UNIDAD DE BÚSQUEDA
DE PERSONAS DADAS POR DESAPARECIDAS

UBPD

Dirección General -

Oficina de Tecnologías de Información y Comunicaciones – OTIC

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

26 de agosto de 2022

TABLA DE CONTENIDO

1. 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 definir, adoptar, implementar y actualizar la Política General de Seguridad de la Información que atiende, 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 misionalidad y la información que surja de los procesos de apoyo, estratégicos y de evaluación y control. 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. Por ello, con el fin de realizar una mejora continua al Sistema se realiza la actualización de esta política, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos.

Así mismo, es de mencionar que la UBPD hace uso de herramientas y servicios que ofrecen las tecnologías de la información y las comunicaciones, con el fin de facilitar y soportar el flujo de información interna y externa, la comunicación electrónica entre sus servidore(a)s contratistas, proveedores, entidades públicas, organizaciones, sociedad civil y ciudadanía, y, de manera general, en el ejercicio de las diferentes actividades de su quehacer.

El creciente uso de las tecnologías de la información y comunicaciones ha venido acompañado de un progresivo incremento en las acciones, que al margen de la Ley, suceden en los medios digitales y las cuales pueden poner en situación de riesgo o vulnerabilidad a comunidades, organizaciones públicas y privadas, personas, no solo en lo que concierne a su patrimonio, sino en su buen nombre, privacidad e incluso integridad física.

La Política General de Seguridad de la Información describe el sustento normativo y establece los criterios y lineamientos que debe seguir cualquier servidor(a), contratista o proveedor 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 relacionada con sus funciones y obligaciones. 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

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

permitan la caracterización del conflicto armado y las modalidades, prácticas y tipologías de desaparición.

2. OBJETIVO

Definir el marco general de actuación institucional, los criterios, directrices, reglas, condiciones y pautas para la gestión en la UBPD de la seguridad de la información, con el fin de garantizar su custodia, integridad, conservación, preservación, disponibilidad, clasificación, reserva legal, confidencialidad y tratamiento seguro, así como una idónea gestión de riesgos asociados a ella.

3. ÁMBITO Y ALCANCE

La Política General de Seguridad 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 en todos los procesos, procedimientos, actividades y aquella que se genere, reciba, almacene o transfiera de sus procesos misionales, estratégicos, de apoyo, de evaluación y control.

La Política General de Seguridad de la Información es de estricta observancia por lo(a)s servidore(a)s, contratistas o proveedores que prestan servicios a la Unidad, inclusive cuando las actividades de gestión o tratamiento de la información no sean parte de su función principal; 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, mediante los mecanismos, dispositivos, sistemas de información, servicios, comunicaciones e infraestructura tecnológica dispuesta por la UBPD.

4. MARCO NORMATIVO

El marco normativo que soporta la Política General de Seguridad de la Información en la UBPD se fundamenta en:

- Constitución Política de Colombia, artículos 8, 15, 20, 23, 74, 94 y 209.
- Declaración de Derechos Humanos, artículo 19.
- Convención Americana de Derechos Humanos, artículo 13.
- Pacto Internacional de Derechos Civiles y Políticos, artículo 19
- Decreto 1081 de 2015, “Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, en lo relativo a las disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional
- Acto Legislativo 01 de 2017, *“Por medio del cual se crea un título de disposiciones transitorias de la Constitución para la terminación del conflicto armado y la*

construcción de una paz estable y duradera y se dictan otras disposiciones" artículos transitorios 3 y 4.

- 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"*. *aquellos que los adicionen o modifiquen*
- Decreto 1393 de 2018 "*Por el cual se establece la estructura interna de la Unidad de Búsqueda de Personas dadas por Desaparecidas en el contexto y en razón del conflicto armado (UBPD) y se determinan las funciones de sus dependencias"*. *aquellos que los adicionen o modifiquen.*
- Ley Estatutaria 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 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 el 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".*
- Sentencias C-067 de 2018 "Por el cual se organiza la Unidad de Búsqueda de Personas dadas por desaparecidas en el contexto y en razón del conflicto armado y C-080 de 2018 de la Corte Constitucional, instrumentos para facilitar y asegurar la implementación y desarrollo normativo del acuerdo final para la terminación del conflicto y construcción de una paz estable y duradera.
- Resolución No. 500 de marzo 10 de 2021 "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*". Y resolución 746 de 2022 "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".

En atención a los fundamentos normativos se desprenden las siguientes consideraciones:

a. **Carácter humanitario y extrajudicial de la UBPD y de su mandato**. La Corte Constitucional equipara la naturaleza de la UBPD con la de un organismo humanitario[2], como, por ejemplo, el Comité Internacional de la Cruz Roja (CICR),

[2] *La Unidad de Búsqueda entonces, es un organismo humanitario como el Comité Internacional de la Cruz Roja (CICR), que refiere el artículo 3 común a los Convenios de Ginebra, que señala que el CICR "podrá ofrecer sus servicios a las Partes en conflicto". El artículo 9 común a los Convenios de Ginebra además establece que "[l]as disposiciones del presente Convenio no son óbice para las actividades humanitarias que el Comité Internacional de la Cruz Roja, u otro organismo humanitario imparcial, emprenda para la protección de los heridos y de los enfermos o de los miembros del personal sanitario y religioso, así como para los socorros que, con el consentimiento de las Partes en conflicto interesadas, se les proporcione". Es decir, la Unidad de Búsqueda es un "organismo humanitario" de los mencionados en los Convenios de Ginebra, similar al CICR, que realizará sus actividades humanitarias, en el marco de la confidencialidad. La confidencialidad le ha permitido al CICR obtener inmunidad frente a los tribunales penales internacionales, en el sentido de que el CICR no está obligado a testificar ni a dar información incriminatoria a la que haya tenido acceso en desarrollo de sus labores humanitarias. En efecto, el artículo 73.4 de las Reglas de Procedimiento y Prueba de la Corte Penal Internacional contempla dicha inmunidad. Así las cosas, el carácter extrajudicial de la UBPD se traduce en que sus actividades ni están dirigidas a la atribución de responsabilidad por la comisión del delito de desaparición forzada, ni harán parte de ningún proceso penal. Por esta razón, la información que reciba o produzca la Unidad no podrá ser utilizada con el fin de atribuir responsabilidades en procesos judiciales, ni en la JEP.*

que adelanta sus actividades en el 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 mecanismo 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 o produzca no podrá ser utilizada con el fin de atribuir responsabilidades en procesos judiciales y no tendrá valor probatorio[3], a excepción de los informes técnico – forenses y los elementos materiales asociados al cadáver. En virtud de lo anterior, la gestión de la UBPD se desarrolla bajo la modalidad del trabajo basado en la confidencialidad, de manera que lo(a)s servidore(a)s, contratistas y proveedores de la UBPD en ejercicio de las actividades previstas en el Decreto Ley 589 de 2017, están exonerado(a)s del deber de denuncia y no podrán ser obligado(a)s a declarar en procesos judiciales por hechos que hayan conocido en desarrollo de sus funciones misionales, y únicamente pueden ser citado(a)s 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[4].

b. **Recolección de información en la UBPD**. La UBPD, de conformidad con su mandato, debe recolectar la información necesaria que apoye a 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 Entidad, señalando entre otras las siguientes: i) el convocar y entrevistar de manera confidencial a personas para que voluntariamente suministren información[5]; y ii) las bases de datos, así como toda información que dispongan personas, entidades del Estado u organizaciones sociales y de víctimas.

c. **Derecho de acceso a la información**. El artículo 74 de la Constitución Política de Colombia, así como el artículo 4 de la Ley 1712 de 2014 establecen el derecho de acceso a la información, el cual 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 pública clasificada y

[3] Decreto Ley 589 de 2017, artículo 3
[4] Decreto Ley 589 de 2017, artículo 19 y Acto Legislativo 01 de 2017, artículo Transitorio 4.
[5] Decreto Ley 589 de 2017, artículo 5 # 1 literal a

pública reservada 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. De igual forma, se debe dar cumplimiento al Decreto 1081 de 2015, por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República, en lo relativo a las disposiciones generales en materia de transparencia y del derecho de acceso a la información pública nacional, el cual tiene por objeto reglamentar la Ley 1712 de 2014, en lo relacionado con la gestión de la información pública.[6]

d. **Facultad de la UBPD para acceder a la información**. La Sentencia C-067 de 2018 señala en el apartado (viii) del Análisis de la constitucionalidad de los artículos 11 al 14 del Decreto Ley 589, especialmente el parágrafo del artículo 14, indicando lo siguiente:

"Cabe señalar que el legislador extraordinario no puede dejar al arbitrio de la UBPD el establecimiento de las condiciones de confidencialidad, como lo hace el texto bajo examen, toda vez que la determinación sobre el tipo de información que se categoriza como reservada o clasificada responde a un criterio de estricta legalidad. Así se prevé en el artículo 74 de la Constitución, al consagrar que todas las personas tienen derecho al acceso a la información pública, "salvo los casos que establezca la ley".

De este modo, las condiciones de confidencialidad solo se pueden fijar de acuerdo con los criterios de información clasificada o reservada, en los términos de los artículos 18 y 19 de la Ley 1712 de 2014, o las normas que los modifiquen o sustituyan. Conforme lo anterior, 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 y reservada, que contribuya a la búsqueda de personas desaparecidas y de celebrar convenios y protocolos de acceso a información con cualquier tipo de organización nacional o internacional de derecho público o privado[7]. 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[8].

[6] Artículo 2.1.1.1.1. Decreto 1081 de 2015
7 Decreto Ley 589 de 2017, Artículo 14
[8] 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

e. **Clasificación de la información para su protección**. La UBPD ha establecido controles para la protección de la información teniendo en cuenta la normatividad vigente sobre el derecho de acceso a la información en Colombia, en especial la Ley Estatutaria 1712 de 2014, la cual establece que toda la información que recolecte o produzca la Entidad es información pública y puede calificarse para restringir su acceso, tal como lo determinan los artículos 18 y 19 de la mencionada Ley, es decir, en Información pública clasificada e Información pública reservada[9]. Dentro de la información reservada, relevante para la búsqueda de personas dadas por desaparecidas, se encuentra:

- 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.
- Información con reserva judicial.
- 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 internacional de derecho público o privado, incluyendo organizaciones de víctimas y de derechos humanos, nacionales o extranjeras.

  Frente a la información clasificada, relevante para el proceso misional, se encuentra la siguiente:

  - Derecho a la intimidad (limitado para servidore(a)s públicos).
  - Derecho a la vida, salud o seguridad.
  - Secretos comerciales, industriales y profesionales.

  Las cuales deben corresponder a las que se establezcan en la "matriz de activos de información e índice de información pública clasificada y publica reservada[10]", entre las cuales se pueden encontrar entre otras:

  - Las Historias de Solicitudes de Implementación de Acciones Humanitarias y Extrajudiciales para la Búsqueda.

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.

[9] GSI-GU-002 Guía de gestión de Activos de información; Sistema Integrado de Gestión/Procesos/Estratégicos/Gestión de seguridad de la Información/guías.

[10] Instrumentos de Gestión de la Información. (2021, diciembre 19). UBPD; Unidad de Búsqueda de Personas dadas por Desaparecidas. https://ubpdbusquedadesaparecidos.co/transparencia/instrumentos-de-gestion-de-la-informacion/

- Las Historias laborales
- Los procesos disciplinarios
- Las acciones constitucionales

Es importante mencionar, que la calificación de la información se encuentra en cabeza de los responsables o líderes de los procesos de la UBPD, quienes, según la naturaleza de esta, deberán definir el tipo de control a implementar.

f. **Protección de datos personales**. Para cumplir con sus funciones, la UBPD debe registrar datos personales tanto de las personas dadas por desaparecidas como de sus familiares, de igual manera, de aquellas personas que entreguen información. Para proteger estos datos, debe darse cumplimiento a la Ley 1581 de 2012 y los decretos que la reglamenten, a la Política de Protección de Datos Personales de la UBPD y aquellos que los adicionen o modifiquen, así como establecer protocolos respecto del almacenamiento de información clasificada y reservada particularmente sensible.

g. **Responsabilidad en la custodia de información**. Los(las) servidore(a)s, contratistas y proveedores de la UBPD tendrán la obligación de suscribir y cumplir el compromiso 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”; la Sentencia C-067 de 2018 de la Corte Constitucional; el Decreto Ley 589 de 2017 aquellos que los adicionen o modifiquen; los principios establecidos en la Ley Estatutaria 1581 de 2012 y su Decreto reglamentario 1377 de 2013; la Ley 1712 de 2014 y su Decreto reglamentario 103 de 2015; la Ley 2094 de 2021; 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; Ley 1273 de 2009 Por medio de la cual 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.

h. **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 las entidades deben contar con un Programa de Gestión Documental[11] que se articule con las políticas, lineamientos, planes, programas y proyectos 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

[11] COLOMBIA. ARCHIVO GENERAL DE LA NACIÒN. Ley 594 de 2000 [en línea]. (14, julio, 2000) [consultado el 8, agosto, 2022]. Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Disponible en Internet: <https://normativa.archivogeneral.gov.co/ley-594-de-2000/>.

con ocasión del conflicto armado interno[12], sin perjuicio del carácter confidencial o bajo reserva legal de la información misional de la UBPD.

i. **Seguridad Digital y Seguridad de la Información.** La UBPD creo el Sistema de Seguridad de la Información - SSI, como herramienta de gestión para implementar y mantener la Política de Seguridad de la Información. La operación del sistema se enmarca en la normatividad aplicable vigente como son: El CONPES 3701 del 14 de julio de 2011 en el cual se establecen los Lineamientos de Política para Ciberseguridad y Ciberdefensa, el COMPES 3854 el 11 de abril de 2016, por medio del cual se establece la política Nacional de Seguridad Digital, el Decreto 1008 de 2018 expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones por medio del cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones. La Resolución No. 500 de marzo 10 de 2021 "*Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital*". El Conpes 3995 del 01 de julio de 2020 por medio del cual se expide la Política Nacional de Confianza y Seguridad Digital. resolución 746 de 2022 "Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".El Decreto 338 de 8 de marzo de 2022, expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones, "Por el cual se adiciona el Titulo 21 a la parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones"

5. 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, planes, programas, proyectos, y mecanismos de seguridad de la información, para el tratamiento seguro de la misma, por parte de sus servidore(a)s, contratistas o

[12] 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.

proveedores en pro del fortalecimiento y mejora del sistema de gestión. 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 confianza necesaria que incentive a la sociedad en general a suministrar información que contribuya a la búsqueda de las personas dadas por desaparecidas en el contexto y en razón del conflicto armado.

A su vez, la UBPD, en atención a su naturaleza especial, carácter humanitario y extrajudicial y su deber de construir confianza, utiliza las tecnologías de la información y comunicaciones, en pro de una gestión eficiente y segura, con lo que se compromete a afrontar las amenazas y vulnerabilidades inherentes a los entornos digitales, a través de lineamientos orientados a proteger y asegurar la información que y produce y a la que tiene acceso en el desarrollo de su misión.

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)[13], 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.

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. Así, se promueven las relaciones de confianza entre la Entidad y las personas que cuenten con información útil que contribuya al proceso de búsqueda de personas dadas por desaparecidas.

Teniendo en cuenta lo anterior, 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:

[13] Congreso de Colombia. Acto legislativo 01 de 2017. Artículo transitorio 5°. Jurisdicción Especial para la Paz. Bogotá, D.C.: [04, abril, 2017]. Disponible en Internet: https://jepvisible.com/images/normatividad/actolegislativo01-2017.pdf

a. **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.

b. **Principio de ética**: los (las) servidore(a)s, contratistas y proveedores 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 proveedores, 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.

c. **Principio pro-persona y pro-búsqueda**: 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 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 y la Política de Gestión de la Información de la UBPD.

d. **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 se manejara bajo la modalidad de la confidencialidad, la cual debe entenderse como una garantía inquebrantable que da la entidad a todas las personas que han solicitado y/o han aportado información que contribuye en las gestiones de búsqueda de las personas dadas por desaparecidas en el contexto y en razón del conflicto armado, sobre todo, porque con la creación de la Unidad de Búsqueda se procura resolver la falta de confianza en la institucionalidad preexistente y en razón de ello, el tratamiento de aquella información que se recibe, recolecta y produce, se gestiona bajo parámetros de confidencialidad.

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; 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, 7 y 10) y 19 (Parágrafo) del Decreto Ley 589 de 2017 y el artículo 14 (numeral 8) del Decreto 1393 de 2018, la Ley 1712 de 2014 el Índice de Información Clasificada y Reservada, así como por lo establecido en la Sentencia C-067 de 2018 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.

e. **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.

f. **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.

g. **Principio de control de la información**: La información entregada por organizaciones, familiares y demás personas que aporten a los procesos de búsqueda y 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 como se menciona en la Política de Protección de datos Personales y en cualquier momento podrá solicitar a la UBPD el borrado de su información.

h. **Principio de uso racional de la información**: la UBPD y sus servidores(as), contratistas, tendrán acceso únicamente a la información, sistemas de información, infraestructura, herramientas o servicios que requieran para el desarrollo de sus funciones y/o obligaciones. La Unidad protegerá la información creada, procesada, o resguardada por sus procesos, y sus canales de trasmisión, con el fin de minimizar impactos operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

i. **Principio de dignidad y respeto**: El respeto de la dignidad de las víctimas debe ser un principio rector en cada una de las fases del proceso de búsqueda de las personas desaparecidas. Durante el proceso de búsqueda, la dignidad de las víctimas requiere su reconocimiento como personas que se encuentran en una situación de especial vulnerabilidad y riesgo, titulares de derechos que deben ser protegidos y que tienen conocimientos importantes que pueden contribuir a la eficacia de la búsqueda. Los funcionarios públicos tienen que ser capacitados para realizar su trabajo con enfoque diferencial. Deben actuar con conciencia de que trabajan para garantizar los derechos de las víctimas y orientar todo su trabajo en favor de ellas.

   Al realizar el tratamiento de datos, deberá respetar y garantizar la protección de la información del titular, dado que es un aspecto fundamental para salvaguardar la vida de las personas, su integridad física, mental y su dignidad, sobre todo en circunstancias difíciles como los conflictos armados y otras emergencias humanitarias.

j. **Principio de enfoque territorial, diferencial y de género:** La UBPD reconoce la existencia de grupos poblacionales o específicos, con características particulares, que han sufrido y sufren aún discriminación, vulnerabilidad, exclusión, invisibilización y desigualdad en un contexto y momento determinado en razón de su pertenencia étnica, edad, género, orientación sexual e identidad de género, discapacidad, características socioeconómicas, territorialidad, origen nacional o familiar, lengua, religión, opinión política o filosófica. Por lo tanto, esta política, las que se desarrollen a partir de ésta, los instrumentos y herramientas institucionales deberán adoptar este principio garantizando el adecuado acceso, protección y administración tanto de la información como de las fuentes de las que procedan[14].

5.3. CONSIDERACIONES GENERALES

La Política General de Seguridad de la Información considera, por una parte, las facultades que tiene la UBPD para acceder a información pública, inclusive aquella clasificada y reservada 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 y reservada debe ser protegida garantizando la confidencialidad

[14] (UBPD, 2020) Lineamientos Técnico de Participación. Documento construido por: Dirección Técnica de Participación, Contacto con las Víctimas y Enfoques Diferenciales

de su contenido y sobre todo la que corresponda con la identidad y contacto de las personas que la entreguen.

Las responsabilidades frente a la seguridad de la información serán compartidas y aceptadas por cada uno de los servidores (as), contratistas o proveedores.

La organización del Sistema de Seguridad de la Información, las autoridades, roles y responsabilidades de seguridad de la información definidas para la UBPD se encuentran declaradas en la Matriz de Roles y Responsabilidades de Seguridad de la Información[15].

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 Integrado de Gestión de la Entidad.

5.3.1. 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 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 de 2018 y C-080 de 2018.

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,

[15] Para ampliar información relacionada consultar el “GSI-MN-001 (SGSI) Manual de seguridad de la información” en https://ubpdbusquedadesaparecidos.co/transparencia/planeacion/

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 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 seguridad 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.

5.3.2. Archivo de derechos humanos

El Archivo de Derechos Humanos será conformado, centralizado y custodiado por la Subdirección de Gestión de Información, quien establecerá las medidas y reglamentos para el acceso a éste en los instrumentos dispuestos por la UBPD, identificando los responsables, usuarios y niveles de acceso.

La identificación de los archivos de derechos humanos se dará en clave de los criterios misionales y temáticos establecidos en 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,* es decir que se identifican como archivos de derechos humanos todos los resultantes de la ejecución del proceso misional y aquellos relacionados con los siguientes temas:

a. *«Los relativos a graves violaciones de los derechos humanos e infracciones al Derecho Internacional Humanitario.*
b. *Los relativos a acciones de exigibilidad de derechos y de recuperación de la memoria histórica por parte de la sociedad y de las víctimas.*
c. *Los relativos a acciones institucionales derivadas de la denuncia de tales violaciones a los derechos humanos o de la reclamación de medidas de atención humanitaria y de las reparaciones materiales y simbólicas.*
d. *Los relativos al contexto local, regional o nacional de desarrollo del conflicto y sus impactos diferenciados en la población.*
e. *Los relativos a los perpetradores de las violaciones a los derechos humanos e infracciones al DIH y su modus operandi.*
f. *Los relativos a respuestas institucionales frente a las violaciones a los derechos humanos o las demandas de reparación de las víctimas*
g. *Los relativos a los modos de vida, proyectos familiares, sociales, políticos y comunitarios afectados por la dinámica del conflicto armado interno.*
h. *Los modos de resistencia de la sociedad civil frente al conflicto armado»*[16]*.*

Consecuencia de esto, es necesario que, para la recuperación de estos archivos con miras a la gestión de información, se efectúen los respectivos procesos de descripción archivística normalizada bajo los criterios establecidos por el custodio (Subdirector de Gestión de Información para la Búsqueda) haciendo el respectivo análisis del contenido informativo y

[16] ARCHIVO GENERAL DE LA NACIÓN y CENTRO NACIONAL DE MEMORIA HISTORICA. 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 [en línea]. Bogotá, D.C.: Los autores, 2017 [consultado el 14, abril, 2022]. P32. Disponible en Internet: <https://centrodememoriahistorica.gov.co/wp-content/uploads/2021/08/Protocolo-gestion-documental.pdf>. ISBN :978-958-8944-46-3.

extrayendo los términos asociados a la misión de la UBPD todos ellos controlados en el tesauro, ontología o lenguaje controlado que se determine para tal fin.

El acceso a la información del archivo de derechos humanos será controlado por el custodio y registrado cada uno de los accesos en los instrumentos dispuestos tanto por el Proceso Estratégico de Gestión de Seguridad de información como por el Proceso de Apoyo de Gestión Documental este último en lo que corresponde al préstamo de documentos en soporte físico.

5.3.3. INFORMACIÓN RESULTANTE DE LOS PROCESOS ADMINISTRATIVOS

La información resultante de los procesos de apoyo, estratégicos y de evaluación y control (confidencial o no), estará a cargo de cada una de las dependencias de la UBPD, en el marco de las consideraciones técnicas desarrolladas por la Secretaria General a través de la Subdirección Administrativa y Financiera y ésta a su vez por medio del Grupo Interno de Trabajo de Gestión Documental, quienes emitirán los lineamientos técnicos, reglas, principios y actividades que permiten la implementación y sostenibilidad del proceso en articulación con las demás áreas.

La organización y la custodia de los archivos en tanto se encuentren en gestión serán responsabilidad de las dependencias responsables de su producción.

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

La información, que se origina en los procesos estratégicos, de apoyo y de evaluación y control, 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.

No obstante, el desarrollo de los procesos administrativos puede producir información que contribuye a los procesos misionales, por ejemplo, el resultado de una ejecución contractual puede ser un producto con información que contribuye a la búsqueda. En estos casos, la información deberá ser administrada, gestionada y controlada por la Subdirección de Gestión de Información quienes aplicarán bajo la línea documental los procesos de organización documental emanados de las dependencias responsables, pero en materia de información la línea se orientará bajo las políticas institucionales que se tengan para gestionar la información. Cuando esto ocurra la información que aporta a las series documentales misionales se deberá ver reflejada en el archivo de gestión centralizado que corresponde al Archivo de Derechos Humanos el cual se responsabilizará de la implementación de las líneas propias para su administración.

5.4. SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Seguridad de la Información (SSI) permite conocer y gestionar los riesgos a los que se enfrenta la Entidad al manejar la información diariamente y establecer los mecanismos necesarios para mitigar sus consecuencias; es por ello que la UBPD ha implementado este sistema, para proteger la información de los servidore(a)s, contratistas, proveedores y la ciudadanía en general. Así mismo, este sistema es caracterizado dentro del Sistema integrado de Gestión como Proceso de Gestión de Seguridad de la Información.

El Sistema de Seguridad de la Información (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), o contratista de la UBPD, quienes deben dar estricto cumplimiento a las directivas, instrucciones y protocolos del SSI.

El Sistema de Seguridad de la Información (SSI) estará liderado por la Dirección General e 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, y un Nivel Operativo establecidos mediante la resolución 588 del 8 de junio de 2020.

Con el fin de desarrollar el marco de actuación apropiado para salvaguardar la información, y dar a conocer los lineamientos en cuanto a seguridad, la UBPD ha establecido la Política General de Seguridad de la Información, y a su vez esta es complementaria con los lineamientos establecidos en el GSI-MN-001 Manual del Sistema de Seguridad de la Información - SSI.

5.4.1. DECLARACIONES

La Dirección General insta a que todos los servidore(a)s, contratistas y proveedores cumplan con los lineamientos en materia de seguridad, con el fin de resguardar la información producida o aportada, apoyando el Plan Nacional y los Planes Regionales de

Búsqueda, de esta forma generar confianza a la ciudadanía y minimizar el sufrimiento de las familias que buscan. Para ello se establecen las siguientes políticas de seguridad que soportan el SSI:

a. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los servidores(as), contratistas o proveedores.
b. La UBPD es la responsable de los activos de información y los administradores de estos activos son los servidore(a)s, contratistas o demás colaboradores que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información, y son los responsables de implementar los controles para su protección, de acuerdo con la clasificación de la información de su propiedad o en custodia.
c. Los servidores(as), contratistas o proveedores deben cumplir los lineamientos e instrucciones descritos en esta política y en los procedimientos, guías e instructivos definidos y los cuales se encuentran publicados dentro del repositorio definido en el Sistema Integrado de Gestión, así como los conceptos y lineamientos en materia de seguridad de la Información generados a solicitud.
d. 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, confidencialidad e integridad.
e. Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento.
f. Con el fin de disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano, la alta dirección destinará los recursos suficientes para el desarrollo de programas de capacitación y sensibilización; es obligación de los servidore(a)s y contratistas asistir a estos eventos o cursos.
g. Los servidores(as) y contratistas tienen la obligación y responsabilidad de la identificación y notificación de cualquier incidente o evento que pudiera comprometer la seguridad de sus activos de información. Asimismo, la Unidad deberá implementar procedimientos para la correcta gestión de los incidentes detectados.

5.5. REVISIÓN DE LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

La Política General de Seguridad de la Información establecida en este documento será revisada y aprobada por el Comité de Seguridad de la Información al menos una vez al año o cuando ocurran cambios significativos, para asegurar su conveniencia, adecuación y eficacia continua.

5.6. PROCESO DISCIPLINARIO O SANCIONATORIO

Todo incumplimiento a la política de seguridad de la información por parte de un servidor(a) o contratista, será tratado de acuerdo con lo establecido en el GSI-MN-001 Manual del Sistema de Seguridad de la Información - SSI.

6. 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[17].

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización[18].

Confidencialidad: Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso[19].

Control: medida que modifica el riesgo. Sinónimo de salvaguarda[20].

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[21].

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[22].

Información: se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen[23].

Información pública: Es aquella información que puede ser obtenida y ofrecida sin reserva alguna y sin importar si la misma sea información general, privada o personal.[24]

Información pública clasificada: Es aquella información que estando en poder o custodia de un sujeto obligado en su 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 las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.[25]

[17] Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información (s.f.). Tomado de https://www.iso27000.es/glosario.html
[18] Ibidem
[19] NTC ISO/IEC 27002:2013
[20] Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información. (s.f.). Tomado de https://www.iso27000.es/glosario.html
[21] Concepto creado por la UBPD
[22] Lista de Glosarios de términos especializados (2017.febrero 17). Recuperado de https://glosarios.servidor-alicante.com/
[23] Ley 1712 del 6 de marzo de 2014, Artículo 6
[24] Corte Constitucional, Sentencia T-114 de 2018 MP. Bernal Pulido Carlos.
[25] Ley Estatutaria 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.[26]

Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos[27]

Observancia: Cumplimiento exacto y puntual de lo que se manda ejecutar, como una ley, un estatuto o una regla.[28]

Ontología: definen conceptos y relaciones de algún dominio, de forma compartida y consensuada, y esta conceptualización debe ser representada de una manera formal, legible y utilizable por los ordenadores[29].

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[30].

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.[31].

Seguridad de la información: es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la información[32].

Sistema de Seguridad de la Información (SSI): diseño, implementación y mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información[33].

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,

[26] Ibídem.
[27] NTC ISO/IEC 27000:2013
[28] Diccionario de la Lengua Española. Real Academia Española (s.f.). Disponible en Internet https://dle.rae.es/observancia?m=form
[29] Martínez Ferreras, D. (s. f.). Los Tesauros. Universidad Oberta de Cataluña, (PID_00143963), p. 7. https://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/1353/1/Los%20tesauros.pdf
[30] Concepto creado por la UBPD
[31] ISO/IEC 27000, (ISO Guía 73:2002)
[32] Seguridad de la Información *[En Wikipedia]*. Recuperado (2022, Mayo 23) de https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n
[33] ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? (2013, febrero 19). Tomado de https://www.firma-e.com/blog/que-es-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/

independientemente de su medio de almacenamiento (CDs, DVDs, USB y demás medios magnéticos, entre otros)[34].

Tercero: hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información[35].

Tesauro: vocabulario controlado de descriptores con un significado previamente establecido y cuyo fin último sería el de definir de manera unívoca el contenido de un documento. El fin último de este lenguaje es el de ser puente de conexión entre los usuarios y las unidades de información, esto es, de servir tanto para la indización como para la recuperación documental.[36]

7. SOCIALIZACIÓN Y DIVULGACIÓN DE LA POLÍTICA

Una vez aprobada la presente política, esta rige a partir de la fecha de publicación y se podrá consultar en la página web de la UBPD https://ubpdbusquedadesaparecidos.co/ en la sección de Transparencia y Acceso a la Información pública, con el fin de que lo(a)s servidore(a)s, contratistas, proveedores y demás colaboradores tengan acceso a esta, la conozcan y apliquen.

Proyectaron: Diana Carolina Rincón, Analista Técnico II; Astrid Johana Vargas Alfonso, Experto Técnico IV; Diego Ferney Ramírez Pulido, Asesor Unidad Especial I; Nancy Mireya Barbosa R., Contratista; Juan de Jesús Aponte Buitrago, Contratista. 19/08/22
Revisaron: Miembros del Comité de Seguridad de la Información. 26/08/22
Aprobaron: Miembros del Comité de Seguridad de la Información - en la sesión No.02 del comité de Seguridad de la Información el 26 de agosto de 2022. 26/08/22

[34] ALCALDIA MAYOR DE BOGOTÁ. Décimo Primer lineamiento distrital: Inventario de activos de información [en línea]. 11. Bogotá, D.C.: [s.n.], 2015 [consultado el 28, julio, 2022]. 28 p. Disponible en Internet: <https://doi.org/chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://secretariageneral.gov.co/sites/default/files/linemientos-distritales/L_11%20Inventario%20de%20Activos%20de%20Información.pdf>.
[35] Manual de Políticas de Seguridad de la Información de la Cámara de Representantes. (2020, Julio). https://www.camara.gov.co/sites/default/files/2021-01/MANUAL%20POLITICAS%20DE%20SEGURIDAD%20-%20V2%2020200702%20%282%29%20%282%29_1.docx
[36] Martínez Ferreras, D. (s. f.). Los Tesauros. Universidad Oberta de Cataluña, (PID_00143963), p. 35. https://biblioteca.udgvirtual.udg.mx/jspui/bitstream/123456789/1353/1/Los%20tesauros.pdf