



**UNIDAD DE BÚSQUEDA**  
DE PERSONAS DADAS POR DESAPARECIDAS

**Dirección General**  
**Proceso Gestión de Tecnologías de la Información y las Comunicaciones**

---

# **MANUAL DE SEGURIDAD DE LA INFORMACIÓN**

Junio de 2023

## TABLA DE CONTENIDO

<b>1. Introducción .....</b>	<b>3</b>
<b>2. Objetivo .....</b>	<b>4</b>
<b>3. Alcance .....</b>	<b>4</b>
<b>4. Definiciones.....</b>	<b>4</b>
<b>5. Marco Normativo.....</b>	<b>6</b>
<b>6. Roles y Responsabilidades.....</b>	<b>6</b>
<b>7. Apoyo / Soporte .....</b>	<b>7</b>
<b>8. Lineamientos y Políticas específicas de Seguridad de la Información.....</b>	<b>8</b>
8.1. Gestión de la información.....	8
8.2. Seguridad de las instalaciones .....	10
8.3. Prevención de riesgos de Seguridad de la Información.....	13
8.4. Gestión de Eventos e Incidentes de Seguridad de la Información.....	14
8.5. Cultura institucional de Seguridad de la Información .....	15
8.6. Uso de dispositivos móviles .....	17
8.7. Manejo de equipos de computo .....	19
8.8. Controles de Acceso Lógicos .....	22
8.9. Control de cuentas privilegiadas .....	24
8.10. Controles para la Gestión de Redes .....	25
8.11. Controles de Uso de Internet.....	26
8.12. Control Copias de Seguridad .....	28
8.13. Desarrollo Seguro .....	30
8.14. Políticas de Seguridad para la Gestión de Proyectos .....	32
8.15. Relación con Proveedores y terceros.....	33
8.16. Protección y Seguridad Digital para el Intercambio o acceso de Información ....	34
8.17. Servicios en la Nube .....	36
8.18. Uso de Dispositivos de Almacenamiento Externos.....	37
8.19. Uso de Correo Electrónico .....	39
8.20. Fortalecimiento de la Infraestructura de Seguridad Digital.....	40
8.21. Control para el Trabajo Seguro a Distancia o en casa .....	42
8.22. Seguimiento y Evaluación al Sistema de Seguridad de la Información .....	43
<b>9. Uso Aceptable de los activos.....</b>	<b>45</b>
<b>10. Sensibilización y Comunicación en Seguridad de la Información .....</b>	<b>50</b>
<b>11. Mejora .....</b>	<b>51</b>
<b>12. Manejo de Desviaciones y Excepciones .....</b>	<b>51</b>
<b>13. Proceso Disciplinario o Sancionatorio.....</b>	<b>52</b>
<b>14. Anexos.....</b>	<b>52</b>

## 1. Introducción

La Unidad de Búsqueda de Personas dadas por Desaparecidas en el Contexto y en Razón del Conflicto Armado en adelante (UBPD) como Entidad de carácter humanitario y extrajudicial funda su mandato en el principio de construcción de confianza, el cual tiene como finalidad garantizar a todas las familias, aportantes, personas y organizaciones que buscan, que la información suministrada a la entidad será tratada bajo el marco de la protección, seguridad y confidencialidad de la información, garantizando que se protegerán sus datos y no serán revelados con el fin de mantener a salvo su integridad y seguridad.

La UBPD se rige por el marco jurídico para el manejo de la información misional de acuerdo a lo establecido en 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, de esta manera adelanta sus actividades en el marco de la confidencialidad con el fin de resguardar la información que produce, recibe, recolecta y gestiona, formulando políticas y lineamientos en seguridad de la información a fin de hacer más eficaz su misionalidad, generar confianza en los ciudadanos, y así obtener información útil para la búsqueda de las personas dadas por desaparecidas.

De otro lado, es importante resaltar que el carácter humanitario y extrajudicial de la UBPD exige condiciones idóneas para la seguridad de la información, que garanticen su confidencialidad; por lo tanto, se hace necesaria la implementación y mantenimiento del Sistema de Seguridad de la Información – en adelante SSI, el cual busca establecer un marco de confianza en su actuar, enmarcado en el cumplimiento de las leyes y en concordancia con la misión de la entidad. Así mismo, entre las estrategias para la gestión de la información se dispondrá de mecanismos que garanticen su confidencialidad, brindando así garantías a los aportantes.

Así mismo, la UBPD hace uso de herramientas y servicios que ofrecen las tecnologías de la información y las comunicaciones TIC, con el fin de facilitar y soportar el flujo de información interna y externa, la comunicación electrónica entre sus servidores y servidoras, contratistas, terceros, entidades públicas, 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 personas, comunidades, organizaciones públicas y privadas, relacionado con su patrimonio, buen nombre, privacidad e integridad física.

Con base en lo expuesto, el Manual de Seguridad de la Información está orientado a documentar, prevenir, mitigar<sup>1</sup> y gestionar los riesgos y amenazas asociados a la información física como digital y el uso de los entornos digitales, en pro del aprovechamiento de las tecnologías de la información y comunicaciones como herramienta estratégica para el cumplimiento específico del mandato institucional, la normatividad vigente y la mejora continua mediante la ejecución de controles que garanticen la confidencialidad, integridad y disponibilidad de la información.

---

<sup>1</sup> Mitigar minimizar el impacto de los riesgos que puedan afectar la seguridad digital de la UBPD

## 2. Objetivo

Establecer las políticas específicas y lineamientos relacionados con la seguridad de la información abordando temáticas específicas definidas en el presente manual, como complemento a lo definido en la “**GTI-PC-001 Política General de Seguridad de la Información**” con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la UBPD.

## 3. Alcance

El presente Manual de Seguridad de la Información aplicará a servidores, servidoras, contratistas, terceros, procesos y controles definidos para el cumplimiento del Sistema de la Seguridad de la Información de la UBPD.

## 4. Definiciones

**ACCIÓN CORRECTIVA:** Acción tomada para eliminar la causa de una no conformidad detectada u otra situación indeseable.<sup>2</sup>

**ACCIÓN DE MEJORA:** Actividad para mejorar el desempeño.<sup>3</sup>

**ACTIVO DE INFORMACIÓN:** Se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas...) que tenga valor para la organización.<sup>4</sup>

**AMENAZA:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.<sup>5</sup>

**AUDITORÍA:** Es un proceso de verificación y/o validación del cumplimiento de una actividad según lo planeado y las directrices estipuladas<sup>6</sup>

**CONFIDENCIALIDAD:** Garantizar que la información es accesible sólo para aquellos autorizados a tener acceso.<sup>7</sup>

**CONTROL:** Medida que modifica el riesgo. Sinónimo de salvaguarda<sup>8</sup>

**DISPONIBILIDAD:** Propiedad de ser accesible y utilizable a pedido por una entidad autorizada.<sup>9</sup>

**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.<sup>10</sup>

**INFORMACIÓN:** Se refiere a un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen.<sup>11</sup>

**INFORMACIÓN PÚBLICA:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.<sup>12</sup>

**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

---

<sup>2</sup> Norma Técnica Colombiana, NTC -ISO 9000:2015 Sistema de Gestión de la Calidad

<sup>3</sup> Ibidem

<sup>4</sup> 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>

<sup>5</sup> Ibidem

<sup>6</sup> GRUPO VIDAWA SAS. (s/f). Auditoría, conceptos y definiciones clave. Kawak.net. Recuperado el 24 de mayo de 2023, de <https://landing.kawak.net/conceptos-y-definiciones-clave-de-auditoria>

<sup>7</sup> NTC ISO/IEC 27002:2013

<sup>8</sup> 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>

<sup>9</sup> Norma ISO 27000:2018

<sup>10</sup> Lista de Glosarios de términos especializados (2017.febrero 17). Recuperado de <https://glosarios.servidor-alicante.com/>

<sup>11</sup> Ley 1712 del 6 de marzo de 2014, Artículo 6

<sup>12</sup> Ley No.1712 del 2014, Ley de Transparencia y del derecho de acceso a la información Pública Nacional

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.<sup>13</sup>

**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.<sup>14</sup>

**INTEGRIDAD:** Propiedad de salvaguardar la exactitud y estado completo de los activos de información.<sup>15</sup>

**NO CONFORMIDAD:** El no cumplimiento de un requisito especificado a la cual se debe dar tratamiento. Debe tratarse con una acción correctiva<sup>16</sup>

**OBSERVANCIA:** Cumplimiento exacto y puntual de lo que se manda ejecutar, como una ley, un estatuto o una regla.<sup>17</sup>

**OTP:** El código OTP es una contraseña de un único uso.

**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.<sup>18</sup>

**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.<sup>19</sup>

**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.<sup>20</sup>

**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.<sup>21</sup>

**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).<sup>22</sup>

---

<sup>13</sup> Ibidem

<sup>14</sup> Ibidem

<sup>15</sup> Ibidem

<sup>16</sup> Norma Técnica Colombiana, NTC -ISO 9000:2015 Sistema de Gestión de la Calidad

<sup>17</sup> NTC ISO/IEC 27000:2013

<sup>18</sup> Concepto creado por la UBPD

<sup>19</sup> ISO/IEC 27000, (ISO Guía 73:2002)

<sup>20</sup> Seguridad de la Información [En Wikipedia]. Recuperado (2022, mayo 23) de

[https://es.wikipedia.org/wiki/Seguridad\\_de\\_la\\_informaci%C3%B3n](https://es.wikipedia.org/wiki/Seguridad_de_la_informaci%C3%B3n)

<sup>21</sup> ¿Qué es un SGSI – Sistema de Gestión de Seguridad de la Información? (2013, febrero 19). Tomado de <https://www.firma-e.com/blog/quees-un-sgsi-sistema-de-gestion-de-seguridad-de-la-informacion/>

<sup>22</sup> ALCALDÍA 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: . 35 Manual de Políticas de Seguridad de la Información de la Cámara de Representante

**Tercero:** Hace referencia a proveedores, empresas, organizaciones o entidades del estado con las que se realice algún convenio de acceso o transferencia de información.<sup>23</sup>

## 5. Marco Normativo

La Unidad de Búsqueda de Personas Dadas por Desaparecidas en el Contexto y en Razón del Conflicto Armado-UBPD establece el Normograma del Modelo de Operación por Procesos de la UBPD (DPE-FT-018) donde se referencia el marco normativo que debe dar cumplimiento el SSI.

## 6. Roles y Responsabilidades

La UBPD ha suscrito el documento Roles y Responsabilidades del SSI, las cuales están sustentadas en la resolución 588 de 2020, que establece:

- Todos los roles necesarios para llevar a cabo las actividades requeridas por el SSI.
- Las responsabilidades que asume cada uno de los actores involucrados en el SSI.
- La responsabilidad del Oficial de Seguridad como encargado de informar sobre el desempeño del SSI a la Dirección y al resto del personal que se encuentre involucrado o interesado.

Cada uno de estos roles y responsabilidades se encuentran mapeados en el “Anexo - Matriz de Roles y Responsabilidades RACI”.

En cuanto a las responsabilidades dentro del presente manual se describen tres tipos de responsables:

- **Implementación:** Se refiere a las áreas, dependencias, servidores(as) que serán responsables de poner en funcionamiento o en práctica cada uno de los lineamientos definidos.  
**Apoyo a la implementación:** Se refiere a las áreas, dependencias, servidores(as) o contratistas que apoyaran al responsable en la implementación de los lineamientos.
- **Cumplimiento:** Se refiere a los servidores(as) contratistas o proveedores que deben cumplir los lineamientos, procedimientos o instructivos definidos por los implementadores o apoyos a la implementación.
- **Acompañamiento y Orientación:** Se refiere a las unidades u oficinas de control interno, auditoría interna o quien haga sus veces, las cuales brindan un nivel de asesoría proactivo y estratégico que vaya más allá de la ejecución eficiente y eficaz del Plan Anual de Auditorías.

---

<sup>23</sup> 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](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)

## **7. Apoyo / Soporte**

### **7.1 Recursos**

La UBPD elabora una vez al año el Presupuesto Anual, en el que también se consideran los recursos requeridos para el establecimiento, implementación, mantenimiento y mejora continua del SSI. Dicho presupuesto es aprobado por el Comité de Contratación, en concordancia con lo establecido en el Plan Anual de Adquisiciones.

Asimismo, se garantiza contar con los recursos humanos necesarios para el SSI, mediante decisión del Comité de Seguridad de la Información o quien haga sus veces. A su vez este Sistema se encuentra liderado por el Servidor con el rol de Oficial de Seguridad de la Información designado por la Dirección General quien es la dependencia responsable del SSI dentro del Sistema Integrado de Gestión-SIG.

Adicionalmente se cuenta con los recursos de infraestructura tecnológica y física, que han sido establecidas y revisadas en el marco de la mejora continua para el cumplimiento de los controles establecidos del SSI.

### **7.2 Competencia**

La UBPD ha determinado las competencias necesarias de las personas que apoyan y asumen funciones específicas ligadas exclusivamente a las tareas del SSI, sobre la base de la educación o experiencia adecuada, seguimiento realizado por la Subdirección de Gestión Humana.

Adicionalmente ha asegurado el cumplimiento de estas competencias mediante las capacitaciones del personal vinculado a la UBPD, lo que se ha documentado en el GCN-PL-001 Plan Institucional de Capacitaciones. Este plan puede ser actualizado si se detectan deficiencias en el conocimiento del personal, de manera que se programan capacitaciones adicionales.

### **7.3 Apropiación**

Las estrategias de concientización son realizadas, según lo especificado en el Plan de Uso y Apropiación en Seguridad.

La difusión de la Política General de Seguridad de Información se realiza mediante envío de dicho documento por medio de comunicación oficial por correo electrónico a todos los servidores(as) de la entidad. Cabe resaltar que la política forma parte de los temas tratados en las charlas de sensibilización y concientización.

Cada charla de capacitación y concientización programada cuenta con la Lista de Asistencia (DPE-FT-002) de Capacitación.

### **7.4 Comunicación**

to que es actualizado conforme se avanza con la implementación del Sistema, éste define:

- Comunicación,

- Emisor,
- Destinatarios,
- Fecha de emisión,
- Procesos afectados,
- Estado.

## 7.5 Documentación de la Información

El SSI cuenta con los documentos y registros necesarios para la implementación de este tomando como referencia los requisitos establecidos en la norma ISO 27001, los cuales son usados para asegurar la efectividad del Sistema. Esta documentación se actualiza de acuerdo con las necesidades que tenga la Entidad, cumplimiento normativo y los requisitos del Sistema.

La documentación del SSI es controlada y garantiza su disponibilidad e idoneidad. Los procedimientos y guías publicadas en el sistema integrado de gestión se controlan siguiendo el procedimiento Control de Información documentada (DPE-PR-001), para la demás documentación y registros se logra a través de la aplicación de actividades de control:

- Distribución restringida, acceso controlado, mecanismos de recuperación y restricciones de uso.
- Condiciones adecuadas de almacenamiento y conservación.
- Control de cambios sobre los documentos, retención y disposición.

Adicionalmente se vela por su adecuada protección.

## 8. Lineamientos y Políticas específicas de Seguridad de la Información.

La UBPD, establece a continuación los lineamientos para la seguridad de la información, los cuales deberán ser cumplidos por todos lo(a)s servidores, servidoras, contratistas, terceros, usuarios y visitantes. Las políticas de seguridad de la información se aplican a los activos de información de la UBPD, a nivel central y en sus equipos territoriales en todos los procesos. Estos lineamientos de seguridad están clasificados en diferentes temáticas, teniendo en cuenta el contexto interno y externo de la entidad:

### 8.1. Gestión de la información

**8.1.1. Objetivo:** Desarrollar lineamientos para garantizar la seguridad de la información, implementando criterios para la adecuada gestión de esta.

#### 8.1.2. Lineamientos

- a. 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 para el manejo de la información pública clasificada y pública reservada GDO-MN-001, y lo establecido dentro de las políticas de Gestión de Información y Gestión Documental.
- b. La información de la UBPD debe ser protegida y asegurada según los lineamientos establecidos en la Política General de Seguridad de la Información.

- c. La información producida que sea resultante del desarrollo de los procedimientos de la UBPD debe encontrarse en los soportes normalizados publicados en el sistema integrado de gestión.
- d. La información producida por la UBPD en razón a sus funciones, procesos y procedimientos debe estar registrada e identificada en la GSI-FT-003 Matriz de Activos de Información e Índice de Información Clasificada y Reservada y ésta debe estar articulada con los instrumentos técnicos archivísticos que la unidad disponga para ello.
- e. La información producida, recibida y/o recolectada por la UBPD goza de protección y seguridad mediante la implementación, seguimiento y mejoramiento de herramientas, controles, procedimientos, etc., con el fin de evitar los riesgos asociados a su disponibilidad, confidencialidad e integridad.
- f. 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.
- g. Toda información producida debe tener definida una persona responsable que custodie dicha información, quien velará por la protección adecuada y seguridad de estos activos.
- h. La información producida, recibida y/o recolectada por la UBPD se gestionará con base en el GTI-PR-016 (SGSI) Procedimiento Gestión de Activos y GTI-GU-015 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.
- i. Lo(a)s servidores(as) y contratistas deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- j. Todo (a) servidor(a), contratista o tercero 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 calificada como clasificada o reservada, conocida por parte de las (os) servidoras (es), contratistas 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.
- k. 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, privacidad y seguridad de la información.

- l. Los activos de información de la UBPD son de uso exclusivo para el desempeño de las actividades designadas.
- m. Lo(a)s servidore(a)s, contratistas de la UBPD deben almacenar toda la información en las carpetas compartidas o en la nube de almacenamiento institucional(drive) según corresponda.
- n. La información producida, recibida y/o recolectada por la UBPD solo puede almacenarse y/o procesarse en las herramientas, equipos de cómputo, repositorios, entre otros definidos por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC para tal fin.
- o. La información calificada como pública clasificada o pública reservada debe estar cifrada haciendo uso de la herramienta definida por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC para tal fin.
- p. La información calificada como pública clasificada o pública reservada no debe ser almacenada en nubes o dispositivos de almacenamiento no autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.

## Responsables

- Líderes de Procesos (implementación)
- Dirección Técnica de Información, Planeación y Localización para la Búsqueda (Apoyo a la implementación)
- Subdirección de Gestión de Información para la Búsqueda (Apoyo a la implementación)
- Subdirección administrativa y financiera (Apoyo a la implementación)
- Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Apoyo a la implementación)
- Servidore(a)s y contratistas (Cumplimiento)

## 8.2. Seguridad de las instalaciones

**8.2.1. 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.

### 8.2.2. 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. Para el acceso a las áreas seguras se deben seguir los lineamientos estipulados en el GTI-PR-015 (SGSI) Trabajo en Áreas Seguras.

- c. Para asegurar la conservación y preservación de cualquier tipo de información se debe aplicar las directrices estipuladas en el GDO-MN-002 Manual del sistema integrado de conservación documental.
- d. Se definirán y delimitan como áreas de acceso restringido/áreas seguras los espacios físicos en los que se aloja la información misional o que pertenezcan a los tipos de áreas seguras definidas:
- Archivos de Gestión
  - Centro de Cómputo y Cuartos de Cableado
  - Oficinas Nivel Restringido
- e. 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).
- f. En las áreas seguras donde se encuentren activos informáticos y de archivo documental, se debe cumplir como mínimo con los siguientes lineamientos:
- No consumir alimentos ni bebidas.
  - No ingresar sustancias inflamables.
  - No permitir el acceso de personal ajeno a la UBPD.
  - No se deben almacenar elementos ajenos a los requeridos de acuerdo con la actividad que se realice en el área segura.
  - No se permite tomar fotos o grabaciones de las áreas seguras sin la previa autorización del responsable de dichas áreas.
  - 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 en el formato GTI-FT-044 (SGSI) Bitácora ingreso áreas seguras.
- g. Para la selección e implementación de controles de seguridad para las áreas 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, inundaciones; y situaciones producidas intencionalmente o resultantes de fallas humanas como incendios, explosiones, actos terroristas, robo, espionaje, infiltración, ataques contra la UBPD o conflictos armados, para ello se tomará como insumo el Plan de Emergencia y Contingencia Nivel central (GTH-PL-004\_V2) y el Manual del Sistema integrado de Conservación Documental (GAD-MN-002), específicamente en el Programa de prevención de emergencias y atención de desastres para material documental.
- h. 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 06 de 2014 sobre conservación de documentos, del Archivo General de la Nación; con base en los cuales la UBPD propenderá por la disposición de:

- Detectores automáticos de humo o de calor conectados con servicios exteriores de urgencia.
  - Personal de vigilancia
  - Sistemas de extinción escogidos con la asesoría de los bomberos: extinguidores manuales, sistemas de extinción fijos.
  - Puertas cortafuego
  - Realizar programas regulares de mantenimiento de las instalaciones eléctricas y asegurarse que las salidas de emergencia sean de fácil acceso y de apertura desde el interior.
  - 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.
  - 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.
- i. Todas las puertas que utilicen 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 y terceros autorizados, evitar que las puertas permanezcan abiertas.
- j. Se exigirá a servidores (as), contratistas o terceros, sin excepción, el porte en un lugar visible del mecanismo de identificación (carné) adoptado por la UBPD, mientras se encuentren dentro de las instalaciones de la entidad o cumpliendo con la misionalidad en terreno.
- k. Las personas que ingresen o salgan de las instalaciones de la UBPD, independientemente de su calidad, deben registrar en la bitácora de vigilancia, el ingreso y salida de los dispositivos tecnológicos institucionales o personales.
- l. Las (os) visitantes deberán permanecer acompañados(as) de un (a) servidor (a) de la UBPD, cuando se encuentren dentro de alguna de las áreas seguras o restringidas de la Entidad.
- m. Es responsabilidad de servidores (as), contratistas o 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.
- n. 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

Coordinación del Grupo Interno de Trabajo de Gestión Documental (Implementación)  
Coordinación del Grupo Interno de Trabajo de Gestión Administrativa (Implementación)  
Oficial de Seguridad de la Información (Apoyo a la Implementación)  
Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Apoyo a la Implementación)  
Servidore(a)s y contratistas (Cumplimiento)

### 8.3. Prevención de riesgos de Seguridad de la Información.

**8.3.1. Objetivo:** Prevenir afectaciones a la integridad, disponibilidad y confidencialidad de la información a través de la identificación y gestión oportuna de los riesgos de seguridad.

#### 8.3.2. Lineamientos

- a. Los servidores(as) y contratistas de la UBPD deberán reportar oportunamente y con carácter obligatorio, los riesgos de seguridad de la información identificados.
- b. Los líderes de los procesos deberán documentar los resultados de la evaluación de riesgos y los planes de tratamiento de los riesgos de seguridad de la información existentes en la Entidad.
- c. La UBPD implementa controles orientados a minimizar la probabilidad de que un riesgo de seguridad de la información se materialice.
- d. Se realizan campañas de socialización y comunicación de la Metodología de Gestión de Riesgos de Seguridad de la Información, 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.
- f. La frecuencia y condiciones para la realización de las Gestiones de Riesgo son las especificadas en la Metodología Gestión de Riesgos de seguridad de la información.
- g. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) realiza Análisis de vulnerabilidades y pruebas de seguridad orientadas a los Sistemas de Información, Infraestructura y Servicios tecnológicos, así como pruebas de Ingeniería Social a servidore(a)s, contratistas y terceros, con el fin de establecer brechas que puedan llegar a materializar riesgos de seguridad de la información.
- h. La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) administra y monitorea proactiva y preventivamente los entornos digitales, con el fin de proteger y asegurar los sistemas de información, herramientas, accesos lógicos, hardware y software dispuestos para la operación segura de la UBPD, mitigando las vulnerabilidades o debilidades identificadas.

## Responsables

Oficial de Seguridad de la Información (implementación)

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)

Proveedores (Cumplimiento)

Servidora(a)s y contratistas (Cumplimiento)

## 8.4. Gestión de Eventos e Incidentes de Seguridad de la Información.

**8.4.1. Objetivo:** Establecer los lineamientos para asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información.

### 8.4.2. Lineamientos

- a. Los servidores(as) y contratistas de la UBPD deberán reportar oportunamente y con carácter obligatorio los incidentes o eventos de seguridad de la información cuando estos se presenten, de acuerdo con lo definido en el GSI-PR-003 Gestión de Incidentes de Seguridad de la Información.
- b. Los incidentes de seguridad deberán documentarse y clasificarse de acuerdo con las actividades definidas en la GSI-GU-001 Guía de Gestión de Incidentes de Seguridad de la Información.
- c. manera inmediata por parte de servidores(as) y contratistas de la UBPD 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 la Gestión de Incidentes de Seguridad de la Información.
- d. 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.
- e. La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC informa a la Dirección General, a(l) (la) Oficial de Seguridad de la Información y/o al Comité de Seguridad de la Información o quien haga sus veces, las vulnerabilidades, riesgos o incidentes de seguridad que se hayan presentado o se estén presentando, que impidan la continuidad de los servicios tecnológicos y/o afecte la confidencialidad y/o integridad de la información impactando la operación normal de la Entidad de acuerdo al nivel de criticidad resultante de la valoración del incidente.
- f. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC realiza la aplicación de medidas o controles de seguridad digital requeridos por la Dirección General en pro del cumplimiento misional de la UBPD, así como, del Comité de Seguridad de la Información o quien haga sus veces, que permitan minimizar la ocurrencia de eventos y/o incidentes de seguridad de la información.

- g. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC implementa las herramientas tecnológicas necesarias para monitorear y prevenir la ocurrencia de incidentes de seguridad de la información.
- h. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC y e(l) (la) Oficial de Seguridad de la Información, deben mantener contacto con grupos de interés especiales como Mintic, ColCert, Csirt entre otros, los cuales le permitan tener conocimiento sobre las mejores prácticas y mantenerse actualizado con la información de seguridad relevante, que ayude a prevenir incidentes de seguridad.
- i. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC podrá solicitar apoyo de entidades externas y/o proveedores para la aplicación de medidas de contención y recuperación de los activos de información afectados previa evaluación y/o análisis del incidente.

### **Responsables**

Oficial de Seguridad de la Información (Implementación)

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)

Proveedores (Cumplimiento)

Servidore(a)s y Contratistas (Cumplimiento)

## **8.5. Cultura institucional de Seguridad de la Información**

**8.5.1. Objetivo:** Generar conocimiento, apropiación e implementación de prácticas de Seguridad de la Información por parte de servidores (as), contratistas y terceros de la UBPD, con base en el fortalecimiento de la cultura institucional respecto al tema.

### **8.5.2. 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).
- b. La UBPD desarrollará procesos para sensibilizar de manera permanente a los servidores, servidoras, contratistas en temas de seguridad de la información.
- c. La Oficina de Tecnologías de la Información y las Comunicaciones – OTIC y el Oficial de Seguridad de la Información, diseñan y desarrollan anualmente el Plan de Uso y Apropiación donde se establecen los temas que se deben comunicar, los temas de sensibilización, los responsables, herramientas, público objetivo y el cronograma para la ejecución de estas actividades, con el fin de realizar la divulgación de los lineamientos, procesos, procedimientos y controles que se establezcan y el fomento del comportamiento responsable y seguro en los entornos digitales.

- d. Los (as) servidores (as), contratistas o terceros de la UBPD deberán participar de manera activa en las jornadas de sensibilización y capacitación orientadas al fortalecimiento de la Seguridad de la Información, con el fin de mantenerse informado y fortalecer los conocimientos y habilidades para responder ante posibles riesgos y amenazas digitales.
- e. La UBPD monitoreará el nivel de conocimiento y conciencia sobre las prácticas de seguridad de la información de servidores(as), contratistas o terceros; con miras a identificar de forma oportuna los aspectos que deben ser reforzados para evitar vulnerabilidades derivadas de la gestión del personal.
- f. 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.
- g. 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 terceros de la entidad.
- h. Los eventos o incidentes de seguridad de la información que tengan como causa el descuido, las malas prácticas, el no acatamiento de las políticas, o recomendaciones socializadas en las actividades establecidas en el Plan de uso y apropiación de Seguridad de la Información serán responsabilidad de lo(a)s servidores(as) y contratistas de la UBPD.
- i. Los(as) servidores(as), contratista de la UBPD deberán acogerse a la implementación de los procedimientos, tal como el procedimiento Organización de los archivos de gestión (GAD-PR-006), 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.
- j. El carné de acceso a las instalaciones es personal por lo tanto no se debe prestar ni permitir el acceso a otras personas con este y se debe portar en todo momento dentro de las instalaciones de la Unidad y en el cumplimiento de la misionalidad en terreno.

### **Responsables**

Oficial de Seguridad de la Información (Implementación)

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)

Subdirección de Gestión Humana (Apoyo en la implementación)

Oficina Asesora de Comunicaciones y Pedagogía (Apoyo en la implementación)

Servidora(e)s y contratistas (Cumplimiento)

### **8.6. Uso de dispositivos móviles**

- 8.6.1. Objetivo:** Establecer los lineamientos para mitigar los riesgos de seguridad de la información y garantizar la protección y seguridad digital de los dispositivos móviles institucionales o personales como celulares, Ipads, GPS, Cámaras entre otros,

autorizados para acceder a los servicios tecnológicos dispuestos por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC de la UBPD.

### 8.6.2. Lineamientos

- a. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC instala, actualiza y configura el software y los controles que considere necesarios para la protección de los dispositivos móviles institucionales, implementa controles en los servicios o infraestructura a la que se accede desde dispositivos móviles personales autorizados; estos controles deben ser aceptados y adoptados por los servidores(a)s, contratistas y terceros, mitigando las pérdidas, fugas de información o la afectación de los mismos ante ciberataques.
- b. El uso de los dispositivos móviles institucionales es exclusivamente para realizar las labores que requiera la UBPD.
- c. La instalación, configuración, mantenimiento preventivo y correctivo, de los dispositivos móviles, propiedad de la UBPD, estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC quién atenderá las solicitudes o programará los mantenimientos a través de la mesa de servicio.
- d. La instalación de software y cambios de configuración en los dispositivos móviles de propiedad de la UBPD debe ser autorizada y coordinada por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.
- e. Cuando el dispositivo móvil propiedad de la UBPD o los dispositivos móviles personales que sean autorizados para acceder a la información, o los sistemas de información sean perdidos, hurtados o se considere que se ha comprometido la seguridad de éste, el usuario debe notificar a la mesa de servicios de manera inmediata directamente o por intermedio del Jefe de la dependencia, para proceder a retirar los accesos y realizar el borrado de la información.
- f. Los dispositivos móviles propiedad de la UBPD y que sean asignados a sus servidores(a)s, contratistas deben cumplir como mínimo con las siguientes condiciones de seguridad:
  - Garantizar el control de acceso al usuario mediante contraseña robusta, reconocimiento de huella, o reconocimiento facial, o PIN o patrón.
  - Activar el bloqueo de pantalla con contraseña después de un tiempo de desuso o por activación manual.
  - Tener instalada y actualizada la herramienta antivirus que defina la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.
  - Tener instalado únicamente el software autorizado por la entidad.
  - Cambiar la contraseña por defecto asignada por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC y actualizarla cada tres meses.
  - Hacer un uso controlado de las diferentes formas de grabación disponibles como son voz, cámaras de video y fotográfica, evitando registros no autorizados o que vayan en contra de la Legislación Colombiana.

- g. Se encuentra prohibido realizar instalaciones de aplicaciones que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información almacenada o transmitida por el dispositivo. En todo caso las instalaciones realizadas en dispositivos móviles deberán realizarse por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.
- h. Es responsabilidad del servidor(a) o contratista al que le sea asignado y use dispositivos móviles institucionales, sincronizar o cargar la información almacenada en los mismos cada vez que finalice la actividad desarrollada, alojándola en los servicios de nube autorizados por la entidad, con el fin de tener respaldo de la información.
- i. Los dispositivos móviles que no sean propiedad de la UBPD y que estén autorizados para acceder a la información, sistemas de información o servicios tecnológicos institucionales, deben contar como mínimo con las siguientes condiciones de seguridad:
- Garantizar control de acceso mediante contraseña o reconocimiento de huella.
  - Tener instalada y actualizada una herramienta de antivirus.
  - Perfil de trabajo independiente para el tratamiento de la información de la Unidad de Búsqueda de Personas dadas por Desaparecidas.
  - Tener actualizado el Sistema Operativo del dispositivo móvil en la versión más reciente y estable.
  - Cumplir con la reglamentación vigente en materia de uso de software legal, por lo anterior, el usuario es responsable de contar con todo el software de su dispositivo debidamente licenciado.
- j. Cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de los dispositivos móviles mencionados en el punto anterior, debe ser reportada como un incidente de seguridad de la información.
- k. Los dispositivos móviles propiedad de la UBPD utilizan mecanismos para la ubicación en caso de pérdida o extravío, cifrado, bloqueo, borrado remoto y el retiro de acceso a los sistemas de información o información cuando el dispositivo haya sido robado, extraviado o esté comprometida su seguridad.
- l. La información producida, recibida y/o recolectada por la UBPD mediante los dispositivos móviles (Celulares, Ipad, GPS, Scanners, cámaras de video y fotográficas, entre otros) debe ser almacenada en el menor tiempo posible en las carpetas compartidas o en la nube de almacenamiento institucional(drive). Una vez almacenada se debe realizar el borrado seguro de esta información.
- m. Las conexiones inalámbricas (Bluetooth, WiFi, NFC, entre otras) solo deben activarse cuando se requiera realizar uso de estas.
- n. Los dispositivos móviles asignados por la entidad deben permanecer en las instalaciones de la entidad, excepto cuando sea necesario retirarlos de estas para ser utilizados en actividades inherentes al desarrollo de las funciones, como en comisiones, reuniones

externas, eventos, trabajo Seguro a Distancia o en casa o cualquier otra actividad de este tipo que esté autorizada, y deben retornar a las instalaciones en el menor tiempo posible una vez culminada dicha actividad.

### **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)  
Coordinador de servicios tecnológicos (Apoyo en la Implementación)  
Servidora(e)s y contratistas. (Cumplimiento)

## **8.7. Manejo de equipos de computo**

**8.7.1. Objetivo:** Realizar un manejo adecuado frente al uso de los computadores de escritorio, portátiles, impresoras y otros dispositivos por personas no autorizadas, en el momento en que se encuentren desatendidos.

### **8.7.2. Lineamientos**

- a. Los equipos asignados a los servidore(a)s y contratistas son para el uso exclusivo e intransferible del cumplimiento de las funciones u obligaciones asignadas, y la responsabilidad de su uso recaerá sobre la persona a la que le fue asignado.
- b. Se recomienda todas las medidas preventivas al momento de consumir bebidas y alimentos en el puesto de trabajo, considerando que el verter líquidos puede causar daños en los documentos y/o equipos electrónicos y esto será responsabilidad del servidor(a) o contratista.
- c. La Unidad se reserva el derecho de monitorear el contenido y software instalado en los equipos de la entidad para verificar el tipo de información, su uso y licenciamiento del software instalado. De esta manera contenidos de música, vídeo, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del funcionario o contratista podrían ser borrados sin previa consulta. Así mismo, el software no autorizado o sin licenciamiento, será desinstalado.
- d. Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar, desconectar, retirar, y/o reparar equipos, son los técnicos de soporte designados por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC previa solicitud a través de la mesa de servicio.
- e. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC a través de la mesa de servicio deberá aprovisionar los computadores antes de ser entregados, garantizando que:
  - Sean formateados a bajo nivel o borrados de manera segura para que la información de los anteriores usuarios no sea recuperable o accesible.
  - El software instalado sea el software base (Software Estándar Corporativo) definido por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC y este cuente con el respectivo licenciamiento.

- Los sistemas operativos y demás aplicativos deberán tener instaladas las últimas actualizaciones estables a la fecha de entrega del equipo.
  - El antivirus deberá permanecer actualizado, funcionando y administrado desde consola.
  - Las herramientas de seguridad establecidas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.
- f. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC a través de la mesa de servicio, se asegura que los usuarios y perfiles de usuario que traen por defecto los sistemas operativos y software instalado en los computadores de escritorio, equipos portátiles, impresoras y demás dispositivos adquiridos por la entidad sean modificados antes de entrar en uso. Dichos elementos deben entregarse sin permisos de acceso con rol de administrador, al usuario final.
- g. El bloqueo automático de la pantalla y la ejecución del protector de pantalla en los computadores de escritorio y/o portátiles de la UBPD después de un tiempo determinado de inactividad (5 min) será implementado como control preventivo de intrusión no autorizada a los equipos. La implementación de estos mecanismos preventivos estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC. Sin embargo, cada usuario deberá garantizar que nadie pueda ingresar al equipo de cómputo durante su ausencia, bloqueando su estación de trabajo antes de alejarse del mismo.
- h. Las impresoras deben permanecer bloqueadas, todas deben hacer uso del pin asignado para realizar la ejecución de tareas en las mismas y cerrar la sesión cuando se hayan finalizado.
- i. Los servidore(a)s y contratistas que tiene asignado para su trabajo computadores de escritorio y/o portátiles deben bloquear, cuando se ausente de su puesto de trabajo o apagar, al finalizar la jornada laboral, para el caso de los dispositivos móviles (iPads y celulares) deben permanecer bloqueados cuando no se esté realizando uso de estos.
- j. El ambiente de escritorio de los computadores y/o portátiles no se debe utilizar para guardar ningún tipo de archivo, excepto los accesos que se configuren desde la Mesa de Servicio.
- k. Los equipos de cómputo, portátiles y/o dispositivos de impresión y digitalización deben apagarse cuando no estén en uso.
- l. Los equipos portátiles de la Unidad deben entregarse con guaya de seguridad cuando sea viable la instalación de ésta y es responsabilidad de la persona que recibe el equipo, mantenerlo asegurado con la guaya provista.
- m. Los equipos de cómputo, portátiles, celulares, memorias USB cifradas, discos duros externos, iPad, GPS, entre otros, deben quedar en custodia de la Entidad en situaciones administrativas (vacaciones, licencias, incapacidades, entre otras) cuando estas sean igual o superior a 15 días.

- n. Los discos duros de los computadores de escritorio y portátiles suministrados por la UBPD deben estar cifrados haciendo uso de la herramienta destinada por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC para tal fin.
- o. Se debe registrar y/o autorizar todos los equipos tecnológicos de la entidad (equipos de cómputo, portátiles, iPad, celulares, GPS, Escáneres, Memorias USB cifradas, servidores, rack, impresoras, ccess point, discos externos, partes de computador, switches, aire acondicionado, televisores, micrófonos y teléfonos, entre otros) y/o personales que ingresen y/o sean retirados en todas las sedes de la entidad, de acuerdo con los procedimientos definidos por la Subdirección Administrativa y Financiera. Para el retiro de los equipos se debe contar con la autorización del jefe inmediato y la solicitud se debe realizar con el formato de retiro de equipos, GRF-FT-009 Autorización Salida de Bienes de la Entidad.
- p. Los dispositivos personales que estén autorizados para acceder a los recursos de la Unidad deberán aplicar las mismas medidas y configuraciones de seguridad a los dispositivos de la Entidad.
- q. Los usuarios deberán mantener actualizados los dispositivos personales autorizados donde traten información de cualquier tipo de la UBPD.
- r. Cualquier incidencia que pueda afectar a la confidencialidad, integridad o disponibilidad de los dispositivos institucionales o personales debe ser reportada a la mesa de servicio.
- s. Los equipos de cómputo asignados por la entidad deben permanecer en las instalaciones de la entidad, excepto cuando sea necesario retirarlos de estas para ser utilizados en actividades inherentes al desarrollo de las funciones, como en comisiones, reuniones externas, eventos, trabajo Seguro a Distancia o en casa o cualquier otra actividad de este tipo que esté autorizada, y deben retornar a las instalaciones en el menor tiempo posible una vez culminada dicha actividad.

### **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones (Implementación)

Coordinador de servicios tecnológicos (Apoyo en la Implementación)

ServidoraEs y contratistas (Cumplimiento)

## **8.8. Controles de Acceso Lógicos**

**8.8.1. Objetivo:** Establecer lineamientos para asegurar el acceso lógico a los sistemas de información, plataforma tecnológica, servicios de red e instalaciones de procesamiento de información que administra la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.

### **8.8.2. Lineamientos**

- a. Los controles y permisos para el acceso a la información, sistemas de información, plataforma tecnológica y servicios de red serán establecidos de acuerdo con la

clasificación de la información, las funciones u obligaciones de lo(a)s servidore(a)s y contratistas según corresponda, las necesidades y requerimientos de cada una de las áreas de la Unidad de Búsqueda de Personas dadas por Desaparecidas orientadas a garantizar la protección y seguridad de la Información.

- b. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC establece una Política de contraseñas adecuada y alineada con las buenas prácticas en seguridad. La política de contraseñas definirá los requisitos de las contraseñas y los plazos de mantenimiento de una misma contraseña. La Política de contraseñas deberá ser conocida por lo(a)s servidore(a)s y contratistas.
- c. Es responsabilidad de los directores, subdirectores, jefes de oficina y líderes de dependencias realizar el análisis de las necesidades y controles requeridos por sus servidores(as) y contratistas para solicitar la asignación de accesos lógicos al administrador de la plataforma tecnológica.
- d. Es responsabilidad de cada servidor(a), contratista o tercero que tenga acceso o uso de cualquier activo informático de la UBPD, el resguardo de sus contraseñas, por lo tanto, no podrán estar escritas o expuestas en su puesto de trabajo, no deben prestarse o compartirse con el fin de evitar que sean conocidas por otras personas.
- e. Los accesos a la información en formato digital, sistemas de información, plataforma tecnológica y servicios de red de la UBPD serán gestionados mediante la asignación de un usuario único para cada servidor(a) o contratista de acuerdo con su perfil y los accesos necesarios para el cumplimiento de sus funciones u obligaciones, asignados mediante el principio de mínimo privilegio, este usuario es intransferible y cada servidor(a) o contratista es responsable de las acciones que se ejecuten con éste.
- f. Los accesos lógicos, asignados a lo(a)s servidore(a)s y contratistas deben ser desactivados una vez se terminen los vínculos contractuales con la UBPD, por solicitud del supervisor del contrato, la Subdirección de Gestión Humana, el Director, Subdirector o jefe. La desactivación de los permisos de acceso de Servidores(as) se debe realizar acorde con la resolución de desvinculación y la de los contratistas de acuerdo a la fecha de terminación del contrato.
- g. El acceso a las instalaciones de procesamiento de información bajo la responsabilidad de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe ser restringido y contar con los controles suficientes que permitan mitigar el acceso no autorizado, la fuga de información o la salida no autorizada de activos de información, dichos accesos se deben registrar de acuerdo con los procedimientos establecidos para tal fin.
- h. Las conexiones a los sistemas de información que se realicen desde fuera de las instalaciones de la UBPD se deberán realizar mediante las herramientas definidas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, las cuales permiten el registro de las actividades realizadas durante el tiempo de conexión.

- i. La conexión de dispositivos de infraestructura a la red de la UBPD debe ser coordinada con la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC a través de la herramienta de mesa de servicio, de acuerdo con el procedimiento definido.
- j. La creación, modificación, deshabilitación o retiro de usuarios en los sistemas de información o servicios de red se realiza de acuerdo con el procedimiento definido en la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC GTI-PR-006-V2\_Solicitudes de Servicios de TI.
- k. Ante cualquier sospecha de que el usuario asignado para el ingreso a cualquiera de las herramientas tecnológicas o sistemas de información de la entidad ha sido utilizado de manera inadecuada, debe informarse inmediatamente a la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, registrando un caso en la mesa de servicios. El caso será asignado al Experto Técnico responsable de Seguridad Digital quién se encargará de validar la afectación de la información accedida.
- l. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, definirá las condiciones y/o requerimientos para la implementación de mecanismos de doble factor de autenticación (Ej: envío de un código al teléfono celular, uso de aplicaciones para generación de OTP's, entre otros) para los servicios o sistemas de información donde sea requerido un mayor nivel de protección en el acceso.
- m. Todos los servicios digitales deben manejar como mínimo un código o contraseña de acceso para los servidore(a)s, contratistas y terceros de la UBPD.
- n. Lo(a)s servidore(a)s y contratistas deben hacer uso de los mecanismos de doble factor de autenticación establecidos por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC facilitando las herramientas y/o información necesaria para su aplicación.
- o. Los responsables de la administración funcional de sistemas de información y/o aplicativos deben definir y mantener actualizada la matriz de accesos de estos a su cargo identificando los roles y perfiles de los usuarios.
- p. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe realizar el mantenimiento, actualización y/o depuración de las cuentas de usuario de los sistemas de información y/o aplicativos, de acuerdo con las novedades administrativas. Además, deberán realizar la validación de las cuentas en períodos de inactividad mayores a 3 meses.
- q. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC realiza la gestión permanente de los accesos lógicos de los usuarios asignados a lo(a)s servidore(a)s, contratistas y terceros, realizando la habilitación, modificación o desactivación de estos de acuerdo con el tiempo que tenga un vínculo con la UBPD, el cargo o funciones que desempeñen, o si sufren alguna modificación en su rol o cambio de dependencia; esto con el fin de prevenir que los accesos a los sistemas queden activos para usuarios que ya no deberían acceder o que ya no tienen vínculo con la Entidad.

## Responsables

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)

Líderes de Proceso (Cumplimiento)

Subdirección de Gestión Humana (Apoyo en el Cumplimiento)

Responsables de Sistemas de Información (Apoyo en la Implementación)

Servidora (e)s y contratistas. (Cumplimiento)

## 8.9. Control de cuentas privilegiadas

**8.9.1. Objetivo:** Establecer lineamientos para la adecuada gestión de las cuentas de usuarios con privilegios de administración sobre las plataformas tecnológicas.

### 8.9.2. Lineamientos

- a. Las cuentas de usuario privilegiado de la plataforma tecnológica que soporta la operación de los sistemas de información o aplicaciones deben ser autorizadas formalmente por el Coordinador de Infraestructura Tecnológica de la OTIC, las cuentas de administración funcional a cargo de áreas diferentes a la OTIC deben ser informadas al experto técnico designado como líder de seguridad digital.
- b. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe mantener un registro actualizado de las cuentas de usuario privilegiadas, el cual debe contener el responsable y la justificación de la necesidad de uso.
- c. Las cuentas de usuario privilegiado sólo deben ser otorgadas a lo(a)s servidore(a)s y contratistas que las requieran, los cuales deben hacer un uso apropiado de estas y usarlas únicamente para el cumplimiento de sus funciones.
- d. Las cuentas de usuario privilegiado sólo podrán ser utilizadas en la actividad de administración o configuración del sistema o plataforma para la cual se requieren dichos privilegios. No podrá ser utilizada en actividades de operación rutinarias para lo cual debe existir un perfil de menores privilegios que lo permita.
- e. Las cuentas de usuario privilegiado o similares, definidas por defecto, en sistemas e infraestructura tecnológica, deben ser usadas únicamente en caso de que no sea posible asignar cuentas de administración sobre usuarios nombrados y/o en caso de pérdida de acceso de los usuarios de administración nombrados. Siempre que sea posible las mismas deben ser eliminadas o deshabilitadas, además de modificadas sus contraseñas por defecto. Se debe contar con un mecanismo de recuperación de acceso privilegiado, dicho mecanismo debe mantener las garantías de confidencialidad
- f. Para las cuentas de usuario privilegiado o similares, en sistemas e infraestructura tecnológica, deberán definirse los requisitos para la caducidad de los derechos de acceso privilegiado.

- g. Las competencias de los usuarios con derechos de acceso privilegiado deberán revisarse regularmente con el objetivo de verificar que se encuentran alineadas con sus obligaciones.
- h. Las credenciales de acceso de los usuarios privilegiados o similares deben ser almacenadas y/o custodiadas estableciendo mecanismos que aseguren la confidencialidad de la información secreta de autenticación, tales como, cifrado, acceso restringido mediante asignación de contraseña compartida entre la OTIC y el área funcional, la OTIC establece el repositorio donde se almacenarán dichas contraseñas.

### **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones (Implementación)  
Servidora (e)s y contratistas (Cumplimiento)

## **8.10. Controles para la Gestión de Redes**

**8.10.1. Objetivo:** Establecer e implementar los lineamientos para mantener la seguridad de las comunicaciones y las redes.

### **8.10.2. Lineamientos**

- a. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC es responsable de garantizar que los puertos físicos y lógicos de diagnósticos y configuración de plataformas que soporten sistemas de información estén siempre restringidos y monitoreados con el fin de prevenir accesos no autorizados.
- b. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe asegurar que la red de invitados no tenga conexión directa a los servidores a fin de evitar afectaciones a la seguridad de la información.
- c. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC deberá definir un esquema de separación de las redes y de los dominios lógicos, teniendo en cuenta los servicios de información, usuarios, aplicaciones y las especificaciones dadas por los líderes de la información, siempre en cumplimiento de la Políticas de Control de Acceso, Uso Aceptable de los Activos de información y los principios de construcción de Sistemas Seguros.
- d. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe sincronizar los relojes de todos los sistemas con una única fuente de referencia de tiempo como la hora legal colombiana (<http://horalegal.inm.gov.co/>), para asegurar la exactitud de todos los registros de auditoría, que puedan ser necesarios.
- e. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC será responsable de verificar que se utilicen arquitecturas de enrutamiento que limiten el acceso remoto a los puntos críticos de la red. Los controles de direccionamiento de red deberán utilizar técnicas de verificación para establecer correctamente las direcciones fuente y destino.

- f. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe establecer el seguimiento continuo de los permisos de acceso validando la rotación que se pueda presentar de Servidores(as) y Contratistas, además, el monitoreo a los canales dispuestos por la entidad y el aseguramiento de los procesos de autenticación.
- g. La red WIFI UBPD y la red LAN es para uso exclusivo de los equipos institucionales tales como equipos de cómputo, celulares, IPAD, entre otros.
- h. Para los equipos personales que necesiten realizar conexión a la red WIFI, se les asignará la red de invitados y deberán cumplir con las políticas de seguridad para equipos de cómputo (línea base de seguridad).

### Responsables

Oficina de Tecnologías de la Información y Comunicaciones (Implementación)  
Servidora(e)s y contratistas (Cumplimiento)  
Secretaría General – Contratos (Apoyo en el Cumplimiento)

## 8.11. Controles de Uso de Internet

**8.11.1. Objetivo:** Gestionar el acceso y uso del servicio de internet por parte de lo(a)s servidore(a)s, contratistas, terceros e invitados de la UBPD, prestando un servicio adecuado del internet y servicios relacionados de acuerdo con las necesidades de la entidad estableciendo controles que permitan mitigar la materialización de los riesgos asociados a su uso.

### 8.11.2. Lineamientos

- a. El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en cada una de las dependencias de la UBPD. Es responsabilidad de cada miembro de la Entidad utilizar los servicios de conexión a Internet de forma productiva y eficiente para la entidad.
- b. La Unidad en cabeza de la Oficina de Tecnologías de la Información y las Comunicaciones- OTIC, define las políticas, restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.
- c. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC implementa los controles necesarios, de acuerdo con los perfiles de uso establecidos en el **Lineamiento de navegación web** entre la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC y el (la) Oficial de Seguridad de la Información. Los accesos se otorgan de acuerdo con el cumplimiento de las funciones, obligaciones y/o cargo de los servidore(a)s o contratistas con la entidad. Lo anterior, con el fin de mitigar los riesgos inherentes al uso de internet, que incrementan los riesgos y vulnerabilidades de la información.

- d. Los usos diferentes a los necesarios para el cumplimiento de las funciones de la Entidad son de entera responsabilidad de lo(a)s servidore(a)s, contratistas, y terceros de la UBPD al que se le asigna la cuenta de acceso al servicio, y el uso no adecuado se considera una violación a la política de seguridad de la información. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC implementa los mecanismos necesarios que soporten el uso seguro de internet haciendo uso de herramientas especializadas, que permitan analizar y registrar de manera detallada el tráfico desde y hacia la entidad, si así se requiere, esto sin vulnerar el derecho a la intimidad y privacidad de lo(a)s servidore(a)s y contratistas.
- e. El acceso a sitios Web o la instalación de aplicaciones para intentar evadir los controles y políticas de seguridad de navegación están totalmente prohibidos y su detección será tratada como un incidente de seguridad.
- f. Descargar archivos provenientes de Internet implica un riesgo para la seguridad de la información por lo cual se solicita que únicamente se haga cuando sea necesario; está prohibido la descarga de archivos con extensiones de tipo .exe, .bat, .prg, .bak, pig, entre otros.
- g. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC se reserva el derecho a monitorear, hacer seguimiento, auditoría y de guardar registro de todos los sitios que se ingresan a través de la red de la Unidad (no lo que se hace en estos), lo que permite a esta Oficina hacer un seguimiento completo de todos los sitios de Internet a los cuales se acceden y definir las restricciones pertinentes, así como las posibles sanciones.
- h. Lo(a)s servidore(a)s, contratistas, y terceros e invitados de la UBPD no podrán utilizar el servicio de internet para el envío, descarga o visualización de información con contenidos restringidos o que atenten contra la integridad moral de las personas o instituciones, o que esté protegida por derechos de autor o que pongan en riesgo la seguridad y reputación de la Entidad, el uso del servicio para actividades comerciales particulares, el acceso a sitios de entretenimiento online, el acceso a sitios Web considerados como ilegales por la normatividad colombiana, incluidos en la Ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.
- i. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC definirá el navegador que será utilizado por lo(a)s servidore(a)s y contratistas en los computadores de la entidad, así como, los controles que permitan garantizar una utilización segura del servicio.
- j. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC verifica y emite concepto sobre la viabilidad o no de habilitar las páginas, servicios o aplicativos webs que se encuentren bloqueados atendiendo el resultado del análisis de seguridad y los criterios establecidos en el lineamiento de navegación web de la UBPD, dichas solicitudes deben ser realizadas a través de la mesa de servicio de acuerdo con los ANS internos y/o procedimientos definidos por la OTIC. La Entidad se reserva el derecho de suspender dichos servicios de acuerdo con situaciones de riesgo identificadas o reportadas a la Oficina de Tecnologías de Información y las Comunicaciones.

- k. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC realiza el monitoreo del origen de las conexiones al servicio de correo electrónico y VPN bloqueando las conexiones que considere sospechosas realizadas desde otros países.
- l. Los usuarios del servicio de internet son responsables de evitar prácticas o usos que comprometan la seguridad de la información de la entidad, tales como descargas de software no autorizado.

### **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones (implementación)  
Oficial de Seguridad de la Información (Apoyo en la implementación)  
Servidora(e)s y contratistas (Cumplimiento)

## **8.12. Control Copias de Seguridad**

**8.12.1. Objetivo:** Establecer las líneas de control generales para la realización, almacenamiento y recuperación de las copias de seguridad de la infraestructura tecnológica y/o Sistemas de Información de la UBPD.

### **8.12.2. Lineamientos**

- a. La Oficina de Tecnologías de Información y las comunicaciones debe asegurar que se realice las copias de respaldo de la información de la Entidad almacenada en los sistemas de Información, servidores, bases de datos, entre otros.
- b. La Oficina de Tecnologías de Información y las comunicaciones en coordinación con los líderes o custodios de la información define la prioridad para efectuar respaldos de los activos de información, estableciendo el plan de copias de seguridad para los mismos, esta periodicidad de ejecución de las copias de respaldo se establece con base en la naturaleza, el tipo y la clasificación del activo, tipo de backup, tamaño, tiempo objetivo de recuperación, punto objetivo de recuperación, tiempo de retención; también se tiene en cuenta la clasificación establecida en la valoración de infraestructura crítica. Estos deben quedar especificados en el plan de copias de seguridad de acuerdo con lo establecido en el procedimiento de copias de respaldo.
- c. Anualmente se debe establecer y desarrollar plan de pruebas de copias de seguridad para realizar restauraciones periódicas de la data o parte de ella (al menos una vez al año), con el fin de verificar el correcto funcionamiento de las copias de respaldo por parte de la OTIC y solicitar el acompañamiento del líder de la información para validar la información restaurada.
- d. La Oficina de Tecnologías de Información y las Comunicaciones-OTIC, de acuerdo con su capacidad tecnológica registra los activos de información a respaldar, la periodicidad, las rutas, los tiempos de retención entre otros, en el plan de copias de seguridad, por lo cual se excluye la ejecución de copias de seguridad de la información almacenada localmente en computadores de escritorio, portátiles, celulares o Ipad.

- e. Es responsabilidad de los servidores y/o contratistas almacenar la información en los repositorios definidos por la Oficina de Tecnologías de Información y las Comunicaciones-OTIC y solo la información alojada en estos repositorios será respaldada. Para los equipos de los usuarios, solo se realizará sincronización de las carpetas “Mis documentos”, “Descargas” e “Imágenes”, de acuerdo a las políticas definidas por la OTIC a través de Mesa de servicio.
- f. La Oficina de Tecnologías de Información y las Comunicaciones-OTIC no hace entrega de copias de seguridad de la información generada, almacenada o a la que tenga acceso el (la) servidor(a) o el contratista cuando éste concluya su vínculo con la entidad debido a la sensibilidad de esta y con el fin de mantener la confidencialidad de la información tratada en la UBPD; en caso de requerir acceso a información por parte del ex servidor o ex contratista en el marco de algún proceso disciplinario, penal, administrativo o de responsabilidad fiscal, la entidad realizará la entrega de dicha información previa solicitud.
- g. Las copias de seguridad realizadas por la Oficina de Tecnologías de Información y las Comunicaciones deben ser almacenadas en un lugar externo diferente a la ubicación principal del sistema de información o plataforma tecnológica, este lugar debe cumplir con las medidas de seguridad para el acceso físico, lógico y de almacenamiento.
- h. Las copias de seguridad almacenadas en dispositivos de almacenamiento externo deben estar cifradas por hardware o software para evitar el acceso no autorizado.
- i. Los medios de respaldo removibles deben ser trasladados únicamente por personal autorizado por el Jefe de la Oficina de Tecnologías de Información y las Comunicaciones-OTIC a un lugar externo que garantice la integridad, la fiabilidad, seguridad y disponibilidad de estos.

### **Responsables**

Oficina de Tecnologías de la Información y las Comunicaciones-OTIC (Implementación)  
Servidora(e)s y contratistas (cumplimiento).

### **8.13. Desarrollo Seguro**

**8.13.1. Objetivo:** Establecer las líneas de control que permitan garantizar el diseño e implementación de la seguridad en todas las fases del ciclo de vida en el desarrollo de software y sistemas de información.

### **8.13.2. Lineamientos**

- a. Los (las) servidore(a)s y contratistas que realicen actividades del ciclo de vida de desarrollo de software, deben tener entrenamiento básico en seguridad de la información y privacidad, y deben conocer la Política General de Seguridad de la Información de la UBPD.
- b. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC debe asegurar que se diseñen e implementen los requerimientos de seguridad en el software, ya sea

desarrollado o adquirido, que incluya controles de autenticación, autorización y auditoría de usuarios, verificación de los datos de entrada y salida, y que implemente buenas prácticas de desarrollo seguro.

- c. La especificación de los requisitos de seguridad de la información para nuevos desarrollos y sistemas de información se deben realizar en la etapa de levantamiento de requerimientos, estos serán identificados de acuerdo con los protocolos, guías y lineamientos establecidos en la Política de Seguridad de la Información y la guía de desarrollo seguro GTI-GU-006.
- d. Los requerimientos de seguridad de la información identificados deben considerar los posibles riesgos, a fin de establecer los mecanismos de seguridad digital, que apliquen para el caso de: software a la medida, software de terceros o desarrollos propios.
- e. Durante el desarrollo del código para software específico o sistemas de información, se deben establecer revisiones de código estático, permitiendo tener un mejor nivel de seguridad, evidenciando tempranamente problemas del software o sistema de información, esta actividad debe ejecutarse previo a la puesta en producción.
- f. El software desarrollado por servidore(a)s de la Unidad debe contar con una herramienta para el control de versiones que permita a los desarrolladores llevar el control de versiones del software desarrollado.
- g. Los contratos establecidos para el desarrollo de software por parte de contratistas de la UBPD o contratados con terceros deben especificar los acuerdos sobre propiedad, entrega y custodia del código fuente y sus respectivas versiones, documentación técnica y de uso del software o sistema de información, derechos de propiedad intelectual, soportes del desarrollo de las actividades establecidas en la presente política.
- h. El software desarrollado por servidore(a)s de la Unidad, en el ejercicio de sus funciones, se entiende propiedad de la entidad quien tendrá los derechos de autor y propiedad intelectual y éste deberá ser documentado, almacenado y controlado de acuerdo con los procedimientos establecidos en el Proceso de Gestión de Tecnologías de la Información y las Comunicaciones.
- i. La información que se encuentra en los sistemas de producción no puede ser disminuida en los niveles de protección, por tanto, para procesos de desarrollo y pruebas, se debe evitar el uso de datos de producción y en caso de ser necesario su utilización, garantizar la eliminación segura al momento de finalización de las pruebas.
- j. Una vez concluido el desarrollo del software o sistema de información se deben ejecutar pruebas de seguridad que permitan establecer el cumplimiento de los requisitos de seguridad identificados, la eficacia de los controles implementados para los posibles riesgos, y la búsqueda de posibles vulnerabilidades de acuerdo a lo establecido en la guía de desarrollo seguro, esta actividad debe ejecutarse previo a la puesta en producción, como resultado el equipo de Seguridad Digital genera el informe correspondiente.

- k. Los equipos de cómputo, servidores, dispositivos móviles, aplicaciones, entre otros utilizados durante el desarrollo y/o pruebas de software deben estar en un segmento de red independiente en el cual no se tenga acceso a los servidores en el ambiente de producción para lo cual la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC implementa los controles necesarios.
- l. Las actividades realizadas por las (los) servidora (e)s y/o contratistas que efectúen labores de desarrollo de software pueden ser monitoreadas y/o auditadas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, para preservar la seguridad de los ambientes de prueba y productivos. En caso de detectarse comportamientos sospechosos o anómalos, estos serán tratados como un incidente de seguridad de la información.
- m. El software utilizado o necesario durante el ciclo de vida de desarrollo debe ser validado por seguridad digital de acuerdo con lo establecido en el procedimiento de solicitud de servicios de seguridad digital, adicionalmente, las herramientas de desarrollo y los componentes de cada sistema de información deben estar actualizados con todos los parches generados para las versiones en uso y se debe verificar que se estén ejecutando la última versión aprobada del sistema.
- n. Las actividades ejecutadas por las (los) servidora€s y/o contratistas que efectúen labores de desarrollo de software a los cuales se le asigne usuarios con permisos de administrador son de su total responsabilidad. En caso de detectarse comportamientos sospechosos o anómalos, estos serán tratados como un incidente de seguridad de la información.
- o. Los cambios de software se realizarán siempre en el ambiente de pruebas dispuesto por la Entidad. Una vez superada la etapa de pruebas, la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC documenta y coordina el paso a producción, previa presentación y aprobación por parte de la mesa de control de cambios.
- p. Si los nuevos desarrollos son adquiridos a través de terceros, se deberá seguir un proceso formal de adquisición. Los contratos con los proveedores tendrán incluidos los requisitos de seguridad de la información y la puesta en producción se realizará previa aprobación de la mesa de control de cambios.
- q. Todo desarrollo de software realizado en la UBPD debe ser autorizado por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC en cabeza del líder de desarrollo y debe estar asociado al Plan de Acción y/o al Plan Estratégico de Tecnologías de la Información – PETI

## **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones (Implementación)

Servidora (e)s y contratistas que ejecutan actividades de desarrollo de software (Implementación)

## 8.14. Políticas de Seguridad para la Gestión de Proyectos

**8.14.1. Objetivo:** Establecer lineamientos en temas de seguridad de la información, para la gestión de proyectos que surgen tanto de iniciativas de OTIC como los asignados por las diferentes áreas de la UBPD.

### 8.14.2. Lineamientos

- a. La Entidad debe enmarcar cada proyecto bajo un estándar de buenas prácticas en seguridad de la información, donde se definan las herramientas, insumos y procesos para el ciclo de vida de cada proyecto definido.
- b. Se debe integrar la seguridad de la información en la gestión de proyectos independiente de su naturaleza, para asegurar que los riesgos de seguridad de la información se identifiquen y traten como parte del proyecto.
- c. Cada proyecto que involucre servicios tecnológicos debe contar como mínimo con un líder técnico, un gerente de proyecto y un líder funcional asignado por el área misional o de apoyo, con el fin de definir roles y responsabilidades en busca de la protección de la información.
- d. En cada proyecto se deben establecer los compromisos de confidencialidad donde se establecen las condiciones bajo las cuales se tratará la información involucrada en el proyecto, de modo que se restrinja su uso y se salvaguarde la confidencialidad e integridad de esta.
- e. Cada proyecto debe velar por que los objetivos del proyecto no vayan en contravía de la Política General de Seguridad de la Información.
- f. Se debe gestionar la matriz de riesgos, la cual incluye los riesgos de seguridad de la información, seguridad digital y ciberseguridad, durante todo el ciclo de vida del proyecto, garantizando el seguimiento y actualización constante de los riesgos.
- g. Antes de la salida a producción de los productos o servicios tecnológicos que entregará el proyecto deben realizarse actividades de análisis de vulnerabilidades, definición de aprovisionamiento y autorización de acceso, entre otros, asegurando que la arquitectura y el diseño de los sistemas operativos y de información estén protegidos contra amenazas conocidas basadas en el entorno operativo.

### Responsables

Oficina de Tecnologías de la Información y Comunicaciones (Implementación)

Lo(a)s servidore(a)s y contratistas (Cumplimiento)

## 8.15. Relación con Proveedores y terceros

**8.15.1. Objetivo:** Establecer las medidas de seguridad para los activos de información a los que pueden acceder, administrar o suministrar a la UBPD los proveedores, a través

de la adopción de controles que minimicen la vulnerabilidad de la confidencialidad, integridad y disponibilidad.

### 8.15.2. Lineamientos

- a. Dentro de los acuerdos, contratos o convenios firmados entre la UBPD y los proveedores se deben definir claramente los requerimientos de seguridad de la información y protección digital.
- b. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC es responsable de incluir en los contratos que tiene bajo su responsabilidad, condiciones en las cuales se establezcan y acuerden los requisitos de seguridad de protección y seguridad de la información relacionadas con el bien o servicio a contratar y de igual forma garantizar los acuerdos de nivel de servicio -ANS- requeridos.
- c. Para otorgar el acceso a los activos de información de la UBPD a un proveedor, se debe tener en cuenta el nivel de clasificación al cual se concederá el permiso, administración, uso o tratamiento para establecer los controles de seguridad apropiados; esto, previo a la firma del compromiso de Confidencialidad y demás requisitos que considere la Política General de Seguridad de la Información.
- d. Los proveedores deben conocer y cumplir las políticas, procedimientos, lineamientos y demás directrices relacionadas a la protección y seguridad de la información de la UBPD que sea inherente a la actividad que va a realizar.
- e. El personal del proveedor o aliados que realicen actividades para la UBPD y tenga acceso a la información y/o a los sistemas de información debe tener firmados los respectivos compromisos de confidencialidad
- f. La UBPD podrá realizar pruebas de análisis de vulnerabilidades o Ethical Hacking en los casos que aplique a los activos de información administrados y/o suministrados a la UBPD por terceros.
- g. El o los proveedores deben suministrar la información solicitada por la UBPD en los términos y condiciones que la entidad requiera sin que se pueda oponer reserva o confidencialidad alguna tratándose de información de la entidad o asociado a la ejecución de sus actividades contractuales.
- h. El proveedor debe apoyar o desarrollar las actividades de remediación de vulnerabilidades o de tratamientos de riesgos asociados a los activos de información que administra o provee a la entidad, de acuerdo con las alertas o resultados de ejercicio de Ethical Hacking desarrollados por la UBPD.
- i. Cuando haya cambio de proveedor o de tecnología suministrada por el proveedor se debe garantizar la devolución de la información y se debe aplicar el borrado seguro de la información, para garantizar que no haya fuga de esta.

## Responsables

Oficina de Tecnologías de la Información y las Comunicaciones-OTIC (Implementación)

Secretaria General – Grupo interno de Contratos (apoyo a la implementación)

Proveedores y terceros (Implementación)

### 8.16. Protección y Seguridad Digital para el Intercambio o acceso de Información

**8.16.1. Objetivo:** Establecer las medidas necesarias y suficientes que garanticen el intercambio de información de forma segura a través de entornos tecnológicos.

#### 8.16.2. Lineamientos

- a. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC establece los estándares tecnológicos de los canales o medios autorizados para el intercambio o acceso de información en formato electrónico.
- b. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC diseña e implementa los controles necesarios para proteger el intercambio o acceso de información a través de los servicios digitales (correo electrónico, VPN, USB y discos cifrados) contra interceptación, copiado, modificación, enrutado y destrucción.
- c. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC establece las herramientas para el uso de técnicas criptográficas, en canales de comunicación, servidores, sistemas de información, dispositivos de almacenamiento externo.
- d. Los acuerdos de intercambio o acceso de información con otras entidades, organizaciones o sociedad civil, que sean gestionados por las diferentes áreas de la UBPD, deberán incorporar en el acuerdo, los estándares tecnológicos establecidos para el intercambio o acceso seguro de información.
- e. Los intercambios o accesos de información a través de medios tecnológicos deben realizarse mediante las herramientas establecidas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, en caso de que deban realizarse por otro medio se debe solicitar el acompañamiento a la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC con el fin identificar los riesgos asociados y establecer controles de seguridad si fuera posible.
- f. La información compartida con externos a través de la nube autorizada y/o soluciones similares debe ser aprobada por el jefe inmediato del solicitante y el Oficial de Seguridad de la Información. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC establecerá el medio más seguro para compartir información, el tiempo que estará habilitado y los controles que se deberán aplicar, los cuales serán definidos por el Experto Técnico encargado de Seguridad Digital.
- g. La información se podrá transferir a terceros en los casos señalados en el Decreto Ley 589 de 2017, de acuerdo con la clasificación establecida en el inventario de activos de

información y en los casos autorizados por los Directores, Subdirectores, Jefes de Oficina o Coordinadores lo requieran.

- h. Las memorias USB cifradas deben ser usadas para almacenar y/o transportar información de manera temporal y esta debe ser borrada de manera segura una vez sea transferida a su repositorio de almacenamiento definitivo.

### **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)

Subdirección General Técnica y Territorial (Apoyo en la implementación)

Secretaría General (Apoyo en la implementación)

Servidore(a)s y contratistas (informados)

## **8.17. Servicios en la Nube**

**8.17.1. Objetivo:** Establecer medidas de seguridad digital para los sistemas de información, servicios e infraestructura, de los que hace uso la UBPD, que se encuentren alojados en plataformas de computación en la nube.

### **8.17.2. Lineamientos**

- a. La administración de la nube es responsabilidad de la Oficina de Tecnologías de la Información y las comunicaciones–OTIC, teniendo en cuenta:
  - i. Contar con acuerdo de confidencialidad con el proveedor.
  - ii. Contar con acuerdos de niveles de servicio con un 99.5% como mínimo.
  - iii. Contar con un procedimiento de gestión de usuarios de la nube. Estos usuarios deben ser autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones–OTIC y/o el líder de la información.
  - iv. Los canales de conexión a la nube deben ser seguros, usar protocolos que permitan la encriptación de las comunicaciones entre el navegador y el servidor web
  - v. Se debe realizar una autenticación segura.
  - vi. Se debe contar con contraseñas robustas de acceso a la nube.
  - vii. Establecer una gestión de capacidad y de disponibilidad de la nube.
  - viii. La información sensible debe ser cifrada
  - ix. Debe contar con medidas preventivas que eviten la denegación del servicio.
- b. Los servicios en la nube (SaaS) contratados directamente por las áreas deben ser aprobados por la Oficina de Tecnologías de la información y las Comunicaciones y deben cumplir las medidas de seguridad establecidas anteriormente.
- c. Para seleccionar el uso de servicios en la nube, se deben identificar y valorar los riesgos asociados a dicho servicio, según la información a gestionarse y clasificación de los activos de información de la UBPD.

- d. Establecer las responsabilidades tanto del proveedor del servicio como de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC y del área o proceso que hacen uso del servicio, cuando sea necesario.
- e. Se deben establecer mecanismos de autenticación, autorización y registro para cada una de las actividades realizadas sobre el almacenamiento en la nube.
- f. El acceso y uso de los servicios, información o sistemas de información en la nube debe ser acorde a la Política General de Seguridad de la Información, lineamientos, conceptos y/o directrices asociadas.
- g. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC es responsable de establecer los medios de acceso, los dispositivos que tienen acceso, las ubicaciones desde las cuales se puede acceder a los servicios en la nube.
- h. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC es responsable de respaldar la información almacenada en la nube.
- i. Lo(a)s servidore(a)s, contratistas de la UBPD son responsables del otorgamiento de accesos y permisos a las carpetas que compartan desde la nube de almacenamiento institucional a otras personas de la entidad y/o externos.
- j. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC administra los accesos a los repositorios ubicados en la nube, para los desarrollos.
- k. Las descargas de información de la nube en equipos personales no autorizados por parte de servidores y/o contratistas será tratado como un incidente de seguridad de la información.

### **Responsables**

Oficina de Tecnologías de la Información y las Comunicaciones-OTIC (Implementación)

Proveedores y terceros (Apoyo en la Implementación)

Lo(a)s servidore(a)s y contratistas (Cumplimiento)

## **8.18. Uso de Dispositivos de Almacenamiento Externos**

**8.18.1. Objetivo:** Establecer medidas de protección de los computadores y medios de almacenamiento externos (Memorias USB, Discos duros, Unidades de CD, Memorias MicroSD, entre otros), institucionales o personales autorizados en el desarrollo de las funciones de las diferentes áreas de la UBPD.

### **8.18.2. Lineamientos**

- a. Los (as) servidore(a)s y contratistas de la UBPD que requieran hacer uso de medios de almacenamiento externos (asignados por la entidad o recibidos) en los computadores

portátiles o de escritorio dispuestos por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, deben aplicar los lineamientos, mecanismos, estándares y controles establecidos en los protocolos, guías o lineamientos enfocados a proteger y asegurar los computadores portátiles o de escritorio.

- b. El uso de dispositivos de almacenamiento externo personal de los(as) servidore(a)s y contratistas de la UBPD, está permitido en modo lectura únicamente para las dependencias misionales, para las demás dependencias podrá ser habilitado en modo de solo lectura, con el aval del Jefe(a) de la dependencia y/o supervisor de contrato, con la justificación y tiempo de uso. Esta solicitud debe realizarse en la herramienta de mesa de servicio y deberá contar con la aprobación de la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC. En caso de requerirse que se habilite en modo escritura deberá contar con la aprobación del Oficial de Seguridad de la Información; el modo de escritura está restringido por protección de fuga de información.
- c. Los(as) servidore(a)s y contratistas de la UBPD, que tengan asignados dispositivos de almacenamiento externo, de uso personal autorizados o recibidos de otras entidades, organizaciones y/o personas que contienen información para el cumplimiento de la misión de la UBPD y que han sido utilizados en equipos de cómputo fuera de la entidad, deben realizar el análisis con las herramientas de prevención dispuestas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC para identificar posibles amenazas y así reducir daños, pérdidas o fugas de información a la infraestructura tecnológica de la UBPD.
- d. La instalación, configuración y activación de dispositivos de almacenamiento externo (asignados o personales), estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC, previa autorización del jefe (a) de la dependencia, las solicitudes se atenderán a través de la mesa de servicio y se comunicará a(l) o (la) Oficial de Seguridad de la Información.
- e. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC implementará las restricciones o mecanismos necesarios para llevar trazabilidad y control de los medios de almacenamiento externos (asignados o personales) conectados a los computadores portátiles o de escritorio propiedad de la UBPD, de acuerdo con los perfiles establecidos y los protocolos, guías o lineamientos, lo cual se comunicará y pondrá en conocimiento de(l) o (la) Oficial de Seguridad de la Información.
- f. Los(as) servidore(a)s y contratistas de la UBPD y terceros deben usar siempre las memorias o discos cifrados de la entidad.
- g. La custodia y el manejo de la información almacenada en dispositivos de almacenamiento externos es responsabilidad del servidor, servidora, contratista, el cual debe velar por su protección para evitar fugas y/o pérdidas de información. En caso de comprometerse información de la entidad almacenada en dispositivos de almacenamiento externos (asignados o personales) será tratado como un incidente de Seguridad de la Información.

- h. Los dispositivos de almacenamiento externo deben permanecer en las instalaciones de la entidad, excepto cuando sea necesario retirarlos de estas para ser utilizados en actividades inherentes al desarrollo de las funciones, como en comisiones, reuniones externas, eventos, trabajo Seguro a Distancia o en casa o cualquier otra actividad de este tipo que esté autorizada, y deben retornar a las instalaciones en el menor tiempo posible una vez culminada dicha actividad.
- i. Los dispositivos de almacenamiento externo son para almacenamiento temporal de información (excepto los usados para almacenar copias de respaldo), una vez transferida a la ubicación de almacenamiento definitivo deben ser borrados de manera segura.

### **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)

Servidoras y contratistas (Cumplimiento)

Jefe o la Jefa de la dependencia (Cumplimiento)

Oficial de Seguridad de la Información (Apoyo en la implementación)

## **8.19. Uso de Correo Electrónico**

**8.19.1. Objetivo:** Establecer e implementar medidas y controles para el uso seguro del servicio de correo electrónico.

### **8.19.2. Lineamientos**

- a. Los correos electrónicos serán considerados parte de los registros de la Entidad y conforme a esto están sujetos a ser almacenados, monitoreados y auditados en los casos permitidos por la ley.
- b. El servicio de correo electrónico debe utilizarse exclusivamente para las actividades propias de la función desarrollada en la UBPD. Cualquier uso diferente al cumplimiento de las funciones u obligaciones con la entidad se consideran una violación a la Política General de Seguridad de la Información por parte de lo(a)s servidore(a)s y contratistas de la UBPD al que se le asigna la cuenta de correo electrónico.
- c. El único correo electrónico autorizado para el manejo de información institucional es el asignado con el dominio @ubpdbusquedadesaparecidos.co, este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.
- d. Está permitido enviar correos a máximo 50 destinatarios, y se debe utilizar el campo CCO (con copia oculta) para mantener la confidencialidad de las cuentas a las que se dirige la comunicación.
- e. El envío de correos masivos está restringido, únicamente será permitida esta actividad por las cuentas designadas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC para esta labor.

- f. Las cuentas de correo electrónico oficiales de la UBPD son las establecidas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC. Los servidores(as), contratistas y terceros de la UBPD, que utilicen otras cuentas de correo para la gestión de sus labores en la UBPD, reconoce y acepta que los incidentes de seguridad de la información generados por el uso de servicios de cuentas de correo electrónico no autorizadas serán de su entera responsabilidad y serán considerados una violación a la política de seguridad de la Información.
- g. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC podrá restringir el acceso a plataformas de correo distintas a la plataforma oficial de correo de la UBPD, con el fin de mitigar los riesgos de fuga o pérdida de información y descarga de software malicioso.
- h. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC se reserva el derecho de filtrar, de manera automática, los tipos de archivo que vengan anexos al correo electrónico para evitar amenazas de virus y otros programas destructivos. Todos los mensajes electrónicos serán analizados por las herramientas de protección definidas para tal fin.
- i. La configuración de acceso a la cuenta de correo desde medios distintos a los asignados por la UBPD debe ser validado y monitoreado periódicamente por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.
- j. No se debe usar el servicio de correo electrónico de la UBPD para el envío o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, que promuevan la discriminación sobre la base de raza, color, pertenencia étnica, origen nacional o social, género, edad, estado marital, orientación sexual, religión o discapacidad, opiniones políticas o de otra índole, posición económica, nacimiento o cualquier otra condición social, o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales o cualquier contenido que represente riesgos para la seguridad de la información.
- k. Lo(a)s servidore(a)s y contratistas de la UBPD deben verificar y reportar los correos sobre los que se dude de su origen, remitente o contenido o se consideren sospechosos a la mesa de servicio, este será tratado como evento de seguridad y deberá clasificarlo como inseguro en el servicio de correo electrónico.
- l. Lo(a)s servidore(a)s y contratistas de la UBPD no deben suministrar los datos de acceso o clave de la cuenta de correo asignada por la entidad. Si se sospecha que esta clave es conocida debe ser cambiada inmediatamente y reportada como un incidente de seguridad de la información.

### **Responsables**

Oficina de Tecnologías de la Información y Comunicaciones-OTIC (Implementación)  
Servidora(e)s y contratistas (Implementación).

## 8.20. Fortalecimiento de la Infraestructura de Seguridad Digital

**8.20.1. Objetivo:** Implementar herramientas tecnológicas que permitan gestionar controles preventivos y detectivos para mitigar los riesgos de seguridad de la información.

### 8.20.2. Lineamientos

- a. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC evalúa la necesidad de adquirir, implementar o actualizar las herramientas que permitan gestionar de manera adecuada los controles de seguridad digital.
- b. Lo(a)s servidore(a)s y contratistas de la UBPD deben usar las herramientas de seguridad digital implementadas o autorizadas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.
- c. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC diseña e implementa el GTI-PL-002 Plan de recuperación de Desastres (DRP) orientado al restablecimiento de los sistemas, servicios, comunicaciones e infraestructura tecnológica de la UBPD, que le permitan continuar con su funcionamiento en caso de presentarse un incidente que amerite su ejecución.
- d. El GTI-PL-002 Plan de Recuperación de Desastres debe ser probado por lo menos una vez al año, para validar que aún siga vigente.
- e. Cada vez que se realicen cambios en las aplicaciones o sistemas de información críticos, se debe tener en cuenta su modificación o inclusión en el F y/o DRP para que no vaya a afectar la disponibilidad de los servicios.
- f. Cada vez que se construya, actualice, pruebe o se ponga en activación el GTI-PL-002 Plan de Recuperación de Desastres DRP, se deberá contemplar la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos, y deberá ser probado con el escenario que simule la materialización de un ataque cibernético.
- g. Se deben implementar las plantillas base y de aseguramiento definidas por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC a sistemas, servicios, equipos de cómputo, servidores, comunicaciones e infraestructura tecnológica de la UBPD de acuerdo con lo establecido en la guía de línea base y aseguramiento de infraestructura tecnológica.
- h. Lo(a)s servidores y contratistas de la UBPD deben hacer uso de los equipos de cómputo institucionales asignados por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC para el acceso, almacenamiento y uso de los sistemas de información, aplicaciones, servicios e información de la UBPD. El acceso, uso y/o almacenamiento de información en equipos personales implica que la custodia, protección, licenciamiento de herramientas tecnológicas que permitan preservar la confidencialidad, integridad y disponibilidad de la información sea responsabilidad del (la) servidor(a)y contratista, así como la materialización de riesgos asociados al uso de estos.

- i. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC establece las Estrategias de seguridad digital para la implementación, gestión y seguimiento de los lineamientos establecidos en la Política General de Seguridad de la Información y demás lineamientos para proteger la infraestructura tecnológica, Sistemas de información, servicios e información de la UBPD.
- j. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC establece las estrategias de ciber resiliencia para poder resistir o responder a ataques o interrupciones imprevistas mediante la gestión, protección, detección e identificación, respuesta y recuperación de amenazas cibernéticas.
- k. Todas las adquisiciones de bienes y/o servicios tecnológicos deben contar con la revisión y/o validación de la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC con el fin de garantizar la inclusión de características asociadas a la preservación de la confidencialidad, integridad y disponibilidad de la información y los entornos digitales.

### **Responsables**

Oficina de Tecnologías de la Información y las Comunicaciones-OTIC (Implementación)  
Dirección General (Apoyo a la Implementación)  
Oficina Asesora de Planeación (Apoyo a la Implementación)  
Secretaría General (Apoyo a la Implementación)  
Servidora(e)s y contratistas (Cumplimiento)

## **8.21. Control para el Trabajo Seguro a Distancia o en casa**

**8.21.1. Objetivo:** Establecer e implementar las medidas mínimas de seguridad de la Información que se deben seguir en el desarrollo de actividades laborales en la modalidad de trabajo remoto.

### **8.21.2. Lineamientos**

- a. Los(as) servidores (as), contratistas deben cumplir con todos los lineamientos establecidos en esta política cuando se esté realizando trabajo seguro a distancia o en casa.
- b. Los equipos personales que se autoricen para el trabajo seguro a distancia o en casa deben ser autorizados por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC cumpliendo como mínimo con los siguientes requisitos:
  - Control de acceso al usuario mediante contraseña o reconocimiento de huella.
  - Tener instalada y actualizada una herramienta de antivirus.
  - Usuario independiente para el manejo de información de la UBPD.
  - Software instalado licenciado en el equipo (Si aplica)
  - Sistema Operativo actualizado

- c. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC implementa controles que permitan la verificación de cumplimiento de condiciones mínimas de seguridad establecidas en el numeral b.
- d. Cuando sea posible la conexión remota a los Sistemas de Información de la UBPD debe realizarse mediante VPN.
- e. Las descargas de información de la UBPD en equipos personales no autorizados por parte de servidores y/o contratistas será tratado como un incidente de seguridad de la información.
- f. En los computadores o dispositivos móviles usados para realizar trabajo remoto no se debe guardar usuarios y contraseñas para conexión a los sistemas de información, correo electrónico, almacenamiento en nube entre otros.
- g. Las conexiones remotas solicitadas por lo(a)s Servidore(a)s, contratistas y proveedores deben ser aprobadas por el jefe inmediato o el supervisor del contrato según aplique especificando los servicios, aplicaciones, servidores tecnológicos, entre otros y el tiempo de conexión requerido, en los formatos establecidos por la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC.
- h. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC monitorea las conexiones remotas a fin de verificar el buen uso y detectar posibles eventos de seguridad, pudiendo bloquear la conexión ante comportamientos anómalos o sospechosos.

### **Responsables**

Subdirección de Gestión Humana (Implementación)

Oficina de Tecnologías de la Información y Comunicaciones (Apoyo a la Implementación)

Servidora (e) s, contratistas y proveedores (Cumplimiento)

## **8.22. Seguimiento y Evaluación al Sistema de Seguridad de la Información**

**8.22.1. Objetivo:** Establecer e implementar los mecanismos de seguimiento y monitoreo de la eficacia en la implementación y ejecución de controles derivados de los lineamientos y líneas de Control de esta política.

### **8.22.2. Lineamientos**

- a. La UBPD mide y evalúa la efectividad del SSI, para lo cual determina que requiere ser monitoreado y medido (procesos y controles de la seguridad de información), Los métodos aplicados para monitorear, medir, analizar y evaluarlos, para obtener resultados válidos, cuándo se llevarán a cabo el monitoreo y las mediciones y cuándo se analizarán y evaluarán los resultados del monitoreo y de las mediciones.

- b. La Oficina de Tecnologías de la Información y las Comunicaciones-OTIC y el (la) Oficial de Seguridad de la Información realizan el seguimiento a la implementación de la normatividad (política, manual, y demás lineamientos establecidos), al menos, una vez al año. Esto con el fin de analizar y considerar las distintas dinámicas que se presenten en la entidad, a su vez coordinará en caso de requerirse su actualización.
- c. Se presentará al Comité de Seguridad de la Información o quien haga sus veces, por parte del Oficial de Seguridad de la Información y la Oficina de Tecnologías de la Información y las Comunicaciones-OTIC los resultados del seguimiento del estado de implementación del Sistema de Seguridad de la Información.
- d. La evaluación del cumplimiento de las acciones propuestas en la política, por medio del ejercicio de revisión por la dirección del SSI, se realizará mediante:
  - Seguimiento de efectividad de los controles.
  - Resultado de metas de indicadores
  - Seguimiento al Plan Estratégico de Seguridad de la Información
  - Seguimiento a las estrategias de sensibilización y concientización.
  - Seguimiento a resultados de auditorías internas y/o externas
- e. La Dirección General y los miembros del Comité de Seguridad de la Información o quien haga sus veces, realizan una revisión anual del SSI para garantizar su disponibilidad, adecuación y efectividad.

Esta revisión comprende:

- El estado de las acciones generadas por revisiones de la Dirección previas.
- Cambios significativos internos y externos, relevantes para el SSI.
- El desempeño de la Seguridad de Información en la empresa:
  - No conformidades y acciones correctivas.
  - Resultados de métricas e indicadores.
  - Resultados de auditorías internas y externas.
- Grado de cumplimiento de los objetivos del SSI.
- Retroalimentación de las partes interesadas.
- Los resultados de la Gestión de Riesgos del SGSI y el estado del Plan de Tratamiento de Riesgos.
- Oportunidades de Mejora Continua.

Todos estos elementos son preparados y presentados a la Dirección mediante Informes, y los resultados de la revisión conlleva a la emisión de acciones correctivas y de mejora.

- f. La Oficina de Control Interno OCI en cumplimiento del rol normativo de “Evaluación y Seguimiento” y de sus funciones, desarrolla actividades de auditoría de interna de manera planeada, documentada, organizada y sistemática, con respecto a las metas estratégicas de gran alcance para la Unidad, lo anterior en el marco de los procedimientos “SEC-PR-003 Auditoría Interna”, “SEC-PR-002 Seguimiento y Evaluación” y “SEC-PR-001 Planes de mejora”; Por otro lado y en cuanto a auditorías externas la implementación del Sistema de Seguridad de la Información SSI, la OCI en desarrollo del rol de “enfoque hacia la

Prevención” articulará de forma armónica y colaborativa, actividades de asesoría y acompañamiento orientadas al cumplimiento en la aplicación de los procedimientos y demás documentos internos que apoyan el ejercicio de auditoría interna por parte de auditores externos.

### **Responsables**

Oficina de Tecnologías de la Información y las Comunicaciones-OTIC (implementación)  
Oficial de Seguridad de la Información(implementación)  
Comité de Seguridad de la Información o quien haga sus veces (Seguimiento)  
Oficina Asesora de Planeación (Apoyo en la implementación)

## **9. Uso Aceptable de los activos**

La información, los sistemas, los servicios y los equipos de cómputo de usuarios, redes, Internet, correo electrónico, aplicaciones, impresoras, teléfonos, entre otros, provistos por la UBPD son activos de información y son proporcionados a los usuarios para uso exclusivo del desarrollo de las labores relacionados con los servicios de la Unidad y temas estrictamente relacionados con el cumplimiento de los propósitos de la Entidad.

Los líderes de la información serán responsables de definir el uso aceptable de los activos de información a su cargo de acuerdo con su clasificación. El uso inapropiado de los recursos tecnológicos y de la información constituye un incumplimiento de las normas y políticas de Seguridad y conlleva a la toma de acciones disciplinarias cuando sea necesario.

Todo(a) servidor(a), contratista o tercero de la UBPD, o cualquier persona que tenga una relación contractual con la Unidad, y que en algún momento utilice o tenga acceso a los activos de información de la Entidad, deberá hacer una aceptación expresa de la Declaración de Responsabilidad de acuerdo con lo definido en el instrumento Acta de entrega de bienes de Mesa de servicio, siendo un documento no controlado, sobre el uso de los activos de información, y será responsable por su manejo y el cumplimiento de los requisitos de seguridad de la información, adicional a los descritos a continuación.

En todo caso, los activos de información deberán siempre ser utilizados de forma ética y en cumplimiento de las leyes y reglamentos vigentes.

A continuación, se enumeran algunas recomendaciones que se deben conocer para hacer buen uso de los activos de información asignados.

### **9.1. Inventario de activos**

- El Oficial de Seguridad de la Información deberá propender porque todos los activos de información sean claramente identificados y consolidados en un inventario, y deberá establecer y mantener los lineamientos para este proceso.
- Los líderes de proceso, con la asesoría del Oficial de Seguridad de la Información deberán elaborar y mantener un inventario de activos de información bajo su responsabilidad, aplicando la GSI-GU-002 Guía de Gestión de Activos de Información.

## 9.2. Protección de la confidencialidad

Cada persona que haga uso del activo debe seguir las siguientes instrucciones para preservar la confidencialidad del activo correspondiente:

- Verificar el nivel de clasificación del activo frente a confidencialidad, esto se hace tomando como guía la GTI-FT-045 Matriz de Activos de Información e Índice de Información Clasificada y Reservada.
- El usuario que accede a la información únicamente puede compartir la información con los usuarios que no tengan restricción para hacerlo, de acuerdo con la Política de Control de Acceso y la Política de Protección de Datos Personales. Se debe contar con la autorización expresa del líder de la Información para suministrar o intercambiar información clasificada o reservada a otras personas o a entes externos.
- Todos los servidores(as), contratistas o proveedores de la Unidad están obligados a reportar a la mesa de servicio accesos no autorizados a un activo de información de acuerdo con su clasificación.
- No se permite el uso de software no autorizado o de propiedad de los usuarios en la plataforma tecnológica de la UBPD.

## 9.3. Protección de la integridad

Cada persona que haga uso del activo debe seguir las siguientes instrucciones para preservar la integridad del activo correspondiente:

- Verificar el nivel de clasificación del activo frente a integridad, esto se hace tomando como guía la GTI-FT-045 Matriz de Activos de Información e Índice de Información Clasificada y Reservada.
- El usuario que modifique la información únicamente puede hacerlo, si la Política de Control de Acceso se lo autoriza.
- Todos los servidores(as) de la UBPD están obligados a reportar a la mesa de servicio las modificaciones no autorizadas a un activo de acuerdo con su clasificación y la Política de Control de Acceso.

## 9.4. Protección de la disponibilidad

Cada persona que haga uso del activo debe seguir las siguientes instrucciones para preservar la disponibilidad del activo correspondiente:

- Verificar el nivel de clasificación del activo frente a disponibilidad, esto se hace tomando como guía la GTI-FT-045 Matriz de Activos de Información e Índice de Información Clasificada y Reservada.
- De acuerdo con la clasificación del activo frente a la disponibilidad, el usuario que haga uso del activo debe validar que dicha acción no afecte el nivel de disponibilidad que dicho activo debe ofrecer de acuerdo con el SSI.

- Todos los funcionarios, contratistas o proveedores de la UBPD están obligados a reportar a la mesa de servicio el uso indebido de un activo que pueda afectar el nivel de disponibilidad que debe ofrecer de acuerdo con el SSI.

#### **9.5. Uso de la Información**

- La información reservada sólo debe conocerla el líder de esta o quien este delegue.
- Los(as) servidores(as), contratistas o terceros de la UBPD son responsables de evitar ser víctimas de Ingeniería Social.
- Los tableros y vidrios deben borrarse una vez terminan las reuniones.
- La información privada de los usuarios no debe ser utilizada para fines diferentes a los autorizados.
- La información debe clasificarse y etiquetarse.
- Los(as) servidores(as), contratistas o terceros deberán realizar la devolución formal de los activos de información asignados y/o desarrollados dentro de sus funciones, al finalizar la relación contractual o laboral con la UBPD, o al presentarse un cambio de cargo, rol, área o responsabilidades.
- En caso de requerir uso de carpetas compartidas el usuario debe garantizar el acceso únicamente a personal autorizado con el rol adecuado.

#### **9.6. Protección física**

Los líderes de la información deberán propender porque las especificaciones físicas, técnicas y ambientales necesarias para la adecuada conservación de un activo de información sean cumplidas.

#### **9.7. Uso del Correo Electrónico**

- Está provisto únicamente para propósitos relacionados con el cumplimiento de la misionalidad de la Unidad.
- Está prohibido enviar mensajes ofensivos, difamatorios, obscenos, bromistas, amenazantes, pornográficos, abusivos, entre otros.
- Cuando se ausente de la oficina se debe activar la opción de fuera de oficina indicando quién puede atender los requerimientos.
- Los mensajes de correo con información clasificada o reservada deben viajar cifrados o protegidos con contraseña.
- Nunca se deben actualizar datos a través de correo electrónico, ni solicitar información a través de links incluidos en dichos correos.
- No se debe participar en cadenas, chistes que se reenvían de forma masiva a través de correo electrónico.

#### **9.8. Uso de Internet**

- Se debe respetar los derechos de reproducción, patentes, marcas registradas y todo lo relacionado con derechos de autor.
- No se debe descargar música, vídeos, barras de menú, protectores de pantalla y otros, éstos pueden descargar también software malicioso.
- La publicación de artículos o contenidos de la Entidad y el uso del nombre e imagen de la UBPD en sitios públicos como chats, blogs, redes sociales, entre otros, es realizada únicamente por personal autorizado.
- Se debe asegurar la validez de los sitios web que piden información confidencial como tarjetas de crédito y datos personales, para evitar ser víctimas de phishing.

### 9.9. Dispositivos móviles

- Los usuarios que tengan asignados dispositivos móviles a su cargo (portátiles, tabletas, celulares, entre otros) serán responsables de dar un correcto uso y protección a la información almacenada en estos, manteniendo los controles dispuestos por la OTIC, dando cumplimiento a la Política de dispositivos móviles.

### 9.10. Manejo de medios de almacenamiento externo

- El uso de medios de almacenamiento externo tales como cintas, memorias de almacenamiento, unidades de almacenamiento externo, discos compactos, disco de video digital, entre otros, deberá ser autorizado y controlado por los líderes de la información.
- El uso de dispositivos de almacenamiento externo personal de los(as) servidore(a)s y contratistas de la UBPD, está permitido en modo lectura únicamente para las dependencias que hacen parte de la Secretaría General Técnica y Territorial, para las demás dependencias podrá ser habilitado en modo de solo lectura, con el aval del Jefe(a) de la dependencia o supervisor de contrato, con la justificación y tiempo de uso.
- Solo se permitirán excepciones, expresamente autorizadas por el líder de la información, en los casos en que la capacidad de los medios de almacenamiento compartido o sistemas de intercambio seguro asignada a un servidor(a), contratista o tercero sea claramente insuficiente para la realización de sus labores, o en aquellos casos en los que se requiera su uso como llave criptográfica o token para firma digital.
- Quien autorice la utilización de medios de almacenamiento externo, se hará co-responsable sobre las consecuencias que se deriven de ésta.
- Todo medio de almacenamiento externo deberá ser analizado por el software antimalware previo a su uso en los equipos de la UBPD.
- Los líderes de la información serán los encargados de registrar la salida de medios que contienen información catalogada como pública clasificada, pública reservada.
- En cualquier caso, un servidor(a), contratista o tercero que esté temporalmente autorizado para usar medios de almacenamiento externo, deberá seguir expresamente y de manera obligatoria las políticas de Uso de Dispositivos de Almacenamiento Externos.

### 9.11. Eliminación de medios

- Se deberá asegurar que la información almacenada en medios lógicos o físicos, y que haya dejado de ser útil para la UBPD, sea debidamente eliminada utilizando la opción de borrado seguro con el uso de herramientas destinadas para este fin.
- El(la) servidor(a), contratista 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.
- Los líderes de la información deberán determinar con la asesoría del Oficial de Seguridad de la Información la disposición final de los medios de acuerdo con la clasificación de la información almacenada, incluyendo los métodos apropiados de destrucción de la información cuando aplique.
- Los usuarios serán responsables de utilizar los métodos definidos para la disposición final de la información, acatando los lineamientos establecidos.

#### **9.12. Reporte de eventos de seguridad de la información**

- Si un usuario final sospecha de una debilidad de seguridad, identifica una exposición inadecuada información de la Entidad, u observa un comportamiento anómalo con sus activos de información, deberá notificar inmediatamente a la Mesa de Servicio siguiendo el Procedimiento de Gestión de Incidentes
- El Oficial de Seguridad de la Información deberá llevar a cabo sesiones de capacitación y sensibilización a todos los funcionarios de la Entidad, acerca de la gestión de incidentes de seguridad de la información.

#### **9.13. Uso de credenciales de acceso**

- El usuario y la contraseña que se asignan para acceder a los sistemas y aplicaciones es personal e intransferible, no se deben compartir ni prestar.
- Se deben construir contraseñas seguras (difíciles para otras personas, fáciles de recordar)
- Las acciones ejecutadas con el usuario y contraseña son responsabilidad del servidor(a), contratista o tercero a quien fueron asignadas.
- El carné de acceso a las instalaciones es personal, no se debe prestar, ni permitir el acceso a otras personas con él.
- Se deben cambiar periódicamente las contraseñas.
- Se debe hacer uso de los mecanismos de doble factor de autenticación establecidos por la OTIC, donde sea requerido un mayor nivel de protección.
- Cualquier sospecha de riesgo de las credenciales de acceso se debe reportar como incidente de seguridad a la mesa de servicio.

#### **9.14. Uso de los Servicios de Red**

- Las tomas eléctricas ubicadas en las canaletas deberán ser usadas únicamente para la conexión de computadores, monitores o teléfonos IP. Los computadores deben ser conectados en las tomas de color naranja y en ninguna circunstancia se puede conectar otros elementos en dichas tomas.
- Dentro de las instalaciones de la UBPD, el uso de dispositivos externos de almacenamiento y conexión a Internet como módems, USB, cable módems, celulares, entre otros, está restringido.
- La UBPD dispone de redes institucionales y red de visitantes. Los equipos institucionales deben hacer uso de las redes institucionales para acceder a los servicios de red y la información, los invitados se deben conectar a la red de visitantes.

#### **9.15. Uso de Impresión y Otros Servicios**

- Se debe hacer uso racional del servicio de impresión.
- Los documentos que se impriman en las impresoras de la UBPD deben ser para el cumplimiento de las funciones laborales o de las obligaciones contractuales.
- Se debe conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- A cada usuario del servicio de impresión se le asigna un PIN o clave para que pueda hacer uso del servicio. Este PIN es personal e intransferible. Esto impedirá la pérdida de documentos impresos.
- Se debe recoger las impresiones inmediatamente.
- Al momento de realizar impresiones, fotocopiado o escaneo de documentos con información pública reservada o pública clasificada, se debe mantener control de la

impresora, por lo cual no se deberá dejar desatendida, preservando la confidencialidad de la información.

- Cuando sea posible se debe imprimir por las 2 caras.
- Se debe reutilizar el papel, excepto si tiene información clasificada.
- Al finalizar la jornada laboral se debe recopilar y asegurar la información.

#### **9.16. Uso del computador y puesto de trabajo**

- Los equipos portátiles deben permanecer asegurados con la guaya de seguridad.
- Se debe bloquear el equipo o apagarlo si se retira del puesto de trabajo.
- Se debe evitar la conexión a redes inalámbricas públicas o desconocidas.
- El puesto de trabajo debe permanecer organizado y protegida la información clasificada o reservada impresa.
- Se debe finalizar la sesión en todas las aplicaciones cuando termine de usarlas o al concluir el día.
- Cualquier configuración de los equipos de cómputo o mantenimiento debe ser realizada por la mesa de servicios.
- Se debe contar con autorización para el retiro de los equipos institucionales fuera de las instalaciones de la UBPD diligenciando el formato GRF-FT-009 Autorización Salida de Bienes de la Entidad.

#### **9.17. Uso de áreas seguras**

- Se prohíbe el consumo de alimentos o bebidas dentro de dichas zonas.
- Solo si hay autorización del líder del área se puede acceder a estas zonas.
- Se debe diligenciar la bitácora de ingreso a áreas seguras.
- Se requiere que los visitantes estén acompañados por un custodio de la zona segura.
- Solo personal autorizado puede acceder a los cuartos de racks de cableado o equipos de comunicaciones.
- Se prohíbe el ingreso de cámaras, equipos de video, almacenamiento, audio o similares, sin previa autorización y justificación.

#### **9.18. Protección de la información en ubicaciones fuera de la UBPD**

- No almacenar en los equipos asignados o personales información clasificada o reservada.
- Si se trata de tu equipo personal:
  - Mantener el sistema operativo y las aplicaciones actualizadas, licenciadas y con los últimos parches de seguridad instalados.
  - Instalar un software de antivirus
- No utilizar conexiones poco confiables (conexiones Wi-Fi abiertas, redes públicas de hoteles, bibliotecas, locutorios, aeropuertos, entre otros)
- Parametrizar el bloqueo automático por inactividad y en lo posible, almacenar la información en los recursos que la UBPD disponga.
- No está permitido que las sesiones remotas VPN establecidas con la UBPD sean utilizadas por una persona diferente al servidor(a) o contratista autorizado.
- Los equipos de cómputo no deben dejarse desatendidos, y se debe evitar transportar el equipo si no es necesario.
- Para el transporte entre la oficina y el lugar o lugares en que se ejecuten las funciones de trabajo en casa, es necesario disponer de un maletín que ofrezca buena resistencia a caídas, golpes, aplastamiento, líquidos u otro riesgo al que se encuentre expuesto el equipo portátil.

## 10. Sensibilización y Comunicación en Seguridad de la Información

La UBPD, a través de sus áreas de Talento Humano y Contratos, incluirá dentro de sus capacitaciones e inducciones las temáticas de seguridad de la información, con el objetivo de que cualquier servidor(a) y/o contratista que se vincule a la entidad tenga pleno conocimiento de las políticas de seguridad de la información, el Oficial de Seguridad de la Información apoyará en dichas inducciones.

## 11. Mejora

### 11.1. No conformidad y acción correctiva

Al presentarse una no conformidad, la UBPD dispone:

- Reacciona frente a la misma, disponiendo la acción para controlarla, corregirla y atender las consecuencias de ésta.
- Considera si es necesario y posible eliminar la causa de la no conformidad, mediante su revisión, determinación de las causas de la no conformidad y verificación de no conformidades similares.
- Implementa las acciones planeadas.
- Revisa la efectividad de las acciones realizadas.
- Realiza cambios sobre el SSI, si es requerido.

El manejo de estas condiciones para las acciones correctivas se encuentra especificado en el DPE-PR-011 V2 Acciones Preventivas, Correctivas y de Mejora. Estas acciones son acordes y proporcionales a las no conformidades que las originaron. Asimismo, se mantiene registro de las correcciones realizadas, en el DPE-FT-019 Acciones correctivas, preventivas y de mejora.

### 11.2. Mejora continua

Para realizar acciones de mejora continua sobre la idoneidad, adecuación y efectividad del SSI, la UBPD establece los lineamientos de Mejora Continua del SSI mencionados anteriormente.

## 12. Manejo de Desviaciones y Excepciones

Las desviaciones y excepciones que sean necesarias en la Gestión de la Seguridad de la Información serán manejadas teniendo en cuenta niveles aceptables de racionalidad, proporcionalidad y necesidad en el tratamiento de la información tanto a nivel interno como la que se obtenga o transfiera con otras entidades; así mismo se entiende que su manejo no podrá ejecutarse sobrepasando la normatividad que regula la materia, ni los principios y directrices establecidas en la GSI-PC-003 Política General de Seguridad de la Información.

Las excepciones a las políticas, procedimientos y controles en la Gestión de Protección y Seguridad Digital deben ser evaluadas por la Oficina de Tecnologías de la Información y Comunicaciones y el (la) Oficial de Seguridad de la Información, teniendo en cuenta:

- a. El evento que genera la excepción.
- c. El posible impacto que pueda generar la excepción.
- d. Las acciones para el manejo de la excepción.

De ser necesario, por el impacto que pueda generar en la operación de la UBPD, continuidad de los servicios, y en términos generales en el cumplimiento de la misionalidad, la situación de excepcionalidad deberá ser informada y escalada al Comité de Seguridad de la Información o quien haga sus veces.

### 13. Proceso Disciplinario o Sancionatorio

Todo incumplimiento a los lineamientos establecidos en la Política General de Seguridad de la Información (GSI-PC-003) o el Manual de Seguridad de la Información (GSI-MN-001) por parte de un servidor(a) o contratista, así como los procedimientos derivados de esta política, pueden dar lugar al inicio de acciones disciplinarias, con las consecuencias legales de que trata la Ley 1952 de 2019 modificada por la Ley 2094 de 2021. En todo caso estos casos serán trasladados y evaluados por la Secretaría General.

### 14. Anexos

#### Matriz de Roles y Responsabilidades

UBPD	Secretaría General	Secretaría Técnica	Unidad Especial de Información	Unidad Especial de Investigación	Unidad Especial de Asesoría y Apoyo	Unidad Especial de Atención al Ciudadano	Unidad Especial de Control Interno	Unidad Especial de Gestión de Recursos Humanos	Unidad Especial de Gestión de Tecnología	Unidad Especial de Gestión de Operaciones	Unidad Especial de Gestión de Proyectos	Unidad Especial de Gestión de Riesgos	Unidad Especial de Gestión de Seguridad	Unidad Especial de Gestión de Servicios	Unidad Especial de Gestión de Sistemas	Unidad Especial de Gestión de Soporte	Unidad Especial de Gestión de Talento Humano	Unidad Especial de Gestión de Transparencia	Unidad Especial de Gestión de Vigilancia
Apoyar los procesos de planeación, desarrollo e implementación de la Política de Seguridad de la Información	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Apoyar los procesos de planeación, desarrollo e implementación de la Política de Seguridad de la Información	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
Coordinar, controlar y evaluar el cumplimiento de la Política de Seguridad de la Información	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

<b>ELABORÓ:</b>	<b>16/05/2023</b>	<b>REVISÓ:</b>	<b>16/05/2023</b>	<b>APROBÓ:</b>	<b>01/06/2023</b>
<b>Nancy Mireya Barbosa R.,</b> Contratista; <b>Juan de Jesús Aponte</b> Buitrago, Experto Técnico 4.		<b>Diego Ramírez</b> Asesor Unidad Especial Oficial de Seguridad de la Información		<b>Diego Ramírez</b> Asesor Unidad Especial Oficial de Seguridad de la Información	

CONTROL DE CAMBIOS		
ASPECTOS QUE CAMBIARON EN EL DOCUMENTO	DETALLE DE LOS CAMBIOS EFECTUADOS	VERSIÓN
<i>No aplica</i>	Elaboración del documento primera versión.	001
<i>Se agregaron los lineamientos de acuerdo con cada control definido</i>	Se modificó el objetivo y el alcance. Se incluyen y actualizan los lineamientos registrados anteriormente en el documento SGI-PC-002 (SGSI) Política de protección y seguridad digital. Se comparte el documento a todos los responsables asociados al mismo, para socializar las responsabilidades con todos los involucrados. Asimismo, se toman las sugerencias que surgen al respecto.	002