personales y que sean objeto de tratamiento por parte de Servicios Postales Nacionales, quien para efectos del presente documento se denominará el responsable. Igualmente, en aquellos casos en que operen como encargadas del tratamiento de datos personales.

El presente documento va encaminado a que los titulares de la información en general tengan alcance y claridad respecto los diferentes tratamientos y fines sobre los que serán objeto sus datos personales, así mismo, tendrán la posibilidad de conocer y ejercer los diferentes derechos que tienen como titulares de la información frente a Servicios Postales Nacionales, cuando esta tenga el rol de responsable del tratamiento de sus datos personales.

La presente política es de obligatorio conocimiento y cumplimiento para todas las personas naturales o jurídicas responsables de la administración de bases de datos personales Servicios Postales Nacionales, en especial los administradores del manejo de estas bases de datos

8.1.3 OBJETO

El presente documento actualiza la Política de Tratamiento de Datos Personales de Servicios Postales Nacionales, con el fin de asegurar una adecuada gestión Institucional.

8.1.4 ÁMBITO DE APLICACIÓN.

La presente Política aplica a los datos personales que reposan en bases de datos y/o archivos que se encuentren en poder de la Entidad, de los servidores públicos, contratistas, operadores, clientes, terceros y todas aquellas personas naturales o jurídicas que tengan algún tipo de relación con Servicios Postales Nacionales, y que de conformidad con la normatividad vigente sean objeto de tratamiento.

Servicios Postales Nacionales en relación con el tratamiento de los datos personales da por entendido que los mismos son propiedad de los titulares, y solo hará uso de aquellos para la finalidad manifiesta al titular. Se exceptúan de este alcance los casos establecidos por el artículo 2o de la Ley 1581 de 2012 y las normas que lo modifiquen, deroguen o subroguen.

8.1.5 OBJETIVO GENERAL DE LA POLÍTICA.

El objetivo general de la presente Política es establecer los lineamientos para garantizar el adecuado cumplimiento de lo dispuesto en la Ley 1581 de 2012 y en el Decreto 1074 de 2015, y la gestión en materia de tratamiento de datos personales.

8.1.6 OBJETIVOS ESPECÍFICOS DE LA POLÍTICA

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

Los objetivos específicos de la presente Política son:

- a. Dar a conocer el responsable del tratamiento de los datos personales que gestiona Servicios Postales Nacionales S.A., en ejecución de sus funciones y como usuario de la información que requiere de los particulares y/o de otros entes del Estado, también en ejecución de sus funciones.
- b. Adoptar los lineamientos generales para el tratamiento de los datos personales administrados por Servicios Postales Nacionales S.A., en cumplimiento de la normatividad vigente sobre la materia.
- c. Establecer el tratamiento al cual son sometidos los datos personales en Servicios Postales Nacionales S.A., y su finalidad.
- d. Definir los procedimientos generales para que los titulares de la información puedan ejercer los derechos a conocer, actualizar, rectificar, suprimir información y revocar la autorización de tratamiento de datos personales en los casos que la ley lo permita.
- e. Establecer los criterios que permitan clasificar Servicios Postales Nacionales la información de carácter personal en cumplimiento de la Ley 1712 de 2014 y al mismo tiempo respetar los derechos fundamentales a la Intimidad, Hábeas data y Protección de datos de los ciudadanos.

8.1.7 PRINCIPIOS RECTORES

Con base en la interpretación y aplicación de la ley 1581 de 2012 y demás normas concordantes, la presente política de tratamiento de datos personales se regirá por los siguientes principios:

- a. **Principio de Legalidad en Materia de Tratamiento de Datos:** El Tratamiento es una actividad reglada que debe sujetarse a lo establecido en la Ley 1581 del 17 de octubre de 2012, decretos reglamentarios y demás disposiciones que la desarrollen.
- b. **Principio de Finalidad:** El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- c. **Principio de Libertad:** El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.
- d. **Principio de Veracidad o Calidad:** La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de Datos parciales, incompletos, fraccionados o que induzcan a error.
- e. **Principio de Transparencia:** En el Tratamiento debe garantizarse el derecho del Titular a obtener del responsable del Tratamiento o del Encargado del Tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.
- f. **Principio de Seguridad:** La información sujeta a Tratamiento por el responsable del Tratamiento o Encargado del Tratamiento a que se refiere la ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- g. **Principio de temporalidad:** Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir las finalidades que justificaron el tratamiento,

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

atendiendo a las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Una vez cumplida la finalidad del tratamiento y los términos establecidos anteriormente, se procederá a la supresión de los datos.

8.1.8 POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

8.1.8.1 Protección de datos personales

La presente Política de Tratamiento ha sido desarrollada teniendo en cuenta lo dispuesto por la Ley Estatutaria 1581 de Protección de datos personales, en adelante LEPD, y su desarrollo reglamentario y será aplicable a todas las bases de datos y/o archivos que contengan datos personales objeto de tratamiento por el responsable del Tratamiento.

Cumpliendo con los requerimientos recogidos en la LEPD relativos a la solicitud de la autorización en el tratamiento de los datos, todo aquel titular que facilite información relativa a sus datos personales, mediante la aceptación o con conocimiento de la presente política, están consintiendo el tratamiento de sus datos por parte de Servicios Postales Nacionales, S.A. (4-72) en los términos y condiciones recogidos en la misma en la misma.

8.1.8.2 Responsable del Tratamiento

El responsable del tratamiento es la persona natural o jurídica, pública o privada que por sí misma o en asocio con otros, decide sobre la base de datos y/o tratamiento de los datos.

En este sentido, el responsable del tratamiento de la base de datos identificada a continuación es **Servicios Postales Nacionales S.A.**, identificado con el número de Nit. 900062917. Cuyos datos de contacto son: Dirección: Diagonal 25G # 95A - 55 Bogotá (Cundinamarca). Teléfono: (571) 4722005, sitio Web: WWW.4-72.COM.CO, correo electrónico habeasdata@4-72.com.co

PARÁGRAFO. El Encargado será la persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del Ministerio/Fondo Único de TIC, y tendrá la obligación de cumplir lo establecido en esta política acorde con la normatividad vigente en materia de protección de datos personales.

1. DEFINICIONES



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Con el objeto de facilitar la lectura y comprensión de la presente política de tratamiento se reflejan las definiciones relativas a conceptos específicos de la protección de datos en general.

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

Aviso de privacidad: Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se informa acerca de la existencia de las políticas de Tratamiento de la información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretende dar a los datos personales.

Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión y oficio y a su calidad de comerciante o servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos sensibles: Se entiende por datos sensibles aquellos que afectan a la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Encargado del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del Tratamiento.

Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o tratamiento de datos.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es Responsable del Tratamiento y se encuentra dentro o fuera del país.

Transmisión: Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un Tratamiento por el Encargado por cuenta del responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Área responsable de la atención a peticiones, quejas, reclamos y consultas: Las peticiones, quejas, reclamos y consultas formuladas por los titulares de datos serán atendidas por el proceso de Servicio al Cliente a través de la Jefatura Nacional de PQR, quien a su vez pasara las diferentes solicitudes al área jurídica, los cuales tendrán un apoyo jurídico a través de la figura la Gestora de Protección de Datos, adscrita a la misma.

Base De Datos: Conjunto organizado de Datos Personales que sean objeto de tratamiento. Incluye archivos físicos y electrónicos.

Calidad Del Dato: El dato personal sometido a tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. Cuando se esté en poder de datos personales parciales, incompletos, fraccionados o que induzcan a error, Servicios Postales Nacionales se abstendrá de someterlos a Tratamiento, o solicitara a su titular la completitud o corrección de la información.

Confidencialidad: Elemento de seguridad de la información que permite establecer quienes y bajo qué circunstancias pueden acceder a la misma.

Dato Personal: Cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables. **Debe entonces entenderse el “dato personal” como una información relacionada con una persona natural** (persona individualmente considerada).

Información Digital: Toda aquella información que es almacenada o transmitida por medios electrónicos y digitales como el correo electrónico u otros sistemas de información.

Líder Nacional de Protección de Datos Personales y Privacidad de la Información: Dependencia o rol que asume dentro de Servicios Postales Nacionales, que depende y reporta al (CISO) Gerente Oficial de Seguridad de la Información y Ciberseguridad; cuya función es la de articular y velar por la implementación y el cumplimiento de los lineamientos para la protección de datos personales y asesorar a las demás áreas la gestión del trámite a las solicitudes de los titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012, sus decretos reglamentarios y las Circulares Externas expedidas por la Superintendencia de Industria y Comercio, resoluciones y decretos del MinTic en materia de protección de datos y por las directrices establecidas de la Alta dirección y demás normas o disposiciones que la modifiquen, complementen o reemplacen.

Profesional Oficial de Protección de Datos Personales: Es la persona o rol dentro de Servicios Postales Nacionales, que depende del Líder Nacional de protección de datos personales y privacidad de la información, que tiene como función u obligación, velar por la implementación efectiva de las políticas y procedimientos adoptados para cumplir la norma de protección de datos personales, así como la implementación de buenas prácticas de gestión de datos personales y privacidad de la información dentro de la Entidad, bajo la orientación y lineamientos del Líder Nacional de Protección de datos personales y las directrices establecidas por la Alta dirección.



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Anonimización: un “dato anónimo” no permite razonablemente establecer a qué persona natural se refiere, vincula o asocia, entonces dicha información no es un dato personal. Los datos personales que hayan sido objeto de procesos de anonimización, cifrado, presentados con un seudónimo o que por cualquier medio, tecnología o proceso se desvinculan o desasocian de una persona natural, pero que puedan utilizarse para volver a identificar a esa persona, siguen siendo datos personales.

2. CATEGORÍAS ESPECIALES DE DATOS

Datos Sensibles. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Tratamiento De Datos Sensibles

Se prohíbe el Tratamiento de datos sensibles, excepto cuando:

- a. El Titular haya dado su autorización explícita a dicho Tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- b. El Tratamiento sea necesario para salvaguardar el interés vital del Titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- c. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- d. El Tratamiento tenga una finalidad histórica, estadística o científica.

En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los titulares.

Autorización Especial De Datos Personales Sensibles

Servicios Postales Nacionales S.A. informará a través de los diversos medios de obtención de la autorización a todos sus titulares, que en virtud de la ley 1581 del 2012 y normas reglamentarias estos poseen un carácter facultativo respecto de los datos sensibles, es decir que no están obligados a otorgar la autorización para el tratamiento de mencionados datos.

En caso de tratamiento de datos relativos a la salud, Servicios Postales Nacionales S.A, implementará las medidas necesarias para proteger la confidencialidad de la información. Los datos sensibles biométricos tratados tienen como finalidad la identificación de las personas, la seguridad, el cumplimiento de obligaciones legales y la adecuada prestación de los productos.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Derechos de los Niños, Niñas y Adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes parámetros y/o requisitos:

- Que respondan y respeten el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales.

Cumplidos los anteriores requisitos, el representante legal de los niños, niñas o adolescentes otorgará la autorización, previo ejercicio del menor de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Los datos personales de los menores de 18 años, salvo aquellos que por su naturaleza son públicos en los términos de la Ley 1581 de 2012, pueden ser objeto de tratamiento siempre y cuando el fin que se persiga con dicho tratamiento responda al interés superior de los niños, las niñas y adolescentes y se asegure sin excepción alguna el respeto de sus derechos prevalentes en el marco de la Ley 1098 de 2006 o cualquiera que la adicione, modifique, derogue o subrogue.

3. FINALIDADES GENERALES PARA LA RECOLECCIÓN Y TRATAMIENTO DE DATOS PERSONALES

En todos los casos los datos personales podrán ser tratados con la finalidad de adelantar los procesos comerciales de contratación y vinculación de diferentes aliados, bajo la oferta y demanda del desarrollo del objeto comercial de la entidad a nivel Nacional e internacional.

La finalidad de la Política de Protección de Datos Personales busca:

1. Instrumentar los procedimientos de recolección y tratamiento de datos personales a las disposiciones de la ley.
2. Generar un esquema organizado para salvaguardar los datos privados, semiprivados, públicos y sensibles de sus titulares.

De acuerdo con lo establecido en la Ley 1581 de 2012 y de conformidad con las autorizaciones impartidas por los titulares de la información, Servicios Postales Nacionales S.A. realizará operaciones o conjunto de operaciones que incluyen recolección de datos, su almacenamiento, uso, circulación y/o supresión.

Este Tratamiento de datos se realizará exclusivamente para las finalidades autorizadas y previstas en la presente Política y en las autorizaciones específicas otorgadas por parte del titular. De la misma forma se realizará Tratamiento de Datos Personales cuando exista una obligación legal o contractual para ello, siempre bajo los lineamientos de las políticas de Seguridad de la Información contemplada en las "Políticas De Seguridad De La Información



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

y Ciberseguridad, Contempladas en el Documento Manuel De Políticas De Ciberseguridad De La Información”, Así mismo y en ejecución del objeto social de Servicios Postales Nacionales S.A., los datos personales serán tratados de acuerdo con el grupo de interés y base de datos aplicables, de acuerdo a su naturaleza y descripción de la finalidad y en proporción a las finalidades que tenga cada tratamiento, como se describe a continuación:

Clientes:

Busca llevar a sus usuarios información y beneficios del uso continuo de sus servicios, así como la prestación de servicios de envío de paquetería, correos y todo lo relacionado con el objeto de que desarrolle la entidad. Por consiguiente, es necesario recolectar este tipo de información, en pro del crecimiento empresarial, la realización de contratos, negociaciones y ejecución de funciones y objeto de la entidad, adicional a ello se obtiene una medición de los servicios prestados, que permiten realizar una mejora continua en la prestación de los diferentes servicios ofrecidos por la entidad, el Usuario acepta que de Servicios Postales Nacionales S.A. y sus aliados, ejecuten las siguientes finalidades:

- Que lo contacten por diferentes canales como teléfono fijo, teléfono celular, mensajes de texto a su celular, correo electrónico y redes sociales, para ofrecerle información y beneficios
- Remisión de las respuestas de las consultas y derechos de petición a los peticionarios.
- Adelantar los trámites, servicios y otros procedimientos administrativos que sean solicitados a la Entidad.
- Actualizar bases de bases de datos, Incluyendo los casos en que se requiera transmitir o transferir a un tercero, la información, para la validación, depuración, enriquecimiento y homogenización de datos, previo cumplimiento de las exigencias legales.
- Manejo de la información por parte de proveedores y/o contratistas para las gestiones relacionadas con tramites y servicios definidos en sus respectivos vínculos con la Entidad y siempre que ello sea estrictamente necesario.
- Elaborar estudios, estadísticas, encuestas, análisis de tendencias, relacionados con los servicios que presta la entidad.
- Presentar informes a entidades externas, tales como, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, Superintendencia de Industria y Comercio, Procuraduría General de la Nación, Fiscalía General de la Nación, entre otras, que permitan dar cumplimiento a las exigencias legales y a análisis estadísticos requeridos a la Entidad.
- Gestionar la información necesaria para el cumplimiento de las obligaciones tributarias, contractuales, comerciales y de registros comerciales, corporativos y contables.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

- Transmitir, transferir y/ realizar una interoperabilidad de la información a encargados nacionales o internacionales con los que se tenga una relación operativa que provean los servicios necesarios para la debida operación de la Entidad.
- Prestar los servicios de información a través de los diferentes medios de contacto
- Evaluar la calidad de los servicios prestados a través de encuestas de diferentes tipos.
- Recolección de grabación de imágenes, imágenes, registros de datos físicos o sistematizados, datos biométricos o cualquier otro registro que sirva de soporte y evidencia de los eventos, control de acceso y demás funcionalidades que pueda captar la entidad
- Mejorar y ofrecer las iniciativas, servicios y productos promocionales de la oferta y portafolio de prestación de servicios, como de actualización de productos y servicios de la Entidad.
- Las demás finalidades que se determinen en procesos de obtención de Datos Personales para su tratamiento, y en todo caso de acuerdo con la Ley y en el marco de las funciones que lo son atribuibles a Servicios Postales Nacionales

Funcionarios:

Es necesario para la entidad recolectar los datos personales de los funcionarios, en pro de las finalidades descritas a continuación, toda vez que, con ello, se maneja un control de funcionarios contratados, la definición de sus roles y cumplimiento de la ley transparencia, así mismo, es una cobertura de cumplimiento legal a nivel laboral.

- Realizar las actividades necesarias para dar cumplimiento a las obligaciones legales en relación con los funcionarios y exfuncionarios de la entidad.
- Controlar el cumplimiento de requisitos relacionados con el Sistema General de Seguridad Social.
- Publicar el directorio corporativo con la finalidad de contacto de los empleados.
- En caso de datos biométricos capturados a través de sistemas de videovigilancia o grabación su tratamiento tendrá como finalidad la identificación, seguridad y la prevención de fraude interno y externo.
- Los datos personales de menores serán tratados con la finalidad de dar cumplimiento a las obligaciones legales.
- Para el caso de los participantes en convocatorias de selección, los datos personales tratados tendrán como finalidad adelantar las gestiones de los procesos de selección; las hojas de vida se gestionarán garantizando el principio de acceso restringido
- Gestionar la cadena presupuestal de la Entidad: pagos de la Entidad, emisión de certificados de ingresos y retenciones (personas naturales y jurídicas) y relaciones de pagos.

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

- Gestionar el proceso Contable de la Entidad.

Empleados:

Esta finalidad incluye específicamente los pagos de salarios y obligaciones como empleador de las afiliaciones y aportes a seguridad social y cajas de compensación, tanto de los empleados como de sus familiares y control de novedades laborales como permisos, incapacidades, control de acceso y horario de trabajo del empleado.

Todos los datos suministrados por los empleados serán almacenados, compilados, utilizados, compartidos, consultados, transmitidos, intercambiados y transferidos, para dar cumplimiento a las obligaciones derivadas de la relación laboral y al ejercicio de los derechos como empleador.

Toda la información relativa a los empleados o exempleados es necesario recolectarla ya que serán conservados con el fin de que la Compañía, pueda cumplir sus obligaciones como empleador y ejercer los derechos que en esa misma condición le corresponden, de acuerdo con la legislación laboral colombiana.

Al momento del ingreso a Servicios Postales Nacionales de empleados nuevos con contrato laboral, es requisito que, al momento del inicio de sus labores asignadas, manifiesten conocer, aceptar y aplicar las Políticas de Protección de Datos Personales.

Proveedores y/o contratistas:

Es necesaria la recolección de los datos personales de los proveedores bajo las siguientes finalidades, toda vez que es impajaritable el contacto permanente para solicitud de cotizaciones y gestión de las relaciones comerciales que surjan, con el objeto de adquirir sus productos o servicios como insumos para el funcionamiento según la razón social de Servicios Postales Nacionales S.A. así mismo:

- Para todos los fines relacionados con el objeto de los procesos de selección, contractuales o relacionados con éstos.
- Realizar todos los trámites internos y el cumplimiento de obligaciones contables, tributarias y de ley.
- Gestionar la cadena presupuestal de la Entidad: pagos de la Entidad, emisión de certificados de ingresos y retenciones (personas naturales y jurídicas) y relaciones de pagos.
- Gestionar el proceso Contable de la Entidad.
- Realizar todas las actividades necesarias para el cumplimiento de las diferentes etapas contractuales en las relaciones con proveedores y contratistas.
- Expedir las certificaciones contractuales solicitadas por los contratistas de la Entidad o solicitudes de los entes de control



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

- Mantener un archivo digital que permita contar con la información correspondiente a cada contrato.
- Las demás finalidades que se determinen en procesos de obtención de Datos Personales para su tratamiento, y en todo caso de acuerdo con la Ley y en el marco de las funciones que lo son atribuibles a Servicios Postales Nacionales.

Visitantes:

Servicios Postales Nacionales S.A. recibe en sus instalaciones y con poca frecuencia cantidades mínimas de visitantes, sin embargo, la información que suministran estos o que se obtienen de las imágenes o videos de las cámaras de seguridad son de necesaria recolección para crear un control de acceso, el cual es registrado por parte del área de la Dirección Nacional de Seguridad Postal / Seguridad Electrónica, en el ingreso de las instalaciones a través de una plantilla o cámaras de video vigilancia, buscando obtener control frente a posibles eventos o incidentes de seguridad física e identificación de las personas que son autorizadas para su ingreso a las instalaciones de la entidad.

4. BASE DE DATOS Y FINALIDADES

Servicios Postales Nacionales, S.A. (4-72) en el desarrollo de su actividad procede al tratamiento, o lo que es lo mismo, la recolección, almacenamiento, uso, circulación. supresión de una serie de datos personales relativos a personas naturales. Dichos datos personales son tratados a través de una serie de bases de datos destinadas, en todo caso, a finalidades legítimas de acuerdo con la Constitución y la Ley.

A continuación, se identifican tales bases de datos, junto con las finalidades asignadas a cada una de ellas con base en el Decreto 1377 de 2013 en su artículo 4° que habla sobre la recolección de los datos personales de la siguiente forma:

“... A solicitud de la Superintendencia de Industria y Comercio, los responsables deberán proveer una descripción de los procedimientos usados para la recolección, almacenamiento, uso, circulación y supresión de información, **como también la descripción de las finalidades para las cuales la información es recolectada y una explicación sobre la necesidad de recolectar los datos en cada caso...**”

BASE DE DATOS	DESCRIPCION DE LAS FINALIDADES	FINALIDAD	NECESIDAD DE RECOLECCION DE DATOS
PQR	Base de datos que contiene información para la gestión de las peticiones, quejas y reclamaciones presentadas por los usuarios de los servicios de 4-72. De acuerdo con	Ejecución del derecho de Habeas Data, ejercido por los titulares de los datos personales, descrito en el art. 15 de la Constitución Política de Colombia.	Goce y disfrute del derecho de habeas data y cumplimiento de las obligaciones como responsable de la información



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

	la ley Estatutaria 1581 de protección de datos personales el interesado autoriza que sus datos, el titular presta su consentimiento para que sus datos, facilitados voluntariamente pasen a formar parte de una base de datos cuyo responsable es 4-72 siendo tratados con la finalidad de gestionar su solicitud, medición de satisfacción y en base a la política de tratamiento.	Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	
Cientes Naturales	Tratamiento de datos personales, en pro de ofertar servicios y medir la satisfacción de los servicios prestados en pro de la una mejora continua del catálogo ofertado por la entidad	Información de clientes en puntos de venta. Transmitir, transferir y/ realizar una interoperabilidad de la información a encargados nacionales o internacionales con los que se tenga una relación operativa que provean los servicios necesarios para la debida operación de la entidad. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Califica el personal de la empresa y el catálogo de servicios ofertados y permite la oferta y creación de nuevos servicios
Cientes Corporativos	Base de datos en la que se registra información de clientes Corporativos de SPN con una negociación actual y con información general y de contacto	Tratamiento de datos personales en pro de la ampliación económica de la entidad a través de la ejecución de contratos y licitaciones. Transmitir, transferir y/ realizar una interoperabilidad de la información a	Mantiene un estándar financiero y corporativo y a su vez permite una ampliación comercial y económica de la entidad



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

		<p>encargados nacionales o internacionales con los que se tenga una relación operativa que provean los servicios necesarios para la debida operación de la Entidad.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	
Proveedores	<p>Base de datos que alberga información necesaria para la contratación de servicios y/o productos a proveedores, así como la remisión de información sobre productos, servicios y actividades promovidos por la entidad.</p>	<p>Tratamiento de datos personales que buscan ampliar un catálogo de aliados comerciales en aras de ampliar la oferta del catálogo de servicios.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	<p>Ampliación de la misión y visión de la empresa a través de diferentes aliados</p>
Gestión humana (Nomina)	<p>Base de datos de trabajadores que alberga información necesaria para la gestión y operación de la entidad.</p>	<p>Tratamiento de datos personales, necesarios para cuantificar y calificar la calidad y la preparación de los empleados contratados por la entidad.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	<p>Protección de la entidad, frente a circunstancias de cumplimiento de índole legal-laboral</p>
Hojas de vida personal contratado	<p>Base de datos que alberga información necesaria para llevar a cabo procesos de selección promovidos por la entidad.</p>	<p>Tratamiento de datos personales dirigidos a la contratación efectiva de profesionales, administrativos,</p>	<p>Necesarios para cuantificar y calificar la calidad y la preparación de los empleados</p>



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

		directivos, técnicos y cargos operativos.	contratados por la entidad
Maestro personal retirado	Base de datos que alberga personal retirado de la entidad	<p>Tratamiento de datos personales en pro de conservar la trazabilidad de las diferentes personas que han prestado su conocimiento y tiempo dentro de la entidad.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	Protección de la entidad, frente a circunstancias de cumplimiento de índole legal-laboral
Videovigilancia	Bases de datos que almacenan imágenes audiovisuales del ingreso y salida de empleados y personas para la sede principal de la ciudad de Bogotá. Para determinar la cantidad de los titulares: (x) horas de grabación del DVR (de cámaras en porterías o recepción de sedes) x cantidad de personas que se graben durante (2) horas, en horario pico de operación (2 horas pico seleccionadas del horario 8am-6:00 pm). Sobre la cantidad de personas que se graben durante (2) horas en horario valle (se estima entre 12:00 pm a 2:00pm).	<p>Obtener el registro de imágenes o videos de las personas que ingresan a las diferentes instalaciones de la entidad a nivel Nacional.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	Conservar los registros de imágenes o videos en pro de la seguridad física de la entidad y posible soporte probatorio
Clientes Casillero Virtual	Base de Datos que contiene Clientes de Casillero Virtual.	<p>Prestación de servicio de mensajería internacional.</p> <p>Transmitir, transferir y/ realizar una interoperabilidad de la información a</p>	Ampliación comercial de la entidad, traspasando fronteras



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

		<p>encargados nacionales o internacionales con los que se tenga una relación operativa que provean los servicios necesarios para la debida operación de la Entidad.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	
Aplicación 472	<p>Recopilar información de clientes que acceden y utilizan los servicios de la aplicación móvil 472.</p>	<p>Prestación de servicios de giros electrónicos.</p> <p>Transmitir, transferir y/ realizar una interoperabilidad de la información a encargados nacionales o internacionales con los que se tenga una relación operativa que provean los servicios necesarios para la debida operación de la Entidad.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	<p>Ampliación de la ejecución del portafolio financiero de la entidad</p>
Consolidado Pagos Auxilios Sindicales Convención Colectiva	<p>Consolidar los registros de pagos por auxilios educativos y de formación del personal sindicalizado</p>	<p>Clasificar cuantitativa y cualitativamente el personal sindicalizado en pro de ejecutar sus derechos y obligaciones.</p> <p>Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.</p>	<p>Método probatorio del cumplimiento legal-laboral de la entidad</p>



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Base Área De Reserva	Base de clientes área de reserva con información de contacto de los clientes para realizar gestión comercial.	Ampliación de oferta del portafolio empresarial. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Determinar y verificar la demanda y la oferta de los productos empresariales
Base Clientes Cámara Comercio De Bogotá	Registros de clientes prospecto adquiridos a la Cámara de Comercio de Bogotá, para ofrecer los productos de SPN.	Tratamiento de datos de potenciales clientes vinculados a la cámara de comercio. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Ampliación comercial de los productos de la entidad a través de acuerdos contractuales
Base rezagos (mes al cual corresponda)	Dar cumplimiento a las exigencias de la resolución Control de gestión de los envíos	Control y verificación de envíos y entregas retrasadas. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Administración y control de la entrega efectiva de los envíos
Base contratos masivos	Llevar control de los contratos vigentes de la unidad de Masivos, como fecha de inicio, fecha de terminación, fechas de prorrogas, adiciones, saldos y lo demás requerido de información de los contratos	Recolección y entrega de paquetes y envíos de forma masiva a determinados clientes. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Cumplimiento contractual de entrega y envío masivo de paquetes
Base de datos Estadística de incautaciones	Reportar mensualmente a torre de control la información referente a las incautaciones realizadas por la Policía	Control y reporte de incautaciones de la policía antinarcóticos. Y demás finalidades generales indicadas en	Cumplimiento del deber legal recopilación de medio probatorios



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

	Antinarcóticos que se generaron en la unidad de exportaciones durante el mes, esta información se consolida para reportar al MINTIC.	la presente política de tratamiento de datos personales.	
Base de datos Cambios de modalidad e inmovilización	Reportar mensualmente a torre de control la información referente a los cambios de modalidad e inmovilizaciones que se generaron luego de la inspección de la DIAN en la unidad de importaciones durante el mes a reportar, esta información se consolida para reportar al MINTIC	Control y reporte de inmovilizaciones ante la Dian. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Cumplimiento del deber legal de reportar ante la entidad competente las irregularidades en la unidad de importaciones
Base de datos Reporte de abandonos	Reportar a la DIAN el informe de los envíos que fueron declarados en abandono legal para su gestión y fines pertinentes	Verificación y reporte de los envíos declarados en abandono para ser reportados ante la Dian. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Identificación y reporte de envío y paquetes abandonados en pro de cumplir los lineamientos y procedimientos destinados para este fin
Contratistas Transporte	Mantener actualizados los datos de contacto de cada uno de los proveedores que manejan un contrato de servicios con la Entidad y que está bajo la supervisión de la vicepresidencia de operaciones.	Tratamiento de datos personales de los diferentes contratistas encargados del área de transporte. Y demás finalidades generales indicadas en la presente política de tratamiento de datos personales.	Necesaria para el correcto control y funcionamiento de la flota de transporte de la entidad.

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

5. TRANSMISIÓN, TRANSFERENCIA E INTEROPERABILIDAD DE DATOS PERSONALES.

Servicios Postales Nacionales, podrá transferir y transmitir los datos personales a terceros con quienes tenga relación operativa que le provean de servicios necesarios para su debida operación, o de conformidad con las funciones establecidas a su cargo en las leyes.

En dichos supuestos, se adoptarán las medidas necesarias para que las personas que tengan acceso a sus datos personales cumplan con la presente Política y con los principios de protección de datos personales y obligaciones establecidas en la Ley.

En conclusión Servicios Postales Nacionales, exclusivamente para el desarrollo de sus objetivos y funciones legales, podrá transmitir a los operadores de los distintos programas e iniciativas, datos personales que haya recolectado y tenga bajo su custodia, quienes suscribirán un contrato de transmisión de datos en los términos del artículo 2.2.2.25.5.2 del Decreto 1074 de 2015, o la norma que lo modifique, subrogue o derogue, así como, realizar la transferencia de información a los entes de control o aquellos estipulados en la ley o cualquiera que indique un mandato judicial, de igual manera, aportando a la transformación digital del Estado, se podrá realizar intercambio de información en el marco de la interoperabilidad con otras entidades, previa suscripción de un documento tipo acuerdo entre las partes que lo formalice.

Sin perjuicio de lo descrito en el artículo 2.2.2.25.5.2 del Decreto 1074 de 2015, Servicios Postales Nacionales, transmitirá los datos a uno o varios encargados ubicados dentro o fuera del territorio de la República de Colombia, establecerá cláusulas contractuales o celebrará un contrato de transmisión de datos personales en el que indicará:

1. Alcances del tratamiento,
2. Las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y,
3. Las obligaciones del Encargado para con el titular y el responsable.

Mediante dicho contrato el Encargado se comprometerá a dar aplicación a las obligaciones del responsable bajo la política de Tratamiento de la información fijada por este y a realizar el tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables vigentes

Además de las obligaciones que impongan normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado:

- a) Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan.
- b) Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales.
- c) Guardar confidencialidad respecto del tratamiento de los datos personales

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

En caso de transferencia se dará cumplimiento a las obligaciones estipuladas en la Ley 1581 de 2012 y normas reglamentarias.

6. DERECHOS DEL TITULAR DE LA INFORMACION Y CONDICIONES DE LEGALIDAD PARA EL TRATAMIENTO DE DATOS

Habeas data. Constitución Política de Colombia. 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 los 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.

Así las cosas, y con base en el mandato constitucional el titular de la información que reposa en Servicios Postales Nacionales podrá consultar de forma gratuita sus datos personales: al menos una vez cada mes calendario, y cada vez que existan modificaciones sustanciales de las Políticas de Tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, Servicios Postales Nacionales, S.A. (4-72) solo podrá cobrar al titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, Servicios Postales Nacionales, S.A. (4-72) deberá demostrar a la SIC, cuando ésta así lo requiera, el soporte de dichos gastos.

Los titulares de los datos, es decir, las personas naturales cuyos datos personales son objeto de tratamiento por parte de Servicios Postales Nacionales, S.A. (4-72) podrán ejercer una serie de derechos en relación con el tratamiento de sus datos personales, los cuales son analizados más adelante.

Estos derechos son considerados de carácter personalísimo, es decir, solo podrán ser ejercidos por las siguientes personas:

- Por el titular, quien deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
- Por sus causahabientes, quienes deberán acreditar tal calidad.
- Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.

Los derechos de los niños, niñas o adolescentes se desarrollarán por las personas que estén facultadas para representarlos.

Derechos de los Titulares

En el Tratamiento de Datos Personales por parte de Servicios Postales Nacionales, se respetarán en todo momento los derechos de los titulares de Datos Personales que son:



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

- a) Conocer, actualizar y rectificar los Datos frente a él o los Encargados del Tratamiento de datos.
- b) Solicitar prueba de la autorización otorgada, o cualquier otra que suscriba el titular de los Datos Personales para el efecto, salvo cuando expresamente se exceptúe como requisito para el Tratamiento de datos de conformidad con la ley.
- c) Ser informado por la Entidad o el Encargado del Tratamiento, previa solicitud, respecto del uso que se le ha dado a los datos.
- d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la presente ley y las demás normas que la modifiquen, adicionen o complementen.
- e) La revocatoria y/o supresión procederá cuando la Autoridad Competente haya determinado que, en el Tratamiento Servicios Postales Nacionales o Encargados del Tratamiento de Datos Personales, han incurrido en conductas contrarias a la ley y a la Constitución. La revocatoria procederá siempre y cuando no exista la obligación legal o contractual de conservar el dato personal.
- f) Acceder en forma gratuita a los Datos Personales que hayan sido objeto de Tratamiento
- g) Abstenerse de diligenciar cualquier instrumento de recolección de datos personales que no cumpla con el marco legal sobre datos personales.

7. AUTORIZACIÓN DEL TITULAR

Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento se requiere la autorización previa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta posterior. Se entenderá que la autorización cumple con estos requisitos cuando se manifieste:

- (i) por escrito
- (ii) de forma oral
- (iii) mediante conductas inequívocas del titular que permitan concluir de forma razonable que otorgó la autorización, como cuando, por ejemplo, se remite a la Entidad una hoja de vida para participar en procesos de selección o cuando se ingresa a las instalaciones a sabiendas de la existencia de sistemas de videovigilancia.

NOTA: En lo que respecta a las conductas inequívocas, es ineludible que dentro de todas las instalaciones de la entidad en sitio público y visible se exponga un aviso de seguridad y privacidad de la información, el modelo del mismo debe ser ceñido a la normatividad por tanto su modelo será proyectado y creado por el Gerente Oficial de Seguridad de Información y Ciberseguridad y/o la Líder de Protección de Datos Personales.

Así mismo, dentro del presente documento se anexa a modo de ejemplo un modelo de autorización del que trata el presente numeral, el cual cuenta con los requisitos exigidos por la ley 1581 de 2012, el Decreto 1377 de 2013 y la Resolución 924 de 2020 del MinTic y demás normas que la adicionen o complementen, para que sea válida.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

De igual manera si los responsables de los procesos y subprocesos como de las áreas de Servicios Postales Nacionales S.A., considera pertinente la implementación del anexo que se referencia a modo de ejemplo, se comunica que todo formato de autorización debe estar debidamente revisado y aprobado, como de su publicación a través de la plataforma tecnológica del Sistema Integrado de Gestión de la Entidad.

En la Ley 1581 de 2012 en su artículo 12 precisa: “Deber de informar al Titular. El responsable del Tratamiento, al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa lo siguiente:

- a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo;
- b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes;
- c) Los derechos que le asisten como Titular;
- d) La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento.

Parágrafo. El responsable del Tratamiento deberá conservar prueba del cumplimiento de lo previsto en el presente artículo y, cuando el Titular lo solicite, entregarle copia de esta”.

Ahora bien, en el Decreto 1377 de 2013 en su artículo 5° nos indican la forma específica en que se debe recolectar la finalidad del tratamiento de la siguiente forma. Autorización. El responsable del Tratamiento deberá adoptar procedimientos para solicitar, a más tardar en el momento de la recolección de sus datos, la autorización del Titular para el Tratamiento de los mismos e informarle los datos personales que serán recolectados, así como todas las finalidades específicas del Tratamiento para las cuales se obtiene el consentimiento.

... En caso de haber cambios sustanciales en el contenido de las políticas del Tratamiento a que se refiere el Capítulo III de este decreto, referidos a la identificación del responsable y a la finalidad del Tratamiento de los datos personales, los cuales puedan afectar el contenido de la autorización, el responsable del Tratamiento debe comunicar estos cambios al Titular antes de o a más tardar al momento de implementar las nuevas políticas. Además, deberá obtener del Titular una nueva autorización cuando el cambio se refiera a la finalidad del Tratamiento...

Sí tiene dudas al diligenciar el formulario anexo, comuníquese con el Gerente Oficial de Seguridad de la Información y Ciberseguridad y/o la líder de Protección de Datos Personales.

Casos en que no es necesaria la autorización del titular:

- a) Información requerida por la Entidad, en ejercicio de sus funciones legales o por orden judicial.
- b) Datos de naturaleza pública.
- c) Casos de urgencia médica o sanitaria.
- d) Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- e) Datos relacionados con el Registro Civil de las Personas.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la Ley 1581 de 2012 y demás normas concordantes y vigentes.

Suministro de la Información

La información solicitada por los Titulares de información personal será suministrada principalmente por medios electrónicos, o por cualquier otro solo si así lo requiere el Titular.

La información suministrada por Servicios Postales Nacionales será entregada sin barreras técnicas que impidan su acceso; su contenido será de fácil lectura, acceso y tendrá que corresponder en un todo a aquella que repose en la base de datos.

Deber de Informar al Titular

Servicios Postales Nacionales al momento de solicitar al Titular la autorización, deberá informarle de manera clara y expresa los siguientes:

- a) El Tratamiento al cual serán sometidos sus datos personales y la finalidad del mismo.
- b) El carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas versen sobre datos sensibles o sobre los datos de las niñas, niños y adolescentes.
- c) Los derechos que le asisten como titular.
- d) La identificación, dirección física o electrónica y teléfono del responsable del Tratamiento

Servicios Postales Nacionales, como responsable del Tratamiento, deberá conservar prueba del cumplimiento de lo previsto en el presente numeral y, cuando el Titular lo solicite, entregarle copia de esta.

Personas a quienes se les puede suministrar la Información

La información que reúna las condiciones establecidas en la ley podrá ser suministrada a las siguientes personas:

- a) A los Titulares y/o sus causahabientes quienes deberán acreditar su identidad en forma suficiente por los medios que Servicios Postales Nacionales le ponga a disposición.
- b) A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial.
- c) A los terceros autorizados por el titular o por la ley
- d) Por el representante y/o apoderado del titular, previa acreditación de la representación o apoderamiento.
- e) Por estipulación a favor de otro o para otro.
- f) Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

8. DEBERES DE LOS RESPONSABLES DEL TRATAMIENTO Y ENCARGADOS DEL TRATAMIENTO

Deberes de los Responsables del Tratamiento

Servicios Postales Nacionales, como responsable del tratamiento, deberá cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el Titular.
- c) Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- d) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- e) Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
- f) Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
- g) Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.
- h) Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.
- i) Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
- j) Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
- k) Adoptar procedimientos específicos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
- l) Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- m) Informar a solicitud del Titular sobre el uso de sus datos.
- n) Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- o) Cumplir las instrucciones y requerimientos que Imparta la Superintendencia de Industria y Comercio.
- p) Anonimizar los datos personales de los titulares siempre que estos sean de carácter semiprivados, privados o sensibles, así como los datos de los niños, niñas y adolescentes de cualquier tipo.

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

Deberes de los Encargados del Tratamiento.

Los Encargados del Tratamiento, y en el evento en el cual Envíos Nacionales de Colombia, actúe como encargado, deberán cumplir los siguientes deberes, sin perjuicio de las demás disposiciones previstas en la ley y en otras que rijan su actividad:

- a) Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- b) Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso.
- c) Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la Ley 1581 de 2012 y demás normas concordantes y vigentes.
- d) Actualizar la información reportada por los responsables del Tratamiento dentro del término establecido por la ley y la presente política respecto de cambios sustanciales y no sustanciales.
- e) Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en la presente política.
- f) Adoptar un Manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.
- g) Registrar en las bases de datos la leyenda "reclamo en trámite" en la forma en que se regula en la ley.
- h) Insertar en la base datos de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- i) Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- j) Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
- k) Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
- l) Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
- m) Verificar que el responsable del Tratamiento tiene la autorización para el tratamiento de datos personales del Titular.

9. ACCIONES GENERALES PARA LA PROTECCIÓN DE DATOS PERSONALES

A continuación, se establecen los lineamientos generales aplicados por Servicios Postales Nacionales con el fin de efectuar con sus obligaciones en cumplimiento de los principios para la administración de datos personales.

Estos lineamientos son complementarios a las políticas, procedimientos o instructivos generales actualmente existentes e implementados, entre las que se encuentran las



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

políticas de gestión de datos e información y el procedimiento gestión de datos e información y en ningún momento pretenden remplazarlas o desconocerlas.

Tratamiento de la Información.

Todos los miembros de la Entidad, al realizar las actividades propias de su cargo, asumirán las responsabilidades y las obligaciones que se tienen en el manejo adecuado de la información personal, desde su recolección, almacenamiento, uso, circulación y hasta su disposición final.

Servicios Postales Nacionales, como responsable del tratamiento de los datos personales contenidos en las bases de datos y/o archivos que gestiona, realizará la recolección a través de medios físicos o digitales, almacenamiento en infraestructura tecnológica o archivos físicos, uso para las finalidades específicas en diferentes medios, circulación permitida en el marco normativo y administración de los mismos de acuerdo a las políticas de operación, sin permitir en ningún caso el acceso a la información por terceros salvo en casos expresamente previstos en la ley, ni la violación de derechos de los titulares, con el fin de:

- a. Permitir el desarrollo del objeto de Servicios Postales Nacionales S.A., en los términos del parágrafo 1º del artículo 38 de la Ley 489 de 1998, las cuales de acuerdo con los artículos 85, 86, y 93 de la Ley 489 de 1998, desarrollan sus actividades conforme a las reglas de derecho privado con las excepciones que consagre específicamente la ley. o las normas que los modifiquen, subroguen o deroguen.
- b. Desarrollar los estudios previos y procesos de selección para la contratación oficial Servicios Postales Nacionales S.A., destinada a garantizar el funcionamiento de la entidad y la ejecución de proyectos y el desarrollo de esquemas de gerencia de proyectos.
- c. Realizar la selección, contratación y/o vinculación de servidores públicos, empleados, funcionarios, y contratistas de prestación de servicios de la entidad.
- d. Formular, ejecutar y evaluar los programas de salud ocupacional y planes de atención a emergencias.
- e. Mantener actualizada la historia laboral y registros de nómina de funcionarios y empleados, de Servicios Postales Nacionales.
- f. Atender y resolver peticiones, quejas, reclamos, consultas y sugerencias.
- g. Conservar evidencia de los eventos realizados, audiencias de adjudicación de contratos, reuniones internas y externas.
- h. Atender requerimientos de información de entes de control tanto internos como externos.
- i. Efectuar la convocatoria y generar evidencia de la realización de sesiones de rendición de cuentas y participación ciudadana.
- j. Medir y realizar seguimiento a los niveles de satisfacción de los usuarios de los servicios de Servicios Postales Nacionales S.A., a través de encuestas.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

- k. Registrar y/o autorizar el ingreso a las instalaciones principales y/o cualquier edificación que sea utilizada para cumplir la misión de Servicios Postales Nacionales S.A.
- l. Realizar análisis de seguridad para garantizar la protección de las personas y los bienes materiales que se encuentren en las instalaciones referidas en el literal k de este numeral.
- m. Realizar monitoreo a través de sistemas de videovigilancia para mitigar riesgos de seguridad física y del entorno en el perímetro e instalaciones de la sede principal de Servicios Postales Nacionales S.A., o cualquier edificación que sea utilizada para cumplir la misión de mencionada entidad.
- n. Anonimizar los datos personales de los titulares, siempre que estos así lo soliciten en pro del principio de confidencialidad, y/o cuando esos datos sean de carácter semiprivados, privados o sensibles, así como los datos de los niños, niñas.

Uso de la Información.

La información de carácter personal contenida en las bases de datos debe ser utilizada y tratada de acuerdo con las finalidades descritas en la presente política y las que se amplíen en cada caso en particular (contratos y demás) con cada titular de los datos personales.

En caso de que algún área identifique nuevos usos diferentes a los descritos en la presente política de tratamiento de datos personales, deberá informar al Oficial de Protección de Datos Personales, quien evaluará y gestionará, cuando aplique, su inclusión en la presente política.

Igualmente, se deben tomar en consideración los siguientes supuestos:

- a. En caso de que un área diferente de la que recolectó inicialmente el dato personal requiera utilizar los datos personales que se han obtenido, ello se podrá hacer siempre que se trate de un uso previsible por el tipo de servicios que ofrece la Entidad y para una finalidad contemplada dentro de la presente Política de Tratamiento de Datos Personales.
- b. Cada área debe garantizar que en las prácticas de reciclaje de documentos físicos no se divulgue información confidencial ni datos personales. Por lo anterior, no se podrán reciclar hojas de vida, ni títulos académicos, ni certificaciones académicas o laborales, ni resultados de exámenes médicos ni ningún documento que contenga información que permita identificar a una persona.
- c. En caso de que un encargado haya facilitado datos personales o bases de datos a algún área para un fin determinado, el área que solicitó los datos personales no debe utilizar dicha información para una finalidad diferente de la relacionada en la Política de Tratamiento de Datos Personales; al finalizar la actividad, es deber del área que solicitó la información, eliminar la base de datos o los datos personales utilizados evitando el riesgo de desactualización de información o casos en los cuales durante ese tiempo un titular haya presentado algún reclamo.
- d. Los funcionarios no podrán tomar decisiones que tengan un impacto significativo en la información personal, o que tengan implicaciones legales, con base



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

exclusivamente en la información que arroja el sistema de información, por lo que deberán validar la información a través de otros instrumentos físicos o de manera manual, y, si es necesario, de manera directa por parte del titular del dato, en los casos en que así sea necesario.

- e. Únicamente los funcionarios y contratistas autorizados pueden introducir, modificar o anular los datos contenidos en las bases de datos o documentos objeto de protección. Los permisos de acceso de los usuarios son concedidos por la Oficina de Tecnología e Informática, de acuerdo con los perfiles establecidos, los cuales serán previamente definidos por los líderes de los procesos donde se requiera el uso de información personal.
- f. Cualquier uso de la información diferente al establecido, será previamente consultado con el Oficial de Protección de Datos Personales.

Almacenamiento de la Información.

El almacenamiento de la información digital y física se realiza en medios o ambientes que cuentan con adecuados controles para la protección de los datos. Esto involucra controles de seguridad física e informática, tecnológicos y de tipo ambiental en áreas restringidas, en instalaciones propias y/o centros de cómputo o centros documentales gestionados por terceros.

Destrucción

La destrucción de medios físicos y electrónicos se realiza a través de mecanismos que no permiten su reconstrucción. Se realiza únicamente en los casos en que no constituya el desconocimiento de norma legal alguna, dejando siempre la respectiva trazabilidad de la acción.

La destrucción comprende información contenida en poder de terceros como en instalaciones propias.

Procedimiento de Gestión de Incidentes con datos personales

Se entiende por incidencia cualquier anomalía que afecte o pudiera afectar la seguridad de las bases de datos o información contenida en las mismas.

En caso de conocer alguna incidencia ocurrida, el usuario debe comunicarla al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y/o al Líder Nacional de Protección de Datos Personales, a través de los correos electrónicos: csirt@4-72.com.co, habeasdata@4-72.com.co que adoptará las medidas oportunas frente al incidente reportado.

El Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y/o el Líder Nacional de Protección de Datos Personales, informará de la incidencia a la Delegatura de Protección de Datos Personales de LA SUPERINTENDENCIA DE INDUSTRIA Y COMERCIO, en el módulo habilitado para tal efecto dentro de los 15 días a partir del conocimiento de esta.

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

Las incidencias pueden afectar tanto a bases de datos digitales como físicas y generarán las siguientes actividades:

- a. Notificación de Incidentes: Cuando se presuma que un incidente pueda afectar o haber afectado a bases de datos con información personal datos personales se deberá informar al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y/o al Líder Nacional de Protección de Datos Personales, quién gestionará su reporte en el Registro Nacional de Bases de Datos.
- b. Gestión de Incidentes: Es responsabilidad de cada funcionario, contratista, consultor o tercero, reportar de manera oportuna cualquier evento sospechoso, debilidad o violación de políticas que pueden afectar la confidencialidad, integridad y disponibilidad de los activos e información personal de la Entidad.
- c. Identificación: Todos los eventos sospechosos o anormales, tales como aquellos en los que se observe el potencial de pérdida de reserva o confidencialidad de la información, deben ser evaluados para determinar si son o no, un incidente y deben ser reportados al nivel adecuado en la organización. Cualquier decisión que involucre a las autoridades de investigación y judiciales debe ser realizada en conjunto entre el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y la Oficina Asesora Jurídica o quien haga sus veces. La comunicación con dichas autoridades será realizada por ellos mismos.
- d. Reporte: Todos los incidentes y eventos sospechosos deben ser reportados tan pronto como sea posible a través de los canales internos establecidos por Servicios Postales Nacionales. Si la información sensible o confidencial es perdida, divulgada a personal no autorizado o se sospecha de alguno de estos eventos, el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y/o al Líder Nacional de protección de Datos Personales, debe ser notificado de forma inmediata.
- e. Los funcionarios deben reportar a su jefe directo y al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y/o al Líder Nacional de Protección de Datos Personales, cualquier daño o pérdida de computadores o cualquiera otro dispositivo, cuando estos contengan datos personales en poder de la Entidad.

A menos que exista una solicitud de la autoridad competente debidamente razonada y justificada, ningún funcionario debe divulgar información sobre sistemas de cómputo, y redes que hayan sido afectadas por un delito informático o abuso de sistema.

Para la entrega de información o datos en virtud de orden de autoridad judicial, la Oficina Asesora Jurídica o quien haga sus veces, deberá intervenir con el fin de prestar el asesoramiento adecuado.

- f. Contención, Investigación y Diagnostico: El Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y/o el Líder Nacional de Protección de Datos Personales, debe garantizar que se tomen las acciones para investigar y diagnosticar las causas que generaron el incidente, así como también debe



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

garantizar que todo el proceso de gestión del incidente sea debidamente documentado, apoyado con Dirección Nacional de Informática y Tecnología.

En caso de que se identifique **un delito informático**, en los términos establecidos en la **Ley 1273 de 2009**, el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y la Oficina Asesora Jurídica o quien haga sus veces, reportara tal información a las autoridades de investigaciones judiciales respectivas.

Durante los procesos de investigación se deberá garantizar la “Cadena de Custodia” con el fin de preservarla en caso de requerirse establecer una acción legal.

- g. Solución: La Dirección Nacional de Informática y Tecnología, así como cualquier área comprometida y los directamente responsables de la gestión de datos personales deben prevenir que el incidente de seguridad se vuelva a presentar, corrigiendo todas las vulnerabilidades existentes.
- h. Cierre de Incidente y Seguimiento: Dirección Nacional de Informática y Tecnología, juntamente con el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y las áreas que usan o requieren la información, iniciarán y documentarán todas las tareas de revisión de las acciones que fueron ejecutadas para remediar el incidente de seguridad. El Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO), preparará un análisis anual de los incidentes reportados. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.
- i. Reporte de incidentes ante la SIC: Como autoridad de control se reportarán como novedades los incidentes de seguridad que afecten la base de datos, de acuerdo con las siguientes reglas:
- ✓ En la parte inferior del menú de cada base de datos registrada en el sistema, se presentan dos (2) opciones para informar las novedades: La violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado.
 - ✓ Deberán reportarse al Registro Nacional de Bases de Datos dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento de la persona o área encargada de atenderlos.
 - ✓ Los líderes de proceso y/o propietarios de activos de información, reportarán de forma interna los incidentes asociados a datos personales ante el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y al Líder Nacional de Protección de Datos Personales, quién dentro del plazo legal procederá a reportarlos ante el Registro Nacional de Bases de Datos de la SIC.



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

10. ÁREA RESPONSABLE DE LA ATENCIÓN A PETICIONES, CONSULTAS, QUEJAS Y RECLAMOS DE LA POLÍTICAS DE TRATAMIENTO DE DATOS PERSONALES.

Las peticiones, consultas y reclamos formulados por los titulares de Datos Personales bajo el Tratamiento de Servicios Postales Nacionales S.A., para ejercer sus derechos a conocer, **actualizar, rectificar y suprimir datos personales**, o **revocar la autorización**, a través de las siguientes:

- **Roles/Dependencias:** Jefatura Nacional de PQR y/o el Líder Nacional de Protección de Datos Personales y Privacidad de la Información.

El rol designado para que asuma la función de protección de datos personales, que dará trámite a las solicitudes de los Titulares, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y demás decretos y normas reglamentarias, será el Líder Gestor Nacional de Protección de Datos Personales y Privacidad de la Información de la entidad o quien haga sus veces, a su vez en conjunto con la Jefatura Nacional de PQR será el área que gestionará las solicitudes de los titulares de Datos Personales, para todos los efectos previstos en esta Política.

11. PROCEDIMIENTO PARA ATENDER LOS DERECHOS DE LOS TITULARES:

En el desarrollo, interpretación y aplicación de la ley, regulaciones, y normatividad vigente, se emplearán, de manera armónica e integral, los siguientes procedimientos:

Procedimiento de Tratamiento de Datos Personales: Se conoce como el tratamiento de datos personales la acción de recolectar, almacenar, usar, poner en circulación o suprimir diferentes datos personales. Así las cosas, el tratamiento de las bases de datos que contienen datos personales dentro de la entidad Servicios Postales Nacionales S.A.

Los titulares de Datos Personales, sin importar el tipo de vinculación que tengan con Servicios Postales Nacionales S.A., pueden ejercer sus derechos a conocer, actualizar, rectificar y suprimir información y/o revocar la autorización otorgada, de acuerdo con el "Procedimiento para actualizar, rectificar y suprimir información y/o revocar autorizaciones PDP"

Definiciones:

- Reclamo de supresión, el derecho del titular a que se supriman los datos que resulten inadecuados, excesivos o no respeten los principios, derechos y garantías constitucionales y legales.
- Reclamo de revocación, el derecho del titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
- Reclamo de infracción, el derecho a solicitar que se proceda a la subsanación del incumplimiento de la normativa en materia de protección de datos.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Procedimiento para el acceso, actualización, rectificación, supresión de datos y revocación de la autorización de tratamiento de datos personales:

En concordancia con el artículo 15 de la Ley 1581 de 2012, los titulares o las personas señaladas en el apartado de “**Autorización del Titular / Personas A Quienes se les puede suministrar la Información**” de la presente Política de Tratamiento de Datos Personales, que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la Ley 1581 de 2012, podrán presentar un reclamo ante Servicios Postales Nacionales, el cual será tramitado bajo los siguientes lineamientos:

Procedimiento de Consultas:

Servicios Postales Nacionales y/o los Encargados, garantizan a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes o personas autorizadas, el derecho de acceder y consultar toda la información contenida en su registro individual o toda aquella que esté vinculada con su identificación conforme se establece en la presente Política de Tratamiento de Datos Personales.

Una vez identificadas las PQR (Peticiónes, quejas, reclamos), que van dirigidas a la PDP (Protección de Datos Personales), el área de recepción de las mismas, se le asignara un CUN (Código Único Numérico) y un manejo especial para este tipo de peticiones, una vez se tenga el CUN, el área o función jurídica de la Jefatura de PQR o quien haga sus veces diligenciará la plantilla o a través de los medios (digitales o físicos) establecidos de manejo de PQR de PDP, la cual serán definidos y aportados por el Líder Nacional de protección de Datos Personales y Privacidad de la información y/o el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) de la entidad.

Esta plantilla o los medios establecidos (físicos o digitales), tendrá como finalidad un control interno de manejo de PQR por parte del área o función jurídica de la Jefatura de PQR o quien haga sus veces, cuando se presente la necesidad de un apoyo jurídico se consultaría al Líder Nacional de Protección de Datos Personales y/o Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) o en efecto a la Oficina Asesora Jurídica de la entidad.

En línea con lo anterior, a través del medio mencionado, se puede llevar un control de la fecha establecida en la ley, decretos y reglamentos, para el reporte ante RNBD (Registro Nacional de la Bases de Datos) ante la (SIC) Superintendencia de Industria y Comercio.

Adicional, es indispensable manejar el control de las plantillas o a través del medio mencionado (físico o digital) donde se lleva el registro y soluciones de fondo dirigidas a las PQRS de PDP, para efectos de la cuantificación de las PQR, frente a cualquier solicitud de un ente de vigilancia, inspección y control externo o auditoría interna.

Mencionada plantilla o a través del medio definido, tendrá la siguiente información: No. CUN, peticionario, numero de cedula, correo electrónico, numero de celular, descripción de la solicitud o reclamo, fecha de radicación de la solicitud, periodo y año en que se va



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

a reportar al Líder Nacional de Protección de Datos Personales y al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO), fecha límite para reportar al Líder Nacional de Protección de Datos y al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO), fecha de respuesta de fondo, fecha de prórroga, motivo de prórroga, tipo de tramite (reclamo o consulta), estado de las PQR (solución de fondo o si está en reclamación), recepción de PQR (física, telefónica o digital), traslado por falta de competencia o por otras circunstancias (fecha en la que se envió al cliente y entidad a la que se envió).

Responsable de atención de consultas:

- A través del área de servicio al cliente y los canales de atención definidos, se recepcionarán las diferentes consultas elevadas que sean dirigidas a la actualización, rectificación, supresión o revocación de autorizaciones de PDP, una vez identificadas estas solicitudes se le asignara un CUN (que lleva el control de este tipo de PQRS), posteriormente se remitirán al área o función jurídica o quien haga sus veces de la Jefatura Nacional de PQR.
- El área o función jurídica o quien haga sus veces de la Jefatura Nacional de PQR, verifica que la solicitud contenga todas las especificaciones requeridas a efectos de poder valorar que el derecho que se ejerza se hace con legitimidad y con el lleno de los requisitos mencionados en la presente política y en los procedimientos internos de tratamiento de datos de la entidad, Una vez recibida la consulta completa, se incluirá en la base de datos interna una leyenda que diga "consulta en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido. Así mismo, de forma inmediata se hará llegar al Líder Nacional de Protección de Datos Personales y al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO), quien será el responsable de emitir un diagnóstico de fondo en un término prudencial y devolverá de nuevo al área o función jurídica de la Jefatura de PQR.
- El área o función jurídica o quien haga sus veces de la Jefatura Nacional de PQR, se encargará de dar una contestación de fondo al titular de la información, en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo, en caso de imposibilidad de atender la consulta dentro de dicho término, se informará al interesado los motivos de la demora, señalando la fecha en que se atenderá su consulta, lo cual tendrá un término máximo de cinco (05) días hábiles contados a partir de la fecha de vencimiento del primer término. Este último plazo es improrrogable.

Las consultas dirigidas a Servicios Postales Nacionales S.A., deberán contener como mínimo la siguiente información:

- a. Nombres y apellidos del Titular y/o su representante y/o causahabientes;
- b. Lo que se pretende consultar
- c. Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

- d. Firma, número de identificación o procedimiento de validación correspondiente.
- e. Haber sido presentada por los medios de consulta habilitados por Servicios Postales Nacionales para esta finalidad.
 - ✓ En caso de que la reclamación se presente sin el cumplimiento de los anteriores requisitos legales, se solicitará al reclamante dentro de los cinco (5) días siguientes a la recepción del reclamo, para que subsane las fallas y presente la información o documentos faltantes.

Desistimiento: Transcurridos dos (2) meses desde la fecha del requerimiento sin subsanación.

El titular podrá optar por uno o varios de los siguientes sistemas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla en puntos de atención y/o venta.
- Escrito respuesta dirigida a la dirección reportada por el peticionario.
- Correo electrónico u otros sistemas de comunicación electrónica o digital

Plazos de Respuesta a consultas:

Las solicitudes recibidas mediante los anteriores medios serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo.

Prórroga del plazo de Respuesta:

En caso de imposibilidad de atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los diez (10) días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer plazo.

Procedimiento De Reclamos:

Derechos Garantizados mediante el procedimiento de reclamos:

- a. Rectificación, Actualización, supresión: Servicios Postales Nacionales y/o los encargados, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de corregir o actualizar los datos personales que reposen en sus bases de datos, mediante presentación de reclamación, cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente Política de Tratamiento de Datos Personales para que sea procedente la solicitud de Corrección o Actualización.
- b. Revocatoria de la autorización o Supresión de los datos Personales: Servicios Postales Nacionales y/o los Encargados, garantizarán a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes, el derecho de Solicitar la Revocatoria de la autorización o solicitar la supresión de la información contenida en su registro individual o toda aquella que esté vinculada con su

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

identificación cuando consideren que se cumplen los parámetros establecidos por la ley o los señalados en la presente Política de Tratamiento de Datos Personales.

Así mismo se garantiza el derecho de presentar reclamos cuando adviertan el presunto incumplimiento de la Ley 1581 de 2012 o de la presente Política de tratamiento de datos personales.

Servicios Postales Nacionales y/o los Encargados, garantizan a los titulares de datos personales contenidos en sus bases de datos o a sus causahabientes o personas autorizadas, el derecho de acceder y consultar toda la información contenida en su registro individual o toda aquella que esté vinculada con su identificación conforme se establece en la presente Política de Tratamiento de Datos Personales.

Una vez identificadas las PQR (Peticiónes, quejas, reclamos), que van dirigidas a la PDP (Protección de Datos Personales), el área de recepción de las mismas, se le asignará un CUN (Código Único Numérico) y un manejo especial para este tipo de peticiones, una vez se tenga el CUN, el área o función jurídica de la Jefatura de PQR o quien haga sus veces diligenciará la plantilla o a través de los medios (digitales o físicos) establecidos de manejo de PQR de PDP, la cual serán definidos y aportados por el Líder Nacional de protección de Datos Personales y Privacidad de la información y/o el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) de la entidad.

Esta plantilla o los medios establecidos (físicos o digitales), tendrá como finalidad un control interno de manejo de PQR por parte del área o función jurídica de la Jefatura de PQR o quien haga sus veces, cuando se presente la necesidad de un apoyo jurídico se consultaría al Líder Nacional de Protección de Datos Personales y/o Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) o en efecto a la Oficina Asesora Jurídica de la entidad.

En línea con lo anterior, a través del medio mencionado, se puede llevar un control de la fecha establecida en la ley, decretos y reglamentos, para el reporte ante RNBD (Registro Nacional de las Bases de Datos) ante la (SIC) Superintendencia de Industria y Comercio.

Adicional, es indispensable manejar el control de las plantillas o a través del medio mencionado (físico o digital) donde se lleva el registro y soluciones de fondo dirigidas a las PQR de PDP, para efectos de la cuantificación de las PQR, frente a cualquier solicitud de un ente de vigilancia, inspección y control externo o auditoría interna.

Mencionada plantilla o a través del medio definido, tendrá la siguiente información: No. CUN, petionario, número de cédula, correo electrónico, número de celular, descripción de la solicitud o reclamo, fecha de radicación de la solicitud, periodo y año en que se va a reportar al Líder Nacional de Protección de Datos Personales y al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO), fecha límite para reportar al Líder Nacional de Protección de Datos y al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO), fecha de respuesta de fondo, fecha de prórroga, motivo de prórroga, tipo de trámite (reclamo o consulta), estado de las PQRS (solución de fondo o si está en reclamación), recepción de PQRS (física, telefónica o digital), traslado por falta de competencia o por otras circunstancias (fecha en la que se envió al cliente y entidad a la que se envió).

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

Responsable de atención de Reclamos:

- A través de los canales de atención definidos, la Jefatura Nacional de PQR tramitara los diferentes reclamos elevados que sean dirigidas a la actualización, rectificación, supresión o revocación de autorizaciones de PDP, una vez identificadas estas solicitudes se le asignara un CUN (que lleva el control de este tipo de PQR), posteriormente se remitirán al área o función jurídica o quien haga sus veces de la Jefatura Nacional de PQR.
- El área o función jurídica o quien haga sus veces de la Jefatura Nacional de PQR, verifica que la solicitud contenga todas las especificaciones requeridas a efectos de poder valorar que el derecho que se ejerza se hace con legitimidad y con el lleno de los requisitos mencionados en la presente política y en los procedimientos internos de tratamiento de datos de la entidad, Una vez recibida el reclamo, se incluirá en la base de datos de PQR una leyenda que diga **"reclamo en trámite"** y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido. Así mismo, de forma inmediata se hará llegar al Líder Nacional de Protección de Datos Personales y al Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO), quien será el responsable de emitir un diagnóstico de fondo en un término prudencial y devolverá de nuevo al área o función jurídica de la Jefatura de PQR.
- El área o función jurídica o quien haga sus veces de la Jefatura Nacional de PQR, se encargará de dar una contestación de fondo al titular de la información, en un término máximo de quince (15) días hábiles contados a partir de la fecha de su recibo, en caso de imposibilidad de atender la consulta dentro de dicho término, se informará al interesado los motivos de la demora, señalando la fecha en que se atenderá su consulta, lo cual tendrá un término máximo de ocho (08) días hábiles contados a partir de la fecha de vencimiento del primer término. Este último plazo es improrrogable.

Las Reclamaciones presentadas deberán contener como mínimo la siguiente Información:

- a. Nombres y apellidos del Titular y/o su representante y/o causahabientes;
- b. Lo que se pretende reclamar
- c. Dirección física, electrónica y teléfono de contacto del Titular y/o sus causahabientes o representantes;
- d. Firma, número de identificación o procedimiento de validación correspondiente.
- e. Haber sido presentada por los medios de consulta habilitados por Servicios Postales Nacionales.

Reclamaciones sin cumplimiento de Requisitos legales:

En caso de que la reclamación se presente sin el cumplimiento de los anteriores requisitos legales, se solicitará al reclamante dentro de los cinco (5) días siguientes a la recepción del reclamo, para que subsane las fallas y presente la información o documentos faltantes.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Desistimiento del Reclamo:

Transcurridos dos (2) meses desde la fecha del requerimiento sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Recepción de reclamos y consultas que no correspondan a la Entidad:

En caso de que Servicios Postales Nacionales, reciba un reclamo que no son de competencia de la entidad, estos serán remitidos a la entidad competente a quien corresponda en un término máximo de dos (2) días hábiles e informará de la situación al reclamante por escrito dentro del mismo termino.

Nota: En caso de requerir una consulta o reclamo sobre una base de datos que administre un **OPERADOR POSTAL OFICIAL diferente a Servicios Postales Nacionales S.A.**, la petición se deberá presentar por el titular del derecho directamente al operador postal oficial responsable (**o en su efecto por el mismo remitente, ante el OPO – Operador Postal Oficial, en el país que se impuso él envió**) debido a que los acuerdos establecidos por la **Unión Postal Universal** no regulan este tipo de solicitudes.

Es de resaltar que es de gran importancia para Servicios Postales Nacionales S.A., proteger y salvaguardar el derecho constitucional de petición de sus clientes, pero desafortunadamente, en el presente caso, no contamos como Entidad con la información específica, ni con las herramientas técnicas y funcionales suficientes para dar una solución de fondo o para remitir por competencia; debido a que las aplicaciones de consulta entre OPOs, solo admiten solicitudes de trazabilidad de los envíos y no en PQR sobre la materia de protección de datos personales.

Inclusión de leyenda en la base de datos:

Recibida la reclamación de forma completa, en un término máximo de dos (2) días hábiles contados desde la recepción, Servicios Postales Nacionales Incluirán en la base de datos donde se encuentren los datos personales del Titular, una leyenda que diga "**reclamo en trámite**" y el motivo de este. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

Plazos de Respuesta a los Reclamos:

El término máximo para atender el reclamo será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo.

Prórroga del plazo de Respuesta:

Cuando no fuere posible atender el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Si vencido el término legal respectivo para la supresión de la información y la revocatoria de la autorización al responsable, no se hubieran eliminado los datos personales, el titular tendrá derecho a solicitar a la Superintendencia de Industria y Comercio que ordene la



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

revocatoria de la autorización y/o la supresión de los datos personales. Para estos efectos se aplicará el procedimiento descrito en el artículo 22 de la Ley 1581 de 2012. No procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

Peticiones o Consultas Solicitadas por Orden de Autoridad Judicial:

Una vez identificadas las PQR, que van dirigidas a la PDP, el área de recepción de estas, se le asignará un CUN (especial para este tipo de peticiones), una vez tenga el CUN, el área o función jurídica de la Jefatura de PQR después de verificar los requisitos de ley de la petición o consulta diligenciará la plantilla de manejo de PQR de PDP solicitada por Autoridad Judicial, la cual será aportada por el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y/o el Líder Nacional de Protección de Datos de la entidad, mencionada plantilla tendrá la siguiente información: No. CUN, peticionario (juez de conocimiento y/o de garantías y/o fiscalía), dirección del despacho, correo electrónico del despacho y/o fiscal o juez, numero de celular y/o oficina con extensión, descripción de la solicitud o finalidad, fecha de radicación de la solicitud, periodo y año en que se va a reportar al el Gerente Oficial de Seguridad de la Información y Ciberseguridad CISO y el Líder Nacional de Protección de Datos Personales, fecha límite para reportar al el Gerente Oficial de Seguridad de la Información y Ciberseguridad CISO y el Líder Nacional de Protección de Datos Personales, fecha de respuesta de fondo, fecha de prórroga, motivo de prórroga, tipo de tramite (reclamo o consulta), estado de las PQR (solución de fondo y en reclamación), corroboración de la PQR ante la autoridad judicial (fecha en que se hizo y medio a través del cual se logró).

Cuando las PQR vengán emanadas por solicitud de una orden judicial, se debe solicitar como requisito obligatorio se aporte el correo electrónico del fiscal o juez de control de garantías y/o conocimiento del cual emana la orden de solicitud de información.

En lo referente a las consultas o solicitudes emanadas por entidad judicial, se debe tener en cuenta que se usa el mismo procedimiento de las PQR general, descrito dentro de la presente política.

Procedimiento de Supresión de Datos Personales:

En caso de resultar procedente la Supresión de los datos personales del titular de la base de datos conforme a la reclamación presentada, Servicios Postales Nacionales, deberá realizar operativamente la supresión de tal manera que la eliminación no permita la recuperación de la información, sin embargo, el Titular deberá tener en cuenta que en algunos casos cierta información deberá permanecer en registros históricos por cumplimiento de deberes legales de la organización por lo que su supresión versará frente al tratamiento activo de los mismos y de acuerdo a la solicitud del titular.

A TENER EN CUENTA:

Una vez cumplidos los términos señalados en la ley 1581 de 2012 y demás normas que la reglamenten y complementen, y no se dé respuesta de fondo a la petición, el titular de la información en ejercicio de su derecho, actualización, rectificación, supresión y revocación

	(MSPI) MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Y CIBERSEGURIDAD	CODIGO: MN-GS-SI-007
		VERSIÓN: 6
		ACTUALIZACIÓN: 18/05/2021
		EMISIÓN: 24/12/2016

podrá poner su caso en conocimiento de la SIC (Superintendencia de Industria y Comercio), ante la delegatura para protección de datos personales.

12. SEGURIDAD Y PROTECCIÓN

Servicios Postales Nacionales, S.A. (4-72), teniendo en cuenta el principio de seguridad regulado por la LEPD (LEY ESTATUTARIA DE PROTECCIÓN DE DATOS), tiene implementadas las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, Servicios Postales Nacionales, S.A. (4-72), a través de la suscripción de los correspondientes contratos de transmisión, requiere a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad requeridas para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

13. CANALES DE ATENCIÓN Y UBICACIÓN DE LA POLÍTICA DE TRATAMIENTO

Los canales de atención y la política de tratamiento de la entidad, podrá ser consultada en los siguientes medios así mismo cualquier tipo de solicitud, producto del ejercicio de los deberes y derechos consagrados en la política, podrá dirigirse a:

- La política de tratamiento de datos a la que se encuentran sujetos los datos personales del titular **se podrá consultar en la siguiente página web:** <http://www.4-72.com.co/Politicadetratamiento>
- **Contac Center.** Lunes a viernes de 8:00 a.m. a 6:00 p.m. • Sábados de 8:00 am. a 12:00 m. Línea nacional: 018000111210 • Bogotá: 472 20 00.
- **Medio escrito en puntos de venta y servicio al cliente autorizados** en forma física a través de carteles o anuncios publicados en diferentes partes de los puntos de venta e información. Confírmelos aquí: <http://www.4-72.com.co/content/puntos-de-atencion>
- **Sitio Web Enlace directo:** <http://www.4-72.com.co/content/peticiones-quejas-y-recursos>
- **Enlace general:** www.4-72.com.co

Redes sociales:

Las redes sociales como Facebook y Twitter, constituyen plataformas complementarias de divulgación de la información (comunicación), las cuales son de gran interconexión de los medios digitales de los usuarios y no se encuentran bajo la responsabilidad de Servicios Postales Nacionales S.A., por ser ajenas a la empresa.

Toda la información que los usuarios proporcionan en las redes sociales en las que participa Servicios Postales Nacionales S.A., como usuario no constituye ni forma parte



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

de los Datos Personales sujetos a la protección de esta Política, siendo de total responsabilidad de la empresa prestadora de esa plataforma.

Videovigilancia: Servicios Postales Nacionales, informa a sus empleados, aliados, contratistas, clientes y visitantes sobre la existencia de mecanismos de seguridad, por medio de la notificación en anuncios de aviso de privacidad de la información y/o de la videovigilancia en sitios visibles.

La entidad, cuenta con un sistema de videovigilancia por medio de cámaras fijas, instaladas en sitios estratégicos en el interior y en perímetro exterior propiedad de la entidad como de sus oficinas e instalaciones, lo cual está establecido en los derechos del tratamiento de datos para los empleados y personas naturales.

Manifestando que la información recolectada solo se utilizará con fines de seguridad de los empleados, personas naturales, bienes y activos que en ella se contengan. Dicha información podrá ser utilizada como prueba en cualquier momento que sea requerida, ante cualquier autoridad, organización oficial y privada que lo solicite, imágenes o videos que se anonimizarían si es necesario.

Los archivos obtenidos de la videovigilancia se almacenan en un sistema que cuenta con condiciones de seguridad, con todo el rigor necesario para tal fin y solo tiene acceso el personal del área de seguridad postal, seguridad electrónica, seguridad de la información y seguridad informática, en cuya vinculación se firmó el acuerdo de confidencialidad.

Así mismo, se determina que es impajaritable que todas y cada una de las instalaciones de Servicios Postales Nacionales S.A., en las que se cuente con CCTV, deben tener expuesto al público a través de avisos de privacidad (modelo que definirá el Gerente Oficial de Seguridad de Información y Ciberseguridad y/o el Líder Nacional de Protección de Datos Personales) la autorización que otorga el titular para que sus datos sean tratados y la comunicación de estar siendo grabado y monitoreado de forma expresa y clara o a través de una conducta inequívoca, previo a utilizar algunos de los servicios que se prestan y/o entrar a las correspondientes instalaciones y dentro de las mismas.

Ahora bien, respecto del aviso de privacidad de PDP, con base en el artículo 2.2.2.25.2.7 y 3.1.1 del Decreto Único Reglamentario 1074 de 2015 que deroga parcialmente el decreto 1377 de 2013. Debe tenerse en cuenta este también debe estar expuesto en un sitio visible a todas las personas que ingresen a las sucursales, puntos de venta o servicio al cliente a nivel Nacional de la entidad.

INSTRUMENTOS DE LA POLÍTICA. Son instrumentos de la presente política las estrategias, programas, manuales, guías, procedimientos, instructivos y formatos documentados y aprobados por el Gerente Oficial de Seguridad de la Información y Ciberseguridad (CISO) y de los diferentes responsables de los procesos y subprocesos, que sean necesarios para la adecuada implementación y gestión de los lineamientos establecidos por la normatividad vigente relacionada con el tratamiento de datos personales y privacidad de la información.



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

14. VIGENCIA DE LA POLÍTICA.

Las bases de datos responsabilidad de Servicios Postales Nacionales, S.A. (4-72) serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad del cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento se realizará el procedimiento de inactivación de la información

Así mismo, la presente Política de Tratamiento y Protección de Datos Personales permanece vigente desde el día 15 de mayo de 2021 y con la presente, se suple dejando sin efecto acuerdos y políticas expedidas con anterioridad, que le sean contrarias. En lo que respecta a las Bases de datos en las que se registran los datos personales, estas tendrán una vigencia igual al tiempo en que se mantenga y utilice la información, para las finalidades descritas en esta política, una vez se cumplan esas finalidades y siempre que no exista un deber legal o contractual de conservar su información, sus datos serán eliminados de nuestras bases de datos. O en su efecto si no sucede lo precedente, serán conservados los datos en nuestras bases de datos, mientras no sea solicitada la supresión por el titular y siempre que no exista el deber legal de conservarlos.

Toda información no contemplada en la presente política se reglamentará de acuerdo al Régimen General de Protección de Datos Personales vigente en Colombia.

La actualización de la Políticas de Protección de Datos Personales dependerá de las instrucciones y lineamientos de la Alta Dirección y los lineamientos ordenados por el MINTIC, así como de las extensiones reglamentarias del ente de vigilancia y control, la Superintendencia de Industria y Comercio.

Cualquier inquietud adicional nos puede escribir al correo habeasdata@4-72.com.co, los mensajes serán atendidos a la mayor brevedad posible por el Gerente Oficial de Seguridad de la Información y Ciberseguridad y/o la Líder Nacional de Protección de Datos Personales y Privacidad de la Información de la entidad, los mensajes serán atendidos a la mayor brevedad posible.

DOCUMENTOS RELACIONADOS

- (MSPI) Manual de Políticas de Seguridad de la Información y Ciberseguridad
- Gestión de Tiempos Solicitudes PQRS
- Manual de Protocolo de Servicio al Cliente
- Procedimiento SAC (Servicio al Cliente)
- Formato presencial Ley Estatutaria
- Caracterización del Proceso Servicio al Cliente
- Y demás formatos, manuales y procedimientos con relación a la Protección de Datos Personales y Privacidad de la Información.



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

ANEXO 1: Ejemplo de Formato de Autorización emitida por los Titulares de los Datos.

- Si tiene dudas al diligenciar el formulario comuníquese con el Gerente Oficial de Seguridad y Ciberseguridad de la entidad y/o el Líder Nacional de Protección de Datos Personales y Privacidad de la Información.

En mi calidad de titular de información personal, actuando de forma libre, voluntaria, *específica e inequívoca* al diligenciar los datos aquí solicitados, autorizo a *SERVICIOS POSTALES NACIONALES S.A. identificada con NIT: 900.062.917-9*, para que de forma directa o a través de terceros realice el tratamiento (el cual consiste en recolectar, almacenar, usar, transferir, transmitir y administrar mis datos personales) *así mismo, preciso que la información suministrada es verídica y clara, para proceder a ejecutar la siguiente finalidad:*

(El área encargada de la recolección debe colocar en detalle todos los datos individuales a recolectar).

Los datos autorizados para el tratamiento se utilizarán únicamente para las siguientes finalidades:

El área encargada de la recolección debe describir en el siguiente cuadro los fines del tratamiento de los datos que solicita recolectar, teniendo como referente los definidos en la política de tratamiento de datos personales de Servicios Postales Nacionales S.A, la cual encontrará en <http://www.4-72.com.co/Politicadetratamiento>

Advertencia: Cada finalidad que usted incluya en este formato debe contar con un mecanismo que le permita al Titular seleccionar por separado si acepta o no que se efectúe ese tratamiento particular.

El diligenciamiento que se vislumbra es solo a modo de ejemplo

FINALIDAD	AUTORIZACION	
	SI	NO
Obtener el registro de imágenes o videos de las personas que ingresan a las diferentes instalaciones de la entidad a nivel Nacional, en pro de la seguridad de todos los que entren a las instalaciones	X	
Tratamiento de datos personales, en pro de ofertar servicios y medir la satisfacción de los servicios prestados en pro de la una mejora continua del catálogo ofertado por la entidad		X

Manifiesto que me informaron el carácter facultativo que tengo en caso de recolección de mi información sensible es decir que tengo derecho a contestar o no las preguntas que me



(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

formulen y a entregar o no los datos solicitados. Entiendo que son datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Manifiesto que me informaron que los datos sensibles que se recolectarán serán utilizados para las siguientes finalidades: (dejar este párrafo solo si recolectamos datos sensibles, de lo contrario borrar del formato)

FINALIDAD	AUTORIZACION	
	SI	NO
Indicar finalidad 1 de los datos sensibles	X	
Indicar finalidad 2 de los datos sensibles		X

De manera expresa manifiesto que he sido informado y entiendo mis derechos como titular de datos personales frente a: i) conocer, actualizar y rectificar los datos personales, ii) solicitar prueba de la autorización otorgada para su tratamiento, iii) ser informado por el Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones, previa solicitud, respecto del uso que le ha dado a los datos personales, iv) presentar quejas ante la Superintendencia de Industria y Comercio por infracciones a la ley, v) revocar la autorización y/o solicitar la supresión del(los) dato(s) en los casos en que sea procedente, vi) acceder en forma gratuita a los mismos, y vii) abstenerse de responder las preguntas sobre datos sensibles o sobre datos de las niñas y niños y adolescentes y que los puedo consultar en Política de Tratamiento de Datos Personales de Servicios Postales Nacionales S.A., en el sitio <http://www.4-72.com.co/Politicadetratamiento>

Lo anterior, de conformidad con el Artículo 15 de la Constitución Política, la Ley Estatutaria 1581 de 2012 y demás normas concordantes.

Manifiesto que he sido informado que, para ejercer mis derechos, lo podré hacer a través de la página web y de la siguiente dependencia de Servicios Postales Nacionales S.A.:

- **Roles/Dependencias:** Líder Nacional de Protección de Datos Personales y Privacidad de la Información / Jefatura Nacional de PQR.
- **Dirección** Diagonal 25G # 95A - 55 Bogotá (Cundinamarca).
- **Teléfono:** (571) 4722005,
- **sitio Web:** WWW.4-72.COM.CO
- **Correo electrónico:** habeasdata@4-72.com.co / servicioalcliente@4-72.com.co
- **Página web:** <https://4-72pqr.com.co/PQRWeb/PQRUsuarioServlet>



**(MSPI) MANUAL DE POLÍTICAS DE
SEGURIDAD DE LA INFORMACIÓN Y
CIBERSEGURIDAD**

CODIGO: MN-GS-SI-007

VERSIÓN: 6

ACTUALIZACIÓN: 18/05/2021

EMISIÓN: 24/12/2016

Leído lo anterior y al diligenciar este formulario **autorizo** de manera previa, explícita e inequívoca a Servicios Postales Nacionales S.A., realizar el tratamiento de los datos personales diligenciados dentro de las finalidades legales, contractuales, comerciales y las aquí contempladas, de acuerdo con la Política de Tratamiento de Datos Personales de Servicios Postales Nacionales; además, declaro ser el titular de la información suministrada en este formulario es completa, confiable, veraz, exacta, y manifiesto que la presente autorización me fue solicitada y puesta de presente antes de entregar mis datos y que la suscribo de forma libre y voluntaria una vez leída en su totalidad.

(La siguiente información debe diligenciarla el ciudadano) –

Conforme con lo anterior:

_____, identificado con cédula de ciudadanía () cédula de extranjería () otro ()
_____ N° _____, a los ___ días del mes de ___ del año __, **AUTORIZO** el tratamiento de mis datos personales para los exclusivos fines aquí referidos y en el marco señalado.

Firma del Titular: _____