

FUERZAS MILITARES DE COLOMBIA
EJÉRCITO NACIONAL



PROCEDIMIENTO			
RECOLECCIÓN DE DATOS PERSONALES			
MACROPROCESO: Direccionamiento Estratégico			
PROCESO: Gestión de Tecnologías y Sistemas de Información C5			
Código: P-JEMPP-CEDE6-506	Versión: 0	Fecha de emisión: 2025-02-21	Número de Páginas: 18

Elaboró	Revisó	Aprobó
 PD06. DEICY DÍAZ GUTIÉRREZ Profesional de Defensa 06 CEDE6	 PS. ALEJANDRA BETANCOURTH Asesora Jurídica CEDE6	 EG. RAFAEL HERNANDO JIMÉNEZ JIMÉNEZ Jefe Departamento de Comunicaciones
 SS. CÉSAR FLÓREZ Suboficial de Prospectiva y Vigilancia Tecnológica C5	 TC. FERNANDO GAMBA MILA Director Prospectiva e Innovación C5 CEDE6	

Recolección de Datos Personales

Control de Actualizaciones

Actualización a la versión No.	Actualización realizada	Fecha de emisión
0	Procedimiento Inicial	2025-02-21



Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

TABLA DE CONTENIDO

1.	OBJETIVO:	4
2.	ALCANCE:	4
3.	CONTROL:	4
4.	DEFINICIONES:.....	5
5.	FLUJOGRAMA DE ACTIVIDADES:.....	9
6.	PRODUCTO DEL PROCEDIMIENTO:	14
7.	DOCUMENTOS RELACIONADOS:.....	14
8.	NORMATIVIDAD APLICABLE:	14
9.	ANEXOS:	15

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

1. OBJETIVO:

Establecer las actividades para recolectar y tratar los datos personales que serán almacenados en las bases de datos administradas por parte del Ejército Nacional, a fin de dar cumplimiento a las obligaciones frente al manejo de la información personal, de conformidad con la Ley 1581 de 2012 y sus decretos reglamentarios.

2. ALCANCE:

Este procedimiento aplica para todas las dependencias y Unidades del Ejército Nacional, en cumplimiento de la Ley 1581 de 2012 de protección de datos personales que protege el derecho de las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas.

La protección de los datos personales es importante para evitar que los datos sean usados para fines distintos a los que se les dio, y para evitar delitos como el robo de identidad.

El procedimiento aplica a todas las bases de datos y/o archivos que contengan datos personales que sean objeto de tratamiento por parte de cada responsable del tratamiento de datos personales clasificados como datos de identificación, laborales, patrimoniales, procedimientos administrativos y jurisdiccionales, académicos, de tránsito y movimientos migratorios, entre otros.

3. CONTROL:

Toda dependencia o unidad es responsable de implementar buenas prácticas para la gestión de datos personales al interior de sus unidades en cumplimiento de la Ley Estatutaria 1581 de 2012 “por la cual se dictan disposiciones generales para la protección de datos personales”, nombrando por orden semanal la dependencia encargada o responsable del tratamiento de datos personales en cada unidad o dependencia.

El Ejército Nacional a través de la Ayudantía General y la oficina de Atención Ciudadana son el área que tiene a cargo dar trámite a las solicitudes de los titulares para hacer efectivos sus derechos a conocer, actualizar, rectificar y suprimir el dato y revocar la autorización, a través de los canales autorizados vigentes:

- Correo Electrónico: peticiones@pqr.mil.co
- Correo certificado: remitir comunicación dirigida al Área de Atención Ciudadana radicada en la Calle 53 #57-93 Barrio La Esmeralda - Bogotá
- Página Web de Peticiones, Quejas y Reclamos www.pqr.mil.co

Recolección de Datos Personales

Las unidades y dependencias que recolectan datos personales no podrán utilizar medios engañosos, fraudulentos ni mecanismos ilegítimos para recolectarlos ni para realizar el tratamiento.

4. DEFINICIONES:

Autorización: es el consentimiento que da cualquier persona para que las empresas o personas responsables del tratamiento de la información, puedan utilizar sus datos personales.

Aviso de privacidad: es una de las opciones de comunicación verbal o escrita o digital que brinda la ley para darle a conocer a los titulares de la información, la existencia y las formas de acceder a las políticas de tratamiento de la información y el objetivo de su recolección y uso.

Base de datos: conjunto organizado de datos personales que son objeto de tratamiento.

Conducta inequívoca: modo de obtener el consentimiento o autorización para el tratamiento de datos personales que trata de actos que permiten inferir que el titular está autorizando el tratamiento de sus datos personales.

Dato personal: se trata de cualquier información vinculada o que pueda asociarse a una persona determinada, como su nombre o número de identificación, o que puedan hacerla determinable, como sus rasgos físicos, domicilio, teléfono particular y/o celular, correo electrónico personal, estado civil, firma, firma electrónica, cartilla militar, lugar y fecha de nacimiento, nacionalidad, edad, fotografía, trayectoria académica, laboral o profesional, contraseñas bancarias, números de tarjetas de crédito, entre otros, los datos que debemos mantener protegidos del mundo exterior, ya que representan el acceso directo a nuestra vida privada y posible violación a nuestra ciberseguridad.

Datos sensibles: son aquellos que afectan la intimidad del titular o pueden dar lugar a que lo discriminen, es decir, aquellos que revelan su origen racial o étnico, su orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos, entre otros.

Encargado del tratamiento: es la persona natural o jurídica que realiza el tratamiento de datos personales, a partir de una delegación que le hace el responsable, recibiendo instrucciones acerca de la forma en la que deberán ser administrados los datos.

Incidente de seguridad de la información: evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen probabilidad

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Oficial de protección de datos:

- a. De acuerdo al Decreto 1074 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo”, artículo 2.2.2.25.4.4 “Medios para el ejercicio de los derechos” (...) todo responsable y encargado debe designar a una persona o área 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 el presente capítulo (...).
- b. La función del oficial de protección de datos o el área encargada de protección de datos en la organización es de velar por la implementación efectiva de las políticas y procedimientos adoptados por ésta para cumplir las normas, así como la implementación de buenas prácticas de gestión de datos personales dentro de la institución.
- c. El oficial de protección de datos tendrá la labor de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente.

Principios de cumplimiento:

- a. **Principio de legalidad en materia de tratamiento de datos:** el tratamiento a que se refiere la presente ley es una actividad que debe sujetarse a lo establecido en ella y en las demás disposiciones que lo 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 solo 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.

Recolección de Datos Personales

- 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 acceso y circulación restringida:** el tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la presente política, el marco legal en protección de datos y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la presente política y el marco legal en protección de datos.
- g. **Los datos personales:** no podrán estar disponibles en internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los titulares o terceros autorizados conforme a la presente política y el marco legal en protección de datos.
- h. **Principio de seguridad:** la información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento, 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.
- i. **Principio de confidencialidad:** todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la presente política y el marco legal en protección de datos.

Titular: es la persona natural cuyos datos personales son objeto de tratamiento.

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

RNBD: registro nacional de la base de datos.

Recolección de Datos Personales

Responsable del tratamiento: es la persona natural o jurídica, pública o privada, que decide sobre la finalidad de las bases de datos y/o el tratamiento de los mismos.

Responsabilidad Demostrada: una obligación o disposición a responder por las acciones propias y la obligación de un individuo o de una organización de rendir cuentas sobre sus actividades, aceptar responsabilidad sobre ellas y divulgar los resultados de manera transparente en cumplimiento a la Ley 1581 de 2012. El principio fundamental de responsabilidad demostrada exige que una entidad que recoge y hace tratamiento de datos personales debe ser responsable del cumplimiento efectivo de las medidas que implementen los principios de privacidad y protección de datos. En este sentido, los responsables del tratamiento deben contar con el Programa Integral de Gestión de Datos Personales (PIGDP) y estar preparados para demostrarle a la autoridad la implementación efectiva de esas medidas en concordancia al Decreto 1377 de 2013 y Directiva Permanente N°. 03 de 2019 del Ministerio de Defensa.

SIC: superintendencia de Industria y Comercio.

Seguridad de la Información: el Ejército Nacional acatando el principio de seguridad en el tratamiento de los datos personales proporcionará 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.

Lo anterior se contextualiza dentro de un proceso de gestión de la seguridad de la información que tiene como objetivo mitigar la probabilidad de ocurrencia de violaciones de confidencialidad, integridad y disponibilidad en contra de los datos personales de los cuales es responsable el Ejército Nacional, siempre alineados a la realidad de que la seguridad de la información no es absoluta y aunque se tomen la mayor cantidad de medidas estaremos sujetos a la ocurrencia de un incidente, que dado el caso se tratará como una acción infortunada, fuera del alcance del Ejército Nacional.

Las anteriores definiciones fueron extraídas de la Ley Estatutaria 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".



Recolección de Datos Personales

5. FLUJOGRAMA DE ACTIVIDADES:

Flujograma	Descripción de la Actividad	Registro de la Actividad	Responsable
<pre> graph TD Inicio([Inicio]) --> Actividad[1. Solicitar la autorización para el tratamiento de datos personales] Actividad --> A{{A}} </pre>	<p>1. Solicitar la autorización para el tratamiento de datos personales: todas las unidades y dependencias que recolectan datos personales deberán a más tardar en el momento de la recolección, solicitar al titular la autorización explícita para el tratamiento, esta puede ser obtenida por cualquier medio que pueda ser objeto de consulta posterior.</p> <p>La autorización será solicitada según el procedimiento interno definido por cada unidad y dependencia, esta puede ser por escrito, de forma oral, formularios electrónicos, en línea o mediante conductas inequívocas.</p> <p>En los siguientes casos no es necesaria la autorización:</p> <ul style="list-style-type: none"> • Cuando la información es requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial. • En caso de hacer tratamiento de datos de naturaleza pública. • Casos de urgencia médica o sanitaria. • Para el tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos. • Cuando se trata de datos relacionados con el registro civil. <p>Trámite de obligatorio cumplimiento:</p> <p>Para los casos donde el Ejército Nacional obra en el rol de encargado de tratamiento de datos personales, la unidad o dependencia que reciba datos personales recolectados por un tercero responsable, deberá asegurarse que el responsable dispone de la autorización para el tratamiento. Es decir, la unidad o dependencia del Ejército Nacional deberá contar con un oficio donde el responsable le indique que los datos personales fueron recolectados con autorización de los titulares, y ellos en el rol de responsables disponen de esta autorización.</p>	<p style="text-align: center;">Autorización para el tratamiento de datos</p>	<p>1. Todas las unidades y dependencias que recolectan datos personales, personal que controlan accesos a edificios, sitios públicos, acceso a sitios restringidos, acceso a dependencias, guardias con archivos excel, libros donde oficiales, suboficiales, soldados y/o personal civil incluyen datos personales.</p> <p>Todo funcionario que se encuentra en la TOE del Ejército Nacional es responsable del tratamiento de datos personales.</p>

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

Flujograma	Descripción de la Actividad	Registro de la Actividad	Responsable
<pre> graph TD A{{A}} --> B[2. Informar al Titular aspectos del tratamiento] B --> C{{B}} </pre>	<p>2. Informar al Titular aspectos del tratamiento: todas las unidades y dependencias que recolectan datos personales, deberán informar al titular en el momento de la recolección, de manera verbal, escrita o mediante el aviso de privacidad de datos personales visible física, en bases de datos y páginas web institucionales, lo siguiente:</p> <ul style="list-style-type: none"> • La finalidad de la recolección de los datos personales, esta debe ser legítima, cierta y tener una razón de ser. Además, los datos personales recolectados deben ser pertinentes y adecuados para alcanzar dicho fin. • Si los datos personales a recolectar son de clasificación datos sensibles, el titular debe saber que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento. • Cuáles datos son sensibles y cuál será la finalidad del tratamiento que se les dará. • Los derechos que tiene el titular de la información. • La identificación, dirección física o electrónica, teléfono del responsable del tratamiento de los datos personales. • La existencia de políticas para el tratamiento de los datos personales. <p>La información suministrada por parte del Ejército Nacional deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso.</p> <p>3. Autorizar el tratamiento de datos personales: el titular de los datos personales deberá a más tardar en el momento de la recolección, otorgar autorización al Ejército Nacional, según el procedimiento establecido internamente por la unidad o dependencia de acuerdo a la Ley 1581 de 2012 de protección de datos personales.</p> <p>Para el caso de la autorización por parte de menores de edad, sus representantes legales podrán dar la autorización previo ejercicio del menor de su derecho a ser escuchado.</p>	<p>Aviso de privacidad de datos personales.</p> <p>Autorización el tratamiento de datos</p>	<p>2. Todas las unidades y dependencias que recolectan datos personales, personal que controlan accesos a edificios, sitios públicos, acceso a sitios restringidos, acceso a dependencias, guardias con archivos excel o Word, hojas o formatos, libros, bases de datos, páginas web institucionales donde oficiales, suboficiales, soldados y/o personal civil incluyen datos personales.</p> <p>Todo funcionario que se encuentra en la TOE del Ejército Nacional es responsable del tratamiento de datos personales.</p> <p>3. Titular o dueño de la información.</p>

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

Flujograma	Descripción de la Actividad	Registro de la Actividad	Responsable
<pre> graph TD B{{B}} --> 4[4. Almacenar la autorización para el tratamiento de datos personales] 4 --> 5[5. Mantener la autorización para el tratamiento de datos personales] 5 --> 6[6. Aplicar medidas de seguridad a los datos personales recolectados] 6 --> 7[7. Revocar la autorización para el tratamiento de datos personales] 7 --> C{{C}} </pre>	<p>4. Almacenar la autorización para el tratamiento de datos personales: cada unidad y dependencia que recolectan datos personales deberá almacenar de manera segura la autorización dada por el titular para el tratamiento de sus datos personales.</p> <p>5. Mantener la autorización para el tratamiento de datos personales: cada unidad y dependencia que recolectan datos personales deberá asegurarse de mantener y conservar de forma segura, la prueba de las autorizaciones dadas por los titulares para el tratamiento de datos personales. Se debe disponer de la autorización en el medio que fue dada, ver actividad No. 3.</p> <p>En cualquier momento, el titular podrá solicitar prueba de la autorización otorgada al responsable del tratamiento, salvo cuando expresamente se exceptúe los casos descritos en la actividad No. 1.</p> <p>6. Aplicar medidas de seguridad a los datos personales recolectados: cada unidad y dependencia que recolectan datos personales, deberán aplicar las medidas de seguridad descritas en las políticas de seguridad de la información, para minimizar los riesgos de un uso no adecuado, pérdida de confidencialidad, integridad o disponibilidad de los datos personales recolectados y tratados.</p> <p>Los datos personales recolectados no podrán ser suministrados ni compartidos excepto a:</p> <ul style="list-style-type: none"> • Los titulares, sus causahabientes o sus representantes legales. • A las entidades públicas o administrativas en ejercicio de sus funciones legales o por orden judicial. • A los terceros autorizados por el titular o por la Ley. <p>7. Revocar la autorización para el tratamiento de datos personales: si el titular de los datos personales solicita revocar la autorización dada al Ejército Nacional para el tratamiento, lo podrá hacer a través de la página web destinada para</p>	<p>Almacenamiento de la autorización para el tratamiento de datos personales</p> <p>Conservar la autorización para el tratamiento de datos personales en el medio que fue dada.</p> <p>Controles implementados:</p> <ol style="list-style-type: none"> 1. Calidad de los datos personales 2. Revisar documentos y fotos 3. Administrar la configuración de seguridad y privacidad de las cuentas y dispositivos. 4. Descargar antivirus. 5. Diligenciar bien el registro en libros sin tachones ni enmendaduras. <p>Solicitud de revocación</p>	<p>4. 5. 6.</p> <p>Todas las unidades y dependencias que recolectan datos personas a través de bases de datos, páginas web, formularios o sistemas automatizados deberán contar con la autorización para la respectiva recolección de datos personales en los diferentes medios y tener nombrado un oficial de protección de datos personales.</p> <p>Todo funcionario que pertenezca a la TOE del Ejército Nacional</p> <p>7. Titular o dueño de los datos</p>

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

Flujograma	Descripción de la Actividad	Registro de la Actividad	Responsable
<pre> graph TD C{{C}} --> B[8. Disponer de un inventario de bases de datos] B --> D{{D}} </pre>	<p>Peticiones, Quejas y Reclamos (PQR), se realizan revocatorias de datos personales o inmediatamente con la unidad que ha recolectado los datos personales.</p> <p>Esta revocatoria sólo procede mientras no exista una relación entre el titular y el responsable de tratamiento.</p> <p>8. Disponer de un inventario de bases de datos: cada unidad y/o dependencia que recolecta datos personales y los almacene en bases de datos, deberán realizar y mantener actualizado un inventario de las bases de datos con las siguientes características:</p> <ul style="list-style-type: none"> • Cantidad de bases de datos con información personal. • Información detallada de los canales o medios que se tienen previstos para atender a los titulares. • Tipo de datos personales contenidos en cada base de datos a los que se realiza tratamiento, como: datos de identificación, ubicación, socioeconómicos, sensibles, privado, semiprivado, público u otros. • Ubicación física de las bases de datos (servidor, base de datos, archivos de Word, Excel almacenados en equipos de cómputo, archivos físicos propios o externos, registros en libros, fichas técnicas, formatos de seguridad, registros fotográficos y de video, entre otros). • Cuando el tratamiento de los datos personales se realice a través de un (unos) encargado (s) del tratamiento, se solicitarán los datos de identificación y ubicación de ese (esos) encargado (s). • Medidas de seguridad y/o controles implementados en la base de datos para minimizar los riesgos de un uso no adecuado de los datos personales tratados. • Indicar si el encargado del tratamiento es interno (Unidad o Dependencia del Ejército Nacional) o externo. • Forma de obtención de los datos (directamente del titular o mediante terceros). • Si se ha realizado transferencia o transmisión internacional de los datos personales contenidos en la base de 	<p>Inventario de bases de datos</p>	<p>8. Todas las unidades y/o dependencias que recolectan datos personales con bases de datos</p>

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

Flujograma	Descripción de la Actividad	Registro de la Actividad	Responsable
<pre> graph TD D{{D}} --> A[9. Gestionar el registro nacional de la base de datos] A --> B[10. Realizar el registro nacional de la base de datos] B --> C[11. Reportar eventos e incidentes de seguridad de la información] C --> F([Fin]) </pre>	<p>datos, a qué países y los datos del destinatario.</p> <ul style="list-style-type: none"> • Conocer si se cuenta con la autorización de los titulares de los datos contenidos en las bases de datos. • Cantidad de titulares por cada base de datos. • Enviar inventario de bases de datos al CAOCC-BRICC. <p>9. Gestionar el registro nacional de la base de datos - RNBD: todas las unidades y dependencias que recolectan datos personales en sus bases de datos, deberán gestionar con el CAOCC-BRICC, el Registro Nacional de las Bases de Datos RNBD sujetas a la aplicación de la Ley 1581 de 2012, en el directorio público de las bases de datos sujetas a tratamiento, ante la Superintendencia de Industria y Comercio – SIC, y CAOCC-BRICC aplicar el procedimiento P-JEMPP-CEDE6-445, FO-JEMPP-CEDE6-1732.</p> <p>10. Realizar el registro nacional de bases de datos personales - RNBD: el CAOCC-BRICC realizará el trámite del RNBD ante la SIC, mediante la página web https://rnbd.sic.gov.co/sisi/login aplicando el procedimiento P-JEMPP-CEDE6-445 y diligenciar el FO-JEMPP-CEDE6-1732. Por otra parte, se puede tomar como apoyo el Manual de Usuario del RNBD de la SIC².</p> <p>11. Reportar eventos e incidentes de seguridad de la información: cada unidad y dependencia que recolectan o en su defecto den tratamiento a datos personales, así como los titulares, deberán reportar los eventos e incidentes detectados de seguridad de la información asociados a los datos personales, de acuerdo al procedimiento de gestión de incidentes de seguridad de la información (P-JEMPP-CEDE6-325)</p>	<p>Solicitud del RNBD</p> <p>Registro Nacional de las Bases de Datos RNBD</p> <p>Registro de Incidentes (FO-JEMPP-CEDE6-1355)</p>	<p>9. CAOCC-BRICC Oficial o suboficial asignado manejo bases de datos con datos personales.</p> <p>10. CAOCC-BRICC Oficial o suboficial asignado manejo bases de datos con datos personales</p> <p>11. CAOCC-BRICC-BACCI Oficial o suboficial asignado a la gestión de incidentes.</p>

²https://www.sic.gov.co/sites/default/files/files/Proteccion_Datos/RNBD/Manual%20de%20Usuario%206_4%20RNBD_2911_2019_V_Final.pdf

Recolección de Datos Personales

6. PRODUCTO DEL PROCEDIMIENTO:

- Avisos de privacidad.
- Autorización para el tratamiento de datos personales.
- Datos personales registrados en las bases de datos.
- Registro nacional de bases de datos personales RNBD ante la Superintendencia de Industria y Comercio SIC.

7. DOCUMENTOS RELACIONADOS:

- Aviso de privacidad público (físico o virtual) (Términos y Condiciones de uso de sitio Web, aplicación WEB (APP) o medio digital).
- Procedimiento de gestión de incidentes de seguridad de la información P-JEMPP-CEDE6-325 emitido por el Departamento de Comunicaciones.
- Procedimiento P-JEMPP-CEDE6-445 Registro Bases de datos con datos personales ante la Superintendencia de Industria y Comercio (SIC).
- Política de seguridad de la información POL-JEMPP-CEDE6-008 emitida por el Departamento de Comunicaciones.
- Manual de usuario del Registro Nacional de Bases de Datos que emite la Superintendencia de Industria y Comercio SIC – RNBD.

8. NORMATIVIDAD APLICABLE:

- Artículo 15 de la Constitución Política de Colombia "(...) Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar (...)".
- Guía de formatos modelo para el tratamiento de datos personales Ley 1581 de 2012 y sus decretos reglamentarios emanados por la Superintendencia de Industria y Comercio.
- Ley 1266 de 2008 "Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones".
- Ley 1273 de 2009 "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones".
- Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales".
- Decreto 1377 de 2013 "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".
- Decreto Reglamentario 886 de 2014 "Por la cual se reglamenta el art. 25 de la Ley 1581 relativo al Registro Nacional de Bases de Datos".

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

- Decreto 1074 de 2015 “Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo”.
- Decreto 090 de 2018 “Por el cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 - Decreto Reglamentario del Sector Comercio, Industria y Turismo”.
- Directiva Permanente N°. 03 de 2019 “Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional.

9. ANEXOS:

9.1 Tratamiento a los datos personales del personal de empleados activos, retirados, clientes y/o personal externo y proveedores, Tratamiento de datos personales por PQR.

Funcionarios Activos y Retirados	
Tipo de información Datos de identificación, de ubicación, información médica, información bancaria, información familiar contenidos socio económico y sensible	
Finalidad <ul style="list-style-type: none">✓ Los datos personales de los funcionarios activos y retirados y su núcleo familiar serán tratados dentro del cumplimiento derivado de la relación laboral, utilizándolos para procesos de identificación, compensación, contacto, gestión laboral, selección de personal, cobros, pagos cumplimiento de parafiscales, prevención de riesgos laborales, promoción de personal y las gestiones contables y financieras entre otras dentro de la relación laboral, acceso a áreas seguras, acceso a sitios con objetivos laborales.✓ El empleado(a), autoriza al Ejército Nacional para tratar los datos personales que se suministren en desarrollo de la relación laboral durante todo el tiempo de permanencia en la entidad y después de terminada la relación siempre y cuando exista un deber de conservación legal o contractual por parte del Ejército Nacional.✓ La autorización de tratamiento de datos personales y se otorga por parte del empleado dentro de lo descrito en la presente Política de Protección de Datos Personales de acuerdo a la ley 1581 de 2012.✓ El funcionario del Ejército Nacional que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, podrá ser denunciado penalmente por el delito de daño informático. Así mismo el funcionario que sin estar facultado para ello, con provecho propio de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, podrá ser denunciado por la conducta de violación de datos personales.✓ En todos los casos el funcionario podrá hacer uso de sus derechos de Habeas Data (conocer, actualizar y rectificar su información) con excepción de lo establecido en la ley.✓ La información del personal retirado se almacena con fines de conservación documental y archivo de información, historia laboral durante el término establecido en la ley laboral.	

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

Personal Candidatos proceso selección o ingreso a la Institución o los diferentes procesos de incorporación	
Tipo de información	Finalidad
Datos de identificación, de ubicación y contenido socio económico, familiar	<ul style="list-style-type: none"> ✓ Se recoge la información de las hojas de vida, certificaciones y referencias personales de quienes se presentan a procesos de selección, incorporación, ingreso. Se busca identificar a los candidatos idóneos o aptos para su respectiva vinculación, con el fin de situar a la persona de acuerdo a su perfil. ✓ Los datos personales del personal a incorporar o seleccionar, serán tratados teniendo como finalidad los servicios de la institución con relación en los procesos internos en ejercicio del objeto misional, utilizándolos para identificación, contacto, eventos de capacitación, servicios, estudios estadísticos, acceso a instalaciones y demás que tengan que ver con las funciones y perfiles laborales.

Datos personales sensibles	
Tipo de información	
Para el caso de datos personales sensibles, se podrá hacer uso y tratamiento de ellos cuando:	
Finalidad	
<ul style="list-style-type: none"> ✓ 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. ✓ El tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado, por tal razón los representantes legales deberán otorgar su autorización. ✓ El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del titular. ✓ El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial. ✓ 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. 	

Personal Externo	
Tipo de información	Finalidad
Datos de identificación, de ubicación y contenido socio económico, o de servicio	<ul style="list-style-type: none"> ✓ Los datos personales del personal externo serán tratados teniendo como finalidad prestar los productos y servicios de la institución con relación en los procesos internos en ejercicio del objeto misional, utilizándolos para identificación, contacto, ofrecimiento de servicios, entrega de información y eventos de capacitación, servicios, estudios estadísticos, acceso a instalaciones a través de videos de identificación, libros de registro para accesos.

Este documento es propiedad del EJÉRCITO NACIONAL
No está autorizado su reproducción total o parcial



Recolección de Datos Personales

Proveedores	
Tipo de información	Finalidad
Datos de identificación, de ubicación y contenido socio económico	<ul style="list-style-type: none"> ✓ Los datos personales de los proveedores serán tratados para la adquisición de productos y servicios requeridos para el ejercicio del objeto social del Ejército Nacional, utilizándolos para identificación, contacto, adquisición de bienes y servicios, cobros y pagos, gestión contable y financiera que aplique a la relación cliente con proveedor, históricos, entre otros, dentro de una relación comercial. ✓ Se busca tener información actualizada, consistente y suficiente acerca de las personas que tienen calidad de proveedores o aspiren a serlo, en su relación contractual y en específico sobre su comportamiento como proveedor, aspectos administrativos, tributarios, financieros y logísticos.

9.2 Tratamiento a los datos personales externos por PQR:

Para efectos de atender las peticiones, consultas y reclamos que el titular pueda tener sobre el tratamiento de sus datos personales y en garantía de sus derechos a conocer, actualizar, rectificar y suprimir sus datos personales, Ejército Nacional ha dispuesto lo siguiente:

a. Atención a consultas: el titular podrá realizar una consulta en referencia al tratamiento de sus datos existentes en las bases de datos tratadas por el Ejército Nacional.

Para esto deberá enviar una solicitud escrita dirigida al Ejército Nacional a algunos de los canales dispuestos a través de la página www.pqr.mil.co correo electrónico o dirección física, al "Área responsable" de tratamiento de datos personales de la Unidad o Dependencia.

La consulta será atendida en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, **se informará al interesado, 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 término.**

b. Atención de quejas y reclamos: el titular que tenga una queja en relación al tratamiento de sus datos o que considere que los datos deben ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes de las leyes, podrán presentar una queja o reclamo.

Las quejas y reclamos se formularán mediante solicitud dirigida al Ejército Nacional a algunos de los dos canales dispuestos, correo electrónico o dirección

Recolección de Datos Personales

física, descritos en el capítulo “Área Responsable” con la identificación del titular, la descripción de los hechos que dan lugar al reclamo, la dirección y acompañando los documentos que se quiera hacer valer.

Si el reclamo resulta incompleto, se incluirá en la base de datos en el registro asociado al titular 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.

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

