MINISTERIO DE DEFENSA NACIONAL

"PROGRAMA INTEGRAL DE PROTECCIÓN DE DATOS PERSONALES"

UNIDAD DE GESTIÓN GENERAL DEL MINISTERIO DE DEFENSA NACIONAL

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

Tabla de contenido

1. INTRODUCCIÓN 4

2. OBJETIVO DEL PROGRAMA 4

3. OBJETO Y ALCANCE 4

4. REFERENCIA NORMATIVA: 5

5. DEFINICIONES 6

6. AMBITO DE APLICACIÓN. 10

7. ROLES Y RESPONSABILIDADES 10

7.1. Alta Dirección 10

7.1.1 Propender por la implementación y cumplimiento de la normatividad de protección de datos personales en todas dependencias de la Unidad de Gestión General. 10

7.1.2 Designar como área responsable de la función de Protección de Datos Personales a la Secretaría General del Ministerio de Defensa Nacional o la que haga sus veces. 10

7.2. Oficial de Protección de Datos Personales 10

7.3. Dirección de Talento Humano 12

7.4. Oficina de Relación con el Ciudadano 12

7.5. Dirección de Tecnologías de la Información y las Comunicaciones 13

7.6. Oficina de Control Interno Sectorial 13

7.7. Oficina de Respuesta a Incidentes Cibernéticos (CSIRT) 13

7.8. Gestor Titular y Suplente tratamiento de Protección de Datos Personales. 14

7.9. Dependencias Unidad de Gestión General 14

8. REGISTRO BASE DE DATOS PERSONALES 16

8.1. Procedimiento 16

8.2. Riesgos y Controles 18

8.3. Formato 19

8.4. Inventario de bases de datos Personales 20

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

9 LINEAMIENTOS PARA EL MANEJO DE DATOS PERSONALES 20

9.1 Tratamiento de Datos Personales 21

9.2 Parámetros para la Eliminación segura de la Información 21

9.3 Consultas y Reclamos 21

9.4 Actualización de las Bases de Datos Registrados en la Plataforma del Registro Nacional de Bases de Datos – RNBD. 22

9.5 Contratistas y Terceras Partes 22

10 GESTIÓN DE VERIFICACIÓN DEL PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES – PIGDP 23

11 INDICADORES 23

12 PLAN DE FORMACIÓN Y SOCIALIZACIÓN 23

12.4 Oficial de Protección de Datos 24

12.5 Gestores 24

12.6 ¿Gestores de? 24

13 EVALUACIÓN, REVISIÓN Y SEGUIMIENTO 24

14 REFERENCIAS 25

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

1. INTRODUCCIÓN

Como muestra del compromiso con el respeto y garantía de los derechos de cada uno de los servidores públicos de la Unidad de Gestión General del Ministerio de Defensa Nacional y terceros, la Unidad de Gestión General (UGG) del MDN, adopta el Programa Integral de Gestión de Datos Personales - PIGDP, siendo de obligatoria aplicación en todas las actividades que involucren, total o parcialmente la recolección, almacenamiento, uso, circulación y supresión de información personal. Cada uno de los miembros del talento humano de la UGG-MDN deberán observar y respetar el siguiente programa en el cumplimiento de las funciones y/o actividades que desarrollen aún después de terminados los vínculos legales existentes. De igual manera se comprometen a guardar estricta confidencialidad en relación con los datos personales tratados.

2. OBJETIVO DEL PROGRAMA

Definir los lineamientos y procedimientos por medio del cual la Unidad de Gestión General del Ministerio de Defensa Nacional se compromete con la protección de la información personal que recolecta de sus titulares dando cumplimiento a la Ley 1581 de 2012 y sus decretos reglamentarios. Así como la implementación de la responsabilidad demostrada frente al tratamiento de datos personales mediante la implementación, desarrollo y seguimiento del Programa Integral de Gestión de Datos Personales.

3. OBJETO Y ALCANCE

El objeto del programa integral de gestión de datos personales es evidenciar el cumplimiento de la ejecución e implementación del plan de trabajo de protección de datos, tendiente a dar cumplimiento a la normatividad en protección de datos y las directrices que imparte la Superintendencia de Industria y Comercio en la materia.

Acreditar gestión, diligencia y adecuado tratamiento de datos personales ante los titulares y ante las autoridades de protección de datos.

Compilar y describir la normatividad interna adoptada para dar cumplimiento a las disposiciones legales en materia de protección de datos personales.

Establecer los lineamientos para las dependencias del Ministerio de Defensa Nacional, como encargadas del tratamiento de datos personales, adopten la política para la recolección, manejo, tratamiento, protección y conservación de datos personales y privacidad de todas las personas, que en algún momento por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales a través de los distintos canales de atención, en cumplimiento de lo previsto en la Ley 1581 de 2012, el Decreto 1377 de 2013, y la Ley 1266 del 2008, con el propósito de garantizar y proteger el derecho fundamental de habeas data en el marco de lo establecido en mencionadas normas. Así mismo, unificar los criterios a publicar en sus respectivos sitios web relacionados con los términos y condiciones de uso.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

4. *REFERENCIA NORMATIVA:*

- *Constitución Política de Colombia, 1991.*
- *Ley Estatutaria 1266 de 2008, "Por la cual se dictan las disposiciones generales del habeas 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 1448 de 2011, "Por la cual se dictan medidas de atención, asistencia y reparación integral a las víctimas del conflicto armado interno y se dictan otras disposiciones".*
- *Ley Estatutaria 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales".*
- *Ley Estatutaria 1621 de 2013, "Por medio de la cual se expiden normas para fortalecer Marco Jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal, y se dictan otras disposiciones".*
- *Ley 1712 de 2014, "Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".*
- *Ley 1719 de 2014, "Por la cual se modifican algunos artículos de las Leyes 599 de 2000, 906 de 2004 y se adoptan medidas para garantizar el acceso a la justicia de las víctimas de violencia sexual, en especial la violencia sexual con ocasión del conflicto armado, y se dictan otras disposiciones",*
- *Decreto 1377 de 2013, "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".*
- *Decreto 857 de .2014, "Por el cual se reglamenta la Ley Estatutaria 1621 del 17 de abril de 2013, "Por medio de la cual se expiden normas para fortalecer el marco legal que permite a los organismos, que llevan a cabo actividades de inteligencia y contrainteligencia, cumplir con. su misión constitucional y legal, y se dictan otras disposiciones".*
- *Decreta 886 de 2014, "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos".*
- *Decreto 103 de 2015, "Por medio del cual se reglamenta parcialmente la Ley 1712 de 201.4 y se dictan otras disposiciones" (Referente -Gestión de la Información Clasificada y Reservada).*
- *Decreto Único Reglamentario 1074 de 2015 "Por media del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo" (Capítulo 25: reglamenta*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

parcialmente la ley 1581 de 2012 y, Capítulo 26: reglamenta la información mínima que debe contener el Registro Nacional de Bases de Datos).

- *Decreto 1759 .de 2016 "Por el cual se modifica el Artículo 2.2.2.26.3.1 del Decreto 1074 de 2015 Decreto único Reglamentario del Sector Comercio, Industria y Turismo (Modifica el Plazo de Inscripción de las bases de datos en el Registro Nacional de Bases de Datos).*

- *Decreto 090 de 2018, Por e) cual se modifican los artículos 2.2.2.26.1.2 y 2.2.2.26.3.1 del Decreto 1074 de 2015 -Decreto Único Reglamentario del Sector Comercio, Industria y Turismo (Modifica el ámbito de aplicación y el plazo de inscripción en el Registro Nacional de Bases de Datos).*
- *Resolución 7870 del 26 de diciembre 2022, "por la cual se emite y adopta la Política de Seguridad y Privacidad de la Información, Seguridad Digital, Ciberseguridad y continuidad de los Servicios Tecnológicos en las Unidades Ejecutoras o Dependencias del Ministerio de Defensa Nacional, Policía Nacional y entidades adscritas y vinculadas al Sector Defensa, y se dictan otras disposiciones.*

- *Circular externa 02 de 2015 "Adicionar e) Capítulo Segundo en el Título V de las Circular única de la Superintendencia de Industria y Comercio".*

- *Circular externa D1 de 2017 de la Superintendencia de Industria y Comercio "Modificar los numerales 2.2, 2.3, 2.6 y 2.7 del Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio, relacionados con el procedimiento de inscripción en el Registro Nacional de Bases de Datos y la información contenida en este".*

- *Circular externa 03 de 2018 de la Superintendencia de Industria y Comercio que "modifica los numerales 2.1 al 2.4 y eliminar los numerales 2.5 a la 2.7 del Capítulo Segundo del Título V de la Circular Única de la Superintendencia de Industria y Comercio".*

- *Manual de Seguridad de la Información OAS-33GL-MDNSG~AS-M001-01 de 2014.*

- *Directiva Permanente 03 del 2019, "Lineamientos para la definición de la Política de Tratamiento de Datos Personales en el Ministerio de Defensa Nacional.*

- *Resolución 1480 del 2022, Por la cual se establece y se adopta la Política de Tratamiento de Datos Personales de la Unidad de Gestión General del Ministerio de Defensa Nacional.*

5. DEFINICIONES

Para la correcta interpretación y aplicación del presente Programa Integral de Protección de Datos Personales, para todos los efectos, se adoptarán las siguientes definiciones:

***Autorización:** Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales. (Art 3. Ley 1581 de 2012).*

***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 le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

mismas y las finalidades del tratamiento que se pretende dar a los datos personales. (Art 3. Decreto 1377 de 2013.

Base de datos: *Conjunto organizado de datos personales que sea objeto de tratamiento (Art 3. Ley 1581 de 2012). Para la aplicación de la presente debe distinguirse dos clases de bases de datos; las automatizadas, es decir, aquellas que se almacenan y administran a través de herramientas informáticas y las bases de datos manuales o archivos, donde la información se encuentra organizada o almacenada en medio físico y contienen información personal, tal como nombre, identificación, números de teléfono, correo electrónico, etc.*

Custodio de /a Información: *Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que la propietaria de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado. (Aspecto que fuera adaptado de la norma ISO/IEC 27001:2013). Numeral 5 de la Guía para la Gestión y Clasificación de Activos de Información emitida por el Ministerio de las Tecnologías de la Información y las Comunicaciones, "Seguridad y Privacidad de la Información".*

Dato o información personal: *corresponde a cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (Art. 3. Ley 1581 de 2012). Para efectos del presente programa se entiende como la información suministrada por el usuario para su registro, lo cual incluye nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros.*

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 u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentas públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Art 3. Decreto 1377 de 2013).*

Dato privado: *Es el dato que por su naturaleza intima o reservada, sólo es relevante para el (titular. (Art 3. Ley 1266 de 2008).*

Dato semiprivado: *Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como dato financiero, y crediticio de actividad comercial o de servicios a que se refiere el título N de la Ley 1266. (Art 3. Ley 1266 de 2008).*

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 étnica, 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. (Art 3. Decreto 1377 de 2013).*

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. (Art 3. Ley 1581 de 2012).*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

Protección de datos personales: *Conjunto de medidas para garantizar y proteger los datos de carácter personal (cualquier información concerniente a personas físicas identificadas o identificables) registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado, a los efectos de garantizar y proteger las libertades públicas y los derechos fundamentales de las personas y especialmente de su honor e intimidad personal y familiar.*

Información: *Se refiere a un conjuntó organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen. (Art 6. Ley 1712 de 2014).*

Información Pública: *Es toda información que un sujeto obligado genere, obtenga, adquiera o controle en su calidad de tal. (Art 6. Ley 1712 de 2014).*

Información Pública Clasificada: *Es aquella información que estando en poder o custodia de un sujeto obligado en calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Art 6. Ley 1712 de 2014).*

Información Pública Reservada: *Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Art 6. Ley 1712 de 2014).*

Programa Integral de Gestión de Datos Personales – PIGDP: *Resultado de un proceso de debida diligencia al interior de la organización que incorpora políticas que respondan a los ciclos internos de gestión de datos y que generen resultados medibles, mediante la aplicación de buenas prácticas de gestión de datos personales. (Guía para la Implementación del Principio de Responsabilidad Demostrada - Accountability, Superintendencia de Industria y Comercio).*

Propietario de la Información: *Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso, (Aspecto que fuera adaptado de la norma ISO/IEC 27002:2013). Numeral S de la Guía para la Gestión y Clasificación de Activos de Información emitida por el Ministerio de las Comunicaciones, "Seguridad y Privacidad de la Tecnologías de la Información".*

Publicar: *Hacer que un documento, o una información, determinados sea visible a través del sitio web institucional. (Estrategia de Gobierno en Línea, Min TIC).*

Registro Nacional de Bases de Datos (RNBD): *El RNBD es el directorio público de las bases de datos sujetas a tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos (Art 25. Ley 1581 de 2012).*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

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 el tratamiento de los datos. (Art 3. Ley 1581 de 2012).*

Servicios: *Son las ayudas en línea que cada unidad ejecutora y/o dependencia del Ministerio de Defensa, la Policía Nacional y las entidades adscritas y vinculadas al MDN proveen actualmente, o que piensa proveer en el futuro a los usuarios, por medio de su respectivo sitio web o cualquier otro medio digital, como publicación de noticias o actividades propias de la gestión institucional, trámites en línea, consultas, foros y buzón de quejas y reclamos, entre otros. (Estrategia de Gobierno en Línea, Min TIC).*

Titular: *Persona natural cuyos datos personales sean objeto de tratamiento. (Art 3. Ley 1581 de 2012).*

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. - (Art 3. Decreto 1377 de 2013).*

Transmisión: *Tratamiento de datos personales que implica la comunicación de estos 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. (Art 3. Decreto 1377 de 2013).*

Tratamiento: *Cualquier operación o conjunto de operaciones sobre datos personales tales como la recolección, almacenamiento, uso, circulación o supresión. (Art 3. Ley 1581 de 2012).*

Usuario: *El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos en la ley 1266 de 2008, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos. En el caso en que el usuario a su vez entregue la información directamente a un operador, aquella tendrá la doble condición de usuario y fuente, y asumirá los deberes y responsabilidades de ambos. (Art 3. Ley 1266 de 2008.*

Recolección: *obtención inicial de los datos personales que suministra el titular a la institución a través de aplicaciones móviles, las visitas a sitios web, los programas de fidelización y los tramites en línea.*

Conservación de los datos personales: *la información se deberá conservar bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.*

Supresión de los datos personales: *es el derecho con el que cuenta el titular de estos para excluir su información de una base de datos, bien porque se está haciendo un uso indebido de ella, o por simple voluntad del titular salvo que exista una obligación legal o contractual que impida la supresión.*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

6. *AMBITO DE APLICACIÓN.*

El programa integral de gestión de datos personales es transversal a todos los procesos de la Unidad de Gestion General del Ministerio de Defensa Nacional, por ello todos los procesos organizacionales del Unidad de Gestión General MDN, que involucren tratamiento de datos personales deben dar cumplimiento al mismo y a las demás disposiciones y protocolos que en adelante se implementen en la materia.

Todos los servidores públicos de la Unidad de Gestión General que en el desarrollo de sus funciones capturen, o gestionen datos personales deberán dar cumplimiento al presente programa. Los nuevos procesos y/o procedimientos que se implementen después de la aprobación del presente programa, deberán tener en cuenta e incluir de ser necesario las disposiciones contempladas en este programa.

Lo establecido en este programa aplica a todas las bases de datos de la Unidad de Gestión General electrónicas o presenciales sea en calidad de responsable o encargado del tratamiento.

7. *ROLES Y RESPONSABILIDADES*

7.1. Alta Dirección

7.1.1 Propender por la implementación y cumplimiento de la normatividad de protección de datos personales en todas dependencias de la Unidad de Gestión General.

7.1.2 Designar como área responsable de la función de Protección de Datos Personales a la Secretaría General del Ministerio de Defensa Nacional o la que haga sus veces.

7.1.3 Designar funciones de Oficial de Protección de Datos Personales dentro de la Unidad de Gestión General al Señor Ayudante General del Ministerio de Defensa Nacional, mediante la Resolución No 1713 16 junio del 2020.

7.1.4 Apoyar, en lo que requiera el oficial de protección de datos, en la creación, implementación, administración y monitoreo del programa integral de gestión de datos personales.

7.1.5 Destinar recursos para el diseño e implementación de este programa.

7.1.6 informar a todo nivel sobre la ejecución del programa Integral de Protección de Datos Personales.

7.2. Oficial de Protección de Datos Personales

7.2.1. Asumir el rol y la función de Protección de Datos Personales de la Unidad de Gestión General del Ministerio de Defensa Nacional.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

7.2.2. Promover el desarrollo de una cultura de Protección de tratamiento de datos Personales y de privacidad.

7.2.3. Proponer y diseñar un "Programa Integral de Gestión de Datos Personales-PIGDP", de que trata el sub-literal e) del numeral I. de las misiones particulares de la Directiva Permanente 03 del 23 de enero de 2019. Así mismo, realizar el respectivo seguimiento a su implementación y cumplimiento.

7.2.4. Adoptar mecanismos internos para poner en práctica las políticas establecidas sobre la protección de datos personales, incluyendo herramientas de implementación, entrenamiento y programas de educación.

7.2.5. Diseñar y Proponer, para aprobación de la dependencia competente, los procedimientos requeridos para la atención y respuesta a consulta, petición y reclamos de los titulares, con respecto a cualquier aspecto del tratamiento.

7.2.6. Mantener un inventario de las bases de datos personales en poder de la respectiva unidad ejecutora, dependencia o institución y clasificar su tipo.

7.2.7. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de habeas data de acuerdo con lo establecido en artículo 17, literal a, de la ley 1581 del 2012.

7.2.8. Establecer, los mecanismos necesarios para solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el titular. (En cuanto a este literal se aplicará la exención prevista en el artículo 10 de la ley 1581 de 2012).

7.2.9. Establecer los mecanismos para informar debida y oportunamente al titular sobre la finalidad de la recolección y los derechos que le asisten en virtud de la autorización otorgada.

7.2.10. Establecer los mecanismos para conservación la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

7.2.11. Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable, siempre y cuando el titular informe oportunamente sus novedades.

7.2.12. Ratificar la Información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.

7.2.13. Suministrar al encargado del tratamiento, según sea el caso, únicamente datos cuyo tratamiento está previamente autorizado de conformidad con lo previsto en la ley y en la Directiva Permanente No. 03 del 23 enero de 2019.

7.2.14. Exigir al encargado del tratamiento en todo momento, el respeto de las condiciones de seguridad y privacidad de la información del titular.

7.2.15. 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 del titular.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

7.2.16. Adoptar y monitorear el cumplimiento de las instrucciones y requerimientos que, sobre el particular, impartan la Superintendencia de Industria y Comercio.

7.2.17. Propender por la correcta divulgación de la política de tratamiento de datos personales mediante aviso de privacidad, en página web y personalmente al titular en el momento de la recolección de los datos.

7.2.18. Permite al titular de la información, conocer en cualquier momento la información que exista sobre él en las bases de datos.

7.3. Dirección de Talento Humano

7.3.1. La Dirección de Talento Humano durante el proceso de vinculación de los servidores públicos militares, policiales y civiles deben realizar, antes de su designación definitiva, las verificaciones necesarias para confirmar la autenticidad de la información suministrada por el personal trasladado a la Unidad de Gestión General del Ministerio de Defensa Nacional.

7.3.2. La Dirección de Talento Humano debe certificar que los Servidores públicos militares, policiales y civiles de la Unidad de Gestión General del Ministerio de Defensa Nacional firmen el formato de autorización de Tratamiento de Datos Personales.

7.3.3. Dirección de Talento Humano debe convocar a los Servidores públicos militares, policiales y civiles de la Unidad de Gestión General del Ministerio de Defensa Nacional, a las charlas, conversatorios y demás eventos programados que promuevan la concienciación en Seguridad y Privacidad de la Información, llevar control de asistencia, aplicando las sanciones pertinentes por falta de asistencia no justificada.

7.3.4. La Dirección de Talento Humano notificará cualquier cambio sobre los responsables o encargados del tratamiento de datos personales al Oficial de Protección de Datos, con el fin de mantener información actualizada para el cumplimiento de la Ley.

7.4. Oficina de Relación con el Ciudadano

7.4.1. Realizar el seguimiento y garantizar el cumplimiento de los requerimientos en materia de política de datos personales conforme a lo indicado en la política de servicio al ciudadano.

7.4.2. Adaptar los lineamientos de protección de datos personales a los propios, conforme a la recolección y tratamiento de datos personales a través de los diferentes canales de atención y herramientas utilizadas con ese propósito.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

7.5. Dirección de Tecnologías de la Información y las Comunicaciones

7.5.1. Coordinar junto con el Oficial de Protección de Datos personales el seguimiento al registro de las bases de datos personales de la Unidad de Gestión General.

7.5.2 Implementar los respectivos ajustes tecnológicos que apoyen la realización, mantenimiento y reporte del inventario de las bases de datos que contengan datos personales.

7.5.3. Implementar las medidas adecuadas tales como la encriptación de las bases de datos y el nivel de cifrado acuerdo al riesgo de seguridad, esto con el fin de garantizar la seguridad de la información de datos personales almacenados en sistemas de bases de datos automatizados y que sean gestionados por la DITIC.

7.5.4. Propender por la preservación de la aceptación del tratamiento de datos personales por parte de titular, cuando la consulta se manifieste a través de medios digitales (aplicaciones móviles, sitios web, chat y herramientas colaborativas, entre otros.).

7.6. Oficina de Control Interno Sectorial

7.6.3. Realizar seguimiento y reportar el cumplimiento a la normatividad legal vigente a nivel nacional y de manera interna acerca de seguridad de la información.

7.6.4. Reportar evolución del Sistema de Seguridad de la Información a los directivos pertinentes en la Unidad de Gestión General del Ministerio de Defensa Nacional.

7.6.5. Realizar revistas anuales al cumplimiento del programa de protección de datos personales acuerdo la normatividad vigente.

7.7. Oficina de Respuesta a Incidentes Cibernéticos (CSIRT)

7.7.3. Asesorar las dependencias en lo referente a definir acciones de concientización y sensibilización con el fin de prevenir incidentes de seguridad digital". El CSIRT no tiene funciones relacionadas con procesos de seguridad tecnológica de bases de datos personales.

7.7.4. Difundir información relacionada la gestión de incidentes cibernéticos con el fin de prevenir posibles amenazas, vulnerabilidades y ataques informáticos que afecten bases de datos y sistemas de información".

7.7.5. Apoyar la coordinación de las capacidades institucionales para el manejo de los incidentes cibernéticos que afecten bases de datos y sistemas de información.

7.7.6. Gestionar y establecer mecanismos de prevención y control cuando se presente un incidente cibernético.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

7.8. Gestor Titular y Suplente tratamiento de Protección de Datos Personales.

7.8.3. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.

7.8.4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

7.8.5. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos de la ley.

7.8.6. Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la ley.

7.8.7. 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.

7.8.8. Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la ley.

7.8.9. Insertar en la base 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.

7.8.10. Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.

7.8.11. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.

7.8.12. 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.

7.8.13. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

7.9. Dependencias Unidad de Gestión General

Son funciones de las áreas y dependencias que hacen parte de la Unidad de Gestion General del Ministerio de Defensa Nacional las siguientes:

7.9.3. Cumplir a cabalidad los lineamientos que imparta la Unidad de Gestion General del Ministerio de Defensa Nacional a través de la Política de Tratamiento de Datos Personales, así como las directrices que se impartan en el marco del Programa Integral de Gestión de Datos Personales, la Ley 1581 de 2012, sus decretos reglamentarios y las instrucciones

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

impartidas por la autoridad nacional de protección de datos y el Oficial de Protección de Datos Personales.

7.9.4. Prestar todo el apoyo necesario al Oficial de Protección de Datos Personales para la identificación, inventario e inscripción de las nuevas bases de datos personales en el Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y Comercio dentro de los dos (2) meses siguientes contados a partir de su creación.

7.9.5. Prestar todo el apoyo necesario al Oficial de Protección de Datos Personales para actualizar en el Registro Nacional de Bases de Datos (RNBD) de la Superintendencia de Industria y Comercio (SIC) las bases de datos personales registradas por la organización, que estén a su cargo, conforme los términos previstos por la normatividad vigente.

7.9.6. Informar y someter a consideración del Oficial de Protección de Datos Personales la creación de nuevas bases de datos personales a cargo de la dependencia, para ser inscritas en el Registro Nacional de Bases de Datos (RNBD) atendiendo las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio (SIC).

7.9.7. Solicitar concepto al Oficial de Protección de Datos Personales respecto a la viabilidad y condiciones para llevar a cabo el acceso y Tratamiento de las bases de datos personales, cuando sea necesario.

7.9.8. Apoyar al Oficial de Protección de Datos Personales en el proceso de gestión de riesgos e identificación de oportunidades de mejora al Programa Integral de Gestión de Datos Personales.

7.9.9. Reportar ante el Oficial de Protección de Datos Personales cualquier violación a los códigos de seguridad, pérdida, robo, y/o acceso no autorizado o fraudulento a la información de las bases de datos personales físicas o electrónicas, para que éste a su vez realice el reporte del incidente ante la SIC, conforme los términos previstos en la normatividad vigente, y considerar dicha información en la actualización del mapa de riesgos de la entidad y el respectivo plan de manejo.

7.9.10. Dar a conocer al Oficial de Protección de Datos Personales las consultas, peticiones, quejas, reclamos, incidentes que conozca relacionados con protección de datos personales.

7.9.11. Participar activamente en las capacitaciones, sensibilizaciones que sobre protección de datos personales imparta la organización.

7.9.12. Apropiar los conocimientos y lineamientos que imparta la Unidad de Gestion General del Ministerio de Defensa Nacional, en materia de protección de datos personales y aplicarlos en las actividades que se realizan diariamente.

7.9.13. Responder con apoyo del Oficial de Protección de Datos Personales las solicitudes de los titulares, sus causahabientes o apoderados, para el ejercicio de los derechos a que se refiere la Ley 1581 de 2012 y el Decreto 1377 de 2013.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

7.9.14. Llevar a cabo las actividades que establezca la normatividad relacionada con la protección de datos personales, que estén a cargo de su dependencia en lo de sus respectivas competencias.

8. REGISTRO BASE DE DATOS PERSONALES

8.5. Procedimiento

8.5.3. Recolección de los Datos Personales

La Unidad de Gestión General del Ministerio de Defensa Nacional cuenta con el formato para realizar una correcta recolección de los datos personales de cada uno de los servidores públicos militares, policiales, civiles y terceros, la autorización debe contener:

- *Las finalidades a las cuales se someterán los datos recolectados.*
- *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.*
- *Los derechos que le asisten como titular.*
- *La identificación, dirección física o electrónica y teléfono del responsable del tratamiento, que en este caso es la Unidad de Gestión General del Ministerio de Defensa Nacional.*
- *Informar el sitio de consulta de la Política de Protección de Datos Personales de la Unidad de Gestión General del Ministerio de Defensa Nacional, que en este caso será la página web.*
- *La autorización se obtendrá por medios escritos o electrónicos, teniendo claro que siempre se deberá guardar constancia de esta, y podrá ser consultada en cualquier momento por el titular o autoridad competente.*

8.5.4. Almacenamiento de Datos Personales

Cada una de las bases de datos que se conformen al interior de la Institución deberán garantizar medidas de seguridad, las cuales permiten demostrar al titular y a la Superintendencia de Industria y Comercio – SIC como ente vigilante, los controles implementados para asegurar la custodia de la información allí contenida. Las medidas de seguridad que se deben implementar, de forma enunciativa, más no limitativa son:

- *Conservar la información en repositorios seguros, en especial se esté frente a datos sensibles.*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

- *La consulta de información contenida en la base de datos será únicamente por personal debidamente autorizado de cada una de las áreas de la Unidad de Gestión General del Ministerio de Defensa Nacional.*

- *El almacenamiento deberá garantizar la integridad de dato, parámetros definidos para ser modificado y su disponibilidad en el tiempo.*

- *Revisión periódica de los accesos concedidos a los funcionarios, con la finalidad de determinar la necesidad de conocer la información contenida en la base de datos para llevar a cabo la ejecución de sus funciones. Esta labor será desarrollada por el líder de proceso o jefe de área.*

- *Informar o alertar al Oficial de Tratamiento de Datos Personales sobre riesgo o posibles afectaciones a la base de datos.*

8.5.5. Uso y Circulación de los Datos Personales

Respecto al uso de la información que cada área les dé a los datos personales, deberá corresponder con las finalidades previamente informadas al momento de haber recolectado la autorización por parte del titular. El compromiso se materializa en que los funcionarios:

- *El tratamiento deberá corresponder a lo informado al momento de haber recolectado la autorización.*

- *Deberían informar el titular en caso de que la finalidad del tratamiento de los datos personales sea modificada.*

- *En los casos en los que la Unidad de Gestión General del Ministerio de Defensa Nacional no tenga la certeza de haber recolectado la autorización en debida forma, se abstendrán de realizar tratamiento de su información, hasta tanto no se solicite nuevamente, o se limite a ejecutar una orden legal o contractual.*

- *Ante dudas en la viabilidad de una eventual circulación de información, deberá consultarse con el Oficial de Tratamiento de Datos Personales.*

8.5.6. Supresión

La supresión de los datos personales es una exigencia de la Ley sobre los cuales no se cuenta con una finalidad legítima para permanecer almacenados al interior de la entidad.

Cuando se eliminen documentos físicos o electrónicos contenidos de datos personales, se deberá efectuar un procedimiento que asegure:

- *Que la eliminación sea autorizada.*

- *Que sea apropiada e irreversible.*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

- *Que sea documentada y confidencial.*

Lo anterior, solo se puede realizar si las series documentales han perdido valor y utilidad administrativa. Cuando el titular tenga una relación contractual vigente, no procederá la solicitud de supresión, ni cuando las normas aplicables exijan la conservación; caso de la información contable y del sistema general de seguridad social.

Cuando se realice la supresión de datos personales de las bases de datos, deberá dejarse constancia de ello a través de un acta o documento equivalente.

8.6. Riesgos y Controles

La Unidad de Gestión General del Ministerio de Defensa Nacional, ha implementado controles que le permitan manejar adecuadamente los riesgos asociados al tratamiento de datos personales, entre ellos los siguientes:

***Normatividad Interna:** para el tratamiento de datos se tienen diferentes documentos, procedimientos, políticas, reglas de negocio, entre otros, para manejar y controlar adecuadamente los riesgos inherentes al tratamiento de datos personales, los cuales se encuentran formalizados y publicados en el Sistema de Gestión Integral (SIG).*

Igualmente, frente a los formatos de recolección de datos personales de los diferentes procesos del Ministerio de Defensa Nacional, estos deben contar con los textos referentes a protección de datos (autorización para el tratamiento y aviso de privacidad).

Sistema de administración de riesgos asociados al tratamiento de datos personales:

***Identificación y medición:** a través de la matriz de riesgos se identifican y miden los riesgos asociados al tratamiento de datos personales el riesgo relacionado con el tratamiento de datos personales se identificó como medio.*

***Control:** los riesgos relacionados con el tratamiento de datos personales se controlan a través de la ejecución del plan de protección de datos y de las diferentes políticas, actividades, capacitaciones, planes, etc. que se aprueban, implementan y ejecutan al interior de la entidad.*

***Monitoreo:** el monitoreo al cumplimiento del programa y sus medidas de control se realiza a través de la auditoría anual a cargo de la auditoría interna. En la auditoría que se realiza al cumplimiento de la normatividad de protección de datos y a las medidas de control implementadas se valida, entre otras cosas:*

Los indicadores los cuales evidencian la efectividad del sistema de administración de riesgos, funcionamiento de forma oportuna, efectiva y eficiente de los controles.

Que los riesgos residuales se encuentren en niveles aceptables ocurrencia y atención de incidentes de seguridad.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

8.7. Formato

La Unidad de Gestión General del Ministerio de Defensa Nacional, ha implementado el formato de recolección de datos personales de los diferentes procesos del Ministerio de Defensa Nacional, estos deben contar con los textos referentes a protección de datos (autorización para el tratamiento y aviso de privacidad).

FORMATO DE AUTORIZACIÓN TRATAMIENTO DE DATOS PERSONALES

De conformidad con lo dispuesto en las normas vigentes sobre protección de datos personales, en especial la Ley 1581 de 2012 y el Decreto 1074 de 2015, autorizo libre, expresa e inequívocamente al **Ministerio de Defensa Nacional**, para que realice la recolección y tratamiento de mis datos personales que suministro de manera veraz y completa, los cuales serán utilizados para los diferentes aspectos relacionados con la gestión del talento humano de la entidad.

Así mismo, declaro que conozco que la recolección y tratamiento de mis datos se realizará de conformidad con la **Política de Protección de Datos Personales** y el **Aviso de Privacidad** disponibles en la página web www.mindefensa.gov.co, manifestando que he sido informado(a) de forma clara y suficiente de los fines de su tratamiento y la posibilidad que tenía de no efectuar la autorización en aquella información considerada sensible.

Manifiesto que como titular de la información, fui informado de los derechos con que cuento como titular de la información, especialmente a conocer, actualizar y rectificar mi información personal, revocar la autorización y solicitar la supresión del dato, las cuales podré ejercer a través de los canales presenciales, El ciudadano podrá presentar personalmente su solicitud relacionada con el tratamiento de sus datos personales en el **Ministerio de Defensa Nacional, ubicado en la Carrera 54 No. 26-25 Edificio Fortaleza - Bogotá D.C. en el correo usuario@mindefensa.gov.co o a través del teléfono: +57 (1) 3150111 y/o Línea de Atención y Orientación Ciudadana 018000913022**

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.

En constancia de lo anterior, se firma este documento a los [__] días, del mes de [__ de 20[__].

Cordialmente,

Firma: _____

Nombre: _____

Identificación: _____

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

8.8. Inventario de bases de datos Personales

La Unidad de Gestión General del Ministerio de Defensa Nacional cuenta con el inventario de bases de datos de las cuales tiene la calidad de responsable.

El inventario de bases de datos está compuesto por tres documentos así:

***Inventario general de bases de datos:** En este documento reposan los reportes por parte de los trabajadores o equipos de trabajo que tienen a cargo o manejan bases de datos con información personal.*

***Consolidado de bases de datos:** En este documento se identifican las bases de datos de manera general, adicionalmente se muestra información del almacenamiento y de responsables por cada etapa del tratamiento al interior de la entidad por cada base de datos.*

***Inventario desagregado de bases de datos:** Este documento contiene cada base de datos, de manera independiente, con la información reportada por parte de los trabajadores o equipo de trabajo. Consultar Inventario de Bases de Datos*

1. *Servidores públicos activos*
2. *Servidores públicos retirados de la UGG*
3. *Aprendices / Practicantes.*
4. *Aspirantes Procesos de Selección de Usuarios o Ciudadanos.*
6. *Oferentes/ Contratistas.*
7. *Proveedores.*
8. *Grupos de Interés.*
9. *Junta Directiva.*
10. *Accionistas*
11. *Pólizas de Seguros.*
12. *Procesos Judiciales.*
13. *Registros de Seguridad.*
14. *Beneficios Convencionales.*
15. *Accidentes eléctricos.*

9 LINEAMIENTOS PARA EL MANEJO DE DATOS PERSONALES

La Unidad de Gestión General del Ministerio de Defensa Nacional, cuenta con la política de Protección de Datos Personales la cual da el lineamiento general para el cumplimiento normativo en el tema, esto a través de la implementación de medidas tendientes a garantizar la seguridad y confidencialidad de la información personal que reposa en sus bases de datos y garantizar el pleno y efectivo ejercicio de los derechos por parte de los titulares.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

9.1 Tratamiento de Datos Personales

En cada etapa del tratamiento la Unidad de Gestión General del Ministerio de Defensa Nacional, a través del instructivo para el tratamiento de datos personales imparte e implementa directrices para realizar un adecuado tratamiento en cada etapa del ciclo de los datos (recolección, almacenamiento, uso, circulación y eliminación o supresión) en todos los procesos de la Unidad de Gestión General del Ministerio de Defensa Nacional.

9.2 Parámetros para la Eliminación segura de la Información

Eliminación segura de la información la Unidad de Gestión General del Ministerio de Defensa Nacional, a través del instructivo para la eliminación segura de la información implementa un procedimiento que garantiza que la eliminación que se realice de la información personal sea de forma segura, garantizando los principios de seguridad y confidencialidad de los datos.

La supresión de los datos personales es una exigencia de la Ley sobre los cuales no se cuenta con una finalidad legítima para permanecer almacenados al interior de la entidad.

Cuando se eliminen documentos físicos o electrónicos con datos personales, se deberá efectuar un procedimiento que asegure:

- *Que la eliminación sea autorizada.*
- *Que sea apropiada e irreversible.*
- *Que sea documentada y confidencial.*

Lo anterior, solo se puede realizar si las series documentales han perdido valor y utilidad administrativa. Cuando el titular tenga una relación contractual vigente, no procederá la solicitud de supresión, ni cuando las normas aplicables exijan la conservación; caso de la información contable y del sistema general de seguridad social.

Cuando se realice la supresión de datos personales de las bases de datos, deberá dejarse constancia de ello a través de un acta o documento equivalente.

9.3 Consultas y Reclamos

Para la atención de peticiones, quejas, reclamos, sugerencias, consultas - PQRSC la Unidad de Gestión General del Ministerio de Defensa Nacional, cuenta con los canales electrónicos y presenciales para su radicación y correspondiente gestión. Lo anterior con el fin de garantizar los derechos de los titulares de la información.

Cada una de las dependencias que conforman la Unidad de Gestión General tendrán la responsabilidad, de gestionar aquellas solicitudes de rectificación de información conforme

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

a este documento a de acuerdo con el procedimiento Gestión de PQRSCF, código RC-P-002.

9.4 Actualización de las Bases de Datos Registrados en la Plataforma del Registro Nacional de Bases de Datos – RNBD.

La obligación a cargo de la Unidad de Gestión General del Ministerio de Defensa Nacional, como responsable del tratamiento no es únicamente lo que concierne al registro de sus bases de datos, pues atendiendo a lo estipulado en la Circular 003 de 2018 deberá cumplir con la fase de actualización, es por eso, que cada una de las áreas responsables de las bases de datos registradas, deberá informar al Oficial de Tratamiento de Datos Personales los cambios o modificaciones que deben realizar, para hacer dentro de los siguientes plazos:

a) Dentro de los diez (10) primeros días hábiles de cada mes, a partir de la inscripción de la base de datos, cuando se realicen cambios sustanciales en la información registrada.

b) Anualmente entre el 2 de enero y el 31 de marzo, a partir de 2020.

Los cambios sustanciales, a los cuales se hace referencia son:

- *Finalidad de las bases de datos.*
- *Encargado del tratamiento.*
- *Canales de atención al titular.*
- *Tipos de datos personales almacenados.*
- *Medidas de seguridad.*
- *Política de Tratamiento de Datos Personales.*
- *Transferencia y transmisión internacional de datos personales.*

9.5 Contratistas y Terceras Partes

Relaciones con encargados del tratamiento en las relaciones contractuales, en virtud de las cuales se realice tratamiento por parte de encargados, se pactan las condiciones de confidencialidad y manejo de la información personal por parte de los contratistas, los cuales en virtud del contrato tienen la calidad de encargados del tratamiento.

Todos los contratistas que tienen la calidad de encargado conocen, aceptan y dan cumplimiento a la norma de protección de datos de la Unidad de Gestión General del Ministerio de Defensa Nacional, igualmente garantizan el cumplimiento a la normatividad de protección de datos y a los requerimientos o directrices que imparta la Superintendencia de Industria y Comercio en la materia, en los documentos condiciones generales contratación de bienes y servicios y en las condiciones contractuales compras menores se pactan cláusulas de protección de datos personales. Consultar documentos de condiciones generales para la contratación.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

Confidencialidad trabajadores de la Unidad de Gestión General del Ministerio de Defensa Nacional, con el fin de garantizar la confidencialidad de la información personal a la que acceden y manejan los trabajadores en el desarrollo de sus funciones, de la Unidad de Gestión General del Ministerio de Defensa Nacional, suscribe, al momento de la firma del contrato de trabajo, acuerdo de confidencialidad donde se regula el manejo que deben dar a la información.

10 GESTIÓN DE VERIFICACIÓN DEL PROGRAMA INTEGRAL DE GESTIÓN DE DATOS PERSONALES – PIGDP

El procedimiento adecuado para realizar una correcta y apropiada verificación del programa integral de gestión de datos personales – PIGDP se hará mediante revisiones de cumplimiento:

- ***Responsable y periodicidad:*** *El Oficial de Tratamiento de Datos Personales deberá realizar una revisión de cumplimiento, por lo menos una vez al año, en la cual deberá determinar el estado de cumplimiento de la entidad frente a cada uno de los controles que componen el Programa Integral de Gestión de Datos Personales.*

- ***Ejecución del nivel de cumplimiento:*** *El Oficial de Tratamiento de Datos Personales o el tercero habilitado para tal fin, ejecutará la revisión del programa en la fecha y hora establecida, para lo cual empleará los instrumentos de diagnóstico a que haya lugar.*

- ***Informe de nivel de cumplimiento:*** *El Oficial de Tratamiento de Datos Personales deberá elaborar un informe donde detalle los hallazgos encontrados, tales hallazgos deberán ser discriminados en debilidades, oportunidades, fortalezas y amenazas, de tal suerte que a partir de ellos sea posible determinar con precisión las acciones correctivas o políticas de administración tendientes a incrementar el nivel de cumplimiento de la entidad frente al régimen de protección de datos personales o a mitigar o erradicar los riesgos del tratamiento.*

- ***Monitoreo del nivel de cumplimiento:*** *Una vez definidas las acciones de mejora o políticas de administración tendientes a superar las debilidades halladas, el Oficial de Tratamiento de Datos Personales procederá a su implementación y seguimiento.*

11 INDICADORES

La creación e implementación del Programa Integral de Gestión de Datos Personales – PIGDP en la Unidad de Gestión General del Ministerio de Defensa Nacional, brinda la oportunidad de medir y mejorar la manera en que se están supervisando las actividades direccionadas a proteger los datos personales._¿Cuáles son?

12 *PLAN DE FORMACIÓN Y SOCIALIZACIÓN*

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

En el plan de Formación y Educación de Unidad de Gestión General del Ministerio de Defensa Nacional, se incluyen anualmente actividades de capacitación en materia de protección de datos los trabajadores de Ministerio de Defensa Nacional son capacitados generalmente en el tema a través de:

***Inducción:** En la inducción a los nuevos funcionarios de la Unidad de Gestión General del Ministerio de Defensa Nacional se capacitan en el tema a través del curso virtual de protección de datos, el curso debe ser aprobado, en caso de no aprobar dicho curso deberá presentarlo nuevamente.*

***Curso virtual:** Este curso se encuentra disponible para los trabajadores en cualquier momento en el siguiente enlace https://campusvirtual.sic.gov.co/webWordp/?project=home-campus-virtual*

12.4 *Oficial de Protección de Datos*

Capacitaciones Oficial de Protección de Datos: El oficial de protección de datos impartirá las capacitaciones que estime necesarias y dependiendo de las necesidades que se tengan al interior en el plan de capacitaciones la Unidad de Gestión General del Ministerio de Defensa Nacional es construido por el área de Desarrollo Humano con el apoyo del Oficial de Protección de datos.

12.5 *Gestores*

Los encargados del tratamiento de datos personales: La Unidad de Gestión General del Ministerio de Defensa Nacional, recibirán capacitación en el tema a través del curso virtual de protección de datos o inducción por parte del oficial de protección de datos.

12.6 *¿Gestores de?*

La Unidad de Gestión General del Ministerio de Defensa Nacional, brindara capacitación en el tema a través del curso virtual de protección de datos o inducción por parte del oficial de protección de datos o los gestores al personal de funcionarios públicos con el fin de tener claridad en lo referente al tema de autorización de recolección de datos, almacenamiento, uso, modificación, circulación y supresión de datos personales.

13 *EVALUACIÓN, REVISIÓN Y SEGUIMIENTO*

***Plan de supervisión y revisión:** anualmente dentro del plan de auditoría se incluye una auditoría al cumplimiento de la normatividad en protección de datos, igualmente el oficial de protección de datos anualmente validará el cumplimiento del presente programa por parte de las diferentes áreas o equipos del Ministerio de Defensa Nacional. Con base en los resultados de la evaluación, el oficial de protección de datos realizará, en caso de ser necesario, las actualizaciones de:*

a) Las normas e instrumentos utilizados para dar cumplimiento al presente programa.
b) Los instrumentos utilizados para la formación de los trabajadores de la Unidad de Gestión General del Ministerio de Defensa Nacional y los controles que se deben aplicar.

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.

Evaluar y revisar los controles del programa: *Con el fin de evaluar y revisar los controles implementados para dar cumplimiento a la normatividad de protección de datos el Oficial de Protección de datos anualmente elaborará un informe el cual debe incluir:*

- *Las últimas amenazas y riesgos al tratamiento de datos personales de la Unidad de Gestión General del Ministerio de Defensa Nacional.*
- *Nuevas amenazas en los controles del programa.*
- *Nuevos servicios que involucren una mayor recolección, uso o divulgación de información personal.*
- *Cumplimiento del plan de capacitaciones en la materia.*

14 *REFERENCIAS*

- *Superintendencia de Industria y Comercio*
- *Directiva Permanente No. 03/ 2019 MDN.*
- *Ley 1581 del 2012*
- *Ley 1712 del 2014*
- *Decreto 0103 del 20 de enero 2015*
- *Decreto 1074 del 26 de mayo 2015*
- *Decreto 1377 del 27 junio 2013*
- *Resolución 1713 del 16 de junio 2020*
- *Resolución 0924 del 04 junio 2020*
- *Resolución 1480 del 29 de marzo 2022*
- *Universidad de Cundinamarca*
- *Universidad EAN*
- *Ley Estatutaria 1266 de 2008*
- *Directiva Permanente DIR2014-18 "Políticas de Seguridad de la Información para el Sector Defensa".*

ANA MARÍA GARZÓN BOTERO
Secretaría General Ministerio de Defensa Nacional

VoBo: DR. JUAN JOSÉ GUARÍN
Asesor jurídico Secretaría General Ministerio de Defensa Nacional

Reviso: CR YOHAN EDUARDO POLANCO SOLER
Oficial de Protección de Datos Personal UGG Ministerio de Defensa Nacional

Reviso: MY LUIS CARLOS HERRERA VELÁSQUEZ
Jefe Oficina CSIRT Ministerio de Defensa Nacional

Elaboró: SVIF VALDERRAMA RAMIREZ YERSON
Gestor Datos Personales Ayudantia General MDN

Este documento es propiedad del Ministerio de Defensa Nacional, no está autorizado su reproducción total o parcial.