POLÍTICA GENERAL DE SEGURIDAD, PROTECCIÓN Y CONFIDENCIALIDAD DE LA INFORMACIÓN DE LA UNIDAD DE BÚSQUEDA DE PERSONAS DADAS POR DESAPARECIDAS EN EL CONTEXTO Y EN RAZÓN DEL CONFLICTO ARMADO -UBPD-

I. INTRODUCCIÓN

La Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (en adelante, la UBPD) tiene la responsabilidad de adoptar e implementar políticas de seguridad de la información que atiendan los requerimientos legales, técnicos y administrativos propios de las entidades públicas y a su vez las necesidades de protección de información para cumplir a cabalidad con su mandato, salvaguardando su carácter humanitario y extrajudicial, así como el carácter confidencial de la información que reciba, recaude o produzca en desarrollo de su misión de búsqueda. Respecto de la primera, se rige por las normas de derecho público y la jurisprudencia. Frente a los temas objeto del desarrollo misional, la UBPD se rige por el marco jurídico para el manejo de la información misional establecido por el Acto Legislativo 1 de 2017, el Decreto Ley 589 de 2017, las Sentencias C-067 de 2018 y C-080 de 2018 de la Corte Constitucional y los decretos reglamentarios que lo desarrollan.

La Política General de Seguridad, Protección y Confidencialidad de la Información describe el sustento normativo y establece los criterios y reglas que debe seguir cualquier servidor (a), contratista o personal delegado de la UBPD cuando genere, acceda, recaude, reciba, almacene, transporte o intercambie información que contribuya a la implementación de acciones humanitarias y extrajudiciales para la búsqueda. La información, contenida en documentos, independientemente de su soporte[1], puede referirse tanto a personas, hechos, lugares, como a contextos de regiones, actores o periodos que permitan la caracterización del conflicto armado y las modalidades, prácticas y tipologías de desaparición. También, incluye los criterios y reglas para el registro de datos que contribuyan a la búsqueda de personas dadas por desaparecidas que sean puestos en conocimiento de la UBPD por distintas vías, como derechos de petición, solicitudes de búsqueda, llamadas telefónicas, redes sociales, contactos directos o espacios de socialización.

II. OBJETIVO

Definir el marco general de actuación institucional, los criterios, reglas, condiciones y pautas para la gestión en la UBPD de la seguridad, protección y confidencialidad de la información que contribuya a la búsqueda de personas dadas por desaparecidas en el contexto y en razón del conflicto armado, con el fin de garantizar su custodia, integridad, conservación, preservación, disponibilidad,

[1] Formato físico o electrónico. Así el formato físico hace referencia al soporte papel y el formato electrónico o formato no tradicional se refiere a los documentos especiales en formato electrónico: audios, vídeos, correos electrónicos, bases de datos, contenidos en redes sociales, entre otros.

clasificación, reserva legal, confidencialidad y tratamiento seguro, así como una idónea gestión de riesgos asociados a ella.

III. ÁMBITO Y ALCANCE

La Política General de Seguridad, Protección y Confidencialidad de la Información aplicará a toda información que contribuya a la búsqueda de personas dadas por desaparecidas en el contexto y en razón del conflicto armado, recibida, recolectada o producida por la UBPD a nivel central y en sus equipos territoriales en todos los procesos, procedimientos y actividades. La Política General de Seguridad, Protección y Confidencialidad de la Información es de estricta observancia por los (las) servidores (as), contratistas o personal delegado de la UBPD, inclusive cuando las actividades de gestión o tratamiento de la información no sean parte de su función principal. La Política General de Seguridad, Protección y Confidencialidad de la Información se aplica a todas las fases de gestión y tratamiento de la información, incluyendo los canales de comunicación usados para su recolección, transporte, almacenamiento, custodia, preservación, conservación o intercambio.

IV. MARCO NORMATIVO

El marco normativo que soporta la Política General de Seguridad, Protección y Confidencialidad de la Información en la UBPD se fundamenta en los artículos 8, 15, 20, 23 y 94 de la Constitución Política, los artículos transitorios 3 y 4 del Acto Legislativo 01 de 2017, el Decreto Ley 589 de 2017, el Decreto 1393 de 2018, la Ley 1712 de 2014, la Ley 1581 de 2012, la Ley 1621 de 2013 y las Sentencias C-067 de 2018 y C-080 de 2018 de la Corte Constitucional, de las cuales se desprenden las siguientes consideraciones:

Esencia humanitaria y carácter extrajudicial de la UBPD y de su mandato. La Corte Constitucional equiparó la naturaleza de la UBPD con la de un organismo humanitario, como, por ejemplo, el Comité Internacional de la Cruz Roja (CICR), que adelanta sus actividades en un marco de la confidencialidad, a fin de generar confianza en los ciudadanos, y así obtener información útil para la búsqueda de las personas dadas por desaparecidas.

Precisamente, como organismo humanitario y extrajudicial, la UBPD cuenta con una serie de privilegios e inmunidades que fueron integrados en la normativa, entre otros, lo relacionado con el manejo de la información, por ello, la información que reciba, recaude no podrá ser utilizada con el fin de atribuir responsabilidades en procesos judiciales y no tendrá valor probatorio[2], a excepción de los informes técnico – forenses y los elementos materiales asociados al cadáver. En virtud de lo anterior, la información misional de la UBPD es confidencial y los (las) servidores (as), contratistas o personal delegado de la UBPD en ejercicio de las actividades previstas en el Decreto Ley 589 de 2017, están

[2] Decreto Ley 589 de 2017, "Por el cual se organiza la Unidad de Búsqueda de Personas Dadas por Desaparecidas en el contexto y en razón del conflicto armado", artículo 3.

exonerados (das) del deber de denuncia y tampoco podrán ser obligados (das) a declarar en procesos judiciales por hechos que hayan conocido en desarrollo de sus funciones misionales, y únicamente pueden ser citados (as) para ratificar y explicar los informes técnicos forenses en los que hayan participado, así como respecto de los elementos asociados al cadáver recaudados por la UBPD[3].

Recolección de información en la UBPD. La UBPD, de conformidad con su mandato, debe recolectar la información necesaria para la búsqueda de las personas dadas por desaparecidas en contexto y en razón del conflicto armado, el establecimiento y caracterización del universo de éstas, la creación e implementación de un registro nacional de fosas, cementerios ilegales y sepulturas. Para ello, el Decreto Ley 589 de 2017 menciona algunas de las fuentes de información a las que puede recurrir la UBPD, señalando entre otras las siguientes: i) las entrevistas confidenciales; y ii) las bases de datos "mecánicas, magnéticas y otras similares", así como toda información que dispongan personas, entidades del Estado u organizaciones sociales y de víctimas.

Facultad de acceso a la información. Como mecanismo extrajudicial y de justicia transicional, los artículos transitorios 3 y 4 del Acto Legislativo 001 de 2017 y el título III del Decreto Ley 589 de 2017 establecen que la UBPD tiene facultades amplias de acceso a información pública, inclusive aquella clasificada, reservada y confidencial, que contribuya a la búsqueda de personas desaparecidas y de celebrar convenios y acuerdos con privados para acceso a información. Estas facultades están acompañadas del deber de garantizar la reserva y confidencialidad de la información a la que accede, recibe y/o produce la UBPD. Sobre estas facultades, la Corte Constitucional declaró la constitucionalidad de las disposiciones del Decreto Ley 589 de 2017 y la constitucionalidad condicionada de algunos apartes de los artículos 12, 13 y 14[4].

Clasificación de la información para su protección. La normatividad sobre el derecho de acceso a la información en Colombia, en especial la Ley 1712 de 2014, establece que toda la información que recolecte o produzca una entidad estatal es información pública y puede clasificarse para restringir su acceso, únicamente de la siguiente manera:

---

[3] Ibídem. Artículo 19 y Artículo Transitorio 4 del Acto Legislativo 01 de 2017.

[4] Al respecto, la Corte aclaró que "el marco jurídico dentro del cual debe comprenderse el acceso a la información de la UBPD para el desarrollo de sus funciones, incorpora tanto los estándares internacionales como los parámetros constitucionales en materia de acceso a la información, específicamente, frente a graves violaciones de los derechos humanos. De esta manera, a la regulación prevista en el Decreto Ley 589 de 2017, se debe agregar lo dispuesto en los artículos 20, 23, 74 y 209 de la Constitución, a partir del contenido y alcance que sobre dichos preceptos se ha fijado por la jurisprudencia de la Corte. Y también debe tenerse en cuenta, con criterio vinculante, lo señalado en los tratados y convenios internacionales ratificados por Colombia, en virtud de lo dispuesto en el artículo 93 del Texto Superior, que al referir al bloque de constitucionalidad en sentido estricto, incorpora como mandatos exigibles a la Declaración Universal de los Derechos Humanos (art. 19), a la Convención Americana de Derechos Humanos (art. 13) y al Pacto Internacional de Derechos Civiles y Políticos (art. 19), en lo referente a la regulación sobre la libertad de expresión y el acceso a información pública (…) También constituyen parámetro imperativos en esta materia, como se expuso en la Sentencia C-017 de 2018, las leyes estatutarias de Transparencia y del Derecho de Acceso a la Información Pública Nacional (Ley 1712 de 2014); de Inteligencia y Contrainteligencia (Ley 1621 de 2013); del Derecho de Petición (Ley 1755 de 2015); y de Protección de Datos Personales (Ley 1581 de 2012), así como los fallos que definieron la constitucionalidad de estas leyes, en lo relacionado con el derecho de acceso a la información, esto es, las Sentencias C-274 de 2013, C-540 de 2012, C-951 de 2014 y C-748 de 2011." Corte Constitucional, Sentencia C-067 de 2018.

- **Información pública clasificada.** Se refiere a aquella información que pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica, por lo que su acceso puede ser negado o exceptuado para proteger su derecho a la intimidad y a la vida, salud o seguridad. Los datos personales para la identificación de las personas dadas por desaparecidas, así como los de sus familiares y los datos personales de las personas que entreguen información a la UBPD son clasificados y deben ser protegidos. Así mismo es clasificada, la Información recibida por la UBPD en virtud del literal a) y c) del numeral 1 del Artículo 5 del Decreto Ley 589 de 2017, es decir aquella información que provenga de personas que voluntariamente suministren información que contribuya a la búsqueda, localización, recuperación e identificación de personas dadas por desaparecidas en el contexto y en razón del conflicto armado, incluyendo quienes hayan participado directa o indirectamente en las hostilidades.

- **Información pública reservada.** Es aquella información, cuyo acceso a la ciudadanía puede ser negado de manera motivada y por escrito, cuando lo establezca una norma legal o constitucional y el contenido de la información pueda poner en riesgo los siguientes intereses: la defensa y seguridad nacional; la seguridad pública; las relaciones internacionales; la prevención, investigación y persecución de los delitos y faltas disciplinarias, mientras que no se haga efectiva la medida de aseguramiento o se formule pliego de cargos; el debido proceso y la igualdad de las partes en los procesos judiciales; la administración efectiva de justicia; los derechos de la infancia y adolescencia; la estabilidad macroeconómica y financiera del país y la salud pública. También se considera información pública reservada "los documentos que contengan opiniones o puntos de vista que formen parte del proceso deliberativo de los servidores públicos"[5]. Dentro de la información reservada, relevante para la búsqueda de personas dadas por desaparecidas, se encuentra:

    A. Información de inteligencia y contrainteligencia de acuerdo con el artículo 33 de la Ley 1621 de 2013 y su Decreto Reglamentario 857 de 2 de mayo de 2014. Además de los Decretos sobre la extinción del Departamento Administrativo de Seguridad – DAS y conformación de la Dirección Nacional de Inteligencia Decretos 4179, 4057 de 2011 y Decreto 1303 de 2014.

    B. Información con reserva judicial de acuerdo con los procedimientos judiciales aplicables.

    C. Información recibida por la UBPD en virtud del artículo 14 del Decreto Ley 589 de 2017, es decir aquella información a la que se acceda por contratos, convenios y/o protocolos de acceso a información con cualquier tipo de organización nacional o

[5] Parágrafo Artículo 19 de la Ley 1712 de 2014.

internacional de derecho público o privado, incluyendo organizaciones de víctimas y de derechos humanos, nacionales o extranjeras.

Derecho de acceso a la información. El artículo 4 de la ley 1712 de 2014 (Ley Estatutaria de Transparencia y del Derecho de Acceso a la Información Pública Nacional) establece que el derecho de acceso a la información se refiere a la posibilidad que tiene todo ciudadano de conocer la existencia y acceder a la información pública en posesión o bajo control de los sujetos obligados. Además, aclara que las restricciones legales se pueden referir al acceso a la información, pero nunca a la existencia de la información. Así las cosas, con el propósito de garantizar el derecho de acceso a la información de la ciudadanía y al mismo tiempo proteger la información clasificada, reservada y confidencial a la que acceda la UBPD, se deben definir criterios, condiciones y pautas para registrar la existencia de la información controlada por la UBPD, poderla clasificar y almacenar de forma adecuada, garantizando las restricciones al acceso de la misma.

Protección de datos personales. Para cumplir con sus funciones, la UBPD debe registrar datos personales tanto de las personas dadas por desaparecidas y de sus familiares, así como de aquellas personas que entreguen información. Para proteger estos datos, debe darse cumplimiento a la Ley 1581 de 2012 y la política de protección de datos personales de la UBPD, así como establecer protocolos respecto del almacenamiento de información clasificada, reservada y confidencial, particularmente sensible.

Responsabilidad en la custodia de información. El artículo 12 del Decreto Ley 589 de 2017 establece que "*(…) cuando se trate de información reservada, la UBPD, en todo caso, deberá garantizar, por escrito, la reserva de la misma, el traslado de la reserva legal de la información, suscribir actas de compromiso de reserva y observar las seguridades y niveles de clasificación consagradas en la Ley Estatutaria 1621 de 2013, la Ley Estatutaria 1712 de 2014, sus Decretos Reglamentarios y otras normas relevantes, sin perjuicio de las acciones penales, disciplinarias y fiscales a que haya lugar por violación de la reserva legal (…)*".

Asimismo, en virtud del artículo 14 del Decreto Ley 589 de 2017, la UBPD está facultada para suscribir contratos, convenios y/o protocolos de acceso a información con cualquier tipo de organización nacional o internacional de derecho público o privado, incluyendo organizaciones de víctimas y de derechos humanos, nacionales o extranjeras. En todo caso, a UBPD deberá establecer las condiciones de confidencialidad que fueren necesarias para su adecuado uso y para la protección de las personas mencionadas en ella y sujetarse en materia de información pública, a los parámetros de información reservada y clasificada de los artículos 18 y 19 de la Ley 1712 de 2014, Estatutaria de Transparencia y del Derecho de Acceso a la Información Pública Nacional, y 24 de la Ley 1755 de 2015, Estatutaria del Derecho de Petición, o a las disposiciones que las reemplacen, sustituyan o deroguen.

Por su parte, el Código Disciplinario Único, Ley 734 de 2002, contempla en el Artículo 35 que "*a todo servidor público le está prohibido: (...) 13. Ocasionar daño o dar lugar a la pérdida de bienes, elementos, expedientes o documentos que hayan llegado a su poder por razón de sus funciones. (...) 21. Dar lugar al acceso o exhibir expedientes, documentos o archivos a personas no autorizadas*".

Por lo tanto, los (las) servidores (as), contratistas o personal delegado de la UBPD tendrán la obligación de suscribir y cumplir el compromiso de guarda de confidencialidad de la información al momento de vincularse a la UBPD, teniendo como fundamento, las siguientes normas: el "Acuerdo Final para la terminación del conflicto armado y la construcción de una paz estable y duradera"; el Decreto Ley 589 de 2017; los principios establecidos en la Ley Estatutaria 1581 de 2012 (Ley de Hábeas Data) y su Decreto reglamentario 1377 de 2013; la Ley 1712 de 2014 (Ley de transparencia y acceso a la información pública) y su Decreto reglamentario 103 de 2015; la Ley 734 de 2002 (Código Disciplinario Único, que será derogada el 1 de julio de 2021 por la ley 1952 de 2019); la Ley 1952 de 2019 (Código General Disciplinario); la Ley 23 de 1982 (Protección de Derechos de Autor); el Código Civil en su artículo 1494; y la Sentencia C-067 de 2018 de la Corte Constitucional.

Gestión documental y Archivo. La Ley 594 de 2000, Ley General de Archivos, especialmente en lo relacionado a las actividades de gestión documental establece que es importante que las disposiciones adicionales se articulen con el Programa General de Gestión Documental que adopte la UBPD. Además, esta política utiliza como referencia el Protocolo de Gestión Documental de los archivos referidos a las graves y manifiestas violaciones a los derechos humanos, e infracciones al Derecho Internacional Humanitario, ocurridas con ocasión del conflicto armado interno[6], sin perjuicio del carácter confidencial o bajo reserva legal de la información misional de la UBPD.

V. ELEMENTOS DE LA POLÍTICA

5.1. DECLARACIÓN DE LA POLÍTICA

La UBPD como responsable de garantizar la custodia, integridad, conservación, preservación, disponibilidad, clasificación, reserva legal, confidencialidad, y tratamiento seguro de la información que produce y a la que tiene acceso en desarrollo de su misión, funciones y deberes, se compromete a establecer estrategias, lineamientos, protocolos, controles, proyectos, programas, planes y mecanismos de seguridad de la información, para el tratamiento seguro de la misma, por parte de sus servidores (as), contratistas o personal delegado. Lo anterior, considerando una gestión apropiada de los riesgos y el cumplimiento de los requisitos legales, las necesidades de la entidad, de los (las) aportantes, familiares y las partes interesadas sobre la seguridad de la información, así, generar la

6 Archivo General de la Nación y Centro Nacional de Memoria Histórica. *Protocolo de Gestión Documental de los archivos referidos a las graves y manifiestas violaciones a los derechos humanos, e infracciones al Derecho Internacional Humanitario, ocurridas con ocasión del conflicto armado interno*. Febrero de 2017. Disponible en http://www.centrodememoriahistorica.gov.co/descargas/protocolo-gestion-documental.pdf Consultado en octubre de 2018.

confianza necesaria que incentive a la sociedad en general a suministrar información para la búsqueda de las personas dadas por desaparecidas en el contexto y en razón del conflicto armado.

5.2. PRINCIPIOS

A cargo de la UBPD está la búsqueda de personas dadas por desaparecidas antes del 1ro de diciembre de 2016 (fecha de entrada en vigencia del Acuerdo Final de Paz) y que corresponden a cualquiera de las siguientes circunstancias, siempre en el contexto y en razón del conflicto armado:

- Desaparición forzada.
- Secuestro.
- Reclutamiento ilícito o constreñimiento de apoyo bélico.
- Desapariciones durante las hostilidades.

Para esta labor, la UBPD tiene un mandato de 20 años en los cuales, además de buscar a las personas dadas por desaparecidas, contribuirá a la satisfacción de los derechos a la verdad y a la reparación de las víctimas, garantizando la participación a través del rol activo de los familiares en cada una de las fases del proceso de búsqueda.

Todo lo anterior tiene como fin último materializar la esencia humanitaria de aliviar el sufrimiento de familiares, allegadas, asociaciones de familiares, organizaciones de derechos humanos que acompañan la búsqueda las comunidades y pueblos étnicos, así como contribuir a la satisfacción de los derechos y, en consecuencia, a la dignificación de quienes buscan a las personas dadas por desaparecidas.

Conforme a lo anterior, la UBPD propende porque todas las acciones humanitarias de búsqueda tengan como eje central a las familias, colectivos, organizaciones, pueblos, comunidades y demás grupos de valor, reconociéndolos como sujetos de derechos que participan activamente, se relacionan de forma consciente y toman decisiones informadas durante proceso de búsqueda, por ello se pretende que toda interacción entre la ciudadanía y la entidad sea dignificante y diferencial. También dentro de este enfoque humanitario están las personas dadas por desaparecidas que se buscan.

Es pertinente recalcar que la esencia humanitaria de la UBPD se complementa con el carácter extrajudicial, lo que produce una serie de consecuencias, entre las que se encuentra, en lo que respecta a la seguridad de la información, la naturaleza confidencial de la información que reciba y produzca. En otros términos, el carácter extrajudicial garantiza la efectividad del trabajo humanitario, pues los datos que reciba o produzca la UBPD no podrán ser utilizados para atribuir responsabilidades en procesos judiciales y no tendrán valor probatorio. Así, se promueven las relaciones de confianza entre la UBPD y las personas que cuenten con información útil que contribuya al proceso de búsqueda de personas dadas por desaparecidas.

Entonces, la esencia humanitaria y el carácter extrajudicial de la UBPD se equipara, según fue destacado por la Corte Constitucional en Sentencia C-080 de 2018, a la de un organismo humanitario, como por ejemplo, el Comité Internacional de la Cruz Roja (CICR). En este sentido, en general, la labor de la UBPD como entidad estatal humanitaria y extrajudicial, se enmarca dentro de los principios fundamentales relacionados con el Derecho Internacional de los Derechos Humanos y el Derecho Internacional Humanitario, a saber:

- **Humanitario:** todas las acciones de la UBPD se guían por la única consideración de brindar alivio al sufrimiento de las personas que buscan y de las personas dadas por desaparecidas. Por tanto, todas las acciones de búsqueda se realizan bajo la presunción de que la persona dada por desaparecida está con vida y que cada una implica la existencia de, como mínimo, una persona que la busca. También, dado que todas las acciones se guían por la lógica humanitaria, el carácter extrajudicial de la UBPD implica que las acciones se realizan exclusivamente para el establecimiento de la suerte y paradero de la persona dada por desaparecida; por tanto, nunca las acciones se guiarán por la lógica judicial, es decir, para establecer responsabilidades a los autores del hecho que generó la desaparición, que incluso podría no constituir delito.

- **Neutralidad:** con el fin de construir la confianza, la UBPD y sus equipos de trabajo deben actuar bajo el principio de neutralidad frente a los actores del conflicto armado, por tanto, pueden favorecer el esfuerzo bélico de una de las partes en conflicto, ni pueden ser percibidos como tales en sus actuaciones, tanto por los actores armados como por la población civil.

- **Imparcialidad:** con el fin de construir la confianza, la UBPD y sus equipos de trabajo deben actuar de manera imparcial y no harán distinción desfavorable respecto de las personas dadas por desaparecidas, así como de las personas que las buscan por razones o motivos de raza, color, sexo, género, orientación sexual, idioma, religión, opiniones políticas o de otra índole, origen nacional o social, nacimiento, posición económica, o cualquier otra condición social; las causas invocadas por las partes en conflicto o atribuidas a ellas, o la participación de las personas en el conflicto armado. Por tanto, las acciones de búsqueda de la UBPD están dirigidas a establecer la suerte y paradero de todas las personas dadas por desaparecidas y abarca todas las formas de desaparición ocurridas en el contexto y en razón del conflicto armado.

- **Confidencialidad:** con el fin de desempeñar con eficacia las acciones humanitarias, la búsqueda extrajudicial que realiza la UBPD se lleva a cabo en condiciones de seguridad de las personas, tanto de las que participan en la búsqueda, como de las que entregan información. Para garantizar la seguridad de las personas es necesario asegurar la confidencialidad de la información. La metodología y protocolos de trabajo de todos los

equipos tiene como base la obligación de preservar, conservar y proteger la información que reciben y producen. Esta metodología y protocolos deben ser consistentes con la disponibilidad de la información dentro de los equipos con funciones de desarrollar el proceso de búsqueda y/o las acciones humanitarias de búsqueda, de manera que cumpla el fin para el cual se recolecta, procesa, almacena y analiza; esto es, determinar la suerte y en lo posible el paradero de las personas desaparecidas para contribuir al alivio del sufrimiento de las personas que las buscan.

- **Autonomía e independencia:** la búsqueda humanitaria y extrajudicial es llevada a cabo por la UBPD, como órgano constitucional autónomo e independiente, que, aun cuando haga parte del sector justicia, no está bajo la tutela o subordinación de otra rama del Poder Público[7].

Teniendo en cuenta las anteriores condiciones normativas, los lineamientos, controles, protocolos, procesos, procedimientos y mecanismos que se deriven de esta política, estarán orientados al cumplimiento de los siguientes principios en clave de seguridad de la información:

- **Principio de precaución desde el enfoque adaptativo:** el Sistema de Gestión de Seguridad de la Información de la UBPD debe garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y mitigados por la UBPD, de una forma documentada, sistemática, estructurada, eficiente y adaptada a los cambios que se produzcan en los riesgos, en el entorno y en las tecnologías.

- **Principio de Ética:** los (las) servidores (as), contratistas o personal delegado de la UBPD deben velar por la protección de la información que contribuya a la búsqueda de personas dadas por desaparecidas en el contexto y en razón del conflicto armado, con el fin de garantizar su preservación, prevenir fugas y usos indebidos o ilegítimos. La objetividad, imparcialidad y la resistencia a cualquier tipo de presión que pretenda manipular la documentación o distorsionar los hechos hacen parte de este principio. Igualmente este principio exigirá de las personas que hacen parte de la UBPD como servidoras (es) o contratistas o delegadas, priorizar en sus decisiones y actuaciones el valor humanitario de contribución al alivio del sufrimiento de las personas que buscan y las que se encuentren desaparecidas.

[7] La CORTE CONSTITUCIONAL, mediante Sentencia C-067 de 2018, M.P. Guerrero Pérez Luis Guillermo, señala: "no implica que la Unidad esté orgánicamente sujeta al Ministerio de Justicia y del Derecho, ya que no se consagra la existencia de una relación de adscripción o de vinculación para el ejercicio de sus funciones, circunstancia que sólo sería posible al tratarse de un organismos descentralizado, lo cual no corresponde con lo señalado ni en el Acto Legislativo 01 de 2017, ni el Decreto Ley 589 de 2017, en donde se señala que la UBPD es un organismo del orden nacional, con naturaleza jurídica especial".

- **Principio pro-persona y pro-víctima:** para preservar el carácter humanitario de la UBPD, especialmente en lo relacionado con la participación de los familiares de personas dadas por desaparecidas en el contexto y en razón del conflicto armado y otras personas, organizaciones de la sociedad civil y pueblos étnicos que buscan a sus seres queridos, la interpretación y aplicación de estos principios se hará de manera tal que la gestión documental contribuya a garantizar la mayor protección de sus derechos y las menores restricciones para su ejercicio en la búsqueda de sus seres queridos. De igual manera, lineamientos, controles, protocolos, procesos, procedimientos y mecanismos, en general, que se deriven de esta política, en lo relacionado con el tratamiento de datos personales, deberán estar integrados con la política de protección de datos personales de la UBPD.

- **Principio de Confidencialidad:** la información que contribuya a la búsqueda de las personas dadas por desaparecidas y que preserve la posibilidad de desarrollar la labor humanitaria y extrajudicial es confidencial; por tanto, la UBPD no revelará, publicará, divulgará, transferirá o dará acceso a información que no sea de dominio público con la salvedad de lo establecido en los artículos 5 (numerales 6 y 7 y Parágrafo) y 19 (Parágrafo) del Decreto Ley 589 de 2017 y los artículos 13 (numeral 1) y 14 (numeral 8) del Decreto 1393 de 2018, así como por lo establecido en la Sentencia C-067/18 de la Corte Constitucional, a personas, entidades, instituciones, organizaciones o procesos no autorizados. La información puede ser vista o estar disponible sólo para las personas autorizadas.

- **Principio de Integridad:** la UBPD establecerá los mecanismos necesarios para garantizar la exactitud, completitud e inalterabilidad de la información recibida o generada en cumplimiento de su mandato constitucional y legal.

- **Principio de Disponibilidad:** la UBPD establecerá los requisitos y criterios necesarios para localizar, recuperar, presentar, interpretar y leer la información en el momento pertinente o requerido por las personas debidamente autorizadas para ello.

- **Principio de Integralidad:** la Política de General Seguridad, Protección y Confidencialidad de la Información será observada por todas (os) las (os) servidoras (es), contratistas o personal delegado de la UBPD, inclusive cuando la gestión o actividades de tratamiento de la información no sean parte de su función principal.

- **Principio de Gestión Documental:** la UBPD desarrollará, en concordancia con el principio de confidencialidad, una sola gestión documental teniendo en cuenta dos instancias. Por un lado, dado que es confidencial la información que contribuya a la búsqueda de las personas dadas por desaparecidas y que preserve la posibilidad de desarrollar la labor humanitaria y extrajudicial, la gestión de la información, es decir, el registro, protección, almacenamiento, disposición, administración y consulta; estará centralizado, como área misional, en la

Subdirección General Técnica y Territorial, específicamente en la Dirección Técnica de Información, Planeación y Localización para la Búsqueda, a través de la Subdirección de Gestión de Información para la Búsqueda. Por otro lado, la información que no contribuya a la búsqueda de personas dadas por desaparecidas (confidencial o no), estará a cargo de cada una de las dependencias de la entidad. La Gestión documental integral y el archivo total estará bajo los lineamientos y directrices de la Secretaría General, específicamente en la Subdirección Administrativa y Financiera.

- **Principio de control de la información:** la información clasificada, es decir, aquella relacionada con datos personales a la que tenga acceso la UBPD, pertenece al sujeto al que hace referencia la misma y, por tanto, éste siempre tendrá el control sobre ella. El control sobre la información implica que la persona deberá estar enterada del tratamiento que se dé a sus datos personales confidenciales y en cualquier momento podrá solicitar a la UBPD el borrado de su información.

- **Principio de uso racional de la información:** la UBPD y sus servidores (as), contratistas o personal delegado, tendrán acceso únicamente a la información que requieran para el desarrollo de su mandato y/o funciones.

5.3. CONSIDERACIONES GENERALES

La Política General de Seguridad, Protección y Confidencialidad de la Información considera, por una parte, las facultades que tiene la UBPD para acceder a información pública, inclusive aquella clasificada, reservada y confidencial, que contribuya a la búsqueda de personas desaparecidas en el contexto y en razón del conflicto armado, o de celebrar contratos, convenios y acuerdos para el acceso a información con cualquier tipo de organización nacional o internacional de derecho público o privado, incluyendo organizaciones de víctimas y de derechos humanos, nacionales o extranjeras; por otra, el deber que tiene la UBPD de garantizar la confidencialidad de la información que obtenga y produzca, salvo las excepciones legales. Lo anterior implica que, en virtud del carácter humanitario y extrajudicial de este mecanismo de justicia transicional, la información clasificada, reservada y confidencial debe ser protegida garantizando la confidencialidad de su contenido y sobre todo la que corresponda con la identidad y contacto de las personas que la entreguen.

A continuación, se describen los elementos de política para la construcción de estrategias, lineamientos, protocolos, controles, proyectos, programas, planes y mecanismos de seguridad, protección y confidencialidad de la información que deben ser detallados dentro del Sistema de Gestión de la entidad.

5.3.1. GESTIÓN DOCUMENTAL

El modelo de gestión de información en la UBPD se enmarca en una sola gestión documental que, en concordancia con el principio de confidencialidad, tiene en cuenta dos instancias. La primera instancia abarca, por una parte, la información misional que contribuye a la búsqueda humanitaria y extrajudicial de personas dadas por desaparecidas, por tanto, las actividades relacionadas con la creación, recepción, mantenimiento, uso, disposición y preservación de los documentos físicos y electrónicos a través de su ciclo vital, deben hacerse considerando las particularidades que exige la salvaguarda de la confidencialidad o reserva legal de la información, con el fin de garantizar la integridad, autenticidad, fiabilidad y accesibilidad únicamente por el personal autorizado, a lo largo del tiempo.

Por otra parte, la información que no contribuye a la búsqueda de personas dadas por desaparecidas, que en general no es clasificada ni reservada, cumple con las pautas en cuanto a la gestión documental y la administración de los archivos de gestión administrativos en todo el ciclo vital de los documentos, desde que se planea hasta su disposición final, incluyendo los diferentes soportes documentales.

A continuación, se describen los demás elementos que conforman este modelo de gestión de información:

- **Usuarios (as) de la información:** se caracterizan para lograr un mejor diseño e implementación de servicios basados en las necesidades de quienes lo requieran, ya sea persona natural o jurídica, interna o externa que aportan o requieren información de la UBPD.

- **Transparencia, acceso a información y lucha anticorrupción:** la UBPD, para garantizar el acceso a la información, usará la matriz de activos de información, el Índice de Información Clasificada y Reservada y la Tabla de retención documental una vez convalidada por el Archivo general de la Nación que permiten clasificar la información en pública, pública clasificada y pública reservada. En tal sentido, se publicarán aquellos que sean obligatorios y no pongan en riesgo o comprometan su naturaleza extrajudicial y humanitaria, y que evidencien las actividades administrativas de la entidad y que sean de interés público.

- **Política de Integridad - Valores:** en todo el desarrollo de la gestión misional de la entidad se debe tener consciencia de los requisitos éticos que se aplican a la recolección y manejo de la información relacionada con las acciones humanitarias y extrajudiciales de búsqueda y localización de personas dadas por desaparecidas en el contexto y en razón del conflicto armado. Por una parte, es necesario comprender e implementar los conceptos de seguridad, protección y confidencialidad de la información y cómo se aplican en el modelo de gestión de la información; y por otra, estar en conformidad con la legislación y marcos regulatorios que pueden afectar el acceso a la misma.

- **Procesos u operaciones de gestión documental:** la información contenida en los documentos misionales es parte integral del programa de gestión documental institucional en el que se estandarizan las acciones a ejecutar en el corto, mediano y largo plazo para el control, administración y permanencia de éstos en todo el ciclo vital de los documentos.

La información que recibe, recolecta o produce la UBPD se divide, en concordancia con el principio de confidencialidad, en dos instancias que le otorgan distinta naturaleza e implicaciones legales.

5.3.1.1. INFORMACIÓN MISIONAL QUE CONTRIBUYE A LA BÚSQUEDA HUMANITARIA Y EXTRAJUDICIAL

La gestión de la información misional que contribuye a la búsqueda humanitaria y extrajudicial de las personas dadas por desaparecidas en el contexto y en razón del conflicto armado, incluida la implementación de la Política General de Seguridad, Protección y Confidencialidad de la Información, está bajo la responsabilidad de la Subdirección General Técnica y Territorial, específicamente en la Dirección Técnica de Información, Planeación y Localización para la Búsqueda, a través de la Subdirección de Gestión de Información para la Búsqueda, y bajo el liderazgo de la Dirección General de la UBPD.

Esta información se rige por el principio de confidencialidad preservando la posibilidad de desarrollar la labor humanitaria y extrajudicial de la UBPD,y cuando sean de aplicación, las normas relativas sobre reserva legal, de conformidad con lo establecido por el Decreto Ley 589 de 2017 y la Corte Constitucional en sus sentencias C-067/18 y C-080/18.

La información misional que contribuye a la búsqueda humanitaria y extrajudicial de personas dadas por desaparecidas en el contexto y en razón del conflicto armado se organiza en los siguientes tipos:

A. Información sobre personas dadas por desaparecidas, sus familiares, organizaciones de la sociedad civil que acompañan la búsqueda y pueblos étnicos;
B. Información sobre hechos de desaparición, incluidos aquellos relacionados con desaparición forzada, reclutamiento, secuestro y desaparición en el curso de las hostilidades;
C. Información sobre lugares de posible desaparición y lugares presuntos, referidos o confirmados, en los que se puede localizar a las personas desaparecidas cuando sigan con vida o sitios de disposición de cuerpos, incluida información sobre fosas, cementerios ilegales y sepulturas donde posiblemente puedan ser halladas personas dadas por desaparecidas;
D. Información sobre prospecciones y exhumaciones realizadas, así como de cuerpos recuperados identificados, identificados sin reclamar y no identificados;
E. Información sobre eventos, actores y dinámicas del conflicto armado relevantes para comprender las diferentes formas de desaparición;

F. Información sobre personas que contribuyan con información o que pueden tener información que contribuya a la búsqueda.

No obstante, dentro de la información que contribuye a la búsqueda humanitaria y extrajudicial, de conformidad con el Decreto Ley 589 de 2017, se encuentra exceptuada del principio de confidencialidad -previo cumplimiento de los criterios definidos en esta Política-, la siguiente:

A. Información que la UBPD pueda entregar durante la ejecución del plan de búsqueda a solicitud de las personas que buscan, como familiares y allegados (as) de las personas dadas por desaparecidas, comunidades y organizaciones que buscan, respetando siempre el derecho a la privacidad de las víctimas. Esto incluye la retroalimentación de la información brindada por ellas, de acuerdo con la estrategia de "recolección, retroalimentación, seguridad de la información y construcción de confianza" del Plan Nacional de Búsqueda;

B. Información sobre el reporte oficial detallado sobre lo acaecido;

C. Información sobre los elementos asociados al cadáver y los informes técnico - forenses cuando sea requerida por las autoridades judiciales competentes;

D. Información contenida en los Planes Regionales de Búsqueda;

E. Información que periódica y públicamente, al menos cada 6 meses, deba la UBPD presentar sobre las actividades de búsqueda, localización, recuperación, identificación, y entrega digna de cuerpos esqueletizados que se realicen, respetando siempre el derecho a la privacidad de las víctimas.

Para que la anterior información se pueda exceptuar del principio de confidencialidad, ésta debe atender los siguientes criterios:

A. No poner en riesgo la confidencialidad de las personas que han ofrecido información para la búsqueda, de tal manera que se garantice la generación de confianza necesaria para que quienes cuenten con información, la sigan aportando o la aporten en el futuro.

B. Resguardar los derechos a la intimidad, privacidad y la seguridad de las víctimas y los (las) aportantes de información.

C. No afectar, limitar o impedir los procesos humanitarios y extrajudiciales de búsqueda.

D. No publicar información que pueda ser utilizada con el fin de atribuir responsabilidades en procesos judiciales.

E. No señalar responsabilidades individuales. Sin embargo, en el caso de que exista una sentencia judicial o un fallo disciplinario de la Procuraduría General de la Nación, en firme y con carácter de cosa juzgada, la información sobre responsabilidades individuales (penales y/o disciplinarias) podría ser incorporada, en los términos en que fueron establecidas por la autoridad judicial o disciplinaria.

F. No reproducir información bajo reserva legal ni identificar las fuentes de carácter confidencial.

5.3.1.2. INFORMACIÓN QUE NO CONTRIBUYE A LA BÚSQUEDA HUMANITARIA Y EXTRAJUDICIAL

La información que no contribuye a la búsqueda de personas dadas por desaparecidas (confidencial o no), estará a cargo de cada una de las dependencias de la UBPD. La Gestión documental integral y el archivo total estará bajo los lineamientos y directrices de la Secretaría General, específicamente en la Subdirección Administrativa y Financiera -SAF-. La SAF se encarga de emitir los lineamientos técnicos, reglas, principios y actividades que permiten la implementación y sostenibilidad del proceso en articulación con las demás áreas y se encargan de la recopilación, organización y custodia de los archivos de la entidad.

En tal sentido, en cumplimiento de la Política General de Seguridad, Protección y Confidencialidad de la Información, la Subdirección Administrativa y Financiera, velará por la construcción y fortalecimiento de buenas prácticas en la administración de los archivos y la ejecución de los procesos de la gestión documental que van en directa relación con la preservación del patrimonio documental.

La información que no contribuye a la búsqueda, que se origina en los procesos estratégicos, de apoyo y de evaluación, y que en general no es clasificada ni reservada, se organiza en las siguientes categorías:

A. Información sobre lineamientos de funcionamiento y operación de la UBPD, tales como políticas, protocolos, guías, procesos, procedimientos y actos administrativos, exceptuando aquellos actos administrativos que contengan información que contribuye a la búsqueda de las personas dadas por desaparecidas en el contexto y en razón del conflicto armado.
B. Información contractual, entre la que se incluye aquella relacionada con el desarrollo de las etapas precontractual, contractual y pos contractual.
C. Información que se genere en el proceso financiero, logístico, recursos físicos, gestión documental, servicio al ciudadano.

D. Información originada en el proceso de seguimiento, evaluación y control como informes de auditoría de control interno, de seguimiento y evaluación a procesos internos y plan anual de auditorías, entre otros.
E. Información que se genere en el proceso de gestión del talento humano.

5.3.2. LÍNEAS DE ACCIÓN PARA LA SEGURIDAD, PROTECCIÓN Y CONFIDENCIALIDAD DE LA INFORMACIÓN

Para la creación, uso, mantenimiento, retención, acceso interno, protección, confidencialidad y preservación de la información se requiere de la aplicación de líneas de acción que deberán ser tenidas en cuenta para la formulación e implementación detallada de políticas, protocolos, programas, planes y proyectos orientados a estos propósitos. Con base en lo anterior, la Política General de Seguridad, Protección y Confidencialidad de la Información, establece las siguientes líneas de acción:

5.3.2.1 Línea de Acción N° 1: Gestión de la información.

Objetivo
Desarrollar prácticas para garantizar la seguridad de la información, implementando criterios para la adecuada gestión de la misma.
Lineamientos
a. Toda la información producida por la UBPD, debe estar clasificada, ordenada y descrita siguiendo los criterios del proceso de gestión documental, de acuerdo con el manual de manejo para la información confidencial, y lo establecido dentro de las políticas de Gestión de Información y Gestión Documental. **b.** Toda la información de la UBPD debe ser protegida y asegurada según los lineamientos establecidos en la Política de Seguridad de la Información. **c.** Toda información producida y que sea resultante del desarrollo funcional y procedimental de la UBPD debe encontrarse en los soportes normalizados por la Oficina Asesora de Planeación en articulación con la oficina productora. **d.** Toda información producida debe estar identificada, caracterizada, clasificada y valorada por un lado a partir de los criterios técnicos archivísticos y por otro, en lo que corresponde a seguridad de la información. **e.** Toda información producida por la UBPD en razón a sus funciones, procesos y procedimientos, debe estar registrada e identificada en la matriz de activos de información y ésta debe estar articulada con los instrumentos técnicos archivísticos que la unidad disponga para ello.

f. Toda la información producida, recibida y/o recolectada por la UBPD goza de protección y seguridad mediante la definición, implementación, seguimiento y mejoramiento de herramientas, controles, procedimientos, etc., con el fin de evitar los riesgos asociados a su disponibilidad, confiabilidad e integridad. **g.** Toda la información producida, recibida y/o recolectada debe tener un control según los mecanismos dispuestos por el sistema de gestión de documentos, el proceso de gestión documental, el programa de gestión de documentos y demás instrumentos relacionados, con el fin de garantizar su ágil recuperación e identificación en las instancias de almacenamiento definidas por la UBPD. **h.** Toda información producida debe tener definida una persona responsable que custodie dicha información, quien velará por la protección adecuada y seguridad de estos activos. **i.** Toda la información producida, recibida y/o recolectada por la UBPD se gestionará con base en el procedimiento de gestión de activos de información y en la Guía de Gestión de Activos de Información, con el fin de mantener los criterios de protección y confidencialidad de la información misional, estratégica, de apoyo a la gestión y de seguimiento y evaluación. **j.** La información estará sujeta a procesos de evaluación continua y sistemática de sus componentes (metadatos, historial de eventos y acceso). Con el fin de identificar posibles desviaciones y establecer acciones de mejora sobre el manejo, administración, protección y seguridad de la información.
Responsables
● Líderes de Procesos ● Dirección Técnica de Información, Planeación y Localización para la Búsqueda ● Subdirección de Gestión de Información para la Búsqueda ● Subdirección administrativa y financiera

5.3.2.2 Línea de Acción N° 2: Seguridad Digital.

Objetivo
Establecer lineamientos para la seguridad de la información gestionados a través de la plataforma tecnológica, los servicios tecnológicos y de comunicación de la UBPD
Lineamientos
a. Todas las prácticas orientadas a garantizar la seguridad de la información gestionada a través de la plataforma, servicios tecnológicos y de comunicación de la UBPD, se implementarán con base en lo establecido en las políticas de Seguridad Digital, la Política

General de Seguridad de la Información y el Manual para el Manejo de la Información Confidencial de la entidad.

b. La gestión de los permisos asignados para el acceso a la plataforma tecnológica y los servicios tecnológicos, serán los adecuados de acuerdo con los perfiles definidos para cada servidor (a), contratista o personal delegado.

c. Los sistemas de información implementarán lineamientos definidos en cuanto a complejidad y uso adecuado de contraseñas por parte de cada servidor (a), contratista o personal delegado.

d. Se gestionarán controles tecnológicos para el intercambio de información seguro de acuerdo con los niveles de clasificación de los activos de información.

e. Se gestionarán controles para realizar conexión remota segura, y garantizar que sean los adecuados para la preservación de la integridad, confidencialidad y disponibilidad de la información.

f. Se implementarán controles criptográficos suficientes para proteger la información transmitida o almacenada.

g. Los nuevos sistemas o cambios a los sistemas existentes contarán con controles de seguridad dentro de todo el ciclo de vida de desarrollo de software.

h. Se implementarán controles de seguridad a los dispositivos móviles autorizados de la UBPD o los personales que sean de uso para almacenar información de la UBPD.

i. Las pruebas de restauración programadas se realizarán de forma oportuna para verificar que las copias de respaldo funcionen cuando sean requeridas.

j. Se establecerán lineamientos orientados a realizar un uso adecuado y autorizado de los diferentes tipos de activos de información.

k. Se verificará que los controles implementados para el acceso a los servicios de la UBPD alojados en la nube, cuenten con los niveles de seguridad adecuados para preservar la integridad, disponibilidad y confidencialidad de la información.

l. Contar en los tiempos establecidos por la UBPD, con la infraestructura tecnológica que soporte los requerimientos de los distintos servicios de TI, en el escenario de una contingencia.

m. Se reducirá a niveles aceptables los riesgos asociados al transporte de la información restringida o privada a través de los canales de telecomunicación de la Entidad.

n. La información clasificada como restringida y privada, se almacenará en un repositorio de acceso restringido para personal no autorizado.

o. Se establecerán directrices encaminadas a evitar que servidores (as), contratistas o personal delegado, nieguen haber realizado alguna acción en las plataformas tecnológicas o de comunicaciones de la entidad.

Responsables
● Oficina de Tecnologías de la Información y las Comunicaciones ● Oficial de Seguridad de la Información ● Subdirección de Gestión Humana

5.3.2.3 Línea de Acción N° 3: Seguridad de las instalaciones.

Objetivo
Garantizar el aseguramiento físico de los activos de información de la UBPD, mediante la implementación de controles de seguridad en el espacio físico de la entidad.
Lineamientos
a. La protección física de los activos de información se debe realizar mediante la creación de diversas barreras o medidas de control físicas, alrededor de los activos de información de la UBPD, de las instalaciones de procesamiento de información y del espacio físico que aloja la documentación existente en medio de conservación análogo. **b.** Se definirán y delimitarán como áreas de acceso restringido/áreas seguras los espacios físicos en los que se aloja la información misional que contribuye a la búsqueda humanitaria y extrajudicial, que se encuentra en medio de conservación análogo. **c.** Todas las áreas que se hayan definido como seguras y los activos de información que la componen, estarán protegidas del acceso no autorizado mediante controles físicos de acceso y tecnologías de autenticación fuerte (por ejemplo: token, tarjetas de proximidad, o, controles biométricos). **d.** En las áreas seguras donde se encuentren activos informáticos y de archivo documental, se debe cumplir como mínimo con los siguientes lineamientos: i. No consumir alimentos ni bebidas. ii. No ingresar sustancias inflamables. iii. No permitir el acceso de personal ajeno a la UBPD iv. No se deben almacenar elementos ajenos a los requeridos de acuerdo con la actividad que se realice en el área segura. v. No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del responsable de dichas áreas. vi. No se permite el ingreso de equipos electrónicos (computadores portátiles, cámaras, celulares, USB, etc.), así como maletas o contenedores; excepto cuando exista debida justificación y autorización para portarlos. En este último caso,

deberán ser registradas al ingreso y salida para mitigar el riesgo de ingreso de elementos no autorizados o la extracción de elementos.

e. Para la selección e implementación de controles de seguridad para las áreas seguras se tendrá en cuenta la posibilidad de daños producidos por incendio, inundación, explosión, agitación civil; otras formas de fenómenos naturales como terremotos, ciclones y erupciones volcánicas; y situaciones producidas intencionalmente o resultantes de fallas humanas como incendios, explosiones, actos terroristas, robo, espionaje, infiltración, ataques contra la UBPD o conflictos armados.

f. Para las áreas de depósito de archivo se tendrá en cuenta lo dispuesto en el Acuerdo 50 de 2000 sobre prevención de deterioro de los documentos de archivo y situaciones de riesgo, y, el Acuerdo 6 de 2014 sobre conservación de documentos, del Archivo General de la Nación; con base en los cuales la UBPD propenderá por la disposición de:

i. Detectores automáticos de humo o de calor conectados con servicios exteriores de urgencia.
ii. Personal de vigilancia
iii. Sistemas de extinción escogidos con la asesoría de los bomberos: extinguidores manuales, sistemas de extinción fijos.
iv. Puertas cortafuego
v. Realizar programas regulares de mantenimiento de las instalaciones eléctricas y asegurarse que las salidas de emergencia sean de fácil acceso y de abertura desde el interior.
vi. Es necesario hacer respetar las medidas restrictivas hacia las (os) fumadoras (es), aislar los productos sensibles como películas de nitrato o productos químicos inflamables y evitar las fotocopias en salas de almacenamiento o en espacios que tengan material inflamable.
vii. La protección contra los efectos del agua incluirá la verificación constante de los sistemas hidráulicos como canales, goteras, terrazas, ventanas, etc. Hay que asegurar el mantenimiento de las canalizaciones y evitar las redes de evacuación o suministro de agua en las placas de las salas de almacenamiento. Prever un pozo o un sistema de evacuación de aguas para las salas subterráneas.

g. Todas las puertas que utilice el sistema de control de acceso donde se procese o almacene activos de información deben permanecer cerradas, y es responsabilidad de todas (os) las (os) servidoras (es), contratistas, personal delegado y terceros autorizados, evitar que las puertas permanezcan abiertas.

h. Se exigirá a servidores (as), contratistas o personal delegado, sin excepción, el porte en un lugar visible del mecanismo de identificación adoptado por la UBPD, mientras se encuentren dentro de las instalaciones de la entidad.

i. Las (os) visitantes deberán permanecer acompañados de un (a) servidor (a) de la UBPD, cuando se encuentren dentro de alguna de las áreas restringidas de la Entidad. **j.** Es responsabilidad de servidores (as), contratistas o personal delegado y terceros que tengan acceso o hagan uso de los activos de información, acatar las normas de seguridad y mecanismos de control de acceso a las instalaciones de la UBPD. **k.** Revisar y registrar los modelos y seriales de los elementos tecnológicos que ingresen a la UBPD, y confrontarlos cuando estos sean retirados de la Entidad.
Responsables
● Oficial de Seguridad de la Información ● Asesor de Seguridad Física

5.3.2.4 Línea de Acción N° 4: Prevención y gestión de riesgos e incidentes de Seguridad de la Información.

Objetivo
Prevenir afectaciones a la integridad, disponibilidad y confidencialidad de la información a través de la identificación y gestión oportuna de los riesgos e incidentes de seguridad.
Lineamientos
Riesgos[1]: **a.** Todo (a) servidor (a), contratista o personal delegado de la UBPD deberá reportar oportunamente y con carácter obligatorio, los riesgos de seguridad de la información identificados. **b.** Deberán documentarse los planes de tratamiento de los riesgos de seguridad de la información existentes en la Entidad. **c.** Se implementarán controles orientados a minimizar la probabilidad de que un riesgo de seguridad de la información se materialice. **d.** Se realizarán campañas de socialización y comunicación de la Metodología de Gestión de Riesgos de Seguridad de la información y Seguridad Digital, para su debida implementación. **e.** Se hará seguimiento a la gestión de riesgos y ejecución de los planes de acción definidos dentro de la misma, revisando periódicamente la variación de la calificación de los riesgos.

Incidentes[2]:

- **a.** Cuando se presenten incidentes o eventos de seguridad de la información, se reportarán de manera oportuna, de acuerdo con lo definido en el procedimiento Gestión de eventos e Incidentes de Seguridad de la Información, y el procedimiento de Gestión de Eventos e Incidentes de Seguridad Digital.
- **b.** Los incidentes de seguridad deberán documentarse y clasificarse de acuerdo con las actividades definidas en el procedimiento de Gestión de Eventos o Incidentes de seguridad de la Información y el procedimiento de Gestión de Eventos e Incidentes de Seguridad Digital.
- **c.** Cuando se realice el análisis de los incidentes de seguridad reportados, se identificará cuáles serán escalados para proceder a realizar el contacto con las autoridades correspondientes, consultando el plan de Gestión y Respuesta a Incidentes o Eventos de Seguridad (GRIES) cuando se estime necesario.
- **d.** Todos los eventos de seguridad digital y de seguridad de la información que se identifiquen por medio del monitoreo y revisión de los registros de eventos que pongan en riesgo la integridad, disponibilidad o confidencialidad de cualquier activo de información, deberán ser reportados de acuerdo con el procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información y el procedimiento de Gestión de Eventos e Incidentes de Seguridad Digital.
- **e.** En los casos que sea necesario realizar recolección y preservación de la evidencia de las investigaciones que se realicen durante el análisis de un incidente de seguridad de la información, esta actividad se llevará a cabo de acuerdo con las directrices del procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información, y el procedimiento de Gestión de Eventos e Incidentes de Seguridad Digital.
- **f.** Se reportarán de manera inmediata las debilidades de seguridad de la información observadas o sospechadas en los sistemas de información, o servicios de la UBPD o lugares físicos donde se evidencie una vulnerabilidad o debilidad, que afecten la confidencialidad, integridad o disponibilidad de la información, de acuerdo con el procedimiento de Gestión de Eventos e Incidentes de Seguridad de la Información y el Procedimiento de Gestión de Eventos e Incidentes de Seguridad Digital.
- **g.** Se mantendrá el registro de lecciones aprendidas de los incidentes de seguridad de la información, que sirva de insumo para el tratamiento adecuado y oportuno de nuevos incidentes de seguridad de la información.

---

[1] El riesgo es entendido como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

[2] Un incidente de seguridad de la información está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información, que tienen una probabilidad significativa de comprometer las operaciones y amenazar la seguridad de los activos de información. (ISO 27001)
Responsables
● Oficial de Seguridad de la Información ● Oficina Asesora de Tecnologías de la Información y las Comunicaciones

5.3.2.5 Línea de Acción N° 5: Cultura institucional de Seguridad de la Información.

Objetivo
Generar conocimiento, apropiación e implementación de prácticas de Seguridad de la Información por parte de servidores (as), contratistas y personal delegado de la UBPD, con base el fortalecimiento de la cultura institucional respecto al tema.
Lineamientos
a. La UBPD se orientará hacia la generación de una cultura interna de buenas prácticas en seguridad y protección de la información, en concordancia con lo establecido en el Decreto Ley 589 de 2017 sobre acceso a la información (Título III). **a.** Todo (a) servidor (a), contratista o personal delegado de la UBPD, deberá firmar un compromiso de confidencialidad que contenga su obligación de no divulgar la información interna y externa que conozcan como parte del desarrollo de sus funciones/obligaciones, en el marco de su vinculación con la Entidad. La firma del compromiso de confidencialidad implica que la información conocida por parte de las (os) servidoras (es), contratistas y personal delegado que tengan acceso o uso de cualquier activo de información de la UBPD, en ninguna circunstancia debe ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización. **b.** La UBPD desarrollará procesos para sensibilizar de manera permanente a los servidores, servidoras, contratistas y personal delegado en temas de seguridad de la información. **c.** Los (as) servidores (as), contratistas o personal delegado de la UBPD deberán participar de manera activa en las jornadas de sensibilización y capacitación orientadas al fortalecimiento de la Seguridad de la Información. **d.** La UBPD monitoreará el nivel conocimiento y conciencia sobre las prácticas de seguridad de la información de servidores (as), contratistas o personal delegado; con miras a

identificar de forma oportuna los aspectos que deben ser reforzados para evitar vulnerabilidades derivadas de la gestión del personal.

e. La UBPD comunicará de forma oportuna y eficiente la emisión de políticas, protocolos, metodologías, manuales y procedimientos definidos para garantizar la seguridad de la información de la entidad.

f. La UBPD realizará campañas para la socialización, sensibilización e implementación de las políticas, protocolos, metodologías, manuales y procedimientos definidos para garantizar la seguridad de la información; dirigidas a servidores (as), contratistas o personal delegado de la entidad.

g. Es responsabilidad de cada servidor (a), contratista o personal delegado que tenga acceso o uso de cualquier activo de información de la UBPD, el resguardo de sus contraseñas, por lo tanto, no podrán estar escritas o expuestas en su puesto de trabajo, con el fin de evitar que sean conocidas por otras personas.

h. Todo (a) servidor (a), contratista o personal delegado de la UBPD deberá acogerse a la implementación de los procedimientos para la destrucción segura de aquella información que no será utilizada o será desechada, evitando que el papel que contiene información clasificada o reservada sea reutilizado o dispuesto en los espacios de impresoras, escáner o lugares de copiado para su reciclaje.

Responsables
● Oficial de Seguridad de la Información ● Subdirección de Gestión Humana ● Oficina Asesora de Comunicaciones y Pedagogía

5.3.3. SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

Para optimizar la implementación de la Política General de Seguridad, Protección y Confidencialidad de la Información, la UBPD contará con un Sistema de Seguridad de la Información (SSI), que será caracterizado dentro del Sistema de Gestión como Proceso de Gestión de Seguridad de la Información.

El SSI estará organizado con una estructura jerárquica, con claros niveles de decisión y la asignación de claras responsabilidades, bajo el liderazgo de la (el) Directora (r) General de la UBPD. Sin embargo, la seguridad es responsabilidad de todo (a) servidor (a), contratista o personal delegado de la UBPD, quienes deben observar escrupulosamente las directivas, instrucciones y protocolos del SSI.

El Sistema de Seguridad de la Información (SSI) el cual estará liderado por la Dirección General y estará integrado por:

a) Un Nivel Directivo, la (el) Directora (r) General de la UBPD y el Comité de Seguridad de la Información, establecido mediante la Resolución 537 de 2020.

b) Un Nivel Ejecutivo, compuesto por la (el) Oficial de Seguridad de la Información de la Dirección General; la Subdirección General Técnica y Territorial; la Dirección Técnica de Información, Planeación y Localización para la Búsqueda; la Oficina de Tecnologías de la Información y las Comunicaciones; y la Subdirección de Gestión de Información para la Búsqueda.

c) Un Nivel Operativo, integrado por la Subdirección General Técnica y Territorial; la Secretaría General; la Subdirección Administrativa y Financiera; la Subdirección de Gestión Humana; los jefes de Oficinas y de Oficinas Asesoras de la Dirección General; los directores de la Dirección Técnica de Información, Planeación y Localización para la Búsqueda, la Dirección Técnica de Prospección, Recuperación e Identificación y de la Dirección Técnica de Participación, Contacto con las Víctimas y Enfoques Diferenciales; y los Coordinadoras de los Equipos Territoriales.

En razón de lo anterior, se debe articular, cooperar y coordinar esta política con:

A. La política de seguridad digital, a través de la garantía de confidencialidad, integridad, disponibilidad de los activos de información mediante la gestión de riesgos que permita establecer el marco de confianza a las partes interesadas en concordancia con la misión y visión de la entidad.
B. La Política de Transparencia Acceso a la Información Pública y la Política de Prevención del Daño Antijurídico de la UBPD recomendando los ajustes necesarios si a ellos hubiere lugar.
C. La Subdirección Administrativa y Financiera, a través del grupo de Gestión Documental y la Subdirección General Técnica y Territorial a través de la Subdirección de Gestión de Información articulará las acciones que sobre gestión documental deban realizarse en el Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), en cuanto a la información Institucional que contribuye y la que no a la búsqueda; toda vez que el SGDEA es el sistema que administrará la información producida en todos los niveles de la UBPD. La información misional gozará de los privilegios de confidencialidad, disponibilidad e integridad según lo establecido en la normativa nacional.
D. El Comité de Gestión, en cuyas funciones está incluida la referida a asegurar la implementación y desarrollo de directrices en materia de seguridad digital y seguridad de la información.
E. El sistema de Gestión de Calidad, porque los procesos y procedimientos den cumplimiento a los requisitos establecidos en la normativa nacional, fortaleciendo el control de documentos y registros que contienen la información de la UBPD.

F. La Oficina de Control Interno: quien vela por el cumplimiento de las normas, políticas, procedimientos, planes, programas, proyectos y metas incluyendo la Política de Prevención del Daño Antijurídico de la UBPD, recomendando ajustes de ser necesarios.

G. Las Oficinas productoras de información como responsables de velar por la integridad, autenticidad, veracidad y fidelidad de la información contenida en los documentos de archivo que estarán bajo la custodia, almacenamiento y protección de la Subdirección de Gestión de Información para la Búsqueda, quien centraliza los archivos de gestión para que se articulen con esta política y con los instrumentos archivísticos garantizando el cumplimiento de los principios de procedencia y orden original.

VI. GLOSARIO

Activo de información: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.

Amenaza: posible causa de un incidente no deseado, que puede producir daño a un sistema u organización.

Confidencialidad: característica de la información por medio de la cual no se revela ni se encuentra a disposición de personas, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible sólo a las personas autorizadas.

Control: medida que modifica el riesgo. Sinónimo de salvaguarda.

Disponibilidad: propiedad relacionada con que sea efectivamente posible localizar, recuperar, presentar, interpretar y leer la información en el momento pertinente para el proceso de búsqueda por las personas debidamente autorizadas para ello.

Gestión de riesgos: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

Información: se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.

Integridad: propiedad de salvaguardar la exactitud, complejidad y completitud de la información.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones. (ISO Guía 73:2002).

Seguridad de la información: característica que adquiere la información cuando se encuentra en un ambiente en el que se preserva su confidencialidad, integridad y disponibilidad.

Soporte documental: medio que contiene la información, sin importar el material empleado. Además de los archivos en papel, también se entenderá como soporte documental el electrónico en que se pueden incluir los archivos audiovisuales, fotográficos, fílmicos, informáticos (textos, listados, bases de datos, cartografías, etc.), orales y sonoros, independientemente de su medio de almacenamiento (cds, dvds, usb y demás medios magnéticos, entre otros).

Proceso de Gestión de Seguridad de la Información (GSI): conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

Protección de la información: conjunto de medidas preventivas y reactivas que deben tomarse para mantener la confidencialidad, la disponibilidad e integridad de la información obtenida para la búsqueda, así como el contacto y protección de personas y organizaciones que aporten información para la búsqueda.

Tercero: hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.

Proyectaron: Astrid Johana Vargas Alfonso- Experto Técnico, Karen Johana Rocha Bello- Experto Técnico, Alexis Astrid López Cárdenas- Experto Técnico, Amaranta Catalina Salazar Fernández - Experto técnico, Cristian Eduardo Zanguña Ruiz - Experto técnico, Juan de Jesús Aponte Buitrago – Contratista de la Oficina de Tecnologías de Información y Comunicaciones, Diana Carolina Rincón Ávila – Analista técnico y Carolina Grajales Rojas - Experto técnico. **Revisaron:** Miembros del Comité de Seguridad de la Información en las sesiones No. 3 del 10 de junio, No. 4 del 24 de junio, No. 5 del 08 de octubre y No. 6 del 05 de noviembre de 2020.
Aprobó: Luz Marina Monzón Cifuentes, Directora General en la sesión No. 6 del comité de Seguridad de la Información del día 05 de noviembre de 2020.